Сервис резервного копирования

Version 7.5

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

Редакция: 29.08.2017

Содержание

1 О сервисе резервного копирования

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

Для управления этой службой применяется веб-интерфейс, который называется консолью резервного копирования.

2 Требования к программному обеспечению

2.1 Поддерживаемые веб-браузеры

Веб-интерфейс сервиса резервного копирования поддерживает перечисленные ниже браузеры:

- Google Chrome 29 или более поздней версии
- Mozilla Firefox 23 или более поздней версии
- Opera 16 или более поздней версии
- Windows Internet Explorer 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.

2.2 Поддерживаемые операционные системы и среды

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 и 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 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 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
- 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
- CentOS 5.x, 6.x, 7, 7.1, 7.2, 7.3
- 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

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 — Apple File System (APFS) не поддерживается

Агент для VMware

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.

VMware ESXi 4.1, 5.0, 5.1, 5.5, 6.0, 6.5

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

Агент для Virtuozzo

Virtuozzo 6.0.10

2.3 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

2.4 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. Восстановление почтовых ящиков и элементов почтового ящика поддерживается, начиная с пакета обновления 1 (SP1).
- **Microsoft Exchange Server 2007** — все выпуски, все пакеты обновления. Восстановление почтовых ящиков и элементов почтовых ящиков не поддерживается.

2.5 Поддерживаемые версии Microsoft SharePoint

Backup Service 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.

2.6 Поддерживаемые платформы виртуализации

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

Платформа	Резервное копирование на уровне гипервизора (резервное копирование без агента)	Резервное копирование изнутри гостевой ОС
VMware		
Версии VMware vSphere: 4.1, 5.0, 5.1, 5.5, 6.0, 6.5 **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		

Платформа	Резервное копирование на уровне гипервизора (резервное копирование без агента)	Резервное копирование изнутри гостевой ОС
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
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		+
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		+
Virtuozzo		
Virtuozzo 6.0.10, 6.0.11	+	(Только виртуальные машины. Контейнеры не поддерживаются)
Amazon		

Платформа	Резервное копирование на уровне гипервизора (резервное копирование без агента)	Резервное копирование изнутри гостевой ОС
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. 40).
  - 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.

2.7 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.

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

3 Поддержка файловых систем

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

<table>
<tr><th rowspan="2">Файловая система</th><th colspan="3">Поддержка</th><th rowspan="2">Ограничения</th></tr>
<tr><th>Агенты</th><th>Загрузочные носители для Windows и Linux</th><th>Загрузочный носитель для Mac</th></tr>
<tr><td>FAT16/32</td><td rowspan="3">Все агенты</td><td>+</td><td>+</td><td rowspan="4">Без ограничений</td></tr>
<tr><td>NTFS</td><td>+</td><td>+</td></tr>
<tr><td>ext2/ext3/ext4</td><td>+</td><td>-</td></tr>
<tr><td>HFS+</td><td>Агент для Mac</td><td>-</td><td>+</td></tr>
<tr><td>JFS</td><td>Агент для Linux</td><td>+</td><td>-</td><td>Файлы невозможно исключить из</td></tr>
</table>

<table>
<tr><th rowspan="2">Файловая система</th><th colspan="3">Поддержка</th><th rowspan="2">Ограничения</th></tr>
<tr><th>Агенты</th><th>Загрузочные носители для Windows и Linux</th><th>Загрузочный носитель для Mac</th></tr>
<tr><td>ReiserFS3</td><td rowspan="2"></td><td>+</td><td>-</td><td>резервной копии диска</td></tr>
<tr><td>ReiserFS4</td><td>+</td><td>-</td><td rowspan="3">▪ Файлы невозможно исключить из резервной копии диска
▪ Невозможно изменить размер томов при выполнении восстановления</td></tr>
<tr><td>ReFS</td><td rowspan="2">Все агенты</td><td>+</td><td>+</td></tr>
<tr><td>XFS</td><td>+</td><td>+</td></tr>
<tr><td>Linux SWAP</td><td>Агент для Linux</td><td>+</td><td>-</td><td>Без ограничений</td></tr>
</table>

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.

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.

5 Доступ к сервису резервного копирования

После активации учетной записи вы сможете войти в сервис резервного копирования.

Порядок входа в сервис резервного копирования

1. Откройте страницу входа в сервис резервного копирования. Адрес страницы входа был указан в сообщении электронной почты со сведениями об активации.

2. Введите имя пользователя и щелкните **Продолжить**.
3. Введите пароль и щелкните **Вход**.
4. Если в сервисе резервного копирования вы имеете роль администратора, щелкните **Резервное копирование и аварийное восстановление**.

   Пользователи без роли администратора входят непосредственно на эту консоль резервного копирования.

Можно изменить язык веб-интерфейса, щелкнув значок в виде фигуры человека в верхнем правом углу.

Администраторы могут переключаться между консолью резервного копирования и порталом управления. Чтобы получить доступ к консоли резервного копирования с портала управления, на вкладке **Обзор** найдите раздел **Резервное копирование и восстановление** и щелкните **Управление службой**. Для доступа к порталу управления с консоли резервного копирования щелкните **Управление учетными записями** в верхнем левом углу.

6 Установка программного обеспечения

6.1 Подготовка

Шаг 1

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, что агент для Windows устанавливается вместе с агентом для Exchange, агентом для SQL, агентом для VMware, агентом для Hyper-V и агентом для Active Directory. 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?
Физические машины		
Физические машины под управлением Windows	Агент для Windows	На машину, резервная копия которой будет создана.
Физические машины под управлением ОС Linux	Агент для Linux	
Физические машины под управлением OS X	Агент для Mac	
Приложения		
Базы данных SQL	Агент для SQL	На машину с сервером Microsoft SQL Server.
Базы данных Exchange	Агент для Exchange	На машину с ролью почтового ящика Microsoft Exchange Server.

Для каких объектов нужно создать резервные копии?	Какой агент следует установить?	Куда его следует установить?
Почтовые ящики Microsoft Office 365	Агент для Office 365	На машину с Windows, которая подключена к Интернету. В зависимости от настроек, выбранных поставщиком услуг, может потребоваться установка агента для Office 365. Дополнительную информацию см. в теме "Защита почтовых ящиков Office 365" (стр. 105).
Машины с доменными службами Active Directory	Агент для Active Directory	На контроллер домена.
Виртуальные машины		
Виртуальные машины VMware ESXi	Агент для VMware	На машину под управлением Windows с сетевым доступом к vCenter Server и хранилищу виртуальных машин.*
Виртуальные машины Hyper-V	Агент для Hyper-V	На хост Hyper-V.
Виртуальные машины и контейнеры Virtuozzo	Агент для Virtuozzo	На хосте Virtuozzo.
Виртуальные машины, размещенные в Amazon EC2	То же самое, что и для физических машин**	На машину, резервная копия которой будет создана.
Виртуальные машины в среде Windows Azure		
Виртуальные машины на хосте Citrix XenServer		
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 «Агент для VMware — резервное копирование без использования локальной сети» (стр. 121).

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

Шаг 2

Проверьте требования к системе для агентов.

Агент	Место на диске, занимаемое агентами
Агент для Windows	550 МБ
Агент для Linux	500 МБ
Агент для Mac	450 МБ
Агент для SQL	600 МБ (50 МБ + 550 МБ для агента для Windows)
Агент для Exchange	750 МБ (200 МБ + 550 МБ для агента для Windows)
Агент для Office 365	550 МБ
Агент для Active Directory	600 МБ (50 МБ + 550 МБ для агента для Windows)
Агент для VMware	700 МБ (150 МБ + 550 МБ для агента для Windows)
Агент для Hyper-V	600 МБ (50 МБ + 550 МБ для агента для Windows)
Агент для Virtuozzo	500 МБ

Как правило, агент использует 300 МБ помимо памяти, потребляемой операционной системой и запущенными приложениями. Максимальное потребление памяти может достигать 2 ГБ в зависимости от объема и типа данных, обрабатываемых агентами.

Шаг 3

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

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

Чтобы сохранить программы установки локально, загрузите пакет со всеми агентами для установки в Windows по ссылке в нижней части страницы **Добавить устройства**. Доступны 32-разрядный и 64-разрядный пакеты. Эти пакеты позволяют настроить список компонентов для установки. С помощью этих пакетов также можно настроить автоматическую установку (например, с использованием групповой политики). Эта процедура для опытных пользователей описана в Руководстве администратора (стр. 23).

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 4

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. 18), который поможет понять, нужно ли конфигурировать эти настройки на каждой машине с запущенным агентом резервного копирования.

6.2 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
```

6.3 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.

6.4 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. 124) 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.

6.5 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**.

6.6 Обновление агентов

Агенты указанных ниже версий можно обновить через веб-интерфейс.

- Агент для Windows, агент для VMware, агент для Hyper-V — 11.9.191 и более поздние версии
- Агент для Linux — 11.9.179 и более поздние версии
- Другие агенты: можно обновить любую версию

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

Если администратором сервиса резервного копирования включено автоматическое обновление, то при выпуске новой версии агенты обновляются автоматически. Если автоматическое обновление отключено или по какой-либо причине его не удалось выполнить, используйте описанную ниже процедуру.

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

Обновление агента через веб-интерфейс

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

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

   Ход обновления отображается в столбце состояния для каждой машины.

6.7 Удаление агентов

В Windows

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

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

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

   Если планируется установить агент снова, не устанавливайте этот флажок. 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 **/usr/lib/Acronis/BackupAndRecovery/uninstall/uninstall**.

2. [Необязательно] Установите флажок **Удалить все элементы трассировки продукта (журналы, задания, хранилища, параметры конфигурации продукта)**.

   Если планируется установить агент снова, не устанавливайте этот флажок. Если установить флажок, 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**.

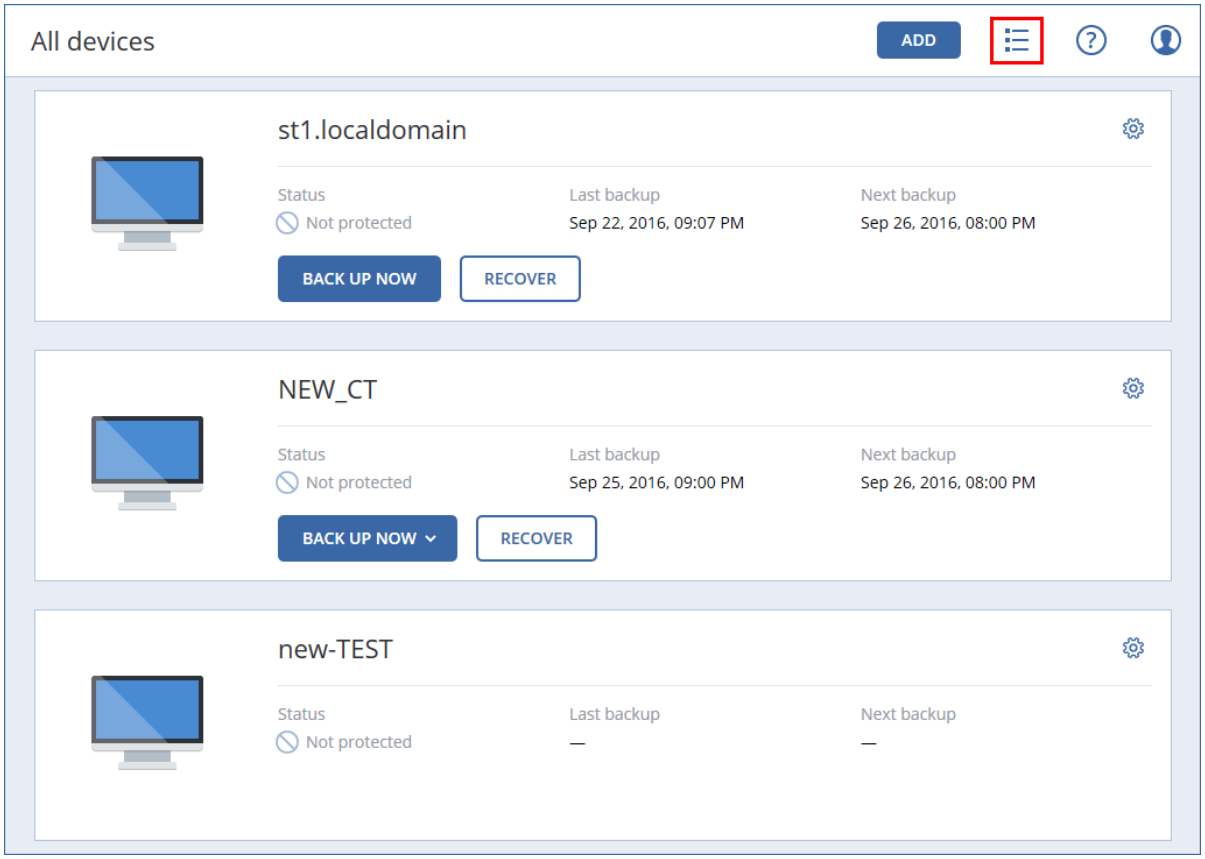
В OS X

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**.

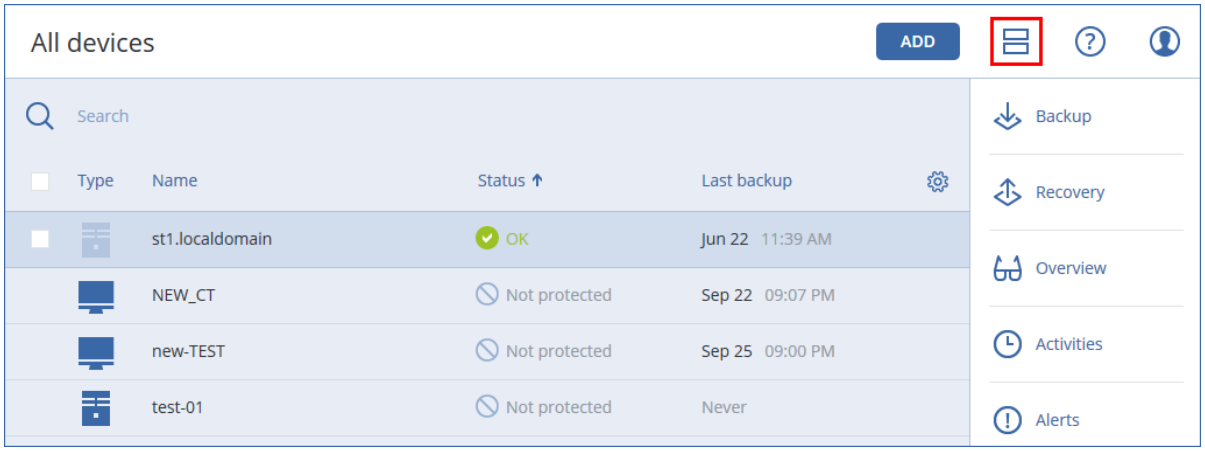
7 Представления консоли резервного копирования

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.

8 Резервная копия

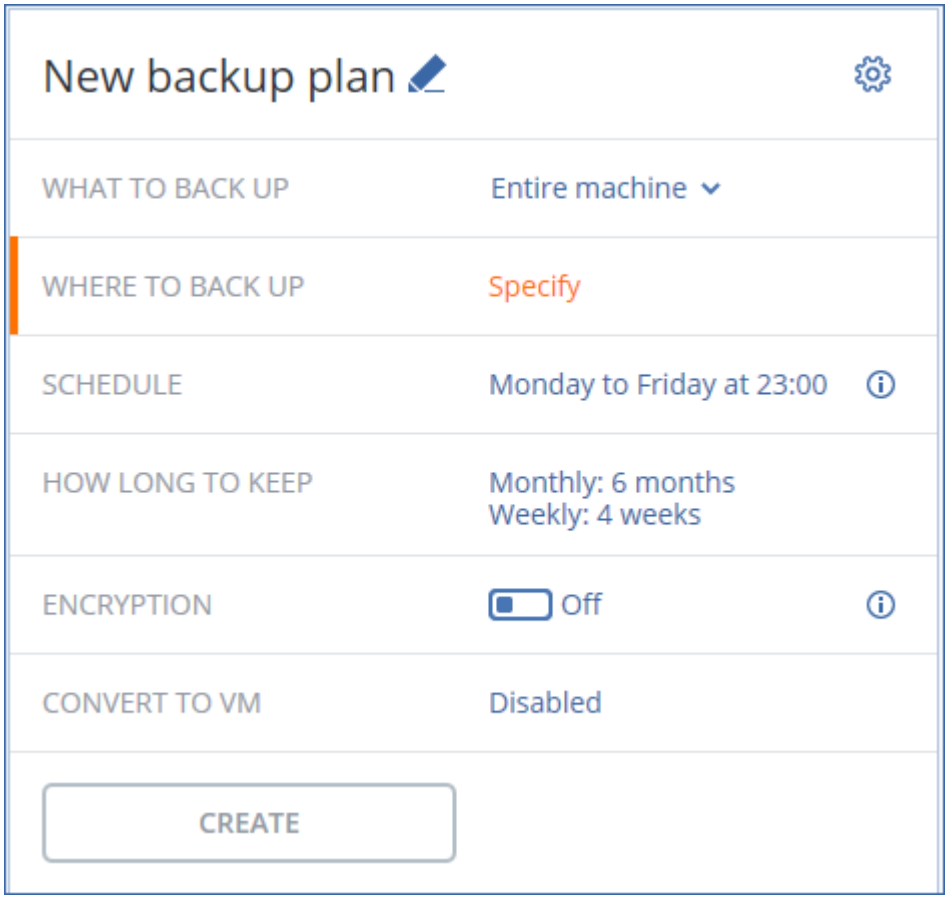
План резервного копирования —это набор правил, который определяет порядок защиты данных на соответствующей машине.

План резервного копирования можно применить к нескольким машинам на этапе его 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.

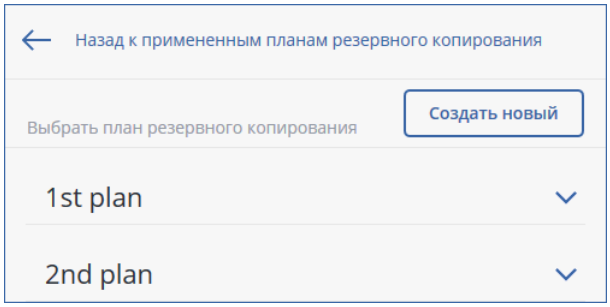


3. [Необязательно] Чтобы изменить имя плана резервного копирования, щелкните имя по умолчанию.
4. Необязательно: чтобы изменить параметры плана, щелкните соответствующий раздел на его панели.
5. [Необязательно] Чтобы изменить параметры резервного копирования, щелкните значок шестеренки.
6. Нажмите кнопку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

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**.

8.1 План резервного копирования: памятка

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. 30) Правила политики (стр. 30) Фильтры файлов (стр. 49)	Облако (стр. 35) Локальная папка (стр. 35) Сетевая папка (стр. 35) NFS (стр. 35)* Зона безопасности (стр. 35)**	Всегда инкрементное (один файл) (стр. 38) Всегда полное (стр. 38) Еженедельно полное, ежедневно инкрементное (стр. 38) Настраиваемый вариант (П-Д-И) (стр. 38)	По возрасту резервной копии (одно правило на набор резервных копий) (стр. 39) По количеству резервных копий (стр. 39) Хранить бессрочно (стр. 39)
Диски/тома (виртуальные машины)	Правила политики (стр. 30) Фильтры файлов (стр. 49)	Облако (стр. 35) Локальная папка (стр. 35) Сетевая папка (стр. 35) NFS (стр. 35)*		
Файлы (только физические машины):	Непосредственный выбор (стр. 33) Правила политики (стр. 33) Фильтры файлов (стр. 49)	Облако (стр. 35) Локальная папка (стр. 35) Сетевая папка (стр. 35) NFS (стр. 35)* Зона безопасности (стр. 35)**	Всегда полное (стр. 38) Еженедельно полное, ежедневно инкрементное (стр. 38) Настраиваемый вариант (П-Д-И) (стр. 38)	
Конфигурация ESXi	Непосредственный выбор (стр. 35)	Локальная папка (стр. 35) Сетевая папка (стр. 35) NFS (стр. 35)*		

Веб-сайты (файлы и базы данных MySQL)	Непосредственный выбор (стр. 110)	Облако (стр. 35)	—	
Состояние системы	Непосредственный выбор (стр. 34)	Облако (стр. 35) Локальная папка (стр. 35) Сетевая папка (стр. 35)	Всегда полное (стр. 38) Еженедельно полное, ежедневно инкрементное (стр. 38) Настраиваемый вариант (П-И) (стр. 38)	
Базы данных SQL	Непосредственный выбор (стр. 94)			
Базы данных Exchange	Непосредственный выбор (стр. 95)			
Почтовые ящики Office 365	Непосредственный выбор (стр. 107)		Всегда инкрементное (один файл) (стр. 38)	

* Резервное копирование в общие папки NFS недоступно в Windows.

** Невозможно создать Зону безопасности на компьютере Mac.

8.2 Выбор данных для резервного копирования

8.2.1 Выбор дисков и томов

Резервная копия диска содержит копию диска или тома в запакованном виде. Из такой копии можно восстановить отдельные диски, тома или файлы. Резервная копия всей машины 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. 49).

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.

8.2.1.1 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. 59) **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. 59)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.

8.2.2 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. 49).

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.
   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 OS X

- 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**.

8.2.3 Выбор состояния системы

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

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

В резервную копию состояния системы включаются файлы перечисленных ниже компонентов.

- Конфигурация планировщика задач
- Хранилище метаданных VSS
- Конфигурация счетчика производительности
- Служба MSSearch

- Фоновая интеллектуальная служба передачи (BITS)
- Реестр
- Инструментарий управления Windows (WMI)
- База данных регистрации классов служб компонентов

8.2.4 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. Последовательно выберите пункты **VMware** > **Хосты и кластеры**.
2. Перейдите к хостам ESXi, для которых требуется создать резервные копии.
3. Выберите хосты ESXi и щелкните **Резервное копирование**.
4. В поле **Выбор данных**, выберите **Конфигурация ESXi**.
5. В поле **Пароль пользователя root ESXi** укажите пароль для учетной записи root на каждом выбранном хосте или примените один пароль ко всем хостам.

8.3 Выбор места назначения

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

- **Облачное хранилище**

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

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

  Если выбрано несколько машин, введите путь к папке. Резервные копии будут сохраняться в этой папке на каждой из выбранных физических машин либо на машине, на которой установлен агент для виртуальных машин. Если папка не существует, она будет создана.
- **Сетевая папка**

  Это папка, общий доступ к которой предоставлен посредством SMB/CIFS/DFS.

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

  - Для общих папок SMB/CIFS: `\\<имя_хоста>\<путь>\` или `smb://<имя_хоста>/<путь>/`

- Для папок DFS: `\\<полное доменное имя DNS>\<корневой каталог DFS>\<путь>`
  Например, `\\example.company.com\shared\files`

После этого нажмите кнопку со стрелкой. Если потребуется, укажите имя пользователя и пароль для доступа к общей папке.

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

  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. 36).

8.3.1 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. 129). 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**.

Создание раздела Зона безопасности

1. Определите диск, на котором необходимо создать раздел Зона безопасности.
2. Чтобы просмотреть номер диска, запустите интерфейс командной строки и введите **`acrocmd list disks`**.
3. Воспользуйтесь командой **`create asz`** утилиты **`acrocmd`**. Эта команда сначала использует перераспределенное пространство на этом диске. Если этого пространства недостаточно, берется свободное пространство с указанных томов. Подробную информацию см. в разделе «Преобразование диска в результате создания раздела Зона безопасности» ниже.

   Примеры:

   - Создание раздела Зона безопасности на диске 1 локальной машины. Будет создан раздел Зона безопасности с размером по умолчанию, который определяется как среднее значение между максимальным (размер всего нераспределенного пространства) и минимальным (около 50 МБ) значениями.

     ```
     acrocmd create asz --disk=1
     ```

   - Создание защищенного паролем раздела Зона безопасности размером 100 ГБ на диске 2 локальной машины. Если нераспределенного пространства недостаточно, пространство будет взято со второго тома этого диска.

     ```
     acrocmd create asz --disk=2 --volume=2-2 --asz_size=100gb --password=abc12345
     ```

   - Создание раздела Зона безопасности размером 20 ГБ на диске 1 удаленной машины.

     ```
     acrocmd create asz --host=192.168.1.2 --credentials=john,pass1 --disk=1
     --asz_size=20gb
     ```

   Подробное описание команды **`create asz`** см. в справке по командной строке.

Преобразование диска в результате создания раздела Зона безопасности

- Раздел Зона безопасности всегда создается в конце жесткого диска. При вычислении окончательной разметки томов программа сначала будет использовать нераспределенное пространство в конце.
- Если в конце диска незанятого пространства нет или недостаточно, но существует незанятое пространство между томами, то эти тома будут перемещены, чтобы добавить больше незанятого пространства к концу.
- Если все незанятое пространство собрано, но его не хватает, то программа заберет свободное пространство из томов по выбору, пропорционально уменьшив их размер. Изменение размера заблокированных томов может потребовать перезагрузки.
- 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.

8.4 Расписание

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.

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. 129).

  Эта схема недоступна при выполнении резервного копирования в Зону безопасности.
- **Всегда полное**

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

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

  Каждый раз создаются полные резервные копии.
- **Еженедельно полное, ежедневно инкрементное**

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

  Раз в неделю создается полная резервная копия. Остальные копии будут инкрементными. Время создания полной резервной копии определяется параметром **Еженедельное резервное копирование** (щелкните значок шестеренки и выберите **Параметры резервного копирования** > **Еженедельное резервное копирование**).
- **Пользовательские**

  Задайте расписания для полных, дифференциальных и инкрементных резервных копий.

  Дифференциальное резервное копирование не выполняется для данных SQL, Exchange и состояния системы.

Дополнительные параметры расписания

Для каждого места назначения можно 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. 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**. Этот параметр включен по умолчанию с максимальной задержкой 30 минут.*

8.5 Правила хранения

1. Щелкните **Время 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. 129). 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.
   - **Хранить резервные копии неопределенно долго**

Примечание. *Резервную копию, которая хранится в локальной или сетевой папке, невозможно удалить, если у нее есть зависимые резервные копии, не подлежащие удалению. Такая цепочка будет удалена полностью только тогда, когда закончится срок хранения всех входящих в нее резервных копий. Для хранения резервных копий, удаление которых отложено, требуется дополнительное место на диске. Кроме того, возраст и количество резервных копий могут превышать указанные вами значения.*

8.6 Репликация

Если включить репликацию резервных копий, то каждая резервная копия копируется во второе хранилище сразу же после создания. Если репликации ранее созданных резервных копий не выполнялась (например, было утрачено сетевое подключение), то программа также выполнит репликацию всех резервных копий, которые появились 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

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

- Локальная папка
- Сетевая папка
- Облачное хранилище данных

Порядок включения репликации резервных копий

1. На панели плана резервного копирования включите переключатель **Реплицировать резервные копии**.

   Этот переключатель отображается только в том случае, если поддерживается репликация из расположения, выбранного в поле **Место сохранения**.
2. В поле **Место для репликации** укажите место назначения репликации, как описано в разделе «Выбор места назначения» (стр. 35).
3. В поле **Срок хранения** укажите правила хранения, как описано в разделе «Правила хранения» (стр. 39).

8.7 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.
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.

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.

После сохранения настроек их нельзя изменить, но их можно сбросить, как описано ниже.

Эта возможность доступна только машин Windows или Linux. Она не поддерживается для OS X.

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.

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 он устанавливается в каталог **%ProgramFiles%\BackupClient**.

- В Linux: **/usr/sbin/acropsh -m manage_creds --set-password** <пароль_шифрования>

Резервные копии будут зашифрованы с использованием алгоритма AES и 256-разрядного ключа.

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 он устанавливается в каталог **%ProgramFiles%\BackupClient**.
   - В Linux: **/usr/sbin/acropsh -m manage_creds --reset**

Внимание! *После сброса настроек шифрования на машине, резервные копирования этой машины не будут выполняться. Чтобы продолжить резервное копирование машины, создайте новый план резервного копирования.*

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.

8.8 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. На панели плана резервного копирования нажмите кнопку **Запустить сейчас**.

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

8.9 Параметры резервного копирования

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, OS X).
- 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	OS X	Windows	Linux	OS X	ESXi	Hyper-V	Virtuozzo	Windows
Оповещения (стр. 46)	+	+	+	+	+	+	+	+	+	+
Консолидация резервных копий (стр. 46)	+	+	+	+	+	+	+	+	+	-
Проверка резервных копий (стр. 47)	+	+	+	+	+	+	+	+	+	+
Функция Changed Block Tracking (CBT) (стр. 47)	+	-	-	-	-	-	+	+	-	-
Уровень сжатия (стр. 47)	+	+	+	+	+	+	+	+	+	+
Обработка ошибок (стр. 48)										
В случае ошибки повторить попытку	+	+	+	+	+	+	+	+	+	+
Не отображать во время работы сообщения и диалоговые окна (режим без вывода сообщений)	+	+	+	+	+	+	+	+	+	+
Пропуск поврежденных секторов	+	+	+	+	+	+	+	+	+	-

	Резервное копирование на уровне дисков			Резервное копирование на уровне файлов			Виртуальные машины			SQL и Exchange
	Windows	Linux	OS X	Windows	Linux	OS X	ESXi	Hyper-V	Virtuozzo	Windows
Повтор попытки в случае ошибки при создании моментального снимка виртуальной машины	-	-	-	-	-	-	+	+	+	-
Быстрое инкрементное/ дифференциальное резервное копирование (стр. 49)	+	+	+	-	-	-	-	-	-	-
Моментальные снимки резервных копий на уровне файлов (стр. 50)	-	-	-	+	+	+	-	-	-	-
Безопасность на уровне файлов (стр. 51)	-	-	-	+	-	-	-	-	-	-
Фильтры файлов (стр. 49)	+	+	+	+	+	+	+	+	+	-
Сокращение журнала (стр. 51)	-	-	-	-	-	-	+	+	-	Только SQL
Создание моментальных снимков LVM (стр. 52)	-	+	-	-	-	-	-	-	-	-
Точки подключения (стр. 52)	-	-	-	+	-	-	-	-	-	-
Многотомные моментальные снимки (стр. 53)	+	-	-	+	-	-	-	-	-	-
Производительность (стр. 53)	+	+	+	+	+	+	+	+	+	+

	Резервное копирование на уровне дисков			Резервное копирование на уровне файлов			Виртуальные машины			SQL и Exchange
	Windows	Linux	OS X	Windows	Linux	OS X	ESXi	Hyper-V	Virtuozzo	Windows
Команды до и после процедуры (стр. 54)	+	+	+	+	+	+	+	+	+	+
Команды до и после захвата данных (стр. 56)	+	+	+	+	+	+	-	-	-	+
Планирование (стр. 58)										
Распределять время запуска по доступному времени	+	+	+	+	+	+	+	+	+	+
Ограничить число одновременно выполняющихся операций резервного копирования	-	-	-	-	-	-	+	+	+	-
Посекторное резервное копирование (стр. 59)	+	+	-	-	-	-	+	+	+	-
Разбиение (стр. 59)	+	+	+	+	+	+	+	+	+	+
Действия при сбое задания (стр. 59)	+	+	+	+	+	+	+	+	+	+
Служба теневого копирования томов (VSS) (стр. 59)	+	-	-	+	-	-	-	+	-	+
Служба теневого копирования томов (VSS) для виртуальных машин (стр. 61)	-	-	-	-	-	-	+	+	-	-

	Резервное копирование на уровне дисков			Резервное копирование на уровне файлов			Виртуальные машины			SQL и Exchange
	Windows	Linux	OS X	Windows	Linux	OS X	ESXi	Hyper-V	Virtuozzo	Windows
Еженедельное резервное копирование (стр. 61)	+	+	+	+	+	+	+	+	+	+
Журнал событий Windows (стр. 61)	+	-	-	+	-	-	+	+	-	+

8.9.1 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.

8.9.2 Консолидация резервной копии

Этот параметр применим для следующих схем резервного копирования: **Всегда полное**, **Еженедельно полное, ежедневно инкрементное** и **Пользовательские**.

Значение по умолчанию: **Отключено**.

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

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

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

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

8.9.3 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. 113) в среде ESXi или Hyper-V.

8.9.4 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.

8.9.5 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.

8.9.6 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.

8.9.7 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.

8.9.8 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 дисков, если 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 ОС Linux или OS X).

  Как в Windows, так и в Linux или OS X в пути к файлу или папке можно использовать прямую 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 знаков * 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**

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.*

8.9.9 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.

8.9.10 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. 79) параметров безопасности. Результат будет тот же — файлы будут наследовать разрешения от родительской папки.

8.9.11 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.

8.9.12 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.

8.9.13 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. 80).
- 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. 80).

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. 80).

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**.

8.9.14 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. 50) 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.

8.9.15 Производительность

Приоритет процесса

Этот параметр определяет приоритет процесса резервного копирования в операционной системе.

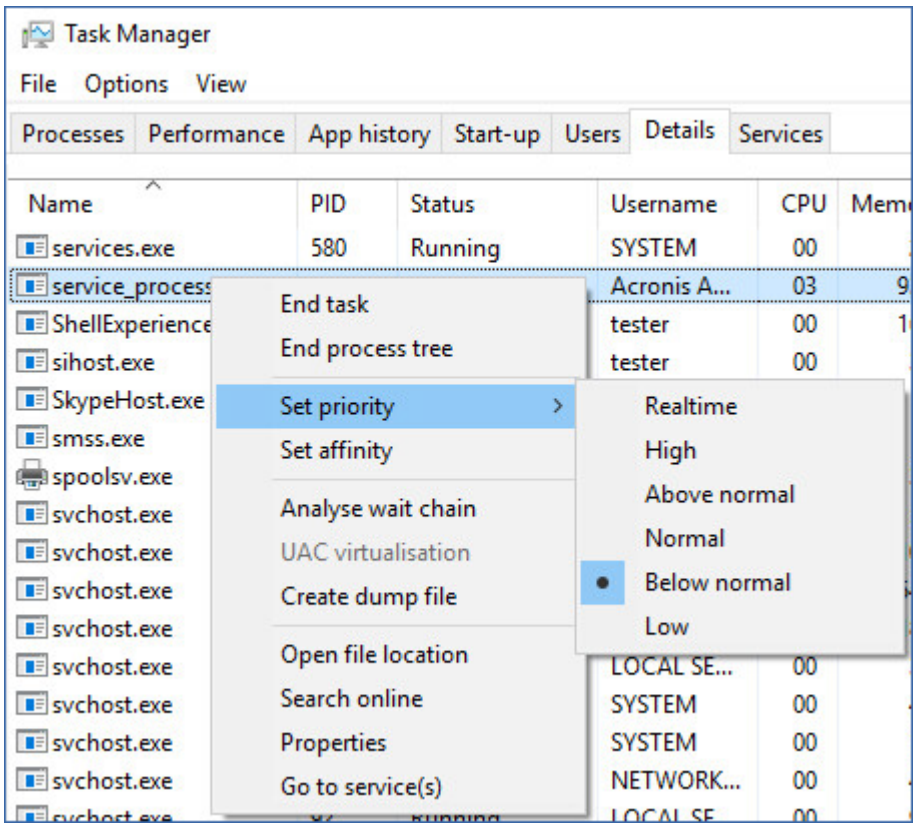
Доступные значения: **Низкий**, **Обычный**, **Высокий**.

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.

8.9.16 Команды до и после процедуры

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

Следующая схема иллюстрирует порядок выполнения команд до и после процедуры.

Команда до резервного копирования	Резервная копия	Команда после резервного копирования

Примеры использования команд до и после процедуры:

- Удаление некоторых временных файлов с диска до начала резервного копирования.

- Настройка антивирусной программы стороннего производителя для запуска до начала резервного копирования.
- Выборочное копирование резервных копий в другое хранилище. 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).

8.9.16.1 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 команды*	Установить	Снять	Установить	Снять
Не продолжать создание резервной копии до завершения выполнения команды	Установить	Установить	Снять	Снять
Результат				
	Предустановка Выполнить резервное копирование только после успешного выполнения команды. Прерывать резервное копирование при сбое команды.	Выполнить резервное копирование после команды независимо от результатов ее выполнения (успешно или ошибка).	Н/Д	Выполнить резервное копирование одновременно с выполнением команды и независимо от результатов выполнения команды.

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

8.9.16.2 Команда после резервного копирования

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

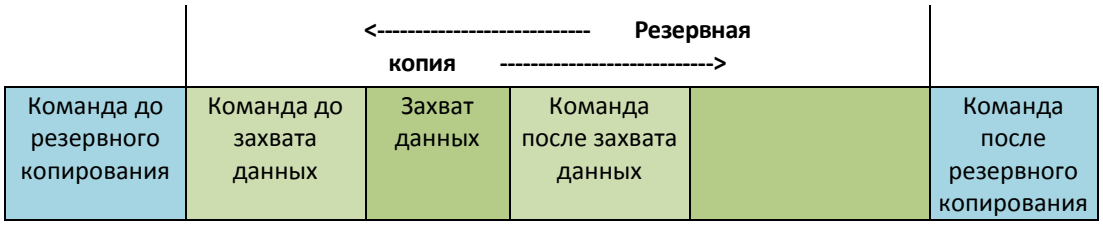
1. Включить переключатель **Выполнение команды после резервного копирования**.
2. В поле **Команда...** введите команду или выберите пакетный файл.
3. В поле **Рабочая папка** укажите путь к папке, в которой будет выполняться команда или пакетный файл.
4. В поле **Аргументы** укажите при необходимости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

8.9.17 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. 59) «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.

8.9.17.1 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.

8.9.17.2 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.

8.9.18 Планирование

Этот параметр определяет, запускаются ли процессы резервного копирования по расписанию или с задержкой, а также количество виртуальных машин, для которых резервное копирование выполняется одновременно.

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

Можно выбрать один из следующих вариантов:

- **Начинать все операции резервного копирования строго по расписанию**

  Резервное копирование физических машин запустится точно в соответствии с расписанием. Резервные копии виртуальных машин будут создаваться поочередно.

- **Распределять время запуска по доступному времени**

  Резервные копии физических машин будут запущены с задержкой от запланированного времени. Значение задержки для каждой машины выбирается случайно и находится в диапазоне от нуля до максимального значения, которое вы укажете. Параметр может быть полезен для резервного копирования нескольких машин в сетевое хранилище, чтобы избежать чрезмерной загрузки сети. Продолжительность задержки для каждой машины определяется при применении плана 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.

8.9.19 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. 47) задано значение **Отсутствует**). Программное обеспечение автоматически перейдет к посекторному резервному копированию для дисков с нераспознанными или неподдерживаемыми файловыми системами.

8.9.20 Разбиение

Этот параметр применим для следующих схем резервного копирования: **Всегда полное**, **Еженедельно полное, ежедневно инкрементное** 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.

8.9.21 Обработка ошибок задания

Этот параметр определяет поведение программы при сбое плана резервного копирования.

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**.

8.9.22 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. 56), 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. 51).

8.9.23 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. 48), 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.

8.9.24 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**.

8.9.25 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**.

9 Восстановление

9.1 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. 63) Использование загрузочного носителя (стр. 68)
Физическая машина (Mac)	Использование загрузочного носителя (стр. 68)
Виртуальная машина (VMware или Hyper-V)	Использование веб-интерфейса (стр. 66) Использование загрузочного носителя (стр. 68)
Виртуальная машина или контейнер (Virtuozzo)	Использование веб-интерфейса (стр. 66)
Конфигурация ESXi	Использование загрузочного носителя (стр. 76)
Файлы и папки	Использование веб-интерфейса (стр. 71) Загрузка файлов из облачного хранилища данных (стр. 72) Использование загрузочного носителя (стр. 74) Извлечение файлов из локальных резервных копий (стр. 75)
Состояние системы	Использование веб-интерфейса (стр. 76)
Базы данных SQL	Использование веб-интерфейса (стр. 97)
Базы данных Exchange	Использование веб-интерфейса (стр. 100)
Почтовые ящики Exchange	Использование веб-интерфейса (стр. 102)
Почтовые ящики Office 365	Использование веб-интерфейса (стр. 107)
Веб-сайты	Использование веб-интерфейса (стр. 112)

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.

9.2 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 такого носителя — 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. Для восстановления OS X потребуется создать отдельный загрузочный носитель на машине под управлением OS X.

Создание загрузочного носителя в Windows и Linux

1. Загрузите ISO-файл загрузочного носителя. Чтобы загрузить данный файл, выберите машину, затем выберите пункты **Восстановление** > **Другие способы восстановления...** > **Загрузить ISO-образ**.
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 машины с BIOS —`Win32DiskImager`. В Linux можно воспользоваться утилитой `dd`.
   - Подключите ISO-файл в качестве CD/DVD-дисковода к виртуальной машине, которую требуется восстановить.

Создание загрузочного носителя в OS X

1. На машине с установленным агентом для Mac щелкните **Приложения** > **Мастер создания загрузочных носителей**.
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.

9.3 Восстановление машины

9.3.1 Физическая машина

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

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

- систему OS X;
- любую операционную систему на «голое железо» либо на отключенной машине.

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.

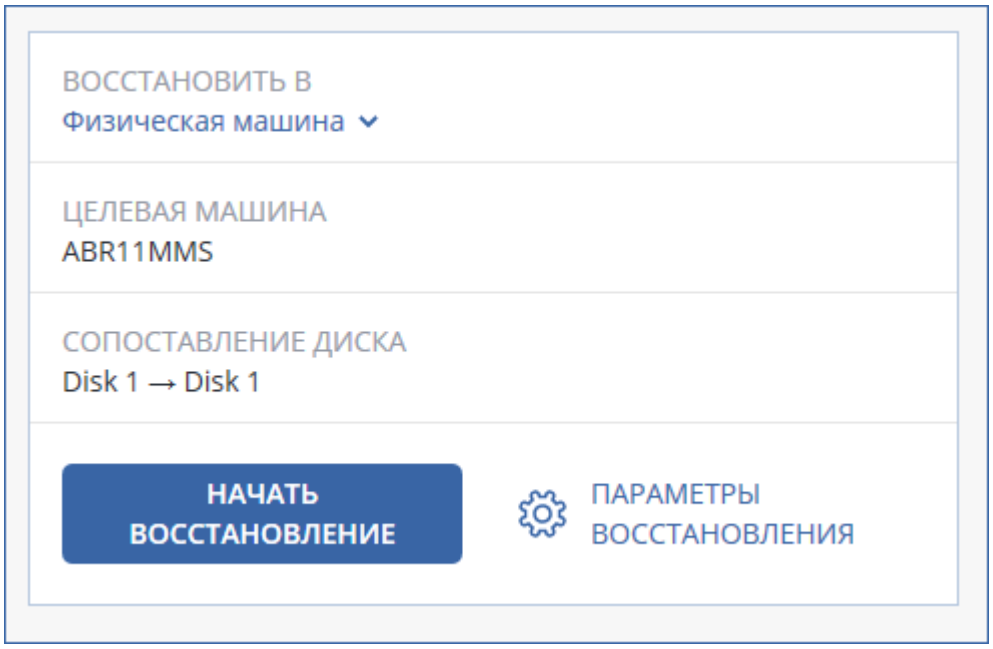
   Если машина отключена, точки восстановления не отображаются. Выполните любое из следующих действий:

- 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. 83).
- Восстановите машину, как описано в теме «Восстановление дисков с помощью загрузочного носителя» (стр. 68).

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.
   - Если выполнить сопоставление не удалось, воспользуйтесь процедурой, которая описана в разделе «Восстановление дисков с помощью загрузочного носителя» (стр. 68). С помощью загрузочного носителя можно выбрать диски для восстановления и вручную сопоставить их.



5. Нажмите кнопку **Запуск восстановления**.
6. Подтвердите перезапись дисков версиями из резервной копии. Укажите, следует ли автоматически перезапустить машину.

Ход восстановления отображается на вкладке **Действия**.

9.3.2 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. 120).

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.

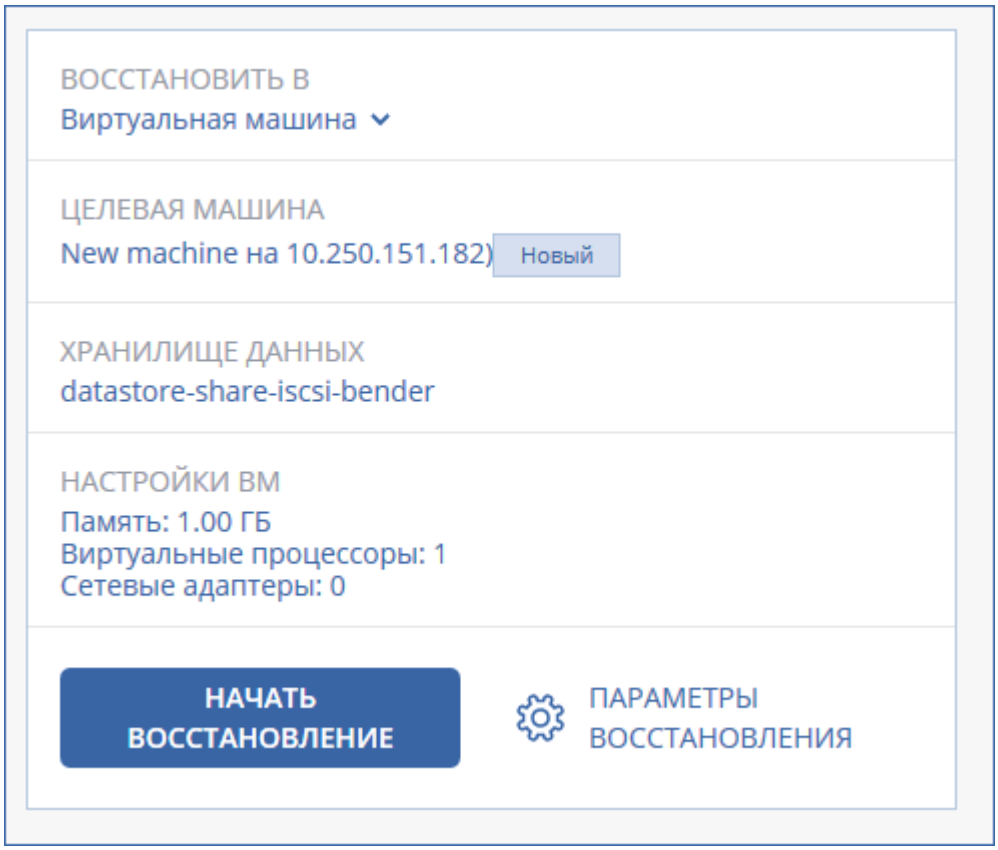
   Если машина отключена, точки восстановления не отображаются. Выполните любое из следующих действий:

   - 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. 83).
   - Восстановите машину, как описано в теме «Восстановление дисков с помощью загрузочного носителя» (стр. 68).
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.

- 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**.

9.3.3 Виртуальная машина

В ходе восстановления данных на виртуальную машину она должна быть остановлена. Программа останавливает ее без предупреждения. После завершения восстановления машину потребуется запустить вручную.

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

Восстановление виртуальной 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. 83).
2. Щелкните **Восстановление** > **Вся машина**.
3. Чтобы выполнить восстановление в 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. 63). В противном случае рекомендуем выполнить миграцию V2P, используя загрузочный носитель (стр. 68).

4. Данное программное обеспечение автоматически выбирает исходную машину в качестве целевой.

   Чтобы выполнить восстановление в другую виртуальную машину, щелкните **Целевая машина** и выполните следующие действия:

   a. Выберите гипервизор (**VMware ESXi**, **Hyper-V** или **Virtuozzo**).

      Только виртуальные машины Virtuozzo можно восстановить в Virtuozzo. Дополнительную информацию о миграции V2V см. в разделе «Миграция машины» (стр. 120).

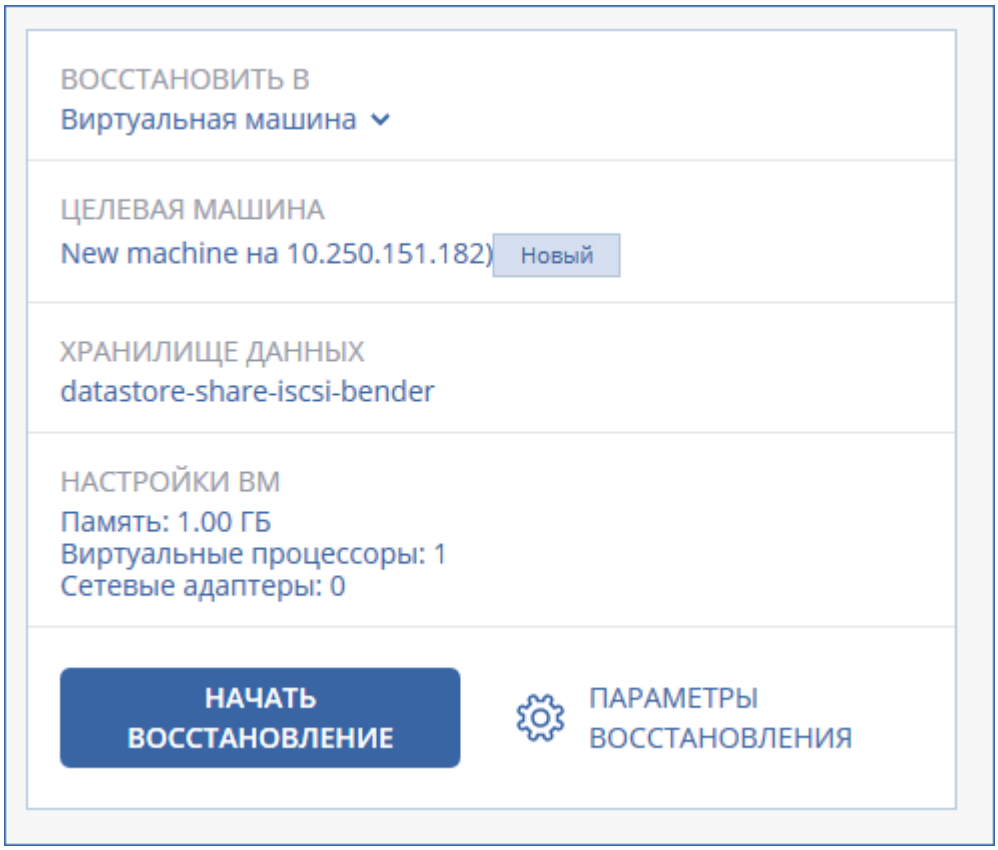
   b. Выберите машину, в которую будут выполняться восстановление: новая или существующая.

   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 Virtuozzo и выберите хранилище данных для данной виртуальной машины.
   - Чтобы изменить размер памяти, количество процессоров и сетевые подключения виртуальной машины, щелкните **Настройки ВМ**.



6. Нажмите **Начать восстановление**.
7. При восстановлении в существующую виртуальную машину подтвердите перезапись дисков.

Ход восстановления отображается на вкладке **Действия**.

9.3.4 Восстановление дисков с помощью загрузочного носителя

Информацию о том, как создать загрузочный носитель, см. в разделе «Создание загрузочного носителя» (стр. 62).

Порядок восстановления дисков с помощью загрузочного носителя

1. Загрузите целевую машину с помощью загрузочного носителя.
2. Выберите **Локальное управление этой машиной** или дважды щелкните **Загрузочный носитель** в зависимости от того, какой тип носителя используете.
3. Если в вашей сети включен прокси-сервер, 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 разделе **Содержимое резервной копии** выберите диски, которые нужно восстановить. Нажмите кнопку **ОК**, чтобы подтвердить выбор.
9. В разделе **Место восстановления** программное обеспечение автоматически сопоставит выбранные диски с целевыми.

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

   Изменение структуры дисков может повлиять на загружаемость операционной системы. Если вы не уверены в полном успехе, используйте исходную структуру дисков машины.
10. [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.
11. [Необязательно] Щелкните **Параметры восстановления**, чтобы указать дополнительные настройки.
12. Нажмите кнопку **ОК**, чтобы начать восстановление.

9.3.5 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. 69).
5. Нажмите кнопку **ОК**.

9.3.5.1 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.

9.3.5.2 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.

9.4 Восстановление файлов

9.4.1 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. 83) или используйте другие способы восстановления:

   - Загрузка файлов из облачного хранилища данных (стр. 72)
   - Использовать загрузочный носитель (стр. 74)
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. 49).

   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 на этой машине установлен агент).
   - Машина, на которой установлен агент для VMware, агент для Hyper-V или агент для Virtuozzo (если файлы изначально находятся на виртуальной машине ESXi, Hyper-V или Virtuozzo).

   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**.

9.4.2 Загрузка файлов из облачного хранилища данных

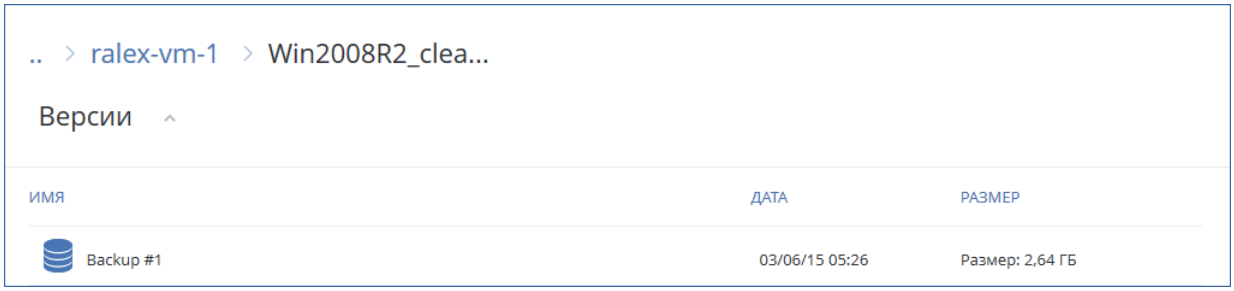
Вы можете просматривать содержимое облачного хранилища данных и резервных копий, а также загружать необходимые файлы.

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**.

9.4.3 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. 71).
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.

9.4.4 Восстановление файлов с помощью загрузочного носителя

Информацию о том, как создать загрузочный носитель, см. в разделе «Создание загрузочного носителя» (стр. 62).

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.

9.4.5 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.

9.5 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**.

9.6 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. 62).

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.

9.7 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 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	OS X	Загрузочный носитель	ESXi, Hyper-V и Virtuozzo	Windows
Проверка резервных копий (стр. 78)	+	+	+	+	+	+	+	+	+
Дата и время для файлов (стр. 79)	–	–	–	+	+	+	+	–	–
Обработка ошибок (стр. 79)	+	+	+	+	+	+	+	+	+
Исключения файлов (стр. 79)	–	–	–	+	+	+	+	–	–

	Диски			Файлы				Виртуальные машины	SQL и Exchange
	Windows	Linux	Загрузочный носитель	Windows	Linux	OS X	Загрузочный носитель	ESXi, Hyper-V и Virtuozzo	Windows
Безопасность на уровне файлов (стр. 79)	–	–	–	+	+	+	+	–	–
Flashback (стр. 80)	+	+	+	–	–	–	–	+	–
Восстановление полного пути (стр. 80)	–	–	–	+	+	+	+	–	–
Точки подключения (стр. 80)	–	–	–	+	–	–	–	–	–
Производительность (стр. 80)	+	+	–	+	+	+	–	+	+
Команды до и после процедуры (стр. 81)	+	+	–	+	+	+	–	+	+
Изменение идентификатора безопасности (стр. 82)	+	–	–	–	–	–	–	–	–
Управление питанием ВМ (стр. 83)	–	–	–	–	–	–	–	+	–
Журнал событий Windows (стр. 83)	+	–	–	+	–	–	–	Только Hyper-V	+

9.7.1 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.

9.7.2 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.

9.7.3 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**.

9.7.4 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.*

9.7.5 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. 51), можно выбрать восстановление разрешений или наследование файлами их разрешений NTFS из папки, в которую они восстановлены.

9.7.6 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.

Если этот параметр включен, восстанавливаются только различия между данными в резервной копии и данными на целевом диске. Это ускоряет восстановление физических и виртуальных машин. Данные сравниваются на уровне блоков.

При восстановлении физической машины предварительно задана настройка **Отключено**.

При восстановлении виртуальной машины предварительно задана настройка **Включено**.

9.7.7 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**.

9.7.8 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. 52).

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.*

9.7.9 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.

9.7.10 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.

9.7.10.1 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	Н/Д	Выполнить

	Выполнить восстановление только после успешного выполнения команды. Прервать восстановление при сбое команды.	восстановление после выполнения команды независимо от результатов ее выполнения (успешно или ошибка).		восстановление параллельно с выполнением команды независимо от результата ее выполнения.

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

9.7.10.2 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.*

9.7.11 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.

9.7.12 Управление питанием ВМ

Эти параметры работают, если восстановление в виртуальную машину выполняется агентом для VMware, агентом для Hyper-V или агентом для Virtuozzo.

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.

9.7.13 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**.

10 Операции с резервными копиями

10.1 Вкладка «Резервные копии»

На вкладке **Резервные копии** предоставлен доступ ко всем резервным копиям, включая автономные машины и машины, которые больше не зарегистрированы в сервисе резервного копирования.

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. Администратор может просматривать резервные копии от имени любой учетной записи, которая принадлежит данному отделу или компании 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.

Чтобы выбрать точку восстановления, используя вкладку «Резервные копии», выполните следующие действия:

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.

10.2 Подключение томов из резервной копии

Подключение томов из резервной копии на уровне дисков позволяет получить доступ к томам так же, как и к физическим дискам. Тома подключаются в режиме только для чтения.

Требования

- Эта функциональность доступна только в Windows при использовании проводника.
- На машине, которая выполняет операцию подключения, должен быть установлен агент для Windows.
- Файловая система, для которой создана резервная копия, должна поддерживаться в той версии Windows, которая выполняется на данной машине.
- Резервная копия должна хранится в локальной папке, сетевой папке (SMB/CIFS) или в Зоне безопасности.

Порядок подключения тома из резервной копии

1. Перейдите в хранилище резервных копий, используя проводник.
2. Дважды щелкните файл резервной копии. Файлы имеют имена на основе следующего шаблона:

   `<имя машины> - <GUID плана 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 тома, для которых созданы резервные копии.

   Совет. *Дважды щелкните том для обзора его содержимого. Можно скопировать файлы и папки из резервной копии в любую папку в файловой системе.*

5. Щелкните подключаемый том правой кнопкой мыши и выберите пункт **В режиме «только чтение»**.
6. Если резервная копия хранится в сетевой папке, укажите учетные данные для доступа. В противном случае пропустите этот шаг.

   Программа подключит выбранный том. Данному тому назначается первая неиспользованная буква.

Порядок отключения тома

1. В проводнике откройте **Компьютер** (**Этот компьютер** в Windows 8.1 и более поздней версии).
2. Правой кнопкой мыши щелкните подключенный том.
3. Щелкните **Отключить**.

   Программа отключит выбранный том.

10.3 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.

11 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.

12 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.

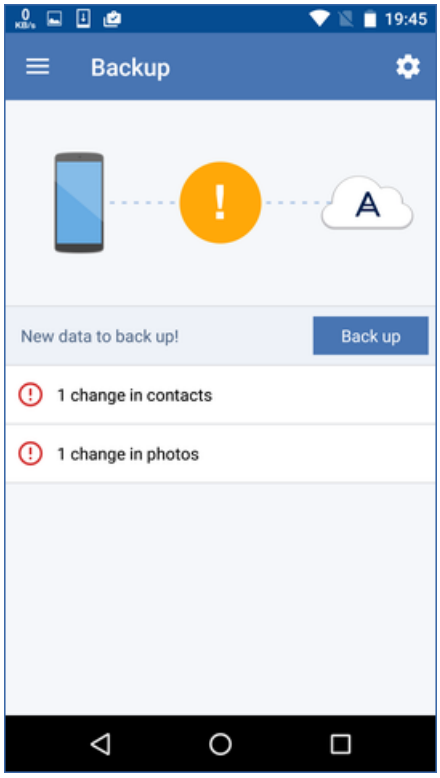
Данные, для которых можно создать резервную копию

- 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, восстановленные данные будут помещены во внутреннее хранилище данных.

Пошаговые инструкции

Порядок получения приложения резервного копирования

1. На мобильном устройстве откройте браузер и введите URL-адрес консоли резервного копирования.
2. Войдите с помощью учетной записи.
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 с помощью учетной записи.
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.

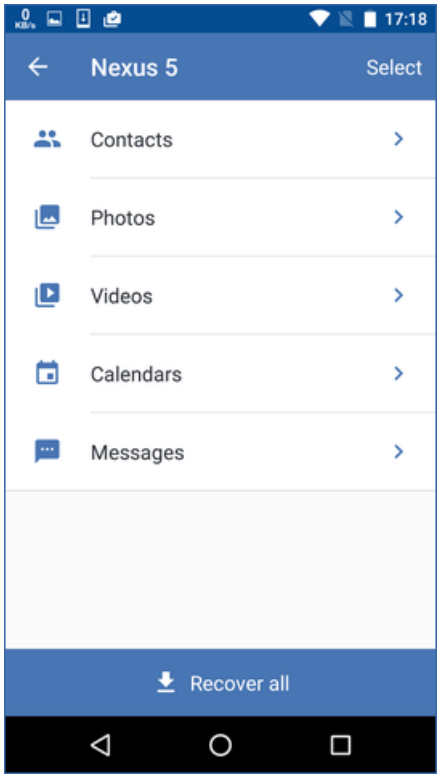
Порядок создания резервной копии устройства Android

1. Откройте приложение резервного копирования.
2. Войдите с помощью учетной записи.
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

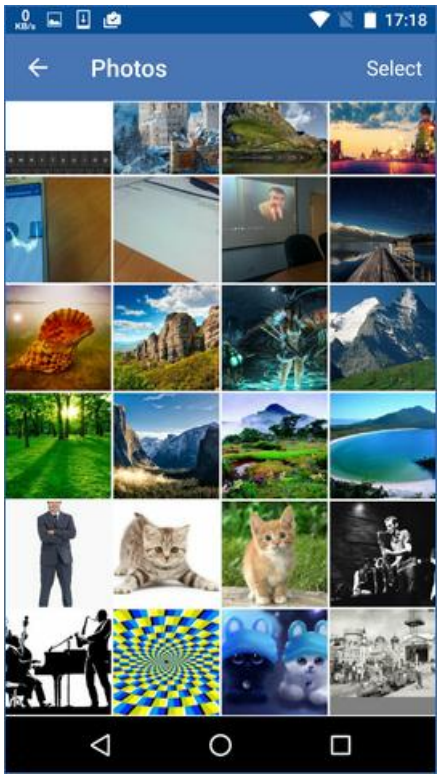
1. Откройте приложение резервного копирования.
2. Смахните влево и коснитесь **Доступ и восстановление**.
3. Коснитесь имени устройства.
4. Выполните одно из следующих действий:
   - Чтобы восстановить все данные, для которых создана резервная копия, коснитесь **Восстановить все**. Никаких дополнительных 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.

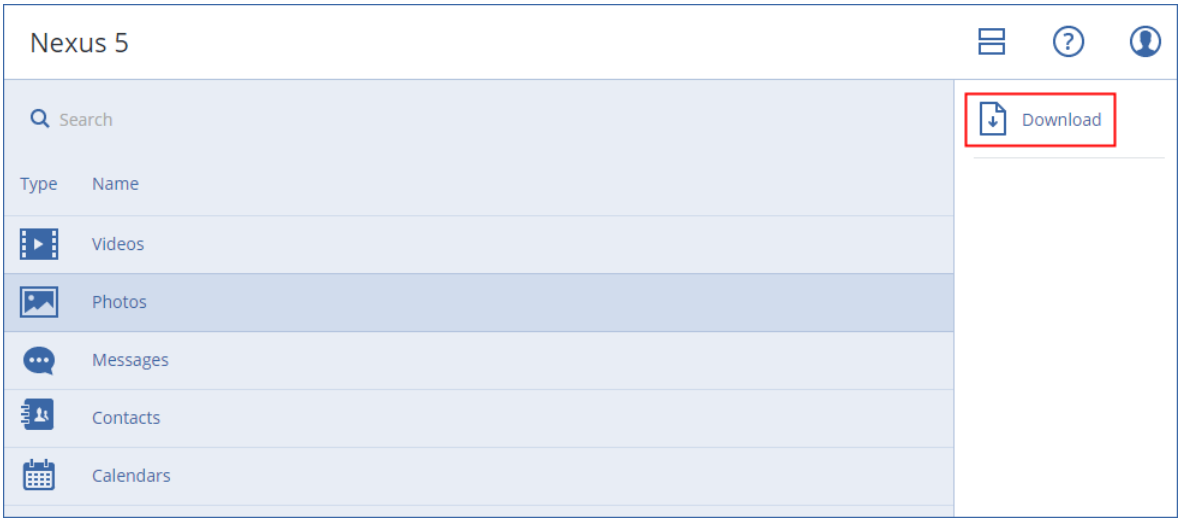
- Чтобы восстановить несколько элементов данных, коснитесь **Выбрать**, затем коснитесь флажков для требуемых элементов данных.



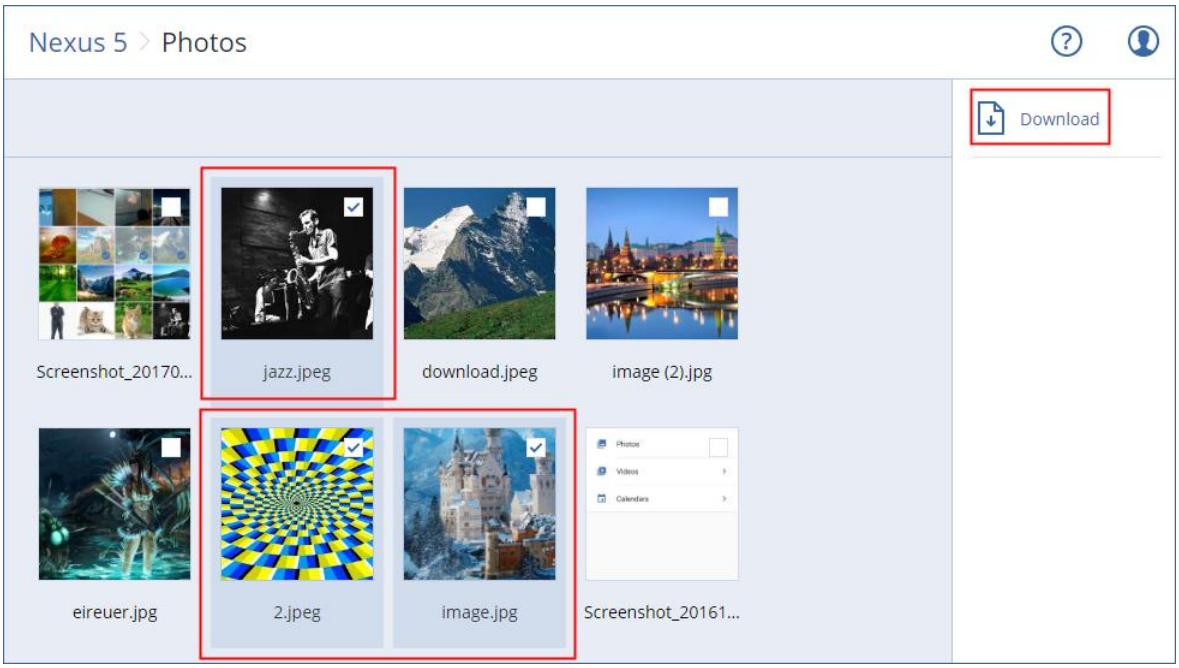
6. Коснитесь значка **Восстановить**.

Порядок получения доступа к данным через консоль резервного копирования

1. На компьютере откройте браузер и введите URL-адрес консоли резервного копирования.
2. Войдите с помощью учетной записи.
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 https://docs.acronis.com/mobile-backup. Эта справка также доступна в приложении резервного копирования (в меню приложения последовательно коснитесь пунктов **Настройки** > **Справка**).

13 Защита приложений

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.

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. 97) Базы данных как файлы (стр. 97)	Вся машина (стр. 63) Базы данных в запущенный экземпляр SQL Server (стр. 97) Базы данных как файлы (стр. 97)	Вся машина (стр. 63)
Microsoft Exchange Server	Базы данных в запущенный Exchange (стр. 100) Базы данных как файлы (стр. 100) Фрагментарное восстановление в запущенный Exchange (стр. 102)	Вся машина (стр. 63) Базы данных в запущенный Exchange (стр. 100) Базы данных как файлы (стр. 100) Фрагментарное восстановление в запущенный Exchange (стр. 102)	Вся машина (стр. 63)
Серверы базы данных Microsoft SharePoint	Базы данных в запущенный экземпляр SQL Server (стр. 97) Базы данных как файлы (стр. 97) фрагментарное восстановление с использованием SharePoint Explorer	Вся машина (стр. 63) Базы данных в запущенный экземпляр SQL Server (стр. 97) Базы данных как файлы (стр. 97) фрагментарное восстановление с использованием SharePoint Explorer	Вся машина (стр. 63)
Интерфейсные веб-серверы Microsoft SharePoint	-	-	Вся машина (стр. 63)

Доменные службы Active Directory	-	Вся машина (стр. 63)	-

13.1 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.
- 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.
- 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. 59).
- Для виртуальных машин включен параметр резервного копирования Служба теневого копирования томов (VSS) для виртуальных машин (стр. 61).

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://code.vmware.com/doc/preview?id=4076#https://vdc-repo.vmware.com/vmwb-repository/dcr-public/17aee92f-6920-4675-b03c-8c85de455bb3/5e2b0233-eea0-44c6-84aa-0d3a5aefe1a1/doc/vddkBkupVadp.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).

13.2 Резервная копия базы данных

Прежде чем приступить к созданию резервных копий баз данных, убедитесь, что выполнены требования, перечисленные в разделе «Предварительные требования» (стр. 93).

Выберите базы данных, как указано ниже, а затем укажите другие настройки плана резервного копирования в зависимости от требований (стр. 29).

13.2.1 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. 51).

Порядок выбора баз данных SQL

1. Щелкните **Microsoft SQL**.

   Появится список машин, на которых установлен агент для SQL.
2. Перейдите к данным, для которых требуется создать резервные копии.

   Дважды щелкните машину, чтобы посмотреть, какие экземпляры SQL Server на ней есть. Дважды щелкните экземпляр, чтобы посмотреть, какие базы данных он содержит.
3. Выберите данные, резервную копию которых необходимо создать. Можно выбирать целые экземпляры или отдельные базы.
   - Если выбрать экземпляр SQL Server, будут созданы резервные копии всех содержащихся в нем баз данных; кроме того, впоследствии будут создаваться резервные копии всех баз, добавляемых в него в будущем.
   - 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 **sysadmin** в каждом из экземпляров, для которых создается резервная копия.

13.2.2 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	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. Щелкните **Microsoft Exchange**.

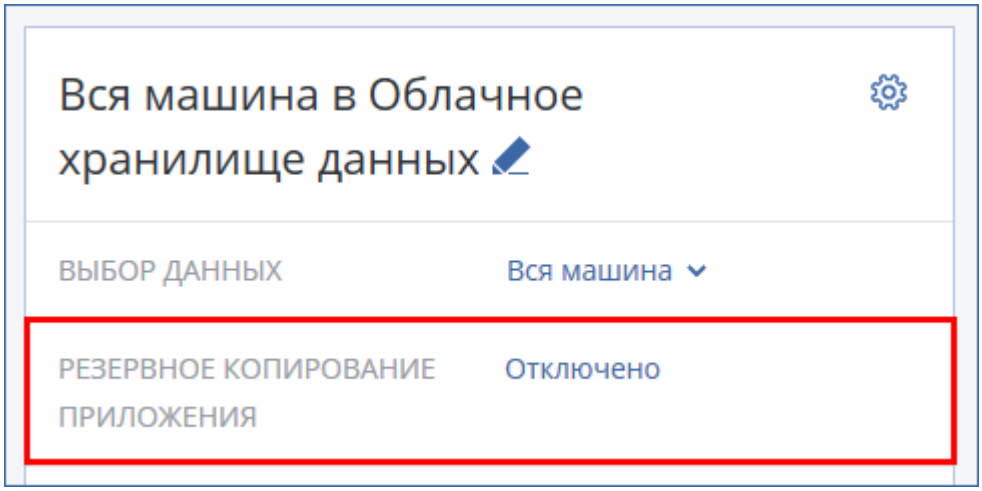
   Появится список машин, на которых установлен агент для Exchange.
2. Перейдите к данным, для которых требуется создать резервные копии.

   Дважды щелкните машину, чтобы посмотреть, какие базы данных (группы хранения) на ней есть.
3. Выберите данные, резервную копию которых необходимо создать. Если потребуется, введите учетные данные для доступа к информации.
4. Нажмите кнопку **Резервное копирование**.

13.3 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. 51). Журналы транзакций Exchange сокращаются только на виртуальных машинах. Чтобы сократить журналы транзакций Exchange на физической машине, можно включить параметр полного восстановления VSS (стр. 59).
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. 93) и «Необходимые права пользователя» (стр. 96).

13.3.1 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.

13.4 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. 99).

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. 99).

Порядок восстановления баз данных SQL

1. При восстановлении из резервной копии базы данных щелкните **Microsoft SQL**. В противном случае пропустите этот шаг.
2. Выберите машину, на которой ранее 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. Выполните одно 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

включенную машину, на которой установлен агент для SQL, а затем выберите точку восстановления.

- Выберите точку восстановления на вкладке «Резервные копии» (стр. 83).

Машина, выбранная для обзора любым из двух вышеописанных действий, становится целевой машиной для восстановления баз данных SQL.

5. Выполните одно из следующих действий:
   - При восстановлении из резервной копии базы данных выберите пункты **Восстановление Базы данных SQL**.
   - При восстановлении из резервной копии с поддержкой приложений выберите пункты **Восстановление** > **Базы данных SQL**.
6. Выберите данные, которые необходимо восстановить. Дважды щелкните экземпляр, чтобы посмотреть, какие базы данных он содержит.
7. Если вы хотите восстановить базы данных в виде файлов, щелкните **Восстановить как файлы**, выберите локальную или сетевую папку, в которую их требуется сохранить, и нажмите **Восстановить**. В противном случае пропустите этот шаг.
8. Нажмите кнопку **Восстановить**.
9. 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.
10. 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.

11. Нажмите кнопку **Запуск восстановления**.

Ход восстановления отображается на вкладке **Действия**.

13.4.1 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.

13.4.2 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**.

13.5 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. 101).

Если используется только агент для VMware, то единственный доступный метод восстановления — восстановить базы данных как файлы.

Восстановление данных Exchange

В этой процедуре как базы данных, так и группы хранения описываются термином «базы данных».

1. При восстановлении из резервной копии базы данных щелкните **Microsoft Exchange**. В противном случае пропустите этот шаг.
2. Выберите машину, на которой ранее 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.

   - Если резервная копия расположена в облачном хранилище или общем хранилище (т .е. другие агенты могут получить к ней доступ), щелкните **Выбрать машину**, выберите

включенную машину, на которой установлен агент для Exchange, а затем выберите точку восстановления.

- Выберите точку восстановления на вкладке «Резервные копии» (стр. 83).

Машина, выбранная для обзора любым из двух вышеописанных действий, становится целевой машиной для восстановления данных Exchange.

5. Щелкните **Восстановление** > **Базы данных Exchange**.
6. Выберите данные, которые необходимо восстановить.
7. Если вы хотите восстановить базы данных в виде файлов, щелкните **Восстановить как файлы**, выберите локальную или сетевую папку, в которую их требуется сохранить, и нажмите **Восстановить**. В противном случае пропустите этот шаг.
8. Нажмите кнопку **Восстановить**. Если потребуется, введите учетные данные для доступа к Exchange Server.
9. 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.
10. Нажмите кнопку **Запуск восстановления**.

Ход восстановления отображается на вкладке **Действия**.

13.5.1 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

13.6 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 и резервных копий с поддержкой приложений.

Обзор

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

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.

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

При восстановлении элементов почтового ящика перезапись не происходит. Элементы почтового ящика всегда восстанавливаются в папку **Восстановленные элементы** целевого 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.

13.6.1 Восстановление почтовых ящиков

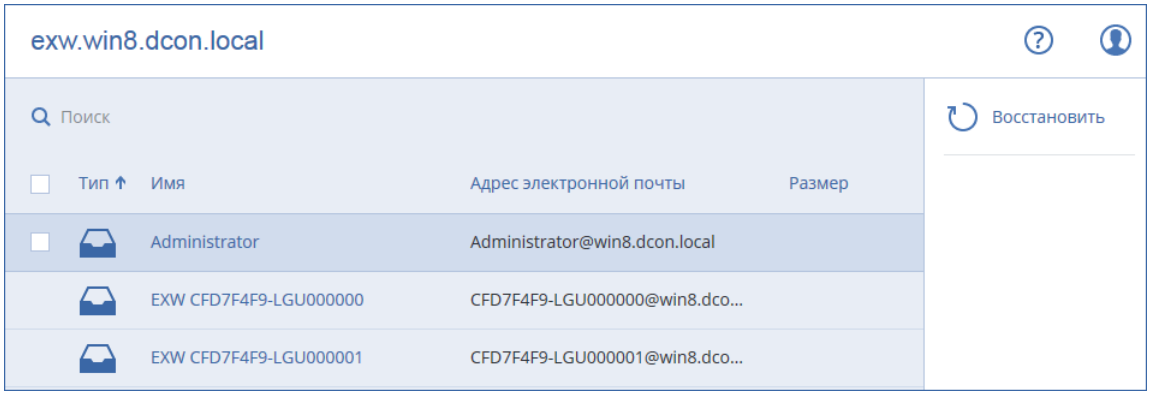
1. При восстановлении из резервной копии базы данных щелкните **Microsoft Exchange**. В противном случае пропустите этот шаг.
2. Выберите машину, на которой ранее располагались данные, которые необходимо восстановить.
3. Щелкните **Восстановление**.
4. Выберите точку восстановления. Обратите внимание на то, что точки восстановления отфильтрованы по хранилищу.

   Если машина отключена, точки восстановления не отображаются. В этом случае воспользуйтесь одним из перечисленных ниже способов.

   - Если резервная копия расположена в облачном или общем хранилище данных (т .е. другие агенты могут получить к ней доступ), щелкните **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. 83).

   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. 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**.
9. [Необязательно] Чтобы изменить автоматически выбранную базу данных, щелкните **База данных для воссоздания отсутствующих почтовых ящиков**.

10. Нажмите кнопку **Запуск восстановления**.
11. Подтвердите операцию.

Ход восстановления отображается на вкладке **Действия**.

13.6.2 Восстановление элементов почтовых ящиков

1. При восстановлении из резервной копии базы данных щелкните **Microsoft Exchange**. В противном случае пропустите этот шаг.
2. Выберите машину, на которой ранее 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.

   - Если резервная копия расположена в облачном или общем хранилище данных (т .е. другие агенты могут получить к ней доступ), щелкните **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. 83).

   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.

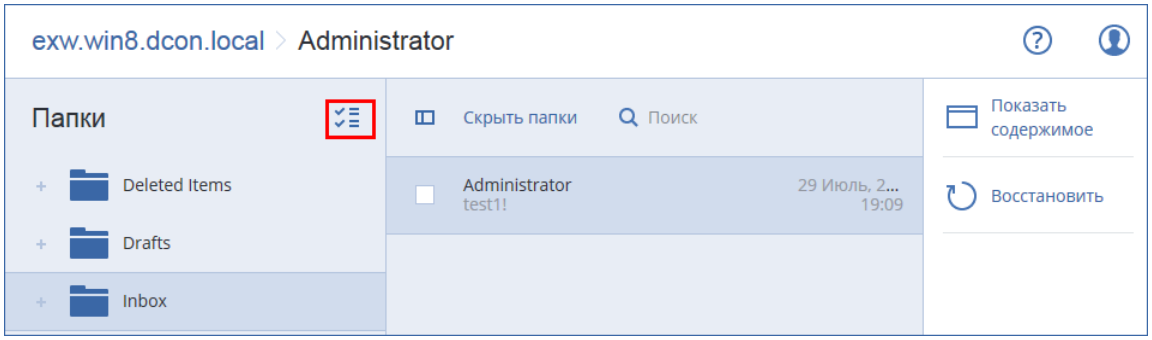
   Доступны указанные ниже параметры поиска. Подстановочные символы не поддерживаются.

   - 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 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 или выбрана целевая машина, которая не является исходной, необходимо указать целевой почтовый ящик.
11. Нажмите кнопку **Запуск восстановления**.
12. Подтвердите операцию.

Ход восстановления отображается на вкладке **Действия**.

14 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?

Агент для Office 365

В зависимости от настроек, выбранных поставщиком услуг, может потребоваться установить агент для Office 365 локально или использовать агент, установленный в данном облаке.

Если используется установленный в облаке агент для Office 365, применяются следующие ограничения:

- В качестве места назначения резервной копии доступно только облачное хранилище данных.
- Резервное копирование выполняется раз в день. Расписание резервного копирования невозможно изменить. Невозможно запустить резервное копирование вручную.

Важно! *В организации (группе компаний) должен быть только один агент для Office 365.*

Учетная запись глобального администратора

Для выполнения резервного копирования и восстановления почтовых ящиков Office 365 вашей учетной записи должна быть назначена роль глобального администратора в Microsoft Office 365. 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**.

Какие элементы можно восстановить?

Из резервной копии почтового ящика можно восстановить следующие элементы:

- почтовые ящики;
- папки электронной почты;
- сообщения электронной почты;
- события календаря;
- задания;
- контакты;
- записи журнала.
- Примечание

Чтобы найти эти элементы, можно воспользоваться поиском.

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

При восстановлении элементов почтового ящика перезапись не происходит. Элементы почтового ящика всегда восстанавливаются в папку **Восстановленные элементы** целевого почтового ящика.

Ограничения

- Невозможно создать резервную копию архивированных почтовых ящиков (**архив на месте**).
- Невозможно выполнить восстановление в новый почтовый ящик. Сначала необходимо создать нового пользователя Office 365, затем восстановить элементы в почтовый ящик этого пользователя.
- Восстановление в учетную запись другой организации Microsoft Office 365 или в локальные развертывания сервера Microsoft Exchange Server не поддерживается.

14.1 Добавление почтовых ящиков Office 365

Порядок добавления почтовых ящиков Office 365

1. Щелкните **Устройства** > **Добавить** > **Microsoft Office 365**.
2. Выполняется одно из указанных ниже действий:
   - Программное обеспечение начинает разворачивать агент для Office 365 в облаке.

- Для программного обеспечения необходим установленный агент для Office 365. Загрузите агент и установите его на машину Windows, которая подключена к Интернету.

3. По окончании установки последовательно выберите пункты **Устройства** > **Microsoft Office 365**, а затем введите учетные данные глобального администратора Office 365.

Важно! *В организации (группе компаний) должен быть только один агент для Office 365.*

14.2 Выбор почтовых ящиков Office 365

Выберите почтовый ящики, как указано ниже, а затем укажите другие настройки плана резервного копирования как требуется (стр. 29).

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**.

14.3 Восстановление почтовых ящиков и элементов почтового ящика Office 365

14.3.1 Восстановление почтовых ящиков

1. Щелкните **Microsoft Office 365**.
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. 83) 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. 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.
6. Нажмите кнопку **Запуск восстановления**.

14.3.2 Восстановление элементов почтовых ящиков

1. Щелкните **Microsoft Office 365**.
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. 83) 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. 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**.
9. Подтвердите операцию.

Элементы почтового ящика всегда восстанавливаются в папку **Восстановленные элементы** целевого почтового ящика.

15 Активная защита

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 Vista и более поздних версий, а также Windows Server 2008 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.
- Папки, в которых не будут отслеживаться изменения файлов.

Процессы могут быть указаны в следующих форматах:

```
C:\Data\Finance\file.exe
file.exe
C:\file*.exe
C:\file?.exe
```

Для определения процессов и папок можно использовать один или несколько подстановочных символов * и ?. Звездочка (*) замещает 0 или более символов. Знак вопроса (?) заменяет только один символ.

План активной защиты

Все настройки активной защиты содержаться в плане активной защиты. Этот план можно применить к нескольким машинам.

В организации (группе компаний) может быть только один план активной защиты. Применять, изменять и отзывать план могут только администраторы компании и администраторы более высоких уровней.

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 Защита веб-сайтов

Несанкционированный доступ или атаки вредоносных программ могут стать причиной повреждения веб-сайта. Чтобы иметь возможность быстро восстановить работу веб-сайта при сбое, создайте его резервную копию.

Что необходимо, чтобы создать резервную копию сайта?

Веб-сайт должен быть доступен по протоколу SFTP или SSH. Если не нужно установить агент, просто добавьте веб-сайт, как описано далее в этом разделе.

Для каких элементов можно создавать резервные копии?

Элементы, для которых можно создать резервные копии:

- **Файлы содержимого веб-сайта**

  Все файлы, доступные для учетной записи, указанной для подключения SFTP или SSH.
- **Связанные базы данных (если существуют) расположены на серверах MySQL.**

  Все базы данных, доступные для указанной учетной записи MySQL.

Если для вашего веб-сайта используются базы данных, рекомендуем создать резервную копию файлов и баз данных с тем, чтобы их можно было восстановить в согласованное состояние.

Ограничения

- Для резервной копии веб-сайта доступно только одно хранилище — облачное хранилище данных.
- План резервного копирования нельзя применить к нескольким веб-сайтам. Для каждого веб-сайта должен быть свой собственный план резервного копирования, даже если все планы резервного копирования имеют одинаковые настройки.
- К веб-сайту можно применить только один план резервного копирования.
- Параметры резервного копирования недоступны.

16.1 Резервное копирование веб-сайта

Порядок добавления веб-сайта и настройки его резервной копии

1. Нажмите **Устройства** > **Добавить**.
2. Щелкните **Веб-сайт**.
3. Задайте указанные ниже настройки для веб-сайта:
   - В поле **Имя веб-сайта** создайте и введите имя веб-сайта. Это имя будет отображаться на консоли резервного копирования.
   - В поле **Хост** укажите имя хоста или IP-адрес, который будет использоваться для доступа к веб-сайту через SFTP или SSH. Например, `my.server.com` или `10.250.100.100`.
   - В поле **Порт** укажите номер порта.
   - В полях **Имя пользователя** и **Пароль** укажите четные данные учетной записи, которые можно использовать для доступа к веб-сайту через SFTP или SSH.

     Важно! *Будет выполняться резервное копирование только тех файлов, которые доступны для указанной учетной записи.*

     Вместо пароля можно указать закрытый ключ SSH. Для этого установите флажок **Использовать закрытый ключ SSH вместо пароля**, затем укажите ключ.
4. Нажмите кнопку **Далее**.
5. Если в веб-сайте используются базы данных MySQL, задайте настройки доступа для баз данных. В противном случае щелкните **Пропустить**.
   a. В поле **Тип подключения** выберите порядок доступа к базам данных из облака:
      - **По протоколу SSH с хоста**: доступ к базам данных будет выполняться через хост, указанный в шаге 3.
      - **Прямое подключение**: к базам данных будет непосредственный доступ. Закройте эту настройку, только если базы данных доступны из Интернета.

   b. В поле **Хост** укажите имя или IP-адрес хоста, на котором выполняется сервер MySQL.

   c. В поле **Порт** укажите номер порта для подключения к серверу по протоколу TCP/IP. Номер порта по умолчанию — 3306.

   d. В полях **Имя пользователя** и **Пароль** укажите учетные данные аккаунта в MySQL.

      Важно! *Будет выполняться резервное копирование только тех баз данных, которые доступны для указанной учетной записи.*

   e. Нажмите кнопку **Создать**.
6. В программе отобразиться новый шаблон плана резервного копирования. При необходимости измените настройки, затем щелкните **Применить**.

Изменение настроек подключения

1. Выберите веб-сайт в разделе **Устройства** > **Веб-сайты**.
2. Нажмите кнопку **Обзор**.
3. Щелкните значок карандаша рядом с веб-сайтом или настройками подключения к базе данных.
4. Внесите необходимые изменения и нажмите кнопку **Сохранить**.

Порядок изменения плана резервного копирования

1. Выберите веб-сайт в разделе **Устройства** > **Веб-сайты**.
2. Нажмите кнопку **Резервное копирование**.

3. Щелкните значок шестеренки рядом с именем плана резервного копирования и выберите команду **Изменить**.
4. Внесите необходимые изменения и нажмите кнопку **Сохранить изменения**.

16.2 Восстановление веб-сайта

Порядок восстановления веб-сайта

1. В разделе **Устройства** > **Веб-сайты** выберите веб-сайт, который необходимо восстановить.

   Можно выполнить поиск веб-сайтов по имени. Подстановочные символы не поддерживаются.
2. Щелкните **Восстановление**.
3. Выберите точку восстановления.
4. Щелкните **Восстановить** и выберите объекты, которые необходимо восстановить: **Файлы/папки** или **Базы данных SQL** (если уместно).

   Чтобы убедиться, что веб-сайт работает в согласованном состоянии, рекомендуем восстановить как файлы, так и базы данных в любом порядке.
5. В зависимости от выбранного варианта выполните одну указанных ниже процедур.

Порядок восстановления файлов/папок веб-сайта

1. 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 файла" (стр. 49).
2. Выберите файлы, которые необходимо восстановить.
3. Чтобы сохранить файлы как ZIP-файл, нажмите кнопку **Загрузить**, выберите расположение для сохранения данных и нажмите кнопку**Сохранить**. В противном случае пропустите этот шаг.
4. Щелкните **Восстановить** и подтвердите действие.

   Выбранные файлы и папки будут восстановлены в исходное расположение.

Порядок восстановления баз данных

1. Выберите базы данных, которые необходимо восстановить.
2. Чтобы сохранить базы данных как ZIP-файл, нажмите кнопку **Загрузить**, выберите расположение для сохранения данных и нажмите кнопку **Сохранить**. В противном случае пропустите этот шаг.
3. Щелкните **Восстановить** и подтвердите действие.

   Выбранные базы данных будут восстановлены в исходное расположение.

17 Специальные операции с виртуальными машинами

17.1 Запуск виртуальной машины из резервной копии (мгновенное восстановление)

Можно запустить виртуальную машину с резервной копии на уровне дисков, которая содержит операционную систему. Эта операция, которая также известна как мгновенное восстановление, позволяет ускорить виртуальный сервер за считанные секунды. Виртуальные диски эмулируются непосредственно с резервной копии и поэтому не занимают место в хранилище данных. Место хранения требуется только для того, чтобы сохранить изменения в виртуальных дисках.

Рекомендуем запустить эту временную виртуальную машину на срок до трех дней. После этого можно полностью удалить ее или преобразовать в обычную виртуальную машину (финализировать) без простоя.

Пока существует временная виртуальная машина, правила хранения нельзя применить к резервной копии, которая используется этой машиной. Резервные копии исходной машины могут продолжать выполняться.

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 или в локальной папке машины, на которой установлен агент для VMware или агент для Hyper-V. Сетевая папка должна быть доступной с данной машины. Виртуальную машину можно также запустить из резервной копии, которая хранится в облачном хранилище данных, но в этом случае она будет работать медленнее. Причина состоит в том, что для этой операции требуется интенсивное чтение из резервной копии с произвольным доступом к данным.
- Резервная копия должна содержать всю машину или все тома, которые необходимы для запуска операционной системы.
- Могут использоваться резервные копии физических и виртуальных машин. Нельзя использовать резервные копии *контейнеров* Virtuozzo.

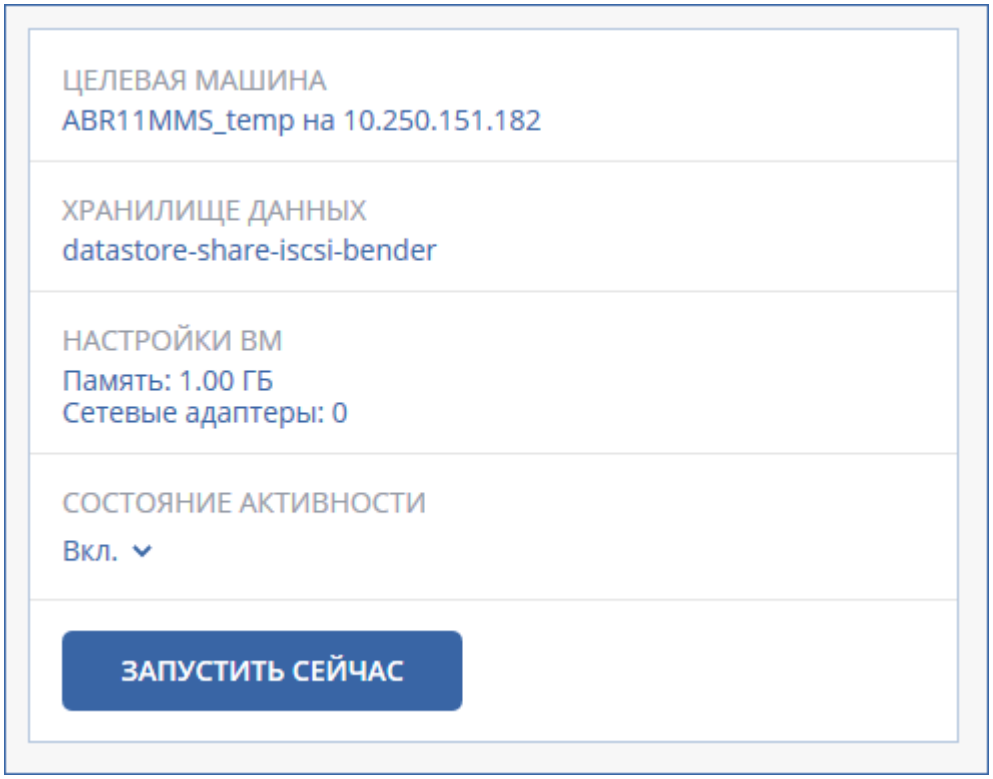
17.1.1 Запуск машины

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. 83).

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.

17.1.2 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.

17.1.3 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.

17.2 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. 119), 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. 117)

  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. 118)

  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.

17.2.1 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. 119).
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: 

17.2.2 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.

17.2.3 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. 118)

  Остановите переход к реплике, если исходная машина исправлена. Реплика будет выключена. Репликация будет продолжена.
- **Выполнить окончательный переход на реплику** (стр. 118)

  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. 119)

  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.

17.2.3.1 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.

17.2.3.2 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**.

17.2.3.3 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. 120).
7. Нажмите кнопку **Запуск восстановления**.
8. Подтвердите операцию.

17.2.4 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. 47).

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. 48).

Команды до и после процедуры

Этот параметр подобен параметру резервного копирования «Команды до и после процедуры» (стр. 54).

Служба теневого копирования томов (VSS) для виртуальных машин

Этот параметр подобен параметру резервного копирования «Служба теневого копирования томов (VSS) для виртуальных машин» (стр. 61).

17.2.5 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. 79).

Производительность

Этот параметр подобен параметру восстановления «Производительность» (стр. 80).

Команды до и после процедуры

Этот параметр подобен параметру восстановления «Команды до и после процедуры» (стр. 81).

Управление питанием ВМ

Этот параметр подобен параметру восстановления «Управление питанием ВМ» (стр. 83).

17.3 Управление средами виртуализации

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

Вкладка **VMware** позволяет изменить учетные данные доступа для vCenter Server или автономного хоста ESXi без переустановки агента.

Изменение учетных данных доступа vCenter Server или хоста ESXi

1. В разделе **Устройства** щелкните **VMware**.
2. Щелкните **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 кнопку **Обзор**.
5. В области **Учетные данные** щелкните имя пользователя.
6. Укажите новые учетные данные доступа и щелкните **ОК**.

17.4 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	Виртуальная машина Virtuozzo	Контейнер Virtuozzo
Физическая машина	+	+	+	-	-
Виртуальная машина VMware ESXi	+	+	+	-	-
Виртуальная машина Hyper-V	+	+	+	-	-
Виртуальная машина Virtuozzo	+	+	+	+	-
Контейнер Virtuozzo	-	-	-	-	+

Инструкции по выполнению миграции см. в следующих разделах:

- Миграция систем с физической машины на виртуальную (P2V): Миграция систем с физической машины на виртуальную (стр. 64)
- Миграция систем с виртуальной машины на виртуальную (V2V): Виртуальная машина (стр. 66)
- Миграция систем с виртуальной машины на физическую (V2P): Виртуальная машина (стр. 66) или Восстановление дисков с помощью загрузочного носителя (стр. 68)

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:

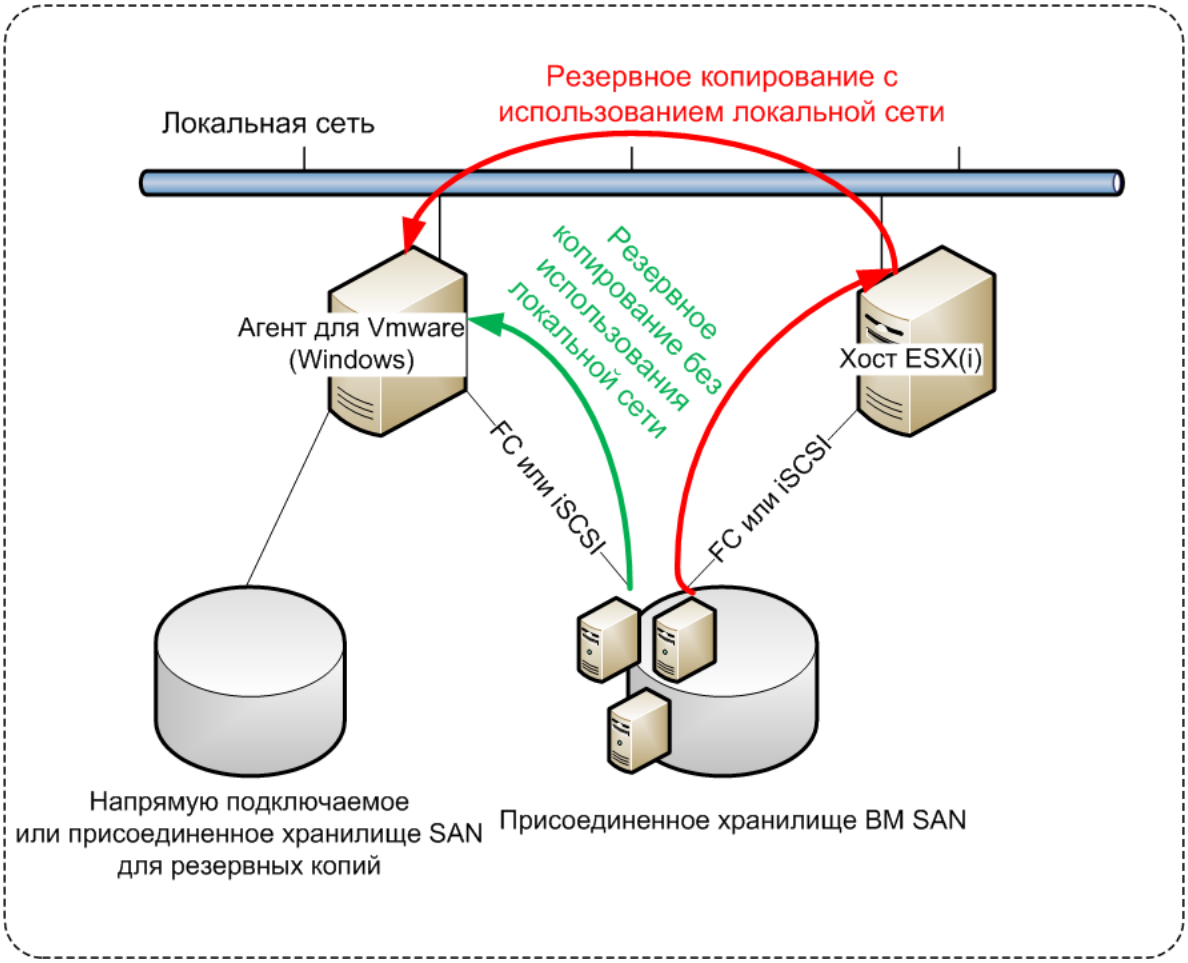
- выбирать отдельные диски или тома для восстановления;
- вручную сопоставлять диски из резервной копии с дисками целевой машины;
- повторно создавать логические тома (LVM) или программные RAID-массивы Linux на целевой машине;
- предоставлять драйверы для определенного оборудования, необходимого для нормальной загрузки системы.

17.5 Агент для VMware — резервное копирование без использования локальной сети

Если с ESXi используется SAN-хранилище, установите агент на машину, подключенную к той же сети SAN. Агент будет создавать резервные копии виртуальных машин прямо из хранилища данных, а не через хост ESXi и локальную сеть. Эта возможность называется резервным копированием без использования локальной сети.

На следующем рисунке показано резервное копирование с использованием и без использования локальной сети. Доступ к виртуальным машинам без использования локальной сети возможен при наличии оптоволоконного канала (FC) или сети хранения данных (SAN) iSCSI. Чтобы полностью исключить передачу резервных копий данных по локальной сети, храните

резервные копии на локальном диске машины с установленным агентом или в присоединенном хранилище SAN.



Порядок включения прямого доступа к хранилищу данных для агента.

1. Установите агент для VMware на машину Windows, на которой есть сетевой доступ к vCenter Server.
2. Подключите к машине логическое устройство, на котором расположено хранилище данных. Примите во внимание следующие соображения:
   - Используйте тот же протокол (iSCSI или FC), который использовался для подключения хранилища данных к ESXi.
   - Логическое устройство *не должно* инициализироваться. Вместо этого оно должно появится как «автономный» диск в разделе **Управление дисками**. Если Windows инициализирует логическое устройство, оно может быть повреждено и стать нечитаемым для VMware vSphere.

В результате агент будет использовать режим транспорта сети SAN для доступа к виртуальным дискам, т. е. он будет посекторно считывать секторы логического устройства по iSCSI/FC, не распознавая файловой системы VMFS (которая неизвестна для Windows).

Ограничения

- В vSphere 6.0 и более поздней версии агент не может использовать режим транспорта SAN, если одни диски ВМ расположены в VMware Virtual Volume (VVol), а другие — на других томах. Резервное копирование таких виртуальных машин приведет к сбою.

- Резервное копирование зашифрованных виртуальных машин (эта функциональная возможность представлена в VMware vSphere 6.5) будет выполняться по локальной сети, даже если настроен режим транспорта сети SAN для агента. Агент выполнит возврат из реплики, используя транспорт NBD, поскольку VMware не поддерживает транспорт сети SAN для резервного копирования зашифрованных виртуальных дисков.

Пример

Если используется сеть хранения данных (SAN) iSCSI, настройте инициатор iSCSI на машине с Windows, на которой установлен агент для VMware.

Настройка политики SAN

1. Войдите как администратор, откройте командную строку, введите **`diskpart`** и нажмите клавишу **ВВОД**.
2. Введите **`san`** и нажмите клавишу **ВВОД**. Убедитесь, что отображается **Политика SAN: На экране отобразится Перевод в автономное состояние всех ресурсов**.
3. Если для политики SAN задано другое значение:
   a. Type **`san policy=offlineall`**.
   b. Нажмите клавишу **Ввод**.
   c. Чтобы проверить правильность применения настройки, выполните шаг 2.
   d. Перезапустите машину.

Настройка инициатора iSCSI

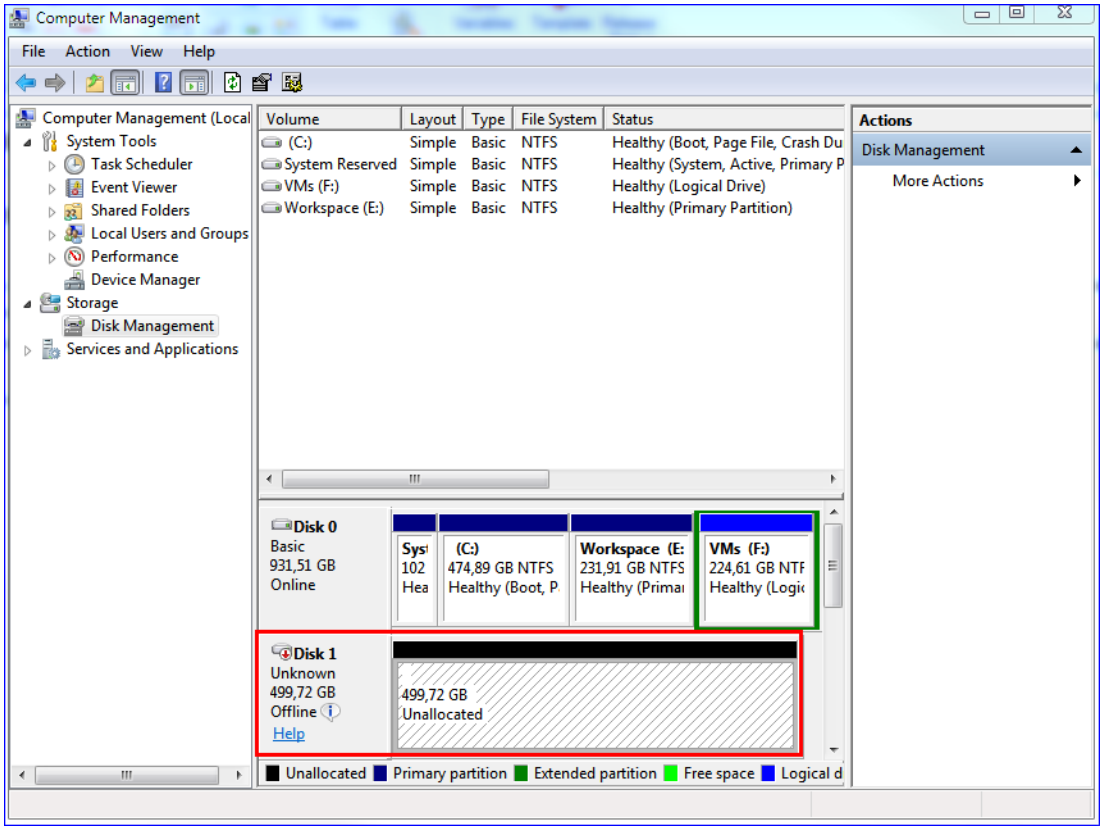
1. Последовательно выберите пункты **Панель управления** > **Администрирование** > **Инициатор iSCSI**.

   ***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.



17.6 Агент для VMware: необходимые привилегии

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 «Управление средами виртуализации» (стр. 120).

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

		Операция			
Объект	**Привилегия**	**Резервное копирование ВМ**	**Восстановление в новую ВМ**	**Восстановление в существующую ВМ**	**Запуск ВМ из резервной копии**
	Обзор хранилища данных				+
	Настройка хранилища данных	+	+	+	+
	Низкоуровневые файловые операции				+
Глобальные	**Лицензии**	+	+	+	+
	Методы отключения	+	+	+	
	Методы включения	+	+	+	
Хост > Конфигурация	**Конфигурация раздела хранения данных**				+
Хост > Локальные операции	**Создание ВМ**				+
	Удаление ВМ				+
	Перенастройка ВМ				+
Сеть	**Назначение сети**		+	+	+
Ресурс	**Назначение ВМ пулу ресурсов**		+	+	+
Виртуальная машина > Конфигурация	**Добавление существующего диска**	+	+		+
	Добавление нового диска		+	+	+
	Добавление или удаление устройства		+		+
	Дополнительно	+	+	+	
	Изменение числа ЦП		+		
	Отслеживание изменений диска	+		+	
	Аренда диска	+		+	
	Память		+		
	Удаление диска	+	+	+	+
	Переименование		+		

		Операция			
Объект	**Привилегия**	**Резервное копирование ВМ**	**Восстановление в новую ВМ**	**Восстановление в существующую ВМ**	**Запуск ВМ из резервной копии**
	Настройка аннотации				+
	Настройки		+	+	+
Виртуальная машина > **Гостевые операции**	**Выполнение программы гостевой операции**	+**			
	Запросы гостевой операции	+**			
	Изменения гостевых операций	+**			
Виртуальная машина > **Взаимодействие**	**Получение контрольного билета гостя** (в vSphere 4.1 и 5.0)				+
	Настройка носителя CD		+	+	
	Управление гостевой операционной системой с помощью API VIX (в vSphere 5.1 и более поздних версий)				+
	Отключение			+	+
	Включение		+	+	+
Виртуальная машина > **Инвентаризация**	**Создание из существующей**		+	+	+
	Создание новой		+	+	+
	Регистрация				+
	Удаление		+	+	+
	Отмена регистрации				+
Виртуальная машина > **Распределение**	**Разрешение доступа к диску**		+	+	+
	Разрешение доступа к диску только для чтения	+		+	

		Операция			
Объект	**Привилегия**	**Резервное копирование ВМ**	**Восстановление в новую ВМ**	**Восстановление в существующую ВМ**	**Запуск ВМ из резервной копии**
	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.

17.7 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.

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. 63). При настройке восстановления выберите новую машину в качестве целевой.

18 Устранение неисправностей

В этом разделе объясняется, как сохранить журнал агента в ZIP-файл. Этот файл поможет сотрудникам технической поддержки определить проблему в случае неудачного резервного копирования по неясной причине.

Получение журналов

1. Выберите машину, для которой нужно сохранить журналы.
2. Нажмите кнопку **Действия**.
3. Нажмите кнопку **Сбор сведений о системе**.

4. При появлении соответствующего запроса в веб-браузере укажите место сохранения файла.

19 Словарь терминов

Д

Дифференциальное резервное копирование

В дифференциальной резервной копии хранятся изменения, произведенные в данных относительно самой поздней версии полной (стр. 129) 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.

Ф

Формат резервной копии в виде одного файла

Новый формат резервных копий, в котором начальная полная и последующие инкрементные резервные копии сохраняются в одном TIBX-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.