Сервис резервного копирования

Version 8.0

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

Редакция: 12.12.2019

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.

1.1 Выпуски Standard, Advanced и Disaster Recovery

Для соответствия потребностям и бюджетам разных клиентов сервис резервного копирования предлагается в трех выпусках. Единовременно компания клиента может использовать только один выпуск.

- Выпуск **Standard** удовлетворяет потребности, характерные для небольших сред.
- Выпуск **Advanced** предназначен для крупных сред. Он обеспечивает расширенную функциональность резервного копирования и восстановления наряду со всеми функциями выпуска Standard.
- Выпуск **Disaster Recovery** помимо функций резервного копирования и восстановления, которые доступны в выпуске Advanced, предоставляет службу аварийного восстановления.

Указанные ниже функции резервного копирования и восстановления доступны только в выпусках Advanced и Disaster Recovery:

- В новом разделе пользовательского интерфейса показаны все планы резервного копирования и планы репликации ВМ (стр. 130)
- Поддержка групп обеспечения доступности Always On Microsoft SQL Server (стр. 137)
- Поддержка для групп обеспечения доступности баз данных Microsoft Exchange Server (стр. 138)
- Возможность создать статические и динамические группы устройств (стр. 221)
- Сохранение резервных копий каждой машины в папке, определенной сценарием (для машин под управлением Windows) (стр. 50)
- Защита Oracle Database путем резервного копирования с поддержкой приложений и резервного копирования базы данных с использованием RMAN (стр. 192)
- Защита SAP HANA путем резервного копирования всей машины с использованием внутреннего моментального снимка SAP HANA (стр. 192)
- Нотаризация файлов: подтверждение целостности файла и отсутствия изменений в нем с момента резервного копирования (стр. 68)
- ASign: позволяет нескольким людям подписывать файлы в резервной копии (стр. 115)

Служба аварийного восстановления описана в документе «Аварийное восстановление».

2 Требования к программному обеспечению

2.1 Поддерживаемые веб-браузеры

Веб-интерфейс сервиса резервного копирования поддерживает перечисленные ниже браузеры:

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

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

2.2 Поддерживаемые операционные системы и среды

Агент для Windows

Windows XP Professional SP1 (x64), SP2 (x64), SP3 (x86)

Windows Server 2003 SP1/2003 R2 и более поздних версий: выпуски Standard и Enterprise (x86, x64)

Windows Small Business Server 2003/2003 R2

Windows Vista — все выпуски

Windows Server 2008 — выпуски Standard, Enterprise, Datacenter 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

Windows Server 2019: все варианты установки, кроме Nano Server

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

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

Агент для Exchange (для резервного копирования почтового ящика)

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

Windows Small Business Server 2008

Windows 7 — все выпуски

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

Windows MultiPoint Server 2010/2011/2012

Windows Small Business Server 2011 — все выпуски

Windows 8/8.1 — все выпуски (x86, x64), за исключением выпусков Windows RT

Windows Server 2012/2012 R2 — все выпуски

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

Windows 10 — выпуски Home, Pro, Education и Enterprise

Windows Server 2016 — все варианты установки, кроме Nano Server

Windows Server 2019: все варианты установки, кроме Nano Server

Агент для Office 365

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

Windows Small Business Server 2008

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

Windows Small Business Server 2011 — все выпуски

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

Windows Server 2012/2012 R2 — все выпуски

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

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

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

Windows Server 2019 — все варианты установки (только x64), кроме Nano Server

Агент для Oracle

Windows Server 2008 R2 — выпуски Standard, Enterprise, Datacenter и Web (x86, x64)

Windows Server 2012 R2 — выпуски Standard, Enterprise, Datacenter и Web (x86, x64)

Linux: все ядра и дистрибутивы, которые поддерживаются агентом для Linux (перечислены ниже)

Агент для Linux

Linux с версией ядра от 2.6.9 до 5.1 и glibc версии 2.3.4 или более поздней

Различные дистрибутивы Linux x86 и x86_64, включая:

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

Oracle Linux 5.x, 6.x, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6 — Unbreakable Enterprise Kernel и Red Hat Compatible Kernel

CloudLinux 5.x, 6.x, 7, 7.1, 7.2, 7.3, 7.4, 7.5

ClearOS 5.x, 6.x, 7, 7.1, 7.4

ALT Linux 7.0

Перед установкой продукта в системе, в которой не используется диспетчер пакетов RPM, такой как Ubuntu, необходимо установить этот диспетчер вручную, например выполнив следующую команду в качестве суперпользователя: **`apt-get install rpm`**

Агент для Mac

OS X Mavericks 10.9

OS X Yosemite 10.10

OS X El Capitan 10.11

macOS Sierra 10.12

macOS High Sierra 10.13

macOS Mojave 10.14

macOS Catalina 10.15

Агент для VMware (виртуальное устройство)

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

VMware ESXi 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7

Агент для VMware (Windows)

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

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

VMware ESXi 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7

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

Windows Server 2019 с Hyper-V — все варианты установки, кроме Nano Server

Microsoft Hyper-V Server 2019

Агент для Virtuozzo

Virtuozzo 6.0.10, 6.0.11, 6.0.12

2.3 Поддерживаемые версии Microsoft SQL Server

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

2.4 Поддерживаемые версии Microsoft Exchange Server

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

2.5 Поддерживаемые версии 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 версии Oracle Database

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

Поддерживаются только конфигурации с одним экземпляром.

2.7 Поддерживаемые версии SAP HANA

Версия HANA 2.0 SPS 03, установленная в RHEL 7.6 на физической машине или виртуальной машине VMware ESXi.

Поскольку SAP HANA не поддерживает восстановление контейнеров баз данных с несколькими арендаторами с использованием моментальных снимков хранилища, данное решение поддерживает контейнеры SAP HANA с базой данных только одного арендатора.

2.8 Поддерживаемые платформы виртуализации

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

Платформа	Резервное копирование на уровне гипервизора (резервное копирование без агента)	Резервное копирование изнутри гостевой ОС
VMware		
Версии VMware vSphere: 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7 **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 Windows Server 2019 с Hyper-V — все варианты установки, кроме Nano Server Microsoft Hyper-V Server 2019	+	+
Microsoft Virtual PC 2004 и 2007 Windows Virtual PC		+
Microsoft Virtual Server 2005		+
Citrix		
Citrix XenServer 4.1.5, 5.5, 5.6, 6.0, 6.1, 6.2, 6.5, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5		Только полностью виртуализированные (известные также как HVM) гостевые системы
Red Hat и Linux		
Red Hat Enterprise Virtualization (RHEV) 2.2, 3.0, 3.1, 3.2, 3.3, 3.4, 3.5, 3.6 Red Hat Virtualization (RHV) 4.0, 4.1		+
Виртуальные машины на основе ядра (KVM)		+
Parallels		
Parallels Workstation		+
Parallels Server 4 Bare Metal		+
Oracle		
Oracle VM Server 3.0, 3.3, 3.4		Только полностью виртуализированные (известные также как HVM) гостевые системы
Oracle VM VirtualBox 4.x		+

Платформа	Резервное копирование на уровне гипервизора (резервное копирование без агента)	Резервное копирование изнутри гостевой ОС
Nutanix		
Nutanix Acropolis Hypervisor (AHV) 20160925.x–20180425.x		+
Virtuozzo		
Virtuozzo 6.0.10, 6.0.11, 6.0.12	+	(Только виртуальные машины. Контейнеры не поддерживаются)
Amazon		
Экземпляры Amazon EC2		+
Microsoft Azure		
Виртуальные машины Azure		+

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

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

Ограничения

- **Отказоустойчивые машины**

  Агент для VMware выполняет резервное копирование отказоустойчивой машины, только если в VMware vSphere 6.0 и более поздней версии включена отказоустойчивость. При выполнении обновления с более ранней версии vSphere достаточно отключить и снова включить отказоустойчивость для каждой машины. При использовании более ранней версии vSphere установите агент в гостевой операционной системе.

- **Независимые диски и RDM-диски**

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

- **Диски прямого доступа**

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

- **Кластеризация гостевых систем Hyper-V**

Агент для Hyper-V не поддерживает резервное копирование виртуальных машин Hyper-V, которые являются узлами отказоустойчивого кластера Windows Server. Моментальный снимок VSS на уровне хоста может даже временно отключить внешний диск кворума от кластера. Если необходимо выполнить резервное копирование этих машин, установите агенты в гостевых операционных системах.

- **Подключение iSCSI в гостевой ОС**

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

- **Машины Linux с логическими томами (LVM)**

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

  - Миграция P2V, миграция V2P и миграция V2V с Virtuozzo. Создание резервной копии и загрузочного носителя для восстановления с помощью агента для Linux.
  - Запуск виртуальной машины с резервной копии, созданной агентом для Linux.

- **Зашифрованные виртуальные машины** (эта функциональная возможность представлена в VMware vSphere 6.5)
  - Резервное копирование зашифрованных виртуальных машин выполняется в незашифрованном состоянии. Если шифрования является критически важным, включите шифрование резервных копий при создании плана резервного копирования (стр. 66).
  - 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.

- **Резервное копирование конфигурации ESXi** не поддерживается для VMware vSphere 6.7.

2.9 Совместимость с программами шифрования

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

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

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

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

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

Типичные правила установки

Настоятельно рекомендуется установить программу шифрования перед установкой агентов резервного копирования.

Способ использования раздела Зона безопасности

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

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

Общее правило резервного копирования

Позволяет выполнить резервное копирование на уровне дисков операционной системы.

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 rowspan="2">Агент для Mac</td><td>–</td><td>+</td></tr>
<tr><td>APFS</td><td>–</td><td>+</td><td>▪ Поддерживается, начиная с macOS High Sierra 10.13.
▪ При восстановлении на машину, отличную от исходной, или на «голое железо» конфигурацию диска необходимо заново создать вручную.</td></tr>
<tr><td>JFS</td><td rowspan="2">Агент для Linux</td><td>+</td><td>-</td><td rowspan="2">▪ Файлы невозможно исключить из резервной копии диска
▪ Невозможно включить быстрое инкрементное/дифференциальное резервное копирование</td></tr>
<tr><td>ReiserFS3</td><td>+</td><td>-</td></tr>
</table>

<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>ReiserFS4</td><td></td><td>+</td><td>-</td><td rowspan="3">▪ Файлы невозможно исключить из резервной копии диска
▪ Невозможно включить быстрое инкрементное/дифференциальное резервное копирование
▪ Невозможно изменить размер томов при выполнении восстановления</td></tr>
<tr><td>ReFS</td><td rowspan="2">Все агенты</td><td>+</td><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>
<tr><td>exFAT</td><td>Все агенты</td><td>+
Если резервная копия хранится в файловой системе exFAT, загрузочный носитель невозможно использовать для восстановления.</td><td>+</td><td>▪ Поддерживается только резервное копирование дисков/томов
▪ Файлы невозможно исключить из резервной копии
▪ Отдельные файлы невозможно восстановить из резервной копии</td></tr>
</table>

Программное обеспечение автоматически перейдет к посекторному резервному копированию для дисков с нераспознанными или неподдерживаемыми файловыми системами. 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 для активации учетной записи.** Перейдите по этой ссылке, чтобы задать пароль для учетной записи. Запомните свое имя для входа, которое отображается на странице активации учетной записи.

  Если администратор включил двухфакторную проверку подлинности, вам будет предложено настроить двухфакторную проверку подлинности для своих учетных записей (стр. 19).
- **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.

4.1 Двухфакторная проверка подлинности

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

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

Порядок настройки двухфакторной проверки подлинности для вашей учетной записи

1. Выберите устройство второго фактора.

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

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

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

7. Вернитесь на страницу входа на консоль резервного копирования и введите сгенерированный вход.

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

При следующем входе можно установить флажок **Сделать браузер доверенным…**. После этого одноразовый код не будет требоваться при входе с этого браузера и на этой машине.

Что если...

...потеряно устройство второго фактора?

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

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

...мне нужно использовать другое устройство второго фактора?

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

5 Доступ к сервису резервного копирования

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

Вход 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 учетной записи в правом верхнем углу.

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

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

Для каких объектов нужно создать резервные копии?	Какой агент следует установить?	Куда его следует установить?
Физические машины		
Физические машины под управлением Windows	Агент для Windows	На машину, резервная копия которой будет создана.
Физические машины под управлением ОС Linux	Агент для Linux	
Физические машины под управлением macOS	Агент для Mac	
Приложения		
Базы данных SQL	Агент для SQL	На машину с сервером Microsoft SQL Server.
Базы данных Exchange	Агент для Exchange	На машину с ролью почтового ящика Microsoft Exchange Server.
Почтовые ящики Microsoft Office 365	Агент для Office 365	На машину с Windows, которая подключена к Интернету. В зависимости того, какие функции вам нужны, может потребоваться установка агента для Office 365. Дополнительную информацию см. в разделе «Защита данных Office 365» (стр. 159).
Файлы Microsoft Office 365 OneDrive и сайты SharePoint Online	—	Резервное копирование этих данных можно выполнить только с помощью агента, установленного в облаке. Дополнительную информацию см. в разделе «Защита данных Office 365» (стр. 159).
Почтовые ящики Gmail G Suite, файлы Google Диск и файлы общего диска	—	Резервное копирование этих данных можно выполнить только с помощью агента, установленного в облаке. Дополнительную информацию см. в разделе «Защита G Suite» (стр. 178).

Для каких объектов нужно создать резервные копии?	Какой агент следует установить?	Куда его следует установить?
Машины с доменными службами Active Directory	Агент для Active Directory	На контроллер домена.
Машины под управлением Oracle Database	Агент для Oracle	На машине с запущенной Oracle Database.
Виртуальные машины		
Виртуальные машины VMware ESXi	Агент для VMware (Windows)	На машину под управлением Windows с сетевым доступом к vCenter Server и хранилищу виртуальных машин.*
	Агент для VMware (виртуальное устройство)	На хосте ESXi.
Виртуальные машины Hyper-V	Агент для Hyper-V	На хост Hyper-V.
Виртуальные машины 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		
Виртуальные машины Nutanix AHV		
Мобильные устройства		
Мобильные устройства с Android	Мобильное приложение для Android	На мобильное устройство, резервную копию которого нужно создать.
Мобильные устройства с iOS	Мобильное приложение для iOS	

* 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. 208).

**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.

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

Шаг 3

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

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

Чтобы сохранить программы установки локально, загрузите пакет со всеми агентами для установки в Windows по ссылке в нижней части страницы **Добавить устройства**. Доступны 32-разрядный и 64-разрядный пакеты. Эти пакеты позволяют настроить список компонентов для установки. С помощью этих пакетов также можно настроить автоматическую установку (например, с использованием групповой политики). Этот расширенный сценарий описан в разделе Развертывание агентов с использованием групповой политики.

Чтобы загрузить программу установки агента для Office 365, щелкните значок учетной записи в правом верхнем углу, а затем выберите пункты **Загрузки** > **Агент для Office 365**.

Установка в ОС Linux и macOS 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. 27), который поможет понять, нужно ли конфигурировать эти настройки на каждой машине с запущенным агентом резервного копирования.

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

6.2 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.
- Библиотека **`libelf-dev`**, **`libelf-devel`** или **`elfutils-libelf-devel`** для сборки ядер, которые имеют версии не ниже 4.15 и настроены с параметром CONFIG_UNWINDER_ORC=y. Для некоторых дистрибутивов, например Fedora 28, их необходимо установить отдельно от заголовков ядра.

Имена этих пакетов зависят от используемого дистрибутива Linux.

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

Установлены ли необходимые пакеты?

Чтобы проверить, установлены ли пакеты, сделайте следующее:

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

   ```
   cat /proc/version
   ```

   Эта команда возвращает примерно такие строки: **`Linux version 2.6.35.6`** и **`gcc version 4.5.1`**
2. Выполните следующую команду, чтобы узнать, установлен ли инструмент Make и компилятор GCC:

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

   Для **gcc** убедитесь, что команда возвращает ту же версию, что и в параметре **`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, что версии пакетов такие же, как в параметре **`Linux version`** в шаге 1.
4. Чтобы выяснить, установлен ли интерпретатор Perl, выполните следующую команду:

   ```
   perl --version
   ```

   Если на экране отображаются сведения о версии Perl, это означает, что интерпретатор установлен.
5. В Red Hat Enterprise Linux, CentOS и Fedora выполните следующую команду, чтобы проверить, установлена ли библиотека **`elfutils-libelf-devel`**:

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

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

Установка пакетов из репозитория

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

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

	perl	Выполните следующую команду: `yum install perl`

Ubuntu
Debian
	linux-headers
	linux-image
	gcc
	make
	perl
		Выполните следующие команды:
		`sudo apt-get update`
		`sudo apt-get install linux-headers-$(uname -r)`
		`sudo apt-get install linux-image-$(uname -r)`
		`sudo apt-get install gcc-<package version>`
		`sudo apt-get install make`
		`sudo apt-get install perl`

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

Пакеты будут загружены из репозитория дистрибутива и установлены.

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

Установка пакетов вручную

Возможно, необходимо будет установить пакеты **вручную**, если:

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

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

- В Red Hat Enterprise Linux, CentOS и Fedora выполните следующую команду как привилегированный пользователь:
  ```
  rpm -ivh 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 этой версии ядра:
   ```
   kernel-devel-2.6.35.6-45.fc14.i686.rpm
   gcc-4.5.1-4.fc14.i686.rpm
   ```

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

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

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

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

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

6.3 Настройки прокси-сервера

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

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

В Windows

Если прокси-сервер настроен в Windows (**Панель управления** > **Свойства браузера** > **Подключения**), то программа установки считает настройки прокси-сервера из реестра и использует их автоматически. Кроме того, можно задать настройки прокси-сервера во время установки (стр. 29) или указать их заранее, используя процедуру, описанную ниже. С помощью той же процедуры эти параметры можно изменить после установки.

Указание параметров прокси-сервера в Windows

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

```
Windows Registry Editor Version 5.00

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

3. Замените `proxy.company.com` именем хоста или IP-адресом прокси-сервера, а `000001bb` — шестнадцатеричным значением номера порта. Например, `000001bb` соответствует номеру порта 443.
4. Если на прокси-сервере необходимо пройти аутентификацию, вместо строк `proxy_login` и `proxy_password` укажите учетные данные прокси-сервера. В противном случае удалите эти строки из файла.
5. Сохраните документ с именем **proxy.reg**.
6. Запустите файл от имени администратора.
7. Подтвердите изменение реестра Windows.
8. Если агент 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
```

В ОС Linux

Запустите установочный файл с параметрами **--http-proxy-host=**АДРЕС **--http-proxy-port=**ПОРТ **--http-proxy-login=**ИМЯ ВХОДА **--http-proxy-password=**ПАРОЛЬ. Чтобы изменить параметры прокси-сервера после установки, используйте описанную ниже процедуру.

Именение параметров прокси-сервера в Linux

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

     ```
     <key name="HttpProxy">
         <value name="Enabled" type="Tdword">"1"</value>
         <value name="Host" type="TString">"АДРЕС"</value>
         <value name="Port" type="Tdword">"ПОРТ"</value>
         <value name="Login" type="TString">"ИМЯ ВХОДА"</value>
         <value name="Password" type="TString">"ПАРОЛЬ"</value>
     </key>
     ```

   - Вы также можете скопировать приведенные выше строки и вставить их между тегами **<registry name="Global">...</registry>**.
3. Замените АДРЕС новым именем хоста или IP-адресом прокси-сервера, а ПОРТ — номером порта в десятичном формате.
4. Если на прокси-сервере необходимо пройти аутентификацию, вместо дескрипторов ИМЯ ВХОДА и ПАРОЛЬ укажите учетные данные прокси-сервера. В противном случае удалите эти строки из файла.
5. Сохраните файл.
6. Перезапустите агент, выполнив следующую команду в любом каталоге:

   ```
   sudo service acronis_mms restart
   ```

В macOS

Параметры прокси-сервера можно указать во время установки (стр. 29) или заранее, как описано в процедуре ниже. С помощью той же процедуры эти параметры можно изменить после установки.

Указание параметров прокси-сервера в macOS

1. Создайте файл **/Library/Application Support/Acronis/Registry/Global.config** и откройте его в текстовом редакторе, например Text Edit.
2. Скопируйте и вставьте в файл следующие строки <?xml version="1.0" ?>
   <registry name="Global">
     <key name="HttpProxy">
       <value name="Enabled" type="Tdword">"1"</value>
       <value name="Host" type="TString">"proxy.company.com"</value>
       <value name="Port" type="Tdword">"443"</value>
       <value name="Login" type="TString">"proxy_login"</value>
       <value name="Password" type="TString">"proxy_password"</value>

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

3. Замените `proxy.company.com` именем хоста или IP-адресом прокси-сервера, а `443` — номером порта в десятичном формате.
4. Если на прокси-сервере необходимо пройти аутентификацию, вместо строк `proxy_login` и `proxy_password` укажите учетные данные прокси-сервера. В противном случае удалите эти строки из файла.
5. Сохраните файл.
6. Если агент 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
```

На загрузочном носителе

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

6.4 Установка агентов

В Windows

1. Убедитесь в том, что машина подключена к Интернету.
2. Войдите как администратор и запустите программу установки.
3. [Необязательно] Щелкните **Настройка параметров установки** и внесите нужные изменения (при необходимости):
   - Изменение устанавливаемых компонентов (в частности, отмена установки монитора резервного копирования и программы командной строки).
   - Изменение метода регистрации машины в сервисе резервного копирования. Можно изменить параметр **Использовать консоль резервного копирования** (по умолчанию) на **Использовать учетные данные** или **Использовать маркер регистрации**.
   - Изменение пути установки.
   - Изменение учетной записи для службы агента.
   - Проверка или изменение имени хоста или IP-адреса, порта и учетных данных прокси-сервера. Если прокси-сервер включен в Windows, он определяется и используется автоматически.
4. Нажмите **Установить**.
5. [Только при установке агента для VMware] Укажите адрес и учетные данные доступа для сервера vCenter Server или автономного хоста ESXi, для которых агент будет создавать резервные копии виртуальных машин, и нажмите кнопку **Готово**. Рекомендуется использовать учетную запись, которой назначена роль **Администратор**. В противном случае укажите учетную запись с необходимыми привилегиями (стр. 215) на vCenter Server или ESXi.
6. [Только при установке на контроллер домена] Укажите учетную запись пользователя, под которой будет работать служба агента, и нажмите кнопку **Готово**. В целях безопасности

программа установки не может автоматически создавать учетные записи на контроллере домена.

7. Если вы оставили способ регистрации по умолчанию **Использовать консоль резервного копирования** в шаге 3, дождитесь появления экрана регистрации и перейдите к следующему шагу. Если нет, дополнительных действий не требуется.
8. Выполните одно из следующих действий:
   - Щелкните **Зарегистрировать машину**. В открытом окне браузере войдите на консоль резервного копирования, проверьте регистрационные сведения и щелкните **Подтвердить регистрацию**.
   - Щелкните **Показать регистрационные сведения**. В программе установки будет показана ссылка на регистрацию и код регистрации. Можно скопировать их и пройти все необходимые этапы регистрации на другой машине. В этом случае необходимо будет ввести код регистрации в форме регистрации. Код регистрации действует только один час.

   В качестве альтернативного варианта доступ к форме регистрации можно получить следующим образом: выберите **Все устройства** > **Добавить**, прокрутите вниз до поля **Регистрация по коду** и нажмите кнопку **Регистрация**.

   Совет *Не выходите из программы установки до подтверждения регистрации. Чтобы начать регистрацию заново, необходимо перезапустить программу установки и щелкнуть* ***Зарегистрировать машину****.*

   Это приведет к тому, что машина будет назначена учетной записи, которая была использована для входа на консоль резервного копирования.

В ОС Linux

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

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

   Если вы хотите изменить метод регистрации машины в службе резервного копирования, используемый по умолчанию, запустите установочный файл с одним из следующих параметров:
   - **--register-with-credentials** — запрос имени пользователя и пароля во время установки;
   - **--token=STRING** — использование маркера регистрации;
   - **--skip-registration** — пропуск регистрации.
3. 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.
4. Если вы оставили метод регистрации по умолчанию в шаге 2, перейдите к следующему шагу. В противном случае введите имя пользователя и пароль для службы резервного копирования или дождитесь регистрации машины с использованием маркера.
5. Выполните одно из следующих действий:

- Щелкните **Зарегистрировать машину**. В открытом окне браузере войдите на консоль резервного копирования, проверьте регистрационные сведения и щелкните **Подтвердить регистрацию**.
- Щелкните **Показать регистрационные сведения**. В программе установки будет показана ссылка на регистрацию и код регистрации. Можно скопировать их и пройти все необходимые этапы регистрации на другой машине. В этом случае необходимо будет ввести код регистрации в форме регистрации. Код регистрации действует только один час.

В качестве альтернативного варианта доступ к форме регистрации можно получить следующим образом: выберите **Все устройства** > **Добавить**, прокрутите вниз до поля **Регистрация по коду** и нажмите кнопку **Регистрация**.

Совет *Не выходите из программы установки до подтверждения регистрации. Чтобы начать регистрацию заново, необходимо будет перезапустить программу установки и повторить процедуру установки.*

Это приведет к тому, что машина будет назначена учетной записи, которая была использована для входа на консоль резервного копирования.

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

Примечание. *Во время установки создается новый ключ для подписания модуля* ***snapapi****. Этот ключ регистрируется как ключ владельца машины (Machine Owner Key, MOK). Для регистрации этого ключа необходимо перезапустить систему. Если не зарегистрировать ключ, агент не будет работать. Если безопасная загрузка UEFI включена после установки агента, повторите установку, включая шаг 6.*

7. После завершения установки выполните одно из следующих действий.
   - Нажмите кнопку **Перезапустить**, если в предыдущем шаге вам было предложено перезапустить систему.

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

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

В macOS

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

- Щелкните **Зарегистрировать машину**. В открытом окне браузере войдите на консоль резервного копирования, проверьте регистрационные сведения и щелкните **Подтвердить регистрацию**.
- Щелкните **Показать регистрационные сведения**. В программе установки будет показана ссылка на регистрацию и код регистрации. Можно скопировать их и пройти все необходимые этапы регистрации на другой машине. В этом случае необходимо будет ввести код регистрации в форме регистрации. Код регистрации действует только один час.

В качестве альтернативного варианта доступ к форме регистрации можно получить следующим образом: выберите **Все устройства** > **Добавить**, прокрутите вниз до поля **Регистрация по коду** и нажмите кнопку **Регистрация**.

Совет *Не выходите из программы установки до подтверждения регистрации. Чтобы начать регистрацию заново, необходимо будет перезапустить программу установки и повторить процедуру установки.*

Это приведет к тому, что машина будет назначена учетной записи, которая была использована для входа на консоль резервного копирования.

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

6.5.1 Перед началом

Системные требования для агента

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

Виртуальные диски устройства занимают не более 6 ТБ. Формат диска («толстый» или «тонкий») не влияет на производительность устройства.

Сколько агентов необходимо?

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

Вполне нормально одновременно использовать виртуальное устройство и агент для VMware (Windows), когда они подключены к одному vCenter Server *или* разным хостам ESXi. Избегайте сценариев, когда один агент подключен к хосту ESXi напрямую, а другой агент подключен к vCenter Server, который управляет этим хостом ESXi.

Если у вас несколько агентов, не рекомендуем использовать локальное хранилище данных (т. е. хранить резервные копии на виртуальных дисках, добавленных в виртуальное устройство). Дополнительную информацию см. в разделе «Использование локально присоединенного хранилища» (стр. 211).

Отключить автоматический DRS для агента

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

6.5.2 Развертывание шаблона OVF

1. Последовательно выберите пункты **Все устройства** > **Добавить** > **VMware ESXi** > **Virtual Appliance (OVF)**.

   ZIP-архив загрузится на машину.
2. Распакуйте ZIP-архив. Папка содержит один OVF-файл и два VMDK-файла.
3. Убедитесь в том, что эти файлы доступны с машины с клиентом vSphere.
4. Запустите клиент vSphere и выполните вход на сервер vCenter Server.
5. Разверните шаблон OVF.
   - При настройке хранилища данных выберите общее хранилище данных, если оно существует. Формат диска («толстый» или «тонкий») не имеет значения, поскольку не влияет на производительность устройства.
   - При настройке сетевых подключений убедитесь, что выбранная сеть позволяет подключиться к Интернету. Это необходимо, чтобы агент мог зарегистрироваться в облаке.

6.5.3 Настройка виртуального устройства

1. **Запуск виртуального устройства**

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

   Если в вашей сети есть прокси-сервер:

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

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

   c. Найдите следующий раздел:

   ```
   <key name="HttpProxy">
       <value name="Enabled" type="Tdword">"0"</value>
       <value name="Host" type="TString">"АДРЕС"</value>
       <value name="Port" type="Tdword">"ПОРТ"</value>
       <value name="Login" type="TString">"ИМЯ ВХОДА"</value>
       <value name="Password" type="TString">"ПАРОЛЬ"</value>
   </key>
   ```

   d. Замените **0** на **1**.

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

   f. Если на прокси-сервере необходимо пройти аутентификацию, вместо дескрипторов ИМЯ ВХОДА и ПАРОЛЬ укажите учетные данные прокси-сервера. В противном случае удалите эти строки из файла.

   g. Сохраните файл.

h. Выполните команду **reboot**.

В противном случае пропустите этот шаг.

3. **Сетевые настройки**

   Сетевое подключение агента настраивается автоматически с помощью протокола DHCP. Чтобы изменить конфигурацию по умолчанию, в подразделе **eth0** раздела **Параметры агента** нажмите кнопку **Изменить** и укажите нужные сетевые настройки.

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

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

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

   Укажите учетные данные, которые будут использоваться агентом для подключения к vCenter Server или ESXi. Рекомендуется использовать учетную запись, которой назначена роль **Администратор**. В противном случае укажите учетную запись с необходимыми привилегиями (стр. 215) на vCenter Server или ESXi.

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

5. **Сервер управления**

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

   b. В поле **Имя/IP-адрес сервера** выберите **Облако**. В программе отображается адрес сервиса резервного копирования. Не меняйте этот адрес, если иное не указано в инструкции.

   c. В полях **Имя пользователя** и **Пароль** укажите имя пользователя и пароль для сервиса резервного копирования. Агент и виртуальные машины, управляемые агентом, будут зарегистрированы с этой учетной записью.

6. **Часовой пояс**

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

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

   К виртуальному устройству можно присоединить дополнительный диск, чтобы агент для VMware мог сохранять резервные копии на этом локально присоединенном хранилище (стр. 211).

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

6.6 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. Формирование маркера регистрации

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

Формирование маркера регистрации

1. Войдите на консоль резервного копирования с учетными данными той учетной записи, для которой необходимо назначить машины.
2. Щелкните **Все устройства** > **Добавить**.
3. Прокрутите вниз до поля **Маркер регистрации** и нажмите кнопку **Создать**.
4. Укажите срок действия маркера и нажмите кнопку **Создать маркер**.
5. Скопируйте маркер или запишите его. Сохраните маркер, если он понадобится в будущем.

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

Шаг 2. Создание MST-преобразования и извлечение пакета установки

1. Войдите как администратор на любую машину в домене.
2. Создайте общую папку, в которой будут находиться пакеты установки. Убедитесь, что у пользователей домена есть доступ к этой папке (для этого можно, например, оставить значение параметра общего доступа по умолчанию для категории **Все**).
3. Запустите программу установки.
4. Щелкните **Создать MST- и MSI-файлы для автоматической установки**.
5. Щелкните **Указать** рядом с пунктом **Настройки регистрации** и введите созданный маркер.

   Можно изменить способ регистрации машины в службе резервного копирования с **Использовать маркер регистрации** (по умолчанию) на **Использовать учетные данные** или **Пропустить регистрацию**. Выбор параметра **Пропустить регистрацию** предполагает, что вы зарегистрируете машину позже.
6. Проверьте и при необходимости измените настройки установки, которые будут добавлены в MST-файл, затем нажмите кнопку **Продолжить**.
7. В поле **Сохранить файлы в** укажите путь к созданной папке.
8. Нажмите кнопку **Создать**.

В результате будет сформировано MST-преобразование, а установочные MSI-пакеты и CAB-пакеты будут извлечены в созданную вами папку.

Шаг 3. Настройка объектов групповой политики

1. Войдите на контроллер домена с правами администратора домена. Если в домене больше одного контроллера, это можно сделать на любом из них.
2. Если вы планируете развернуть агент в рамках организационной единицы, она должна быть создана до начала установки. В противном случае пропустите этот шаг.
3. В меню **Пуск** выберите пункт **Администрирование**, а затем щелкните **Пользователи и компьютеры Active Directory** (в ОС Windows Server 2003) или **Управление групповой политикой** (в Windows Server 2008 или более поздних версий).
4. В Windows Server 2003:
   - Правой кнопкой мыши щелкните имя домена или организационной единицы и выберите пункт **Свойства**. В диалоговом окне перейдите на вкладку **Групповая политика** и нажмите кнопку **Создать**.

   В Windows Server 2008 или более поздних версий:
   - Правой кнопкой мыши щелкните имя домена или организационной единицы, а затем щелкните **Создать объект GPO в этом домене и связать его**.
5. Назовите новый объект групповой политики **Агент для Windows**.
6. Откройте объект групповой политики **Агент для Windows** для изменения с помощью описанных ниже действий:
   - В Windows Server 2003 щелкните объект групповой политики, а затем выберите **Изменить**.
   - В Windows Server 2008 или более поздних версий в разделе **Объекты групповой политики** щелкните правой кнопкой мыши объект групповой политики, а затем щелкните **Изменить**.
7. В оснастке «Редактор объектов групповой политики» разверните узел **Конфигурация компьютера**.
8. В Windows Server 2003 и Windows Server 2008:
   - Разверните узел **Конфигурация программ**.

   В Windows Server 2012 или более поздних версий:
   - Разверните узел **Политики** > **Конфигурация программ**.
9. Щелкните правой кнопкой мыши узел **Установка программ**, выберите пункт **Создать**, затем щелкните **Пакет**.
10. Выберите MSI-пакет установки агента в созданной ранее общей папке и нажмите кнопку **Открыть**.
11. В диалоговом окне **Развертывание программ** выберите **особый**, затем нажмите кнопку **ОК**.
12. На вкладке **Изменения** нажмите кнопку **Добавить** и выберите созданное ранее MST-преобразование.
13. Нажмите кнопку **ОК**, чтобы закрыть диалоговое окно **Развертывание программ**.

6.7 Обновление агентов

Агенты указанных ниже версий можно обновить через веб-интерфейс.

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

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

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

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**.

Порядок обновления агента для VMware (виртуального устройства)

1. Щелкните **Настройки** > **Агенты**, выберите агент, который необходимо обновить, затем щелкните **Сведения** и изучите данные раздела **Назначенные виртуальные машины**. После обновления необходимо заново ввести эти настройки.
   a. Запомните положение переключателя **Автоматическое назначение**.
   b. Чтобы узнать, какие виртуальные машины вручную назначены этому агенту, щелкните ссылку **Назначено:**. В программе будет выведен список назначенных виртуальных машин. Запишите виртуальные машины, которые имеют букву **(M)** после имени агента в столбце **Агент**.
2. Удалите агент для VMware (виртуальное устройство), как описано в разделе "Удаление агентов" (стр. 38). В шаге 5 удалите агент из раздела **Настройки** > **Агенты**, даже если вы планируете установить агент снова.
3. Разверните агент для VMware (виртуальное устройство), как описано в разделе "Развертывание шаблона OVF" (стр. 33).
4. Настройте агент для VMware (виртуальное устройство), как описано в разделе "Настройка виртуального устройства" (стр. 33).

   Чтобы восстановить локальное хранилище данных, в шаге 7 выполните следующие действия:
   a. Добавьте на виртуальное устройство диск с локальным хранилищем данных.
   b. Последовательно выберите пункты **Обновить** > **Создать хранилище** > **Подключить**.
   c. В программе отображается оригинальная **буква** и **метка** диска. Не меняйте их.
   d. Нажмите кнопку **ОК**.
5. Щелкните **Настройки** > **Агенты**, выберите агент, который необходимо обновить, затем щелкните **Сведения** и восстановите настройки, которые вы записали на шаге 1. Если агенту были вручную назначены виртуальные машины, назначьте их снова, как описано в разделе «Привязка виртуальной машины» (стр. 212).

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

6.8 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 Агент резервного копирования**> **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 последовательно выберите пункты **Настройки** > **Агенты**, выберите машину с установленным агентом и 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 последовательно выберите пункты **Настройки** > **Агенты**, выберите машину с установленным агентом и щелкните **Удалить**.

В macOS

1. Дважды щелкните DMG-файл установки.
2. Дождитесь, пока операционная система подключит образ установочного диска.
3. В данном образе дважды щелкните **Удалить**.
4. При необходимости введите учетные данные администратора.
5. Подтвердите операцию.
6. Если планируется установить агент снова, пропустите этот шаг. В противном случае на консоли резервного копирования последовательно выберите пункты **Настройки** > **Агенты**, выберите машину с установленным агентом и щелкните **Удалить**.

Удаление агента для VMware (виртуальное устройство)

1. Запустите клиент vSphere и выполните вход на сервер vCenter Server.

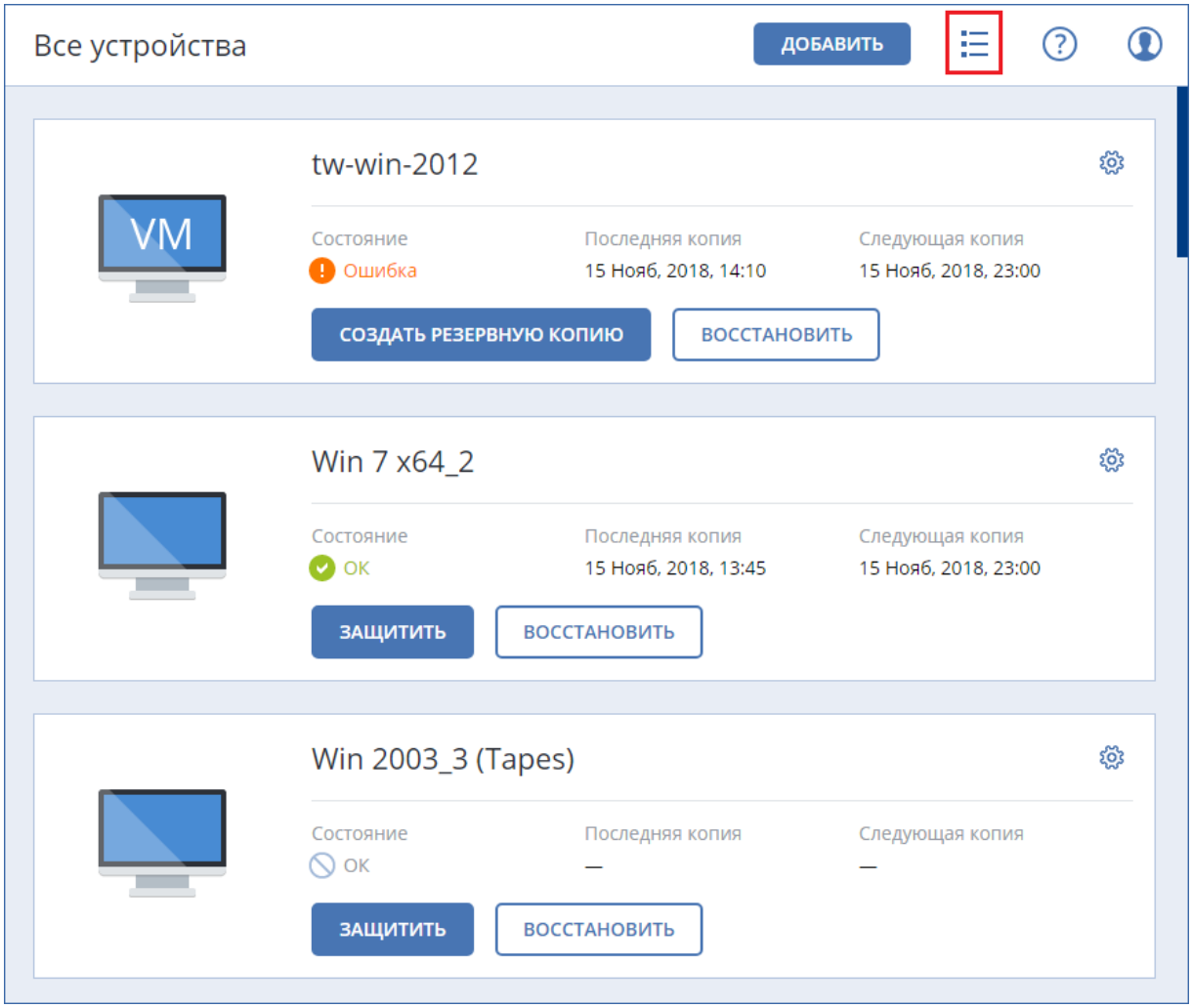
2. Если виртуальное устройство включено, щелкните его правой кнопкой мыши, а затем выберите пункт **Питание** > **Выключить питание**. Подтвердите операцию.
3. Если виртуальное устройство использует локально присоединенное хранилище на виртуальном диске и нужно сохранить данные на диске, выполните указанные ниже действия.
   a. Щелкните ВУ правой кнопкой мыши и выберите пункт **Изменить настройки**.
   b. Выберите диск с хранилищем и щелкните **Удалить**. В разделе **Параметры удаления** нажмите кнопку **Удалить из виртуальной машины**.
   c. Нажмите кнопку **ОК**.

   В результате диск остается в хранилище данных. Можно подключить другой диск к другому виртуальному устройству.
4. Щелкните ВУ правой кнопкой мыши и выберите пункт **Удалить с диска**. Подтвердите операцию.
5. Если планируется установить агент снова, пропустите этот шаг. В противном случае на консоли резервного копирования выполните следующие действия:
   a. Последовательно выберите пункты **Настройки** > **Агенты**, затем выберите виртуальное устройство и щелкните **Удалить**.
   b. Щелкните **Резервные копии** > **Хранилища** и удалите локальное хранилище.

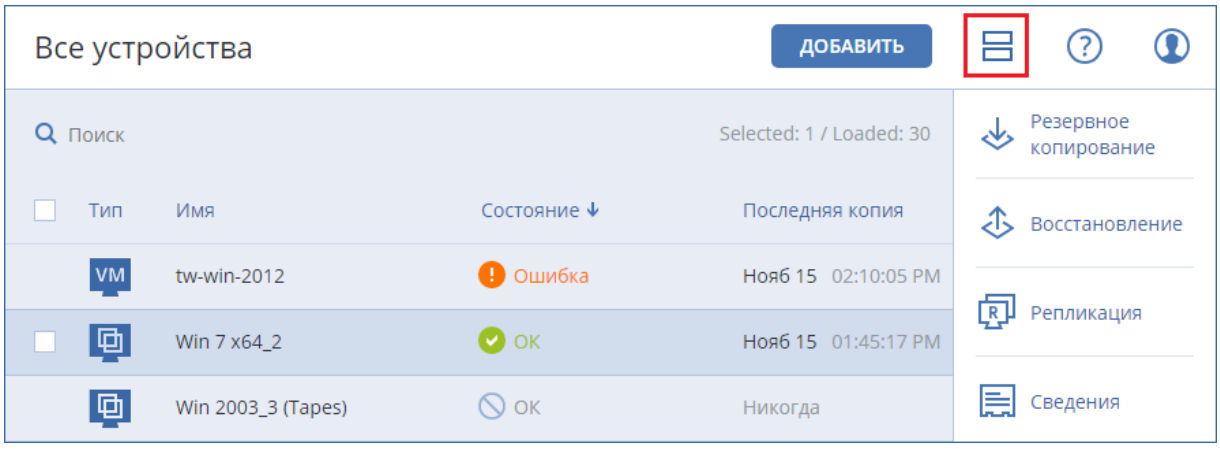
7 Представления консоли резервного копирования

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

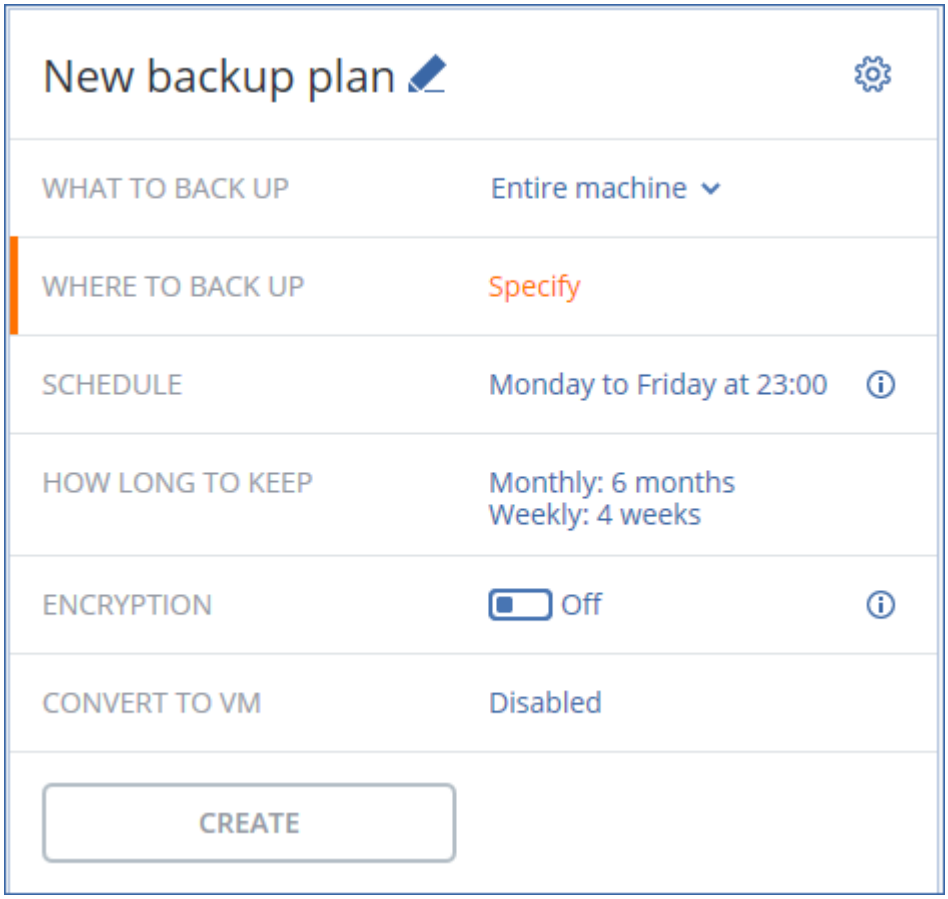
План резервного копирования —это набор правил, который определяет порядок защиты данных на соответствующей машине.

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.

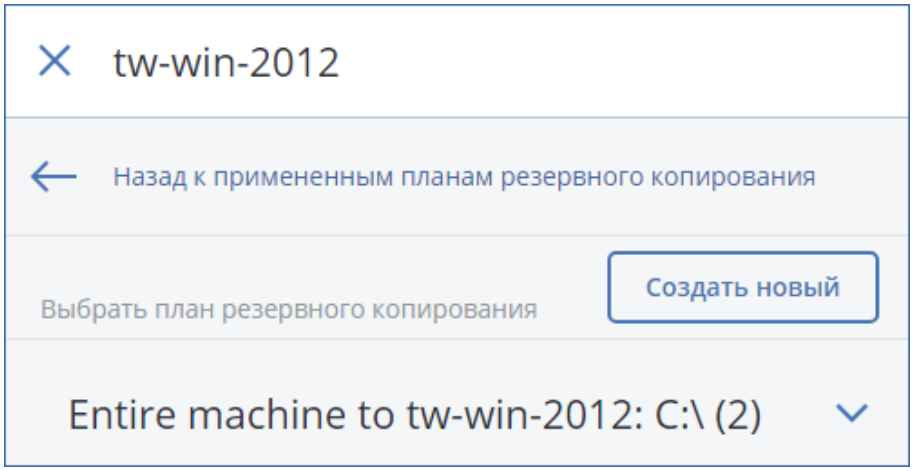


3. [Необязательно] Чтобы изменить имя плана резервного копирования, щелкните имя по умолчанию.
4. Необязательно: чтобы изменить параметры плана, щелкните соответствующий раздел на его панели.
5. [Необязательно] Чтобы изменить параметры резервного копирования, щелкните значок шестеренки.
6. Нажмите кнопку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

Применение существующего плана резервного копирования

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

В программе отображаются ранее созданные планы резервного копирования.



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

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**	**ВРЕМЯ ХРАНЕНИЯ**
Диски/тома (физические машины)	Непосредственный выбор (стр. 44) Правила политики (стр. 44) Фильтры файлов (стр. 84)	Облако (стр. 50) Локальная папка (стр. 50) Сетевая папка (стр. 50) NFS (стр. 50)* Зона безопасности (стр. 50)**	Всегда инкрементное (один файл) (стр. 54) Всегда полное (стр. 54) Еженедельно полное, ежедневно инкрементное (стр. 54) Ежемесячно полное, еженедельно дифференциальное, ежедневно инкрементное (GFS) (стр. 54) Настраиваемый вариант (П-Д-И) (стр. 54)	По возрасту резервной копии (одно правило на набор резервных копий) (стр. 64) По количеству резервных копий (стр. 64) По общему размеру резервных копий (стр. 64)*** Хранить бессрочно (стр. 64)
Диски/тома (виртуальные машины)	Правила политики (стр. 44) Фильтры файлов (стр. 84)	Облако (стр. 50) Локальная папка (стр. 50) Сетевая папка (стр. 50) NFS (стр. 50)*		

<table>
<tr><th colspan="2">ЭЛЕМЕНТЫ ДЛЯ РЕЗЕРВНОГО КОПИРОВАНИЯ</th><th>ЭЛЕМЕНТЫ ДЛЯ РЕЗЕРВНОГО КОПИРОВАНИЯ
Способы выбора</th><th>МЕСТО СОХРАНЕНИЯ</th><th>РАСПИСАНИЕ
Схемы резервного копирования</th><th>ВРЕМЯ ХРАНЕНИЯ</th></tr>
<tr><td colspan="2">Файлы (только физические машины)</td><td>Непосредственный выбор (стр. 47)
Правила политики (стр. 47)
Фильтры файлов (стр. 84)</td><td>Облако (стр. 50)
Локальная папка (стр. 50)
Сетевая папка (стр. 50)
NFS (стр. 50)*
Зона безопасности (стр. 50)**</td><td rowspan="2">Всегда инкрементное (один файл) (стр. 54)
Всегда полное (стр. 54)
Еженедельно полное, ежедневно инкрементное (стр. 54)
Ежемесячно полное, еженедельно дифференциальное, ежедневно инкрементное (GFS) (стр. 54)
Настраиваемый вариант (П-Д-И) (стр. 54)</td><td rowspan="13"></td></tr>
<tr><td colspan="2">Конфигурация ESXi</td><td>Непосредственный выбор (стр. 49)</td><td>Локальная папка (стр. 50)
Сетевая папка (стр. 50)
NFS (стр. 50)*</td></tr>
<tr><td colspan="2">Веб-сайты (файлы и базы данных MySQL)</td><td>Непосредственный выбор (стр. 195)</td><td>Облако (стр. 50)</td><td>—</td></tr>
<tr><td colspan="2">Состояние системы</td><td>Непосредственный выбор (стр. 49)</td><td rowspan="3">Облако (стр. 50)
Локальная папка (стр. 50)
Сетевая папка (стр. 50)</td><td rowspan="3">Всегда полное (стр. 54)
Еженедельно полное, ежедневно инкрементное (стр. 54)
Настраиваемый вариант (П-И) (стр. 54)</td></tr>
<tr><td colspan="2">Базы данных SQL</td><td>Непосредственный выбор (стр. 135)</td></tr>
<tr><td colspan="2">Базы данных Exchange</td><td>Непосредственный выбор (стр. 136)</td></tr>
<tr><td rowspan="4">Microsoft Office 365</td><td>почтовые ящики; (локальный агент для Office 365)</td><td>Непосредственный выбор (стр. 162)</td><td>Облако (стр. 50)
Локальная папка (стр. 50)
Сетевая папка (стр. 50)</td><td>Всегда инкрементное (один файл) (стр. 54)</td></tr>
<tr><td>почтовые ящики; (облачный агент для Office 365)</td><td>Непосредственный выбор (стр. 166)</td><td rowspan="3">Облако (стр. 50)</td><td rowspan="3">—</td></tr>
<tr><td>общие папки;</td><td>Непосредственный выбор (стр. 166)</td></tr>
<tr><td>Файлы OneDrive</td><td>Непосредственный выбор (стр. 171)
Правила политики (стр. 171)</td></tr>
</table>

ЭЛЕМЕНТЫ ДЛЯ РЕЗЕРВНОГО КОПИРОВАНИЯ		ЭЛЕМЕНТЫ ДЛЯ РЕЗЕРВНОГО КОПИРОВАНИЯ Способы выбора	МЕСТО СОХРАНЕНИЯ	РАСПИСАНИЕ Схемы резервного копирования	ВРЕМЯ ХРАНЕНИЯ
	Данные SharePoint Online	Непосредственный выбор (стр. 175) Правила политики (стр. 175)			
G Suite	Почтовые ящики Gmail	Непосредственный выбор (стр. 181)	Облако (стр. 50)	—	
	Файлы Google Диск	Непосредственный выбор (стр. 185) Правила политики (стр. 185)			
	Файлы общего диска	Непосредственный выбор (стр. 188) Правила политики (стр. 188)			

* Резервное копирование в общие папки NFS недоступно в Windows.

** Невозможно создать Зону безопасности на компьютере Mac.

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

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.

Есть два способа выбора дисков/томов: непосредственно на каждой машине или с помощью правил политики. Исключить файлы из резервной копии можно с помощью фильтров файлов (стр. 84).

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 macOS

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

Правила для Windows

- Буква диска (например, **C:**) обозначает том с указанной буквой.
- **[Fixed Volumes (Physical machines)]** 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 путь к нему, отображаемый после выполнения команды **ls /dev/mapper** в учетной записи привилегированного пользователя. Например:

```
[root@localhost ~]# ls /dev/mapper/
control vg_1-lv1 vg_1-lv2
```

В выходных данных отображаются два логических тома, **lv1** и **lv2**, принадлежащие к группе томов **vg_1**. Для создания резервных копий этих томов введите:

```
/dev/mapper/vg_1-lv1
/dev/mapper/vg-1-lv2
```

Правила для macOS

- **[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. 97) **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. 98)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 для физических и виртуальных машин, если для них настроено резервное копирование с помощью агента, установленного в гостевой системе.

Для восстановления операционной системы резервной копии на уровне файлов недостаточно. Выберите этот способ, если необходимо сохранять только определенные данные (например, текущий проект). Это позволит уменьшить размер архива и тем самым сократить потребность в дисковом пространстве.

Есть два способа выбора файлов: непосредственно на каждой машине или с помощью правил политики. Для каждого из этих способов выбор можно уточнить с помощью фильтров файлов (стр. 84).

Непосредственный выбор

1. В области **Элементы для резервного копирования** выберите вариант **Файлы/папки**.
2. Нажмите **Элементы для резервного копирования**.
3. В области **Выберите элементы для резервного копирования** выберите вариант **Непосредственно**.
4. Для каждой машины, включенной в план резервного копирования, выполните указанные ниже действия.
   a. Щелкните **Выбрать файлы и папки**.
   b. Щелкните **Локальная папка** или **Сетевая папка**.

      Общая папка должна быть доступна с выбранной машины.
   c. Перейдите к требуемым файлам и папкам или введите путь и нажмите кнопку со стрелкой. Если потребуется, укажите имя пользователя и пароль для доступа к общей папке.

      Резервное копирование папки с анонимным доступом не поддерживается.
   d. Выберите файлы и папки.
   e. Нажмите кнопку **Готово**.

Использование правил политики

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

Правила политики будут применены ко всем машинам, которые входят в план резервного копирования. Если на машине при запуске резервного копирования отсутствуют объекты, соответствующие хотя бы одному правилу, копирование завершится сбоем.

5. Нажмите кнопку **Готово**.

Правила выбора для Windows

- Полный путь к файлу или папке, например **D:\Work\Text.doc** или **C:\Windows**.
- Шаблоны
  - **[All Files]** позволяет выбрать все файлы на всех томах машины.
  - **[All Profiles Folder]** позволяет выбрать папку, в которой хранятся все профили пользователей (обычно это **C:\Users** или **C:\Documents and Settings**).
- Переменные среды:
  - **%ALLUSERSPROFILE%** позволяет выбрать папку, в которой хранятся общие данные всех профилей пользователей (обычно это **C:\ProgramData** или **C:\Documents and Settings\All Users**).
  - **%PROGRAMFILES%** позволяет выбрать папку с файлами программ (например, **C:\Program Files**).
  - **%WINDIR%** позволяет выбрать папку, в которой находится система Windows (например, **C:\Windows**).

  Можно использовать другие переменные среды или их сочетание с текстом. Например, чтобы выбрать папку Java в папке Program Files, введите **%PROGRAMFILES%\Java**.

Правила выбора для Linux

- Полный путь к файлу или каталогу. Например, чтобы создать резервную копию файла **file.txt** в томе **/dev/hda3**, подключенном к каталогу **/home/usr/docs**, введите **/dev/hda3/file.txt** или **/home/usr/docs/file.txt**.
  - **/home** позволяет выбрать домашний каталог стандартных пользователей.
  - **/root** позволяет выбрать домашний каталог привилегированного пользователя.
  - **/usr** позволяет выбрать каталог для всех пользовательских программ.
  - **/etc** позволяет выбрать каталог с конфигурационными файлами системы.
- Шаблоны:
  - **[All Profiles Folder]** позволяет выбрать каталог **/home**. В этой папке по умолчанию размещены все профили пользователя.

Правила выбора для macOS

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

Примеры:

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

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.

Ограничения

- Резервное копирование конфигурации ESXi не поддерживается для VMware vSphere 6.7.
- Не удается выполнить резервное копирование конфигурации ESXi в облачное хранилище данных.

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 данных**

  Резервные копии будут храниться в облачном центре обработки данных.

- **Локальные папки**

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

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

- **Сетевая папка**

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

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

  - Для общих папок SMB/CIFS: `\\<имя_хоста>\<путь>\` или `smb://<имя_хоста>/<путь>/`
  - Для папок DFS: `\\<полное доменное имя DNS>\<корневой каталог DFS>\<путь>`

    Например, `\\example.company.com\shared\files`

  После этого нажмите кнопку со стрелкой. Если потребуется, укажите имя пользователя и пароль для доступа к общей папке. Эти учетные данные можно изменить в любое время. Для этого щелкните значок ключа рядом с именем папки.

  Резервное копирование в папку с анонимным доступом не поддерживается.

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

  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. 51).

Расширенный выбор расположений хранения

Примечание. *Эта функциональность недоступна в Стандартной редакции программы резервного копирования.*

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

  Можно хранить резервную копию каждой машины в папке, определенной сценарием. Программное обеспечение поддерживает сценарии на языках JScript, VBScript или Python 3.5. При развертывании плана резервного копирования программа выполняет сценарий на каждой машине. Выходными данными сценария для каждой машины является путь к локальной или сетевой папке. Если папка не существует, она будет создана. Действует следующее ограничение: сценарии на языке Python не могут создавать папки в сетевых папках. На вкладке **Резервные копии** каждая папка показана в виде отдельного хранилища резервных копий.

В поле **Тип сценария** выберите тип сценария (**JScript**, **VBScript** или **Python**), а затем импортируйте или скопируйте и вставьте сценарий. Для сетевых папок укажите учетные данные доступа с правами чтения/записи

Пример. Следующий сценарий JScript выводит расположение архивных копий для машины в формате **\\bkpsrv**<имя машины>:

```
WScript.echo("\\\\bkpsrv\\" +
WScript.CreateObject("WScript.Network").ComputerName);
```

В результате резервные копии каждой машины будут сохранены в папке с тем же именем на сервере **bkpsrv**.

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. 232). При изменении назначения на раздел Зона безопасности в плане резервного копирования, который имеет схему резервного копирования **Всегда инкрементное (один файл)**, данная схема заменяется схемой **Еженедельно полное, ежедневно инкрементное**.

Преобразование диска в результате создания раздела Зона безопасности

- Раздел Зона безопасности всегда создается в конце жесткого диска.

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

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

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

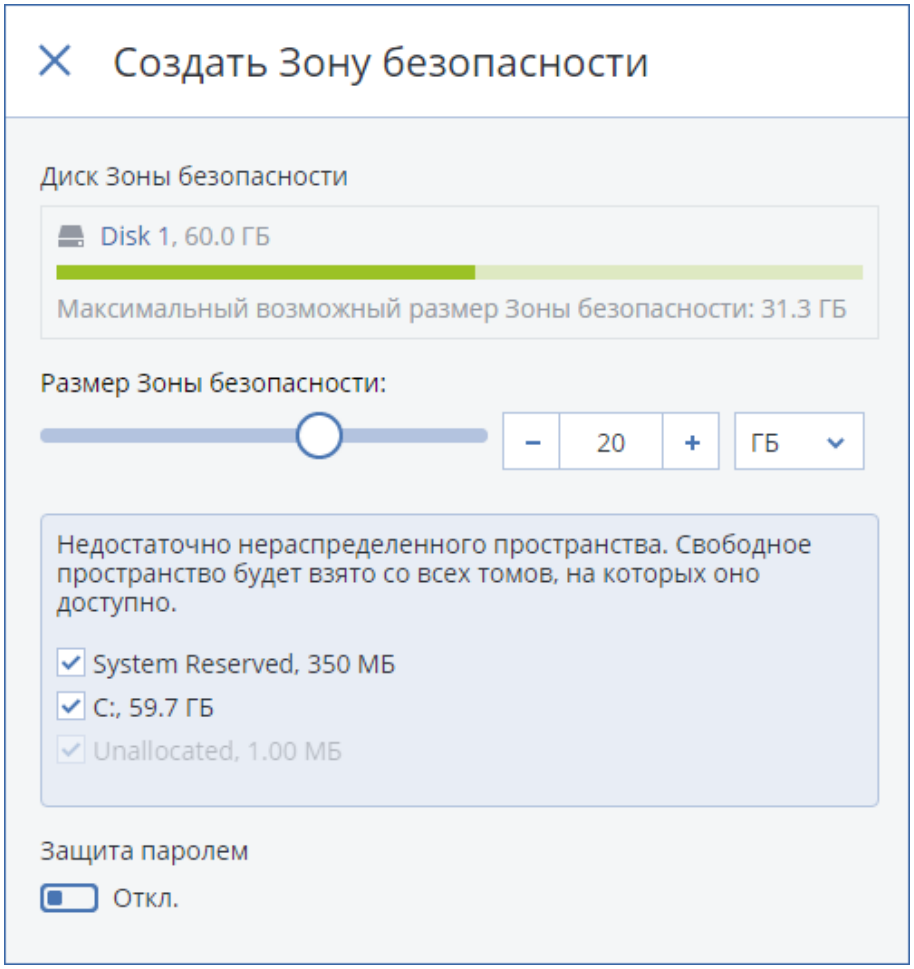
Создание раздела Зона безопасности

1. Выберите машину, на которой необходимо создать раздел Зона безопасности.
2. Выберите **Сведения** > **Создать раздел Зона безопасности**.
3. В разделе **Диск раздела Зона безопасности** щелкните **Выбрать**, выберите жесткий диск (если их несколько), на котором нужно создать зону.

   Программа рассчитает максимальный возможный размер раздела Зона безопасности.
4. Введите размер раздела Зона безопасности или перетащите ползунок, чтобы выбрать любой размер между минимальным и максимальным.

   Минимальный размер зоны составляет около 50 МБ в зависимости от геометрии жесткого диска. Максимальный размер складывается из размера нераспределенного пространства и суммарного свободного пространства всех томов диска.

5. Если всего нераспределенного пространства не хватает для указанного размера, то программа заберет свободное пространство от существующих томов. По умолчанию выбраны все тома. Чтобы исключить некоторые тома, щелкните **Выбрать тома**. В противном случае пропустите этот шаг.



6. [Необязательно] Включите переключатель **Защита паролем** и укажите пароль.

   Для доступа к резервным копиям, расположенным в разделе Зона безопасности, необходимо будет указать пароль. Для резервного копирования в раздел Зона безопасности пароль не требуется, за исключением случая, когда резервное копирование выполняется в системе, загруженной с загрузочного носителя.
7. Нажмите кнопку **Создать**.

   Программа покажет предполагаемую структуру разделов. Нажмите кнопку **ОК**.
8. Подождите, пока программа создаст раздел Зона безопасности.

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

Порядок удаления раздела Зона безопасности

1. Выберите машину с разделом Зона безопасности.
2. Нажмите **Сведения**.
3. Щелкните значок шестеренки рядом с разделом **Зона безопасности**, затем щелкните **Удалить**.
4. [Дополнительно] Укажите тома, на которые будет добавлено пространство, которое занимала зона безопасности. По умолчанию выбраны все тома.

Пространство будет распределено между выбранными томами поровну. Если ни один том не выбран, освобожденное пространство становится нераспределенным.

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

5. Щелкните **Удалить**.

В результате раздел Зона безопасности будет удален вместе со всеми содержащимися в нем резервными копиями.

8.4 Расписание

В расписании используются настройки времени (включая часовой пояс) операционной системы, в которой установлен агент. Часовой пояс агента для VMware (виртуальное устройство) можно настроить в интерфейсе агента (стр. 33).

Пример: если план резервного копирования, который применен к нескольким машинам в разных часовых поясах, запанирован к запуску в 21:00, то процесс резервного копирования на каждой машине начнется в 21:00 по местному времени данной машины.

Схемы резервного копирования

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.

- **Всегда инкрементное (один файл)**

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

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

  Для резервных копий используется формат резервной копии в виде одного файла (стр. 232).

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

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

  Эта схема недоступна при выполнении резервного копирования в Зону безопасности.

- **Всегда полное**

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

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

  Каждый раз создаются полные резервные копии.

- **Еженедельно полное, ежедневно инкрементное**

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

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

- **Ежемесячно полное, еженедельно дифференциальное, ежедневно инкрементное (GFS)**

  По умолчанию инкрементное резервное копирование выполняется ежедневно с понедельника по пятницу; дифференциальное резервное копирование выполняется каждую субботу; полное резервное копирование выполняется в первый день каждого месяца. Это расписание и время запуска резервного копирования можно изменить.

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

- **Пользовательские**

  Задайте расписания для полных, дифференциальных и инкрементных резервных копий.

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

Для любой схемы резервного копирования можно запланировать резервное копирование по событиям, а не по времени. Для этого выберите тип события в настройках расписания. Дополнительную информацию см. в разделе «Расписание по событиям» (стр. 56).

Дополнительные параметры расписания

Для каждого места назначения можно выполнить следующие действия:

- Задайте условия запуска резервного копирования так, чтобы запланированное резервное копирование выполнялось только при соблюдении этих условий. Дополнительную информацию см. в разделе «Условия запуска» (стр. 58).
- 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.*

- Щелкните **Подробнее**, чтобы получить доступ к указанным ниже параметрам:
  - **Если машина выключена, выполнить пропущенные задания при ее загрузке** (по умолчанию отключено)

- **Отключить переход в спящий режим или режим гибернации при выполнении резервного копирования** (по умолчанию включено)

  Этот параметр действует только для машин с ОС Windows.
- **Выйти из спящего режима или режима гибернации для запуска запланированного резервного копирования** (отключено по умолчанию)

  Этот параметр действует только для машин с ОС Windows. Этот параметр не действует, когда машина выключена, т. е. данный параметр не использует функциональность Wake-on-LAN.

8.4.1 Планирование по событиям

При составлении расписания для плана резервного копирования выберите тип события в настройках расписания. Резервное копирование будет запущено, как только произойдет событие.

Можно выбрать одно из следующих событий

- **С заданной периодичностью**

  Через определенное время после завершения последнего успешного резервного копирования в рамках одного плана резервного копирования. Укажите период времени.
- **При входе пользователя в учетную запись**

  По умолчанию резервное копирование запустится при входе в учетную запись любого пользователя. Вместо любого пользователя можно указать конкретную учетную запись.
- **При выходе пользователя из учетной записи**

  По умолчанию резервное копирование запустится при выходе из учетной записи любого пользователя. Вместо любого пользователя можно указать конкретную учетную запись.

  Примечание *Резервное копирование не будет запущено при завершении работы системы, поскольку завершение работы не эквивалентно выходу из учетной записи.*
- **При запуске системы**
- **При завершении работы системы**
- **По событию в журнале событий Windows**

  Вы должны указать свойства события (стр. 57).

В следующей таблице перечислены события, доступные для различных данных в ОС Windows, Linux и macOS.

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

Почтовые ящики Office 365	Windows	–	–	–	–	Windows
Базы данных и почтовые ящики Exchange	Windows	–	–	–	–	Windows
Базы данных SQL	Windows	–	–	–	–	Windows

8.4.1.1 По событию в журнале событий Windows

Можно запланировать запуск резервного копирования в случае записи определенного события в один из журналов событий Windows (**журнал приложения**, **журнал безопасности** или **системный журнал**).

Например, можно задать план резервного копирования, по которому аварийное полное резервное копирование данных будет запускаться автоматически, как только ОС Windows обнаружит вероятность отказа жесткого диска.

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

Свойства событий

Имя журнала

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

Источник события

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

Тип события

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

Идентификатор события

Указывает номер события, который обычно определяет тип событий среди событий из одного источника.

Например, событие **Ошибка** с источником события **диск** и идентификатором события **7** происходит в случае, если ОС Windows обнаруживает плохой блок на диске, а событие **Ошибка** с источником события **диск** и идентификатором события **15** — в случае, если диск пока недоступен.

Пример. Аварийное резервное копирование при обнаружении «плохого блока»

Появление одного или нескольких плохих блоков на жестком диске обычно означает, что диск скоро выйдет из строя. Предположим, требуется план резервного копирования, который создаст резервную копию данных жесткого диска в такой ситуации.

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

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

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

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

8.4.2 Условия запуска

Такие настройки делают планировщик более гибким, позволяя выполнять резервное копирование в соответствии с определенными условиями. Если условий несколько, для запуска резервного копирования все они должны выполняться одновременно. Начальные условия не действуют, если резервная копия запущена вручную.

Для доступа к этим настройкам щелкните **Показать больше** при настройке расписания для плана резервного копирования.

Поведение планировщика заданий в случае, если событие происходит, а одно или несколько условий не выполнено, определяется параметром резервного копирования Условия запуска резервного копирования (стр. 79). Чтобы предусмотреть случаи, когда условия не выполняются в течение слишком долгого времени и дальнейшая отсрочка резервного копирования становится рискованной, можно установить временной промежуток, после которого задание запустится независимо от условия.

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

ЭЛЕМЕНТЫ ДЛЯ РЕЗЕРВНОГО КОПИРОВАНИЯ	Диски/тома или файлы (физические машины)	Диски/тома (виртуальные машины)	Конфигурация ESXi	Почтовые ящики Office 365	Базы данных и почтовые ящики Exchange	Базы данных SQL
Пользователь неактивен (стр. 59)	Windows	–	–	–	–	–
Хост хранилища резервных копий доступен (стр. 59)	Windows, Linux, macOS	Windows, Linux	Windows, Linux	Windows	Windows	Windows
Пользователи завершили сеанс (стр. 60)	Windows	–	–	–	–	–
В интервале времени (стр. 60)	Windows, Linux, macOS	Windows, Linux	–	–	–	–
Сэкономить заряд батареи (стр. 61)	Windows	–	–	–	–	–

Не запускать при работе на лимитном подключении (стр. 62)	Windows	–	–	–	–	–
Не запускать при подключении к следующим сетям Wi-Fi (стр. 62)	Windows	–	–	–	–	–
Проверить IP-адрес устройства (стр. 63)	Windows	–	–	–	–	–

8.4.2.1 Пользователь неактивен

«Пользователь неактивен» означает, что машина заблокирована или на экране отражается заставка.

Пример

Запускать резервное копирование на машине каждый день в 21:00 — желательно, когда пользователь неактивен. Если в 23:00 пользователь все еще активен, все равно запустить резервное копирование.

- Расписание: Ежедневно, запускать каждый день. Запускать в: **21:00**.
- Условие: **Пользователь неактивен**.
- Условия запуска резервного копирования: **Ждать выполнения условий, все равно запустить резервное копирование через 2** часа.

В результате:

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

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

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

8.4.2.2 Хост хранилища резервных копий доступен

Строка «Хост хранилища резервных копий доступен» означает, что машина, служащая назначением для хранения резервных копий, доступна в сети.

Данное условие эффективно для сетевых папок, облачных хранилищ и хранилищ под управлением узла хранения.

Данное условие перекрывает доступность хоста, а не доступность самого хранилища. Например, если хост доступен, но отсутствует доступ к сетевой папке на хосте или учетные данные для доступа к папке недействительны, условия все еще считаются соблюденными.

Пример

Резервное копирование данных в сетевую папку выполняется каждый рабочий день в 21:00. Если машина, на которой находится папка, в это время недоступна (например, из-за профилактических работ), вам необходимо пропустить резервное копирование и ждать запланированного запуска на следующий рабочий день.

- Расписание: ежедневно, запускать с понедельника по пятницу. Запускать в: **21:00**.
- Условие: **Хост хранилища резервных копий доступен**.
- Условия запуска резервного копирования: **Пропустить запланированное резервное копирование**.

В результате:

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

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

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

8.4.2.3 Пользователи завершили сеанс

Позволяет поставить выполнение резервного копирования на ожидание до тех пор, пока все пользователи не выйдут из системы Windows.

Пример

Запуск резервного копирования в 20:00 каждую пятницу, желательно, когда все пользователи завершили сеанс. Если один из пользователей все еще находится в системе в 23:00, все равно запустить резервное копирование

- Расписание: Еженедельно, по пятницам. Запускать в: **20:00**.
- Условие: **Пользователи завершили сеанс**.
- Условия запуска резервного копирования: **Ждать выполнения условий**, **все равно запустить резервное копирование через 3** часа.

В результате:

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

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

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

8.4.2.4 В интервале времени

Ограничивает время запуска резервного копирования определенным интервалом.

Пример

Для резервного копирования данных пользователей и серверов компания использует разные области на одном и том же сетевом устройстве хранения. Рабочий день начинается в 8:00 и заканчивается в 17:00. Копирование данных пользователя должно начинаться, как только пользователи выйдут из системы, но не раньше 16:30. Каждый день в 23:00 начинается резервное копирование серверов компании. К этому времени резервное копирование пользовательских данных должно закончиться, чтобы освободить пропускную способность сети. Считается, что резервное копирование данных пользователей занимает не больше часа, так что самое позднее время начала резервного копирования — 22:00. Если в заданный период времени пользователь все еще находится в системе или выходит из системы в любое другое время, резервное копирование пользовательских данных не производится, то есть, резервное копирование пропускается.

- Событие: **При выходе пользователя из системы**. Укажите учетную запись пользователя: **Любой пользователь**.
- Условие: **В интервале времени** от **16:30** до **22:00**.
- Условия запуска резервного копирования: **Пропустить запланированное резервное копирование**.

В результате:

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

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

8.4.2.5 Сэкономить заряд батареи

Предотвращает резервное копирование, если устройство (ноутбук или планшетный ПК) не подключено к источнику питания. В зависимости от значения параметра резервного копирования Условия запуска резервного копирования (стр. 79) пропущенное резервное копирование запускается или не запускается после подключения устройства к источнику питания. Доступны следующие параметры:

- **Не запускать при работе от батареи**

  Резервное копирование запускается, только если устройство подключено к источнику питания.
- **Запускать при работе от батареи, если уровень ее заряда больше**

  Резервное копирование запускается, если устройство подключено к источнику питания или если уровень заряда аккумуляторной батареи больше указанного значения.

Пример

Резервное копирование данных выполняется каждый рабочий день в 21:00. Если устройство не подключено к источнику питания (например, пользователь допоздна задерживается на собрании), уместно не выполнять резервное копирование до тех пор, пока устройство не будет подключено к источнику питания. Это позволит сэкономить заряд батареи.

- Расписание: ежедневно, запускать с понедельника по пятницу. Запускать в: 21:00.
- Условие: **Сэкономить заряд батареи**, **Не запускать при работе от батареи**.
- Условия запуска резервного копирования: **Ожидайте выполнения условий**.

В результате:

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

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

8.4.2.6 Не запускать при работе на лимитном подключении

Предотвращает резервное копирование (включая резервное копирование на локальный диск), если устройство подключено к Интернету через лимитное подключение в Windows. Дополнительную информацию о лимитных подключениях в Windows см. по ссылке https://support.microsoft.com/en-us/help/17452/windows-metered-internet-connections-faq.

Дополнительная мера предотвращения резервного копирования через мобильные точки доступа: если включено условие **Не запускать при работе на лимитном подключении**, условие **Не запускать при подключении к следующим сетям Wi-Fi** включается автоматически. По умолчанию указаны следующие сетевые имена: "android", "phone", "mobile" и "modem". Эти имена можно удалить из списка, щелкнув значок X.

Пример

Резервное копирование данных выполняется каждый рабочий день в 21:00. Если устройство подключено к Интернету через лимитное подключение (например, пользователь в командировке), возможно, предпочтительнее будет не выполнять резервное копирование, дождавшись запланированного запуска на следующий рабочий день. Это позволит сэкономить сетевой трафик.

- Расписание: ежедневно, запускать с понедельника по пятницу. Запускать в: 21:00.
- Условие: **Не запускать при работе на лимитном подключении**
- Условия запуска резервного копирования: **Пропустить запланированное резервное копирование**.

В результате:

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

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

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

8.4.2.7 Не запускать при подключении к следующим сетям Wi-Fi

Предотвращает резервное копирование (включая резервное копирование на локальный диск), если устройство подключено к любой указанной беспроводной сети. Можно указать имена сети Wi-Fi, также известные как идентификаторы беспроводной сети (SSID).

Это ограничение применяется ко всем сетям, которые содержат указанное имя (с учетом регистра) как подстроку в своем имени. Например, если в качестве сетевого имени указать "phone", резервная копия не запустится, если устройство подключено к любой из указанных ниже сетей: "John's iPhone", "phone_wifi", или "my_PHONE_wifi".

Это условие полезно, чтобы предотвратить резервное копирование, когда устройство подключено к Интернету через мобильную точку доступа.

Дополнительная мера предотвращения резервного копирования через мобильные точки доступа: условие **Не запускать при подключении к следующим сетям Wi-Fi** включается автоматически при включении условия **Не запускать при работе на лимитном подключении**. По умолчанию указаны следующие сетевые имена: "android", "phone", "mobile" и "modem". Эти имена можно удалить из списка, щелкнув значок X.

Пример

Резервное копирование данных выполняется каждый рабочий день в 21:00. Если устройство подключено к Интернету через мобильную точку доступа (например, ноутбук подключен через мобильный телефон в режиме модема), возможно, предпочтительнее будет не выполнять резервное копирование, дождавшись запланированного запуска на следующий рабочий день.

- Расписание: ежедневно, запускать с понедельника по пятницу. Запускать в: 21:00.
- Условие: **Не запускать при подключении к следующим сетям**, **Сетевое имя**: `<SSID сети доступа>`.
- Условия запуска резервного копирования: **Пропустить запланированное резервное копирование**.

В результате:

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

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

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

8.4.2.8 Проверить IP-адрес устройства

Предотвращает резервное копирование (включая резервное копирование на локальный диск), если любой из IP-адресов устройства находится в указанном диапазоне IP-адресов или вне этого диапазона. Доступны следующие параметры:

- **Запустить, если вне диапазона IP-адресов**
- **Запустить, если в диапазоне IP-адресов**

В обоих параметрах можно указать разные диапазоны. Поддерживаются только адреса IPv4.

Это условие позволяет избежать затрат на передачу больших объемов данных, если пользователь физически находится на большом расстоянии. Кроме того, оно помогает предотвратить резервное копирование через подключение VPN.

Пример

Резервное копирование данных выполняется каждый рабочий день в 21:00. Если устройство подключено к корпоративной сети через VPN-туннель (например, пользователь работает из дома), уместно не выполнять резервное копирование до тех пор, пока устройство не будет в офисе.

- Расписание: ежедневно, запускать с понедельника по пятницу. Запускать в: 21:00.

- Условие: **Проверить IP-адрес устройства**, **Запустить, если вне диапазона IP-адресов**, **От**: <начало диапазона IP-адресов VPN>, **До**: <конец диапазона IP-адресов VPN>.
- Условия запуска резервного копирования: **Ожидайте выполнения условий**.

В результате:

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

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

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

8.5 Правила хранения

1. Нажмите **Срок хранения**.
2. В разделе **Очистка** выберите один из перечисленных ниже вариантов.
   - **По возрасту резервной копии** (по умолчанию)

     Укажите, в течение какого срока нужно хранить резервные копии, созданные планом резервного копирования. По умолчанию правила хранения задаются отдельно для каждого набора резервных копий (стр. 232). Чтобы использовать одно правило для всех резервных копий, щелкните **Перейти на использование одного правила для всех наборов резервных копий**.
   - **По количеству резервных копий**

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

     Укажите максимальный общий размер резервных копий.

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

     Правила хранения будут применены после создания новой резервной копии.
   - **До резервного копирования**

     Правила хранения будут применены до создания новой резервной копии.

     Эта настройка недоступна при резервном копировании кластеров Microsoft SQL Server или сервера Microsoft Exchange.

Что еще нужно знать

- Если в соответствии со схемой резервного копирования и форматом резервного копирования каждая резервная копия хранится в отдельном файле, этот файл не может быть удален до окончания времени существования всех зависимых от него резервных копий (инкрементных и дифференциальных). Для хранения резервных копий, удаление которых отложено, требуется дополнительное место на диске. Кроме того, возраст, количество или размер резервных копий могут превышать указанные вами значения.

  Это поведение можно изменить, используя опцию резервного копирования «Консолидация резервной копии» (стр. 74).

- Правила хранения — составная часть плана резервного копирования. Они прекращают действовать для резервных копий машины, как только с нее отозван или удален план резервного копирования, или когда сама машина удалена из сервиса резервного копирования. Если вам больше не нужны резервные копии, созданные данным планом, удалите их, как описано в разделе "Удаление резервных копий" (стр. 128).

8.6 Репликация

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

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

Примеры использования

- **Надежное аварийное восстановление**

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

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

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

Поддерживаемые расположения

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

- Локальная папка
- Сетевая папка
- Зона безопасности

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

- Локальная папка
- Сетевая папка
- Облачное хранилище данных

Включение репликации резервных копий

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

   Элемент управления **Добавить хранилище** отображается только в том случае, если поддерживается репликация *из*последнего выбранного хранилища.
2. Укажите хранилище, в котором будет проведена репликация резервных копий.
3. [Необязательно] В поле **Срок хранения** измените правила хранения для указанного хранилища, как описано в разделе «Правила хранения» (стр. 64).

4. [Необязательно] Щелкните значок шестерни > **Производительность и окно резервного копирования**, затем задайте окно резервного копирования для выбранного расположения, как описано в теме «Производительность и окно резервного копирования» (стр. 88). Эти настройки определят производительность репликации.
5. [Необязательно] Повторите шаги 1–4 для всех хранилищ, где необходимо реплицировать резервные копии. Можно использовать до пяти последовательных хранилищ (включая основное).

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

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

- **Планы резервного копирования, которые уже применены к машине.** Если настройки шифрования в плане резервного копирования разные, процессы резервного копирования завершатся сбоем.
- **Планы резервного копирования, которые будут применены к машине позже.** Настройки шифрования, сохраненные на машине, переопределят настройки шифрования в плане

резервного копирования. Любая резервная копия будет зашифрована, даже если шифрование отключено в настройках плана резервного копирования.

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

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

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

Сохранение настроек шифрования на машине

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

     Здесь <путь_установки> — 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>

Сброс настроек шифрования на машине

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

     Здесь <путь_установки> — это путь к установленному агенту резервного копирования. По умолчанию он устанавливается в каталог **%ProgramFiles%\BackupClient**.
   - В Linux: **/usr/sbin/acropsh -m manage_creds --reset**

Для изменения настроек шифрования с помощью монитора резервного копирования

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

Порядок работы шифрования

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

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

8.8 Нотаризация

Примечание. *Эта функциональность недоступна в Стандартной редакции программы резервного копирования.*

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

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

Нотаризация *недоступна*:

- Если используется формат резервной копии **Версия 11**
- Если местом назначения резервной копии является Зона безопасности

Использование нотаризации

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

При настройке восстановления нотаризованные файлы будут помечены значком, и вы сможете верифицировать подлинность файла (стр. 114).

Принципы работы

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

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

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

8.9 Запуск резервного копирования вручную

1. Выберите машину, для которой задан хотя бы один план резервного копирования.
2. Нажмите кнопку **Резервное копирование**.

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

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

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

8.10 Параметры резервного копирования по умолчанию

Значения по умолчанию параметров резервного копирования (стр. 69) существуют только на уровнях компании, отдела и пользователя. При создании отдела или учетной записи пользователя в компании или отделе создаваемая сущность наследует значения по умолчанию, заданные для компании или отдела.

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

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

Для изменения используемых по умолчанию параметров

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

8.11 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, macOS).
- Тип данных, для которых выполняется резервное копирование (диски, файлы, виртуальные машины, данные приложения).
- Место назначения резервной копии (облачное хранилище данных, локальная или сетевая папка).

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

	Резервное копирование на уровне дисков			**Резервное копирование на уровне файлов**			**Виртуальные машины**			**SQL и Exchange**
	Windows	Linux	macOS	Windows	Linux	macOS	ESXi	Hyper-V	Virtuozzo	Windows
Оповещения (стр. 74)	+	+	+	+	+	+	+	+	+	+
Консолидация резервных копий (стр. 74)	+	+	+	+	+	+	+	+	+	–
Имя файла резервной копии (стр. 75)	+	+	+	+	+	+	+	+	+	+
Формат резервной копии (стр. 78)	+	+	+	+	+	+	+	+	+	+
Проверка резервных копий (стр. 79)	+	+	+	+	+	+	+	+	+	+
Условия запуска резервного копирования (стр. 79)	+	+	–	+	+	–	+	+	+	+
Функция Changed Block Tracking (CBT) (стр. 80)	+	–	–	–	–	–	+	+	–	–
Способ резервного копирования кластера (стр. 80)	–	–	–	–	–	–	–	–	–	+

	Резервное копирование на уровне дисков			**Резервное копирование на уровне файлов**			**Виртуальные машины**			**SQL и Exchange**
	Windows	Linux	macOS	Windows	Linux	macOS	ESXi	Hyper-V	Virtuozzo	Windows
Уровень сжатия (стр. 82)	+	+	+	+	+	+	+	+	+	+
Обработка ошибок (стр. 82)										
В случае ошибки повторить попытку	+	+	+	+	+	+	+	+	+	+
Не отображать во время обработки сообщения и диалоговые окна (режим без вывода сообщений)	+	+	+	+	+	+	+	+	+	+
Пропуск поврежденных секторов	+	+	+	+	+	+	+	+	+	–
Повтор попытки в случае ошибки при создании моментального снимка виртуальной машины	–	–	–	–	–	–	+	+	+	–
Быстрое инкрементное/ дифференциальное резервное копирование (стр. 83)	+	+	+	–	–	–	–	–	–	–
Моментальные снимки резервных копий на уровне файлов (стр. 85)	–	–	–	+	+	+	–	–	–	–
Фильтры файлов (стр. 84)	+	+	+	+	+	+	+	+	+	–

	Резервное копирование на уровне дисков			**Резервное копирование на уровне файлов**			**Виртуальные машины**			**SQL и Exchange**
	Windows	Linux	macOS	Windows	Linux	macOS	ESXi	Hyper-V	Virtuozzo	Windows
Сокращение журнала (стр. 86)	–	–	–	–	–	–	+	+	–	Только SQL
Создание моментальных снимков LVM (стр. 86)	–	+	–	–	–	–	–	–	–	–
Точки подключения (стр. 87)	–	–	–	+	–	–	–	–	–	–
Многотомные моментальные снимки (стр. 87)	+	+	–	+	+	–	–	–	–	–
Производительность и окно резервного копирования (стр. 88)	+	+	+	+	+	+	+	+	+	+
Физическая доставка данных (стр. 91)	+	+	+	+	+	+	+	+	+	–
Команды до и после процедуры (стр. 92)	+	+	+	+	+	+	+	+	+	+
Команды до и после захвата данных (стр. 94)	+	+	+	+	+	+	–	–	–	+
Планирование (стр. 96)										
Распределять время запуска по доступному времени	+	+	+	+	+	+	+	+	+	+

	Резервное копирование на уровне дисков			**Резервное копирование на уровне файлов**			**Виртуальные машины**			**SQL и Exchange**
	Windows	Linux	macOS	Windows	Linux	macOS	ESXi	Hyper-V	Virtuozzo	Windows
Ограничить число одновременно выполняющихся операций резервного копирования	–	–	–	–	–	–	+	+	+	–
Посекторное резервное копирование (стр. 97)	+	+	–	–	–	–	+	+	+	–
Разбиение (стр. 97)	+	+	+	+	+	+	+	+	+	+
Действия при сбое задания (стр. 97)	+	+	+	+	+	+	+	+	+	+
Служба теневого копирования томов (VSS) (стр. 98)	+	–	–	+	–	–	–	+	–	+
Служба теневого копирования томов (VSS) для виртуальных машин (стр. 99)	–	–	–	–	–	–	+	+	–	–
Еженедельное резервное копирование (стр. 99)	+	+	+	+	+	+	+	+	+	+
Журнал событий Windows (стр. 99)	+	–	–	+	–	–	+	+	–	+

8.11.1 Оповещения

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

Значение по умолчанию: **Отключено**.

Этот параметр определяет, будет ли создаваться оповещение, если за указанный период времени планом резервного копирования не будет успешно создано ни одной резервной копии. Помимо процессов резервного копирования, которые завершились сбоем, программа считает резервные копии, которые не выполняются по расписанию (отсутствующие резервные копии).

Оповещения создаются для конкретной машины и отображаются на вкладке **Оповещения**.

Можно задать количество дней подряд без созданных резервных копий. По истечении указанного периода будет сформировано уведомление.

8.11.2 Консолидация резервных копий

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

Значение по умолчанию: **Отключено**.

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

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

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

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

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

- Местом назначения резервной копии является облачное хранилище данных.
- Используется схема резервного копирования **Всегда инкрементное (один файл)**.
- Используется формат резервной копии (стр. 78) **Версии 12**.

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

Однако если используется формат версии 12 и при этом есть несколько цепочек резервных копий (каждая цепочка хранится в отдельном файле), консолидация работает только для последней цепочки. Все цепочки, за исключением первой, удаляются. Первая цепочка

сжимается до минимально необходимого размера для хранения метаданных (~12 КБ). Эти метаданные требуются, чтобы обеспечить согласованность данных при одновременном выполнении операций чтения и записи. Сразу же после применения правила хранения резервные копии, входящие в эти цепочки, исчезают из графического интерфейса пользователя, хотя физически они существуют до удаления всей цепочки.

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

8.11.3 Имя файла резервной копии

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

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

Что такое файл резервной копии?

В зависимости от схемы резервного копирования и используемого формата резервной копии (стр. 78) каждый план резервного копирования создает один или несколько файлов в хранилище резервных копий. В следующей таблице перечислены файлы, которые могут быть созданы на каждой машине или почтовом ящике.

	Всегда инкрементное (один файл)	**Другие схемы резервного копирования**
Формат резервной копии **Версии 11**	Один файл .tib и один файл метаданных .xml	Несколько файлов .tib и один файл метаданных .xml
Формат резервной копии **Версии 12**	Один файл .tibx на каждую цепочку резервных копий (полное или дифференциальное резервное копирование и все зависящие от них инкрементные резервные копии). Если размер файла, сохраненного в локальной или сетевой (SMB) папке превышает 200 ГБ, он по умолчанию разбивается на файлы по 200 ГБ.	

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

После изменения имени файла резервной копии следующей будет полная резервная копия, если не указано имя файла существующей резервной копии той же машины. В последнем случае будет создана полная, инкрементная или дифференциальная резервная копия в соответствии с расписанием плана резервного копирования.

Обратите внимание, что можно задать имена файлов резервных копий для хранилищ, обзор которых невозможно выполнить с помощью диспетчера файлов (например, облачного хранилища данных). Это целесообразно в том случае, если требуется просмотр пользовательских имен на вкладке **Резервные копии**.

Где можно просмотреть имена файлов резервных копий?

Выберите вкладку **Резервные копии**, а затем выберите группу резервных копий.

- Имя файла по умолчанию отображаются на панели **Подробности**.
- Если имена файлов заданы не по умолчанию, они отобразятся непосредственно на вкладке **Резервные копии** в колонке **Имя**.

Ограничения для имени файла резервной копии

- Имя файла резервной копии не должно заканчиваться цифрой.

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

Имя файла резервной копии по умолчанию

По умолчанию для имени файла резервной копии всей физической или виртуальной машины, дисков/томов, файлов/папок, баз данных Microsoft SQL Server и Microsoft Exchange, а также конфигурации ESXi используется такой формат: **[Machine Name]-[Plan ID]-[Unique ID]A**.

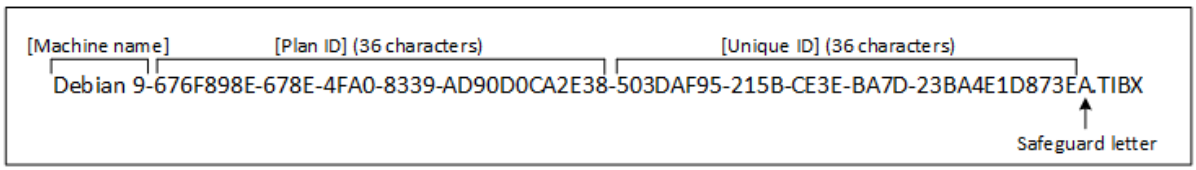
Для резервных копий почтовых ящиков Exchange и Office 365, созданных агентом для Office 365, по умолчанию задается имя **[Mailbox ID]_mailbox_[Plan ID]A**.

Для облачных резервных копий приложения, созданных облачными агентами, по умолчанию задается имя **[Resource Name]_[Resource Type]_[Resource Id]_[Plan Id]A**.

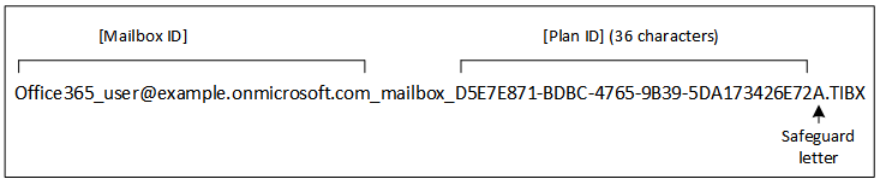
Имя по умолчанию состоит из следующих переменных:

- **[Machine Name]** Эта переменная заменяется именем машины (такое же имя отображается на консоли резервного копирования).
- **[Plan ID], [Plan Id]** Эти переменные заменяются уникальным идентификатором плана резервного копирования. При переименовании плана это значение не изменяется.
- **[Unique ID]** Эта переменная заменяется уникальным идентификатором выбранной машины. При переименовании машины это значение не изменяется.
- **[Mailbox ID]** Эта переменная заменяется именем участника-пользователя (UPN) почтового ящика.
- **[Resource Name]** Эта переменная заменяется именем облачного источника данных. Это может быть имя участника-пользователя (UPN), URL-адрес сайта SharePoint или имя общей папки.
- **[Resource Type]** Эта переменная заменяется типом облачного источника данных **mailbox**, **O365Mailbox**, **O365PublicFolder**, **OneDrive**, **SharePoint**, **GDrive**.
- **[Resource ID]** Эта переменная заменяется уникальным идентификатором облачного источника данных. Это значение не меняется при переименовании облачного источника данных.
- **"A"** — это защитная буква, которая добавляется для того, чтобы имя файла не заканчивалось цифрой.

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



На приведенной ниже диаграмме показано имя по умолчанию для файлов резервных копий почтового ящика Office 365, созданного локальным агентом.



Имена без переменных

Если вы измените имя файла резервной копии на **MyBackup**, файлы резервной копии будут выглядеть как в следующих примерах. Оба примера предполагают, что ежедневные инкрементальные резервные копирования запланированы в 14:40, начиная с 13 сентября 2016 года.

Для формата **Версии 12** со схемой резервного копирования **Всегда инкрементное (один файл)**:

```
MyBackup.tibx
```

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

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

Использование переменных

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

- Переменная **[Plan name]**, которая заменяется именем плана резервного копирования.
- Переменная **[Virtualization Server Type]**, вместо которой используется «vmwesx» (если резервная копия виртуальных машин создана агентом для VMware) или «mshyperv» (если резервная копия виртуальных машин создана агентом для Hyper-V).

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

Примеры использования

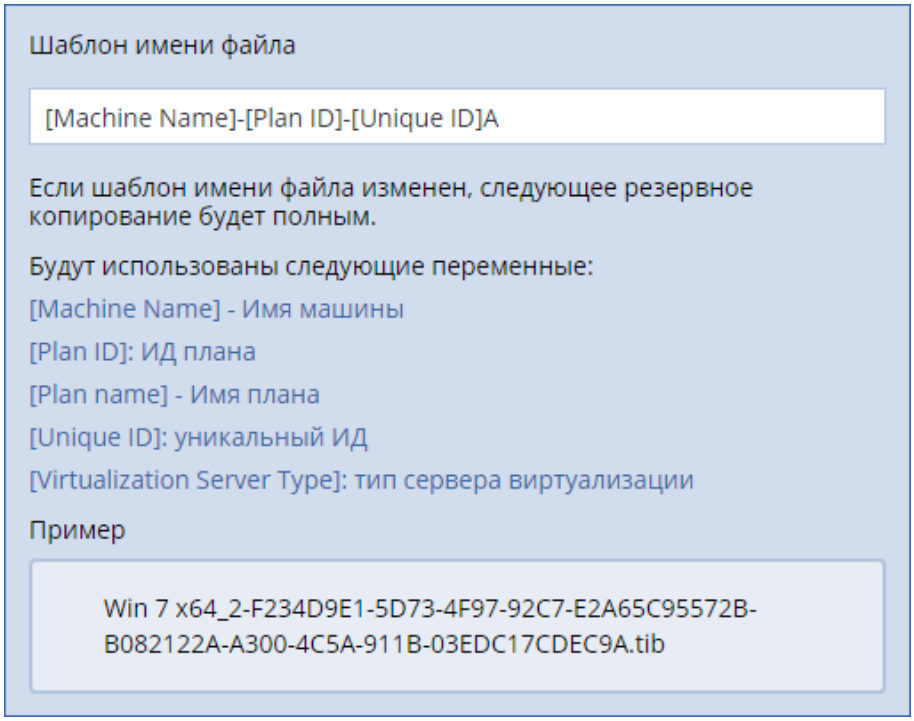
- **Просмотр дружественных к пользователю имен файлов**

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

- **Продолжение существующей последовательности резервных копий**

  Предположим, что план резервного копирования применен к одной машине и необходимо удалить эту машину из консоли резервного копирования или удалить агента вместе с его настройками конфигурации. После повторного добавления машины или установки агента можно применить план резервного копирования для продолжения выполнения резервного копирования в ту же резервную копию или последовательность резервных копий. Просто перейдите к этому параметру, щелкните **Выбрать** и выберите требуемую резервную копию.

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



8.11.4 Формат резервной копии

Этот параметр определяет формат резервных копий, создаваемых планом резервного копирования. Есть два следующих формата:

- **Версия 11**

  Устаревший формат, который используется для обеспечения обратной совместимости.

- **Версия 12**

  Новый формат, разработанный для более быстрого резервного копирования и восстановления. Каждая цепочка резервных копий (полного или дифференциального копирования, и всех зависящих от них инкрементных резервных копий) сохраняется в один файл .tibx.

Параметр **Формат резервной копии** отображается только для тех планов резервного копирования, для которых уже используется формат **Версия 11**. В этом случае формат резервного копирования можно изменить на **Версия 12**.

Формат резервной копии и файлы резервных копий

Для хранилищ резервных копий, обзор которых можно выполнить с помощью диспетчера файлов (например, локальные или сетевые папки), формат резервных копий определяет количество файлов и их расширение. В следующей таблице перечислены файлы, которые могут быть созданы на каждой машине или почтовом ящике.

	Всегда инкрементное (один файл)	**Другие схемы резервного копирования**
Формат резервной копии **Версии 11**	Один файл .tib и один файл метаданных .xml	Несколько файлов .tib и один файл метаданных .xml

Формат резервной копии **Версии 12**	Один файл .tibx на каждую цепочку резервных копий (полное или дифференциальное резервное копирование и все зависящие от них инкрементные резервные копии). Если размер файла, сохраненного в локальной или сетевой (SMB) папке превышает 200 ГБ, он по умолчанию разбивается на файлы по 200 ГБ.

Изменение формата резервной копии

Если формат резервной копии изменен:

- Следующая резервная копия будет полной.
- В хранилищах резервных копий, которые доступны для обзора в диспетчере файлов (например, локальные или сетевые папки), создается новый файл с расширением .tibx. Новый файл имеет имя исходного файла с добавлением суффикса **_v12A**.
- Правила хранения и репликации применяются только к новым резервным копиям.
- Старые резервные копии не удаляются и остаются доступными на вкладке **Резервные копии**. Их можно удалить вручную.
- Старые облачные резервные копии не будут занимать пространство в пределах квоты **Облачное хранилище данных**.
- Старые локальные резервные копии будут занимать пространство в пределах квоты **Локальная резервная копия** до тех пор, пока не вы не удалите их вручную.

8.11.5 Проверка резервных копий

Проверка — это операция по определению возможности восстановления данных из резервной копии. Если этот параметр включен, то каждая резервная копия, созданная в соответствии с планом 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. 199) в среде ESXi или Hyper-V.

8.11.6 Условия запуска резервного копирования

Этот параметр применим в операционных системах Windows и Linux.

Этот параметр определяет поведение программы в том случае, если резервное копирование готово к запуску (наступает запланированное время или событие, указанное в расписании),

однако условие (или любое из нескольких условий) не выполнено. Дополнительную информацию об условиях см. в разделе «Условия запуска» (стр. 58).

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

Ждать выполнения условий

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

Чтобы предусмотреть случаи, когда условия не выполняются в течение слишком долгого времени и дальнейшая отсрочка резервного копирования становится рискованной, можно установить временной промежуток, после которого задание запустится независимо от условия. Выберите **Запустить резервное копирование в любом случае через** и укажите временной промежуток. Резервное копирование запустится, если будут выполнены условия ИЛИ истечет максимальное время задержки, в зависимости от того, что наступит раньше.

Пропустить запланированное резервное копирование

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

8.11.7 Функция Changed Block Tracking (CBT)

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

Значение по умолчанию: **Включено**.

Этот параметр определяет, будет ли использоваться технология Changed Block Tracking (CBT) при выполнении инкрементного или дифференциального резервного копирования.

Технология CBT ускоряет процесс резервного копирования. Изменения содержимого диска или базы данных постоянно отслеживаются на уровне блоков. При запуске резервного копирования изменения могут быть незамедлительно сохранены в резервную копию.

8.11.8 Способ резервного копирования кластера

Примечание. *Эта функциональность недоступна в Стандартной редакции программы резервного копирования.*

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

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

Microsoft SQL Server

Этот параметр определяет режим резервного копирования для группы доступности SQL Server Always On (AAG). Чтобы этот параметр действовал, агент для SQL должен быть установлен на всех узлах AAG. Дополнительные сведения о резервном копировании групп доступности Always On см. в разделе «Защита группы доступности Always On (AAG)» (стр. 137).

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

Можно выбрать один из следующих вариантов:

- **Дополнительная реплика, если возможно**

  Если все дополнительные реплики отключены от сети, создается резервная копия основной реплики. Резервное копирование основной реплики может замедлить работу SQL Server, но будет обеспечено самое актуальное состояние данных в резервной копии.

- **Дополнительная реплика**

  Если все дополнительные реплики отключены, резервное копирование не будет выполнено. Создание резервной копии дополнительной реплики не влияет на производительность сервера SQL и позволяет расширить окно резервного копирования. Однако пассивные реплики могут содержать не самые последние данные, так как часто настроены на асинхронное обновление (с отставанием).

- **Основная реплика**

  Если основная реплика отключена, резервное копирование не будет выполнено. Резервное копирование основной реплики может замедлить работу SQL Server, но будет обеспечено самое актуальное состояние данных в резервной копии.

Независимо от значения данного параметра, для обеспечения целостности базы данных, программа пропускает базы данных, которые до начала резервного копирования *не находятся* в состоянии **СИНХРОНИЗИРОВАНО** или **СИНХРОНИЗАЦИЯ**. Если пропущены все базы данных, резервное копирование не будет выполнено.

Microsoft Exchange Server

Этот параметр определяет режим резервного копирования для группы обеспечения доступности баз данных Exchange Server (DAG). Чтобы этот параметр действовал, агент для Exchange должен быть установлен на всех узлах DAG. Дополнительные сведения о резервном копировании групп обеспечения доступности баз данных см. раздел«Защита групп обеспечения доступности базы данных (DAG)» (стр. 138).

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

Можно выбрать один из следующих вариантов:

- **Пассивная копия, если возможно**

  Если все пассивные копии выключены, создается резервная копия активной копии. Резервное копирование активной копии может замедлить работу Exchange Server, но будет обеспечено самое актуальное состояние данных в резервной копии.

- **Пассивная копия**

  Если все пассивные копии выключены, резервное копирование завершится сбоем. Создание резервной копии пассивных копий не влияет на производительность Exchange Server и позволяет расширить окно резервного копирования. Однако пассивные копии могут содержать не самые последние данные, так как часто настроены на асинхронное обновление (с отставанием).

- **Активная копия**

Если активная копия выключена, резервное копирование завершится сбоем. Резервное копирование активной копии может замедлить работу Exchange Server, но будет обеспечено самое актуальное состояние данных в резервной копии.

Независимо от значения данного параметра, для обеспечения целостности базы данных, программа пропускает базы данных, которые до начала резервного копирования *не находятся* в состоянии **ИСПРАВНА** или **АКТИВНА**. Если пропущены все базы данных, резервное копирование не будет выполнено.

8.11.9 Уровень сжатия

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

Значение по умолчанию: **Обычное**.

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

Оптимальный уровень сжатия данных зависит от типа копируемых данных. Даже максимальное сжатие не уменьшит значительно размер резервной копии, состоящей из уже сжатых файлов, например JPG, PDF или MP3. Но такие форматы, как DOC или XLS, сжимаются хорошо.

8.11.10 Обработка ошибок

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

В случае ошибки повторить попытку

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

Если возникла устранимая ошибка, программа будет продолжать попытки выполнить операцию. Задайте временной интервал и количество попыток. Попытки будут прекращены 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.

Облачное хранилище данных

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

В этом случае фактическое количество попыток не ограничено, а время ожидания до возврата ошибки о сбое резервного копирования рассчитывается по следующей формуле: (300 секунд + **Интервал между попытками**) * (**Количество попыток** + 1).

Примеры:

- Со значениями по умолчанию для сбоя резервного копирования должно пройти (300 секунд + 30 секунд) * (300 + 1) = 99330 секунд, или ~27,6 часов.
- Если параметру **Количество попыток** задано значение 1, а параметру **Интервал между попытками** — значение 1, сбой резервного копирования должен произойти через (300 секунд + 1 секунда) * (1 + 1) = 602 секунды или ~10 минут.

Если рассчитанное время ожидания превышает 30 минут, а передача данных еще не началась, для фактического времени ожидания устанавливается время 30 минут.

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

Значение по умолчанию: **Включено**.

В режиме без вывода сообщений ситуации, требующие вмешательства пользователя, разрешаются автоматически (за исключением обработки поврежденных секторов, что задается отдельным параметром). Если операция не может быть продолжена без вмешательства пользователя, она не будет выполнена. Дополнительные сведения об операции, включая информацию об ошибках (если они есть), см. в журнале операций.

Пропуск поврежденных секторов

Значение по умолчанию: **Отключено**.

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

Повтор попытки в случае ошибки при создании моментального снимка виртуальной машины

Значение по умолчанию: **Включено. Количество попыток: 3. Интервал между попытками: 5 минут.**

Если не удастся создать моментальный снимок виртуальной машины, программа будет продолжать попытки выполнить операцию. Задайте временной интервал и количество попыток. Попытки будут прекращены, как только операция будет успешно выполнена, или по достижении указанного максимального количества попыток (в зависимости от того, что наступит раньше).

8.11.11 Быстрое инкрементное/дифференциальное резервное копирование

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

Этот параметр не работает (всегда отключен) для томов с файловыми системами JFS, ReiserFS3, ReiserFS4, ReFS или XFS.

Значение по умолчанию: **Включено**.

Инкрементная или дифференциальная резервная копия содержит только изменения данных. Чтобы ускорить процесс резервного копирования, программа определяет, есть ли изменения в файле по размеру, дате и времени последнего изменения файла. Если эта функция отключена, то программа будет сравнивать все содержимое файла с тем содержимым, которое сохранено в резервной копии.

8.11.12 Фильтры файлов

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

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

Включение фильтров файлов

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

Исключить файлы, соответствующие определенным критериям

Есть два параметра с противоположными принципами действия.

- **Создавать резервные копии файлов, соответствующих следующим критериям**

  Пример: Если выбрать резервное копирование всей машины и указать в качестве условия фильтрации **C:\File.exe**, будет создана резервная копия только этого файла.

  Примечание *Этот фильтр не работает для резервной копии на уровне файлов, если в поле* ***Формат резервной копии*** *(стр. 78) выбрано* ***Версия 11****, и при этом местом назначения резервной копии не является облачное хранилище данных.*

- **Не создавать резервные копии файлов, соответствующих следующим критериям**

  Пример: Если выбрать резервное копирование всей машины и указать в качестве условия фильтрации **C:\File.exe**, будет пропущен только этот файл.

Оба параметра можно использовать одновременно. При этом второй имеет приоритет над первым (т. е. если указать **C:\File.exe** в обоих полях, этот файл будет пропущен при резервном копировании).

Условия

- **Полный путь**

  Укажите полный путь к файлу или папке, начиная с буквы диска (при резервном копировании ОС Windows) или с корневого каталога (при резервном копировании Linux или macOS).

  Как в Windows, так и в Linux/macOS, в пути к файлу или папке можно использовать косую черту (например, **C:/Temp/File.tmp**). В Windows также можно использовать традиционную обратную косую черту (например, **C:\Temp\File.tmp**).

- **Имя**

  Укажите имя файла или папки, например **Document.txt**. Будут выбраны все файлы и папки с этим названием.

В условиях *не* учитывается регистр символов. Например, путь **C:\Temp** включает варианты **C:\TEMP**, **C:\temp** и т. п.

В условии можно использовать любое количество подстановочных символов (*, ** и ?). Эти символы можно использовать как в полном пути, так и в имени файла или папки.

Звездочка (*) замещает 0 или несколько символов имени файла. Например, условие **Doc*.txt** включает в себя файлы **Doc.txt** и **Document.txt**

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

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

Исключить скрытые файлы и папки

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

Исключить системные файлы и папки

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

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

8.11.13 Моментальные снимки резервных копий на уровне файлов

Этот параметр действует только резервной копии на уровне файлов.

Этот параметр определяет, выполнять последовательное резервное копирование файлов или делать моментальный снимок данных.

Примечание *Резервное копирование файлов, расположенных в сетевых папках, всегда выполняется последовательно.*

Значение по умолчанию:

- Если для резервного копирования выбраны только машины с ОС Linux: **Не создавать моментальный снимок.**
- В противном случае: **По возможности создавать моментальный снимок.**

Можно выбрать один из следующих вариантов:

- **По возможности создавать моментальный снимок**

  Прямое резервное копирование файлов, если создание моментального снимка невозможно.
- **Всегда создавать моментальный снимок**

Моментальный снимок позволяет выполнять резервное копирование всех файлов, включая те, которые открыты с монопольным доступом. Все файлы в резервной копии будут сохранены в состоянии на данный момент времени. Выберите эту настройку только в случае, если эти факторы имеют важное значение, т. е. резервное копирование файлов без создания моментального снимка лишено смысла. Если моментальный снимок не может быть сделан, резервное копирование завершится ошибкой.

- **Не создавать моментальный снимок**

  Всегда выполнять прямое резервное копирование файлов. Попытка резервного копирования файлов, открытых с монопольным доступом, приведет к ошибке чтения. Файлы в резервной копии могут быть не синхронизированы по времени.

8.11.14 Сокращение журнала

Этот параметр применим для резервного копирования баз данных Microsoft SQL Server и резервного копирования на уровне дисков с включенным резервным копированием приложения Microsoft SQL Server.

Этот параметр определяет, будут ли сокращаться журналы транзакций SQL Server после успешного резервного копирования.

Значение по умолчанию: **включено**.

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

8.11.15 Создание моментальных снимков LVM

Этот параметр действует только для физических машин.

Этот параметр действует только для резервного копирования на уровне дисков томов, управляемых диспетчера логических томов Linux (LVM). Такие тома также называются логическими томами.

Этот параметр определяет способ создания моментального снимка логического тома. Программа резервного копирования может выполнить это самостоятельно или воспользоваться для этого диспетчером логических томов Linux (LVM).

Значение по умолчанию: **С помощью программы для резервного копирования**.

- **С помощью программы для резервного копирования**. Данные моментального снимка хранятся в основном в ОЗУ. Так резервное копирование выполняется быстрее, а в группе томов не требуется нераспределенное пространство. Поэтому рекомендуется изменять заранее заданное значение только при возникновении неполадок с резервным копированием логических томов.
- **С помощью LVM**. Моментальный снимок сохраняется в нераспределеном пространстве группы тома. При отсутствии нераспределенного пространства моментальный снимок будет создан программой резервного копирования.

8.11.16 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. 123).
- 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. 123).

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. 123).

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**.

8.11.17 Многотомные моментальные снимки

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

Этот параметр применяется к резервному копированию дисков. Также этот параметр применим к резервному копированию файлов, если оно выполняется посредством создания моментального снимка. (Параметр «Моментальный снимок файлов» (стр. 85) указывает, будет ли создан моментальный снимок при резервном копировании на уровне файлов).

Этот параметр определяет, создаются моментальные снимки нескольких томов одновременно или последовательно.

Значение по умолчанию:

- Если хотя бы одна машина под управлением Windows выбрана для резервного копирования: **Включено**.
- В противном случае: **Отключено**.

Если этот параметр включен, то моментальные снимки всех томов, для которых выполняется резервное копирование, создаются одновременно. Используйте этот параметр для создания синхронизированных по времени резервных копий данных, расположенных на нескольких томах, например в базе данных Oracle.

Если этот параметр отключен, то моментальные снимки томов будут созданы последовательно. В результате, если данные расположены на нескольких томах, результирующие резервные копии могут быть не синхронизированы по времени.

8.11.18 Производительность и окно резервного копирования

Позволяет задавать один из трех уровней производительности резервного копирования (высокий, низкий, запрещено) для каждого часа недели. Таким образом можно определить окно времени, в течение которого разрешено запускать и выполнять процессы резервного копирования. Высокий и низкий уровни производительности настраиваются в плане приоритета процесса и скорости вывода.

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

Этот параметр можно настроить отдельно для каждого хранилища, указанного в плане резервного копирования. Чтобы настроить этот параметр для хранилища репликации, щелкните значок шестерни рядом с именем хранилища и щелкните **Производительность и окно резервного копирования**.

Этот параметр действует только для резервного копирования и репликации резервной копии. Команды после резервного копирования и другие операции, входящие в план резервного копирования (проверка, преобразование в виртуальную машину), запускаются независимо от значения этого параметра.

Значение по умолчанию:**Отключено**.

Если этот параметр отключен, процессы резервного копирования разрешено запускать в любое время с указанными ниже параметрами (при этом не имеет значения, было ли изменено предустановленное значение параметра):

- Приоритет ЦП: **Низкий** (в Windows, соответствует **Ниже обычного**).
- Скорость вывода: **Без ограничений**.

Если этот параметр включен, запланированные резервные копии разрешаются или блокируются согласно параметрам, указанным для текущего часа. В начале часа блокировки резервного копирования процесс резервного копирования автоматически останавливается; появляется соответствующее оповещение.

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

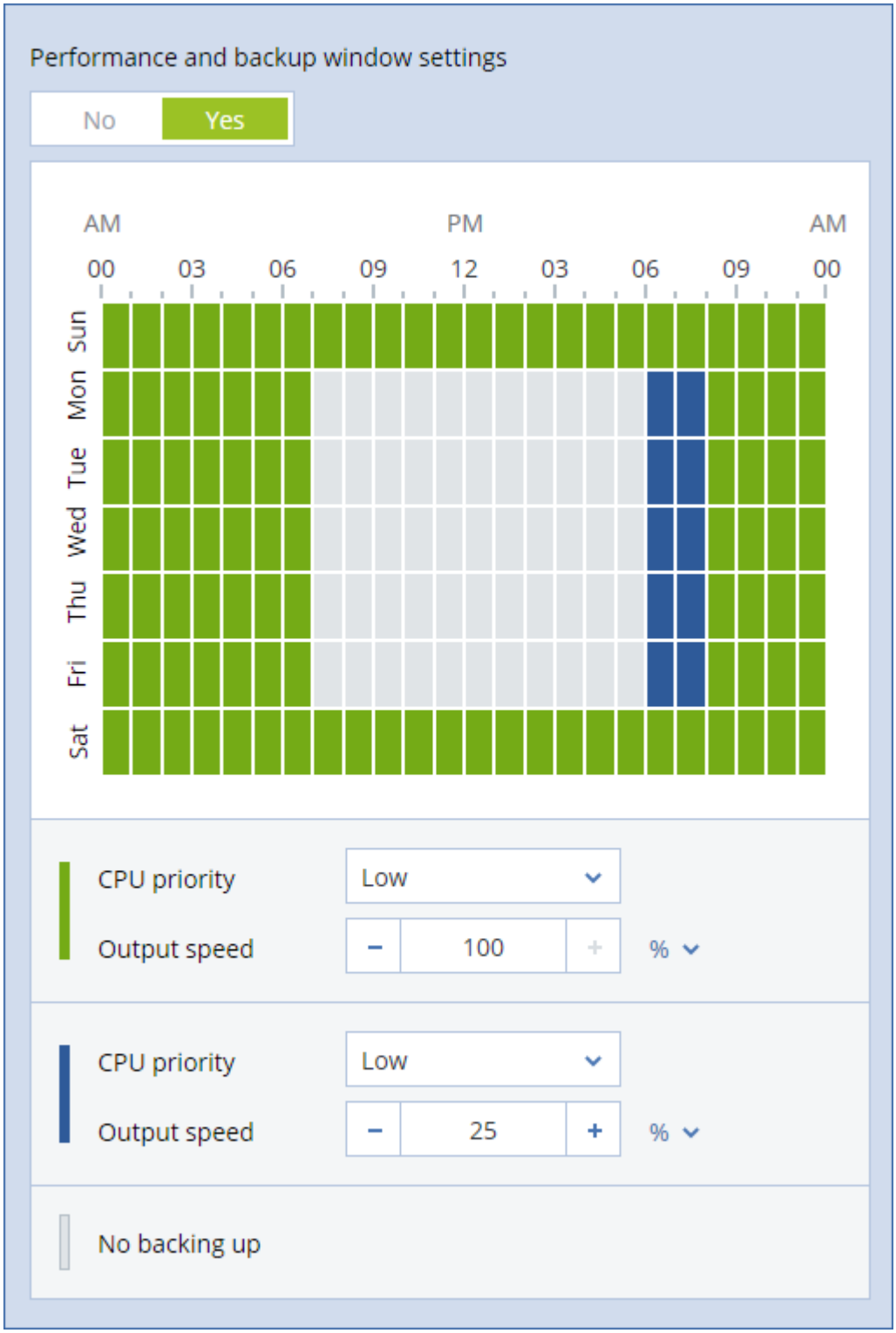
Окно резервного копирования

Каждый прямоугольник представляет один час в пределах рабочего дня. По щелчку прямоугольника можно поочередно переходить между указанными состояниями:

- **Зеленый:** резервное копирование разрешено с параметрами, указанными в зеленом разделе ниже.
- **Синий:** резервное копирование разрешено с параметрами, указанными в синем разделе ниже.

  Это состояние недоступно, если для формата резервной копии задано значение **Версия 11**.
- **Серый:** резервное копирование заблокировано.

Чтобы одновременно изменить состояние нескольких прямоугольников, щелкните один из них и расширьте выделение путем перетаскивания.



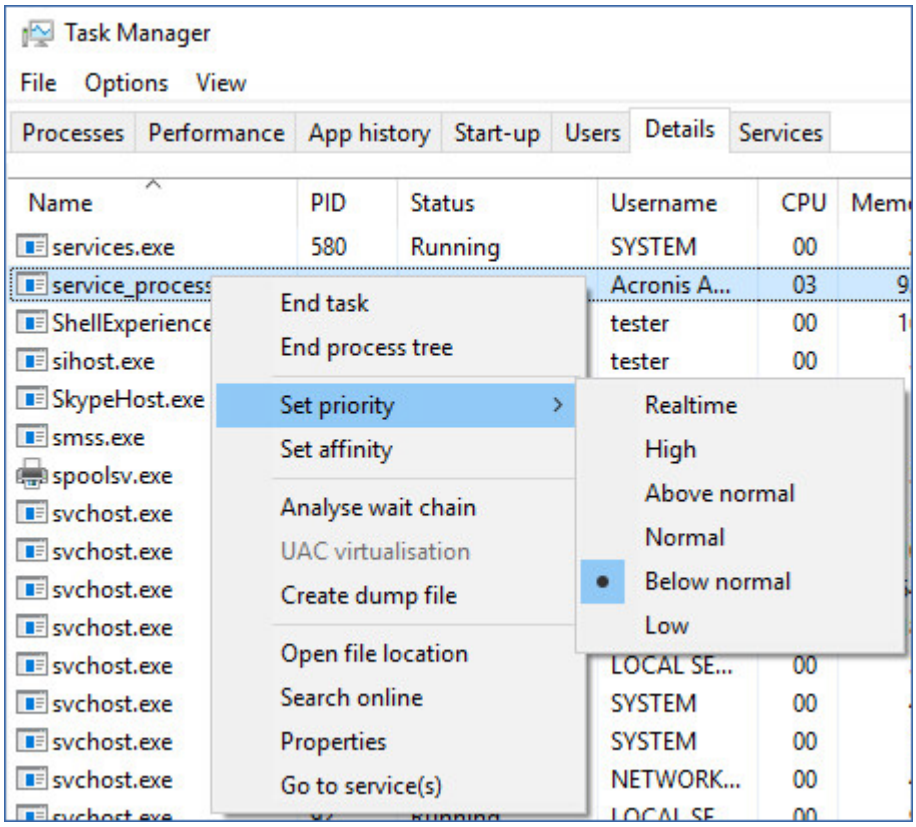
Приоритет ЦП

Этот параметр определяет приоритет процесса резервного копирования в операционной системе.

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

Приоритет процесса, выполняющегося в системе, определяет количество выделенных ему ресурсов ЦП и системы. Понижение приоритета резервного копирования освободит часть ресурсов для других приложений. Повышение приоритета копирования ускорит процесс создания резервных копий за счет того, что операционная система выделит программе резервного копирования больше ресурсов, например ресурсов ЦП. Однако результат будет зависеть от общего использования процессора и других факторов, например от скорости ввода-вывода диска и загруженности сети.

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



Скорость вывода при резервном копировании

Этот параметр позволяет ограничить скорость записи на жесткий диск (при выполнении резервного копирования в локальную папку) или скорость передачи данных резервной копии по сети (при резервном копировании в сетевую папку или облачное хранилище данных).

Если этот параметр включен, можно указать максимально разрешенную скорость вывода:

- В процентах от оценочной скорости записи на целевом жестком диске (при резервном копировании в локальную папку) или оценочной максимальной скорости сетевого подключения (при резервном копировании сетевой папки или облачного хранилища данных).

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

8.11.19 Доставка физических данных

Этот параметр действует, если местом назначения резервной копии является облачное хранилище, а в качестве формата резервной копии (стр. 78) выбрана **версия 12**.

Этот параметр действует для резервных копий на уровне дисков и резервных копий файлов, созданных с помощью агента для Windows, агента для Linux, агента для Mac, агента для VMware, агента для Hyper-V и агента для Virtuozzo.

Этот параметр определяет, будет ли первая полная резервная копия, созданная в рамках плана резервного копирования, отправлена в облачное хранилище на жестком диске с использованием службы доставки физических данных. Последующие инкрементные резервные копии можно передавать по сети.

Значение по умолчанию: **Отключено**.

Сведения о службе доставки физических данных

Веб-интерфейс службы доставки физических данных доступен только администраторам.

Подробные инструкции по использованию этой службы и средства создания заказов см. в руководстве администратора службы доставки физических данных. Для доступа к этому документу в веб-интерфейсе службы доставки физических данных щелкните значок вопроса.

Обзор процесса доставки физических данных

1. Создайте новый план резервного копирования. В этом плане активируйте параметр резервного копирования **Доставка физических данных**.

   Вы можете выполнять резервное копирование непосредственно на диск или в локальную либо сетевую папку, а затем скопировать или перенести резервные копии на диск.

   Важно! *После создания первоначальной полной резервной копии все последующие копии создаются в том же плане резервного копирования. Для другого плана резервного копирования (даже с теми же параметрами на той же машине) потребуется другой цикл доставки физических данных.*

2. После завершения первого резервного копирования с помощью веб-интерфейса службы доставки физических данных загрузите инструмент создания заказов и создайте заказ.

   Для доступа к этому веб-интерфейсу последовательно выберите пункты **Обзор** > **Использование**, а затем щелкните пункт **Настроить службу** в разделе **Доставка физических данных**.

3. Упакуйте диски и отправьте их в центр обработки данных.

   Важно! *Следуйте инструкциям по упаковке, приведенным в руководстве администратора службы доставки физических данных.*

4. Для отслеживания статуса заказа используйте веб-интерфейс службы доставки физических данных. Обратите внимание, что для создания последующих резервных копий начальная копия сначала должна быть загружена в облачное хранилище.

8.11.20 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).

8.11.20.1 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.

8.11.20.2 Команда после резервного копирования

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

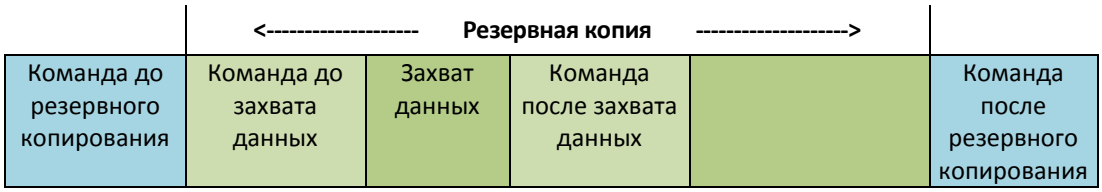
1. Включить переключатель **Выполнение команды после резервного копирования**.
2. В поле **Команда...** введите команду или выберите пакетный файл.
3. В поле **Рабочая папка** укажите путь к папке, в которой будет выполняться команда или пакетный файл.
4. В поле **Аргументы** укажите при необходимости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

8.11.21 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. 98) «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.

8.11.21.1 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.

8.11.21.2 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.

8.11.22 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. Однако если агент выполняет несколько планов резервного копирования, которые пересекаются по времени,

указанные в их параметрах числа суммируются. Вы можете ограничить общее количество виртуальных машин (стр. 219), для которых агент может одновременно создавать резервные копии, вне зависимости от количества выполняемых планов резервного копирования.

Резервное копирование физических машин запустится точно в соответствии с расписанием.

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

8.11.24 Разбиение

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

Значение по умолчанию:

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

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

Доступны следующие настройки:

- **Автоматически**

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

  Введите или выберите из раскрывающегося списка нужный размер файла.

8.11.25 Действия при сбое задания

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

Если этот параметр включен, то программа попытается еще раз выполнить план резервного копирования. Можно задать временной интервал между попытками и количеством попыток. Попытки будут прекращены, когда задание будет выполнено успешно ИЛИ количество попыток достигнет указанного предела.

Значение по умолчанию: **Отключено**.

8.11.26 Служба теневого копирования томов (VSS)

Этот параметр работает только в операционных системах Windows.

Этот параметр указывает, должен ли поставщик службы теневого копирования томов (VSS) уведомлять VSS-совместимые приложения о предстоящем запуске резервного копирования. Это обеспечивает согласованное состояние всех данных, используемых приложениями. В частности, завершение всех транзакций в момент создания моментального снимка данных программным обеспечением резервного копирования. Согласованность данных, в свою очередь, обеспечивает восстановление приложения в корректном состоянии и возможность использования сразу после восстановления.

Значение по умолчанию: **Включено**. **Автоматический выбор поставщика моментальных снимков**.

Можно выбрать один из следующих вариантов:

- **Автоматически выбирать поставщика моментальных снимков**

  Автоматический выбор из следующих вариантов: аппаратный поставщик моментальных снимков, программные поставщики моментальных снимков и программный поставщик теневого копирования (Microsoft).
- **Использовать программный поставщик теневого копирования (Microsoft)**

  Мы рекомендуем выбрать этот параметр при резервном копировании серверов приложений (Microsoft Exchange Server, Microsoft SQL Server, Microsoft 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. 94), 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. 86).

8.11.27 Служба теневого копирования томов (VSS) для виртуальных машин

Этот параметр определяет, следует ли создавать замороженные моментальные снимки виртуальных машин. Чтобы создать замороженный моментальный снимок, программное обеспечение резервного копирования применяет VSS в виртуальной машине, используя VMware Tools 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. 82), 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.

8.11.28 Еженедельное резервное копирование

Этот параметр определяет то, какие процессы резервного копирования считаются «еженедельными» в правилах хранения и схемах резервного копирования. «Еженедельная» резервная копия — это первая копия, которая создается после начала недели.

Значение по умолчанию: **Понедельник**.

8.11.29 Журнал событий Windows

Этот параметр работает только в ОС Windows.

Этот параметр указывает, должны ли агенты записывать события операций резервного копирования в журнал событий приложений Windows (чтобы просмотреть этот журнал, запустите файл eventvwr.exe или выберите **Панель управления** > **Администрирование** > **Просмотр событий**). 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. 103) Использование загрузочного носителя (стр. 108)
Физическая машина (Mac)		Использование загрузочного носителя (стр. 108)
Виртуальная машина (VMware или Hyper-V)		Использование веб-интерфейса (стр. 106) Использование загрузочного носителя (стр. 108)
Виртуальная машина или контейнер (Virtuozzo)		Использование веб-интерфейса (стр. 106)
Конфигурация ESXi		Использование загрузочного носителя (стр. 118)
Файлы и папки		Использование веб-интерфейса (стр. 112) Загрузка файлов из облачного хранилища данных (стр. 113) Использование загрузочного носителя (стр. 116) Извлечение файлов из локальных резервных копий (стр. 117)
Состояние системы		Использование веб-интерфейса (стр. 117)
Базы данных SQL		Использование веб-интерфейса (стр. 143)
Базы данных Exchange		Использование веб-интерфейса (стр. 147)
Почтовые ящики Exchange		Использование веб-интерфейса (стр. 149)
Веб-сайты		Использование веб-интерфейса (стр. 197)
Microsoft Office 365	почтовые ящики; (локальный агент для Office 365)	Использование веб-интерфейса (стр. 163)
	почтовые ящики; (облачный агент для Office 365)	Использование веб-интерфейса (стр. 167)
	общие папки;	Использование веб-интерфейса (стр. 169)
	Файлы OneDrive	Использование веб-интерфейса (стр. 172)
	Данные SharePoint Online	Использование веб-интерфейса (стр. 176)
G Suite	почтовые ящики;	Использование веб-интерфейса (стр. 182)
	Файлы Google Диск	Использование веб-интерфейса (стр. 186)
	Файлы общего диска	Использование веб-интерфейса (стр. 189)

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, для которой применяются такие носители, — восстановление операционной системы, которую не удается загрузить.

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

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

Создание загрузочного носителя в Windows и Linux

1. Загрузите ISO-файл загрузочного носителя. Чтобы загрузить файл, выберите машину и последовательно выберите пункты **Восстановить** > **Другие способы восстановления…** > **Загрузить ISO-образ**.
2. [Необязательно] Скопируйте и распечатайте или запишите маркер регистрации, который отображается на консоли резервного копирования.

   Этот маркер позволят получить доступ к облачному хранилищу данных с загрузочного носителя без ввода имени входа и пароля. Он необходим, если у вас нет учетных данных для входа в облако напрямую, а вместо этого вы используете стороннюю аутентификацию.
3. Выполните любое из следующих действий:
   - Запишите компакт- или DVD-диск, используя ISO-файл.
   - Создайте загрузочный флэш-накопитель USB, используя ISO-файл и один из бесплатных инструментов, доступных в Интернете.

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

Порядок создания загрузочного носителя в macOS

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

   Предупреждение *Все данные на диске будут удалены.*
3. Нажмите кнопку **Создать**.
4. Дождитесь создания загрузочного носителя.

9.3 Startup Recovery Manager

Startup Recovery Manager — это загрузочный компонент, находящийся на системном диске Windows или в разделе /boot Linux и настроенный на запуск во время загрузки системы при нажатии клавиши F11. При его использовании не требуется отдельный носитель или сетевое подключение для запуска загрузочной утилиты аварийного восстановления.

Startup Recovery Manager особенно полезен для мобильных пользователей. В случае сбоя перезагрузите машину, дождитесь появления запроса «Press F11 for Acronis Startup Recovery Manager...» и нажмите клавишу F11. Программа запустится, и можно будет выполнить восстановление.

Кроме того, с помощью Startup Recovery Manager можно «на ходу» выполнять резервное копирование.

На машинах с установленным загрузчиком GRUB пользователь не нажимает клавишу F11, а выбирает Startup Recovery Manager в меню загрузки.

Машина, загруженная с помощью Startup Recovery Manager, может быть зарегистрирована на сервере управления таким же образом, как машина, загруженная с загрузочного носителя. Для этого выберите **Инструменты** > **Зарегистрировать носитель на сервере управления**, а затем следуйте пошаговой процедуре, описанной в разделе «Регистрация носителя на сервере управления».

Активация Startup Recovery Manager

На машине, где работает агент для Windows или агент для Linux, Startup Recovery Manager можно активировать с помощью консоли резервного копирования.

Для активации Startup Recovery Manager с помощью консоли резервного копирования

1. Выберите машину, на которой нужно активировать Startup Recovery Manager.
2. Нажмите **Сведения**.
3. Активируйте переключатель **Startup Recovery Manager**.
4. Дождитесь активации Startup Recovery Manager программным обеспечением.

Для активации Startup Recovery Manager на машине без агента

1. Загрузите машину с загрузочного носителя.
2. Выберите **Инструменты** > **Активировать Startup Recovery Manager**.
3. Дождитесь активации Startup Recovery Manager программным обеспечением.

Что происходит при активации Startup Recovery Manager

Активация включает при загрузке подсказку «Press F11 for Acronis Startup Recovery Manager...» (при отсутствии загрузчика GRUB) или добавляет пункт «Startup Recovery Manager» в меню загрузчика GRUB (при его наличии).

Для активации Startup Recovery Manager системный диск (или раздел /boot в Linux) должен иметь по крайней мере 100 МБ свободного пространства.

За исключением случая, когда используется загрузчик GRUB и он установлен в основную загрузочную запись (MBR), активация Startup Recovery Manager перезаписывает основную загрузочную запись (MBR) своим собственным загрузочным кодом. Таким образом, при использовании загрузчиков сторонних производителей может потребоваться их повторное активирование.

В ОС Linux при использовании загрузчика, отличного от GRUB (такого как LILO), возможна его установка в загрузочную запись корневого (или загрузочного) раздела Linux вместо MBR до активации Startup Recovery Manager. В противном случае измените конфигурацию этого загрузчика вручную после активации.

Деактивация Startup Recovery Manager

Деактивация выполняется аналогично активации.

Деактивация отключает подсказку «Press F11 for Acronis Startup Recovery Manager…» при загрузке (или пункт меню в GRUB). Если Startup Recovery Manager не активирован, для восстановления системы, которая не смогла загрузиться, требуется выполнить одно из следующих действий:

- загрузить машину с отдельного загрузочного носителя.
- использовать сеть, чтобы загрузиться с PXE-сервера или службы удаленной установки Microsoft (RIS).

9.4 Восстановление машины

9.4.1 Физическая машина

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

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

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

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

Восстановление физической машины

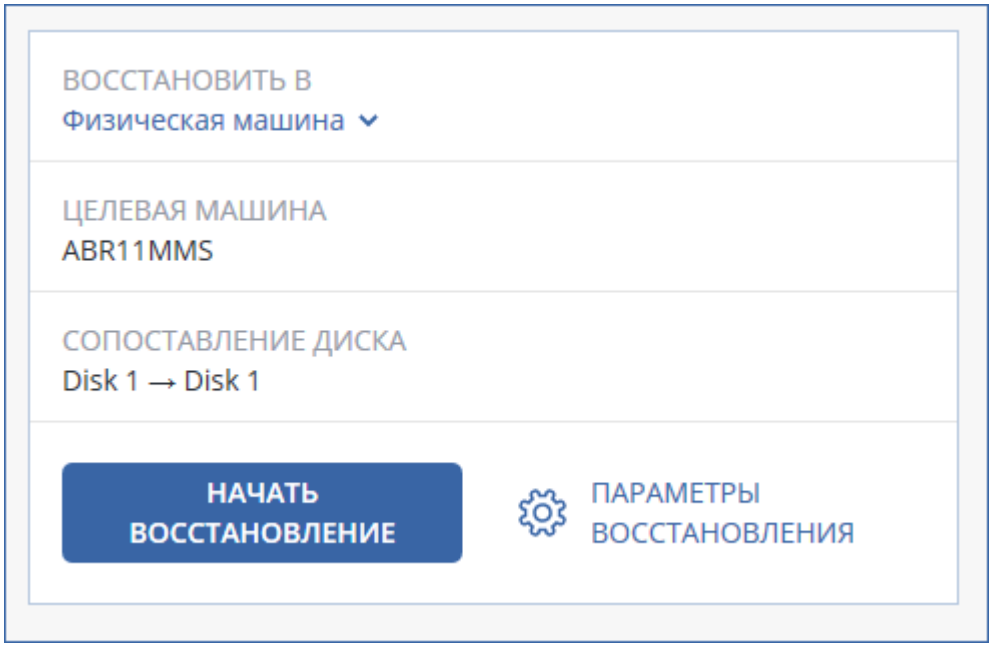
1. Выберите машину, для которой есть резервная копия.
2. Щелкните **Восстановление**.
3. Выберите точку восстановления. Обратите внимание на то, что точки восстановления отфильтрованы по хранилищу.

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

   - Если резервная копия расположена в облачном или общем хранилище данных (т .е. другие агенты могут получить к ней доступ), щелкните **Выбрать машину**, выберите целевую машину, которая подключена, а затем выберите точку восстановления.
   - Выберите точку восстановления на вкладке «Резервные копии» (стр. 126).
   - Восстановите машину, как описано в теме «Восстановление дисков с помощью загрузочного носителя» (стр. 108).
4. Последовательно выберите пункты **Восстановление** > **Вся машина**.

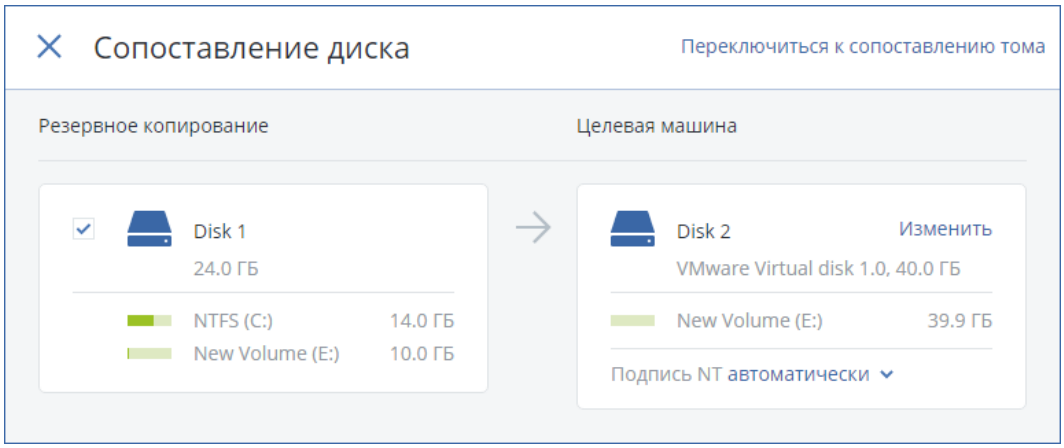
   Программное обеспечение автоматически сопоставит диски из резервной копии с дисками целевой машины.

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



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

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



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

Ход восстановления отображается на вкладке **Действия**.

9.4.2 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. 220).

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. 126).
   - Восстановите машину, как описано в теме «Восстановление дисков с помощью загрузочного носителя» (стр. 108).
4. Последовательно выберите пункты **Восстановление** > **Вся машина**.
5. В поле **Восстановить в** выберите пункт **Виртуальная машина**.
6. Щелкните **Целевая машина**.
   a. Выберите гипервизор (**VMware ESXi** или **Hyper-V**).

      Должен быть установлен хотя один агент для VMware или агент для Hyper-V.

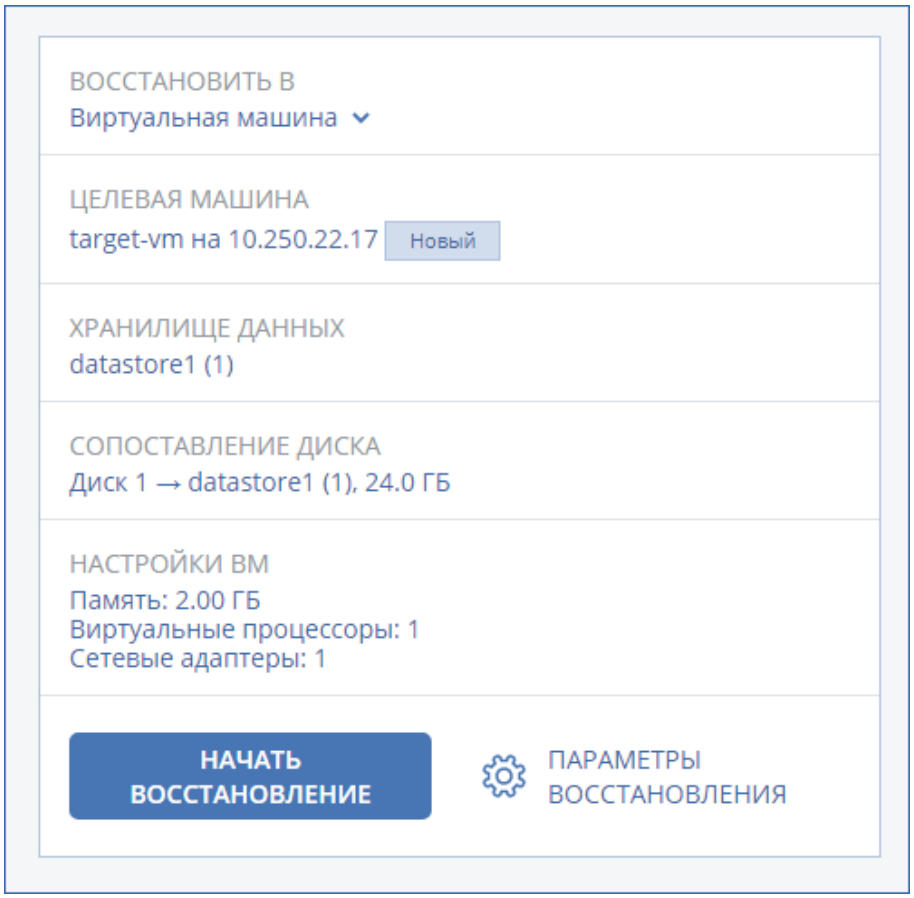
   b. Выберите машину, в которую будут выполняться восстановление: новая или существующая. Выбор новой машины предпочтительнее, поскольку для нее не требуется, чтобы конфигурация диска целевой машины в точности соответствовала конфигурации диска в резервной копии.

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

   d. Нажмите кнопку **ОК**.
7. [Необязательно] При восстановлении в новую машину также можно выполнить следующие действия:

   - Щелкните **Хранилище данных** для ESXi или **Путь** для Hyper-V и выберите хранилище данных для данной виртуальной машины.
   - Щелкните **Сопоставление дисков**, чтобы выбрать хранилище данных, интерфейс и режим распределения для каждого виртуального диска. Раздел сопоставления также позволяет выбирать отдельные диски для восстановления.

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



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

Ход восстановления отображается на вкладке **Действия**.

9.4.3 Виртуальная машина

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

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

Восстановление виртуальной машины

1. Выполните одно из следующих действий:
   - Выберите машину, для которой создана резервная копия, выберите **Восстановление** и выберите точку восстановления.
   - Выберите точку восстановления на вкладке «Резервные копии» (стр. 126).
2. Последовательно выберите пункты **Восстановление** > **Вся машина**.
3. Чтобы выполнить восстановление на физическую машину, в списке **Восстановить в** выберите пункт **Физическая машина**. В противном случае пропустите этот шаг.

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

Если это имеет место, продолжите с шага 4 в разделе «Физическая машина» (стр. 103). В противном случае рекомендуется выполнить миграцию V2P, используя загрузочный носитель (стр. 108).

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

   Чтобы выполнить восстановление на = другую виртуальную машину, выберите **Целевая машина** и выполните следующие действия:

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

      Только виртуальные машины Virtuozzo можно восстановить в Virtuozzo. Дополнительную информацию о миграции V2V см. в теме «Миграция машины» (стр. 220).

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

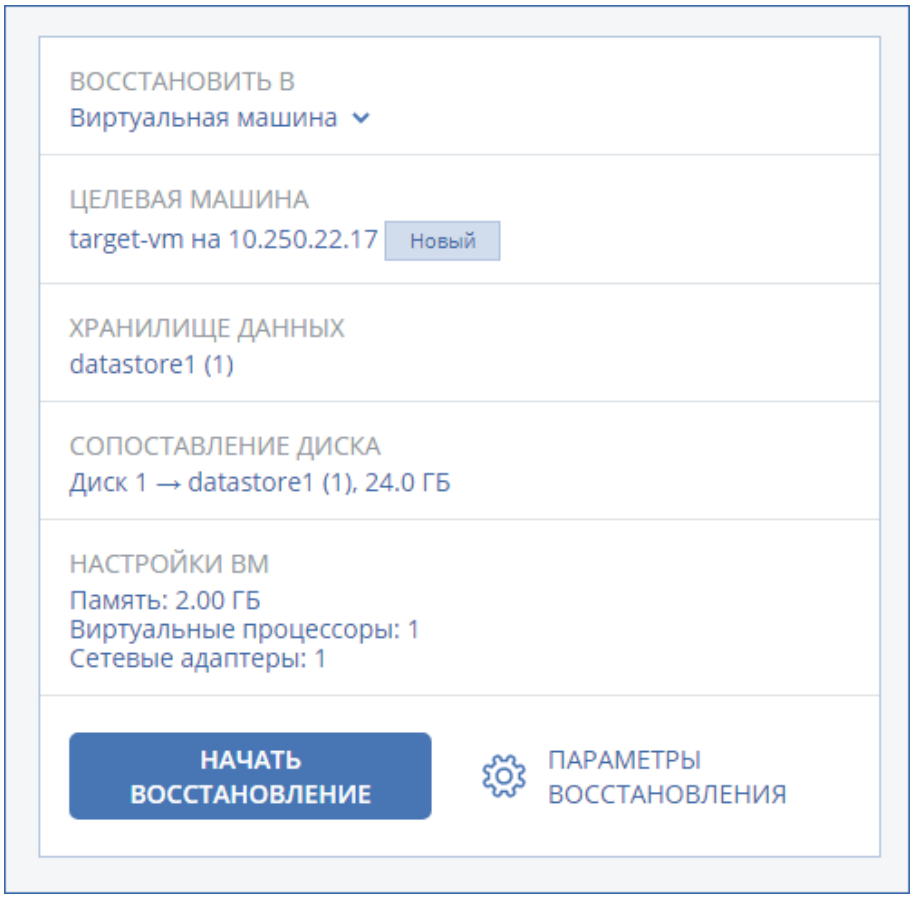
   c. Выберите хост и укажите имя новой машины или выберите существующую целевую машину.

   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.
   - Щелкните **Сопоставление дисков**, чтобы просмотреть хранилище данных, интерфейс и режим распределения для каждого виртуального диска. Эти настройки можно изменить, за исключением случаев, когда восстанавливается контейнер Virtuozzo. Раздел сопоставления также позволяет выбирать отдельные диски для восстановления.

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



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

Ход восстановления отображается на вкладке **Действия**.

9.4.4 Восстановление дисков с помощью загрузочного носителя

Информацию о том, как создать загрузочный носитель, см. в разделе «Создание загрузочного носителя» (стр. 101).

Порядок восстановления дисков с помощью загрузочного носителя

1. Загрузите целевую машину с помощью загрузочного носителя.
2. [Только при восстановлении Mac] При восстановлении дисков (томов) в формате APFS на машину, отличную от исходной, или на «голое железо» заново создайте конфигурацию оригинального диска вручную:
   a. Щелкните **Утилита проверки диска**.
   b. Заново создайте конфигурацию оригинального диска. Инструкции см. по ссылке https://support.apple.com/guide/disk-utility/welcome.
   c. Щелкните **Утилита проверки диска** > **Выйти из утилиты проверки диска**.
3. Выберите **Локальное управление этой машиной** или дважды щелкните **Загрузочный носитель** в зависимости от того, какой тип носителя используете.

4. Если в вашей сети включен прокси-сервер, последовательно выберите пункты **Инструменты** > **Прокси-сервер** и укажите имя хоста или IP-адрес, порт и учетные данные прокси-сервера. В противном случае пропустите этот шаг.
5. [Необязательно] При восстановлении Windows или Linux последовательно выберите пункты **Инструменты** > **Зарегистрировать носитель в сервисе резервного копирования** и введите маркер регистрации, полученный при загрузке носителя. Если вы сделаете это, для доступа к облачному хранилищу данных (процедура описана в шаге 8) не нужно будет вводить учетные данные или код регистрации.
6. На экране приветствия нажмите кнопку **Восстановить**.
7. Щелкните **Выбрать данные** и нажмите кнопку **Обзор**.
8. Укажите хранилище резервных копий.
   - Чтобы восстановить данные из облачного хранилища данных, выберите **Облачное хранилище данных**. Введите данные учетной записи резервного копирования, связанной с машиной, резервная копия которой вам нужна.

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

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

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

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

9.4.5 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. 110).
5. Нажмите кнопку **ОК**.

9.4.5.1 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.

9.4.5.2 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.

9.5 Восстановление файлов

9.5.1 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. Выполните любое из следующих действий:

   - [Рекомендуется] Если резервная копия расположена в облачном или общем хранилище данных (т. е. другие агенты могут получить к ней доступ), щелкните **Выбрать машину**, выберите целевую машину, которая подключена, а затем выберите точку восстановления.
   - Выберите точку восстановления на вкладке «Резервные копии» (стр. 126).
   - Загрузка файлов из облачного хранилища данных (стр. 113).
   - Использовать загрузочный носитель (стр. 116).
4. Последовательно выберите пункты **Восстановление** > **Файлы/папки**.
5. Перейдите к нужной папке или используйте поиск для получения списка нужных файлов и папок.

Можно использовать один или несколько подстановочных символов (* и ?). Подробную информацию об использовании подстановочных символов см. в разделе «Фильтры файлов» (стр. 84)..

Примечание *Поиск недоступен для резервных копий на уровне дисков, которые хранятся в облачном хранилище данных.*

6. Выберите файлы, которые необходимо восстановить.
7. Чтобы сохранить файлы как ZIP-файл, нажмите кнопку **Загрузить**, выберите расположение для сохранения данных и нажмите кнопку**Сохранить**. В противном случае пропустите этот шаг.

   Загрузка недоступна, если среди выбранных элементов есть папки или общий размер выбранных файлов превышает 100 МБ.
8. Нажмите кнопку **Восстановить**.

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

   - Машина, на которой изначально были файлы, которые необходимо восстановить (если на этой машине установлен агент).
   - Машина, на которой установлен агент для VMware, агент для Hyper-V или агент для 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. Щелкните **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**.

9.5.2 Загрузка файлов из облачного хранилища данных

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

Ограничения

- резервные копии состояния системы, баз данных SQL и Exchange недоступны для просмотра.
- Чтобы загрузка выполнялась без проблем, загружайте не более 100 МБ данных за один раз. Чтобы быстро извлечь большие объемы данных из облака, воспользуйтесь процедурой восстановления файлов (стр. 112).

Загрузка файлов из облачного хранилища данных

1. Выберите машину, для которой была создана резервная копия.

2. Последовательно выберите пункты **Восстановить** > **Другие способы восстановления...** > **Загрузить файлы**.
3. Введите данные учетной записи резервного копирования, связанной с машиной, резервная копия которой вам нужна.
4. [При просмотре резервных копий на уровне дисков] В разделе **Версии** щелчком мыши выберите резервную копию, с которой необходимо восстановить файлы.

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

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

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

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

9.5.3 Проверка подлинности файла с использованием службы нотаризации

Если нотаризация была включена при проведении резервного копирования (стр. 68), можно проверить подлинность файла в резервной копии.

Проверка подлинности

1. Выберите файл, как описано в шагах 1-6 раздела «Восстановление файлов с помощью веб-интерфейса» (стр. 112).

2. Убедитесь, что выбранный файл помечен следующим значком:  . Это означает, что файл нотаризован.
3. Выполните одно из следующих действий:
   - Нажмите **Проверить**.

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

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

9.5.4 Подпись файла с использованием службы ASign

Примечание. *Эта функциональность недоступна в Стандартной редакции программы резервного копирования.*

ASign — это служба, позволяющая нескольким пользователям подписывать скопированный файл электронной подписью. Данная функция применима только к резервным копиям на уровне файлов, 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. 112).
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.

9.5.5 Восстановление файлов с помощью загрузочного носителя

Информацию о том, как создать загрузочный носитель, см. в разделе «Создание загрузочного носителя» (стр. 101).

Восстановление файлов с помощью загрузочного носителя

1. Загрузите целевую машину с помощью загрузочного носителя.
2. Выберите **Локальное управление этой машиной** или дважды щелкните **Загрузочный носитель** в зависимости от того, какой тип носителя используете.
3. Если в вашей сети включен прокси-сервер, последовательно выберите пункты **Инструменты** > **Прокси-сервер** и укажите имя хоста или IP-адрес, порт и учетные данные прокси-сервера. В противном случае пропустите этот шаг.
4. [Необязательно] При восстановлении Windows или Linux последовательно выберите пункты **Инструменты** > **Зарегистрировать носитель в сервисе резервного копирования** и введите маркер регистрации, полученный при загрузке носителя. Если вы сделаете это, для доступа к облачному хранилищу данных (процедура описана в шаге 7) не нужно будет вводить учетные данные или код регистрации.
5. На экране приветствия нажмите кнопку **Восстановить**.
6. Щелкните **Выбрать данные** и нажмите кнопку **Обзор**.
7. Укажите хранилище резервных копий.
   - Чтобы восстановить данные из облачного хранилища данных, выберите **Облачное хранилище данных**. Введите данные учетной записи резервного копирования, связанной с машиной, резервная копия которой вам нужна.

     При восстановлении Windows или Linux есть возможность запросить код регистрации и использовать его вместо учетных данных. Последовательно выберите пункты **Использовать код регистрации** > **Запросить код**. В программе будет показана ссылка на регистрацию и код регистрации. Можно скопировать их и пройти все необходимые этапы регистрации на другой машине. Код регистрации действует только один час.

- Чтобы восстановить данные из локальной или сетевой папки, укажите ее в разделе **Локальные папки** или **Сетевые папки**.

Нажмите кнопку **ОК**, чтобы подтвердить выбор.

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

9.5.6 Извлечение файлов из локальных резервных копий

Можно просмотреть содержимое резервных копий и извлечь необходимые файлы.

Требования

- Эта функциональность доступна только в Windows при использовании проводника.
- На машине, на которой выполняется поиск резервной копии, необходимо установить агент резервного копирования.
- Файловая система, для которой создается резервная копия, должна иметь один из следующих типов: FAT16, FAT32, NTFS, ReFS, Ext2, Ext3, Ext4, XFS или HFS+.
- Резервная копия должна хранится в локальной папке или в сетевой папке (SMB/CIFS).

Порядок извлечения файлов из резервной копии

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

   `<имя машины> - <GUID плана 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.

9.6 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**.

9.7 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. 101).

Если при восстановлении конфигурации ESXi на хост, который не является исходным, исходный хост ESXi все еще подключен к vCenter Server, отключите и удалите этот хост из vCenter Server, чтобы избежать неожиданных проблем при восстановлении. Чтобы сохранить исходный хост вместе с восстановленным, можно снова добавить его по окончании восстановления.

Виртуальные машины, которые выполняются на данном хосте, не включены в резервную копию конфигурации ESXi. Создать для них резервную копию и восстановить их можно отдельно.

Порядок восстановления конфигурации ESXi

1. Загрузите целевую машину с помощью загрузочного носителя.
2. Щелкните **Локальное управление этой машиной**.
3. На экране приветствия нажмите кнопку **Восстановить**.
4. Щелкните **Выбрать данные** и нажмите кнопку **Обзор**.
5. Укажите хранилище резервных копий.
   - Укажите папку в разделе **Локальные папки** или **Сетевые папки**.

   Нажмите кнопку **ОК**, чтобы подтвердить выбор.
6. В поле **Показать** выберите **Конфигурации ESXi**.
7. Выберите резервную копию, из которой необходимо восстановить данные. При появлении соответствующего запроса введите пароль для резервной копии.
8. Нажмите кнопку **ОК**.
9. В разделе **Диски для новых хранилищ данных** выполните следующие действия:
   - В поле **Восстановить ESXi в** выберите диск, на который будет восстановлена конфигурация хоста. При восстановлении конфигурации на исходный хост исходный диск выбирается по умолчанию.
   - [Необязательно] В поле **Использовать для новых хранилищ данных** выберите диски, в которых будут созданы новые хранилища данных. Будьте внимательны, поскольку все данные на выбранных дисках могут быть утрачены. Чтобы сохранить виртуальные машины в существующих хранилищах данных, не выбирайте никакие диски.
10. Если для новых хранилищ данных выбраны какие-либо диски, выберите метод создания хранилища данных в поле **Создание новых хранилищ данных**: **Создать одно хранилище данных на диск** или **Создать одно хранилище на всех выбранных жестких дисках**.
11. [Необязательно] В разделе **Сопоставление сети** измените результат автоматического сопоставления виртуальных коммутаторов, присутствующих в резервной копии, с физическими сетевыми картами.
12. [Необязательно] Щелкните **Параметры восстановления**, чтобы указать дополнительные настройки.
13. Нажмите кнопку **ОК**, чтобы начать восстановление.

9.8 Параметры восстановления

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

Доступность параметров восстановления

Набор доступных параметров восстановления зависит от следующих факторов.

- Среда, в которой работает агент, выполняющий восстановление (Windows, Linux, macOS или загрузочный носитель).
- Тип данных, для которых выполняется восстановление (диски, файлы, виртуальные машины, данные приложения).

Следующая таблица включает в себя общие сведения о доступности параметров восстановления.

	Диски			**Файлы**				**Виртуальные машины**	**SQL и Exchange**
	Windows	Linux	Загрузочный носитель	Windows	Linux	macOS	Загрузочный носитель	ESXi, Hyper-V и Virtuozzo	Windows
Проверка резервных копий (стр. 120)	+	+	+	+	+	+	+	+	+
Режим загрузки (стр. 120)	+	–	–	–	–	–	–	+	–
Дата и время для файлов (стр. 121)	–	–	–	+	+	+	+	–	–
Обработка ошибок (стр. 122)	+	+	+	+	+	+	+	+	+
Исключения файлов (стр. 122)	–	–	–	+	+	+	+	–	–
Безопасность на уровне файлов (стр. 123)	–	–	–	+	–	–	–	–	–
Flashback (стр. 123)	+	+	+	–	–	–	–	+	–
Восстановление полного пути (стр. 123)	–	–	–	+	+	+	+	–	–
Точки подключения (стр. 123)	–	–	–	+	–	–	–	–	–
Производительность (стр. 124)	+	+	–	+	+	+	–	+	+

	Диски			Файлы				Виртуальные машины	SQL и Exchange
	Windows	Linux	Загрузочный носитель	Windows	Linux	macOS	Загрузочный носитель	ESXi, Hyper-V и Virtuozzo	Windows
Команды до и после процедуры (стр. 124)	+	+	–	+	+	+	–	+	+
Изменение идентификатора безопасности (стр. 125)	+	–	–	–	–	–	–	–	–
Управление питанием ВМ (стр. 126)	–	–	–	–	–	–	–	+	–
Журнал событий Windows (стр. 126)	+	–	–	+	–	–	–	Только Hyper-V	+

9.8.1 Проверка резервных копий

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.

9.8.2 Режим загрузки

Этот параметр работает при восстановлении физической или виртуальной машины с резервной копии на уровне дисков, которая содержит операционную систему Windows.

Этот параметр позволяет выбрать режим загрузки (BIOS или UEFI), который Windows будет использовать после восстановления. Если режим загрузки исходной машины отличается от выбранного режима загрузки, программа:

- Инициализирует диск, на который восстанавливается системный том в соответствии с выбранным режимом загрузки (MBR для BIOS, GPT для UEFI).

- Адаптирует операционную систему Windows для запуска в выбранном режиме загрузки.

Значение по умолчанию: **Как и в целевой машине.**

Можно выбрать один из следующих вариантов:

- **Как и в целевой машине**

  Агент, запущенный на целевой машине, определяет режим загрузки, который в настоящее время используется Windows, и вносит изменения в соответствии с обнаруженным режимом загрузки.

  Это наиболее безопасное значение, которое автоматически приводит к созданию загрузочной системы, если только не применяются указанные ниже ограничения. Поскольку параметр **Режим загрузки** отсутствует на загрузочном носителе, агент на носителе всегда работает таким образом, словно это значение выбрано.
- **Как и в машине, для которой есть резервная копия**

  Агент, запущенный на целевой машине, считывает режим загрузки с резервной копии и вносит изменения в соответствии этим режимом загрузки. Это помогает восстановить систему на другой машине, даже если на этой машине используется другой режим загрузки, а затем заменить диск на машине, для которой создана резервная копия.
- **BIOS**

  Агент, запущенный на целевой машине, вносит изменения для использования BIOS.
- **UEFI**

  Агент, запущенный на целевой машине, вносит изменения для использования UEFI.

После изменения параметра будет повторно выполнена процедура сопоставления диска. Это займет некоторое время.

Рекомендации

Чтобы передать Windows между UEFI и BIOS, выполните указанные ниже действия:

- Восстановите весь диск, на котором расположен системный том. При восстановлении только системного тома поверх существующего тома агент не сможет правильно инициализировать целевой диск.
- Помните, что BIOS не позволяет использовать более 2 ТБ дискового пространства.

Ограничения

- Перенос между UEFI и BIOS поддерживается для:
  - 64-разрядных операционных систем Windows, начиная с Windows Vista SP1.
  - 64-разрядных операционных систем Windows Server, начиная с Windows Server 2008 SP1.
- Перенос между UEFI и BIOS не поддерживается, если резервная копи хранится на ленточном устройстве.

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

9.8.3 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**.

9.8.4 Обработка ошибок

Они позволяют указать, как должны обрабатываться ошибки, возникшие при восстановлении.

В случае ошибки повторить попытку

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

Если возникла устранимая ошибка, программа будет продолжать попытки выполнить операцию. Задайте временной интервал и количество попыток. Попытки будут прекращены, как только операция будет успешно выполнена ИЛИ по достижении указанного максимального количества попыток (в зависимости от того, что наступит раньше).

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

Значение по умолчанию: **Отключено**.

В режиме без вывода сообщений программа автоматически разрешает ситуации, требующие вмешательства пользователя. Если операция не может быть продолжена без вмешательства пользователя, она не будет выполнена. Дополнительные сведения об операции, включая информацию об ошибках (если они есть), см. в журнале операций.

Сохранить сведения о системе при сбое восстановления с перезагрузкой

Этот параметр применим для диска или тома восстановления на физическую машину с Windows или Linux.

Значение по умолчанию: **Отключено**.

Если этот параметр включен, можно указать папку на локальном диске (включая устройства флэш-памяти или жесткие диски (HDD), подсоединенные к целевой машине) или на сетевой папке, в которую будут сохраняться журналы, сведения о системе и файлы аварийных дампов. Этот файл поможет сотрудникам технической поддержки определить проблему.

9.8.5 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.*

9.8.6 Безопасность на уровне файлов

Этот параметр действует только при восстановлении файлов томов NTFS с диска и резервных копий на уровне файлов.

Этот параметр определяет, должны ли восстанавливаться разрешения NTFS вместе с файлами.

Значение по умолчанию: **Включено**.

Можно выбрать восстановление разрешений или наследование файлами их разрешений NTFS из папки, в которую они восстанавливаются.

9.8.7 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**.

9.8.8 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**.

9.8.9 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. 87).

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.*

9.8.10 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.

9.8.11 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.

9.8.11.1 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	Установить	Установить	Снять	Снять

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

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

9.8.11.2 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.*

9.8.12 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.

9.8.13 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.

9.8.14 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

В этом разделе

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.

Резервные копии, созданные *облачным* агентом для Office 365, отображаются не в **облачном хранилище данных**, а в отдельном разделе с названием **Резервные копии приложений в облаке**.

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.

Если некоторые резервные копии добавлены или удалены в диспетчере файлов, щелкните значок шестерни рядом с именем хранилища, затем щелкните **Обновить**.

Хранилище резервных копий (за исключением облачного хранилища данных) исчезает с вкладки **Резервные копии**, если все машины, для которых когда-либо создавалась резервная копия в данном хранилище, были удалены из сервиса резервного копирования. Это гарантирует, что вам не нужно будет платить за резервные копии, которые хранятся в этом хранилище. Как только в этом хранилище создается резервная копия, оно заново добавляется на вкладку резервных копий вместе со всеми резервными копиями в нем.

Порядок выбора точки восстановления с использованием вкладки «Резервные копии»

1. На вкладке **Резервные копии** выберите хранилище резервных копий.

   В программном обеспечении отображаются все резервные копии, которые разрешено просматривать в выбранном хранилище для вашей учетной записи. Резервные копии объединены по группам. Группы имеют имена на основе следующего шаблона:

   `<имя машины> - <имя плана резервного копирования>`
2. Выберите группу, с которой необходимо восстановить данные.
3. [Необязательно] Щелкните **Изменить** рядом с полем **Машина для обзора** и выберите другую машину. Обзор некоторых резервных копий могут выполнить только определенные агенты. Например, чтобы просмотреть резервные копии баз данных Microsoft SQL Server, необходимо выбрать машину с запущенным агентом для SQL.

   Важная информация. *Имейте в виду, что расположение, указанное в поле **Машина для обзора**, является расположением по умолчанию для восстановления с резервной копии физической машины. После того как вы выберете точку восстановления и щелкните **Восстановление**, дважды проверьте настройку **Целевая машина**, чтобы убедиться в правильности указанной машины, в которую будут выполнено восстановление. Чтобы изменить целевое место восстановления, укажите другую машину в поле **Машина для обзора**.*
4. Щелкните **Показать резервные копии**.
5. Выберите точку восстановления.

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

Предупреждение. *При удалении резервной копии все ее данные удаляются окончательно. Удаленные данные невозможно восстановить.*

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 X.
   - 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, а затем щелкните значок X.
   - Чтобы удалить выбранную группу, щелкните **Удалить**.
4. Подтвердите операцию.

Порядок удаления резервных копий непосредственно из облачного хранилища данных

1. Войдите в облачное хранилище данных, как описано в разделе "Загрузка файлов из облачного хранилища данных" (стр. 113).
2. Щелкните имя машины, для которой необходимо удалить резервные копии.

   В программе будет показано несколько групп резервных копий.
3. Щелкните значок шестерни рядом с группой резервных копий, которую необходимо удалить.
4. Нажмите кнопку **Удалить**.
5. Подтвердите операцию.

Если вы удалили локальные резервные копии в диспетчере файлов

Мы рекомендуем удалять резервные копии на консоли резервного копирования всегда, когда это возможно. Если вы удалили локальные резервные копии в диспетчере файлов, выполните следующие действия:

1. На вкладке **Резервные копии** щелкните значок шестерни рядом с именем хранилища.
2. Нажмите кнопку **Обновить**.

Таким образом вы передадите в сервис резервного копирования информацию об уменьшении использования локального хранилища данных.

11 Операции с планами резервного копирования

Информацию о том, как создать план резервного копирования, см. в разделе «Резервное копирование» (стр. 41).

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 значок шестеренки рядом с именем плана резервного копирования и выберите команду **Изменить**.
5. Чтобы изменить параметры плана, щелкните соответствующий раздел на его панели.
6. Щелкните **Сохранить изменения**.
7. Чтобы изменить план резервного копирования для всех машин, к которым 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 значок шестеренки рядом с именем плана резервного копирования и выберите пункт **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 значок шестеренки рядом с именем плана резервного копирования и выберите пункт **Удалить**.

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

12 Вкладка «Планы»

Примечание. *Эта функциональность недоступна в Стандартной редакции программы резервного копирования.*

Планами резервного копирования и прочими планами можно управлять на вкладке **Планы**.

Каждый раздел вкладки **Планы** содержит планы конкретного типа. Доступны следующие разделы

- **Резервное копирование** (стр. 131)
- **Облачная резервная копия приложения** (стр. 131)
- **Репликация ВМ** (стр. 203)

12.1 Резервное копирование

В разделе **Резервное копирование** показаны планы резервного копирования, назначенные агентам, которые выполняются на вашей локальной площадке.

В разделе **Резервное копирование** можно выполнить указанные ниже операции:

- Создавать, просматривать, запускать, останавливать, изменять, клонировать, отключать, включать и удалять план резервного копирования

  В отличии от остановки резервного копирования на вкладке **Устройства**, план резервного копирования будет остановлен на всех устройствах, на которых он выполняется. Если на разных устройствах резервное копирование запускается в разное время, то после остановки плана резервного копирования оно не будет запускаться на тех устройствах, на которых оно еще не выполнялось.
- Просматривать действия, относящиеся к каждому плану резервного копирования
- Просматривать оповещения, относящиеся к каждому плану резервного копирования
- Экспортировать план в файл
- Импортировать ранее экспортированный план

12.2 Планы резервного копирования для облачных приложений

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

В этом разделе можно выполнить указанные ниже операции:

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

Дополнительную информацию о резервных копиях приложений в облаке см. в следующих темах:

- Защита данных Office 365 (стр. 159)
- Защита данных G Suite (стр. 178)

Запуск процессов резервного копирования «облако в облако» вручную

Во избежание прерывания работы сервиса резервного копирования количество ручных запусков резервного копирования «облако в облако» ограничено 10 запусками в час на одну организацию Office 365 или G Suite. По достижении этого количества число разрешенных запусков сбрасывается до одного в час, а каждый последующий час становится доступным один дополнительный запуск. Пример: первый час — 10 запусков, второй час — 1 запуск, третий час — 2 запуска и т. д. до достижения показателя в 10 запусков в час.

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

13 Защита приложений Microsoft

Защита Microsoft SQL Server и Microsoft Exchange Server

Есть два метода для защиты этих приложений:

- **Резервная копия базы данных**

  Это резервное копирование на уровне файлов базы данных и метаданных, связанных с ней. Базы данных можно восстановить в запущенное приложение или как файлы.

- **Резервное копирование с поддержкой приложений**

  Это резервное копирование на уровне дисков, при котором также выполняется сбор метаданных приложений. Эти метаданные позволяют выполнить обзор и восстановление данных приложений, не восстанавливая весь диск или том. Диск или том также можно восстановить полностью. Это означает, что можно использовать единое решение и один план резервного копирования как для аварийного восстановления, так и для защиты данных.

Для Microsoft Exchange Server вы можете выбрать **Резервное копирование почтового ящика**. При выборе данной опции будут созданы резервные копии отдельных почтовых ящиков посредством протокола Exchange Web Services. Почтовые ящики или элементы почтового ящика могут быть восстановлены на запущенный Exchange Server или на Microsoft Office 365. Резервное копирование почтовых ящиков поддерживается Microsoft Exchange Server 2010 Service Pack 1 (SP1) и более поздней версии.

Защита Microsoft SharePoint

Ферма Microsoft SharePoint состоит из серверов веб-интерфейса, на которых выполняются службы SharePoint, серверов баз данных, на которых выполняется Microsoft SQL Server и (необязательно) серверов приложений, которые разгружают серверы веб-интерфейса от некоторых служб SharePoint. Некоторые серверы веб-интерфейса и серверы приложений могут быть идентичны друг другу.

Чтобы защитить всю ферму SharePoint, выполните указанные ниже действия:

- Создайте резервные копии серверов базы данных, выполнив резервное копирование с поддержкой приложений.
- Создайте резервные копии всех уникальных серверов веб-интерфейса и серверов приложений, выполнив обычное резервное копирование на уровне дисков.

Резервные копии всех серверов должны быть выполнены по одному расписанию.

Чтобы защитить только содержимое, можно создать резервные копии баз данных по отдельности.

Защита контроллера домена

Машину под управлением доменных служб Active Directory можно защитить резервным копированием с поддержкой приложений. Если домен содержит несколько контроллеров домена, то при восстановлении одного из них выполняется непринудительное восстановление; при этом откат USN не выполняется после восстановления.

Восстановление приложений

В таблице приведена сводка доступных методов восстановления приложений.

	Из резервной копии базы данных	Из резервной копии с поддержкой приложений	Из резервной копии диска
Microsoft SQL Server	Базы данных в запущенный экземпляр SQL Server (стр. 143) Базы данных как файлы (стр. 143)	Вся машина (стр. 103) Базы данных в запущенный экземпляр SQL Server (стр. 143) Базы данных как файлы (стр. 143)	Вся машина (стр. 103)
Microsoft Exchange Server	Базы данных в запущенный Exchange (стр. 147) Базы данных как файлы (стр. 147) Фрагментарное восстановление в запущенный Exchange или Office 365* (стр. 149)	Вся машина (стр. 103) Базы данных в запущенный Exchange (стр. 147) Базы данных как файлы (стр. 147) Фрагментарное восстановление в запущенный Exchange или Office 365* (стр. 149)	Вся машина (стр. 103)
Серверы базы данных Microsoft SharePoint	Базы данных в запущенный экземпляр SQL Server (стр. 143) Базы данных как файлы (стр. 143) Фрагментарное восстановление с использованием SharePoint Explorer	Вся машина (стр. 103) Базы данных в запущенный экземпляр SQL Server (стр. 143) Базы данных как файлы (стр. 143) Фрагментарное восстановление с использованием SharePoint Explorer	Вся машина (стр. 103)
Интерфейсные веб-серверы Microsoft SharePoint	–	–	Вся машина (стр. 103)
Доменные службы Active Directory	–	Вся машина (стр. 103)	–

* Фрагментарное восстановление также доступно из резервной копии почтового ящика. Восстановление элементов данных Exchange в Office 365 и наоборот поддерживается в том случае, когда агент для Office 365 установлен локально.

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.
- 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. 98).
- Для виртуальных машин включен параметр резервного копирования Служба теневого копирования томов (VSS) для виртуальных машин (стр. 99).

Дополнительные требования для операций резервного копирования с поддержкой приложений

При создании плана резервного копирования убедитесь, что для резервного копирования выбран параметр **Вся машина**. В плане резервного копирования необходимо отключить параметр резервного копирования **Sector-by-sector (Посекторно)**; в противном случае невозможно будет восстановить данные приложения из таких резервных копий. Если данный план выполнен в режиме **Sector-by-sector (Посекторно)** из-за автоматического перехода в этот режим, то и в этом случае восстановить данные приложения будет невозможно.

Требования для виртуальных машин ESXi

Если приложение выполняется на виртуальной машине, резервная копия которой создана агентом для VMware, убедитесь, что выполнены следующие условия:

- На машине установлен и обновлен набор утилит VMware Tools.
- Учетные записи пользователей (UAC) отключены на машине. Если вы не хотите отключать учетные записи пользователей (UAC), то при включении резервного копирования приложения необходимо предоставить учетные данные встроенного администратора домена (DOMAIN\Administrator).

Требования для виртуальных машин Hyper-V

Если приложение выполняется на виртуальной машине, резервная копия которой создана агентом для Hyper-V, убедитесь, что выполнены следующие условия:

- В качестве гостевой операционной системы используется Windows Server 2008 или более поздней версии.
- Для Hyper-V 2008 R2: в качестве гостевой операционной системы используется Windows Server 2008/2008 R2/2012.
- Виртуальная машина не имеет динамических дисков.

- Между хостом Hyper-V и гостевой операционной системой установлено сетевое подключение. Это необходимо для выполнения удаленных запросов WMI в виртуальной машине.
- Учетные записи пользователей (UAC) отключены на машине. Если вы не хотите отключать учетные записи пользователей (UAC), то при включении резервного копирования приложения необходимо предоставить учетные данные встроенного администратора домена (DOMAIN\Administrator).
- Конфигурация виртуальной машины соответствует следующем критерию:
  - Службы интеграции Hyper-V установлены и обновлены. Должно быть установлено критическое обновление, доступное по ссылке https://support.microsoft.com/en-us/help/3063109/hyper-v-integration-components-update-for-windows-virtual-machines
  - В настройках виртуальной машины включен параметр **Управление** > **Службы интеграции** > **Резервное копирование (контрольная точка тома)**.
  - Для Hyper-V 2012 и более поздних версий: виртуальная машина не имеет контрольных точек.
  - Для Hyper-V 2012 и более поздних версий: виртуальная машина имеет контроллер SCSI (проверьте **Настройки** > **Оборудования**).

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. 133).

Выберите базы данных, как указано ниже, а затем укажите другие настройки плана резервного копирования в зависимости от требований (стр. 42).

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. 86).

Порядок выбора баз данных SQL

1. Нажмите **Устройства** > **Microsoft SQL**.

   /Программное обеспечение отобразит дерево групп Always On Availability Groups (AAG) сервера SQL Server, машины, на которых запущен Microsoft SQL Server, экземпляры SQL Server и базы данных.
2. Перейдите к данным, для которых требуется создать резервные копии.

   Разверните узлы дерева или дважды щелкните элементы списка, расположенного справа от дерева.
3. Выберите данные, резервную копию которых необходимо создать. Выберите AAGs, машины, на которых запущен SQL Server, экземпляры SQL Server или отдельные базы данных.

- При выборе AAG, для всех баз данных, включенных в выбранную AAG, будет создана резервная копия. Дополнительные сведения о резервном копировании групп AAG см. в разделе «Защита групп Always On Availability Groups (AAG)» (стр. 137).
- При выборе машины на которых запущен SQL Server, будет создана резервная копия всех баз данных, подключенных к экземпляру SQL Server.
- При выборе экземпляра SQL Server, для всех баз данных, подключенных к выбранному экземпляру, будет создана резервная копия.
- Если выбрать отдельные базы, будут созданы резервные копии только для них.

4. Нажмите кнопку **Резервное копирование**. Если потребуется, введите учетные данные для доступа к SQL Server. Соответствующая учетная запись должна входить в группу **Операторы архива** или **Администраторы** на этой машине, а также иметь роль **системный администратор** в каждом из экземпляров, для которых создается резервная копия.

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**
2010/2013/2016/2019	Базы данных, Группы обеспечения доступности баз данных (DAG)	Участие в группе ролей **Управление сервером**.

При полном резервном копировании в копию включаются все выбранные данные Exchange Server.

Инкрементная резервная копия содержит измененные блоки файлов баз данных, файлы контрольных точек, а также небольшое количество файлов журналов, более новых по отношению к соответствующим контрольным точкам базы. Поскольку в резервную копию включаются изменения, внесенные в базу данных, добавлять в нее все записи из журналов транзакций с момента предыдущего резервного копирования не нужно. После восстановления воспроизводится только журнал, более новый, чем контрольная точка. Это позволяет ускорить восстановление и обеспечить резервное копирование базы, даже если включено циклическое ведение журнала.

После каждого успешного резервного копирования выполняется усечение файлов журнала транзакций.

Порядок выбора данных Exchange Server

1. Нажмите **Устройства** > **Microsoft Exchange**.

   Программное обеспечение отобразит дерево групп обеспечения доступности баз данных (DAG) Exchange Server, машины, на которых запущен Microsoft Exchange Server, и базы данных Exchange Server. Если агент для Exchange настроен, как описано в разделе «Резервное копирование почтовых ящиков» (стр. 142), в этом дереве также отображаются почтовые ящики.
2. Перейдите к данным, для которых требуется создать резервные копии.

   Разверните узлы дерева или дважды щелкните элементы списка, расположенного справа от дерева.
3. Выберите данные, резервную копию которых необходимо создать.

- При выборе DAG создаются резервные копии одной из копий каждой кластеризованной базы данных. Дополнительные сведения о резервном копировании групп DAG см. в разделе«Защита групп обеспечения доступности базы данных (DAG)» (стр. 138).
- При выборе машины на которых запущен сервер Microsoft Exchange, будет создана резервная копия всех баз данных, подключенных к серверу Exchange.
- Если выбрать отдельные базы, будут созданы резервные копии только для них.
- Если агент для Exchange настроен, как описано в разделе «Резервное копирование почтовых ящиков» (стр. 142), можно выбрать почтовые ящики для резервного копирования (стр. 143).

4. Если потребуется, введите учетные данные для доступа к информации.
5. Нажмите кнопку **Резервное копирование**.

13.2.3 Защита группы Always On Availability Groups (AAG)

Примечание. *Эта функциональность недоступна в Стандартной редакции программы резервного копирования.*

Обзор решений для SQL Server высокой доступности

Функция отказоустойчивой кластеризации Windows Server (WSFC) позволяет настроить SQL-сервер с высоким уровнем доступности посредством избыточности на уровне экземпляра (экземпляр отказоустойчивого кластера, FCI) или на уровне базы данных (AlwaysOn Availability Group, AAG). Оба метода можно сочетать.

В экземпляре отказоустойчивого кластера базы данных SQL расположены в общем хранилище. Доступ к этому хранилищу возможен только с активного узла кластера. При сбое активного узла происходит переход, и активным становится другой узел.

В группе обеспечения доступности все реплики баз данных располагаются на разных узлах. Если основная реплика становится недоступна, основная роль назначается дополнительной реплике, расположенной на другом узле.

Таким образом, уже сами кластеры являются решением по аварийному восстановлению. Однако в некоторых случаях кластеры не могут обеспечить защиту данных: например, при логическом повреждении базы данных, отсутствии копии или реплики какой-то базы данных в кластере или отказе всего кластера. Кроме того, кластерные решения не защищают от вредоносных изменений содержимого, поскольку обычно эти изменения немедленно реплицируются на все узлы кластера.

Поддерживаемые конфигурации кластеров

Это программное обеспечение поддерживает *только* группы обеспечения доступности Always On SQL Server (AAG) для SQL Server 2012 или более поздних версий. Прочие конфигурации кластеров, такие как, например, Failover Cluster Instances, зеркальное отображение базы данных и доставка журналов, *не* поддерживаются.

Сколько требуется агентов для резервного копирования и восстановления данных кластера?

Для успешного резервного копирования и восстановления данных кластера необходимо установить агент для SQL на каждом узле кластера WSFC.

В AAG включено резервное копирование баз данных

1. Установите агент для SQL на каждый узел кластера WSFC.

   Подсказка *После установки агента на одном из узлов программное обеспечение отобразит AAG и ее узлы в поле* ***Устройства*** *>* ***Microsoft SQL*** *>* ***Базы данных****. Для установки агента для SQL на остальных узлах выберите AAG, нажмите* ***Сведения****, после чего нажмите* ***Установить агент*** *возле каждого узла.*

2. Выберите AAG для создания резервной копии в соответствии с инструкциями «Выбор баз данных SQL» (стр. 135).

   Важно! *Вы должны выбрать именно AAG, а не отдельные содержащиеся в ней узлы и базы данных. Если вы выберете отдельные элементы, содержащиеся в AAG, резервные копии не будут поддерживать кластеры и будут созданы резервные копии только выбранных копий элементов.*

3. Настройте параметр резервного копирования «Способ резервного копирования кластера» (стр. 80).

Восстановление баз данных, включенных в AAG

1. Выберите базы данных, которые необходимо восстановить, а затем выберите желаемую точку восстановления данных.

   При переходе **Устройства** > **Microsoft SQL** > **Базы данных**, выборе кластеризованной базы данных и нажатии **Восстановить**, программное обеспечение отобразит только те точки восстановления, которые соответствуют временам создания резервной копии выбранной копии базы данных.

   Самый легкий способ просмотра всех точек восстановления кластеризованной базы данных — выбор резервной копии всей AAG на вкладке «Резервные копии» (стр. 126). Имена резервных копий AAG помечены особым значком и составляются по следующему шаблону: `<имя AAG> - <имя плана резервного копирования>`.

2. Для конфигурирования восстановления выполните действия, описанные в разделе «Восстановление баз данных SQL» (стр. 143) (начиная с шага 5).

   Программное обеспечение автоматически определяет узел кластера, на который будут восстановлены данные. Имя узла отображается в поле **Восстановить на**. Вы можете вручную изменить целевой узел.

   Важно! *База данных, включенная в группу Always On Availability Group, не может быть перезаписана во время восстановления, поскольку это запрещено правилами Microsoft SQL Server. Необходимо исключить целевую базу данных из AAG перед восстановлением. Либо можно просто восстановить базу данных как новую базу, не входящую в AAG. После завершения восстановления можно воссоздать исходную конфигурацию AAG.*

13.2.4 Защита групп обеспечения доступности базы данных (DAG)

Примечание. *Эта функциональность недоступна в Стандартной редакции программы резервного копирования.*

Обзор кластеров Exchange Server

Основная идея кластеров Exchange обеспечить высокую доступность базы данных с быстрым переходом к реплике и без потери данных. Обычно для этого одна или несколько копий баз данных или групп хранения находятся на элементах (узлах) кластера. В случае отказа узла кластера, на котором находится активная копия базы данных, или самой активной копии базы данных, другой узел кластера, содержащий пассивную копию, автоматически берет на себя

операции с отказавшего узла и предоставляет доступ к службам Exchange с минимальным простоем. Таким образом, уже сами кластеры являются решением по аварийному восстановлению.

Однако в некоторых случаях решение с использованием отказоустойчивых кластеров не может обеспечить защиту данных: например, при логическом повреждении базы данных, отсутствии копии или реплики какой-то базы данных в кластере или отказе всего кластера. Кроме того, кластерные решения не защищают от вредоносных изменений содержимого, поскольку обычно эти изменения немедленно реплицируются на все узлы кластера.

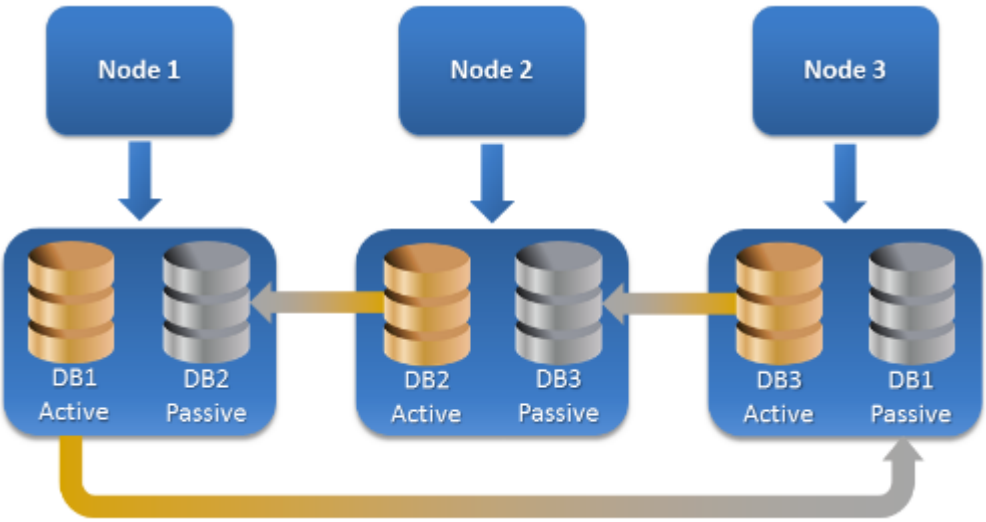
Резервное копирование с поддержкой кластеров

Используя резервное копирование с поддержкой кластеров, вы создаете только одну копию кластеризированных данных. Если данные меняют свое расположение в кластере (например, из-за переключения или перехода к реплике), программное обеспечение отслеживает все перемещения этих данных и благополучно создает их резервную копию.

Поддерживаемые конфигурации кластеров

Резервное копирование с поддержкой кластеров поддерживается *только* для группы обеспечения доступности баз данных (DAG) в Exchange Server 2010 или более поздней версии. Другие кластерные конфигурации, такие как кластер с единым хранилищем (SCC) и непрерывная репликация кластера (CCR) для Exchange 2007 *не* поддерживаются.

Группа DAG включает до 16 серверов почтовых ящиков Exchange. На любом узле может располагаться копия базы данных почтовых ящиков с любого другого узла. Каждый узел может содержать пассивные и активные копии базы данных. Может быть создано до 16 копий каждой базы данных.



Сколько требуется агентов для резервного копирования и восстановления данных кластера?

Для успешного резервного копирования и восстановления кластеризованных баз данных необходимо установить агент для Exchange на каждом узле кластера Exchange.

Подсказка *После установки агента на одном из узлов программное обеспечение отобразит DAG и ее узлы в поле* ***Устройства*** *>* ***Microsoft Exchange*** *>* ***Базы данных****. Для установки агента для Exchange на остальных узлах выберите DAG, нажмите* ***Сведения****, после чего нажмите* ***Установить агент*** *возле каждого узла.*

Создание резервной копии данных кластера Exchange

1. При создании плана резервного копирования выберите DAG в соответствии с инструкциями в разделе «Выбор данных Exchange Server» (стр. 136).
2. Настройте параметр резервного копирования «Способ резервного копирования кластера» (стр. 80).
3. Укажите другие необходимые (стр. 42) настройки плана резервного копирования.

Важная информация *Для резервного копирования с поддержкой кластеров необходимо выбрать саму группу обеспечения доступности баз данных. Если выбрать отдельные узлы или базы данных в группе обеспечения доступности баз данных, то будет создана резервная копия только для выбранных элементов, а параметр* ***Способ резервного копирования кластера*** *будет проигнорирован.*

Восстановление данных кластера Exchange

1. Выберите точку восстановления для базы данных, которую необходимо восстановить. Резервное копирование всего кластера для восстановления невозможно.

   Если в разделе **Устройства** > **Microsoft Exchange** > **Базы данных** > <имя кластера> > <имя узла> выбрать копию кластеризованной базы данных и нажать кнопку **Восстановить**, в программном обеспечении будут показаны только те точки восстановления, которые соответствуют времени создания резервной копии выбранной копии базы данных.

   Самый легкий способ просмотра всех точек восстановления кластеризованной базы данных — выбор соответствующей резервной копии на вкладке «Резервные копии» (стр. 126).
2. Выполните действия, описанные в разделе «Восстановление баз данных Exchange», начиная с шага 5.

   Программное обеспечение автоматически определяет узел кластера, на который будут восстановлены данные. Имя узла отображается в поле **Восстановить на**. Вы можете вручную изменить целевой узел.

13.3 Резервное копирование с поддержкой приложений

Резервная копия на уровне дисков с поддержкой приложений доступна для физических машин, виртуальных машин ESXi и виртуальных машин Hyper-V.

При резервном копировании машины, на которой выполняется Microsoft SQL Server, Microsoft Exchange Server или доменные службы Active Directory, включите **Резервное копирование приложений** для дополнительной защиты данных этих приложений.

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. 86). Журналы транзакций Exchange сокращаются только на виртуальных машинах. Чтобы урезать размер журналов транзакций Exchange на физической машине, можно включить параметр полного восстановления VSS (стр. 98).
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) или агентом для Hyper-V.

Агент для VMware (виртуальное устройство) может создать резервные копии с поддержкой приложений, но не может восстановить из них данные приложений. Чтобы восстановить данные приложений из резервных копий, созданных этим агентом, необходимо иметь агент для VMware (Windows), агент для SQL или агент для Exchange на машине с доступом к хранилищу, в котором хранятся резервные копии. При настройке восстановления данных приложения выберите точку восстановления на вкладке **Резервные копии**, а затем выберите эту машину в списке **Машина для обзора**.

Другие требования перечислены в разделах «Предварительные требования» (стр. 133) и «Необходимые права пользователя» (стр. 141).

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.

Дополнительные требования для виртуальных машин

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

13.4 Резервная копия почтового ящика

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

Резервная копия почтового ящика доступна, если на сервере управления зарегистрирован по меньшей мере один агент для Exchange. Этот агент должен быть установлен на машине, которая находится в одном лесу Active Directory с сервером Microsoft Exchange Server.

Перед выполнением резервного копирования почтовых ящиков вы должны подключить агент для Exchange к машине с серверной ролью (CAS) **Client Access** сервера Microsoft Exchange Server. В Exchange 2016 и более поздних версиях роль CAS не устанавливается отдельно. Она устанавливается автоматически как часть роли сервера почтовых ящиков. Таким образом, можно подключить агент к любому серверу, которому присвоена **роль почтовых ящиков**.

Как подключить агент для Exchange к CAS

1. Нажмите **Устройства** > **Добавить**.
2. Нажмите **Microsoft Exchange Server**.
3. Щелкните **Почтовые ящики Exchange**.

   Если на сервере управления не зарегистрировано ни одного агента для Exchange, программное обеспечение попросит вас установить агент. После установки повторите эту процедуру с шага 1.
4. [Необязательно] Если на сервере управления зарегистрировано несколько агентов для Exchange, щелкните **Агент** и измените агент, который выполнит резервное копирование.
5. На сервере **Client Access Server** укажите полное доменное имя машины (FQDN), на которой включена роль **Клиентский доступ** Microsoft Exchange Server.

   В Exchange 2016 и более поздних версиях службы клиентского доступа автоматически устанавливаются в рамках роли сервера почтовых ящиков. Таким образом, можно указать любой сервер, которому присвоена **роль почтовых ящиков**. В этом разделе подобный сервер обозначается аббревиатурой CAS.
6. В пункте **Тип аутентификации**, выберите тип аутентификации, используемый CAS. Можно выбрать **Kerberos** (по умолчанию) или **Базовый**.
7. [Только для базовой аутентификации] Выберите используемый протокол. Можно выбрать **HTTPS** (по умолчанию) или **HTTP**.
8. [Только для базовой аутентификации с протоколом HTTPS] Если CAS использует сертификат SSL, полученный от сертифицирующей организации, и вы желаете, чтобы программное обеспечение проверяло сертификат SSL при подключении к CAS, установите флажок **Проверять сертификат SSL**. В противном случае пропустите этот шаг.
9. Укажите учетные данные учетной записи, которые будут использоваться для доступа к CAS. Требования к этой учетной записи указаны в разделе «Требуемые права пользователя» (стр. 143).
10. Нажмите кнопку **Добавить**.

В результате почтовый ящик будет находиться по пути **Устройства** > **Microsoft Exchange** > **Почтовые ящики**.

13.4.1 Выбор почтовых ящиков сервера Exchange

Выберите почтовый ящики, как указано ниже, а затем укажите другие настройки плана резервного копирования как требуется (стр. 42).

Выбор почтовых ящиков Exchange

1. Нажмите **Устройства** > **Microsoft Exchange**.

   Программное обеспечение отобразит дерево баз данных и почтовых ящиков Exchange
2. Нажмите **Почтовые ящики**, после чего выберите почтовые ящики, для которых необходимо создать резервные копии.
3. Нажмите кнопку **Резервное копирование**.

13.4.2 Требуемые права пользователя

Чтобы получить доступ к почтовым ящикам, агенту для Exchange необходима учетная запись с соответствующими правами. При настройке различных операций с почтовыми ящиками пользователю поступает запрос на указание учетной записи.

Членство учетной записи в группе ролей **Управление организацией** позволяет получить доступ к любому почтовому ящику, включая почтовые ящики, которые будут созданы в будущем.

Минимальные требуемые права пользователя:

- Учетная запись должна входить в группы ролей **Управление сервером** и **Управление получателями**.
- Для учетной записи должна быть включена роль управления **ApplicationImpersonation** для всех пользователей или групп пользователей, к почтовым ящикам которых будет обращаться агент.

  Информацию о настройке роли управления **ApplicationImpersonation** см. в следующей статье базы знаний Microsoft: https://msdn.microsoft.com/en-us/library/office/dn722376.aspx.

13.5 Восстановление баз данных SQL

В этом разделе описано восстановление из резервных копий базы данных и резервных копий с поддержкой приложений.

Можно восстановить базы данных SQL в экземпляр SQL Server, если на машине с этим экземпляром установлен агент для SQL. Для этого потребуется указать данные учетной записи, которая входит в группу **Операторы архива** или **Администраторы** на этой машине, а также имеет роль **sysadmin** на целевом экземпляре.

Базы данных также можно восстанавливать в виде файлов. Это может быть полезным при необходимости извлечь данные для интеллектуального анализа данных, аудита или дальнейшей обработки с использованием инструментов сторонних поставщиков. Можно присоединить файлы базы данных SQL к экземпляру SQL Server, как описано в теме «Подключение баз данных SQL Server» (стр. 146).

Если используется только агент для VMware (Windows), то единственный доступный метод восстановления — восстановить базы данных как файлы. Невозможно восстановить базы данных с помощью агента для VMware (виртуальное устройство).

Системные базы данных восстанавливаются в целом так же, как и пользовательские. Особенности этой процедуры описаны в разделе «Восстановление системных баз данных» (стр. 146).

/Восстановление базы данных в запущенный экземпляр SQL Server

1. Выполните одно из следующих действий:
   - При восстановлении из резервной копии с поддержкой приложений в пункте **Устройства** выберите машину, на которой изначально располагались данные, которые необходимо восстановить.
   - При восстановлении из резервной копии базы данных нажмите **Устройства** > **Microsoft SQL** и затем выберите базы данных, которые необходимо восстановить.
2. Щелкните **Восстановление**.
3. Выберите точку восстановления. Обратите внимание на то, что точки восстановления отфильтрованы по хранилищу.

   Если машина отключена, точки восстановления не отображаются. Выполните одно из следующих действий:
   - [Только при восстановлении из резервной копии с поддержкой приложений] Если резервная копия расположена в облачном хранилище или общем хранилище (т. е., другие агенты могут получить к ней доступ), нажмите **Выбрать машину**, выберите включенную машину, на которой установлен агент для SQL, а затем выберите точку восстановления.
   - Выберите точку восстановления на вкладке «Резервные копии» (стр. 126).

   Машина, выбранная для обзора любым из двух вышеописанных действий, становится целевой машиной для восстановления баз данных SQL.
4. Выполните одно из следующих действий:
   - При восстановлении из резервной копии с поддержкой приложений нажмите **Восстановить** > **Базы данных SQL**, выберите базу данных, которую нужно восстановить, и затем нажмите **Восстановить**.
   - При восстановлении из резервной копии базы данных выберите **Восстановить** > **Базы данных в экземпляр**.
5. По умолчанию данные восстанавливаются в исходных базах. Если исходная база данных не существует, она будет создана. Можно выбрать другой экземпляр сервера SQL Server (запущенный на той же машине), в который требуется восстановить базы данных.

   Восстановление данных в другой базе на том же экземпляре
   a. Щелкните имя базы данных.
   b. В поле **Восстановить в** выберите вариант **Новая база данных**.
   c. Укажите имя новой базы данных.
   d. Укажите путь к новой базе данных и журналу. В указанной папке не должно быть файлов исходной базы данных и ее журналов.
6. Необязательно: чтобы изменить состояние базы данных после восстановления, щелкните ее имя и выберите один из перечисленных ниже вариантов.
   - **Готово к использованию (RESTORE WITH RECOVERY)** (по умолчанию)

     После завершения восстановления база данных будет готова к использованию. Пользователи будут иметь к ней полный доступ. Программа выполнит откат всех незафиксированных транзакций восстановленной базы данных, хранящихся в журналах транзакций. Вы не сможете восстановить дополнительные журналы транзакций из резервных копий в собственном формате Microsoft SQL.

- **Не работает (RESTORE WITH NORECOVERY)**

  Использовать базу данных после завершения восстановления будет невозможно. Пользователи не будут иметь к ней доступа. Программа сохранит все незафиксированные транзакции восстановленной базы данных. Вы сможете восстановить дополнительные журналы транзакций из резервных копий в собственном формате Microsoft SQL и таким образом достичь нужной точки восстановления.

- **Только чтение (RESTORE WITH STANDBY)**

  После завершения восстановления база данных будет доступна пользователям только для чтения. Программа выполнит откат всех незафиксированных транзакций. Однако действия по откату будут сохранены во временный резервный файл, чтобы можно было вернуть базу данных в состояние до восстановления.

  Это значение в основном используется для определения точки во времени, где произошла ошибка SQL Server.

7. Щелкните **Запуск восстановления**.

Ход восстановления отображается на вкладке **Действия**.

/Восстановление баз данных SQL в виде файлов

1. Выполните одно из следующих действий:
   - При восстановлении из резервной копии с поддержкой приложений в пункте **Устройства** выберите машину, на которой изначально располагались данные, которые необходимо восстановить.
   - При восстановлении из резервной копии базы данных нажмите **Устройства** > **Microsoft SQL** и затем выберите базы данных, которые необходимо восстановить.
2. Щелкните **Восстановление**.
3. Выберите точку восстановления. Обратите внимание на то, что точки восстановления отфильтрованы по хранилищу.

   Если машина отключена, точки восстановления не отображаются. Выполните одно из следующих действий:
   - [Только при восстановлении из резервной копии с поддержкой приложений] Если резервная копия расположена в облачном хранилище или общем хранилище (т. е., другие агенты могут получить к ней доступ), нажмите **Выбрать машину**, выберите включенную машину, на которой установлен агент для SQL или агент для VMware, а затем выберите точку восстановления.
   - Выберите точку восстановления на вкладке «Резервные копии» (стр. 126).

   Машина, выбранная для обзора любым из двух вышеописанных действий, становится целевой машиной для восстановления баз данных SQL.
4. Выполните одно из следующих действий:
   - При восстановлении из резервной копии с поддержкой приложений нажмите **Восстановить** > **Базы данных SQL**, выберите базу данных, которую нужно восстановить, и затем нажмите **Восстановить как файлы**.
   - При восстановлении из резервной копии базы данных выберите **Восстановить** > **Базы данных как файлы**.
5. Нажмите **Обзор** и затем выберите локальную или сетевую папку, в которую требуется сохранить файлы.
6. Щелкните **Запуск восстановления**.

Ход восстановления отображается на вкладке **Действия**.

13.5.1 Восстановление системных баз данных

Все системные базы данных экземпляра восстанавливаются одновременно. При восстановлении системных баз программа автоматически перезапускает целевой экземпляр в однопользовательском режиме. После завершения восстановления программа перезапускает экземпляр и восстанавливает другие базы данных (если есть).

При восстановлении системной базы данных также обращайте внимание на перечисленные ниже моменты.

- Системные базы данных можно восстановить только на экземпляре той же версии, что и исходный.
- Системные базы данных всегда восстанавливаются в состоянии «готово к использованию».

Восстановление базы данных master

В число системных баз данных входит база **master**. В базе данных **master** содержатся сведения обо всех базах данных экземпляра. Это означает, что база данных **master** в резервной копии содержит информацию о базах данных, существовавших в экземпляре на момент резервного копирования. После восстановления базы данных **master** может потребоваться следующее.

- Базы данных, которые появились в экземпляре после выполнения резервного копирования, становятся невидимыми для экземпляра. Чтобы снова перевести их в режим эксплуатации, прикрепите их к экземпляру вручную с помощью SQL Server Management Studio.
- Базы данных, которые были удалены после выполнения резервного копирования, отображаются в экземпляре как находящиеся в автономном режиме. Удалите эти базы данных с помощью SQL Server Management Studio.

13.5.2 Подключение баз данных SQL Server

В этом разделе описывается процедура подключения базы данных в SQL Server с помощью среды SQL Server Management Studio. Одновременно может быть подключена только одна база данных.

Для подключения базы данных необходимо иметь любое из следующих разрешений: **CREATE DATABASE** (Создание базы данных), **CREATE ANY DATABASE** (Создание любой базы данных) или **ALTER ANY DATABASE**(Изменение любой базы данных). Обычно эти разрешения предоставляются роли **sysadmin** экземпляра.

Как подключить базу данных

1. Запустите среду Microsoft SQL Server Management Studio.
2. Подключитесь к требуемому экземпляру SQL Server и разверните его.
3. Щелкните правой кнопкой мыши пункт **Базы данных** и выберите **Подключить**.
4. Нажмите кнопку **Добавить**.
5. В диалоговом окне **Поиск файлов баз данных** найдите и выберите MDF-файл базы данных.
6. В разделе **Сведения о базе данных** убедитесь, что остальные файлы базы данных (NDB-файлы и LDF-файлы) также найдены.

   Подробнее. Файлы базы данных SQL Server могут быть не найдены автоматически, если:

   - Они находятся в расположении, отличном от расположения по умолчанию, или они не находятся в одной папке с основным файлом базы данных (MDF). Решение. Укажите путь к требуемым файлам вручную в столбце **Путь к текущему файлу**.

- Вы восстановили неполный набор файлов, составляющих базу данных. Решение. Восстановите отсутствующие файлы базы данных SQL Server из резервной копии.

7. Когда все файлы будут найдены, нажмите кнопку **ОК**.

13.6 Восстановление баз данных Exchange

В этом разделе описано восстановление из резервных копий базы данных и резервных копий с поддержкой приложений.

Можно восстановить данные Exchange Server в работающий Exchange Server. Это может быть исходный Exchange Server или Exchange Server той же версии, выполняющийся на машине с таким же полным доменным именем (FQDN). Агент для Exchange должен быть установлен на целевой машине.

В таблице ниже приведены основные сведения о том, какие именно данные Exchange Server можно выбрать для восстановления, а также о минимальных правах пользователя, которые для этого необходимы.

Версия Exchange	Элементы данных	Права пользователя
2007	Группы хранения	Участие в группе ролей **Администраторы организации Exchange**.
2010/2013/2016/2019	Базы данных	Участие в группе ролей **Управление сервером**.

Базы данных (группы хранения) также можно восстанавливать в виде файлов. Файлы баз данных и журналы транзакций извлекаются из резервной копии в указанную папку. Это может оказаться полезно, если необходимо извлечь данные для аудита или дальнейшей обработки средствами сторонних производителей либо в случае, когда выполнить восстановление по какой-либо причине не удается и требуется обходное решение для подключения баз данных вручную (стр. 149).

Если используется только агент для VMware (Windows), то единственный доступный метод восстановления — восстановить базы данных как файлы. Невозможно восстановить базы данных с помощью агента для VMware (виртуальное устройство).

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

/Для восстановления баз данных Exchange на запущенный сервер Exchange Server/

1. Выполните одно из следующих действий:
   - При восстановлении из резервной копии с поддержкой приложений в пункте **Устройства** выберите машину, на которой изначально располагались данные, которые необходимо восстановить.
   - При восстановлении из резервной копии базы данных нажмите **Устройства** > **Microsoft Exchange** > **Базы данных** и затем выберите базы данных, которые необходимо восстановить.
2. Щелкните **Восстановление**.
3. Выберите точку восстановления. Обратите внимание на то, что точки восстановления отфильтрованы по хранилищу.

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

- [Только при восстановлении из резервной копии с поддержкой приложений] Если резервная копия расположена в облачном хранилище или общем хранилище (т. е., другие агенты могут получить к ней доступ), нажмите **Выбрать машину**, выберите включенную машину, на которой установлен агент для Exchange, а затем выберите точку восстановления.
- Выберите точку восстановления на вкладке «Резервные копии» (стр. 126).

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

4. Выполните одно из следующих действий:
   - При восстановлении из резервной копии с поддержкой приложений нажмите **Восстановить** > **Базы данных Exchange**, выберите базу данных, которую нужно восстановить, и затем нажмите **Восстановить**.
   - При восстановлении из резервной копии базы данных выберите **Восстановить** > **Базы данных на сервер Exchange**.
5. По умолчанию данные восстанавливаются в исходных базах. Если исходная база данных не существует, она будет создана.

   Восстановление данных в другой базе
   a. Щелкните имя базы данных.
   b. В поле **Восстановить в** выберите вариант **Новая база данных**.
   c. Укажите имя новой базы данных.
   d. Укажите путь к новой базе данных и журналу. В указанной папке не должно быть файлов исходной базы данных и ее журналов.
6. Нажмите кнопку **Запуск восстановления**.

Ход восстановления отображается на вкладке **Действия**.

Восстановление баз данных Exchange в виде файлов

1. Выполните одно из следующих действий:
   - При восстановлении из резервной копии с поддержкой приложений в пункте **Устройства** выберите машину, на которой изначально располагались данные, которые необходимо восстановить.
   - При восстановлении из резервной копии базы данных нажмите **Устройства** > **Microsoft Exchange** > **Базы данных** и затем выберите базы данных, которые необходимо восстановить.
2. Щелкните **Восстановление**.
3. Выберите точку восстановления. Обратите внимание на то, что точки восстановления отфильтрованы по хранилищу.

   Если машина отключена, точки восстановления не отображаются. Выполните одно из следующих действий:
   - [Только при восстановлении из резервной копии с поддержкой приложений] Если резервная копия расположена в облачном хранилище или общем хранилище (т. е., другие агенты могут получить к ней доступ), нажмите **Выбрать машину**, выберите включенную машину, на которой установлен агент для Exchange или агент для VMware, а затем выберите точку восстановления.
   - Выберите точку восстановления на вкладке «Резервные копии» (стр. 126).

   Машина, выбранная для обзора любым из двух вышеописанных действий, становится целевой машиной для восстановления данных Exchange.
4. Выполните одно из следующих действий:

- При восстановлении из резервной копии с поддержкой приложений нажмите **Восстановить** > **Базы данных Exchange**, выберите базу данных, которую нужно восстановить, и затем нажмите **Восстановить как файлы**.
- При восстановлении из резервной копии базы данных выберите **Восстановить** > **Базы данных как файлы**.

5. Нажмите **Обзор** и затем выберите локальную или сетевую папку, в которую требуется сохранить файлы.
6. Щелкните **Запуск восстановления**.

Ход восстановления отображается на вкладке **Действия**.

13.6.1 Подключение баз данных Exchange Server

Восстановив файлы баз данных, можно перевести базы данных в оперативный режим, подключив их. Для подключения базы данных используйте консоль управления Exchange, диспетчер Exchange или командную консоль Exchange.

Восстановленная база данных будет в состоянии «грязного отключения». Если база данных находится в состоянии «грязного отключения», она может быть подключена системой, если была восстановлена в исходном расположении (т. е. сведения об исходной базе данных присутствуют 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, используемой для прикрепления базы данных, должна быть делегирована роль «Администратор сервера Exchange Server» и локальная группа «Администраторы» для целевого сервера.

Дополнительные сведения о подключении баз данных см. в следующих статьях:

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

13.7 Восстановление почтовых ящиков Exchange и элементов почтового ящика

В этом разделе описана процедура восстановления почтовых ящиков Exchange и элементов почтового ящика из резервных копий базы данных, резервных копий с поддержкой приложений и из резервных копий почтового ящика. Почтовые ящики или элементы почтового ящика могут быть восстановлены на запущенный Exchange Server или на Microsoft Office 365.

Можно восстановить следующие элементы:

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

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

Чтобы найти эти элементы, можно воспользоваться поиском.

Восстановление на Exchange Server

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

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

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

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

Требования к учетным записям пользователей

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

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

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

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

Восстановить в Office 365

Восстановление элементов данных Exchange в Office 365 и наоборот поддерживается в том случае, когда агент для Office 365 установлен локально.

Восстановление можно выполнить из резервных копий Microsoft Exchange Server 2010 и более поздней версии.

Если почтовый ящик восстанавливается в существующий почтовый ящик Office 365, существующие элементы не затрагиваются, а восстановленные элементы помещаются рядом с ними.

При восстановлении одного почтового ящика необходимо выбрать целевой ящик Office 365. При восстановлении нескольких почтовых ящиков в рамках одной операции восстановления программное обеспечение попытается восстановить каждый почтовый ящик в почтовый ящик пользователя с таким же именем. Если пользователь не найден, почтовый ящик пропускается.

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

Дополнительную информацию о восстановлении Office 365 см. в разделе «Защита почтовых ящиков Office 365» (стр. 159).

13.7.1 Восстановление почтовых ящиков

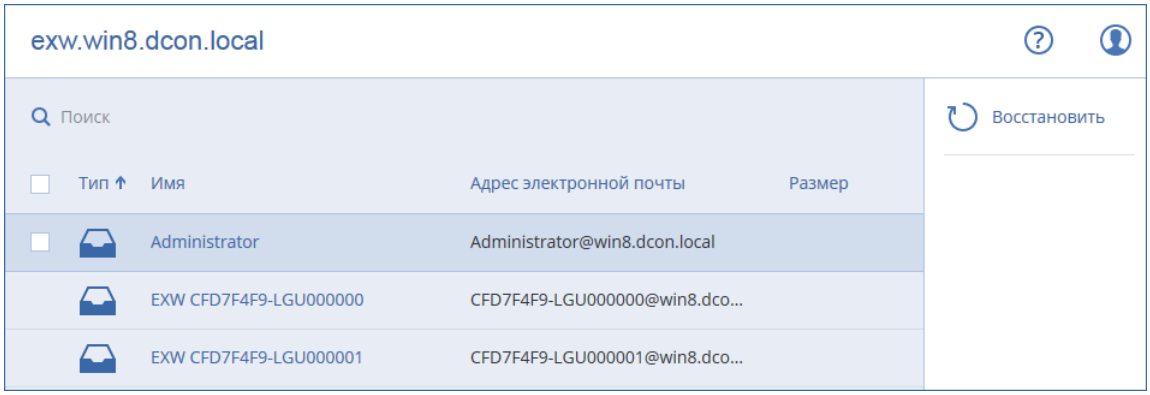
Порядок восстановления почтовых ящиков из резервной копии с поддержкой приложений или резервной копии базы данных

1. [Только при восстановлении из базы данных в Office 365] Если агент для Office 365 не установлен на машине с Exchange Server, резервная копия которой создается, выполните одно из указанных ниже действий:
   - Если в вашей организации нет агента для Office 365, установите агент для Office 365 на машине, для которой создана резервная копия, или на другой машине с такой же версией Microsoft Exchange Server.
   - Если в вашей организации уже есть агент для Office 365, скопируйте библиотеки с машины, для которой создана резервная копия, или с другой машины с такой же версией Microsoft Exchange Server на машину с агентом Office 365, как описано в разделе «Копирование библиотек Microsoft Exchange» (стр. 155).
2. Выполните одно из следующих действий:
   - При восстановлении из резервной копии с поддержкой приложений: в пункте **Устройства** выберите машину, на которой изначально располагались данные, которые необходимо восстановить.
   - При восстановлении из резервной копии базы данных нажмите **Устройства** > **Microsoft Exchange** > **Базы данных** и затем выберите базу данных, в которой изначально располагались данные, которые необходимо восстановить.
3. Щелкните **Восстановление**.
4. Выберите точку восстановления. Обратите внимание на то, что точки восстановления отфильтрованы по хранилищу.

   Если машина отключена, точки восстановления не отображаются. В этом случае воспользуйтесь одним из перечисленных ниже способов.
   - [Только при восстановлении из резервной копии с поддержкой приложений] Если резервная копия расположена в облачном хранилище или общем хранилище (т. е., другие агенты могут получить к ней доступ), нажмите **Выбрать машину**, выберите включенную машину, на которой установлен агент для Exchange или агент для VMware, а затем выберите точку восстановления.
   - Выберите точку восстановления на вкладке «Резервные копии» (стр. 126).

   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. [Только при восстановлении в Office 365]:
   a. В поле **Восстановить в** выберите пункт **Microsoft Office 365**.
   b. [Если в шаге 6 выбран только один почтовый ящик] В поле **Целевой почтовый ящик** укажите целевой почтовый ящик.
   c. Щелкните **Запуск восстановления**.

   Для этой процедуры не требуется никаких дополнительных шагов.
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 (FQDN) машины, на которой включена роль **Клиентский доступ** (в Microsoft Exchange Server 2010/2013) или **Роль почтовых ящиков** (в Microsoft Exchange Server 2016 или более поздних версиях). Эта машина должна принадлежать тому же лесу Active Directory, что и машина, которая выполняет восстановление.

   При поступлении соответствующего запроса укажите данные учетной записи, которая будет использоваться для доступа к компьютеру. Требования к этой учетной записи указаны в разделе «Требуемые права пользователя» (стр. 143).
10. [Необязательно] Чтобы изменить автоматически выбранную базу данных, щелкните **База данных для воссоздания отсутствующих почтовых ящиков**.
11. Щелкните **Запуск восстановления**.

Ход восстановления отображается на вкладке **Действия**.

Порядок восстановления почтового ящика из резервной копии почтового ящика

1. Нажмите **Устройства** > **Microsoft Exchange** > **Почтовые ящики**.
2. Выберите почтовый ящик для восстановления и щелкните **Восстановить**.

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

   Если почтовый ящик был удален, выберите его на вкладке Резервные копии (стр. 126) и щелкните **Показать резервные копии**.
3. Выберите точку восстановления. Обратите внимание на то, что точки восстановления отфильтрованы по хранилищу.
4. Последовательно выберите пункты **Восстановление** > **Почтовый ящик**.
5. Выполняйте шаги 8-11 вышеописанной процедуры.

13.7.2 Восстановление элементов почтовых ящиков

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

1. [Только при восстановлении из базы данных в Office 365] Если агент для Office 365 не установлен на машине с Exchange Server, резервная копия которой создается, выполните одно из указанных ниже действий:
   - Если в вашей организации нет агента для Office 365, установите агент для Office 365 на машине, для которой создана резервная копия, или на другой машине с такой же версией Microsoft Exchange Server.
   - Если в вашей организации уже есть агент для Office 365, скопируйте библиотеки с машины, для которой создана резервная копия, или с другой машины с такой же версией Microsoft Exchange Server на машину с агентом Office 365, как описано в разделе «Копирование библиотек Microsoft Exchange» (стр. 155).
2. Выполните одно из следующих действий:
   - При восстановлении из резервной копии с поддержкой приложений: в пункте **Устройства** выберите машину, на которой изначально располагались данные, которые необходимо восстановить.
   - При восстановлении из резервной копии базы данных нажмите **Устройства** > **Microsoft Exchange** > **Базы данных** и затем выберите базу данных, в которой изначально располагались данные, которые необходимо восстановить.
3. Щелкните **Восстановление**.
4. Выберите точку восстановления. Обратите внимание на то, что точки восстановления отфильтрованы по хранилищу.

   Если машина отключена, точки восстановления не отображаются. В этом случае воспользуйтесь одним из перечисленных ниже способов.
   - [Только при восстановлении из резервной копии с поддержкой приложений] Если резервная копия расположена в облачном хранилище или общем хранилище (т. е., другие агенты могут получить к ней доступ), нажмите **Выбрать машину**, выберите включенную машину, на которой установлен агент для Exchange или агент для VMware, а затем выберите точку восстановления.
   - Выберите точку восстановления на вкладке «Резервные копии» (стр. 126).

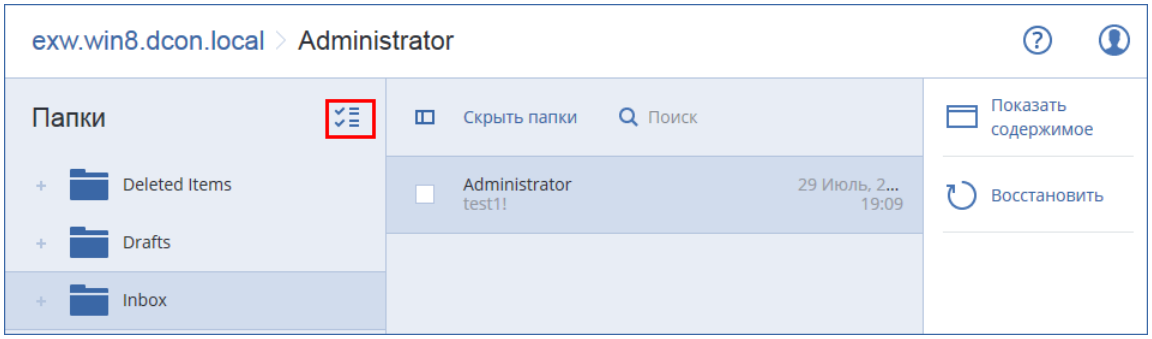
   Вместо выключенной исходной машины восстановление будет выполнено машиной, которая выбранная для просмотра одним из двух указанных выше действий.
5. Щелкните **Восстановление** > **Почтовые ящики Exchange**.
6. Щелкните почтовый ящик, в котором изначально содержались элементы, которые необходимо восстановить.
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 папки, щелкните значок восстановления папок.



8. Нажмите кнопку **Восстановить**.
9. Чтобы выполнить восстановление в Office 365, выберите **Microsoft Office 365** в поле **Восстановить в**.

   Чтобы выполнить восстановление на Exchange Server, сохраните значение по умолчанию **Microsoft Exchange** в поле **Восстановить в**.
10. [Только при восстановлении на Exchange Server] Чтобы выбрать или изменить целевую машину, щелкните **Целевая машина с Microsoft Exchange Server**. Это действие позволит восстановить машину, на которой не запущен агент для Exchange.

    Укажите полное доменное имя (FQDN) машины, на которой включена роль **Клиентский доступ** (в Microsoft Exchange Server 2010/2013) или **Роль почтовых ящиков** (в Microsoft Exchange Server 2016 или более поздних версиях). Эта машина должна принадлежать тому же лесу Active Directory, что и машина, которая выполняет восстановление.

    При поступлении соответствующего запроса укажите данные учетной записи, которая будет использоваться для доступа к компьютеру. Требования к этой учетной записи указаны в разделе «Требуемые права пользователя» (стр. 143).
11. Раздел **Целевой почтовый ящик** позволяет просмотреть, изменить или указать целевой почтовый ящик.

    По умолчанию выбран исходный почтовый ящик. Если этот почтовый ящик не существует или выбрана целевая машина, которая не является исходной, необходимо указать целевой почтовый ящик.
12. [Только при восстановлении сообщений электронной почты] В поле **Целевая папка** просмотрите или измените целевую папку в целевом почтовом ящике. По умолчанию выбрана папка **Восстановленные элементы**.
13. Щелкните **Запуск восстановления**.

Ход восстановления отображается на вкладке **Действия**.

Порядок восстановления элемента почтового ящика из резервной копии почтового ящика

1. Нажмите **Устройства** > **Microsoft Exchange** > **Почтовые ящики**.
2. Выберите почтовый ящик, в котором изначально содержались элементы, которые необходимо восстановить, и нажмите кнопку **Восстановить**.

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

Если почтовый ящик был удален, выберите его на вкладке Резервные копии (стр. 126) и щелкните **Показать резервные копии**.

3. Выберите точку восстановления. Обратите внимание на то, что точки восстановления отфильтрованы по хранилищу.
4. Последовательно выберите пункты **Восстановление** > **Сообщения электронной почты**.
5. Выберите элементы, которые необходимо восстановить.

   Доступны указанные ниже параметры поиска. Подстановочные символы не поддерживаются.

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

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

   Совет *Чтобы загрузить вложенный файл, щелкните его имя.*

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

   Чтобы иметь возможность выбрать папки, щелкните значок восстановления папок: 
6. Нажмите кнопку **Восстановить**.
7. Выполните шаги 9–13 вышеописанной процедуры.

13.7.3 Копирование библиотек Microsoft Exchange Server

При восстановлении почтовых ящиков Exchange или элементов почтовых ящиков в Office 365 (стр. 149), возможно, необходимо будет скопировать указанные ниже библиотеки с машины, для которой создана резервная копия, или с другой машины с такой же версией Microsoft Exchange Server на машину с агентом для Office 365.

Скопируйте указанные ниже файлы в соответствии с версией Microsoft Exchange Server, для которой создана резервная копия.

Версия Microsoft Exchange Server	**Ленточные библиотеки**	**Хранилище по умолчанию**
Microsoft Exchange Server 2010	ese.dll esebcli2.dll store.exe	%ProgramFiles%\Microsoft\Exchange Server\V14\bin
Microsoft Exchange Server 2013	ese.dll	%ProgramFiles%\Microsoft\Exchange Server\V15\bin
	msvcr110.dll	%WINDIR%\system32
Microsoft Exchange Server 2016, 2019	ese.dll	%ProgramFiles%\Microsoft\Exchange Server\V15\bin

	msvcr110.dll msvcp110.dll	%WINDIR%\system32

Библиотеки необходимо поместить в папку **%ProgramData%\Acronis\ese**. Если папка не существует, создайте ее вручную.

13.8 Изменение учетных данных для доступа к SQL Server или Exchange Server.

Можно изменить учетные данные для доступа к SQL Server или Exchange Server без переустановки агента.

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

1. Щелкните **Устройства**, а затем щелкните **Microsoft SQL** или **Microsoft Exchange**.
2. Выберите группу обеспечения доступности Always On, группу обеспечения доступности баз данных, экземпляр SQL Server или Exchange Server, для которых необходимо изменить учетные данные.
3. Щелкните **Укажите учетные данные**
4. Укажите новые учетные данные доступа, а затем нажмите кнопку **ОК**.

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

1. Щелкните **Устройства** > **Microsoft Exchange** и разверните узел **Почтовые ящики**.
2. Выберите Microsoft Exchange для которого необходимо изменить учетные данные для доступа.
3. Щелкните **Настройки**.
4. Ниже поля **Учетная запись администратора Exchange** укажите новые учетные данные для доступа, а затем щелкните **Сохранить**.

14 Защита мобильных устройств

Приложение резервного копирования позволяет выполнять резервное копирование мобильных данных в облачное хранилище данных, а затем восстанавливать их при утрате или повреждении. Обратите внимание, что для резервного копирования в облачное хранилище данных требуется учетная запись и подписка для облачного хранилища данных.

Поддерживаемые мобильные устройства

Приложение резервного копирования можно установить на мобильном устройстве с одной из следующих операционных систем:

- iOS 10.3 или более поздней версии (устройства iPhone, iPod и iPad)
- Android 5.0 или более поздней версии

Данные, для которых можно создать резервную копию

- Контакты
- Фотографии
- Видео
- Календари

- 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 запустить резервное копирование вручную.
- Функция **Непрерывное резервное копирование** включена по умолчанию. Если она включена:
  - Для Android 7.0 или более поздней версии приложение резервного копирования автоматически («на лету») определяет новые данные и передает их в облако.
  - Для Android 5 и 6 наличие изменений проверяется каждые три часа. Непрерывное резервное копирование можно отключить в настройках приложения.
- Параметр **Использовать только Wi-Fi** по умолчанию включен в настройках программы. Если эта настройка включена, приложение резервного копирования создает резервную копию ваших данных, только когда доступно подключение к сети Wi-Fi. При отсутствии подключения к сети Wi-Fi процесс резервного копирования не запускается. Чтобы приложение использовало подключение к мобильной сети, отключите этот параметр.
- Есть два способа снизить энергопотребление:
  - Использовать функцию **Адаптивное энергопотребление** (отключена по умолчанию). Если эта настройка включена, приложение резервного копирования создает резервную копию ваших данных, только когда устройство подключено в источнику питания. Если при выполнении непрерывного резервного копирования устройство отключается от источника питания, резервное копирование останавливается.
  - Использовать функцию **Режим экономии энергии** (включена по умолчанию). Если эта настройка включена, приложение резервного копирования создает резервную копию ваших данных только при достаточном уровне заряда аккумулятора. Когда уровень заряда аккумулятора становится низким, непрерывное резервное копирование останавливается. Этот параметр доступен для Android 8 или более поздней версии.
- 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, консоль резервного копирования позволяет загрузить фотографии, видео или контакты на любое устройство.
- 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.
- Приложение резервного копирования позволяет восстановить данные только с новейших версий резервных копий. Если необходимо выполнить восстановление с других версий резервный копий, используйте консоль резервного копирования на планшетном ПК или компьютере.
- Правила хранения не применяются к резервным копиям мобильных устройств.
- [Только для устройств Android] При наличии SD-карты в ходе выполнения резервного копирования хранящиеся на ней данные также будут скопированы. Эти данные будут восстановлены на SD-карту в папку **Recovered by Backup**, если она будет доступна при восстановлении. В противном случае приложение потребует указать другое расположение для восстановления данных.

Где получить приложение резервного копирования?

В зависимости от используемого мобильного устройства установите приложение с App Store или Google Play.

Запуск резервного копирования данных

1. Откройте приложение.
2. Войдите с помощью учетной записи.
3. Коснитесь **Настроить**, чтобы создать резервную копию. Обратите внимание, что эта кнопка доступна только в том случае, если на мобильном устройстве нет резервной копии.
4. Выберите категории данных, резервную копию которых необходимо создать. По умолчанию выбраны все категории.
5. [Необязательно] Чтобы защитить свою резервную копию шифрованием, включите **Шифровать резервную копию**. В этом случае необходимо будет выполнить следующие действия:
    1. Дважды введите пароль шифрования.

       Вы должны запомнить пароль, поскольку забытый пароль невозможно ни восстановить, ни изменить.

    1. Коснитесь значка **Зашифровать**.
1. Коснитесь значка **Создать резервную копию**.
2. 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.

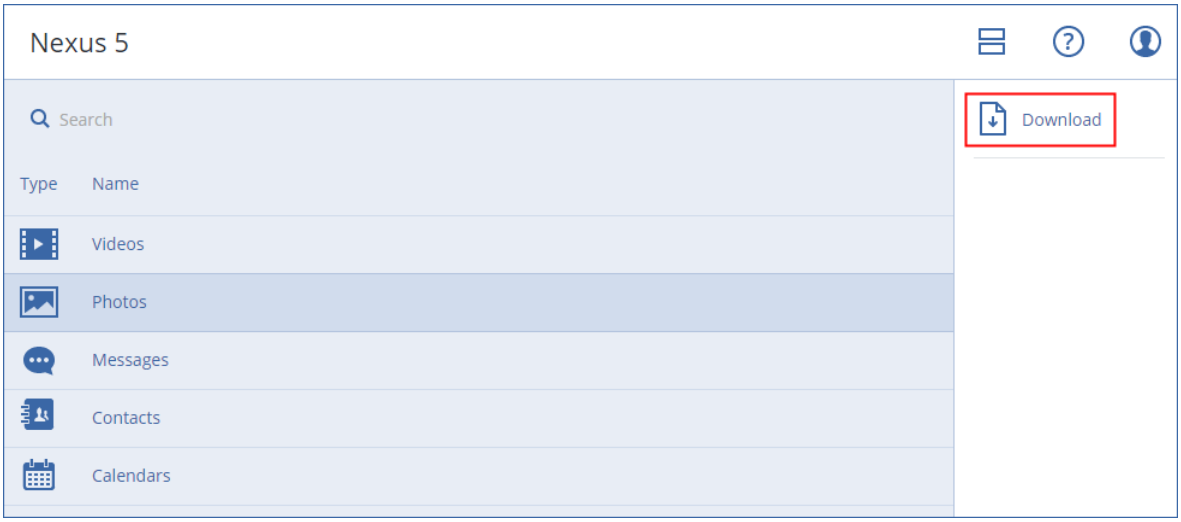
Порядок восстановления данных на мобильное устройство

1. Откройте приложение резервного копирования.
2. Коснитесь значка **Обзор**.
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**.

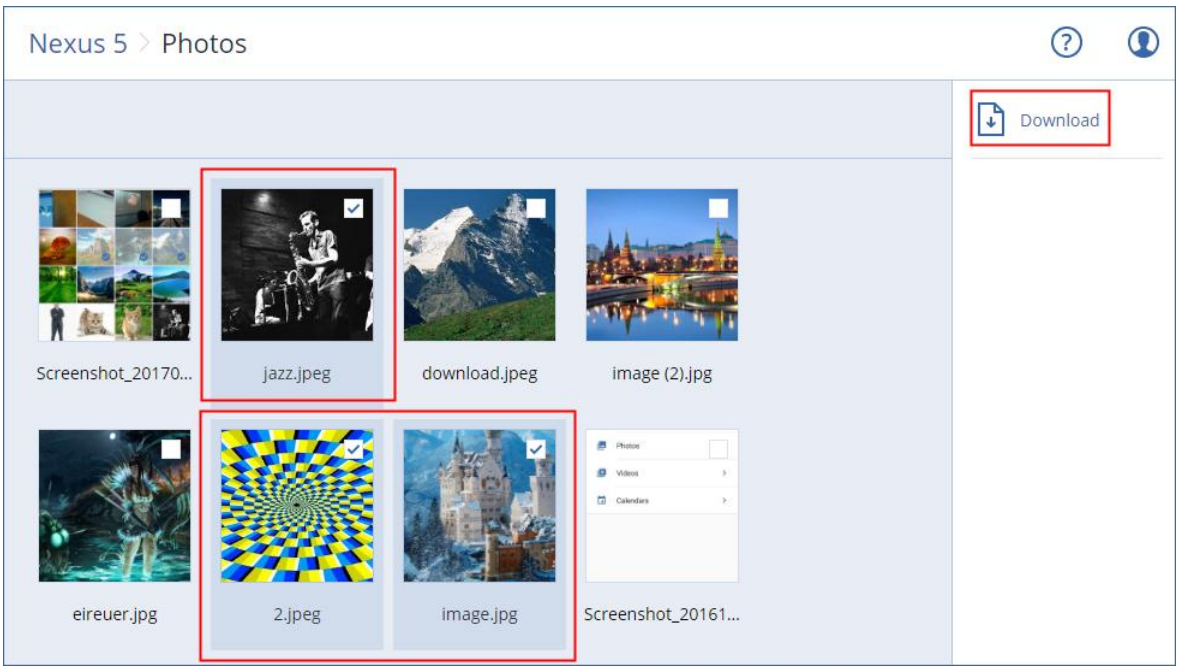
Проверка данных через консоль резервного копирования

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

3. В разделе **Все устройства** под именем мобильного устройства щелкните **Восстановить**.
4. Выполните любое из следующих действий:
   - Чтобы загрузить все фотографии, видео, контакты, календари или напоминания, выберите соответствующую категорию данных. Нажмите кнопку **Загрузить**.



   - Чтобы загрузить отдельные фотографии, видео, контакты, календари или напоминания, 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.

15 Защита данных Office 365

Зачем выполнять резервное копирование данных Office 365?

Несмотря на то, что Microsoft Office 365 — это набор облачных сервисов, регулярное создание резервных копий обеспечит дополнительную защиту 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 Exchange Online, если это необходимо для соблюдения нормативных требований.

Агент для Office 365

В зависимости того, какие функции вам нужны, можно установить агент для Office 365 локально и (или) использовать агент, установленный в облаке. В следующей таблице представлена сводная информация о функциональности локального и облачного агента.

	Локальный агент для Office 365	**Облачный агент для Office 365**
Элементы данных, для которых можно создать резервную копию	**Exchange Online**: почтовые ящики пользователя и общие почтовые ящики	▪ **Exchange Online**: почтовые ящики пользователя, общие почтовые ящики и почтовые ящики группы, а также общие папки ▪ **OneDrive**: файлы и папки пользователя ▪ **SharePoint Online**: семейства классических веб-сайтов, сайты группы (рабочей группы), информационные сайты, отдельные элементы данных
Резервное копирование архивных почтовых ящиков (**архив на месте**).	No	Да
Расписание резервного копирования	Определено пользователем (стр. 54)	Невозможно изменить. Каждый план резервного копирования запускается ежедневно в одно и то же время.*
Хранилища резервных копий	Облачное хранилище данных, локальная или сетевая папка	Только облачное хранилище данных
Автоматическая защита новых пользователей, групп и сайтов Office 365	No	Да, за счет применения плана резервного копирования к группам **Все пользователи**, **Все группы** и **Все сайты**
Защита нескольких организаций Office 365	No	Yes
Фрагментарное восстановление	Yes	Yes
Восстановление в расположение другого пользователя в одной организации	Yes	Yes
Восстановление в расположение другой организации	No	Yes

	Локальный агент для Office 365	Облачный агент для Office 365
Восстановление на локальный Microsoft Exchange Server	No	No
Максимальное количество элементов для резервного копирования без снижения производительности	При выполнении резервного копирования в облачное хранилище данных: 5000 почтовых ящиков на компанию При выполнении резервного копирование в другие целевые места: 2000 почтовых ящиков на один план резервного копирования (без ограничений на количество почтовых ящиков для одной компании)	5000 защищенных элементов (почтовые ящики, хранилища OneDrive или сайты) для одной компании
Максимальное количество ручных запусков резервного копирования	No	10 ручных запусков резервного копирования в час (стр. 131)
Максимальное количество одновременных операций восстановления	No	10 операций, включая операции восстановления G Suite

* Поскольку облачным агентом пользуются многие клиенты, он автоматически выбирает время запуска каждого плана резервного копирования таким образом, чтобы обеспечить равномерную нагрузку в течение дня и одинаковое качество обслуживания для всех клиентов.

Ограничение

Автоматическое создание пользователей, общих папок, групп или сайтов невозможно во время восстановления. Пример: чтобы восстановить удаленный сайт SharePoint Online, сначала создайте новый сайт вручную, затем укажите его как целевой сайт при восстановлении.

Требуемые права пользователя

В сервисе резервного копирования

Любой агент для Office 365, локальный или облачный, необходимо зарегистрировать в учетной записи администратора пользователя. Администраторы и пользователи отдела не могут создавать резервные копии данных Office 365 или восстанавливать их.

В Microsoft Office 365

Вашей учетной записи должна быть назначена роль глобального администратора в Microsoft Office 365.

- Локальный агент войдет в Office 365 с этой учетной записью. Чтобы обеспечить доступ агента к содержимому всех почтовых ящиков, этой учетной записи будет назначена роль управления **ApplicationImpersonation**. Если вы изменили пароль учетной записи, обновите его в консоли резервного копирования, как описано в разделе «Изменение учетных данных для доступа к Office 365» (стр. 164).
- Облачный агент не входит в Office 365. Агенту предоставляются необходимые разрешения непосредственно от Microsoft Office 365. Подтвердить предоставление этих разрешений необходимо только один раз с учетными данными глобального администратора. Агент не хранит учетные данные вашей учетной записи и не использует их для резервного копирования и восстановления. Изменение пароля учетной записи в Office 365 не влияет на работу агента.

15.1 Использование локального агента для Office 365

15.1.1 Добавление организации Microsoft Office 365

Порядок добавления организации Microsoft Office 365

1. Войдите на консоль резервного копирования с учетной записью администратора компании.
2. Щелкните значок учетной записи в правом верхнем углу, а затем выберите пункты **Загрузки** > **Агент для Office 365**.
3. Загрузите агент и установите его на машину Windows, которая подключена к Интернету.
4. 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 локальный агент для Office 365.*

После этого элементы данных вашей организации появятся на консоли резервного копирования на странице **Microsoft Office 365**.

15.1.2 Защита почтовых ящиков Exchange Online

Для каких элементов можно создавать резервные копии?

Можно создать резервную копию почтовых ящиков пользователя и общих почтовых ящиков. Невозможно создать резервную копию почтовых ящиков группы и архивных почтовых ящиков (**архив на месте**).

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. Вместо этого в целевой папке заново создается полный путь к элементу почтового ящика.

15.1.2.1 Выбор почтовых ящиков

Выберите почтовый ящики, как указано ниже, а затем укажите другие настройки плана резервного копирования как требуется (стр. 42).

Порядок выбора почтовых ящиков

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**.

15.1.2.2 Восстановление почтовых ящиков и элементов почтовых ящиков

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. 126) 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**.

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. 126) 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.

15.1.2.3 Изменение учетных данных для доступа к Office 365

Можно изменить учетные данные для доступа к Office 365 без переустановки агента.

Для изменения учетных данных для доступа к Office 365

1. Щелкните **Устройства** > **Microsoft Office 365**.
2. Щелкните **Укажите учетные данные**
3. Введите учетные данные глобального администратора Office 365 и нажмите кнопку **ОК**.

   Агент будет входить в Office 365, используя эту учетную запись. Чтобы обеспечить доступ агента к содержимому всех почтовых ящиков, этой учетной записи будет назначена роль управления **ApplicationImpersonation**.

15.2 Использование облачного агента для Office 365

15.2.1 Добавление организации Microsoft Office 365

Порядок добавления организации Microsoft Office 365

1. Войдите на консоль резервного копирования с учетной записью администратора компании.
2. Последовательно выберите пункты **Устройства** > **Добавить** > **Microsoft Office 365 for Business**.
3. Выберите центр обработки данных Microsoft, используемый вашей организацией.

   Программа перенаправит вас на страницу входа Microsoft Office 365.
4. Войдите с учетными данными глобального администратора Office 365.

   В Microsoft Office 365 отображается список разрешений, которые необходимы для резервного копирования и восстановления данных вашей организации.
5. Подтвердите, что предоставили службе резервного копирования эти разрешения.

После этого элементы данных вашей организации появятся на консоли резервного копирования на странице **Microsoft Office 365**.

Советы по дальнейшему использованию

- Облачный агент синхронизируется с Office 365 каждые 24 часа после добавления организации в сервис резервного копирования. После добавления или удаления пользователя, группы или сайта соответствующие изменения отображаются на консоли резервного копирования через некоторое время. Чтобы принудительно синхронизировать облачный агент с Office 365, выберите организацию на странице **Microsoft Office 365** и щелкните **Обновить**.
- Если к группе **Все пользователи**, **Все группы** или **Все сайты** применен план резервного копирования, новые добавленные элементы включаются в состав резервной копии только после синхронизации.
- В соответствии с политикой корпорации Microsoft после удаления пользователя, группы или сайта из графического интерфейса пользователя Office 365 они остаются доступными в течение нескольких дней через API. В течение этого периода удаленный элемент будет неактивным (серым) на консоли резервного копирования, а резервное копирование этого элемента выполняться не будет. Когда удаленный элемент станет недоступным через API, он исчезнет с консоли резервного копирования. Чтобы получить доступ к его резервным копиям (при наличии), последовательно выберите пункты **Резервные копии** > **Резервные копии приложений в облаке**.

15.2.2 Защита данных Exchange Online

Для каких элементов можно создавать резервные копии?

Можно создать резервную копию почтовых ящиков пользователя, общих почтовых ящиков и почтовых ящиков группы. При необходимости можно выбрать резервное копирование архивных почтовых ящиков (**архив на месте**) для выбранных почтовых ящиков.

Сервис резервного копирования, начиная с версии 8.0, позволяет создавать резервные копии общих папок. Если ваша организация была добавлена в сервис резервного копирования до выпуска версии 8.0, то для получения этой функциональности необходимо будет заново добавить организацию. Не удаляйте организацию, просто повторите действия, описанные в теме «Добавление организации Microsoft Office 365» (стр. 164). В результате сервис резервного копирования получит разрешения на использование соответствующего API.

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

Указанные ниже элементы можно восстановить с резервной копии общей папки:

- Подпапки

- Публикации
- сообщения электронной почты;

Чтобы найти эти элементы, можно воспользоваться поиском.

При восстановлении почтовых ящиков, элементов почтовых ящиков, общих папок и элементов общих папок можно выбрать, перезаписывать ли элементы в целевое расположение.

15.2.2.1 Выбор почтовых ящиков

Выберите почтовый ящики, как указано ниже, а затем укажите другие настройки плана резервного копирования как требуется (стр. 42).

Порядок выбора почтовых ящиков Exchange Online

1. Щелкните **Microsoft Office 365**.
2. Если в сервис резервного копирования добавлено несколько организаций Office 365, выберите ту организацию, для пользователей которой необходимо создать резервные копии их данных. В противном случае пропустите этот шаг.
3. Выполните одно из следующих действий:
   - Чтобы создать резервную копию почтовых ящиков всех пользователей и всех общих почтовых ящиков (включая почтовые ящики, которые будут созданы в будущем), разверните узел **Пользователи**, выберите **Все пользователи** и щелкните **Групповое резервное копирование**.
   - Чтобы создать резервную копию почтовых ящиков отдельных пользователей или общих почтовых ящиков, разверните узел **Пользователи**, выберите **Все пользователи**, затем выберите пользователей, для почтовых ящиков которых необходимо создать резервные копии, и щелкните **Резервное копирование**.
   - Чтобы создать резервную копию почтовых ящиков всех групп (включая почтовые ящики групп, которые будут созданы в будущем), разверните узел **Группы**, выберите **Все группы** и щелкните **Групповое резервное копирование**.
   - Чтобы создать резервную копию почтовых ящиков отдельных групп, разверните узел **Группы**, выберите **Все группы**, затем выберите группы, для почтовых ящиков которых необходимо создать резервные копии, и щелкните **Резервное копирование**.
4. На панели плана резервного копирования:
   - Убедитесь, что в области **Выбор данных** выбран элемент **Почтовые ящики Office 365**.
   - Если вы не хотите создавать резервную копию архивных почтовых ящиков, деактивируйте переключатель **Почтовый ящик архива**.

15.2.2.2 Выбор общих папок

Выберите общие папки, как описано ниже, а затем укажите другие настройки плана резервного копирования должным образом (стр. 42).

Порядок выбора общедоступных папок Exchange Online

1. Щелкните **Microsoft Office 365**.
2. Если в сервис резервного копирования добавлено несколько организаций Office 365, разверните ту организацию, для пользователей которой необходимо создать резервные копии их данных. В противном случае пропустите этот шаг.
3. Разверните узел **Общие папки**, а затем выберите **Все общие папки**.
4. Выполните одно из следующих действий:

- Чтобы создать резервную копию всех общих папок (включая общие папки, которые будут созданы в будущем), щелкните **Групповое резервное копирование**.
- Чтобы создать резервную копию для отдельных общедоступных папок, выберите их и щелкните **Резервное копирование**.

5. Убедитесь, что на панели плана резервного копирования в области **Выбор данных** выбран элемент **Почтовые ящики Office 365**.

15.2.2.3 Восстановление почтовых ящиков и элементов почтовых ящиков

Восстановление почтовых ящиков

1. Щелкните **Microsoft Office 365**.
2. Если в сервис резервного копирования добавлено несколько организаций Office 365, выберите ту организацию, данные которой необходимо восстановить из резервной копии. В противном случае пропустите этот шаг.
3. Выполните одно из следующих действий:
   - Чтобы восстановить почтовый ящик пользователя, разверните узел **Пользователи**, выберите **Все пользователи**, затем выберите пользователя, почтовый ящик которого необходимо восстановить, и щелкните **Восстановить**.
   - Чтобы восстановить общий почтовый ящик, разверните узел **Пользователи**, выберите **Все пользователи**, затем выберите общий почтовый ящик, который необходимо восстановить, и щелкните **Восстановить**.
   - Чтобы восстановить почтовый ящик группы, разверните узел **Группы**, выберите **Все группы**, затем выберите группу, почтовый ящик которой необходимо восстановить, и щелкните **Восстановить**.
   - Если пользователь, группа или общий почтовый ящик удалены, выберите элемент в разделе **Резервные копии приложений в облаке** на вкладке Резервные копии (стр. 126) и щелкните **Показать резервные копии**.

   Можно выполнить поиск по имени пользователей и групп. Подстановочные символы не поддерживаются.
4. Выберите точку восстановления.

   Подсказка. *Чтобы просмотреть только те точки восстановления, которые содержат почтовые ящики, в поле* ***Фильтровать по содержимому*** *выберите пункт* ***Почтовые ящики****.*
5. Последовательно выберите пункты **Восстановить** > **Весь почтовый ящик**.
6. Если в сервис резервного копирования добавлено несколько организаций Office 365, щелкните **Организация Office 365** для просмотра, изменения или указания целевой организации.

   По умолчанию выбрана исходная организация. Если эта организация больше не зарегистрирована в сервисе резервного копирования, необходимо указать целевую организацию.
7. Раздел **Восстановить в почтовый ящик** позволяет просматривать, изменять или указывать целевой почтовый ящик.

   По умолчанию выбран исходный почтовый ящик. Если этот почтовый ящик не существует или выбрана организация, которая не является исходной, необходимо указать целевой почтовый ящик.
8. Щелкните **Запуск восстановления**.

9. Выберите один из вариантов перезаписи:
   - **Перезаписывать существующие элементы**
   - **Не перезаписывать существующие элементы**
10. Щелкните **Продолжить**, чтобы подтвердить решение.

Восстановление элементов почтовых ящиков

1. Щелкните **Microsoft Office 365**.
2. Если в сервис резервного копирования добавлено несколько организаций Office 365, выберите ту организацию, данные которой необходимо восстановить из резервной копии. В противном случае пропустите этот шаг.
3. Выполните одно из следующих действий:
   - Чтобы восстановить элементы с почтового ящика пользователя, разверните узел **Пользователи**, выберите **Все пользователи**, затем выберите пользователя, почтовый ящик которого изначально содержал элементы для восстановления, и щелкните **Восстановить**.
   - Чтобы восстановить элементы из общего почтового ящика, разверните узел **Пользователи**, выберите **Все пользователи**, затем выберите общий почтовый ящик, который изначально содержал элементы для восстановления, и щелкните **Восстановить**.
   - Чтобы восстановить элементы с почтового ящика группы, разверните узел **Группы**, выберите **Все группы**, затем выберите группу, в почтовом ящике которой изначально содержались элементы для восстановления, и щелкните **Восстановить**.
   - Если пользователь, группа или общий почтовый ящик удалены, выберите элемент в разделе **Резервные копии приложений в облаке** на вкладке Резервные копии (стр. 126) и щелкните **Показать резервные копии**.

   Можно выполнить поиск по имени пользователей и групп. Подстановочные символы не поддерживаются.
4. Выберите точку восстановления.

   Подсказка. *Чтобы просмотреть только те точки восстановления, которые содержат почтовые ящики, в поле* ***Фильтровать по содержимому*** *выберите пункт* ***Почтовые ящики****.*
5. Последовательно выберите пункты **Восстановление** > **Сообщения электронной почты**.
6. Перейдите к нужной папке или используйте поиск для получения списка нужных элементов.

   Доступны указанные ниже параметры поиска. Подстановочные символы не поддерживаются.
   - Для сообщений электронной почты: выполните поиск по теме, отправителю, получателю и дате.
   - Для событий: выполните поиск по заголовку и дате.
   - Для задач: выполните поиск по теме и дате.
   - Для контактов: выполните поиск по имени, адресу электронной почты и номеру телефона.
7. Выберите элементы, которые необходимо восстановить. Чтобы иметь возможность выбрать папки, щелкните значок восстановления папок: 

   Кроме того, можно выполнить любое из следующих действий:

- Чтобы просмотреть содержимое выбранного элемента вместе с вложениями, щелкните **Показать содержимое**. Чтобы загрузить вложенный файл, щелкните его имя.
- После выбора сообщения электронной почты или календаря щелкните **Отправить как сообщение электронной почты**, чтобы отправить элемент по указанному адресу электронной почты. Можно выбрать отправителя и записать текст, который будет добавлен к пересылаемому элементу.
- Только в том случае, если вы выполнили поиск в незашифрованной резервной копии и выбрали один элемент в результатах поиска, можно щелкнуть **Показать версии**, чтобы выбрать версию элемента для восстановления. Можно выбрать любую версию в резервной копии, датированную до или после точки восстановления.

8. Нажмите кнопку **Восстановить**.
9. Если в сервис резервного копирования добавлено несколько организаций Office 365, щелкните **Организация Office 365** для просмотра, изменения или указания целевой организации.

   По умолчанию выбрана исходная организация. Если эта организация больше не зарегистрирована в сервисе резервного копирования, необходимо указать целевую организацию.
10. Раздел **Восстановить в почтовый ящик** позволяет просматривать, изменять или указывать целевой почтовый ящик.

    По умолчанию выбран исходный почтовый ящик. Если этот почтовый ящик не существует или выбрана организация, которая не является исходной, необходимо указать целевой почтовый ящик.
11. [Только при восстановлении в почтовый ящик пользователя или общий почтовый ящик] В поле **Путь** просмотрите или измените целевую папку в целевом почтовом ящике. По умолчанию выбрана папка **Восстановленные элементы**.

    Элементы почтового ящика группы всегда восстанавливаются в папку **Входящие**.
12. Щелкните **Запуск восстановления**.
13. Выберите один из вариантов перезаписи:
    - **Перезаписывать существующие элементы**
    - **Не перезаписывать существующие элементы**
14. Щелкните **Продолжить**, чтобы подтвердить решение.

15.2.2.4 Восстановление общедоступных папок и элементов папок

Для восстановления общедоступной папки и элементов общедоступной папки хотя бы один администратор целевой организации Office 365 должен иметь права **Владелец** для целевой общей папки. Если не удается выполнить восстановление по причине отказа в доступе, назначьте эти права в свойствах целевой папки, выберите целевую организацию на консоли резервного копирования, щелкните **Обновить** и повторите попытку восстановления.

Порядок восстановления общедоступной папки или элементов папок

1. Щелкните **Microsoft Office 365**.
2. Если в сервис резервного копирования добавлено несколько организаций Office 365, разверните ту организацию, данные которой необходимо восстановить из резервной копии. В противном случае пропустите этот шаг.
3. Выполните одно из следующих действий:

- Разверните узел **Общие папки**, выберите **Все общие папки**, затем выберите общую папку для восстановления или ту общую папку, которая изначально содержала элементы для восстановления, и щелкните **Восстановить**.
- Если общедоступная папка удалена, выберите его в разделе **Резервные копии приложений в облаке** на вкладке Резервные копии (стр. 126) и щелкните **Показать резервные копии**.

Общие папки можно найти по имени. Подстановочные символы не поддерживаются.

4. Выберите точку восстановления.
5. Щелкните **Восстановить данные**.
6. Перейдите к нужной папке или используйте поиск для получения списка нужных элементов.

   Сообщения электронной почты и публикации можно искать по теме, отправителю, получателю и дате. Подстановочные символы не поддерживаются.
7. Выберите элементы, которые необходимо восстановить. Чтобы иметь возможность выбрать папки, щелкните значок восстановления папок: 

   Кроме того, можно выполнить любое из следующих действий:
   - Чтобы просмотреть содержимое выбранного сообщения электронной почты или записи с вложениями, щелкните **Показать содержимое**. Чтобы загрузить вложенный файл, щелкните его имя.
   - После выбора сообщения электронной почты или публикации щелкните **Отправить как сообщение электронной почты**, чтобы отправить элемент по указанному адресу электронной почты. Можно выбрать отправителя и записать текст, который будет добавлен к пересылаемому элементу.
   - Только в том случае, если вы выполнили поиск в незашифрованной резервной копии и выбрали один элемент в результатах поиска, можно щелкнуть **Показать версии**, чтобы выбрать версию элемента для восстановления. Можно выбрать любую версию в резервной копии, датированную до или после точки восстановления.
8. Нажмите кнопку **Восстановить**.
9. Если в сервис резервного копирования добавлено несколько организаций Office 365, щелкните **Организация Office 365** для просмотра, изменения или указания целевой организации.

   По умолчанию выбрана исходная организация. Если эта организация больше не зарегистрирована в сервисе резервного копирования, необходимо указать целевую организацию.
10. В разделе **Восстановить в общую папку** можно просмотреть, изменить или указать целевую общую папку.

    По умолчанию выбрана исходная папка. Если эта папка не существует или выбрана организация, которая не является исходной, необходимо указать целевую папку.
11. В поле **Путь** просмотрите или измените целевую подпапку в целевой общей папке. По умолчанию исходный путь будет выбран заново.
12. Щелкните **Запуск восстановления**.
13. Выберите один из вариантов перезаписи:
    - **Перезаписывать существующие элементы**
    - **Не перезаписывать существующие элементы**
14. Щелкните **Продолжить**, чтобы подтвердить решение.

15.2.3 Защита файлов OneDrive

Для каких элементов можно создавать резервные копии?

Можно создать резервную копию всего хранилища OneDrive или отдельных файлов и папок.

Для файлов создается резервная копия вместе с их разрешениями общего доступа. При этом расширенные уровни разрешения (**Разработка**, **Полные**, **Участие**) не включаются в резервную копию.

Какие элементы можно восстановить?

Можно восстановить все хранилище OneDrive или любые файлы и папки, для которых созданы резервные копии.

Чтобы найти эти элементы, можно воспользоваться поиском.

Можно выбрать восстановление разрешений предоставления общего доступа или наследование файлами их разрешений из папки, в которую они восстанавливаются.

Ссылки на общий доступ к файлам и папкам не восстанавливаются.

15.2.3.1 Выбор файлов OneDrive

Выберите файлы, как описано ниже, а затем укажите другие настройки плана резервного копирования должным образом (стр. 42).

Порядок выбора файлов OneDrive

1. Щелкните **Microsoft Office 365**.
2. Если в сервис резервного копирования добавлено несколько организаций Office 365, выберите ту организацию, для пользователей которой необходимо создать резервные копии их данных. В противном случае пропустите этот шаг.
3. Выполните одно из следующих действий:
   - Чтобы создать резервную копию файлов всех пользователей (включая пользователей, которые будут созданы в будущем), разверните узел **Пользователи**, выберите **Все пользователи** и щелкните **Групповое резервное копирование**.
   - Чтобы создать резервную копию файлов отдельных пользователей, разверните узел **Пользователи**, выберите **Все пользователи**, затем выберите пользователей, для файлов которых необходимо создать резервные копии, и щелкните **Резервное копирование**.
4. На панели плана резервного копирования:
   - Убедитесь, что в области **Выбор данных** выбран элемент **OneDrive**.
   - В элементе управления **Элементы для резервного копирования** выполните одно из указанных ниже действий:
     - Не маняйте настройку по умолчанию **[Все]** (все файлы).
     - Укажите файлы и папки для резервного копирования, добавив их имена или пути.

       Можно использовать подстановочные символы (*, ** и ?). Подробную информацию об указании путей и использовании подстановочных символов см. в разделе «Фильтры файлов» (стр. 84).
     - В проводнике выберите файлы и папки для резервного копирования.

       Ссылка **Обзор** доступна только при создании плана резервного копирования для одного пользователя.

- [Необязательно] В элементе управления **Элементы для резервного копирования** щелкните **Показать исключения**, чтобы указать файлы и папки для пропуска при выполнении резервного копирования.

  Исключенные файлы имеют приоритет над выбранными файлами: если указать один файл в обоих полях, этот файл будет пропущен при резервном копировании.

15.2.3.2 Восстановление OneDrive и файлов OneDrive

Восстановление со всего OneDrive

1. Щелкните **Microsoft Office 365**.
2. Если в сервис резервного копирования добавлено несколько организаций Office 365, выберите ту организацию, данные которой необходимо восстановить из резервной копии. В противном случае пропустите этот шаг.
3. Разверните узел **Пользователи**, выберите **Все пользователи**, затем выберите пользователя, для которого необходимо восстановить OneDrive, и щелкните **Восстановить**.

   Если пользователь удален, выберите его в разделе **Резервные копии приложений в облаке** на вкладке Резервные копии приложений в облаке (стр. 126) и щелкните **Показать резервные копии**.

   Можно выполнить поиск по имени пользователей. Подстановочные символы не поддерживаются.
4. Выберите точку восстановления.

   ***Подсказка**. Чтобы просмотреть только те точки восстановления, которые содержат файлы OneDrive, в поле **Фильтровать по содержимому** выберите пункт **OneDrive**.*
5. Последовательно выберите пункты **Восстановить** > **Весь OneDrive**.
6. Если в сервис резервного копирования добавлено несколько организаций Office 365, щелкните **Организация Office 365** для просмотра, изменения или указания целевой организации.

   По умолчанию выбрана исходная организация. Если эта организация больше не зарегистрирована в сервисе резервного копирования, необходимо указать целевую организацию.
7. Раздел **Восстановить на диск** позволяет просматривать, изменять или указывать целевого пользователя.

   По умолчанию выбран исходный пользователь. Если этот пользователь не существует или выбрана организация, которая не является исходной, необходимо указать целевого пользователя.
8. Выберите, восстанавливать ли разрешения предоставления общего доступа для данных файлов.
9. Щелкните **Запуск восстановления**.
10. Выберите один из вариантов перезаписи:
    - **Перезаписывать существующие файлы**
    - **Перезаписывать существующий файл, если он старше**
    - **Не перезаписывать существующие файлы**
11. Щелкните **Продолжить**, чтобы подтвердить решение.

Восстановление файлов OneDrive

1. Щелкните **Microsoft Office 365**.

2. Если в сервис резервного копирования добавлено несколько организаций Office 365, выберите ту организацию, данные которой необходимо восстановить из резервной копии. В противном случае пропустите этот шаг.
3. Разверните узел **Пользователи**, выберите **Все пользователи**, затем выберите пользователя, для которого необходимо восстановить файлы OneDrive, и щелкните **Восстановить**.

   Если пользователь удален, выберите его в разделе **Резервные копии приложений в облаке** на вкладке Резервные копии (стр. 126) и щелкните **Показать резервные копии**.

   Можно выполнить поиск по имени пользователей. Подстановочные символы не поддерживаются.
4. Выберите точку восстановления.

   ***Подсказка**. Чтобы просмотреть только те точки восстановления, которые содержат файлы OneDrive, в поле **Фильтровать по содержимому** выберите пункт **OneDrive**.*
5. Последовательно выберите пункты **Восстановление** > **Файлы/папки**.
6. Перейдите к нужной папке или используйте поиск для получения списка нужных файлов и папок.

   Можно использовать один или несколько подстановочных символов (* и ?). Подробную информацию об использовании подстановочных символов см. в разделе «Фильтры файлов» (стр. 84).

   Поиск недоступен, если резервная копия зашифрована.
7. Выберите файлы, которые необходимо восстановить.

   Если вы выбрали один файл в незашифрованной резервной копии, можно щелкнуть **Показать версии**, чтобы выбрать версию файла для восстановления. Можно выбрать любую версию в резервной копии, датированную до или после точки восстановления.
8. Чтобы загрузить выбранный файл, выберите его, щелкните **Загрузить**, выберите расположение для сохранения файла и щелкните **Сохранить**. В противном случае пропустите этот шаг.
9. Нажмите кнопку **Восстановить**.
10. Если в сервис резервного копирования добавлено несколько организаций Office 365, щелкните **Организация Office 365** для просмотра, изменения или указания целевой организации.

    По умолчанию выбрана исходная организация. Если эта организация больше не зарегистрирована в сервисе резервного копирования, необходимо указать целевую организацию.
11. Раздел **Восстановить на диск** позволяет просматривать, изменять или указывать целевого пользователя.

    По умолчанию выбран исходный пользователь. Если этот пользователь не существует или выбрана организация, которая не является исходной, необходимо указать целевого пользователя.
12. В поле **Путь** просмотрите или измените целевую папку в хранилище OneDrive целевого пользователя. По умолчанию выбрано исходное хранилище.
13. Выберите, восстанавливать ли разрешения предоставления общего доступа для данных файлов.
14. Щелкните **Запуск восстановления**.
15. Выберите один из вариантов перезаписи файла:
    - **Перезаписывать существующие файлы**
    - **Перезаписывать существующий файл, если он старше**

- **Не перезаписывать существующие файлы**

16. Щелкните **Продолжить**, чтобы подтвердить решение.

15.2.4 Защита сайтов SharePoint Online

Для каких элементов можно создавать резервные копии?

Можно создать резервные копии для семейства классических веб-сайтов SharePoint, сайтов группы (рабочей группы) и информационных сайтов. Кроме того, можно выбрать отдельные подсайты, списки и библиотеки для резервного копирования.

При выполнении резервного копирования *пропускаются* следующие элементы:

- Настройки сайта **Настройка интерфейса пользователя** (за исключением **заголовка, описания и логотипа**).
- Комментарии страницы сайта и настройки комментариев страницы (комментарии **Вкл./Выкл.**).
- Настройки сайта **Компоненты сайта**.
- Страницы веб-части и веб-части, встроенные в страницы wiki (из-за ограничений API SharePoint Online).
- Файлы OneNote (из-за ограничений API SharePoint Online).
- Столбцы с внешними данными и управляемыми метаданными.
- По умолчанию используется семейство сайтов «domain-my.sharepoint.com». Это то семейство, в котором располагаются все файлы OneDrive пользователей данной организации.
- Содержимое корзины.

Ограничения

- При выполнении резервного копирования заголовки и описания сайтов/подсайтов/списков/столбцов урезаются, если размер заголовка/описания превышает 10000 байт.

Какие элементы можно восстановить?

Из резервной копии сайта можно восстановить следующие элементы:

- Весь сайт
- Подсайты
- Списки
- Элементы списка
- Библиотеки документов
- Документы
- Вложения элементов списка
- Страницы сайта и страницы wiki

Чтобы найти эти элементы, можно воспользоваться поиском.

Элементы можно восстановить на исходный сайт или тот сайт, который не является исходным. Путь к восстановленному элементу будет таким же, как и путь к исходному элементу. Если путь не существует, он будет создан.

Можно выбрать восстановление разрешений предоставления общего доступа или наследование элементами разрешений из родительского объекта после восстановления.

Указанные ниже элементы не подлежат восстановлению:

- Подсайты на основе шаблона **Репозиторий процесса Visio**.
- Списки всех указанных ниже типов: **список опроса**, **список задач**, **галерея**, **ссылки**, **календарь**, **доска обсуждений**, **внешний** и **электронная таблица импорта**.
- Списки, для которых включено несколько типов содержимого.

15.2.4.1 Выбор данных SharePoint Online

Выберите данные, как описано ниже, а затем укажите другие настройки плана резервного копирования должным образом (стр. 42).

Порядок выбора данных SharePoint Online

1. Щелкните **Microsoft Office 365**.
2. Если в сервис резервного копирования добавлено несколько организаций Office 365, выберите ту организацию, для пользователей которой необходимо создать резервные копии их данных. В противном случае пропустите этот шаг.
3. Выполните одно из следующих действий:
   - Чтобы создать резервную копию всех классических сайтов SharePoint в организации (включая сайты, которые будут созданы в будущем), разверните узел **Коллекции сайтов**, выберите **Все коллекции сайтов** и щелкните **Групповое резервное копирование**.
   - Чтобы создать резервную копию отдельных классических веб-сайтов, разверните узел **Коллекции сайтов**, выберите **Все коллекции сайтов**, затем выберите сайты, для которых необходимо создать резервные копии, и щелкните **Резервное копирование**.
   - Чтобы создать резервную копию сайтов всех групп (включая сайты, которые будут созданы в будущем), разверните узел **Группы**, выберите **Все группы** и щелкните **Групповое резервное копирование**.
   - Чтобы создать резервную копию отдельных сайтов группы, разверните узел **Группы**, выберите **Все группы**, затем выберите группы, для сайтов которых необходимо создать резервные копии, и щелкните **Резервное копирование**.
4. На панели плана резервного копирования:
   - Убедитесь, что в области **Выбор данных** выбран элемент **Сайты SharePoint**.
   - В элементе управления **Элементы для резервного копирования** выполните одно из указанных ниже действий:
     - Не меняйте настройку по умолчанию **[Все]** (все элементы выбранных сайтов).
     - Укажите подсайты, списки и библиотеки для резервного копирования, добавив их имена или пути.

       Чтобы создать резервную копию подсайта или списка/библиотеки сайта верхнего уровня, укажите его отображаемое имя в следующем формате: `/отображаемое имя/**`

       Чтобы создать резервную копию списка/библиотеки подсайта, укажите его отображаемое имя в следующем формате: `/отображаемое имя подсайта/отображаемое имя списка/**`

       Отображаемые имена подсайтов, списков и библиотек отображаются на странице **Содержимое сайта** на сайте или подсайте SharePoint.
     - В проводнике выберите подсайты для резервного копирования.

Ссылка **Обзор** доступна только при создании плана резервного копирования для одного сайта.

- [Необязательно] В элементе управления **Элементы для резервного копирования** щелкните **Показать исключения**, чтобы указать подсайты, списки и библиотеки для пропуска при выполнении резервного копирования.

  Исключенные элементы имеют приоритет над выбранными элементами: если указать один подсайт в обоих полях, этот подсайт будет пропущен при резервном копировании.

15.2.4.2 Восстановление данных SharePoint Online

1. Щелкните **Microsoft Office 365**.
2. Если в сервис резервного копирования добавлено несколько организаций Office 365, выберите ту организацию, данные которой необходимо восстановить из резервной копии. В противном случае пропустите этот шаг.
3. Выполните одно из следующих действий:
   - Чтобы восстановить данные с сайта группы, разверните узел **Группы**, выберите **Все группы**, затем выберите группу, в сайте которой изначально содержались элементы для восстановления, и щелкните **Восстановить**.
   - Чтобы восстановить данные с классического сайта, разверните узел **Коллекции сайтов**, выберите **Все коллекции сайтов**, затем выберите сайт, который изначально содержал элементы для восстановления, и щелкните **Восстановить**.
   - Если сайт удален, выберите его в разделе **Резервные копии приложений в облаке** на вкладке Резервные копии (стр. 126) и щелкните **Показать резервные копии**.

   Можно выполнить поиск групп и сайтов по имени. Подстановочные символы не поддерживаются.
4. Выберите точку восстановления.

   Подсказка. *Чтобы просмотреть только те точки восстановления, которые содержат сайты SharePoint, в поле* ***Фильтровать по содержимому*** *выберите пункт* ***Сайты SharePoint****.*
5. Щелкните **Восстановить файлы SharePoint**.
6. Перейдите к нужной папке или воспользуйтесь поиском, чтобы получить список нужных элементов данных.

   Можно использовать один или несколько подстановочных символов (* и ?). Подробную информацию об использовании подстановочных символов см. в разделе «Фильтры файлов» (стр. 84).

   Поиск недоступен, если резервная копия зашифрована.
7. Выберите элементы, которые необходимо восстановить.

   Если вы выполнили поиск в незашифрованной резервной копии и выбрали один элемент в результатах поиска, можно щелкнуть **Показать версии**, чтобы выбрать версию элемента для восстановления. Можно выбрать любую версию в резервной копии, датированную до или после точки восстановления.
8. Чтобы загрузить элемент, выберите его, щелкните **Загрузить**, выберите расположение для его сохранения и щелкните **Сохранить**. В противном случае пропустите этот шаг.
9. Нажмите кнопку **Восстановить**.
10. Если в сервис резервного копирования добавлено несколько организаций Office 365, щелкните **Организация Office 365** для просмотра, изменения или указания целевой организации.

По умолчанию выбрана исходная организация. Если эта организация больше не зарегистрирована в сервисе резервного копирования, необходимо указать целевую организацию.

11. В разделе **Восстановить на сайт** можно просматривать, изменять или указывать целевой сайт.

    По умолчанию выбран исходный сайт. Если этот сайт не существует или выбрана организация, которая не является исходной, необходимо указать целевой сайт.
12. Выберите, восстанавливать ли разрешения предоставления общего доступа для выбранных элементов.
13. Щелкните **Запуск восстановления**.
14. Выберите один из вариантов перезаписи:
    - **Перезаписывать существующие файлы**
    - **Перезаписывать существующий файл, если он старше**
    - **Не перезаписывать существующие файлы**
15. Щелкните **Продолжить**, чтобы подтвердить решение.

15.2.5 Обновление облачного агента

В этом разделе описана процедура обновления решения резервного копирования для Microsoft Office 365 до последней версии. В этой версии поддерживаются резервные копии OneDrive и SharePoint Online, а также повышена производительность резервного копирования и восстановления. Начиная с версии 8.0 службы резервного копирования, следующие функции больше не поддерживаются в прежнем решении: редактирование, удаление, применение и отмена плана резервного копирования.

Доступность обновления зависит от готовности центра обработки данных и настроек, установленных вашим поставщиком услуг. Если обновление доступно, на консоли резервного копирования отображается уведомление в верхней части вкладки **Microsoft Office 365 (v1)**.

Процесс обновления

При обновлении пользователи Office 365 в вашей организации добавляются в новое решение резервного копирования. Планы резервного копирования переносятся и применяются к соответствующим пользователям.

Ранее созданные резервные копии копируются из одного хранилище в облаке в другое. На вкладке **Резервные копии** скопированные резервные копии отображаются в отдельном разделе **Резервные копии приложений в облаке**, а исходные резервные копии остаются в хранилище **Облачное хранилище данных**. По окончании процесса обновления исходные резервные копии удаляются из хранилища **Облачное хранилище данных**.

Обновление может занять несколько часов или даже дней в зависимости от количества пользователей в организации, количества резервных копий и скорости доступа к Office 365. Во время обновления можно выполнить восстановление из ранее созданных резервных копий. Однако резервные копии и планы резервного копирования, созданные во время обновления, будут утрачены.

В маловероятном случае сбоя обновления решения резервного копирования остаются полностью функциональными, а само обновление можно перезапустить с момента сбоя.

Порядок запуска процесса обновления

1. Щелкните **Microsoft Office 365 (v1)**.

2. В уведомлении в верхней части экрана щелкните **Обновить**.
3. Подтвердите запуск процесса обновления.
4. Выберите центр обработки данных Microsoft, используемый вашей организацией.

   Программа перенаправит вас на страницу входа Microsoft Office 365.
5. Войдите с учетными данными глобального администратора Office 365.

   В Microsoft Office 365 отображается список разрешений, которые необходимы для резервного копирования и восстановления данных вашей организации.
6. Подтвердите, что предоставили службе резервного копирования эти разрешения.

   Будет выполнено перенаправление на консоль резервного копирования, после чего запустится процесс обновления. Ход выполнения обновления отображается на панели **Microsoft Office 365** > **Действия**.

16 Защита данных G Suite

Что означает защита G Suite?

- Резервное копирование и восстановление «облако в облако» данных пользователя G Suite (почтовые ящики Gmail, календари, контакты, хранилища Google Диск) и общих дисков G Suite.
- Фрагментарное восстановление сообщений электронной почты, файлов и других элементов.
- Поддержка восстановления нескольких организаций G Suite, а также восстановления разных организаций.
- Необязательная нотаризация файлов в резервных копиях с использованием базы данных на основе цепочки блоков Ethereum. Нотаризация позволяет подтвердить целостность файла и отсутствие изменений в нем с момента резервного копирования.
- При необходимости можно воспользоваться полнотекстовым поиском. Полнотекстовый поиск позволяет искать сообщения электронной почты по их содержимому.
- Для одной компании можно защитить до 5000 элементов (почтовые ящики, хранилища Google Диск и общие диски) без снижения быстродействия.

Требуемые права пользователя

В сервисе резервного копирования

В сервисе резервного копирования необходимо работать с учетной записью администратора компании. Администраторы и пользователи отдела не могут создавать резервные копии данных G Suite или восстанавливать их.

В G Suite

Чтобы добавить организацию G Suite в службу резервного копирования, необходимо войти как суперадминистратор и убедиться, что включен доступ к API (**Безопасность** > **Справочник по API** > **Включить доступ к API** в консоли администратора Google).

Пароль суперадминистратора не сохраняется нигде и не используется для выполнения резервного копирования и восстановления. Изменение этого пароля в G Suite не влияет на работу сервиса резервного копирования.

Если суперадминистратор, который добавил организацию G Suite, удален из G Suite, или ему назначена роль с меньшими правами, резервное копирование завершится ошибкой,

наподобие «Отказано в доступе». В этом случае повторите процедуру «Добавление организации G Suite» (стр. 179) и укажите действительный учетные данные суперадминистратора. Во избежание этой ситуации рекомендуем создать пользователя с правами суперадминистратора специально для выполнения операций резервного копирования и восстановления.

О расписании резервного копирования

Поскольку облачным агентом пользуются многие клиенты, он автоматически выбирает время запуска каждого плана резервного копирования таким образом, чтобы обеспечить равномерную нагрузку в течение дня и одинаковое качество обслуживания для всех клиентов.

Каждый план резервного копирования запускается ежедневно в одно и то же время дня.

Ограничения

- Поиск в зашифрованных резервных копиях не поддерживается.
- Не больше 10 ручных запусков резервного копирования в час (стр. 131).
- Не более 10 одновременных операций восстановления (сюда входят операции восстановления как для Office 365, так и для G Suite).

16.1 Добавление организации G Suite

Порядок добавления организации G Suite

1. Войдите на консоль резервного копирования с учетной записью администратора компании.
2. Последовательно выберите пункты **Устройства** > **Добавить** > **G Suite**.
3. Следуйте инструкциям, которые выводятся в программе:
   a. Щелкните **Открыть Marketplace**.
   b. Войдите с учетными данными суперадминистратора.
   c. Щелкните **Установить в домене**.
   d. Подтвердите установку во всем домене.

      В G Suite отображается список разрешений, которые необходимы для резервного копирования и восстановления данных вашей организации.
   e. Подтвердите, что предоставили службе резервного копирования эти разрешения.
   f. Завершите работу мастера установки.
   g. Щелкните **Запуск**.

Будет выполнено перенаправление на консоль резервного копирования. Элементы данных вашей организации появятся на консоли резервного копирования на странице **G Suite**.

Советы по дальнейшему использованию

- Облачный агент синхронизируется с G Suite каждые 24 часа после добавления организации в сервис резервного копирования. После добавления или удаления пользователя или хранилища общего диска соответствующие изменения отображаются на консоли резервного копирования через некоторое время. Чтобы принудительно синхронизировать облачный агент с G Suite, выберите организацию на странице **G Suite** и щелкните **Обновить**.
- Если к группе **Все пользователи** или **Все общие диски** применен план резервного копирования, новые добавленные элементы включаются в состав резервной копии только после синхронизации.

- В соответствии с политикой Google после удаления пользователя или общего диска из графического интерфейса пользователя G Suite они остаются доступными в течение нескольких дней через API. В течение этого периода удаленный элемент будет неактивным (серым) на консоли резервного копирования, а резервное копирование этого элемента выполняться не будет. Когда удаленный элемент станет недоступным через API, он исчезнет с консоли резервного копирования. Чтобы получить доступ к его резервным копиям (при наличии), последовательно выберите пункты **Резервные копии** > **Резервные копии приложений в облаке**.

16.2 Защита данных Gmail

Для каких элементов можно создавать резервные копии?

Можно создать резервную копию почтовых ящиков пользователей Gmail. В резервную копию почтового ящика также входят данные календаря и контактов. При необходимости можно выбрать резервное копирование совместно используемых календарей.

При выполнении резервного копирования *пропускаются* следующие элементы:

- Календари **Дни рождения**, **Напоминания**, **Задачи**
- Папки, прикрепленные к событиям календаря
- Папка **Каталог** в контактах

Указанные ниже элементы календаря *пропускаются* из-за ограничений API службы «Google Календарь»:

- Назначенные слоты
- Поле конференц-связи для события
- Настройка календаря **Мероприятия на весь день**
- Настройка календаря **Автоматически принять приглашения** (в календарях для помещений или общих пространств)

Указанные ниже элементы контактов *пропускаются* из-за ограничений API службы «Google People»:

- Папка **Другие контакты**
- Внешние профили контакта (**Профиль каталога**, **Профиль Google**)
- Поле контакта **Файл как**

Какие элементы можно восстановить?

Из резервной копии почтового ящика можно восстановить следующие элементы:

- почтовые ящики;
- Папки электронной почты («метки» согласно терминологии Google. **Метки** представлены в программе резервного копирования как папки (для соответствия с другим представлением данных).
- сообщения электронной почты;
- события календаря;
- контакты;

Чтобы найти элементы в незашифрованной резервной копии, можно воспользоваться поиском. Поиск в зашифрованных резервных копиях не поддерживается.

При восстановлении почтовых ящиков и элементов почтовых ящиков можно выбрать, перезаписывать ли элементы в целевое расположение.

Ограничения

- Фотографии контакта невозможно восстановить
- Элемент календаря **Нет на месте** восстанавливается как обычное событие календаря из-за ограничений API службы Google Календарь

16.2.1 Выбор почтовых ящиков

Выберите почтовый ящики, как указано ниже, а затем укажите другие настройки плана резервного копирования как требуется (стр. 42).

Порядок выбора почтовых ящиков Gmail

1. Щелкните **G Suite**.
2. Если в сервис резервного копирования добавлено несколько организаций G Suite, выберите ту организацию, для пользователей которой необходимо создать резервные копии их данных. В противном случае пропустите этот шаг.
3. Выполните одно из следующих действий:
   - Чтобы создать резервную копию почтовых ящиков всех пользователей (включая почтовые ящики, которые будут созданы в будущем), разверните узел **Пользователи**, выберите **Все пользователи** и щелкните **Групповое резервное копирование**.
   - Чтобы создать резервную копию почтовых ящиков отдельных пользователей, разверните узел **Пользователи**, выберите **Все пользователи**, затем выберите пользователей, для почтовых ящиков которых необходимо создать резервные копии, и щелкните **Резервное копирование**.
4. На панели плана резервного копирования:
   - Убедитесь, что в области **Выбор данных** выбран элемент **Gmail**.
   - Чтобы создать резервную копию календарей, которые используются совместно с другими пользователями, включите переключатель **Включить общие календари**.
   - Решите, необходимо ли использовать полнотекстовый поиск (стр. 181) в резервных копиях сообщений электронной почты. Для доступа к этому параметру щелкните значок шестеренки, затем последовательно выберите пункты **Параметры резервного копирования** > **Полнотекстовый поиск**.

16.2.1.1 Полнотекстовый поиск

Этот параметр определяет, индексируются ли сообщения электронной почты облачным агентом.

Значение по умолчанию: **Включено**.

Если этот параметр включен, содержимое сообщений индексируется, после чего их можно искать по содержимому. В противном случае доступен только поиск по теме, отправителю, получателю или дате.

Примечание *Поиск в зашифрованных резервных копиях не поддерживается.*

Процесс индексирования не влияет на производительность резервного копирования, поскольку оно выполняется другим компонентом программного обеспечения. Индексирование

первой (полной) резервной копии может занять некоторое время, поэтому ее содержимое появляется с определенной задержкой после окончания ее создания.

Индекс занимает 10–30 % объема ресурсов хранения, занятых резервными копиями почтовых ящиков. Чтобы узнать точное значение, последовательно выберите пункты **Резервные копии** > **Резервные копии приложений в облаке** и просмотрите столбец **Размер индекса**. Для экономии места, возможно, нужно будет отключить полнотекстовый поиск. Значение в столбце **Размер индекса** уменьшится до нескольких магабайт после следующего резервного копирования. Это минимальный объем метаданных, необходимый для выполнения поиска по теме, отправителю, получателю или дате.

При повторном включении полнотекстового поиска программа индексирует все резервные копии, ранее созданные планом резервного копирования. Это также займет некоторое время.

16.2.2 Восстановление почтовых ящиков и элементов почтовых ящиков

16.2.2.1 Восстановление почтовых ящиков

1. Щелкните **G Suite**.
2. Если в сервис резервного копирования добавлено несколько организаций G Suite, выберите ту организацию, данные которой необходимо восстановить из резервной копии. В противном случае пропустите этот шаг.
3. Разверните узел **Пользователи**, выберите **Все пользователи**, затем выберите пользователя, для которого необходимо восстановить почтовый ящик, и щелкните **Восстановить**.

   Если пользователь удален, выберите его в разделе **Резервные копии приложений в облаке** на вкладке Резервные копии приложений в облаке (стр. 126) и щелкните **Показать резервные копии**.

   Можно выполнить поиск по имени пользователей и групп. Подстановочные символы не поддерживаются.
4. Выберите точку восстановления.

   Подсказка. *Чтобы просмотреть только те точки восстановления, которые содержат почтовые ящики, в поле **Фильтровать по содержимому** выберите пункт **Gmail**.*
5. Последовательно выберите пункты **Восстановить** > **Весь почтовый ящик**.
6. Если в сервис резервного копирования добавлено несколько организаций G Suite, щелкните **Организация G Suite** для просмотра, изменения или указания целевой организации.

   По умолчанию выбрана исходная организация. Если эта организация больше не зарегистрирована в сервисе резервного копирования, необходимо указать целевую организацию.
7. Раздел **Восстановить в почтовый ящик** позволяет просматривать, изменять или указывать целевой почтовый ящик.

   По умолчанию выбран исходный почтовый ящик. Если этот почтовый ящик не существует или выбрана организация, которая не является исходной, необходимо указать целевой почтовый ящик.
8. Щелкните **Запуск восстановления**.
9. Выберите один из вариантов перезаписи:
   - **Перезаписывать существующие элементы**

- **Не перезаписывать существующие элементы**

10. Щелкните **Продолжить**, чтобы подтвердить решение.

16.2.2.2 Восстановление элементов почтовых ящиков

1. Щелкните **G Suite**.
2. Если в сервис резервного копирования добавлено несколько организаций G Suite, выберите ту организацию, данные которой необходимо восстановить из резервной копии. В противном случае пропустите этот шаг.
3. Разверните узел **Пользователи**, выберите **Все пользователи**, затем выберите пользователя, почтовый ящик которого изначально содержал элементы для восстановления, и щелкните **Восстановить**.

   Если пользователь удален, выберите его в разделе **Резервные копии приложений в облаке** на вкладке Резервные копии приложений в облаке (стр. 126) и щелкните **Показать резервные копии**.

   Можно выполнить поиск по имени пользователей и групп. Подстановочные символы не поддерживаются.
4. Выберите точку восстановления.

   Подсказка. *Чтобы просмотреть только те точки восстановления, которые содержат почтовые ящики, в поле* ***Фильтровать по содержимому*** *выберите пункт* ***Gmail****.*
5. Последовательно выберите пункты **Восстановление** > **Сообщения электронной почты**.
6. Обзор требуемой папки. Если резервная копия не защищена, можно использовать поиск для получения списка нужных элементов.

   Доступны указанные ниже параметры поиска. Подстановочные символы не поддерживаются.
   - Для сообщений электронной почты: выполните поиск по теме, отправителю, получателю, дате, названию вложения и содержимому сообщения. Последние два параметра результативны только в том случае, если при резервном копировании был включен параметр **Полнотекстовый поиск**. Язык искомого фрагмента сообщения можно указать в дополнительном параметре.
   - Для событий: выполните поиск по заголовку и дате.
   - Для контактов: выполните поиск по имени, адресу электронной почты и номеру телефона.
7. Выберите элементы, которые необходимо восстановить. Чтобы иметь возможность выбрать папки, щелкните значок восстановления папок: 

   Кроме того, можно выполнить любое из следующих действий:
   - Чтобы просмотреть содержимое выбранного элемента вместе с вложениями, щелкните **Показать содержимое**. Чтобы загрузить вложенный файл, щелкните его имя.
   - Только в том случае, если вы выполнили поиск в незашифрованной резервной копии и выбрали один элемент в результатах поиска, можно щелкнуть **Показать версии**, чтобы выбрать версию элемента для восстановления. Можно выбрать любую версию в резервной копии, датированную до или после точки восстановления.
8. Нажмите кнопку **Восстановить**.
9. Если в сервис резервного копирования добавлено несколько организаций G Suite, щелкните **Организация G Suite** для просмотра, изменения или указания целевой организации.

По умолчанию выбрана исходная организация. Если эта организация больше не зарегистрирована в сервисе резервного копирования, необходимо указать целевую организацию.

10. Раздел **Восстановить в почтовый ящик** позволяет просматривать, изменять или указывать целевой почтовый ящик.

    По умолчанию выбран исходный почтовый ящик. Если этот почтовый ящик не существует или выбрана организация, которая не является исходной, необходимо указать целевой почтовый ящик.
11. В поле **Путь** просмотрите или измените целевую папку в целевом почтовом ящике. По умолчанию выбрана исходная папка.
12. Щелкните **Запуск восстановления**.
13. Выберите один из вариантов перезаписи:
    - **Перезаписывать существующие элементы**
    - **Не перезаписывать существующие элементы**
14. Щелкните **Продолжить**, чтобы подтвердить решение.

16.3 Защита файлов Google Диск

Для каких элементов можно создавать резервные копии?

Можно создать резервную копию всего хранилища Google Диск или отдельных файлов и папок. При необходимости можно выбрать резервное копирование файлов, к которым открыт общий доступ для пользователя Google Диск.

Для файлов создается резервная копия вместе с их разрешениями общего доступа.

При выполнении резервного копирования *пропускаются* следующие элементы:

- Общий файл, если в отношении него пользователь имеет права доступ комментатора или просматривающего, а собственник файла отключил параметры загрузки, печати и копирования для комментаторов и просматривающих.
- В папке **Компьютеры** (создана клиентом резервного копирования и синхронизации)

Ограничения

- Из всех файлов формата Google резервные копии создаются только для документов Google, листов Google, слайдов Google и чертежей Google.

Какие элементы можно восстановить?

Можно восстановить все хранилище Google Диск или любой файл или папку, для которых создана резервная копия.

Чтобы найти элементы в незашифрованной резервной копии, можно воспользоваться поиском. Поиск в зашифрованных резервных копиях не поддерживается.

Можно выбрать восстановление разрешений предоставления общего доступа или наследование файлами их разрешений из папки, в которую они восстанавливаются.

Ограничения

- Комментарии в файлах не восстанавливаются.
- Ссылки на общий доступ к файлам и папкам не восстанавливаются.
- **Настройки владельца**, которые обеспечивают доступ только для чтения для общих файлов (**Не разрешать редакторам изменять права доступа и добавлять новых пользователей** и

Отключить параметры загрузки, печати и копирования для комментаторов и просматривающих), невозможно изменить в ходе восстановления.

- Если для папки включен параметр **Не разрешать редакторам изменять права доступа и добавлять новых пользователей**, то право владения для этой папки невозможно изменить при выполнении восстановления. Эта не позволяет API Google Диск выводит список разрешений папки. Право владения в отношении файлов в папке восстанавливается правильно.

16.3.1 Выбор файлов Google Диск

Выберите файлы, как описано ниже, а затем укажите другие настройки плана резервного копирования должным образом (стр. 42).

Порядок выбора файлов Google Диск

1. Щелкните **G Suite**.
2. Если в сервис резервного копирования добавлено несколько организаций G Suite, выберите ту организацию, для пользователей которой необходимо создать резервные копии их данных. В противном случае пропустите этот шаг.
3. Выполните одно из следующих действий:
   - Чтобы создать резервную копию файлов всех пользователей (включая пользователей, которые будут созданы в будущем), разверните узел **Пользователи**, выберите **Все пользователи** и щелкните **Групповое резервное копирование**.
   - Чтобы создать резервную копию файлов отдельных пользователей, разверните узел **Пользователи**, выберите **Все пользователи**, затем выберите пользователей, для файлов которых необходимо создать резервные копии, и щелкните **Резервное копирование**.
4. На панели плана резервного копирования:
   - Убедитесь, что в области **Выбор данных** выбран элемент **Google Диск**.
   - В элементе управления **Элементы для резервного копирования** выполните одно из указанных ниже действий:
     - Не меняйте настройку по умолчанию **[Все]** (все файлы).
     - Укажите файлы и папки для резервного копирования, добавив их имена или пути.

       Можно использовать подстановочные символы (*, ** и ?). Подробную информацию об указании путей и использовании подстановочных символов см. в разделе «Фильтры файлов» (стр. 84).
     - В проводнике выберите файлы и папки для резервного копирования.

       Ссылка **Обзор** доступна только при создании плана резервного копирования для одного пользователя.
   - [Необязательно] В элементе управления **Элементы для резервного копирования** щелкните **Показать исключения**, чтобы указать файлы и папки для пропуска при выполнении резервного копирования.

     Исключенные файлы имеют приоритет над выбранными файлами: если указать один файл в обоих полях, этот файл будет пропущен при резервном копировании.
   - Чтобы создать резервную копию файлов, которые используются совместно с другими пользователями, включите переключатель **Включить общие файлы**.
   - Для включения нотаризации для всех файлов, выбранных для резервного копирования, включите переключатель **Нотаризация**. Дополнительную информацию о нотаризации см. в разделе «Нотаризация» (стр. 191).

16.3.2 Восстановление Google Диск и файлов Google Диск

16.3.2.1 Восстановление со всего хранилища Google Диск

1. Щелкните **G Suite**.
2. Если в сервис резервного копирования добавлено несколько организаций G Suite, выберите ту организацию, данные которой необходимо восстановить из резервной копии. В противном случае пропустите этот шаг.
3. Разверните узел **Пользователи**, выберите **Все пользователи**, затем выберите пользователя, для которого необходимо восстановить Google Диск, и щелкните **Восстановить**.

   Если пользователь удален, выберите его в разделе **Резервные копии приложений в облаке** на вкладке Резервные копии приложений в облаке (стр. 126) и щелкните **Показать резервные копии**.

   Можно выполнить поиск по имени пользователей. Подстановочные символы не поддерживаются.
4. Выберите точку восстановления.

   ***Подсказка**. Чтобы просмотреть только те точки восстановления, которые содержат файлы Google Диск, в поле **Фильтровать по содержимому** выберите пункт **Google Диск**.*
5. Последовательно выберите пункты **Восстановление** > **Весь Drive**.
6. Если в сервис резервного копирования добавлено несколько организаций G Suite, щелкните **Организация G Suite** для просмотра, изменения или указания целевой организации.

   По умолчанию выбрана исходная организация. Если эта организация больше не зарегистрирована в сервисе резервного копирования, необходимо указать целевую организацию.
7. Раздел **Восстановить на диск** позволяет просматривать, изменять или указывать целевого пользователя или целевой общий диск.

   По умолчанию выбран исходный пользователь. Если этот пользователь не существует или выбрана организация, которая не является исходной, необходимо указать целевого пользователя или целевой общий диск.

   Если в резервной копии есть общие файлы, они восстанавливаются в корневую папку целевого диска.
8. Выберите, восстанавливать ли разрешения предоставления общего доступа для данных файлов.
9. Щелкните **Запуск восстановления**.
10. Выберите один из вариантов перезаписи:
    - **Перезаписывать существующие файлы**
    - **Перезаписывать существующий файл, если он старше**
    - **Не перезаписывать существующие файлы**
11. Щелкните **Продолжить**, чтобы подтвердить решение.

16.3.2.2 Восстановление файлов Google Диск

1. Щелкните **G Suite**.
2. Если в сервис резервного копирования добавлено несколько организаций G Suite, выберите ту организацию, данные которой необходимо восстановить из резервной копии. В противном случае пропустите этот шаг.

3. Разверните узел **Пользователи**, выберите **Все пользователи**, затем выберите пользователя, для которого необходимо восстановить файлы Google Диск, и щелкните **Восстановить**.

   Если пользователь удален, выберите его в разделе **Резервные копии приложений в облаке** на вкладке Резервные копии приложений в облаке (стр. 126) и щелкните **Показать резервные копии**.

   Можно выполнить поиск по имени пользователей. Подстановочные символы не поддерживаются.
4. Выберите точку восстановления.

   ***Подсказка**. Чтобы просмотреть только те точки восстановления, которые содержат файлы Google Диск, в поле **Фильтровать по содержимому** выберите пункт **Google Диск**.*
5. Последовательно выберите пункты **Восстановление** > **Файлы/папки**.
6. Перейдите к нужной папке или используйте поиск для получения списка нужных файлов и папок.

   Можно использовать один или несколько подстановочных символов (* и ?). Подробную информацию об использовании подстановочных символов см. в разделе «Фильтры файлов» (стр. 84)..

   Поиск недоступен, если резервная копия зашифрована.
7. Выберите файлы, которые необходимо восстановить.

   Если вы выбрали один файл в незашифрованной резервной копии, можно щелкнуть **Показать версии**, чтобы выбрать версию файла для восстановления. Можно выбрать любую версию в резервной копии, датированную до или после точки восстановления.
8. Чтобы загрузить выбранный файл, выберите его, щелкните **Загрузить**, выберите расположение для сохранения файла и щелкните **Сохранить**. В противном случае пропустите этот шаг.
9. Нажмите кнопку **Восстановить**.
10. Если в сервис резервного копирования добавлено несколько организаций G Suite, щелкните **Организация G Suite** для просмотра, изменения или указания целевой организации.

    По умолчанию выбрана исходная организация. Если эта организация больше не зарегистрирована в сервисе резервного копирования, необходимо указать целевую организацию.
11. Раздел **Восстановить на диск** позволяет просматривать, изменять или указывать целевого пользователя или целевой общий диск.

    По умолчанию выбран исходный пользователь. Если этот пользователь не существует или выбрана организация, которая не является исходной, необходимо указать целевого пользователя или целевой общий диск.
12. В поле **Путь** просмотрите или измените целевую папку в хранилище Google Диск целевого пользователя или на целевом общем диске. По умолчанию выбрано исходное хранилище.
13. Выберите, восстанавливать ли разрешения предоставления общего доступа для данных файлов.
14. Щелкните **Запуск восстановления**.
15. Выберите один из вариантов перезаписи файла:
    - **Перезаписывать существующие файлы**
    - **Перезаписывать существующий файл, если он старше**
    - **Не перезаписывать существующие файлы**
16. Щелкните **Продолжить**, чтобы подтвердить решение.

16.4 Защита файлов общего диска

Для каких элементов можно создавать резервные копии?

Можно создать резервную копию всего общего диска или отдельных файлов и папок.

Для файлов создается резервная копия вместе с их разрешениями общего доступа.

Ограничения

- Для общего диска без участников невозможно создать резервную копию из-за ограничений API Google Диск.
- Из всех файлов формата Google резервные копии создаются только для документов Google, листов Google, слайдов Google и чертежей Google.

Какие элементы можно восстановить?

Можно восстановить весь общий диск или любой файл или папку, для которых создана резервная копия.

Чтобы найти элементы в незашифрованной резервной копии, можно воспользоваться поиском. Поиск в зашифрованных резервных копиях не поддерживается.

Можно выбрать восстановление разрешений предоставления общего доступа или наследование файлами их разрешений из папки, в которую они восстанавливаются.

Следующие элементы не восстанавливаются:

- Если в целевом общем диске отключено предоставление общего доступа вне организации, разрешения предоставления общего доступа к файлу, совместно используемому с пользователем вне организации, не восстанавливаются.
- Если в целевом общем диске отключен параметр **Общий доступ для внешних пользователей**, разрешения предоставления общего доступа к файлу для пользователя, который не является участником целевого общего диска, не восстанавливаются.

Ограничения

- Комментарии в файлах не восстанавливаются.
- Ссылки на общий доступ к файлам и папкам не восстанавливаются.

16.4.1 Выбор файлов общей папки

Выберите файлы, как описано ниже, а затем укажите другие настройки плана резервного копирования должным образом (стр. 42).

Порядок выбора файлов общей папки

1. Щелкните **G Suite**.
2. Если в сервис резервного копирования добавлено несколько организаций G Suite, выберите ту организацию, для пользователей которой необходимо создать резервные копии их данных. В противном случае пропустите этот шаг.
3. Выполните одно из следующих действий:
   - Чтобы создать резервную копию файлов всех общих дисков (включая общие диски, которые будут созданы в будущем), разверните узел **Общие диски**, выберите **Все общие диски**, а затем щелкните **Групповое резервное копирование**.

- Чтобы создать резервную копию файлов отдельных общих дисков, разверните узел **Общие диски**, выберите **Все общие диски**, затем выберите общие диски, для которых необходимо создать резервные копии, и щелкните **Резервное копирование**.

4. На панели плана резервного копирования:
   - В элементе управления **Элементы для резервного копирования** выполните одно из указанных ниже действий:
     - Не маняйте настройку по умолчанию **[Все]** (все файлы).
     - Укажите файлы и папки для резервного копирования, добавив их имена или пути.

       Можно использовать подстановочные символы (*, ** и ?). Подробную информацию об указании путей и использовании подстановочных символов см. в разделе «Фильтры файлов» (стр. 84).
     - В проводнике выберите файлы и папки для резервного копирования.

       Ссылка **Обзор** доступна только при создании плана резервного копирования для одного общего диска.
   - [Необязательно] В элементе управления **Элементы для резервного копирования** щелкните **Показать исключения**, чтобы указать файлы и папки для пропуска при выполнении резервного копирования.

     Исключенные файлы имеют приоритет над выбранными файлами: если указать один файл в обоих полях, этот файл будет пропущен при резервном копировании.
   - Для включения нотаризации для всех файлов, выбранных для резервного копирования, включите переключатель **Нотаризация**. Дополнительную информацию о нотаризации см. в разделе «Нотаризация» (стр. 191).

16.4.2 Восстановление общего диска и файлов общего диска

16.4.2.1 Восстановление всего общего диска

1. Щелкните **G Suite**.
2. Если в сервис резервного копирования добавлено несколько организаций G Suite, выберите ту организацию, данные которой необходимо восстановить из резервной копии. В противном случае пропустите этот шаг.
3. Разверните узел **Общие диски**, выберите **Все общие диски**, а затем выберите общий диск для восстановления и щелкните **Восстановить**.

   Если общий диск был удален, выберите его в разделе **Резервные копии приложений в облаке** на вкладке Резервные копии (стр. 126) и щелкните **Показать резервные копии**.

   Можно выполнить поиск общих дисков по имени. Подстановочные символы не поддерживаются.
4. Выберите точку восстановления.
5. Последовательно выберите пункты **Восстановить** > **Весь общий диск**.
6. Если в сервис резервного копирования добавлено несколько организаций G Suite, щелкните **Организация G Suite** для просмотра, изменения или указания целевой организации.

   По умолчанию выбрана исходная организация. Если эта организация больше не зарегистрирована в сервисе резервного копирования, необходимо указать целевую организацию.

7. Раздел **Восстановить на диск** позволяет просматривать, изменять или указывать целевой общий диск или целевого пользователя. Если указать пользователя, данные восстанавливаются в хранилище Google Диск этого пользователя.

   По умолчанию выбран исходный общий диск. Если этот общий диск не существует, или выбрана организация, которая не является исходной, необходимо указать целевой общий диск или целевого пользователя.
8. Выберите, восстанавливать ли разрешения предоставления общего доступа для данных файлов.
9. Щелкните **Запуск восстановления**.
10. Выберите один из вариантов перезаписи:
    - **Перезаписывать существующие файлы**
    - **Перезаписывать существующий файл, если он старше**
    - **Не перезаписывать существующие файлы**
11. Щелкните **Продолжить**, чтобы подтвердить решение.

16.4.2.2 Восстановление файлов общего диска

1. Щелкните **G Suite**.
2. Если в сервис резервного копирования добавлено несколько организаций G Suite, выберите ту организацию, данные которой необходимо восстановить из резервной копии. В противном случае пропустите этот шаг.
3. Разверните узел **Общие диски**, выберите **Все общие диски**, затем выберите общий диск, который изначально содержал файлы для восстановления, и щелкните **Восстановить**.

   Если общий диск был удален, выберите его в разделе **Резервные копии приложений в облаке** на вкладке Резервные копии (стр. 126) и щелкните **Показать резервные копии**.

   Можно выполнить поиск общих дисков по имени. Подстановочные символы не поддерживаются.
4. Выберите точку восстановления.
5. Последовательно выберите пункты **Восстановление** > **Файлы/папки**.
6. Перейдите к нужной папке или используйте поиск для получения списка нужных файлов и папок.

   Можно использовать один или несколько подстановочных символов (* и ?). Подробную информацию об использовании подстановочных символов см. в разделе «Фильтры файлов» (стр. 84)..

   Поиск недоступен, если резервная копия зашифрована.
7. Выберите файлы, которые необходимо восстановить.

   Если вы выбрали один файл в незашифрованной резервной копии, можно щелкнуть **Показать версии**, чтобы выбрать версию файла для восстановления. Можно выбрать любую версию в резервной копии, датированную до или после точки восстановления.
8. Чтобы загрузить выбранный файл, выберите его, щелкните **Загрузить**, выберите расположение для сохранения файла и щелкните **Сохранить**. В противном случае пропустите этот шаг.
9. Нажмите кнопку **Восстановить**.
10. Если в сервис резервного копирования добавлено несколько организаций G Suite, щелкните **Организация G Suite** для просмотра, изменения или указания целевой организации.

По умолчанию выбрана исходная организация. Если эта организация больше не зарегистрирована в сервисе резервного копирования, необходимо указать целевую организацию.

11. Раздел **Восстановить на диск** позволяет просматривать, изменять или указывать целевой общий диск или целевого пользователя. Если указать пользователя, данные восстанавливаются в хранилище Google Диск этого пользователя.

    По умолчанию выбран исходный общий диск. Если этот общий диск не существует, или выбрана организация, которая не является исходной, необходимо указать целевой общий диск или целевого пользователя.
12. В поле **Путь** просмотрите или измените целевую папку на целевом общем диске или в хранилище Google Диск целевого пользователя. По умолчанию выбрано исходное хранилище.
13. Выберите, восстанавливать ли разрешения предоставления общего доступа для данных файлов.
14. Щелкните **Запуск восстановления**.
15. Выберите один из вариантов перезаписи файла:
    - **Перезаписывать существующие файлы**
    - **Перезаписывать существующий файл, если он старше**
    - **Не перезаписывать существующие файлы**
16. Щелкните **Продолжить**, чтобы подтвердить решение.

16.5 Нотаризация

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

Нотаризация доступна только для резервных копий файлов Google Диск и файлов общего диска G Suite.

Использование нотаризации

Для включения нотаризации для всех файлов, выбранных для резервного копирования, включите переключатель **Нотаризация** при создании плана резервного копирования.

При настройке восстановления нотаризованные файлы будут помечены значком, и вы сможете верифицировать подлинность файла (стр. 114).

Принципы работы

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

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

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

16.5.1 Проверка подлинности файла с использованием службы нотаризации

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

Проверка подлинности

1. Выполните одно из следующих действий:
   - Для проверки аутентичности файла Google Диск, выберите его, как описано в шагах 1–7 раздела «Восстановление файлов Google Диск» (стр. 186).
   - Для проверки аутентичности файла общего диска учетной записи G Suite, выберите его, как описано в шагах 1–7 темы «Восстановление файлов общего диска» (стр. 190).
2. Убедитесь, что выбранный файл помечен следующим значком:  . Это означает, что файл нотаризован.
3. Выполните одно из следующих действий:
   - Нажмите **Проверить**.

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

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

17 Защита Oracle Database

Защита Oracle Database описана в отдельном документе, который доступен по ссылке https://dl.managed-protection.com/u/pdf/OracleBackup_whitepaper.pdf

Примечание. *Эта функциональность недоступна в Стандартной редакции программы резервного копирования.*

18 Защита SAP HANA

Защита SAP HANA описана в отдельном документе, который доступен по ссылке https://dl.managed-protection.com/u/pdf/SAP%20HANA_backup_whitepaper.pdf

Примечание. *Эта функциональность недоступна в Стандартной редакции программы резервного копирования.*

19 Active Protection

Active Protection обеспечивает защиту системы от программ-вымогателей и криптомайнеров. Программы-вымогатели шифруют файлы и требуют выкуп за предоставление ключа шифрования. Криптомайнеры выполняют математические расчеты в фоновом режиме и таким образом несанкционированно используют вычислительные мощности и сетевой трафик.

Active Protection доступна для машин, работающих под управлением ОС Windows 7 и более поздних версий, а также Windows Server 2008 R2 и более поздних версий. На машине должен быть установлен агент для Windows.

Active Protection доступна для агентов, начиная с версии 12.0.4290. Чтобы обновить агент, следуйте инструкциям в разделе «Обновление агентов» (стр. 36).

Принципы работы

Active Protection контролирует процессы, выполняемые на защищенной машине. Когда сторонний процесс пытается зашифровать файлы или запустить майнинг криптовалют, Active Protection выдает уведомление и выполняет дополнительные действия, заданные в конфигурации.

Кроме того, Active Protection предотвращает несанкционированные изменения собственных процессов программного обеспечения для резервного копирования, записей в реестрах, исполняемых файлов и файлов конфигурации, а также резервных копий в локальных папках.

Для идентификации вредоносных процессов Active Protection использует поведенческую эвристику. Active Protection сравнивает цепочку действий, выполняемых процессом, с цепочками событий, записанными в базе данных вредоносных моделей поведения. Этот подход позволяет Active Protection обнаруживать новые вредоносные программы по их типичному поведению.

Настройки Active Protection

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, подписанныv Microsoft, можно всегда доверять.
- Вредные процессы, которые всегда рассматриваться как связанные с программами-вымогателями. Эти процессы не смогут запуститься, пока на машине включена Active Protection.
- Папки, в которых не будут отслеживаться изменения файлов.

Укажите полный путь к выполняемому процессу, начиная с буквы диска. Например, **`C:\Windows\Temp\er76s7sdkh.exe`**.

Чтобы указать папки, можно использовать подстановочные символы * и ?. Звездочка (*) замещает 0 или более символов. Знак вопроса (?) заменяет только один символ. Нельзя использовать переменные среды, такие как %AppData%.

План Active Protection

Все настройки Active Protection содержатся в плане Active Protection. Этот план можно применить к нескольким машинам.

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

Применение плана Active Protection

1. Выберите машины, для которых необходимо активировать Active Protection.
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**

       Программа выдаст оповещение о процессе.
     - **Остановить процесс** (по умолчанию)

       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, подписанныv 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 резервных копий в локальных папках. Не рекомендуется выключать эту функцию.
   - Измените **Параметры защиты** (стр. 194).
4. После изменения настроек нажмите кнопку **Сохранить настройки**. Изменения будут применены ко всем машинам, на которых включена Active Protection.
5. Нажмите кнопку **Применить**.

19.1 Параметры защиты

Резервные копии

Этот параметр действует, когда в плане Active Protection включен параметр **Самозащита**.

Этот параметр применяется к файлам, которые имеют расширения .tibx, .tib, .tia и расположены в локальных папках.

Этот параметр позволяет указать процессы, которым разрешено изменять файлы резервных копий, даже когда эти файлы защищены самозащитой. Это удобно, например, при удалении файлов резервной копии или их перемещении в другое расположение с помощью сценария.

Значение по умолчанию: **Включено**.

Если этот параметр включен, файлы резервной копии могут быть изменены только процессами, подписанными поставщиком программного обеспечения для резервного копирования. Это позволит программному обеспечению применять правила хранения и удалять резервные копии при поступлении с веб-интерфейса соответствующего запроса от пользователя. Другие процессы (независимо от того, подозрительные они или нет) не могут вносить изменения в резервные копии.

Если этот параметр отключен, можно разрешить другим процессам вносить изменения в резервные копии. Укажите полный путь к выполняемому процессу, начиная с буквы диска.

Защита от криптомайнеров

Этот параметр позволяет включить или отключить выявление потенциальных криптомайнеров в Active Protection.

Значение по умолчанию: **Отключено**.

При выявлении активности, связанной с майнингом криптовалют, выполняется выбранное **Действие при обнаружении** (за исключением отмены изменений файлов на основе данных кэша, поскольку нет объектов для отмены изменений).

Криптомайнеры снижают производительность полезных приложений, повышают расход электроэнергии, могут привести к сбою системы и даже повреждению оборудования из-за нарушений характеристик его работы. Чтобы предотвратить запуск криптомайнеров, рекомендуем добавить их в список **Вредные процессы**.

Подключенные диски

Этот параметр определяет, защищает ли Active Protection сетевые папки, которые подключены как локальные диски.

Этот параметр применяется к папкам, общий доступ к которым предоставлен по SMB или NFS.

Значение по умолчанию: **Включено**.

Если файл изначально расположен на подключенном диске, его невозможно сохранить в исходное расположение, если он извлечен из кэша с помощью действия **Отменить изменения, используя кэш**. Вместо этого он будет сохранен в папку, указанную в настройках этого параметра. По умолчанию используется папка **C:\ProgramData\Acronis\Restored Network Files**. Если эта папка не существует, она будет создана. Если вы хотите изменить путь, необходимо указать локальную папку. Сетевые папки, включая папки на подключенных дисках, не поддерживаются.

20 Защита веб-сайтов и серверов хостинга

20.1 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.
- Можно использовать для веб-сайта несколько планов резервного копирования, но выполняться по расписанию может только один из них. Другие планы должны запускаться вручную.
- Единственный доступный параметр резервного копирования — «Имя файла резервной копии» (стр. 75).

20.1.1 Резервное копирование веб-сайта

Порядок добавления веб-сайта

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**.

Веб-сайт отображается в консоли резервного копирования в разделе **Устройства** > **Веб-сайты**.

Изменение настроек подключения

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

Порядок создания плана резервного копирования для веб-сайтов

1. Выберите веб-сайт или несколько веб-сайтов в разделе **Устройства** > **Веб-сайты**.
2. Нажмите кнопку **Резервное копирование**.
3. (Необязательно.) Включите резервное копирование баз данных.

   Если выбрано несколько веб-сайтов, резервное копирование баз данных по умолчанию отключено.
4. (Необязательно.) Измените правила хранения (стр. 64).
5. (Необязательно.) Включите шифрование резервных копий (стр. 66).
6. (Необязательно.) Щелкните значок шестеренки, чтобы изменить параметр **Имя файла резервной копии** (стр. 75). Это может быть полезно в двух случаях.
   - Если вы ранее создали резервную копию сайта и хотите сохранить текущую последовательность резервного копирования.
   - Если вы хотите, чтобы на вкладке **Резервные копии** отображалось настроенное имя.
7. Нажмите кнопку **Применить**.

Планы резервного копирования веб-сайтов можно изменять, отменять и удалять, как и планы для машин. Эти операции описаны в разделе «Операции с планами резервного копирования» (стр. 129).

20.1.2 Восстановление веб-сайта

Порядок восстановления веб-сайта

1. Выполните одно из следующих действий:
   - В разделе **Устройства** > **Веб-сайты** выберите веб-сайт, который необходимо восстановить, и нажмите **Восстановление**.

     Можно выполнить поиск веб-сайтов по имени. Подстановочные символы не поддерживаются.
   - Если сайт удален, выберите его в разделе **Резервные копии приложений в облаке** на вкладке Резервные копии (стр. 126) и щелкните **Показать резервные копии**.

Чтобы восстановить удаленный веб-сайт, необходимо добавить его как устройство.

2. Выберите точку восстановления.
3. Щелкните **Восстановить** и выберите объекты, которые необходимо восстановить: **Весь веб-сайт**, **Базы данных** (если применимо) или **Файлы/папки**.

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

Порядок восстановления веб-сайта целиком

1. В разделе **Восстановить на веб-сайт** просмотрите или измените целевой веб-сайт.

   По умолчанию выбран исходный веб-сайт. Если он не существует, необходимо выбрать целевой веб-сайт.
2. Выберите, восстанавливать ли разрешения предоставления общего доступа для выбранных элементов.
3. Щелкните **Начать восстановление** и подтвердите действие.

Порядок восстановления баз данных

1. Выберите базы данных, которые необходимо восстановить.
2. Чтобы загрузить базу данных как файл, щелкните **Загрузить**, выберите расположение для сохранения файла и щелкните **Сохранить**. В противном случае пропустите этот шаг.
3. Нажмите кнопку **Восстановить**.
4. В разделе **Восстановить на веб-сайт** просмотрите или измените целевой веб-сайт.

   По умолчанию выбран исходный веб-сайт. Если он не существует, необходимо выбрать целевой веб-сайт.
5. Щелкните **Начать восстановление** и подтвердите действие.

Порядок восстановления файлов/папок веб-сайта

1. Выберите файлы и папки, которые нужно восстановить.
2. Чтобы загрузить файл, щелкните **Загрузить**, выберите расположение для сохранения файла и щелкните **Сохранить**. В противном случае пропустите этот шаг.
3. Нажмите кнопку **Восстановить**.
4. В разделе **Восстановить на веб-сайт** просмотрите или измените целевой веб-сайт.

   По умолчанию выбран исходный веб-сайт. Если он не существует, необходимо выбрать целевой веб-сайт.
5. Выберите, восстанавливать ли разрешения предоставления общего доступа для выбранных элементов.
6. Щелкните **Начать восстановление** и подтвердите действие.

20.2 Защита серверов веб-хостинга

Администраторы веб-хостинга, которые используют платформы Plesk или cPanel, могут интегрировать их с сервисом резервного копирования.

Интеграция позволяет администратору выполнить следующие действия:

- Создать резервные копии сервера Plesk или cPanel на уровне дисков в облачном хранилище данных.
- Восстанавливать весь сервер, включая все веб-сайты.

- Для Plesk: выполнять фрагментарное восстановление веб-сайтов, отдельных файлов, почтовых ящиков или баз данных.
- Для cPanel: выполнять фрагментарное восстановление веб-сайтов, отдельных файлов, почтовых ящиков, почтовых фильтров, серверов пересылки почты, баз данных и учетных записей.
- Включать возможность самостоятельного восстановления для клиентов Plesk и cPanel.

Интеграция реализуется с помощью расширения сервиса резервного копирования. Чтобы получить расширение для Plesk или cPanel, обратитесь к поставщику сервиса резервного копирования.

Поддерживаемые версии Plesk и cPanel

- Plesk для Linux 17.0 и более поздних версий
- Любая версия cPanel с PHP 5.6 и более поздних версий

Квоты

Каждая резервная копия сервера Plesk или cPanel использует место в рамках квоты **Серверы веб-хостинга**. Если эта квота отключена или имеет место выход за переделы ее превышения, действуют следующие положения:

- Для физического сервера используется квота **Серверы**. Если эта квота отключена или имеет место выход за переделы ее превышения, резервное копирование завершается сбоем.
- Для виртуального сервера используется квота **Виртуальные машины**. Если эта квота отключена или имеет место выход за переделы ее превышения, используется квота **Серверы**. Если эта квота отключена или имеет место выход за переделы ее превышения, резервное копирование завершается сбоем.

21 Специальные операции с виртуальными машинами

21.1 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.

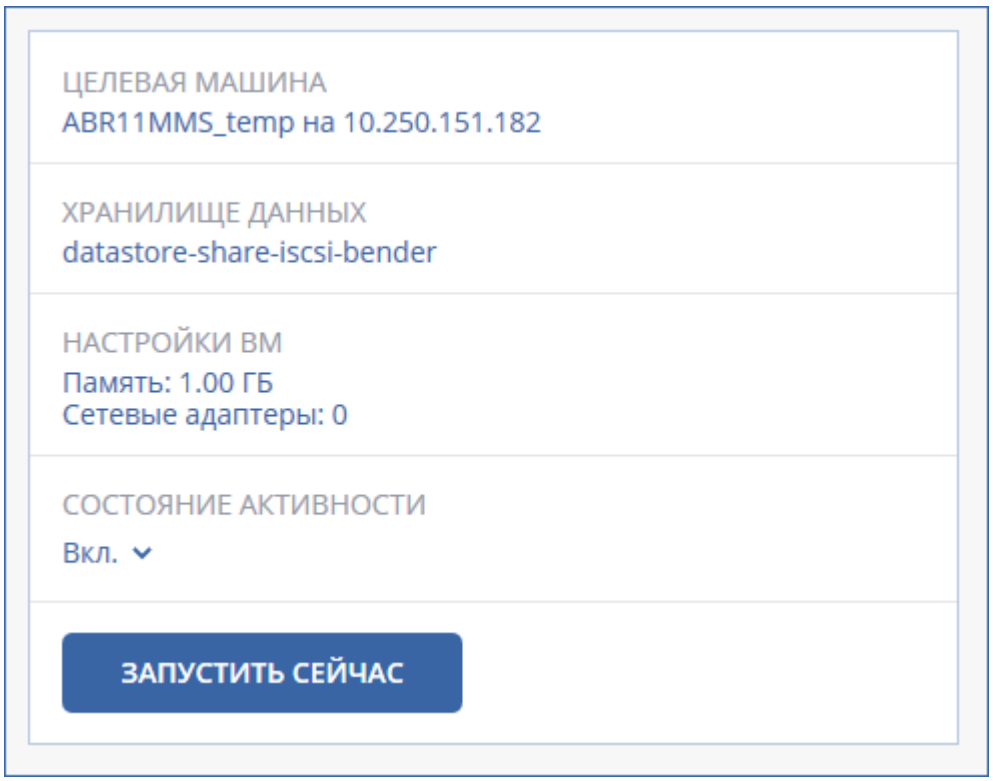
Предварительные требования

- 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.
- Резервные копии с логическими томами Linux (LVM) должны создаваться агентом для VMware или агентом для Hyper-V. При этом тип виртуальной машины должен быть идентичен типу исходной машины (ESXi или Hyper-V).

21.1.1 Запуск машины

1. Выполните одно из следующих действий:
   - Выберите машину, для которой создана резервная копия, выберите **Восстановление** и выберите точку восстановления.
   - Выберите точку восстановления на вкладке «Резервные копии» (стр. 126).
2. Щелкните **Запустить как ВМ**.

Программа автоматически выберет хост и другие требуемые параметры.



3. [Необязательно] Щелкните **Целевая машина**, затем измените тип виртуальной машины (ESXi или Hyper-V), хост или имя виртуальной машины.
4. [Необязательно] Щелкните **Хранилище данных** для ESXi или **Путь** для Hyper-V и выберите хранилище данных для виртуальной машины.

   Изменения, внесенные в виртуальные диски, накапливаются, пока машина запущена. Убедитесь, что в выбранном хранилище данных достаточно свободного пространства. Если вы намерены сохранить эти изменения, сделав виртуальную машину постоянной (стр. 202), выберите хранилище данных, подходящее для запуска машины в рабочей среде.
5. [Необязательно] Щелкните **Настройки ВМ**, чтобы изменить размер памяти и сетевые подключения виртуальной машины.
6. [Необязательно] Выберите состояние активности ВМ (**Включено**/**Выключено**).
7. Щелкните **Запустить сейчас**.

В результате этого машина появляется в веб-интерфейсе с одним из следующих значков:  или 

. Такие виртуальные машины невозможно выбрать для резервного копирования.

21.1.2 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.

21.1.3 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.

Эту машину можно сделать постоянной, то есть восстановить все ее виртуальные диски вместе с изменениями, внесенными при работе машины, в хранилище данных, в котором хранятся эти изменения. Этот процесс называется финализацией.

Финализация выполняется без простоя. При выполнении финализации виртуальная машина *не* выключается.

Расположение окончательных виртуальных жестких дисков определяется в параметрах операции **Запустить как ВМ** (стр. 200) (**Хранилище данных** для ESXi или **Путь** для Hyper-V). Прежде чем запускать финализацию, что свободное место, возможности предоставления общего доступа и производительность этого хранилища данных позволяют запустить машину в рабочей среде.

Примечание. *Финализация не поддерживается для Hyper-V, который выполняется в Windows Server 2008/2008 R2 и Microsoft Hyper-V Server 2008/2008 R2, поскольку в этих версиях Hyper-V отсутствует необходимый API.*

Порядок финализации машины, которая запущена из резервной копии

1. На вкладке **Все устройства** выберите машину, которая запущена из резервной копии.
2. Щелкните **Финализировать**.
3. [Необязательно] Укажите новое имя для данной машины.
4. [Необязательно] Измените режим распределения ресурсов диска. По умолчанию задана настройка **Экономное**.
5. Щелкните **Финализировать**.

Имя машины сразу же меняется. Ход выполнения восстановления показан на вкладке **Действия**. После выполнения восстановления значок машины меняется на значок постоянной виртуальной машины.

Полезная информация о финализации

Сравнение финализации и обычного восстановления

Процесс финализации выполняется медленнее обычного восстановления по указанным ниже причинам:

- При выполнении финализации агент в случайном порядке выбирает разные части резервной копии. При восстановлении всей машины агент считывает данные из резервной копии последовательно.
- Если при выполнении финализации запущена виртуальная машина, агент считывает данные из резервной копии более часто. Это необходимо для одновременной поддержки обоих процессов. При обычном восстановлении виртуальная машина останавливается.

Финализация машин, запушенных из резервных копий в облаке

Из-за интенсивного доступа к данным в резервных копиях скорость финализации сильно зависит от пропускной способности подключения между хранилищем резервных копий и агентом. Для резервных копий, расположенных в облаке, финализация будет выполняться медленнее, чем для локальных резервных копий. При медленном или нестабильном подключении к Интернету финализация машины, которая выполняется из резервной копии в облаке, может завершиться сбоем. Если вы планируете выполнять финализацию, рекомендуем запускать виртуальные машины с локальных резервных копий (при наличии такой возможности).

21.2 Работа в VMware vSphere

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

21.2.1 Репликация виртуальных машин

Репликация доступна только для виртуальных машин VMware ESXi.

Репликация — это процесс создания точной копии (реплики) виртуальной машины с последующей поддержкой реплики в синхронизированном состоянии с исходной машиной. Репликация критически важных машин позволяет всегда иметь копию этой машины в готовом к запуску состоянии.

Репликацию можно запустить вручную или по расписанию, которое определяется пользователем. Первая репликация является полной (выполняется копирование всей машины). Все последующие репликации являются инкрементными и выполняются с помощью функции Changed Block Tracking (стр. 207), 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. 205)

  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. 205)

  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.

21.2.1.1 Создание плана репликации

План репликации необходимо создать отдельно для каждой машины. Невозможно применить существующий план к другим машинам.

Порядок создания плана репликации

1. Выберите виртуальную машину для репликации.
2. Нажмите кнопку **Репликация**.

   В программе отображается новый шаблон плана репликации.
3. [Необязательно] Чтобы изменить имя плана репликации, щелкните имя по умолчанию.
4. Щелкните **Целевая машина** и выполните указанные ниже действия:
   a. Выберите, создавать ли новую или использовать уже существующую реплику исходной машины.
   b. Выберите хост ESXi и укажите имя новой реплики или выберите существующую реплику.

      Новая реплика будет иметь имя по умолчанию **[Имя исходной машины]_replica**.
   c. Нажмите кнопку **ОК**.
5. [Только при репликации на новую машину] Щелкните **Хранилище данных** и выберите хранилище данных для виртуальной машины.
6. [Необязательно] Щелкните **Расписание**, чтобы изменить расписание репликации.

   По умолчанию репликация выполняется ежедневно с понедельника по пятницу. Можно выбрать время для запуска репликации.

   Чтобы изменить частоту выполнения репликации, перетащите ползунок и задайте расписание.

   Можно также выполнить следующие действия:

- Задать интервал дат, в течение которого будет использоваться указанное расписание. Установите флажок **Выполнять план в диапазоне дат** и укажите диапазон дат.
- Отключить расписание. В этом случае репликацию можно запустить вручную.

7. [Необязательно] Щелкните значок шестерни, чтобы изменить параметры репликации (стр. 207).
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: 

21.2.1.2 Тестирование реплики

Порядок подготовки реплики к тестированию

1. Выберите реплику для тестирования.
2. Нажмите кнопку **Тестировать реплику**.
3. Нажмите кнопку **Начать тестирование**.
4. Выберите, подключить ли включенную реплику к сети. По умолчанию реплика не будут подключена к сети.
5. [Необязательно] Если выбрано подключение реплики к сети, установите флажок **Остановить исходную виртуальную машину**, чтобы остановить исходную виртуальную машину до включения реплики.
6. Нажмите кнопку **Запустить**.

Порядок остановки тестирования реплики

1. Выберите реплику, для которой выполняется тестирование
2. Нажмите кнопку **Тестировать реплику**.
3. Нажмите кнопку **Остановить тестирование**.
4. Подтвердите операцию.

21.2.1.3 Переход к реплике

Переход с машины к реплике

1. Выберите реплику, к которой необходимо перейти.
2. Щелкните **Действия с репликой**.
3. Щелкните **Переход к реплике**.
4. Выберите, подключить ли включенную реплику к сети. По умолчанию реплика будет подключена к той же сети, что и исходная машина.
5. [Необязательно] Если выбрано подключение реплики к сети, снимите флажок **Остановить исходную виртуальную машину**, чтобы не выключать исходную виртуальную машину.
6. Нажмите кнопку **Запустить**.

При выполнении перехода к реплике можно выбрать одно из указанных ниже действий:

- **Остановить переход к реплике** (стр. 206)

  Остановите переход к реплике, если исходная машина исправлена. Реплика будет выключена. Репликация будет продолжена.

- **Выполнить окончательный переход на реплику** (стр. 206)

  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. 206)

  Выполните возврат из реплики, если выполнен переход на площадку, которая не предназначена для непрерывных операций. Реплика будет восстановлена на исходную или новую виртуальную машину. По окончании восстановления на исходную машину она включается и репликация продолжается. Если выбрано восстановление на новую машину, измените план репликации таким образом, чтобы эта машина была выбрана как исходная.

Остановка перехода к реплике

Порядок остановки перехода к реплике

1. Выберите реплику, к которой выполняется переход.
2. Щелкните **Действия с репликой**.
3. Щелкните **Остановить переход к реплике**.
4. Подтвердите операцию.

Выполнение окончательного перехода на реплику

Порядок выполнения окончательного перехода на реплику

1. Выберите реплику, к которой выполняется переход.
2. Щелкните **Действия с репликой**.
3. Щелкните **Окончательный переход на реплику**.
4. [Необязательно] Измените имя виртуальной машины.
5. [Необязательно] Установите флажок **Остановить исходную виртуальную машину**.
6. Нажмите кнопку **Запустить**.

Возврат из реплики

Порядок выполнения возврата из реплики

1. Выберите реплику, к которой выполняется переход.
2. Щелкните **Действия с репликой**.
3. Щелкните **Возврат из реплики**.

   Данное программное обеспечение автоматически выбирает исходную машину в качестве целевой.
4. [Необязательно] Щелкните **Целевая машина** и выполните следующие действия:
   a. Выберите новую или существующую машину для возврата из реплики.
   b. Выберите хост ESXi и укажите имя новой машины или выберите существующую машину.
   c. Нажмите кнопку **ОК**.
5. [Необязательно] При возврате из реплики на новую машину также можно выполнить следующие действия:
   - Щелкните **Хранилище данных**, чтобы выбрать хранилище данных для виртуальной машины.

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

6. [Необязательно] Щелкните **Параметры восстановления**, чтобы изменить параметры возврата из реплики (стр. 207).
7. Нажмите кнопку **Запуск восстановления**.
8. Подтвердите операцию.

21.2.1.4 Параметры репликации

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

Функция Changed Block Tracking (CBT)

Этот параметр подобен параметру резервного копирования «Changed Block Tracking (CBT)» (стр. 80).

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. 82).

Команды до и после процедуры

Этот параметр подобен параметру резервного копирования «Команды до и после процедуры» (стр. 92).

Служба теневого копирования томов (VSS) для виртуальных машин

Этот параметр подобен параметру резервного копирования «Служба теневого копирования томов (VSS) для виртуальных машин» (стр. 99).

21.2.1.5 Параметры возврата из реплики

Чтобы изменить параметры возврата из реплики, щелкните **Параметры восстановления** при настройке возврата из реплики.

Обработка ошибок

Этот параметр подобен параметру восстановления «Обработка ошибок» (стр. 122).

Производительность

Этот параметр подобен параметру восстановления «Производительность» (стр. 124).

Команды до и после процедуры

Этот параметр подобен параметру восстановления «Команды до и после процедуры» (стр. 124).

Управление питанием ВМ

Этот параметр подобен параметру восстановления «Управление питанием ВМ» (стр. 126).

21.2.1.6 Сохранение первоначальной реплики

Чтобы ускорить репликацию в удаленное расположение и сэкономить пропускную способность сети, можно выполнить сохранение реплики.

Внимание! *Для сохранения реплики агент для VMware (виртуальное устройство) должен работать на целевом хосте ESXi.*

Сохранение первоначальной реплики

1. Выполните одно из следующих действий:
   - Если исходную виртуальную машину можно выключить, сделайте это, а затем перейдите к шагу 4.
   - Если исходную виртуальную машину нельзя выключить, перейдите к следующему шагу.
2. Создайте план репликации (стр. 204).

   При создании плана в разделе **Целевая машина** выберите пункт **Создать реплику** и хост ESXi, на котором размещена исходная машина.
3. Запустите план однократно.

   На исходном хосте ESXi будет создана реплика.
4. Экспортируйте файлы виртуальной машины (или реплики) на внешний жесткий диск.
   a. Подключите внешний жесткий диск к машине, на которой работает клиент vSphere.
   b. Подключите клиент vSphere к исходному хосту vCenter\ESXi.
   c. Выберите только что созданную реплику в списке.
   d. Выберите пункты **Файл** > **Экспорт** > **Экспорт шаблона OVF**.
   e. В поле **Папка** укажите папку на внешнем жестком диске.
   f. Нажмите кнопку **ОК**.
5. Перенесите жесткий диск в удаленное расположение.
6. Импортируйте реплику на целевой хост ESXi.
   a. Подключите внешний жесткий диск к машине, на которой работает клиент vSphere.
   b. Подключите клиент vSphere к целевому хосту vCenter\ESXi.
   c. Выберите пункт **Файл** > **Развернуть шаблон OVF**.
   d. В поле **Развернуть из файла или URL-адреса** укажите шаблон, экспортированный на шаге 4.
   e. Завершите процедуру импорта.
7. Измените план репликации, созданный на шаге 2. В поле **Целевая машина** выберите значение **Существующая реплика**, а затем выберите импортированную реплику.

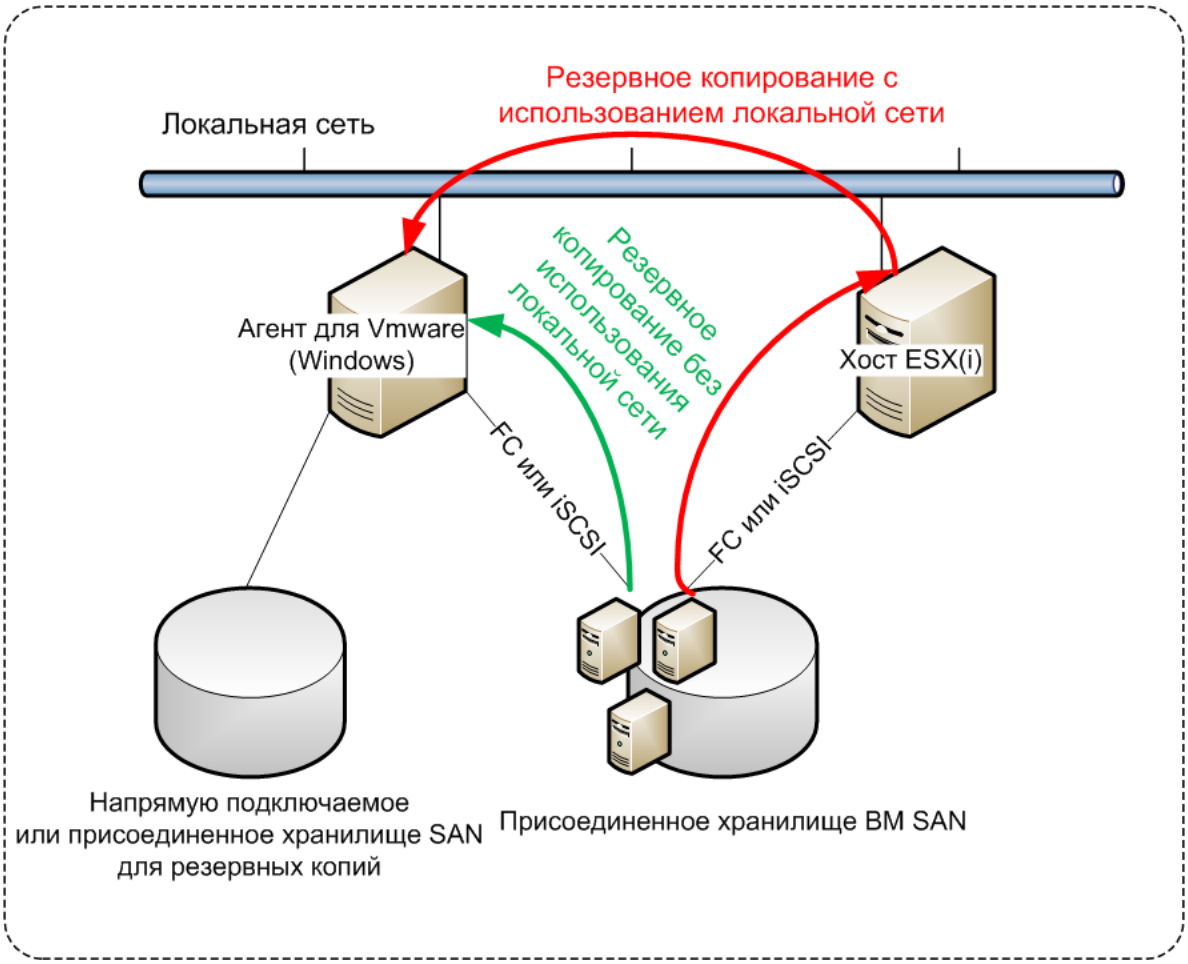
В результате программа продолжит обновлять реплику. Все репликации будут инкрементными.

21.2.2 Агент для VMware — резервное копирование без использования локальной сети

Если с ESXi используется SAN-хранилище, установите агент на машину, подключенную к той же сети SAN. Агент будет создавать резервные копии виртуальных машин прямо из хранилища

данных, а не через хост ESXi и локальную сеть. Эта возможность называется резервным копированием без использования локальной сети.

На следующем рисунке показано резервное копирование с использованием и без использования локальной сети. Доступ к виртуальным машинам без использования локальной сети возможен при наличии оптоволоконного канала (FC) или сети хранения данных (SAN) iSCSI. Чтобы полностью исключить передачу резервных копий данных по локальной сети, храните резервные копии на локальном диске машины с установленным агентом или в присоединенном хранилище SAN.



Порядок включения прямого доступа к хранилищу данных для агента.

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

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

Ограничения

- В vSphere 6.0 и более поздней версии агент не может использовать режим транспорта SAN, если одни диски ВМ расположены в VMware Virtual Volume (VVol), а другие — на других томах. Резервное копирование таких виртуальных машин приведет к сбою.
- Резервное копирование зашифрованных виртуальных машин (эта функциональная возможность представлена в VMware vSphere 6.5) будет выполняться по локальной сети, даже если настроен режим транспорта сети SAN для агента. Агент выполнит возврат из реплики, используя транспорт NBD, поскольку VMware не поддерживает транспорт сети SAN для резервного копирования зашифрованных виртуальных дисков.

Пример

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

Настройка политики SAN

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

Настройка инициатора iSCSI

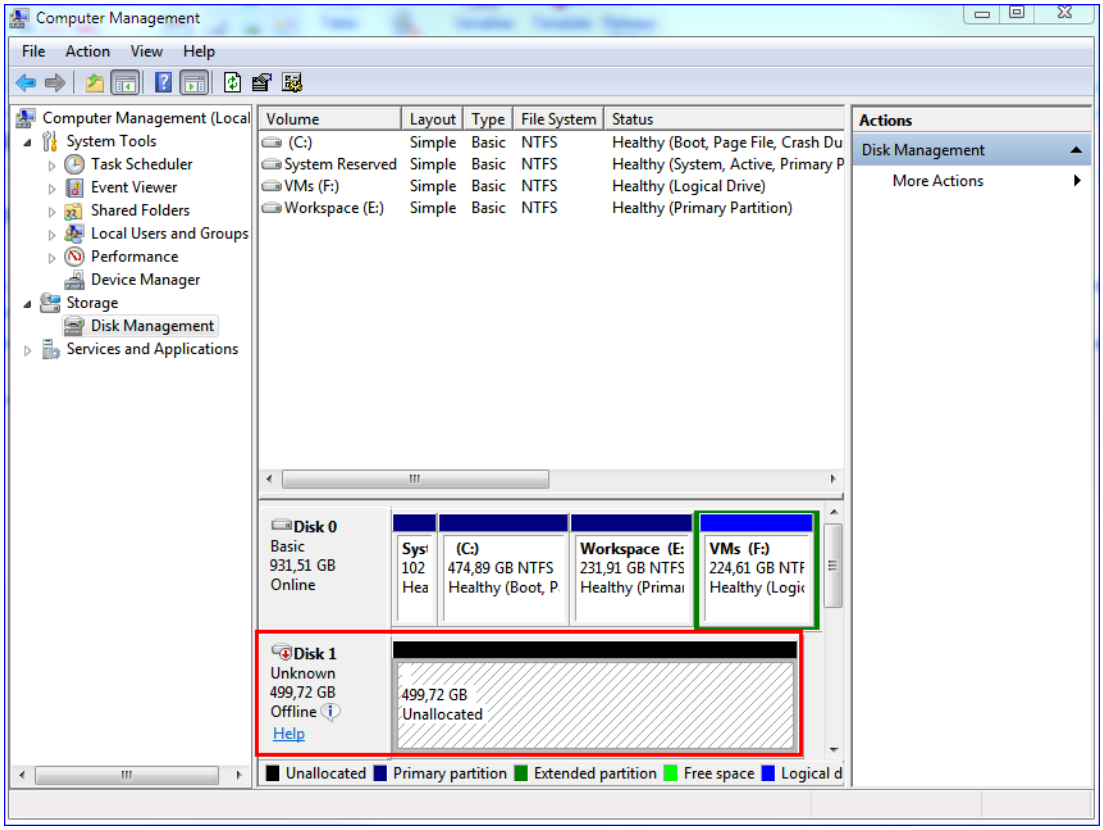
1. Последовательно выберите пункты **Панель управления** > **Администрирование** > **Инициатор iSCSI**.

   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.



21.2.3 Использование локально присоединенного хранилища

К агенту для виртуального устройства VMware можно подключить дополнительный диск, чтобы агент мог создавать резервные копии в этом локальном хранилище. Этот подход устраняет сетевой трафик между агентом и хранилищем резервных копий.

Виртуальное устройство, которое выполняется на одном хосте или в одном кластере с виртуальными машинами, для которых созданы резервные копии, имеет прямой доступ к хранилищам данных, в которых расположены эти машины. Это означает, что устройство может присоединить диски, для которых созданы резервные копии, используя транспорт HotAdd. В этом случае трафик резервного копирования направляется от одного локального диска к другому. Если хранилище данных подключено как **диск/логическое устройство (LUN)**, а не как **NFS**, резервная копия будет работать без использования локальной сети. В случае хранилища данных NFS, будет иметь место сетевой трафик между хранилищем данных и хостом.

При использовании локально присоединенного хранилища предполагается, что агент всегда создает резервную копию для одних и тех же машин. Если несколько агентов работают в рамках vSphere и один или несколько из них используют локально присоединенные хранилища, необходимо вручную привязать (стр. 212) каждый агент ко всем машинам, для которых он должен создавать резервные копии. В противном случае, если сервер управления произведет перераспределение машин среди агентов, резервные копии машин могут оказаться рассредоточенными по нескольким хранилищам.

Можно добавить хранилище к уже работающему агенту или сделать это при развертывании агентаиз шаблона OVF (стр. 33).

Как прикрепить хранилище к уже работающему агенту

1. В списке VMware vSphere щелкните правой кнопкой мыши агент для виртуального устройства VMware.
2. Добавьте диск путем внесения изменений в параметры виртуальной машины. Размер диска должен составлять по меньшей мере 10 ГБ.

   Предупреждение *Необходимо соблюдать осторожность при добавлении уже существующего диска. После создания хранилища все данные, содержавшиеся ранее на этом диске, будут потеряны.*
3. Перейдите на консоль виртуального устройства. Ссылка **Создать хранилище** доступна в нижней части экрана. Если этого не происходит, нажмите **Обновить**.
4. Нажмите ссылку **Создать хранилище**, выберите диск и укажите для него метку. Длина метки ограничена 16 символами в связи с ограничениями файловой системы.

Как выбрать локально присоединенное хранилище в качестве места назначения резервной копии

При создании плана резервного копирования (стр. 41), в **Место сохранения резервной копии** выберите **Локальные папки** и введите букву диска, соответствующую локально присоединенному хранилищу, например**D:**.

21.2.4 Привязка виртуальной машины

В этом разделе показано, как сервис резервного копирования организует работу нескольких агентов в VMware vCenter.

Нижеуказанный алгоритм распределения работает как для виртуальных устройств, так и для агентов, установленных в Windows.

Алгоритм распределения

Виртуальные машины автоматически равномерно распределяются между агентами для VMware. Под равномерностью имеется в виду, что все агенты управляют равным количеством машин. Объем пространства, занимаемого в хранилище виртуальной машиной, не учитывается.

При выборе агента для машины программное обеспечение пытается оптимизировать общую производительность системы. В частности, программное обеспечение учитывает расположение агента и виртуальной машины. Предпочтительным является агент, размещенный на том же хосте. Если на том же хосте агента нет, по возможности выбирается агент из того же кластера.

Когда виртуальная машина назначается агенту, все централизованные резервные копии этой машины делегируются этому агенту.

Перераспределение

Перераспределение происходит каждый раз, когда нарушается этот баланс, или, точнее, когда дисбаланс нагрузки между агентами достигает 20 процентов. Это может произойти при добавлении или удалении машины или агента, при переносе машины на другой хост или в другой кластер или если машина привязывается к агенту вручную. В этом случае сервис резервного копирования перераспределяет машины с помощью одного алгоритма.

Например, вы понимаете, что для необходимой пропускной способности требуется больше агентов, и развертываете в кластере дополнительное виртуальное устройство. Сервис

резервного копирования назначит новому агенту наиболее подходящие машины. Нагрузка на старые агенты уменьшится.

Если агент удаляется из сервиса резервного копирования, то машины, назначенные этому агенту, распределяются между оставшимися агентами. Однако этого не произойдет, если агент поврежден или вручную удален из vSphere. Перераспределение начнется только после удаления такого агента из веб-интерфейса.

Просмотр результата распределения

Можно просмотреть результат автоматического распределения:

- в столбце **Агент** для каждой виртуальной машины в разделе **Все устройства**;
- в разделе **Назначенные виртуальные машины** на панели **Сведения** при выборе агента в разделе **Настройки** > **Агенты**.

Привязка вручную

Привязка агента для VMware позволяет исключить виртуальную машину из этого процесса распределения, указав агент, который должен всегда выполнять резервное копирование этой машины. Общий баланс будет поддерживаться, но конкретная машина может быть передана другому агенту только в случае удаления исходного агента.

Порядок привязки машины к агенту

1. Выберите машину.
2. Нажмите **Сведения**.

   В разделе**Назначенные агенты** программное обеспечение отобразит агент, который в данный момент управляет выбранной машиной.
3. Нажмите **Изменить**.
4. Выберите **Вручную**.
5. Выберите агент, к которому вы хотите привязать машину.
6. Нажмите кнопку **Сохранить**.

Как отвязать машину от агента

1. Выберите машину.
2. Нажмите **Сведения**.

   В разделе**Назначенные агенты** программное обеспечение отобразит агент, который в данный момент управляет выбранной машиной.
3. Нажмите **Изменить**.
4. Выберите **Автоматически**.
5. Нажмите кнопку **Сохранить**.

Отключение автоматического назначения для агента

Для отключения автоматического назначения для агента VMware, чтобы исключить его из процесса распределения, укажите список машин, для которых этот агент должен выполнять резервное копирование. Прочие агенты будут поддерживать общий баланс.

Невозможно отключить автоматическое назначение для агента при отсутствии прочих зарегистрированных агентов или при отключенном автоматическом назначении для прочих агентов.

Отключение автоматического назначения для агента

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

2. Выберите агент для VMware, для которого вы хотите отключить автоматическое назначение.
3. Нажмите **Сведения**.
4. Отключите **Автоматическое назначение**, нажав на переключатель.

Примеры использования

- Привязка вручную может быть удобна если необходимо, чтобы агент для VMware (Windows) создал резервную копию конкретной (очень большой) машины через волоконный канал, тогда как резервные копии других машин создаются виртуальными устройствами.
- Виртуальные машины необходимо привязать к агенту, если к агенту локально прикреплено хранилище. (стр. 211)
- Отключение автоматического назначения дает возможность убедиться в том, что резервное копирование конкретной машины гарантировано будет проходить по указанному вами расписанию. Агент, отвечающий за резервное копирование только одной машины, не может быть привлечен к резервному копированию других машин в запланированное время.
- Отключение автоматического назначения полезно при наличии нескольких географически разделенных хостов ESXi. При отключении автоматического назначения и последующей привязке виртуальных машин на каждом хосте к агенту, запущенному на том же хосте вы можете быть уверены, что агент не будет выполнять резервное копирование машин, запущенных на удаленных хостах ESXi, что позволит сэкономить сетевой трафик.

21.2.5 Поддержка миграции VM

В этом разделе рассказывается об особенностях миграции виртуальных машин в среде vSphere, включая перемещение виртуальных машин между узлами ESXi, входящими в кластер vSphere.

vMotion

vMotion перемещает состояние и конфигурацию виртуальной машины на другой хост. При этом диски машины остаются в той же папке общего хранилища данных.

- Функциональная возможность vMotion агента для VMware (виртуальное устройство) не поддерживается и отключена.
- Функциональная возможность vMotion виртуальной машины отключена при выполнении резервного копирования. Выполнение резервного копирования будет продолжено после завершения миграции.

Storage vMotion

Storage vMotion перемещает диски виртуальной машины из одного хранилища данных в другое.

- Функциональная возможность Storage vMotion агента для VMware (виртуальное устройство) не поддерживается и отключена.
- Функциональная возможность Storage vMotion виртуальной машины отключена при выполнении резервного копирования. Процессы резервного копирования продолжат выполняться после миграции.

21.2.6 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** выберите **VMware**.
2. Выберите **Хосты и кластеры**.
3. В списке **Хосты и кластеры** (справа от дерева **Хосты и кластеры**) выберите vCenter Server или автономный хост ESXi, который был указан при установке агента для VMware.
4. Нажмите **Сведения**.
5. В области **Учетные данные** выберите имя пользователя.
6. Укажите новые учетные данные доступа, а затем нажмите кнопку **ОК**.

21.2.7 Просмотр статуса резервного копирования в клиенте vSphere

Можно просмотреть статус резервного копирования и время создания последней резервной копии виртуальной машины в клиенте vSphere.

Эти сведения появляются в сводке по виртуальной машине (**Сводка** > **Настраиваемые атрибуты**/**Аннотации**/**Примечания** в зависимости от типа клиента и версии vSphere). Можно также включить столбцы **Последняя резервная копия** и **Состояние резервного копирования** на вкладке **Виртуальные машины** для любого хоста, ЦОД, папки, пула ресурсов или для всего экземпляра vCenter Server.

Для предоставления этих атрибутов, помимо прав, описанных в разделе «Агент для VMware — необходимые привилегии» (стр. 215), агенту для VMware должны быть предоставлены следующие права:

- **Глобальные** > **Управление настраиваемыми атрибутами**
- **Глобальные** > **Настройка настраиваемых атрибутов**

21.2.8 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. 215).

		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**		+	+	+
	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		+		

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

		Операция			
Объект	**Привилегия**	**Резервное копирование ВМ**	**Восстановление в новую ВМ**	**Восстановление в существующую ВМ**	**Запуск ВМ из резервной копии**
Виртуальная машина > Распределение	**Разрешение доступа к диску**		+	+	+
	Разрешение доступа к диску только для чтения	+		+	
	Разрешение загрузки ВМ	+	+	+	+
Виртуальная машина > Состояние	**Создание моментального снимка**	+		+	+
	Удаление снимка	+		+	+
Импорт	**Добавить виртуальную машину**				+

* Эта привилегия требуется только для резервного копирования зашифрованных машин.

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

21.3 Резервное копирование кластеризованных машин Hyper-V

В кластере Hyper-V виртуальные машины могут мигрировать между узлами кластера. Следуйте приведенным ниже рекомендациям для настройки правильного резервного копирования кластеризованных машин Hyper-V.

1. Машина должна быть доступна для резервного копирования независимо от того, на какой узел она переносится. Чтобы убедиться в том, что агент для Hyper-V имеет доступ к машине на любом узле, необходимо запустить службу агента (стр. 29) под учетной записью пользователя домена с правами администратора на каждом из узлов кластера.

   Рекомендуется указать такую учетную запись для службы агента в процессе установки агента для Hyper-V.
2. Установите агент для Hyper-V на каждом узле кластера.
3. Зарегистрируйте все агенты в службе резервного копирования.

Высокая доступность восстановленной машины

При восстановлении резервных копий дисков на *существующей* виртуальной машине Hyper-V свойство высокой доступности данной машины остается без изменений.

В случае восстановления резервных копий дисков на *новой* виртуальной машине Hyper-V целевая виртуальная машина не обладает свойством высокой доступности. Она считается запасной и обычно выключена. Если машину необходимо использовать в производственной среде, можно настроить для нее свойство высокой доступности с помощью оснастки **Управление отказоустойчивым кластером**.

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

Параметр **планирования** (стр. 96) резервного копирования определяет, для какого количества виртуальных машин агент может одновременно осуществлять резервное копирование при выполнении заданного плана резервного копирования.

Если несколько планов резервного копирования пересекаются по времени, указанные в их параметрах числа суммируются. Хотя суммарное количество программным образом ограничено до 10, пересечение планов может влиять на производительность резервного копирования, а также оказывать избыточную нагрузку на хранилище хоста и виртуальной машины.

Вы можете дополнительно ограничить общее количество виртуальных машин, для которых агент для VMware или агент для Hyper-V может одновременно создавать резервные копии.

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

1. На машине, на которой запущен агент, создайте новый текстовый документ и откройте его в текстовом редакторе, например в Блокноте.
2. Скопируйте и вставьте в этот файл следующие строки:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\MMS\Configuration\ManagedMachine\SimultaneousBackupsLimits]
"MaxNumberOfSimultaneousBackups"=dword:00000001
```

3. Вместо `00000001` укажите нужное ограничение в шестнадцатеричном формате. Например `00000001` означает 1, а `0000000A` — 10.
4. Сохраните документ под именем **limit.reg**.
5. Запустите файл от имени администратора.
6. Подтвердите изменение реестра Windows.
7. Выполните указанные ниже действия, чтобы перезапустить агент.
   a. В меню **Пуск** выберите команду **Выполнить** и введите: **cmd**
   b. Нажмите кнопку **ОК**.
   c. Выполните следующие команды:

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

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

1. Чтобы запустить командную оболочку, в пользовательском интерфейсе виртуального устройства нажмите клавиши CTRL+SHIFT+F2.
2. Откройте файл **/etc/Acronis/MMS.config** в текстовом редакторе, например в **vi**.
3. Найдите следующий раздел:

```
<key name="SimultaneousBackupsLimits">
    <value name="MaxNumberOfSimultaneousBackups" type="Tdword">"10"</value>
</key>
```

4. Вместо `10` укажите нужное ограничение в десятичном формате.
5. Сохраните файл.
6. Чтобы перезапустить агент, выполните команду **`reboot`**.

21.5 Миграция машины

Можно выполнить миграцию машины, восстановив ее резервную копию на машину, которая не является исходной.

Доступные варианты выполнения миграции приведены в следующей таблице.

Тип архивированной машины	**Доступные места восстановления**				
	Физическая машина	Виртуальная машина ESXi	Виртуальная машина Hyper-V	Виртуальная машина Virtuozzo	Контейнер Virtuozzo
Физическая машина	+	+	+	–	–
Виртуальная машина VMware ESXi	+	+	+	–	–
Виртуальная машина Hyper-V	+	+	+	–	–
Виртуальная машина Virtuozzo	+	+	+	+	–
Контейнер Virtuozzo	–	–	–	–	+

Инструкции о выполнении миграции см. в следующих разделах:

- Миграция систем с физической машины на виртуальную (P2V): Миграция систем с физической машины на виртуальную (стр. 104)
- Миграция систем с виртуальной машины на виртуальную (V2V): Виртуальная машина (стр. 106)
- Миграция систем с виртуальной машины на физическую (V2P): Виртуальная машина (стр. 106) или Восстановление дисков с помощью загрузочного носителя (стр. 108)

Хотя можно выполнить миграцию V2P в веб-интерфейсе, в определенных случаях рекомендуется использовать загрузочный носитель. Иногда вы можете создать носитель для миграции в ESXi или Hyper-V.

Носитель позволяет выполнить следующие действия:

- Выполнить миграцию P2V, миграцию V2P или миграцию V2V с Virtuozzo или машины Linux с логическими томами (LVM). Используйте агент для Linux или загрузочный носитель, чтобы создать резервную копию, и загрузочный носитель для восстановления.
- Предоставить драйверы для определенного оборудования, которое имеет критически важное значения для загружаемости системы.

21.6 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. 103). При настройке восстановления выберите новую машину в качестве целевой.

22 Группы устройств

Примечание. *Эта функциональность недоступна в Стандартной редакции программы резервного копирования.*

Группы устройств призваны обеспечить простое управление большим количеством зарегистрированных устройств.

Вы можете применить план резервного копирования к группе. После появления нового устройства в группе, это устройство будет защищено планом. Если устройство удалено из группы, оно больше не будет защищено планом. Если план применим к группе, нельзя отменить его применение к одному из членов группы, только ко всей группе.

В группу могут быть добавлены устройства только одного типа. Например в **Hyper-V** вы можете создать группу виртуальных машин Hyper-V. В разделе **Машины с агентами** можно создать группу машин с установленными агентами. В разделе **Все устройства** невозможно создать группу.

Одно устройство может входить в несколько групп.

Встроенные группы

После регистрации устройства оно появляется в одной из встроенных корневых групп на вкладке **Устройства**.

Корневые группы *невозможно* редактировать или удалить. *Невозможно* применить план к корневым группам.

Некоторые корневые группы содержат встроенные подкорневые группы. Такие группы *невозможно* редактировать или удалить. Однако *возможно* применить планы к подкорневым встроенным группам.

Пользовательские группы

Защита всех устройств во встроенной группе с помощью одного плана резервного копирования может быть неудовлетворительной из-за разных ролей машин. У каждого отдела есть свои данные для резервного копирования. Для некоторых данных резервные копии требуется создавать часто, тогда как для других — пару раз в год. Поэтому может потребоваться создать различные планы резервного копирования, применяющиеся на разных группах машин. В этом случае следует рассмотреть возможность создания пользовательских групп.

Пользовательская группа может включать одну или несколько вложенных групп. Любую пользовательскую группу можно изменить или удалить. Существует несколько типов пользовательских групп.

- **Статические группы**

  Статические группы содержат машины, добавленные вручную. Состав статической группы меняется, только если вы специально добавите или удалите машину.

  Пример. Вы создали пользовательскую группу для отдела бухгалтерии и вручную добавили в группу машины бухгалтеров. Когда к этой группе будет применен план резервного копирования, машины сотрудников бухгалтерии будут защищены. Если в отдел пришел новый сотрудник, следует включить его машину в эту группу вручную.

- **Динамические группы**

  Динамические группы содержат машины, добавленные автоматически в соответствии с поисковыми критериями, определенными при создании группы. Состав динамической группы меняется автоматически. Машина остается в группе до тех пор, пока отвечает заданным критериям.

  Пример 1. Имена хостов машин, принадлежащих к отделу бухгалтерии, содержат слово «бухгалтерия». Достаточно задать часть имени машины в качестве критерия членства в группе и применить к этой группе план резервного копирования. Машина нового бухгалтера добавляется в группу сразу после регистрации. Таким образом она будет автоматически защищена.

  Пример 2. Отдел бухгалтерии формирует отдельную организационную единицу Active Directory (OU). Укажите организационную единицу бухгалтерии как критерий членства в группе и примените к данной группе план резервного копирования. Машина нового бухгалтера добавляется в группу сразу после регистрации и добавления к организационной единице независимо от того, какое действие выполняется первым. Таким образом она будет автоматически защищена.

22.1 Создание статической группы

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

   Новая группа появится на дереве групп.

22.2 Добавление устройств в статические группы

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

Программное обеспечение отобразит дерево групп, в которые можно добавить выбранное устройство.

3. Если требуется создать новую группу, выполните следующие действия. В противном случае пропустите этот шаг.
   a. Выберите группой, в которой необходимо создать группу.
   b. Нажмите кнопку **Новая группа**.
   c. Укажите имя группы и затем нажмите кнопку **ОК**.
4. Выберите группу, в которую необходимо добавить устройство, а затем нажмите кнопку **Выполнено**.

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

22.3 Создание динамической группы

1. Нажмите **Устройства**и выберите группу, которая содержит устройства, для которых необходимо создать динамическую группу.
2. Выполните поиск устройств с помощью поля поиска. Можно использовать составные условия поиска и операторы, описанные ниже.
3. Щелкните **Сохранить как** рядом с полем поиска.
4. Укажите имя группы, а затем щелкните **ОК**.

Условия поиска

Доступные условия поиска приведены в следующей таблице.

Критерий	Значение	Примеры поисковых запросов
`name`	▪ Имя хоста для физических машин ▪ Имя для виртуальных машин ▪ Имя базы данных ▪ Адрес электронной почты для почтовых ящиков	`name = 'ru-00'`
`comment`	Комментарий для устройства. Значение по умолчанию: ▪ Для физических машин с ОС Windows описание компьютера считывается в свойствах компьютера в Windows. ▪ Пусто для других устройств. Чтобы просмотреть комментарий, в разделе **Устройства** выберите устройство и щелкните **Подробнее**, затем перейдите к разделу **Комментарий**. Чтобы добавить или изменить комментарий, щелкните **Добавить** или **Изменить**.	`comment = 'important machine'` `comment = ''` (все машины без комментария)
`ip`	IP-адрес (только для физических машин)	`ip RANGE ('10.250.176.1','10.250.176.50')`

Критерий	Значение	Примеры поисковых запросов
memorySize	Размер ОЗУ в мегабайтах (Мб)	**memorySize < 1024**
insideVm	Виртуальная машина с агентами в ней. Возможные значения: ▪ **true** ▪ **false**	**insideVm = true**
osName	Название операционной системы.	**osName LIKE '%Windows XP%'**
osType	Тип операционной системы. Возможные значения: ▪ **'windows'** ▪ **'linux'** ▪ **'macosx'**	**osType IN ('linux', 'macosx')**
osProductType	Тип продукта операционной системы. Возможные значения: ▪ **'dc'** Означает контроллер домена. ▪ **'server'** ▪ **'workstation'**	**osProductType = 'server'**
tenant	Название отдела, которому принадлежит устройство.	**tenant = 'Unit 1'**
tenantId	Идентификатор отдела, которому принадлежит устройство. Для получения идентификатора отдела напротив пункта **Устройства** выберите устройство и выберите пункт **Сведения** > **Все свойства**. Идентификатор отобразится в поле **ownerId**.	**tenantId = '3bfe6ca9-9c6a-4953-9cb2-a1323f454fc9'**

Критерий	Значение	Примеры поисковых запросов
state	Состояние устройства. Возможные значения: ▪ **'idle'** ▪ **'interactionRequired'** ▪ **'canceling'** ▪ **'backup'** ▪ **'recover'** ▪ **'install'** ▪ **'reboot'** ▪ **'failback'** ▪ **'testReplica'** ▪ **'run_from_image'** ▪ **'finalize'** ▪ **'failover'** ▪ **'replication'** ▪ **'createAsz'** ▪ **'deleteAsz'** ▪ **'resizeAsz'**	**state = 'backup'**
protectedByPlan	Устройство защищено посредством плана резервного копирования с указанным идентификатором. Для получения идентификатора плана нажмите **Планы** > **Резервное копирование**, выберите план, нажмите на диаграмму в колонке **Статус** и затем нажмите на статус. Будет создан новый поиск с идентификатором плана.	**protectedByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'**
okByPlan	Устройства, защищенные посредством плана резервного копирования с указанным идентификатором и со статусом **OK**.	**okByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'**
errorByPlan	Устройства, защищенные посредством плана резервного копирования с указанным идентификатором и со статусом **Ошибка**.	**errorByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'**
warningByPlan	Устройства, защищенные посредством плана резервного копирования с указанным идентификатором и со статусом **Внимание**.	**warningByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'**

Критерий	Значение	Примеры поисковых запросов
runningByPlan	Устройства, защищенные посредством плана резервного копирования с указанным идентификатором и со статусом **Выполняется**.	**runningByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'**
interactionByPlan	Устройства, защищенные посредством плана резервного копирования с указанным идентификатором и со статусом **Требуется вмешательство**.	**interactionByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'**
ou	Машины, которые принадлежат к указанной организационной единице Active Directory.	**ou IN ('RnD', 'Computers')**
id	Идентификатор устройства. Для получения идентификатора устройства напротив пункта **Устройства** выберите устройство и выберите пункт **Сведения** > **Все свойства**. Идентификатор отобразится в поле **id**.	**id != '4B2A7A93-A44F-4155-BDE3-A023C57C9431'**
lastBackupTime	Дата и время последнего успешного создания резервной копии. Формат данных следующий: 'ГГГГ-ММ-ДД ЧЧ:ММ'.	**lastBackupTime > '2016-03-11'** **lastBackupTime <= '2016-03-11 00:15'** **lastBackupTime is null**
lastBackupTryTime	Время последней попытки резервного копирования. Формат данных следующий: 'ГГГГ-ММ-ДД ЧЧ:ММ'.	**lastBackupTryTime >= '2016-03-11'**
nextBackupTime	Время следующего резервного копирования. Формат данных следующий: 'ГГГГ-ММ-ДД ЧЧ:ММ'.	**nextBackupTime >= '2016-03-11'**
agentVersion	Версия установленного агента резервного копирования.	**agentVersion LIKE '12.0.*'**
hostId	Внешний идентификатор агента резервного копирования. Для получения идентификатора агента резервного копирования напротив пункта **Устройства** выберите машину и выберите пункт **Сведения** > **Все свойства**. Используйте значение **"id"** свойства **agent**.	**hostId = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'**

Операторы

Доступные операторы приведены в следующей таблице.

Оператор	Значение	Примеры
AND	Логический оператор конъюнкции.	**name like 'ru-00' AND tenant = 'Unit 1'**

Оператор	Значение	Примеры
OR	Логический оператор дизъюнкции.	**state = 'backup' OR state = 'interactionRequired'**
NOT	Логический оператор отрицания.	**NOT(osProductType = 'workstation')**
LIKE 'шаблон подстановочного символа'	Этот оператор используется для проверки того, соответствует ли выражение шаблону подстановочного символа. В этом параметре не учитывается регистр. Могут быть использованы следующие операторы подстановочного знака: ▪ * или % Астериск или знак процента могут заменять собой ни одного, один или несколько символов. ▪ _ Нижнее подчеркивание может заменять собой один символ.	**name LIKE 'ru-00'** **name LIKE '*ru-00'** **name LIKE '*ru-00*'** **name LIKE 'ru-00_'**
IN (<значение1>,...<значениеN>**)**	Этот оператор используется для проверки того, соответствует ли выражение любому значению из указанного списка значений. В этом параметре учитывается регистр.	**osType IN ('windows', 'linux')**
RANGE((<начальное_значение>, <конечное_значение>**))**	Этот оператор используется для проверки того, находится ли значение в диапазоне значений (включительно).	**ip RANGE('10.250.176.1','10.250.176.50')**

22.4 Применение плана резервного копирования к группе

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

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

   В программе выводится список планов резервного копирования, которые можно применить к группе.
4. Выполните одно из следующих действий:
   - Разверните существующий план резервного копирования, а затем щелкните **Применить**.
   - Щелкните **Создать новый** и создайте новый план резервного копирования, как описано в теме «Резервное копирование» (стр. 41).

23 Управление учетными записями пользователей и отделами организации

Управление учетными записями пользователей и отделами организации доступно на портале управления. Для доступа к порталу управления щелкните **Портал управления** при входе в

сервис резервного копирования или щелкните  значок в правом верхнем углу, затем щелкните **Портал управления**. Доступ к порталу могут получить только те пользователи, которые имеют права администратора.

Информацию об администрировании учетных записей пользователя и отделов организации см. в документе «Руководство администратора портала управления». Для доступа к этому документу щелкните значок вопроса на портале управления.

В этом разделе предоставлена дополнительная информация по управлению сервисом резервного копирования.

23.1 Квоты

Квоты позволяют ограничить возможности пользователей использовать службу. Чтобы задать квоты, выберите пользователя на вкладке **Пользователи**, затем щелкните значок карандаша в разделе **Квоты**.

При превышении квоты на адрес электронной почты пользователя отправляется оповещение. Если превышение квоты не задано, квота рассматривается как «мягкая». Это значит, что ограничения по использованию сервиса резервного копирования, не применяются.

Также можно задать превышения квоты. Превышение позволяет превысить квоты на указанное значение. При выходе за пределы значения превышения применяются ограничения на использование службы резервного копирования.

Подобным образом поставщики управляемых служб также могут указать квоты для компаний пользователя.

23.1.1 Резервное копирование

Можно указать квоту облачного хранилища данных, квоту локального резервного копирования и максимальное количество машин/устройств/веб-сайтов, которые может защитить пользователь. Доступны указанные ниже квоты.

Квоты для устройств

- **Рабочие станции**
- **Серверы**
- **Виртуальные машины**
- **Мобильные устройства**
- **Серверы веб-хостинга**
- **Веб-сайты**

Машина/устройство/веб-сайт считаются защищенными, если к ним применен как минимум один план резервного копирования. Мобильное устройство становится защищенным после первого резервного копирования.

При превышении количества устройств пользователь не может применить план резервного копирования к дополнительным устройствам.

Квоты для источников облачных данных

- **Рабочие места Office 365**

Эта квота применяется поставщиком услуг для всей компании. Компании можно предоставить разрешение на защиту **почтовых ящиков** и (или) файлов **OneDrive**. Администраторы компании могут просматривать квоты и использование на портале управления, но не могут задавать квоты для пользователя.

- **Office 365 SharePoint Online**

  Эта квота применяется поставщиком услуг для всей компании. Эта квота активирует или отключает возможность защитить сайты SharePoint Online. Если эта квота включена, можно включить защиту для любого количества сайтов SharePoint Online. Администраторы компании не могут просматривать данную квоту на портале управления, но могут просматривать объем хранилища, занятого резервными копиями SharePoint Online в отчетах об использовании.

- **Рабочие места G Suite**

  Эта квота применяется поставщиком услуг для всей компании. Компании можно предоставить разрешение на защиту почтовых ящиков **Gmail** (включая календари и контакты) и (или) хранилища **Google Диск**. Администраторы компании могут просматривать квоты и использование на портале управления, но не могут задавать квоты для пользователя.

- **Общий диск G Suite**

  Эта квота применяется поставщиком услуг для всей компании. Эта квота активирует или отключает возможность защитить общие диски G Suite. Если эта квота включена, можно включить защиту для любого количества общих дисков. Администраторы компании не могут просматривать данную квоту на портале управления, но могут просматривать объем хранилища, занятого резервными копиями общего диска в отчетах об использовании.

Рабочее место Office 365 считается защищенным, если к почтовому ящику или OneDrive пользователя применен как минимум один план резервного копирования. Рабочее место G Suite считается защищенным, если к почтовому ящику или хранилищу Google Диск пользователя применен как минимум один план резервного копирования.

При превышении количества рабочих мест администратор компании не может применить план резервного копирования к дополнительным рабочим местам.

Квоты для хранилища данных

- **Локальное резервное копирование**

  Квота **Локальное резервное копирование** ограничивает общий размер локальных резервных копий, созданных с использованием облачной инфраструктуры. Для этой квоты нельзя задать превышение.

- **Облачные ресурсы**

  Квота **Облачные ресурсы** состоит из коты для хранилища резервных копий и квот для аварийного восстановления. Квота хранения данных ограничивает общий размер резервных копий, размещенных в облачном хранилище данных. При выходе за пределы значения превышения квоты хранения резервной копии резервное копирование не выполняется.

23.1.2 Изменение квоты для устройства

Служба резервного копирования автоматически сопоставляет квоты с устройствами. Чтобы узнать, к какой квоте отнесено устройство, посмотрите раздел **Квота службы** в разделе устройства **Подробности**.

В редких случаях может потребоваться изменить эту конфигурацию вручную. Например, виртуальная машина относится к квоте **Рабочие станции**. После приобретения квоты **Виртуальные машины** вы можете соотнести машину с этой более дешевой квотой.

Порядок изменения квоты для устройства

1. Выберите устройство.
2. Нажмите **Сведения**.
3. В разделе **Квота службы** щелкните **Изменить**.
4. Выберите новую квоту или **Без квоты**. **Без квоты** означает, что используемая квота будет освобождена и ее можно соотнести с другим устройством.
5. Подтвердите операцию.

23.2 Уведомления

Чтобы изменить настройки уведомлений для пользователя, выберите пользователя на вкладке **Пользователи**, затем щелкните значок карандаша в разделе **Настройки**. Доступны следующие настройки уведомлений:

- **Оповещения о превышении квоты** (включено по умолчанию)

  Оповещения о превышенных квотах.
- **Запланированные отчеты использования**

  Описанные ниже отчеты об использовании, которые отправляются в первый день каждого месяца.
- **Уведомления о сбое**, **Уведомления с предупреждениями** и **Успешные уведомления** (отключено по умолчанию)

  Уведомления о результатах выполнения планов резервного копирования и результатах операций аварийного восстановления для каждого устройства.
- **Ежедневные краткие сведения об активных оповещениях** (включено по умолчанию)

  Краткие сведения о неудавшихся процессах резервного копирования, отсутствующих процессах резервного копирования и других проблемах. Краткие сведения отправляются в 10:00 (время центра обработки данных)). Если по состоянию на данный момент никаких проблем не возникало, краткие сведения не отправляются.

Все уведомления отправляются на адрес электронной почты пользователя.

23.3 Отчеты об использовании

В отчете об использовании сервиса резервного копирования содержатся следующие данные о компании или отделе:

- Размер резервных копий по отделам, пользователям и типам устройств.
- Количество защищенных устройств по отделам, пользователям и типам устройств.
- Цена по отделам, пользователям и типам устройств.
- Общий размер резервных копий.
- Общее количество защищенных устройств.
- Общая стоимость.

24 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.

25 Словарь терминов

Д

Дифференциальное резервное копирование

В дифференциальной резервной копии хранятся изменения, произведенные в данных относительно самой поздней версии полной (стр. 232) 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 последовательно выберите пункты **Параметры резервного копирования** > **Еженедельная резервная копия**).

  Если еженедельная копия является первой с начала месяца, она считается ежемесячной. В этом случае еженедельная резервная копия создается в назначенный день на следующей неделе.
- Ежедневная резервная копия — это первая копия, которая создается после начала дня, если только она не является ежемесячной или еженедельной.
- Почасовая резервная копия — это первая копия, которая создается после начала часа, если только она не является ежемесячной, еженедельной или ежедневной

П

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

Формат резервных копий, в котором первоначальная полная и последующие инкрементные резервные копии сохраняются в одном TIBX-файле. Преимуществом этого формата является скорость инкрементного метода; при этом он лишен основного недостатка — сложностей, связанных с удалением устаревших копий. Программа помечает блоки, которые используются такими копиями, как свободные, и записывает на их место новые резервные копии. В результате очистка выполняется очень быстро и с минимальным потреблением ресурсов.

Формат резервной копии в виде одного файла недоступен при резервном копировании в хранилища, которые не поддерживают операции произвольного чтения и записи.