

Veeam Backup & Replication

Новые возможности v11

Veeam® Backup & Replication™ v11 предлагает единую платформу для комплексного управления данными, достаточно эффективную и гибкую, чтобы обеспечить защиту данных на всех стадиях их жизненного цикла. Она позволяет справиться со всеми сложностями использования гибридной мультиоблачной среды. В этом документе перечислены новые возможности и улучшения, представленные в V11.

Непрерывная защита данных (CDP)

Предотвращение простоев и минимизация потерь данных для важнейших систем VMware vSphere благодаря встроенным возможностям непрерывной защиты данных (CDP). Мгновенное восстановление данных в последнее состояние или желаемую точку времени обеспечивает достижение лучших показателей RTO и RPO.

Уникальные преимущества **CDP от Veeam**:

- **Отсутствие снимков ВМ** — Veeam CDP перехватывает операции записи непосредственно на пути переноса данных с помощью *сертифицированного VMware драйвера фильтра ввода-вывода*, что исключает необходимость создания снимков ВМ, как в случае классических заданий репликации. Благодаря отслеживанию уровня ввода-вывода только измененные данные переносятся на резервную площадку, в отличие от более крупных блоков виртуальных дисков, которые переносятся при отслеживании изменений блоков.
- **Отсутствие зависимости от оборудования или типов систем** — защита ЛЮБЫХ ОС и приложений, которые могут работать на ВМ vSphere. В отличие от аппаратной репликации Veeam CDP может использовать разнородные массивы хранения, гиперконвергентные инфраструктуры и локальные хранилища vSphere ESXi.
- **Асинхронная репликация** — в отличие от синхронной аппаратной репликации Veeam CDP может преодолевать любые расстояния и загружает сеть намного меньше благодаря сжатию трафика и консолидации ввода-вывода, когда один и тот же блок перезаписывается несколько раз.
- **Защита на основе политик** — не надо беспокоиться о планировании заданий, как это приходилось делать при настройке обычных заданий репликации. Просто задайте требуемые показатели RPO (максимально допустимая потеря данных при аварии), и политика CDP обеспечит

NEW Veeam® Backup & Replication™

v11 предотвращает потери данных, защищает от программ-вымогателей и помогает в 20 раз снизить расходы на долгосрочное архивирование. Решение «4-в-1» объединяет резервное копирование, репликацию, аппаратные снимки и НОВУЮ функцию непрерывной защиты данных (CDP) в рамках единой платформы. В нем реализованы возможности более быстрой и гибкой защиты, восстановления и долгосрочного хранения данных. Более 200 новых функций и улучшений версии 11 позволяют добиться высокой отказоустойчивости в компаниях любого размера:

- Предотвращение потерь данных благодаря **Veeam CDP**
- Защита от программ-вымогателей благодаря неизменности резервных копий за счет их хранения в **защищенном репозитории Linux**
- Предотвращение простоев благодаря **мгновенному восстановлению данных NAS, Microsoft SQL и Oracle**
- Сокращение затрат на долгосрочное хранение более чем в 20 раз благодаря **архивированию данных в облако Amazon S3 Glacier и Azure Blob Archive**
- Объединение **защиты облачных систем для AWS и Azure**
- Простое решение сложных задач с помощью **BaaS и DRaaS на основе Veeam**

Дополните **Veeam Backup & Replication v11** аналитической информацией, отчетами и возможностями контроля, которые предоставляет **Veeam ONE™ v11. Veeam Availability Suite™ v11** объединяет оба эти решения, позволяя обеспечить ваши потребности и в защите данных, и в аналитике.

Добавьте возможности автоматизации и тестирования восстановления площадок с помощью **Veeam Disaster Recovery Orchestrator v4**. Это решение обеспечит непрерывную работу бизнеса благодаря оркестрации в любых масштабах.

Поддерживаемые среды

Полный список поддерживаемых сред представлен в [Примечаниях к выпуску](#).

выполнение необходимых циклов синхронизации. Чтобы сократить количество оповещений системы мониторинга, можно задать пороги допустимого отклонения от RPO, тогда спонтанные нарушения соединения не будут приводить к срабатыванию оповещений.

- **Гибкие возможности хранения** — можно настроить *краткосрочное хранение* для не согласованного с состоянием приложений восстановления на определенный момент времени с гранулярными RPO, а также *долгосрочное хранение* с опциональными периодическими точками восстановления, согласованными с состоянием приложений, что обеспечит дополнительный уровень защиты.
- **Гибкие модели установки** — в зависимости от объема защищаемых данных можно выбрать виртуальные прокси-серверы CDP или использовать *выделенные физические прокси-серверы CDP*. Это позволит полностью снять нагрузку по обработке данных с хостов vSphere и избежать воздействия на коэффициент консолидации VM. В любом случае для одного кластера vSphere требуется только один прокси-сервер. Для обеспечения избыточности и повышенной масштабируемости можно задействовать дополнительные прокси-серверы.
Примечание. Прокси-сервер CDP — это новая роль, которая может быть установлена на одном сервере с другими компонентами Veeam.
- **Помощь при установке** — встроенный калькулятор установки анализирует историю операций ввода-вывода виртуальных машин, выбранных для защиты, и определяет пропускную способность сети, необходимую для достижения требуемых RPO. Ресурсы используемого прокси-сервера CDP оцениваются на соответствие ретроспективному уровню изменений.
- **Без дополнительной оплаты** — Veeam CDP входит в Универсальную лицензию Veeam наряду с другими методами защиты данных для VM vSphere, такими как: резервное копирование и репликация на базе хоста, резервное копирование с помощью агентов, резервное копирование на уровне приложений и аппаратные снимки. Как и раньше, *использование нескольких методов защиты для одной VM не требует дополнительных лицензий!* Вам больше не придется выбирать, для каких VM использовать дорогостоящую лицензию CDP от сторонних компаний — отныне ваша креативность в планировании стратегии послеаварийного восстановления будет ограничена только пропускной способностью сети!

ПРИМЕЧАНИЕ. *Функциональность Veeam CDP требует установки фильтра ввода-вывода как на исходный, так и на целевой кластеры vSphere. Это можно сделать, кликнув на кластере правой кнопкой мыши в иерархии вновь добавленных кластеров на вкладке Backup Infrastructure.*

Veeam CDP входит в **Универсальную лицензию Veeam**. При использовании лицензии по количеству сокетов требуется редакция **Enterprise Plus**.

Защищенный репозиторий

Безопасное хранение резервных копий в защищенных репозиториях, недоступных для хакеров и программ-вымогателей. Неизменность резервных копий предотвращает их шифрование и удаление в результате действий вредоносного кода или злонамеренных лиц. Это достигается благодаря следующим улучшениям для репозитория резервных копий на базе Linux:

- **Одноразовые учетные данные** — для работы с защищенным репозиторием необходимы одноразовые учетные данные, которые применяются только при установке продукта и его обновлений и никогда не хранятся в конфигурационной базе данных. Таким образом, у хакеров не будет возможности извлечь эти учетные данные из скомпрометированного сервера резервного копирования и подключиться с их помощью к репозиторию.

- **Отсутствие зависимости от протокола SSH** — все предыдущее использование протокола SSH было инкапсулировано в расширенный транспортный протокол. В результате, подключение по SSH требуется только при установке продукта и его обновлений. Это позволяет заказчикам обезопасить использование SSH с помощью интерактивной мультифакторной аутентификации (MFA) или полностью отключить сервер SSH, чтобы защитить репозиторий даже от будущих уязвимостей нулевого дня.
- **Неизменяемые резервные копии** — попрощайтесь со случайными удалениями резервных копий, программами-вымогателями и хакерами! Неизменность резервных копий на уровне образа можно обеспечить на определенный период времени. Резервные копии GFS защищаются на всем протяжении срока их хранения согласно политике. Эта возможность использует нативную функцию Linux по обеспечению неизменности файлов, которая ограничивает изменение и удаление файлов при установленном соответствующем флаге. Флаг может быть удален только пользователем с корневыми привилегиями. При этом использование одноразовых учетных данных гарантирует, что корневые учетные данные не хранятся на сервере резервного копирования. Поэтому, достаточно просто убедиться, что эти данные не сохранены в каком-либо приложении. Список Sudoers также должен быть пустым!

Для избыточности метка окончания срока действия режима неизменности хранится в двух местах: 1) в специальном конфигурационном файле и 2) в расширенных свойствах каждого файла резервной копии. Первый срок продляется автоматически, по мере добавления в цепочку резервных копий новых зависимых инкрементальных точек восстановления. Также возможно продление (но не сокращение) этого срока вручную с помощью PowerShell в целях судебного удержания. Вторая метка остается в первоначальном виде, т.к. она является частью неизменяемого файла. Флаг неизменности снимается с резервной копии только когда локальное время на репозитории выходит за рамки значений *обеих* меток.

V11 успешно прошел независимую оценку на соответствие требованиям нормативов финансовой отрасли США к хранилищам WORM (одна запись, много чтений). Соответствующая нормативам конфигурация защищенного репозитория обеспечивает защиту данных резервных копий от манипуляций и удовлетворяет требованиям к хранилищам, не допускающим перезапись и удаление, согласно предписаниям SEC 17a-4(f), FINRA 4511(c) и CFTC 1.31(c)-(d). Оценка на соответствие нормативам была выполнена компанией [Cohasset Associates](#).

ПРИМЕЧАНИЕ. Поскольку мы не поддерживаем режимы резервного копирования, которые допускают модификацию резервных копий в защищенном репозитории, это ограничивает ваш выбор классическим инкрементальным резервным копированием с периодическим созданием полных резервных копий. Это делает XFS идеальной файловой системой для таких репозиториях, благодаря новой технологии создания синтетической полной резервной копии, основанной на нашей расширенной интеграции с XFS (впервые представленной в V10).

Расширенная поддержка объектных хранилищ

Сокращение затрат на долгосрочное хранение и архивирование данных до 20 раз, отказ от ручного управления магнитной лентой и управление всем жизненным циклом резервных копий благодаря расширенной поддержке горячих объектных хранилищ в Capacity Tier и поддержке холодных объектных хранилищ в NOBOM Archive Tier — уровнях масштабируемого репозитория (SOBR).

Для Capacity Tier и архивирования версий файлов NAS, помимо имеющихся широких возможностей выбора, вы можете использовать **Google Cloud Storage (GCS)** в качестве объектного хранилища. Интеграция использует проприетарный API объектного хранилища GCS, но она пока не поддерживает режим неизменности резервных копий, поскольку в GCS отсутствует возможность блокировки объектов.

Для Archive Tier мы предоставляем поддержку **Amazon S3 Glacier** (включая Deep Archive) и **Microsoft Azure Blob Storage Archive Tier**. Экономические характеристики холодных уровней адаптированы

к сценариям “одна запись, ноль чтений”. Поэтому эти уровни лучше всего подходят для долгосрочного архивирования резервных копий GFS. Их значительно более высокие цены, связанные с API и извлечением данных, а также время извлечения данных, измеряемое в часах, привели к созданию выделенного уровня Archive Tier, который обеспечивает недорогое и органичное управление жизненным циклом резервных копий.

Основные возможности Archive Tier:

- **Неизменяемые резервные копии** — для обеспечения соответствия нормативам резервные копии, архивированные в Amazon S3 Glacier, могут опционально быть сделаны неизменяемыми на протяжении всего срока хранения согласно политике.
- **Перенос на основе политик** — аналогично Capacity Tier, без создания и управления заданиями переноса! Задайте окно архивирования таким образом, чтобы гарантировать архивирование только тех точек восстановления, доступ к которым вам вряд ли понадобится (в обычных условиях), — и умный, программно-определяемый масштабируемый репозиторий обеспечит перенос данных между уровнями. Просто проверяйте ежедневный отчет о статусе SOBR, чтобы убедиться, что все статусы «зеленые»!
- **Архивирование, оптимизированное по цене** — ввиду высоких цен, связанных с API холодных уровней объектных хранилищ, перенесенные блоки данных объединяются в более крупные объекты (размером до 512 МБ) с помощью вспомогательных устройств, автоматически выделяемых в публичном облаке на всем протяжении сессии архивирования. Кроме того, чтобы избежать штрафов за раннее удаление, мы автоматически пропускаем архивирование точек восстановления, сроки хранения которых истекают ранее, чем минимальный срок хранения данных в используемом классе хранилища.
- **Гибкие методы хранения** — для снижения затрат при переносе данных в Archive Tier по умолчанию используется постоянно инкрементальный подход, когда для каждой точки восстановления переносятся и хранятся только изменения по сравнению с предыдущей точкой восстановления. Однако для экстремально длительных сроков хранения предоставляется возможность автономного хранения каждой полной резервной копии GFS. Это позволяет избежать ситуаций, когда цепочка резервного копирования длится десятилетиями. При этом общие затраты останутся разумными благодаря использованию хранилищ класса Amazon S3 Glacier Deep Archive.
- **Самодостаточные архивы** — архивированные резервные копии являются самодостаточными и не зависят от каких-либо внешних мета-данных, что позволяет импортировать их при утрате связи с сервером резервного копирования на локальной площадке. Более того, нет привязки к какому-либо поставщику, поскольку архивированные резервные копии можно импортировать из объектного хранилища и восстанавливать в любой будущей точке времени с помощью Veeam Backup & Replication *Community Edition*, для чего не требуется действующая лицензия. Другими словами, мы не держим ваши данные в заложниках!
- **Без дополнительных затрат** — в отличие от поставщиков резервных СХД, которые, очевидно, не рады, если данные покидают их дорогостоящие устройства, Veeam не взимает потербайтную оплату за архивирование данных в объектные хранилища. Другими словами, у нас нет “налога на использование облака”!

Archive Tier масштабируемого репозитория входит в **Универсальную лицензию Veeam**. При использовании лицензии по количеству сокетов требуется редакция **Enterprise Plus**.

Расширенное мгновенное восстановление данных

Доступность еще большего количества систем дата-центра может быть мгновенно возобновлена благодаря возможностям восстановления новых типов систем от пионера мгновенного восстановления ВМ:

- **Мгновенное восстановление баз данных Microsoft SQL Server и Oracle** — База данных не запускается? Разработчики случайно удалили критически важную таблицу? Ничего страшного! Любые базы данных Microsoft SQL Server и Oracle могут быть восстановлены из резервных копий в последнее состояние или на более ранний момент времени, на любой производственный сервер или кластер (физический или виртуальный) за несколько минут, независимо от размера.

Выбранные базы данных мгновенно становятся доступными для производственных приложений и клиентов. Базы данных можно модифицировать, при этом все изменения сохраняются в кэш, а сама резервная копия никак не изменяется. Veeam в фоновом режиме автоматически восстанавливает файлы базы данных на производственную СХД и потом синхронизирует текущее (измененное) состояние базы данных.

Чтобы завершить восстановление, необходимо переключиться на базу данных, размещенную на производственной СХД. Простой при этом минимальный — такой же, как при обычном перезапуске базы данных. Переключение можно выполнить вручную или автоматически — по окончании синхронизации базы данных или во время ближайшего периода техобслуживания.

В отличие от функциональности интерактивной публикации мгновенное восстановление баз данных использует архитектуру на основе сервисов и не требует запуска пользовательского интерфейса Veeam Explorer™. Если в процессе мгновенного восстановления произойдет перезапуск какого-либо компонента инфраструктуры резервного копирования, конвейер мгновенного восстановления автоматически возобновится, как только станут доступны все необходимые серверы (в случае сбоя длительностью более одного часа мгновенное восстановление можно возобновить вручную из пользовательского интерфейса Veeam Explorer).

Мгновенное восстановление баз данных входит в **Универсальную лицензию Veeam**. При использовании лицензии по количеству сокетов требуется редакция **Enterprise** или выше.

- **Мгновенная публикация резервных копий NAS** — потеряли NAS или файловый сервер? Случайно удалили весь общий файловый ресурс? Ничего страшного! Общие файловые ресурсы SMB можно опубликовать на выбранном подключенном сервере в последнее состояние или на более ранний момент времени прямо из резервной копии. Пользователи получают мгновенный доступ к своим данным, пока вы устраняете проблему или восстанавливаете данные.

Другие сценарии использования, обнаруженные нашими бета-тестерами V11, включают предоставление сторонним приложениям и скриптам мгновенного доступа к содержимому любой резервной копии для интеллектуального анализа данных или их другого **повторного использования**. Применение для этих целей СХД для хранения резервных копий, которые обычно простаивают в производственные часы, позволяет избежать блокировки файлов и воздействия на производственную среду. Прототипы были созданы участниками сообщества, которые специализировались в различных сферах: машинное обучение (ML), поиск персонально идентифицируемой информации (PII) для помощи в выполнении требований GDPR, а также обнаружение вредоносного кода (автоматическое сканирование файлов антивирусным ПО для выявления "спящей" инфекции).

- **Мгновенное восстановление ЛЮБЫХ данных в Microsoft Hyper-V** — V11 позволяет восстанавливать ЛЮБЫЕ резервные копии физических серверов, рабочих станций, виртуальных машин и облачных инстансов в виде VM Microsoft Hyper-V, независимо от того, с помощью какого продукта Veeam была создана резервная копия. Какого-либо специального обучения не требуется, так как восстановление просто работает благодаря встроенной логике конвертации P2V/V2V. Она выводит скорость и гибкость восстановления и миграции на новый уровень, открывая возможности для послеаварийного восстановления с использованием гибридного облака.

А поскольку сервер резервного копирования Veeam работает на Microsoft Windows, хост Hyper-V фактически встроен в каждый сервер резервного копирования и готов к использованию для всех желающих! В качестве целевого хоста для этой функциональности мы также поддерживаем Windows 10 Hyper-V. Это позволяет поставщикам управляемых услуг (MSP) создавать сверхдешевые универсальные устройства на базе Windows 10 для послеаварийного восстановления на основе Veeam, которые можно устанавливать на площадках заказчиков.

Другие улучшения

Помимо перечисленных основных новых возможностей, V11 также включает более 200 улучшений, добавленных по просьбам заказчиков и как результат постоянных исследований и разработок. Наиболее важные улучшения представлены ниже.

Общие улучшения

Механизм резервного копирования

V11 более чем удваивает производительность универсальных установок Veeam на серверах общего назначения. Скорость резервного копирования может достигать более 11 ГБ/с на одном узле — при условии, что основные массивы и сеть хранения данных имеют достаточно ресурсов! Этот гигантский шаг вперед стал возможен благодаря многочисленным улучшениям для серверов корпоративного класса и оборудования для хранения данных:

- **Обход системного кэша** — в V11 сервисы Data Mover на целевом устройстве обходят кэш операционной системы (ОС), чтобы исключить его воздействие на кэширование на стороне контроллера и расширенную оптимизацию ввода-вывода RAID-контроллеров корпоративного класса. В комплексе это позволяет снизить загрузку ЦП репозитория и повысить производительность до 50%.
- **Выровненные операции записи** — невыровненные операции записи влияют как на загрузку ЦП хранилища, так и на производительность, поэтому в V11 такие операции предотвращаются за счет выравнивания блоков данных каждой резервной копии по границе в 4 Кб. Эта функция включена по умолчанию для вновь созданных репозитория, а также может быть массово включена для существующих репозитория с помощью командлета [Set-VBRBackupRepository](#). Активная полная резервная копия не требуется для включения этой настройки.
- **Улучшенный транспорт общей памяти** — когда скорость обработки данных приближается к 100 Гбит/с, скорость ОЗУ начинает играть роль в общей производительности обработки данных. V11 оптимизирует взаимодействия ОЗУ, что значительно повышает скорость переноса данных между исходными и целевыми сервисами Data Mover, когда они работают на одном сервере.
- **Поддержка NUMA** — во избежание перегрузки внутренней шины из-за трафика между узлами NUMA, на серверах с несколькими ЦП зависимые процессы в идеале должны размещаться в рамках одного узла. V11 предлагает полную поддержку NUMA и гарантирует, что исходный и целевой сервисы Data Mover никогда не окажутся на разных узлах.

- **Улучшения оптимального сжатия** — мы обновили реализацию алгоритма сжатия, используемого по умолчанию. Благодаря этому немного повысился коэффициент сжатия и значительно ускорилась производительность декомпрессии. Например, выполнение запроса SQL, возвращающего 30 ГБ данных, относящегося к базе данных переполнения стека, работающей на мгновенно восстановленной ВМ, теперь занимает на 28% меньше времени по сравнению с V10.
- **Улучшения планировщика ресурсов** — мы выполнили несколько оптимизаций планировщика ресурсов инфраструктуры, что позволило сократить время предоставления ресурсов до 50%. Это значительно ускоряет начало выполнения задания. Это улучшение особенно значительно для сред с большим количеством прокси-серверов и экстендов масштабируемого репозитория.

Механизм восстановления

Получив отличную обратную связь на применение нашей расширенной технологии переноса данных к функциональности полного экспорта на виртуальную магнитную ленту для репозитория на базе Windows в V10, мы решили распространить этот механизм на репозитории на базе Linux. Кроме того, мы теперь используем ее для ВСЕХ функций, которые считывают содержимое файлов резервных копий из репозитория Veeam. Лучшие результаты достигаются на СХД корпоративного класса и в процессе массового переноса данных, включая полное восстановление изображений, перенос резервных копий, перенос данных в объектные хранилища и др.

PowerShell

- **Модуль PowerShell** — по многочисленным запросам мы перешли от программного компонента PowerShell к модулю PowerShell, который может использоваться на любой машине с установленной консолью резервного копирования. Кроме того, на сервере резервного копирования больше не требуется устанавливать PowerShell 2.0, с которым возникали проблемы у многих заказчиков.
- **Новые командлеты PowerShell** — в V11 появились 184 новых командлета, как для вновь добавленных функций, так и для расширенной поддержки существующих функций, с особым фокусом на восстановлении.

RESTful API

- **RESTful API для сервера резервного копирования** — существующий RESTful API для Veeam Backup Enterprise Manager предоставляет только ту функциональность, которая доступна в веб-интерфейсе EM. Поэтому мы добавляем RESTful API для самого сервера резервного копирования, с фокусом на типичных потребностях управления этим сервером. V11 предлагает новый REST API, который покрывает самые популярные сценарии использования для заказчиков и партнеров, включая управление заданиями и инфраструктурой резервного копирования, а также массовый импорт/экспорт для упрощенной установки и миграции инфраструктуры и заданий резервного копирования. Ваша обратная связь поможет нам правильно расставить приоритеты! Зайдите на форум Veeam R&D и расскажите, какие функции вы бы хотели увидеть реализованными.

RESTful API входит в **Универсальную лицензию Veeam**. При использовании лицензии по количеству сокетов требуется редакция **Enterprise Plus**.

Резервное копирование

Обработка данных с учетом приложений

- **Постоянный агент гостевой ОС** — вы можете опционально использовать постоянный агент гостевой ОС для VM на базе Windows. Установить агент можно с помощью групповой политики или вашего стандартного инструмента для дистрибуции ПО. Этот подход позволяет сократить использование сетевых портов до всего нескольких статических портов (в зависимости от используемой функциональности), а также снизить требования к привилегиям учетной записи, связанным с преодолением UAC для установки на гостевой системе модуля Veeam. При этом также уменьшается загрузка сети и ускоряется обработка данных гостевых ОС. На гостевые системы необходимо установить только один крохотный компонент-установщик; все остальные компоненты устанавливаются (и обновляются) автоматически.
- **Интеграция с SQL Server** — механизм обработки данных с учетом состояния приложений теперь использует нативный провайдер MSOLEDBSQL, если он доступен на SQL Server. Это позволяет обрабатывать SQL Server с принудительно введенным TLS 1.2, не редактируя реестр. Кроме того, теперь будут учитываться предпочтения по резервному копированию баз данных для групп HA.
- **Улучшенный контроль защиты баз данных SQL** — новая экспериментальная опция для SQL Server позволяет завершать сессию резервного копирования на уровне образа, если не может быть выполнена инициализация журнала транзакций или базы данных SQL не найдены. Используйте значение реестра `AAIPSQLShowExperimentalOptions` (DWORD, 1) на сервере резервного копирования, чтобы соответствующий флажок появился в настройках обработки данных с учетом состояния приложений. Оставьте, пожалуйста, отзыв об этой новой возможности на форумах Veeam R&D!

Задания резервного копирования

- **Задания с высоким приоритетом** — теперь можно обозначить некоторые задания резервного копирования как высокоприоритетные. Такие задания будут помещать свои ожидающие выполнения задачи в выделенную очередь планировщика ресурсов. Задачи из этой очереди будут предлагаться ресурсам инфраструктуры резервного копирования раньше, чем задачи с обычным приоритетом. Эту настройку можно использовать для заданий, защищающих системы, чувствительные ко времени начала резервного копирования или для периодических заданий со строгими требованиями к RPO.
- **Фоновая обработка хранения по схеме GFS** — хранение полных резервных копий по схеме GFS теперь обрабатывается независимо от выполнения задания резервного копирования, как фоновая системная деятельность на репозитории Veeam. Это гарантирует, что полные резервные копии с истекшим сроком хранения не будут продолжать занимать дисковое пространство, если задание резервного копирования отключится на длительное время.
- **Хранение потерянных резервных копий GFS** — политика хранения теперь применяется к резервным копиям GFS, не имеющим ассоциированных с ними заданий резервного копирования, на основе их последней известной политики хранения. Это устраняет необходимость в обходных путях, например сохранении ненужных заданий, защищающих единственную фиктивную машину.
- **Улучшения хранения удаленных VM** — хранение удаленных VM больше не будет применяться, если задание резервного копирования не смогло построить список обработанных машин. Это позволит избежать удаления резервных копий из-за временных проблем инфраструктуры.

Задания копирования резервных копий

Задания копирования резервных копий теперь используют ту же логику хранения по схеме GFS, что и основные задания резервного копирования. Это гарантирует согласованность внутри продукта и обеспечивает совместимость с новыми возможностями, такими как неизменность резервных копий в защищенном репозитории или фоновая обработка хранения резервных копий по схеме GFS. Это означает следующие изменения:

- **Хранение по схеме GFS на основе времени** — хранение дополнительных резервных копий по схеме GFS теперь основано на времени, а не на количестве точек восстановления в каждом поколении. Это гарантирует, что точки восстановления GFS будут храниться не меньше, чем нужно, даже в случае случайного создания резервной копии GFS вручную.
- **Время создания полной резервной копии GFS** — полные резервные копии GFS теперь создаются и запечатываются точно в запланированный день, а не тогда, когда соответствующая точка восстановления становится самой старой в цепочке инкрементальных резервных копий. Это должно устранить постоянную путаницу и опасения заказчиков, связанные с этим процессом.
- **Отсутствие ежеквартальных резервных копий** — для согласованности с хранением по схеме GFS для заданий резервного копирования, возможность создания ежеквартальных резервных копий больше не предоставляется. Существующие ежеквартальные расписания будут преобразованы в ежемесячные путем соответственного увеличения их срока хранения при обновлении до V11. Существующие задания копирования резервных копий с хранением по схеме GFS будут обновлены автоматически при переходе на новую версию.

Другие улучшения заданий копирования резервных копий:

- **Репозиторий как источник** — теперь можно выбрать весь репозиторий в качестве источника для заданий копирования резервных копий при использовании режима немедленного копирования.
- **Срок хранения в днях** — для недавних копий, созданных заданием копирования резервных копий, можно задать срок хранения как на основе точек восстановления, так и на основе времени, измеряемом в днях.

Задания репликации

- **Поддержка репозитория NFS** — в задании репликации можно выбрать репозиторий на основе NFS для хранения метаданных реплики.

Задания Quick Migration

- **Попор SmartSwitch** — наше внутреннее тестирование показало, что выполнение Quick Migration в режиме SmartSwitch занимает слишком много времени для VM с большим объемом ОЗУ — до такой степени, что иногда оно просто теряет смысл. Причина кроется во времени, которое необходимо для переноса состояния памяти по протоколу NFC. В результате, начиная с V11, мы будем принудительно использовать холодную миграцию (через отключение питания) для машин с ОЗУ более 8 ГБ. Для переопределения порога можно использовать значение реестра `QMSmartSwitchRAMThresholdGB` (DWORD) на сервере резервного копирования.

Восстановление

API для интеграции данных

- **Поддержка целевых устройств на базе Linux** — API для интеграции данных (DIAP) теперь поддерживает подключение содержимого резервной копии напрямую к серверу Linux.
- **Расширенная поддержка платформ** — V11 позволяет публиковать резервные копии на уровне образа всех платформ, поддерживаемых Veeam, с помощью DIAP. Это включает облачные резервные копии AWS, Microsoft Azure и Google Cloud Platform, а также резервные копии Nutanix AHV и VMware Cloud Director.

Восстановление файлов (FLR)

- **Восстановление файлов Linux без вспомогательного устройства** — для восстановления файлов файловых систем Linux теперь можно подключать резервные копии к ЛЮБОЙ машине Linux: выделенной, целевой или исходной (что всегда гарантирует распознавание файловой системы, с которой вы пытаетесь восстановить файлы). Такой подход снимает необходимость запуска вспомогательного устройства на хосте vSphere или Hyper-V и позволяет упростить настройку сети и устранить проблемы безопасности, связанные с применением устройства. Кроме того, заказчики теперь могут восстанавливать файлы непосредственно из облачных инфраструктур VMware.

***ПРИМЕЧАНИЕ.** Вспомогательное устройство остается доступным в качестве опции, например, из архивированных резервных копий с файловыми системами, более не используемыми в производственной среде.*

- **Улучшение производительности восстановления файлов Linux** — производительность восстановления файлов файловых систем, не относящихся к Windows, увеличилась до 50%, независимо от того, используете ли вы вспомогательное устройство или нет.

Veeam Explorer for Microsoft Active Directory

- **Восстановление конфигурации DFS** — теперь можно восстанавливать конфигурацию распределенной файловой системы (DFS) в системном контейнере.

Veeam Explorer for Microsoft Teams

- **Восстановление объектов Microsoft Teams** — восстановление объектов Microsoft Teams непосредственно из резервной копии, созданной с помощью сервера резервного копирования Veeam Backup for Microsoft Office 365.

Инфраструктура резервного копирования

Репозиторий резервных копий

- **Улучшенная производительность создания синтетических полных резервных копий на ReFS** — Синтетическое полное резервное копирование теперь завершается в два раза быстрее на ReFS благодаря снижению использованию достаточно длительных обращений к Windows API, необходимых для создания синтетических полных резервных копий.
- **Отключение потоков целостности ReFS** — для резервных копий Veeam теперь можно отключить потоки целостности ReFS с помощью значения реестра *DisableRefsIntegrityStreams* (DWORD, 1) на сервере резервного копирования. Хотя мы не рекомендуем отключать потоки целостности, т.к. целостность данных имеет первостепенное значение для их защиты, некоторые заказчики настаивали на такой опции, чтобы получить возможность повышать производительность.

Масштабируемый репозиторий

- **Перенос на другой уровень резервных копий VeeamZIP™ и экспортированных резервных копий** — полные резервные копии, созданные с помощью VeeamZIP и экспорта резервных копий, а также потерянные резервные копии, теперь обрабатываются политиками Capacity Tier и Archive Tier как обычные резервные копии и могут быть скопированы или перенесены в объектное хранилище обычным образом. Импортированные резервные копии не будут переноситься на другой уровень, как и раньше.
- **Поддержка быстрого клонирования** — планировщик экстенсов масштабируемого репозитория теперь будет учитывать необходимость быстрого клонирования вновь созданных файлов синтетических полных резервных копий и не будет требовать от предпочитаемого экстенста наличия достаточного свободного пространства для размещения синтетических полных резервных копий, не требующих быстрого клонирования. В предыдущих версиях масштабируемый репозиторий мог “взорваться”, когда некоторые экстенсты приближались к полной загрузке, потому что планировщик начинал размещать синтетические полные резервные копии не в предпочитаемом экстенсте.
- **Операции переноса в журнале событий Windows** — операции копирования и переноса, связанные с Capacity Tier и Archive Tier, теперь будут создавать соответствующие события в системном журнале событий. Это обеспечит лучший контроль над этими процессами для пользователей, выполняющих мониторинг на основе журнала событий.

Объектные хранилища

- **Ограничение количества заданий** — добавлена возможность ограничивать количество одновременно выполняемых заданий. Это поможет улучшить совместимость с локальным объектным хранилищем, которое может быть легко перегружено большим количеством одновременных обращений к API. Это ограничение не предназначено для большинства объектных хранилищ в публичном облаке, поскольку они являются бесконечно масштабируемыми. Тем не менее, это ограничение может быть полезным, когда в настройках объектного хранилища вы указываете шлюзовый сервер для обеспечения интернет-доступа. Тогда, в зависимости от объема ресурсов ЦП и ОЗУ на этом сервере, ему может не хватить этих ресурсов при обработке слишком большого количества одновременно выполняемых заданий.
- **Производительность восстановления** — Производительность восстановления данных из локального объектного хранилища, размещенного на медленном оборудовании, повысилась в несколько раз.
- **Разрешение ListAllMyBuckets больше не требуется** — контейнеры объектных хранилищ S3 и Google теперь можно вручную указывать в мастере Object Storage Repository, без необходимости их поиска. Это позволяет поставщикам услуг создавать отдельные контейнеры для своих заказчиков и делегировать разрешения с помощью политики IAM. Таким образом, заказчики не смогут видеть список контейнеров других заказчиков (по названиям).
- **Декомпрессия блоков перед хранением** — Теперь можно выполнять декомпрессию блоков данных резервных копий перед их записью в объектное хранилище. Это позволяет локальным объектным хранилищам со встроенной функцией дедупликации более эффективно обрабатывать данные резервных копий Veeam. Чтобы включить эту функцию, создайте значение реестра *ObjectStorageDisableCompression* (DWORD, 1) на сервере резервного копирования.

Veeam Cloud Connect

- **Cloud Connect Backup в режиме MSP** — когда флажок “Allow this Veeam Backup & Replication installation to be managed by the service provider” установлен в мастере Service Provider на сервере резервного копирования со стороны пользователя, метаданные резервных копий, такие как названия машин, не будут скрыты на сервере резервного копирования со стороны поставщика услуг. Это позволит поставщикам MSP повысить эффективность предоставляемых сервисов управляемого резервного копирования.

- **Пользователи на базе Microsoft Active Directory** — для упрощения защиты удаленных рабочих станций и ноутбуков с помощью автономного Veeam Agent for Microsoft Windows, установленного в корпоративной среде, Veeam Cloud Connect теперь поддерживает квоты для пользователей на основе учетных записей Active Directory (AD). Таким образом, пользователи могут подключаться к облачному репозиторию, используя свою учетную запись AD. Инфраструктура Cloud Connect выполняет аутентификацию пользователя с помощью AD. Во время выполнения резервного копирования для аутентификации используется дополнительный пароль, чтобы изменение пароля не помешало резервному копированию. Однако восстановление с нуля из облачного репозитория всегда требует успешной аутентификации учетной записи с помощью AD и с использованием текущего пароля до того, как будет предоставлен доступ к резервным копиям. Если учетная запись AD заблокирована, выполнение резервного копирования и восстановления невозможно.
- **Эвакуация пользователей** — пользователей теперь можно эвакуировать из экстенсов масштабируемого репозитория с помощью командлета Start-VBRCloudTenantBackupEvacuation.
- **Регулирование WAN-акселератора** — настройка "Limit incoming traffic from this tenant" теперь относится к пользователям, выполняющим перенос данных с помощью WAN-акселераторов. Раньше она работала только для режима прямого переноса данных.
- **Потребление ОЗУ на сервере Cloud Connect** — мы значительно снизили потребление ОЗУ на сервере Cloud Connect во время входящей репликации.

Доступ к Veeam Cloud Connect для поставщиков услуг требует наличия **арендной лицензии**. Для доступа к Veeam Cloud Connect for the Enterprise свяжитесь, пожалуйста, с представителем Veeam.

Платформы

Google Cloud Platform (GCP)

- **Интеграция Veeam Backup for Google Cloud Platform** — зарегистрируйте контейнеры Google Cloud Storage (GCS) с резервными копиями, созданными Veeam Backup for Google Cloud Platform, в качестве внешних репозиториях. Это позволит выполнять все типы восстановления и копировать резервные копии ВМ GCP в репозитории на локальной площадке или на магнитную ленту, для обеспечения послеаварийного восстановления и соблюдения правила 3-2-1.

Linux

- **Постоянный сервис Data Mover для Linux** — транспортные компоненты теперь устанавливаются на постоянной основе при регистрации сервера Linux в Veeam. Это улучшает производительность и масштабируемость, так как больше не надо устанавливать Data Movers на сервере при запуске каждого задания. Необходимые правила для встроенных брандмауэров Linux создаются автоматически на время выполнения резервного копирования (поддерживаются iptables, ufw и firewallld).

ПРИМЕЧАНИЕ. Для хостов Linux, которые еще не поддерживают постоянные Data Movers, V11 продолжит использовать динамический Data Mover.

- **Расширенная безопасность Data Mover** — при использовании одноразовых учетных данных постоянный Data Mover будет работать как ограниченный пользователь из набора учетных данных, с которыми он был установлен. В результате никакие потенциальные уязвимости во внутреннем API Data Mover не смогут быть использованы хакерами для получения контроля над операционной системой.

- **Аутентификация на базе сертификата** — в отличие от использования сохраненных учетных данных Linux, мы будем задействовать технологию инфраструктуры публичных ключей (PKI) для аутентификации между сервером резервного копирования и транспортными компонентами во время обработки заданий резервного копирования. Пары ключей будут автоматически генерироваться во время установки транспорта.

Microsoft Azure

- **Полностью интегрированное резервное копирование Azure** — возможности защиты облачных данных Azure теперь встроены непосредственно в консоль Veeam Backup & Replication. Для этого необходим Veeam Backup for Microsoft Azure v2.
- **Поддержка Azure Stack HCI** — добавлена поддержка новой операционной системы для гиперконвергентной инфраструктуры (HCI) от Microsoft, которая, по сути, является инфраструктурой Hyper-V на локальной площадке, предоставляемой в качестве сервиса [Azure](#).
- **Восстановление на VM 2-го поколения** — добавлена экспериментальная поддержка Direct Restore to Microsoft Azure для использования VM 2-го поколения в качестве целевого устройства. Чтобы включить эту функциональность, создайте значение реестра `AzureEnableGeneration2VMRestore` (DWORD, 1) на сервере резервного копирования.

Nutanix AHV

- **Veeam Backup for Nutanix AHV 2.1** — новые возможности позволяют исключать диски из заданий резервного копирования, предлагают улучшенную интеграцию с Nutanix Volume Groups для восстановления данных, улучшения пользовательского интерфейса и др. Полный список новых возможностей представлен в документе "Примечания к выпуску".

VMware vSphere

- **Мгновенное восстановление диска первого класса** — при выполнении мгновенного восстановления диска пользователи могут выбрать восстановление диска из резервной копии в виде стандартного VMDK, подключенного к определенной VM vSphere, или в виде диска первого класса (FCD), который может управляться независимо от VM vSphere и напрямую использоваться контейнерными приложениями нового поколения.
- **AND для тегов vSphere** — помимо указания нескольких отдельных тегов vSphere для определения области действия задания, теперь можете использовать комбинацию тегов vSphere. В этом случае будут обработаны только машины с каждым выбранным тегом (классическое поведение при использовании оператора AND). При использовании этого подхода следует более тщательно отслеживать незащищенные VM, например, с помощью Veeam ONE™, поскольку становится легче случайно потерять какую-нибудь VM из защищаемой области и оставить ее без свежих резервных копий.
- **Обратное переключение в два шага** — чтобы сделать время обратного переключения более предсказуемым для крупных VM и сократить простои, мы сделали процесс обратного переключения более контролируемым. На первой стадии процесса, который занимает больше всего времени, реплика VM все еще работает, но вычисляются хэш-суммы, а целевая машина восстанавливается в состояние снимка. По окончании этих процессов реплика VM помещается в состояние готовности к переключению, которое может произойти за минимальное время, необходимое для переноса финальной дельты. Операцию переключения можно выполнить вручную или автоматически — или по готовности реплики, или в запланированное время в течение периода техобслуживания.

- **Транспортные режимы прокси-сервера Linux** — поддерживаемые транспортные режимы теперь включают Direct Storage Access (для блочных хранилищ и NFS), сетевой режим (NBD/NBDSSL) и резервное копирование из аппаратных снимков (только для блочных хранилищ). Кроме того, производительность режима Hot-Add была значительно улучшена за счет применения передовой технологии модуля переноса данных, которая ранее использовалась только для прокси-серверов Windows.
- **Восстановление на основе CBT для прокси-серверов Linux** — добавлена поддержка быстрого отката для прокси-серверов Linux, для полного восстановления VM и обратного переключения в исходное местоположение.
- **Многопоточность NBD** — механизм резервного копирования теперь может устанавливать несколько подключений NBD для одного VMDK, для лучшей производительности сетевого транспортного режима. В то же время, ввиду малого количества подключений по NBD, возможных для одного хоста ESXi, возникает проблема надежности, связанная с увеличением количества таких подключений. Хотя наш планировщик ресурсов отслеживает количество заданий NBD на каждом хосте, чтобы гарантировать, что они остаются в рамках ограничений, мы решили, что незначительное повышение производительности не стоит риска применения этого нового поведения для всех заказчиков, поскольку могут быть еще и внешние подключения по NBD. Однако если вы хотите попробовать эту функциональность, используйте значение реестра *VMwareNBDConnectionsPerDisk* (DWORD) на сервере резервного копирования. Наше внутреннее тестирование показало, что наилучшая производительность достигается при двух NBD-подключениях на диск. Поделитесь, пожалуйста, своими результатами на форумах Veeam R&D. Это поможет нам решить, активировать ли эту функцию по умолчанию в следующих обновлениях!
- **Поддержка удаленной консоли VMware** — функциональность пользовательского интерфейса, которая позволяет открывать консоль VM, теперь использует более безопасную удаленную консоль VMware. Вам будет предоставлена возможность скачать и установить эту консоль при первой попытке использовать связанную с этим функциональность.
- **Обновление версии VDDK** — VDDK 6.7 был обновлен до версии 6.7.3, что, помимо прочего, должно исправить проблему с использованием асинхронного ввода-вывода NBD.

VMware Cloud Director

- **Репликация Cloud Director** — новое специальное задание репликации позволяет поставщикам услуг выполнять репликацию vApp в пределах инстанса и между инстансами vCloud Director (VCD). Задание репликации обрабатывает VM и метаданные vApp (метаданные могут включать настройки сети и порядок запуска VM) для создания в целевом экземпляре vCloud Director готовой к применению реплики vApp, которая может быть мгновенно использована в случае аварии.
- **Плагин для Cloud Director** — используя эту новую возможность, поставщики услуг могут расширить пользовательский интерфейс vCloud Director путем включения в него функциональности Veeam Backup & Replication. Благодаря этому пользователи смогут управлять своим резервным копированием и восстановлением, не покидая веб-консоль vCloud Director. Эта интеграция основана на портале самостоятельного резервного копирования Veeam для Cloud Director.
- **Поддержка нескольких серверов Cloud Director** — портал самостоятельного резервного копирования для Cloud Director теперь поддерживает среды с несколькими серверами VCD, зарегистрированными в Veeam Backup & Replication. Вы можете выбрать желаемый сервер VCD при создании конфигурации вашей организации.
- **Поддержка нескольких конфигураций** — портал самостоятельного резервного копирования для Cloud Director теперь поддерживает создание нескольких конфигураций самообслуживания для одной организации VCD.

- **Улучшенная гибкость доступа к portalу Cloud Director** — можно указать роли VCD с помощью значений `vCloudPortalBackupAdminRole` (STRING) и `vCloudPortalRestoreOperatorRole` (STRING) на сервере резервного копирования. Это обеспечит всем пользователям VCD с соответствующей ролью VCD доступ к portalу самостоятельного восстановления для их организации с ролью администратора резервного копирования или оператора восстановления на portalе. При отсутствии этих значений реестра поведение останется таким же, как и в предыдущих версиях: только пользователи VCD с правами администратора для организации VCD смогут иметь доступ к portalу самостоятельного резервного копирования для соответствующей организации с ролью администратора резервного копирования на portalе.
- **Поддержка Cloud Director 10.2** — полная поддержка установки на локальной площадке и в облаке с сервисом VMware Cloud Director.

Интеграция с производственными СХД

Общие улучшения

- **Мгновенное восстановление дисков из аппаратных снимков** — сокращение объема требуемых для мгновенного восстановления ресурсов благодаря восстановлению только необходимых дисков крупных VM vSphere (например, только диск с ОС или только диск с данными) непосредственно из аппаратных снимков. Мгновенное подключение дисков из аппаратных снимков к выбранной VM для других сценариев использования, например, сравнения содержимого диска или выполнения массовых восстановлений файлов с помощью сторонних инструментов.
- **Хранение на базе точек восстановления для аппаратных снимков** — хранение точек восстановления в аппаратных снимках теперь обрабатывается для каждой VM. Ранее сами аппаратные снимки рассматривались как точки восстановления, что приводило к различным проблемам в сложных ситуациях, таких как неудачные повторные попытки, миграция VM на другой том и др.

Dell EMC VNX/VNXe/Unity/Unity XT

- **Версия интеграционного инструмента** — инструменты Dell EMC Navisphere и Unisphere CLI обновлены до последней версии для поддержки TLS 1.2.

HPE 3PAR/Primera

- **Поддержка 3PAR Remote Copy** — асинхронная периодическая репликация 3PAR/Primera теперь поддерживается для всей функциональности интеграции аппаратных снимков. Это включает управление репликацией аппаратных снимков, отдельным хранением реплик аппаратных снимков и резервных копий, созданных из этих реплик, на резервном массиве для предотвращения воздействия резервного копирования на основной массив.
- **Поддержка мультипротокола Nimble** — интеграция аппаратных снимков теперь поддерживает хранилища Nimble с протоколами FC и iSCSI, включенными на одном массиве.
- **Поддержка версий** — добавлена поддержка 3PAR OS 3.3.1 MU5 и прекращена поддержка 3PAR OS версий ниже 3.2.2 и WSAPI до версии 1.5.

Lenovo

- **Поддержка Lenovo DM** — добавлена интеграция аппаратных снимков Lenovo ThinkSystem DM Series.

NetApp

- **Поддержка ONTAP 9.8** — добавлена поддержка интеграции аппаратных снимков NetApp ONTAP 9.8, кроме обработки ВМ, размещенных на томах FlexGroup. Примечание. Вы можете использовать обычное резервное копирование на базе хоста или агента для защиты таких ВМ.

Интеграция с резервными СХД

ExaGrid

- **Поддержка аутентификации на базе AD** — добавлена поддержка аутентификации на базе Microsoft Active Directory для регистрации ExaGrid в Veeam.
- **Логика размещения в SOBR** — по запросу ExaGrid и в свете предоставляемой ими глобальной дедупликации, мы отключили специальную логику планирования экстендов масштабируемого репозитория (SOBR), предназначенную для дедуплицирующих СХД. Согласно этой логике SOBR предпочитал размещать новые полные резервные копии на том же экстенде, что и предыдущие полные резервные копии. Вернуться к предыдущей логике можно путем создания значения *ExaGridEnableNewFullToSameExtent* (DWORD, 1) в ключе реестра HKLM\SOFTWARE\Veeam\Veeam Backup and Replication на сервере резервного копирования.
- **Настройки по умолчанию в пользовательском интерфейсе** — мы рекомендуем устанавливать уровень сжатия Optimal в мастере настройки задания резервного копирования, когда ExaGrid выбран в качестве целевого репозитория. При регистрации репозитория, основанного на ExaGrid, опция "Decompress backup data blocks before storing" включена по умолчанию в мастере настроек репозитория. Новые настройки по умолчанию позволят ExaGrid эффективно выполнять дедупликацию, независимо от защищаемой системы.

Dell EMC Data Domain

- **Поддержка Data Domain OS support** — добавлена поддержка DD OS версий 7.1, 7.2 и 7.3, прекращена поддержка всех версий DD OS ниже 6.1. Обновите, пожалуйста, версию DD OS до перехода на V11.
- **Версия Data Domain Boost SDK** — DD Boost SDK обновлен до версии 7.0.

HPE StoreOnce

- **Задания копирования резервных копий на источнике** — задания копирования резервных копий теперь могут использоваться в качестве источника для заданий Catalyst Copy. Ранее только основные задания резервного копирования могли служить источником.
- **Перенос на ленту резервных копий Catalyst Copy** — задания резервного копирования на ленту теперь поддерживают использование заданий Catalyst Copy в качестве источника.
- **Производительность проверки состояния** — производительность проверки состояния заданий Catalyst Copy повысилась в несколько раз благодаря параллельной обработке данных.
- **Пользовательский интерфейс для контроля задержки удаления копий** — задания Catalyst Copy активируют задержку удаления копий из резервного хранилища, что приводит к их более длительному хранению на целевых устройствах Catalyst Copy. Эта задержка удаления теперь может контролироваться напрямую из пользовательского интерфейса, а не через реестр. Эта функциональность совместима с HPE StoreOnce и HPE Cloud Volumes Backup.

- **Поддержка Cloud Volumes Backup** — V11 добавляет официальную поддержку заданий Catalyst Copy на HPE Cloud Volumes Backup.
- **Версия Catalyst SDK** — HPE StoreOnce Catalyst SDK обновлен до версии 4.2.4 с версией протокола V11.
- **Тегирование сессий Catalyst API** — Veeam задания резервного копирования общих файловых ресурсов Veeam теперь тегируют запросы Catalyst API специальным тегом VeeamNAS. Служба поддержки HPE намеревается использовать эту информацию для дифференциации типов систем Veeam в заявках для их скорейшего разрешения.

Quantum DXi

- **Поддержка Quantum FastClone** — V11 официально поддерживает активацию быстрого клонирования в репозиториях на базе моделей Quantum DXi, которые поддерживают эту функциональность. Свяжитесь, пожалуйста, со службой поддержки Quantum, чтобы подтвердить статус модели СХД, которую вы используете.
- **Улучшенная производительность полного восстановления ВМ** — мы добавили оптимизированную логику полного восстановления ВМ, которая уже используется в интеграциях с другими дедуплицирующими СХД. Прокси-сервер Veeam теперь будет выполнять последовательные операции чтения с Quantum и произвольные операции записи на целевые диски, в отличие от восстановления блоков в том же порядке, в котором они хранятся на целевом диске.

Возможности интеграции с дедуплицирующими СХД входят в **Универсальную лицензию Veeam**. При использовании лицензии по количеству сокетов требуется редакция **Enterprise** или выше.

Использование магнитной ленты

- **Копирование ленточных носителей** — простое клонирование отдельных ленточных носителей для создания дополнительных копий на удаленной площадке, обновления хранимых данных для борьбы с физической деградацией или миграции архивов на LTO современного или иных поколений. Сервер резервного копирования обновляет каталог резервных копий, добавляя ссылки на клонированные (целевые) носители, также сохраняя ссылки на оригинальные (исходные) носители.
- **Верификация ленточных устройств** — периодическая верификация архивированных носителей позволяет гарантировать целостность и читаемость хранящихся данных. Верификация ленточных устройств может понадобиться для соблюдения нормативов, и вам не придется волноваться!
- **Восстановление всех данных с ленточного носителя** — простое восстановление всех данных с набора носителей, который включает проблемную магнитную ленту, путем вывода всех читаемых файлов в указанное местоположение.
- **Режим обслуживания** — перевод всей ленточной библиотеки или отдельного накопителя в режим обслуживания, чтобы они временно не использовались.
- **Ограничение использования накопителя для задания** — использование ленточного накопителя можно ограничить на уровне отдельного задания резервного копирования на ленту.
- **Принудительная очистка ленты** — процесс очистки ленты будет теперь игнорировать все не критичные ошибки, такие как проблемы с размерами блока или заголовком, поскольку они неактуальны для носителя, данные с которого удаляются.
- **Резервное копирование с поддержкой кластеров для хранилищ на базе NetApp ONTAP** — резервное копирование с поддержкой кластеров является расширением протокола NDMP v4, позволяющим серверу NDMP устанавливать подключение к узлу, который является владельцем тома. За счет этого оптимизируется поток данных и повышается производительность резервного копирования NDMP.

- **Источники заданий резервного копирования на магнитную ленту** — задания резервного копирования на магнитную ленту теперь могут обрабатывать копии резервных копий Nutanix AHV и Mac, а также облачных резервных копий AWS, Azure и Google. Это позволяет архивировать облачные резервные копии на ленту для соблюдения нормативов.
- **Улучшение производительности заданий копирования файлов на ленту** — улучшенная логика предварительной обработки данных заданий копирования файлов на ленту позволяет до 10 раз быстрее выполнять операции резервного копирования и восстановления для наборов данных с большим количеством файлов и папок, нуждающихся в защите.
- **Диапазон защиты заданий копирования файлов на ленту** — теперь можно указать весь источник данных (Windows Server или файловый сервер SMB/NFS) в качестве источника для задания копирования файлов на ленту. Это позволит защитить все общие ресурсы и экспорты, включая вновь добавленные. Эта новая возможность потребовала внесения изменений в мастер восстановления файлов с ленты для поддержки восстановления из таких резервных копий. В качестве побочного эффекта этих изменений теперь можно настраивать массовое восстановление нескольких общих файловых ресурсов за один запуск мастера.
- **Улучшенное создание отчетов** — задания резервного копирования, восстановления и верификации магнитной ленты теперь создают в папке журнала задания CSV-файл со всеми файлами, которые не смогли быть обработаны.
- **Улучшения пользовательского интерфейса восстановления с ленты** — для каждой точки восстановления, выбранной в мастере, автоматически отображаются необходимые носители. Вам больше не нужно просматривать каждую выбранную точку восстановления — просто нажмите Next и ждите приглашения вставить ленточные носители в устройство.
- **Улучшения пользовательского интерфейса управления носителями** — к диалогу свойств магнитной ленты добавлено время существования очищающего носителя, а к диалогу свойств устройства — серийные номера ленточной библиотеки и накопителя. Сессия повторного сканирования ленты теперь содержит индикацию завершения. На серверах NDMP можно установить тег локации. Контекстные меню на вкладке Tape Infrastructure обновлены и стали более четкими. Ширина всех колонок откорректирована, чтобы контент помещался в них без дополнительных настроек.
- **Поддержка LTO-9** — вся функциональность поддержки магнитной ленты в V11 была успешно валидирована с использованием образцов LTO-9, любезно предоставленных нам IBM. Если магнитная лента — наше будущее, то с V11 вы готовы к нему!

Агенты резервного копирования

Управление решениями Veeam Agents

- **Резервное копирование из аппаратных снимков** — теперь можно выполнять резервное копирование серверов Microsoft Windows с томами, размещенными на поддерживаемых массивах хранения. Для этого используются “управляемые сервером” задания резервного копирования из аппаратных снимков с использованием агентов. Такой подход позволяет перенести обработку данных с защищаемого сервера на выделенный прокси-сервер. Более того, использование аппаратных снимков устраняет непроизводительную нагрузку ввода-вывода, которую создает система, работающая из снимков, созданных с помощью программного VSS, на протяжении всего резервного копирования. Решая эти две классические проблемы резервного копирования с применением агентов, V11 предлагает резервное копирование без использования LAN и без воздействия на производственную среду. *Процесс идентичен резервному копированию VM VMware и Hyper-V на другой хост, для физических серверов и кластеров, что позволяет защищать самые загруженные 24/7 системы с соблюдением условий*

SLA. Поддерживаются все встроенные и основанные на универсальном API интеграции с системами хранения с подключением по iSCSI или FibreChannel; не требуется использование аппаратного VSS-провайдера, предназначенного для конкретного поставщика.

- **Группы защиты для предустановленных агентов** — этот тип группы защиты (PG) предлагает удобный способ установки агентов с помощью сторонних решений для дистрибуции ПО, когда невозможно их распространить с помощью сервера резервного копирования ввиду ограничений, вызванных требованиями безопасности и возможностями сети. Мастер группы защиты создает пакет установки агента, который позволяет агенту автоматически подключаться к серверу резервного копирования с аутентификацией на базе PKI с сертификатом PG. После этого сервер добавляет агент к группе защиты, которая создала пакет установки, и выпускает новый персональный сертификат аутентификации. На этом этапе вы можете использовать агент в политиках «управляемого агентом» резервного копирования обычным образом. Возможность подключения сервера резервного копирования к агентам по сети не требуется, поскольку агенты будут сами запрашивать сервер об изменениях в настройках политики несколько раз в день.
- **Улучшения экспорта в виде виртуального диска** — диски из резервных копий, созданных с помощью агентов, могут экспортироваться в виде фиксированных дисков VHD/VHDX, что позволяет подключить их в сервисах Microsoft Azure (ранее диски могли экспортироваться только как динамические).
- **Оповещение по почте о незащищенных хостах** — добавлено опциональное почтовое уведомление о хостах, резервное копирование которых не выполнялось по крайней мере один раз в течение количества дней, указанного в политике резервного копирования, «управляемого агентом».
- **Удаление из конфигурации** — теперь удалять машины из групп защиты можно с помощью контекстного меню хоста.
- **Образ восстановления из дополнительных резервных копий** — теперь образ восстановления можно создавать из резервных копий, созданных заданиями копирования резервных копий.
- **Veeam Agent for Microsoft Windows** — мастер резервного копирования на основе агента теперь позволяет конфигурировать настройку «Backup all volumes except excluded» для резервного копирования на уровне томов, исключать из обработки папку OneDrive и использовать режим резервного копирования профиля пользователя.

Veeam Agents

- **Veeam Agent for Microsoft Windows v5:** новые возможности включают поддержку Microsoft Windows 10 версии 20H2, расширенную совместимость с версиями Microsoft .NET Framework во избежание требований перезагрузки после установки .NET, опции хранения по количеству дней и по схеме GFS для серверов, резервное копирование профилей пользователей на уровне файлов, улучшенное выявление подключений по VPN, соблюдение требований FIPS и многое другое. Полный список новых возможностей представлен в соответствующем документе «Новые возможности».
- **Veeam Agent for Linux v5:** новые функции включают поддержку новых версий ОС, расширенные атрибуты резервного копирования файлов, несколько улучшений образа восстановления, соблюдение требований FIPS и многое другое. Полный список новых возможностей представлен в соответствующем документе «Новые возможности».
- **Veeam Agent for Mac:** новый агент предлагает управляемое резервное копирование данных пользователей с помощью Veeam Backup & Replication для любых устройств на базе macOS. Это позволяет органично интегрировать защиту данных ноутбуков и рабочих станций на базе Mac в вашу общую стратегию защиты данных. В отличие от встроенного ПО Time Machine от Apple, Veeam Agent for Mac позволяет соблюдать правило 3-2-1 за счет создания дополнительных резервных копий на локальной и удаленной площадках с помощью знакомых возможностей и функциональности Veeam.

Veeam Agent for Mac основан на проверенном механизме Veeam Agent *for Linux* и предлагает следующие возможности:

- Резервное копирование данных пользователей и содержимого внешних USB-дисков
- Интеграция с конфигурационными профилями решений MDM
- Простое самостоятельное восстановление файлов пользователями через локальный пользовательский интерфейс

Плагины для корпоративных приложений

Общие улучшения

- **Поддержка Capacity Tier масштабируемого репозитория** — основные и дополнительные копии корпоративных приложений теперь могут быть скопированы или перенесены в объектное хранилище уровня Capacity Tier масштабируемого репозитория. Как и для резервных копий на уровне образа, восстановление из резервных копий в объектном хранилище выполняется абсолютно прозрачно.
- **Улучшения производительности** — мы заметно повысили производительность во всех аспектах, в частности благодаря новому подходу к работе с метаданными. Файлы метаданных для каждой резервной копии значительно повысили общую производительность. Сведения о том, как перевести существующие резервные копии в новый формат метаданных представлены в документации по обновлению.
- **Самовосстановление метаданных** — периодическая проверка состояния резервных копий сканирует все точки восстановления каждые 6 часов и воссоздает недостающие файлы метаданных, которые могли пострадать, если резервное копирование прерывалось каким-либо внешним событием. Что бы изменить интервал времени, создайте значение реестра `DbPluginMissingMetaRegenerationAttemptIntervalMinutes` (DWORD) на сервере резервного копирования.
- .

Veeam Plug-in for Oracle RMAN

- **Поддержка Oracle Data Guard** — полная поддержка резервного копирования установок Oracle Data Guard.
- **Улучшенная совместимость с RAC** — теперь поддерживаются установки Oracle RAC с пустым файлом /etc/oratab.

Veeam Plug-in for Oracle RMAN on AIX

Этот новый плагин предлагает те же возможности, принцип установки и настройки, как и плагин для Solaris. Поддерживаемые версии включают IBM AIX 6.1, 7.1, 7.2 и Oracle 11, 12, 18, 19 (версия prc64).

Veeam Plug-in for SAP HANA

- **Поддержка SAP HANA 1.0** — в дополнение к существующей поддержке SAP HANA 2.0 эта версия поддерживает SAP HANA Database 1.0 SPS 12 или позже (инструкции по установке представлены в KB2997). Плагин официально сертифицирован SAP для HANA версий 1.0 и 2.0.

Veeam Plug-in for SAP on Oracle

Этот новый, сертифицированный SAP плагин обеспечивает интеграцию с SAP BR*Tools, что позволяет выполнять резервное копирование баз данных Oracle непосредственно в репозитории Veeam с поддержкой режимов `util_file` и `util_file_online`. Заметьте, что Veeam Plug-in for Oracle RMAN и Veeam Plug-in for SAP on Oracle могут использоваться вместе для выполнения резервного копирования в режиме `rman_util`. Поддерживаются 64-разрядные версии следующих продуктов:

- OC: SLES 11,12 и 15; RHEL 6 и 7; Oracle Linux 6 и 7
- Oracle: от 11.2 до 19.1
- BR*tools: 7.20 Patch 42 или позже

Плагины для корпоративных приложений входят в **Универсальную лицензию Veeam**. При использовании лицензии по количеству сокетов требуется редакция **Enterprise Plus**.

Резервное копирование NAS

Общие улучшения

- **Корневой диапазон защиты** — теперь можно указать весь источник данных (файловый сервер SMB/NFS) в качестве источника для задания резервного копирования общего файлового ресурса. Это позволит защитить все общие ресурсы и экспорты, включая вновь добавленные. Эта новая возможность потребовала внесения изменений в мастер восстановления общих файловых ресурсов для поддержки восстановления из таких резервных копий. В качестве побочного эффекта таких изменений теперь можно настраивать массовое восстановление нескольких общих файловых ресурсов за один запуск мастера. Кроме того, папки, содержащие аппаратные снимки, будут автоматически исключены из обработки при их обнаружении, поэтому вам больше не требуется добавлять их к списку исключений задания резервного копирования.

ПРИМЕЧАНИЕ. Можно конвертировать существующие резервные копии в формат, допустимый для сопоставления с корневым диапазоном во вновь созданном задании резервного копирования с помощью командлета [Convert-VBRNASBackupRootFormat](#).

- **Улучшенная производительность** — производительность заданий резервного копирования общих файловых ресурсов и копирования резервных копий повысилась до 2х раз благодаря использованию нескольких потоков данных между исходным и целевым сервисами Data Mover. Наибольший выигрыш от этого улучшения достигается при переносе данных по сетям с высоким уровнем задержки.
- **Интеллектуальное распределение нагрузки** — при наличии нескольких прокси-серверов задания резервного копирования общих файловых ресурсов будут автоматически выявлять и использовать прокси-сервер с наименьшей загрузкой (как уже делают задания резервного копирования VM). Это позволит повысить нагрузку и еще более эффективно использовать вычислительные ресурсы.
- **Оповещения о заблокированных файлах** — теперь вы сами можете контролировать, показывать ли предупреждения о проблемах с обработкой файлов и их атрибутов в результатах резервного копирования общих файловых ресурсов. Кроме того, путь к файлу аудита, содержащему список заблокированных файлов, теперь указывается в журнале задания.
- **Хранение на основе версий** — чтобы лучше контролировать потребление ресурсов репозитория, вы можете выбрать одну из двух опций: использовать хранение на основе версий только для файлов в архивном репозитории (как в V10) или применять общие настройки хранения для архивного репозитория и репозитория резервных копий.

- **Автоматическое сопоставление при копировании резервных копий** — процессы копирования резервных копий при первом запуске будут автоматически искать первоначальную резервную копию и при ее обнаружении продолжат копирование в инкрементальном режиме.

Интеграция с производственными СХД

- **Интеграция с файлером корпоративных NAS** — интеграции с Dell EMC Isilon, Lenovo DM и NetApp FAS позволяют зарегистрировать весь файлер в качестве источника данных и выполнять резервное копирование общих файловых ресурсов без необходимости получать права доступа к каждому защищаемому ресурсу. Кроме того, резервное копирование для таких источников будет выполняться из нативных аппаратных снимков во избежание блокировки файлов — без сложной настройки и использования скриптов для управления снимками.

***ПРИМЕЧАНИЕ.** Можно конвертировать существующие резервные копии в формат, допустимый для сопоставления с диапазоном на основе файлера NAS во вновь созданном задании резервного копирования с помощью командлета [Convert-VBRNASBackupStorageFormat](#).*

- **Интеграция с нативным отслеживанием изменений файлов** — в V11 задания резервного копирования общих файловых ресурсов могут интегрироваться с Dell EMC Isilon Changelist API для снижения нагрузки на хранилище и улучшения производительности инкрементального резервного копирования в сценариях, когда защищаемые ресурсы имеют большое количество подпапок с низким уровнем изменений.

Интеграция с резервными СХД

- **Крупные BLOB-объекты** — задания резервного копирования общих файловых ресурсов и копирования резервных копий будут автоматически переключаться на использование BLOB-объектов размером 1 ГБ, когда целевым устройством является дедуплицирующая СХД. В результате до 20 раз повышается масштабируемость для СХД, которые поддерживают ограниченное количество файлов на устройстве (например, HPE StoreOnce) и до нескольких раз улучшается производительность резервного копирования и восстановления для дедуплицирующих СХД.

***ПРИМЕЧАНИЕ.** Перевести существующие задания на использование крупных BLOB-объектов можно с помощью командлета [Convert-VBRNASBackupStorageFormat](#).*

- **Экстенды для метаданных** — при использовании масштабируемых репозиторий, состоящих исключительно из медленных устройств, как, например, дедуплицирующие СХД, вы можете повысить производительность резервного копирования и восстановления в несколько раз, добавив небольшой экстенд на основе быстрого устройства, который будет использоваться только для хранения метаданных резервных копий. Эта возможность настраивается только через PowerShell с помощью командлета [Set-VBRRepositoryExtent](#).

Пользовательский интерфейс

Консоль резервного копирования

- **Отсутствие требования прав локального администратора** — консоль резервного копирования больше не требует наличия у оператора учетной записи локального администратора в системе, на которой работает консоль. Это помогает улучшить безопасность, поскольку административные привилегии не придется выдавать всем операторам консоли. Когда потребуются обновление консоли или выполнение сценариев восстановления, для которых требуются права локального администратора, вам будет предложена возможность перезапуска консоли и повторного входа в систему с нужными правами.

- **Потерянные резервные копии** — благодаря новому узлу Orphaned под Backups теперь намного легче отследить резервные копии, не связанные с каким-либо заданием. Ранее такие резервные копии оказывались в узле Imported backups, где их было невозможно выявить.
- **Узлы заданий на основе фильтра** — настраиваемые представления заданий (функция V10) теперь можно добавлять в качестве постоянного узла дерева управления для быстрого доступа к предпочитаемым представлениям, которые вы используете чаще всего.
- **Информация о неизменности резервной копии** — к диалогу свойств резервной копии добавлена колонка, которая показывает срок окончания действия режима неизменности для резервных копий, хранящихся в защищенном репозитории Linux.
- **Временные метки журнала действий** — по многочисленным запросам, помимо колонки продолжительности операции, добавлена колонка временной метки, которая показывает время начала каждой операции. Чтобы отобразить колонку, кликните правой кнопкой мыши на заголовке журнала.
- **Интеграция с центром уведомлений Windows** — теперь мы используем центр уведомлений Windows для демонстрации интерактивных оповещений, например, о том, что конфигурационная БД SQL Server приближается к максимальному размеру (новая возможность V11), задание резервного копирования ждет предоставления носителя и другие важные сообщения, которые раньше показывались во всплывающем сообщении панели задач.
- **Больше не будет путаницы с кнопкой Finish** — кнопка Finish на последнем шаге мастера восстановления файлов и объектов переименована в Browse. Это позволит лучше передать информацию о том, что процесс продолжится выбором объектов. Ранее многие пользователи боялись нажимать эту кнопку из опасений, что восстановление начнется до того, как они выберут, что восстанавливать.
- **Консоль Swagger** — теперь можно открывать интерактивную документацию (на базе Swagger) по RESTful API для сервера резервного копирования непосредственно из главного меню.
- **Устаревшие возможности** — функция преобразования предыдущих цепочек резервного копирования в откаты устарела, поэтому соответствующий флажок был удален в пользовательском интерфейсе для вновь создаваемых заданий. Если вам нужна помощь в переходе с этого режима резервного копирования на другой, изложите, пожалуйста, свой сценарий на форумах Veeam R&D. Мы планируем полностью убрать эту функцию в следующей основной версии в 2022 г.

Enterprise Manager

- **Локализация веб-интерфейса** — мы добавили к Enterprise Manager стандартную для отрасли систему локализации GetText и теперь, благодаря нашим техническим консультантам, Veeam Backup Enterprise Manager v11 поставляется со встроенным переводом на следующие языки: французский, немецкий, итальянский, японский, испанский и упрощенный китайский.
- **Удобный единый вход в систему** — мы изменили пользовательский интерфейс входа в систему, чтобы при едином входе в систему не запрашивалось имя пользователя. Вместо этого мы немедленно перенаправляем пользователей к поставщику услуг идентификации для аутентификации. Это позволяет пользователям из организаций, использующих аутентификацию без ввода учетных данных (например, по смарткарте), подключаться к Enterprise Manager и его порталам.
- **Поддержка SAML для портала самостоятельного резервного копирования vSphere** — портал вызвал большой интерес у многих лиц, не входящих в первоначальную целевую аудиторию, особенно у поставщиков услуг. Чтобы поддержать эту тенденцию, мы добавили интеграцию с SAML, что позволяет поставщикам услуг предоставлять своим заказчикам доступ к portalу путем выделения квот внешним пользователям и группам пользователей. При использовании SAML единственный поддерживаемый режим делегирования — теги vSphere.

- **Улучшения пользовательского интерфейса** — при восстановлении объектов Microsoft Exchange мы теперь будем показывать название почтового ящика рядом с именем пользователя, чтобы избежать путаницы, когда у людей похожи имена. Мы также добавили функциональность поиска объектов при определении области действия роли оператора восстановления.

Лицензирование

Общие улучшения

- **Лучшие изменения — это их отсутствие!** — V11 использует тот же формат лицензионного файла, который был предложен в V10. Такие лицензионные файлы больше не привязаны к конкретным версиям продукта, что позволяет использовать лицензию V10 с V11 при наличии действующего контракта поддержки.
- **Автообновление лицензии** — при обновлении с V9 мастер установки предложит вам автоматически скачать лицензионный файл для V11. Это потребует загрузки ваших установленных лицензий на серверы Veeam. Если ваш сервер резервного копирования не подключен к интернету или вы не хотите загружать действующие лицензии, вы можете скачать файл лицензии с [портала для заказчиков](#).
- **Автообновление лицензии в продукте** — при установке лицензионного файла вам будет предложено выбрать автоматическое обновление лицензии при продлении или расширении вашего контракта. Для этой опции требуется, чтобы сервер резервного копирования периодически отправлял на серверы Veeam идентификаторы лицензии и установки, а также значения счетчиков использования систем. Если вы предпочитаете не делиться этой информацией с Veeam, не активируйте эту функциональность. Вы сможете скачать обновленные файлы лицензии с [портала для заказчиков](#) и установить их вручную.
- **Упрощенное обновление лицензии** — процесс обновления лицензии можно инициировать прямо из диалога с информацией о лицензии. Кнопка Renew перенаправляет пользователя на веб-сайт Veeam, к форме запроса обновления лицензии. Некоторые поля запроса уже будут заполнены на основе информации из вашей установленной лицензии.

Универсальная лицензия Veeam (VUL)

- **Удвоенная защита NAS** — после рассмотрения средней величины скидок, которые наш отдел продаж предоставлял на возможности защиты NAS с помощью VUL, мы решили удвоить объем данных NAS, защищаемый одной лицензией с 250 ГБ до 500 ГБ. Это изменение также означает, что теперь вы можете бесплатно защитить первые 500 ГБ из любого файлового источника (вдвое больше, чем 250 ГБ в V10a) Чтобы воспользоваться этой новой возможностью защиты данных NAS, необходимо перейти на V11.
- **Отказ от редакции Starter** — эта редакция была отменена осенью 2020 г., поэтому V11 не будет принимать такие лицензионные файлы. Скачайте, пожалуйста, замещающий лицензионный файл для Veeam Backup Essentials™ с [портала для заказчиков](#) — это бесплатное обновление на оставшийся срок действия вашего контракта.

Лицензии по количеству сокетов

- **Отказ от редакций продукта** — как и VUL, лицензии по количеству сокетов теперь предлагаются новым заказчикам в единой, полнофункциональной редакции, ранее известной как Enterprise Plus. Заказчики с действующей лицензией по количеству сокетов могут использовать, обновлять и расширять лицензию в имеющейся у них редакции. Если вас интересуют функциональные возможности, не представленные в вашей версии продукта, свяжитесь с представителем Veeam, чтобы узнать о специальных предложениях по переходу на другую редакцию лицензии по количеству сокетов или на VUL.

Редакция Community

- **Теперь еще больше возможностей** — обновленная редакция *Community* V11 включает все новые возможности и улучшения V11, кроме тех, для которых действуют особые требования к лицензированию. Эта редакция также выиграла от изменений в объеме защищаемых данных NAS; теперь бесплатная лицензия обеспечивает защиту 5 ТБ данных NAS. При этом, первые 500 ГБ данных общего файлового ресурса не входят в этот объем.

Поддержите редакцию *Community* путем обновления до [Veeam Backup Essentials](#), если есть такая возможность! Подписка стоит меньше, чем ужин в хорошем ресторане, при этом вы получите доступ ко ВСЕМ функциям и поддержку 24/7! Такие обновления помогают нам и дальше обеспечивать защиту данных корпоративного класса для тех, кто не может себе это позволить.

 Подробнее на
veeam.com/ru

 Скачать бесплатную пробную версию
vee.am/backupru