Повреждение данных и как его избежать. Руководство для новичков.

Содержание

При выборе решения для резервного копирования данных одним из важнейших факторов является его надежность. И это абсолютно оправданно, ведь администраторам нужны гарантии в том, что при необходимости данные можно будет восстановить. Учитывая сложность темы повреждения данных и обилие в ней нюансов, можно с уверенностью сказать, что поставщик, который гарантирует 100%-ную надежность резервных копий, говорит не всю правду.

Тем не менее, многие администраторы резервного копирования уверены в отказоустойчивости резервных копий. Поэтому невозможность восстановления данных из резервной копии вызывает шок и зачастую уверенность в том, что поставщик решения для резервного копирования не выполняет своих обязательств. В реальности существует несколько типов повреждения данных. У каждого из них свои причины, поэтому неправильно возлагать вину исключительно на решение для резервного копирования. Далее вы сможете убедиться, что Veeam® Backup & Replication™ не может являться причиной ни одного из приведенных здесь повреждений данных. В противном случае команда Veeam давно бы все исправила. Многие поставщики решений для резервного копирования, и Veeam в том числе, предоставляют ряд инструментов для снижения риска появления "невосстановимой" резервной копии.

За мой многолетний опыт работы в техподдержке Veeam я часто оказывался в центре подобных ситуаций. В этой статье будут рассмотрены несколько типов повреждений данных и представлены варианты контрмер, которые помогли в реальных ситуациях работы с различными типами инфраструктур Veeam Backup & Replication. Если вы обдумываете вопрос приобретения Veeam Backup & Replication и используете нашу тестовую версию, надеюсь, что статья поможет вам в двух аспектах:

1. Сформировать правильные ожидания от решения Veeam: что мы можем и не можем обещать.

2. Убедиться, что Veeam Backup & Replication обладает всеми нужными инструментами, которые, при их правильном использовании, могут защитить от потери данных.

Заказчикам с действующей лицензией я советую прочитать всю статью, чтобы узнать о потенциальных рисках и оптимальных настройках Veeam Backup & Replication, и убедиться, что вы используете все возможности решения.

Важное замечание.

Большинство рекомендаций является результатом личного опыта работы с запросами заказчиков в службу поддержки. Эта статья не призвана служить исчерпывающим руководством и не может охватить все возможные ситуации. В будущем возможно появление новых угроз. Если у вас возникла проблема с повреждением данных, мы всегда рекомендуем создать запрос в службу поддержки Veeam, где инженеры смогут проанализировать и решить вашу проблему.

"Но резервное копирование было успешным!"

Именно эту фразу сотрудники службы поддержки иногда слышат от заказчиков, когда сообщают им неутешительные известия. Для нас, инженеров службы поддержки, это означает только одно — фундаментальное недопонимание процесса резервного копирования и возможностей Veeam Backup & Replication. Перенос ответственности за состояние оборудования, операционной системы и приложений с инструментов для мониторинга на Veeam Backup & Replication — большая ошибка. Конечно, иногда кажется, что у Veeam Backup & Replication есть подобные возможности. Решение состоит из нескольких компонентов и использует большое количество API сторонних производителей, поэтому в моей практике я встречал многочисленные случаи, когда ошибки в Veeam Backup & Replication открывали инфраструктурные проблемы, о которых заказчики даже не подозревали. Однако это, хоть и позитивный, но побочный эффект.

Перед тем, как мы перейдем к углубленному обсуждению типов повреждения данных и соответствующих контрмер, важно осветить несколько фундаментальных принципов, которые сами по себе могут помочь в выявлении потенциальных рисков повреждения резервных копий. Главный факт состоит в том, что: Veeam Backup & Replication выполняет резервное копирование ВМ на уровне образа ее диска и сохраняет эту информацию в виде файла резервной копии. Если ВМ содержит поврежденные данные (например, один из томов превратился в неформатированное пространство), они в таком же виде будут находиться и в резервной копии. Если ВМ неправильно сконфигурирована (например, использует независимый диск или физический RDM), это приведет к отсутствию соответствующих данных в резервной копии. Если что-то случится с резервной копией (из-за проблем с хранилищем, вирусных атак или случайного удаления), эту резервную копию уже нельзя будет использовать.

Все эти примеры могут казаться очевидными, но они превосходно иллюстрируют некоторые из жалоб, которые мы получаем в нашей повседневной практике. Таким образом, вы можете стать своим собственным консультантом: правильно оценивайте качество данных, резервное копирование которых вы выполняете, а при возникновении потенциальных проблем старайтесь выявить первопричину в вашей среде.

Типы повреждения данных

В этом разделе мы рассмотрим самые распространенные ситуации, которые могут привести к невозможности восстановления данных из резервной копии.

"Не удалось выполнить декомпрессию блока LZ4" и похожие случаи

Как выявить повреждение данных: SureBackup®, проверка состояния, Veeam Validator, попытка выполнить декомпрессию поврежденного блока.

Статья базы знаний на эту тему: https://www.veeam.com/kb1795

Данные внутри резервных копий (.VBK, .VIB, .VRB) хранятся в сжатых блоках. Из-за проблем хранилища блок может быть сохранен некорректно. Передаю слово нашему старшему вице-президенту Антону Гостеву, который проводит интересную аналогию.

> *"Если выражаться человеческим языком, проблема выглядит так:*
>
> *1) Мы просим хранилище написать "мама", но оно пишет "папа" и сообщает об успешном выполнении операции.*
>
> *2) Мы просим хранилище написать "мама" и оно пишет "мама" и сообщает об успешном выполнении. Но при попытке чтения вы получаете "мапа".*
>
> *3) Мы просим хранилище записать "мама" на диски, и оно сообщает об успешном выполнении, но на самом деле не записывает данные на диски, а только держит их в буфере памяти в течение короткого времени для оптимизации производительности массива."*
>
> *Отвечая на ваш потенциальный вопрос, мы можем судить об успешности операции только по сообщениям хранилища, и потому считаем задание успешно выполненным. Поэтому очень важно использовать технологию SureBackup для проверки корректности записанных в резервную копию данных, особенно если подобная ошибка уже возникала и хранилище, таким образом, находится под подозрением.*

Даже если данные были записаны корректно, они могут быть повреждены в дальнейшем. Например, в результате так называемой деградации данных (термин "bit rot"). Ни один поставщик систем хранения не может гарантировать абсолютную целостность данных, скорее нужно говорить о количестве ошибок на определенный объем данных. Мы можем только порекомендовать не пользоваться дешевыми NAS-устройствами. В них применяются сомнительные технологии оптимизации для повышения производительности, которые могут привести к повреждению данных. Данную информацию Антон озвучил уже несколько лет назад на форуме Veeam.

Если пара нулей и единичек внутри сжатого блока данных поменяются местами, попытка выполнить декомпрессию (обычно, во время восстановления) не увенчается успехом. В подобных случаях есть хорошие, а есть и плохие новости. Хорошая новость состоит в том, что выполнить восстановление из такой резервной копии все-таки возможно. Служба поддержки Veeam может предоставить специальные модифицированные агенты, которые позволяют пропустить поврежденные блоки. Таким образом, если повреждение данных минимально, сохраняется достаточно высокий шанс на восстановление. А плохая новость состоит в том, что такое повреждение данных довольно-таки сложно выявить. Большинство операций в Veeam Backup & Replication не требует декомпрессии блоков. Поврежденный блок данных может переноситься из одной резервной копии в другую — через слияние, архивирование, создание синтетической полной резервной копии — и при этом он не будет обнаружен. Контрмерой в подобном случае будет регулярная верификация резервных копий и некоторые специальные настройки заданий резервного копирования, которые мы обсудим чуть дальше в статье.

Заметьте, что сообщения об ошибках могут быть разными, в зависимости от того, какая часть резервной копии пострадала. Здесь невозможно дать описание каждой ошибки, поэтому в случае возникновения проблем обязательно создайте запрос в службу поддержки Veeam.

Ошибка "Повреждены все экземпляры метаданных в хранилище"

Как выявить повреждение данных: SureBackup, проверка состояния, Veeam Validator, практически любая попытка использовать резервную копию.

Статья базы знаний на эту тему: https://www.veeam.com/kb1886

Внутри каждого файла резервной копии (.VBK, .VIB, .VRB) существуют специальные метаданные, которые содержат информацию о том, что хранится в файле, и где именно (аналогично главной файловой таблице NTFS). Без метаданных содержимое каждого файла резервной копии становится бессмысленным набором нулей и единичек. Учитывая важность метаданных, они сохраняются дважды в файле резервной копии, причем оба экземпляра метаданных никогда не обновляются одновременно.

Если один из экземпляров метаданных будет поврежден, это не приведет ни к каким плохим последствиям. Veeam продолжит нормально работать и рано или поздно метаданные будут обновлены актуальной информацией. В случае же повреждения обоих экземпляров метаданных часть цепочки резервных копий, в которую входит поврежденный файл, станет невосстанавливаемой. К сожалению, восстановить данные из подобной резервной копии невозможно. Создание цепочки резервных копий необходимо будет начать заново, путем выполнения полного резервного копирования.

Если вы столкнетесь с подобным повреждением данных, скорее всего оно будет результатом серьезных проблем с хранилищем, так как для этого должны быть повреждены две различные части файла, причем за короткий промежуток времени. В следующей главе мы поговорим об инструментах, которые могут помочь проверить состояние хранилищ данных.

Как обычно, в такой ситуации есть хорошие и плохие новости. Плохая новость состоит в том, что такую резервную копию не получится использовать для восстановления данных. В подобных случаях, к сожалению, не сможет помочь даже служба поддержки Veeam. Единственным утешением может служить то, что если цепочка резервных копий активно используется, то такое повреждение будет выявлено довольно быстро. Даже если не выполняются периодические проверки, любая попытка использовать поврежденный файл (например, при инкрементальном резервном копировании или архивировании резервных копий) приведет к следующей ошибке: "Все экземпляры метаданных повреждены. Не удалось скачать диск. Соединение по переподключаемому протоколу закрыто. Не удалось загрузить диск. Агенту не удалось задействовать метод {DataTransfer.SyncDisk}."

Повреждение данных, вызванное ошибками отслеживания измененных блоков данных (CBT)

Как выявить повреждение данных: SureBackup или восстановление вручную.

Статьи базы знаний на эту тему:
https://www.veeam.com/kb1940, https://www.veeam.com/kb2075, https://kb.vmware.com/s/article/55800

Повреждение данных, вызванное ошибками CBT, стало кошмаром для многих пользователей vSphere, а также отличным примером "скрытого повреждения данных." Действительно, резервное копирование выполнялось нормально, а проверка состояния копий не выявила повреждения данных. Однако, если решение для резервного копирования будет обрабатывать испорченные данные, тот они же и будут в резервных копиях. А CBT иногда передает решению Veeam Backup & Replication именно такие данные. Повреждение данных, вызванное ошибками CBT, можно обнаружить только с помощью технологии SureBackup, которая запускает ВМ в изолированной среде, или при попытке восстановления данных (но тогда это может быть слишком поздно).

Несколько версий vSphere содержали различные ошибки CBT. Они были в версии 5.5, в версии 6.0 (дважды), а из последних версий — в 6.5 и 6.7, когда использовались vVols. Поэтому, хотя сейчас все выглядит стабильно, нет гарантии, что ошибки не появятся снова. Это подчеркивает необходимость внедрения соответствующего процесса верификации, который мы обсудим позднее.

Внутренние неполадки ВМ

Как выявить повреждение данных: SureBackup, ручное восстановление, правильный инструмент мониторинга в гостевой ОС.

До сих пор мы исходили из того, что данные повреждаются из-за внешнего воздействия. Но это далеко от правды. Данные внутри ВМ точно так же подвержены повреждениям. Нередки случаи, когда дисковый том с записанными на нем данными превращается в неформатированное пространство или редко используемая база данных становится несогласованной. При отсутствии должного мониторинга до обнаружения проблемы может пройти немало времени. Особенно печально, когда отсутствует долгосрочное хранение данных и после выявления повреждения оказывается, что последняя валидная точка восстановления уже была удалена.

Можно ли винить за это решение для резервного копирования? По-моему, нет. Правильное резервное копирование подразумевает хорошее состояние исходных данных (вы же помните — повреждения на входе, повреждения на выходе!). Veeam Backup & Replication не предлагает возможностей мониторинга приложений или операционной системы (ОС). Хотя, некоторые настройки заданий резервного копирования могут помочь (подробная информация будет представлена дальше). Однако полное перекладывание ответственности — рецепт катастрофы.

Ошибки конфигурации

Ошибки конфигурации также могут привести к потерям данных, поэтому их необходимо упомянуть. Большинство ошибок конфигурации происходят из-за неправильного понимания резервного копирования на уровне гипервизора и смысла конкретных настроек. Результатом обычно является отсутствие каких-либо данных в резервной копии или присутствие всех данных, но некоторых — в невосстанавливаемом виде. Вот некоторые примеры из практики службы поддержки:

1. **Независимые диски и физические RMD**. Невозможно сделать их снимок, поэтому эти данные не входят в резервную копию. Veeam Backup & Replication информирует пользователя об этой ситуации в разделе статистики задания, но зачастую эта информация остается незамеченной, пока не становится слишком поздно.

2. **iSCSI-диски гостевой ОС виртуальной машины**. На уровне гипервизора эти диски не видны, а значит их данные не будут включены в резервную копию.

3. **Исключения в заданиях резервного копирования**. Veeam Backup & Replication позволяет исключать из резервного копирования отдельные диски и ВМ целиком (если ВМ добавляются как часть контейнера). Из-за ошибки оператора такие исключения могут быть забыты.

4. **Удаление данных ВМ из-за настроек хранения** Если резервное копирование ВМ не выполняется в течение какого-то периода (например, ВМ добавляется к заданию как часть контейнера, а затем переносится и перестает быть частью контейнера), данные ВМ могут быть утеряны. Если резервное копирование выполняется в прямом инкрементальном режиме, данные ВМ могут быть потеряны, когда будет удалена последняя точка восстановления, содержащая эту ВМ. При использовании других режимов резервного копирования не забывайте об опции "стереть удаленные объекты". Если ее значение слишком низкое, вы рискуете случайно потерять свои данные!

5. **Стаб-файлы.** Некоторые поставщики предлагают ПО, которое переносит файлы в специальное хранилище, а вместо файлов оставляет на диске "ссылки-заглушки". При резервном копировании ВМ с такими ссылками вы не копируете реальные файлы. Вместо этого вы получаете резервную копию с "пустыми" файлами.

Дисковые пространства Microsoft в ВМ. Такую конфигурацию не поддерживают ни Veeam, ни Microsoft. Подробнее: https://www.veeam.com/kb1989

Встречается немало случаев, которые заставляют инженеров службы поддержки задуматься. Золотое правило — заранее попробовать несколько различных восстановлений, чтобы избежать сюрпризов в критические моменты.

Инструменты и советы

Теперь, когда мы познакомились с потенциальными проблемами, посмотрим, что может предложить Veeam Backup & Replication для минимизации риска невозможности восстановить данные.

Стратегия резервного копирования "3-2-1"

Все проверки, которые предлагает Veeam Backup & Replication, служат для заблаговременного предупреждения пользователя о невозможности восстановления данных. Они не помогут в ситуации, когда данные уже отсутствуют в производственной среде. Если вы храните более одного экземпляра резервной копии, это поможет восстановить данные. Поэтому внедрение правила "3-2-1" должно быть вашим основным приоритетом, если вы хотите существенно снизить риски потери данных. К счастью, Veeam Backup & Replication поддерживает ряд разнообразных целевых устройств для выполнения резервного копирования: Архивирование резервных копий (в том числе, в облако), магнитная лента и аппаратные снимки (если у вас совместимое хранилище).

SureBackup

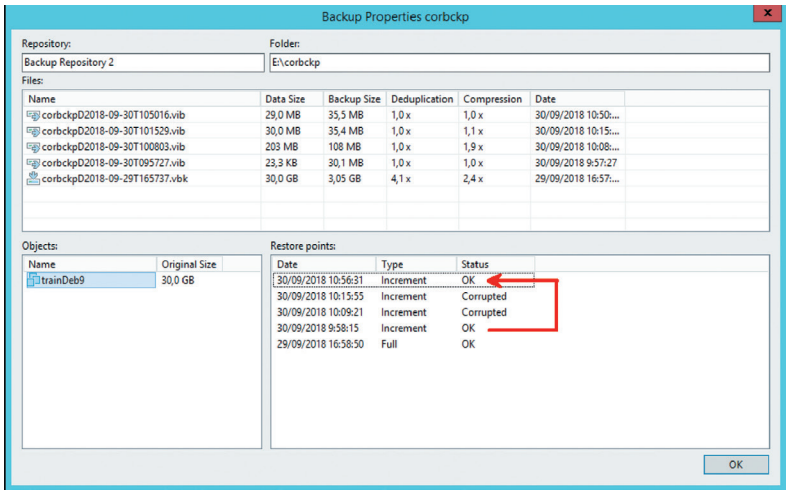
SureBackup — инструмент Veeam Backup & Replication для проверки возможности восстановления данных из резервной копии. Этот инструмент позволяет убедиться в том, что гостевая ОС загружается, а приложения отвечают. (Veeam Backup & Replication содержит ряд преднастроенных тестовых скриптов для некоторых приложений, но вы также можете создать собственные.)

Проверка состояния

Проверка состояния — относительно новая функциональность, которая заключается в повторном вычислении хеш-значений каждого блока данных в резервной копии и сравнении их со значениями, хранящимися в метаданных файла. Обратите внимание:

1) Проверка выполняется после резервного копирования. Это значит, что она запускается только после того, как была создана новая точка восстановления. Если вы запланируете эту проверку на день, в который не выполняется резервное копирование, проверка запустится после следующего раза, когда будет выполнено резервное копирование.
2) Проверка состояния — очень ресурсоемкое задание, поэтому занимает достаточно много времени. Точная продолжительность зависит от производительности хранилища. Для устройств NAS требуется больше времени, но длительнее всего эта проверка происходит на дедуплицирующих СХД.
3) Если задание использует прямой инкрементальный режим, а цепочка резервных копий состоит из нескольких сегментов (VBK+VIB), будет проверен только самый последний сегмент.
4) На проверку состояния оказывают воздействие настройки окна резервного копирования. Учитывая длительность проверки состояния, низкая продолжительность окна резервного копирования может привести к постоянным сбоям этой проверки.

Если проверка состояния найдет повреждение данных, она проинформирует пользователя (резервное копирование завершится с ошибкой) и немедленно начнет процесс исправления. В зависимости от режима резервного копирования, типа повреждения данных и типа точек восстановления возможны несколько сценариев:



Ошибка декомпрессии в инкрементальной резервной копии. Обратите внимание на картинку. Во время проверки было выявлено повреждение данных в инкрементальной резервной копии corbckpD2018-09-30T100803.vib. Соответственно, следующие две инкрементальные резервные копии также были признаны непригодными. После этого начинается процесс исправления. Этот процесс создает снимок ВМ в производственной среде и переносит поврежденные блоки от ВМ к последней точке восстановления, "переподключая" последний файл VIB к самой последней валидной точке восстановления. Поврежденные точки восстановления останутся в цепочке резервных копий, но их нельзя будет использовать. Они все еще содержат некоторые валидные блоки, поэтому мы не будем их удалять, чтобы минимизировать нагрузку на сеть в процессе исправления (однако Veeam Backup & Replication все равно будет вынужден читать все содержимое диска ВМ, чтобы найти нужные блоки).

Ошибка декомпрессии в полной резервной копии. Аналогично предыдущему сценарию, однако, поскольку поврежден файл VBK, Veeam Backup & Replication будет вынужден признать непригодной для восстановления полную цепочку резервных копий. Далее недостающие блоки переносятся в последний файл VIB, что позволит восстановить ВМ в ее последнее состояние.

Повреждение метаданных в инкрементальной резервной копии Поскольку повреждение метаданных приводит к полной непригодности резервных копий, информация о поврежденном инкременте и всех зависимых инкрементах удаляется из цепочки. После этого процесс проверки состояния создает новый инкремент с нуля и подключает его к последней валидной точке восстановления в цепочке резервных копий. Имейте в виду, что, хотя поврежденные точки восстановления удаляются из базы данных Veeam Backup & Replication, файлы остаются в репозитории (для аналитики). Вам будет необходимо удалить их вручную, чтобы освободить место.

Повреждение метаданных в полной резервной копии. Если повреждены метаданные в файле VBK, вся цепочка резервных копий становится непригодной. Задание запустит активное полное резервное копирование, чтобы воссоздать файл VBK с нуля.

Обратно инкрементальная цепочка резервных копий. Проверка состояния не проверяет точки восстановления (.VRB). Проверяются только файлы VBK. В зависимости от типа повреждения файлы дополняются валидными блоками или полностью воссоздаются.

Veeam Validator

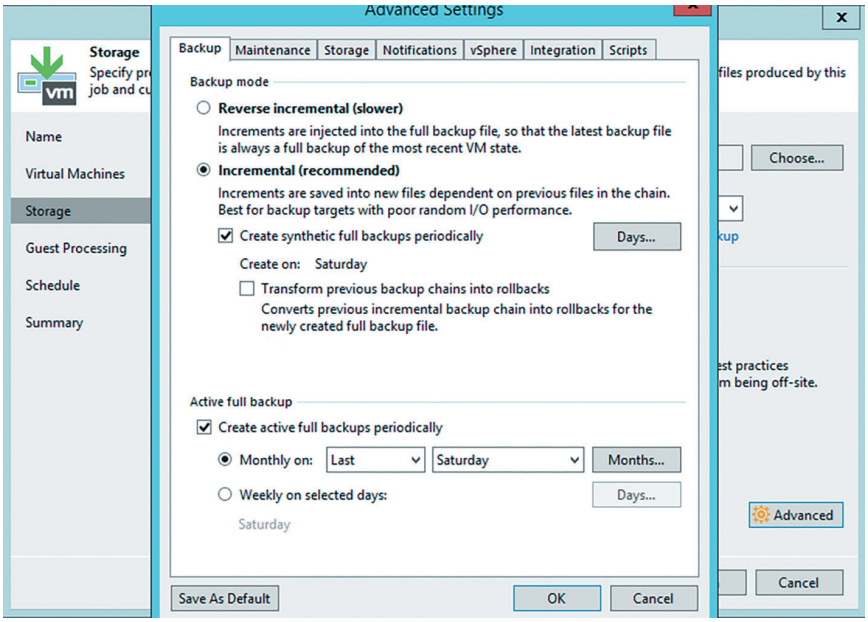
Проверка состояния может выполняться только после создания новой точки восстановления, но Validator — автономный инструмент, который позволяет выполнять аналогичные проверки по ситуации. Подробная информация об использовании этого инструмента представлена в статье базы знаний https://www.veeam.com/kb2086. Процесс верификации, который использует Validator, идентичен процедуре проверки состояния. Однако, в отличие от этой процедуры, Validator не может исправить поврежденные блоки в случае их обнаружения.

Если проверка постоянно выявляет поврежденные точки восстановления, что-то может быть не в порядке с вашим хранилищем. В этом случае вы можете протестировать хранилище с помощью инструмента с открытым кодом Corruption Finder (CoFi), разработанного инженером службы поддержки Veeam Всеволодом Зубаревым. CoFi эмулирует поведение Veeam Backup & Replication, записывая блоки данных и вычисляя их хеш-значения. Позже хеш-значения вычисляются заново, чтобы убедиться, что они изменились. В зависимости от частоты обнаружения повреждений, вы можете настроить CoFi для записи и проверки определенного объема данных. Скачать CoFi можно по ссылке https://github.com/yandexx/cofi.

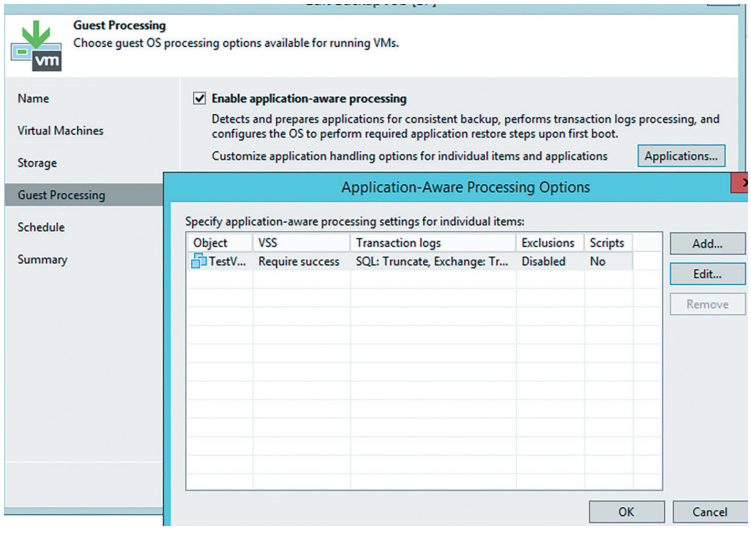
Рекомендуемые настройки заданий Veeam Backup & Replication

Выбор правильных настроек для заданий Veeam Backup & Replication может прямо или косвенно повысить отказоустойчивость резервного копирования.

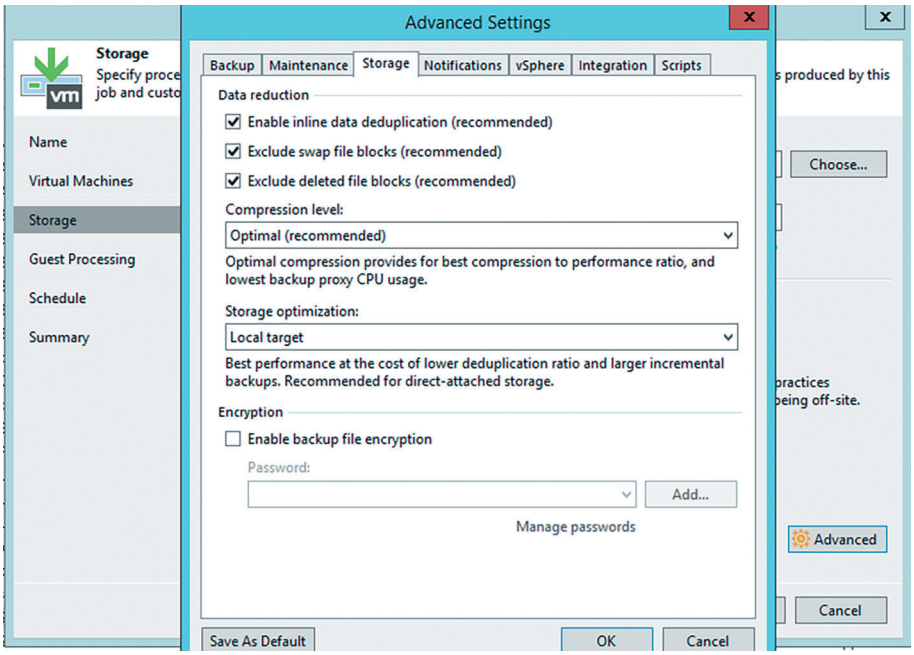
Режим резервного копирования. У каждого из режимов есть свои плюсы и минусы, но самым надежным однозначно считается прямой инкрементальный режим. Регулярно создавая полные резервные копии, вы разделяете цепочку резервных копий на несколько сегментов, снижая таким образом вероятность потери всей цепочки сразу. Полные резервные копии могут быть созданы "активно" или синтетически. Как уже было отмечено, поврежденный блок данных может быть перенесен в синтетическую полную резервную копию из предыдущей точки восстановления, что делает активную полную резервную копию более надежной. Если вы не хотите регулярно создавать активные полные резервные копии, можно использовать смешанный сценарий. Например, создавать синтетическую копию еженедельно, а активную полную — раз в месяц. Если, согласно расписанию, в какой-то день должны быть созданы обе эти копии, Veeam Backup & Replication создаст только активную полную резервную копию.



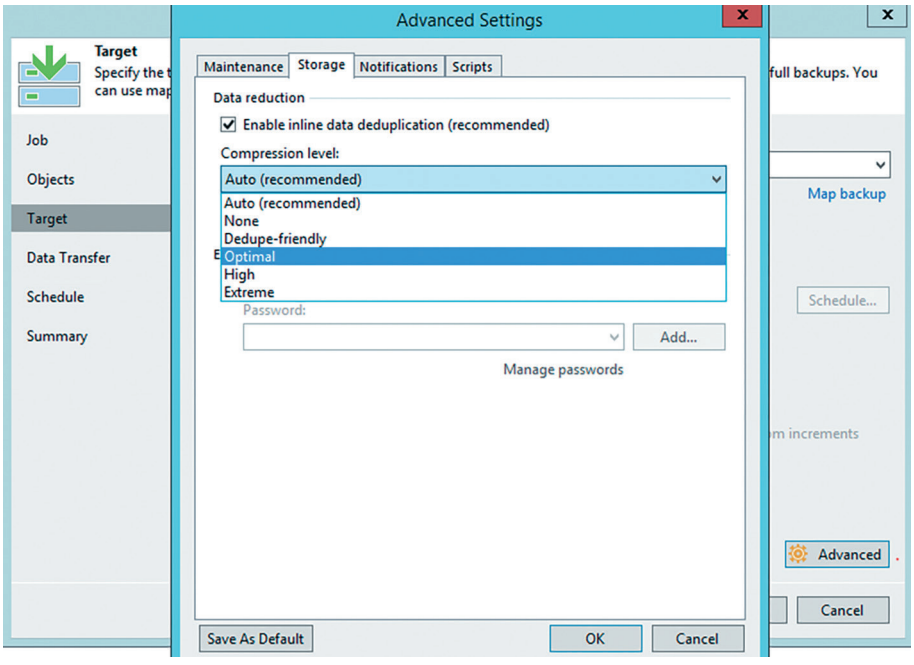
Обработка данных с учетом состояния приложений (AAP). На машинах под управлением ОС Windows эта настройка использует технологию VSS, которая работает с поддерживающими ее томами и приложениями. AAP используется в первую очередь для создания резервной копии, согласованной на уровне приложений. Однако, поскольку VSS — это часть функциональности Windows, иногда ошибки VSS помогают обнаружить более глубокие проблемы с ВМ или приложениями. Но не забудьте выставить "require success" в ее настройках.



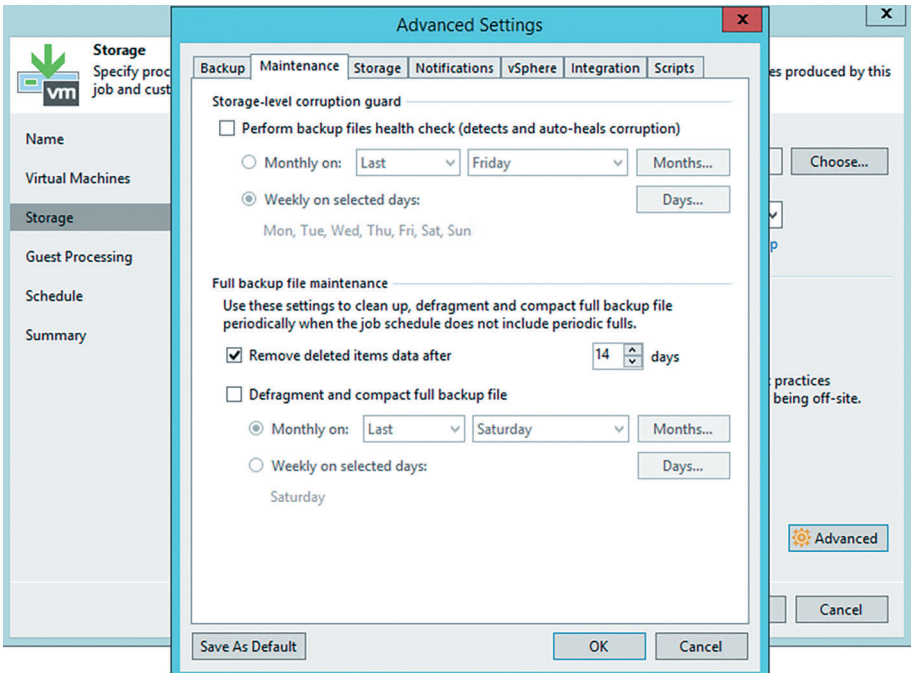
Исключение блоков файлов подкачки и удаленных файлов. Основной целью этих технологий также является сокращение размеров резервных копий. Однако, поскольку технологии действуют путем чтения главной файловой таблицы NTFS, их ошибки могут означать проблемы с томом. Исключения работают только с томами NTFS.



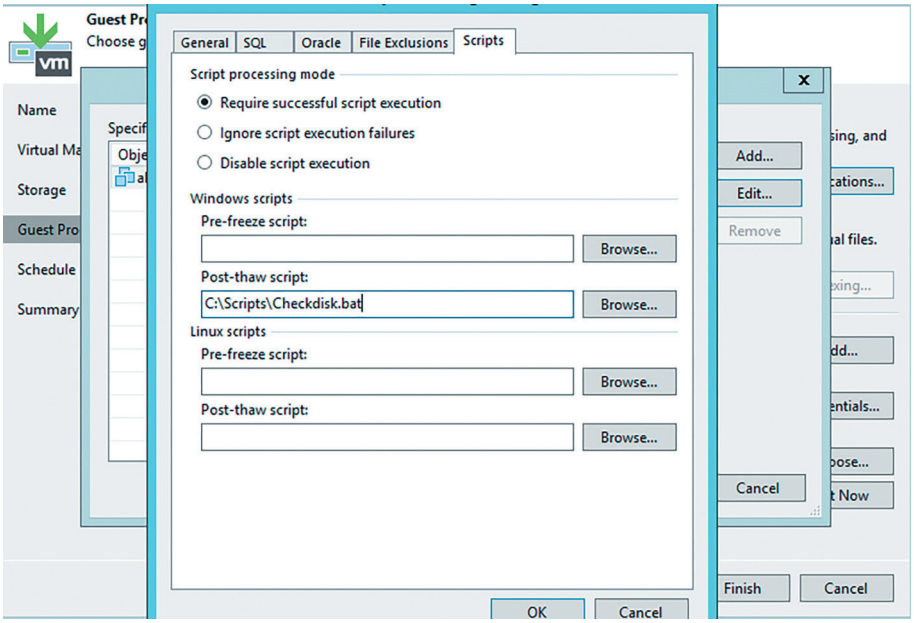
Архивирование резервных копий. Задания архивирования резервных копий также можно использовать для проверки возможности восстановления. Эти задания позволяют выбрать режим сжатия данных. По умолчанию он является автоматическим, то есть задание архивирования использует тот же механизм сжатия данных, что и исходное задание резервного копирования. Это также означает, что поврежденный блок данных может быть скопирован "как есть", и в итоге он окажется в архивной цепочке резервных копий. Если вы выберете другой механизм сжатия, отличный от использованного в задании резервного копирования, сжатие данных будет выполняться заново. При этом сначала будет осуществляться декомпрессия, а для поврежденных блоков данных она завершится с ошибкой. Не рекомендуется выбирать высокие уровни сжатия данных, так как они приводят к интенсивной нагрузке ЦП. Лучше попробуйте "оптимальный" уровень и уровень "с поддержкой дедупликации", особенно если ваше целевое устройство — дедуплицирующая СХД.



Стирание удаленных объектов. Если задание работает в режиме, отличном от прямого инкрементального, не выбирайте слишком низкие значения для этой опции. Например, если вы выберете значение в один день, а какая-либо ВМ будет исключена на один день из резервного копирования, все ее данные будут стерты из цепочки резервных копий.



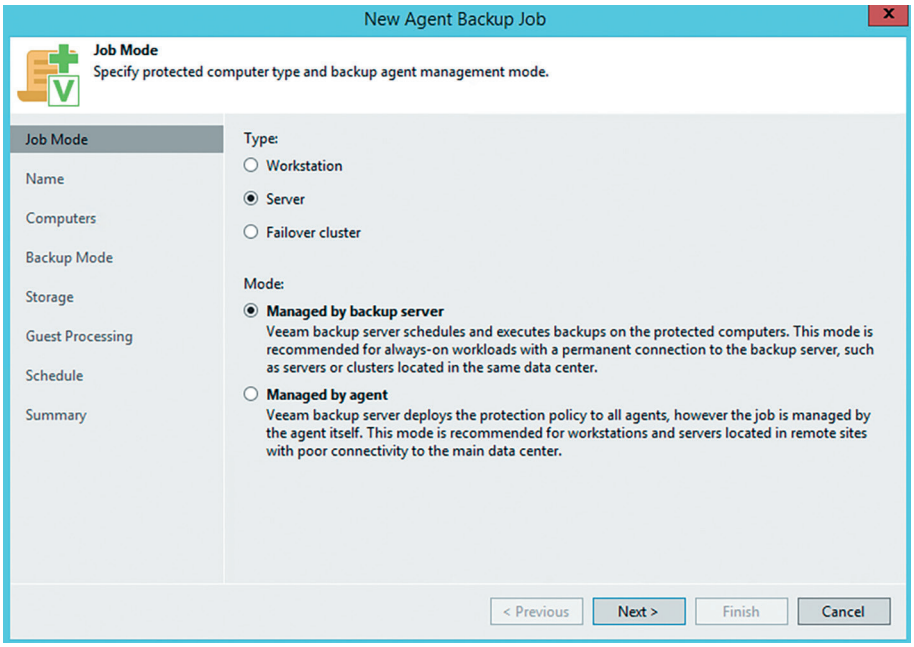
Скрипты для гостевой ОС. В ходе выполнения заданий Veeam Backup & Replication позволяет пользователям выполнять их собственные заранее подготовленные скрипты для гостевой ОС. Например, вы можете написать скрипт для запуска Checkdisk и создания отчета.



А что насчет Veeam Agents?

Новые решения Veeam Agent *for Microsoft Windows* и Veeam Agent *for Linux* уже приобрели популярность среди заказчиков Veeam. Поэтому было бы ошибкой не упомянуть здесь о них. Поскольку Veeam Agent *for Microsoft Windows* и Veeam Agent *for Linux* предназначены для резервного копирования физических машин, они работают непосредственно на уровне ОС и многие из соображений, изложенных в этой статье, к ним неприменимы. Однако две самые распространенные проблемы — ошибки декомпрессии и повреждения метаданных — актуальны и для резервных копий, созданных с помощью этих решений. Что может предложить Veeam в качестве меры безопасности?

Veeam Backup & Replication 9.5 Update 3 позволяет управлять решениями Veeam Agents из консоли Veeam Backup & Replication. Благодаря такой интеграции Veeam Agents могут использовать преимущества Veeam Backup & Replication. Управление Veeam Agents может осуществляться двумя способами: с помощью "политик резервного копирования" или "заданий резервного копирования". "Политика резервного копирования" — это конфигурация, которая может быть направлена независимо установленному Veeam Agent. Если вы выбираете репозиторий Veeam Backup & Replication в качестве целевого устройства, это обеспечивает только ограниченную интеграцию. Для полной интеграции необходимо создать "задание резервного копирования" и выбрать опцию "Managed by backup server" (управление сервером резервного копирования).



После этого вы сможете включить периодические проверки состояний в разделе Storage — Advanced — Maintenance. Резервные копии, созданные с помощью Veeam Agents, также можно будет архивировать или переносить на магнитную ленту с помощью соответствующих заданий — для соблюдения правила "3-2-1". К сожалению, наш самый эффективный инструмент, SureBackup, не может быть использован с Veeam Agents (по крайней мере, пока), поскольку эти решения работают с физическими машинами.

Интеграция с консолью Veeam Backup & Replication предлагается для платных редакций Veeam Agents.

Заключение

Риск повреждения данных резервных копий присутствует всегда. Минимизация этого риска — задача каждого ответственного администратора резервного копирования. Veeam Backup & Replication предлагает все необходимые инструменты для минимизации риска потери данных. Мы надеемся, что эта статья помогла вам лучше разобраться в причинах возникновения повреждений данных и предоставила некоторые идеи для улучшений в вашей среде.

Как мы уже упомянули, одной из самых эффективных возможностей Veeam для предотвращения повреждений данных является технология SureBackup. Она помогает выявить неполадки инфраструктуры (например, систем хранения), а также потенциальные системные проблемы с записью резервных копий Veeam.

О компании Veeam Software

Veeam® — мировой лидер в сфере управления данными в облаке. Платформа Veeam Availability Platform™ — это наиболее полное решение, позволяющее заказчикам автоматизировать управление данными и обеспечить их доступность. Компания Veeam насчитывает более 330 000 заказчиков в разных странах, в том числе 82% компаний из списка «Fortune 500» и 58% компаний из списка «Global 2000». Veeam лидирует по показателям удовлетворенности заказчиков, в 3,5 раза превышая средний уровень по отрасли. Глобальная экосистема Veeam включает в себя несколько тысяч партнеров, эксклюзивных реселлеров, включая Cisco, HPE, Lenovo и NetApp, а также 21 700 поставщиков облачных услуг и сервисов. Главный офис Veeam расположен в г. Баар, Швейцария, а региональные офисы открыты более чем в 30 странах. Подробную информацию о компании можно найти на сайте https://www.veeam.com. Подписывайтесь на Veeam в Твиттере @veeam.

VEEAM

Cloud Data

Backup for what's next

5 Stages of Cloud Data Management –
start your journey today!