10 рекомендаций по резервному копированию данных vSphere

Дата: 30 июля, 2019 г.
Veeam Version 9.5 Update 4b
VMware Version 6.7

Ханнес Каспарик
Старший аналитик, Veeam Product Management

Краткий обзор

Практика виртуализации серверов широко распространена по всему миру. В 2019 г. VMware по-прежнему является лидером этого сектора рынка, а многие заказчики Veeam® предпочитают использовать именно VMware vSphere в качестве платформы виртуализации. Эта статья предлагает рекомендации по резервному копированию и обеспечению доступности данных VMware vSphere с помощью Veeam Backup & Replication™ 9.5. Статья не содержит рекомендаций по работе с Hyper-V или решениями Veeam Agents.

Предисловие

Практика виртуализации серверов широко распространена по всему миру. В 2019 г. VMware по-прежнему является лидером этого сектора рынка, а многие заказчики Veeam предпочитают использовать именно VMware vSphere в качестве платформы виртуализации. Резервное копирование виртуальных машин (ВМ) vSphere — это только часть обеспечения доступности сервисов. Резервные копии — основа для восстановления данных, поэтому они всегда должны быть под рукой. Больше всего для резервного копирования важно правило «3-2-1».

Оно означает, что необходимо хранить как минимум три экземпляра данных: производственные данные, основную резервную копию и дополнительную резервную копию. Резервные копии рекомендуется хранить на двух различных, независимых типах носителей. Независимость означает отсутствие зависимостей с технической точки зрения и очень важна здесь! Одну из резервных копий следует разместить в удаленном автономном хранилище, подальше от стихийных бедствий, вредоносного ПО и неавторизованного персонала. Например, мы добавили защиту от «инсайдеров» для Veeam Cloud Connect в Veeam Backup & Replication 9.5 Update 3. Магнитная лента по-прежнему актуальна для удаленного хранения резервных копий.

Veeam Backup & Replication помогает превратить правило «3-2-1» в правило «3-2-1-0». Ноль означает отсутствие проблем при восстановлении данных благодаря автоматизированному тестированию резервных копий с помощью технологии Veeam SureBackup®. Эта технология помогает находить логические проблемы в резервных копиях. Например, если кто-то установил обновления, но не перезагрузил систему. Тогда после перезагрузки может появиться синий экран.

В этом документе представлены рекомендации по работе с Veeam Backup & Replication и VMware vSphere. Рекомендации относятся только к Veeam и VMware. Обратите внимание, что статья не содержит рекомендаций для других гипервизоров.

В статье представлены следующие рекомендации:

- обязательное наличие стратегии резервного копирования и восстановления данных, соответствующей потребностям вашего бизнеса;
- правильное определение необходимого объема ресурсов;
- обеспечение работы VSS на машинах Windows;
- обеспечение достаточного количества свободного пространства в хранилище резервных копий.

Эти рекомендации актуальны для резервного копирования данных как VMware и Hyper-V, так и физических серверов.

Перед планированием или внедрением любого решения необходимо с точностью сформулировать требования. В идеальном мире требования предъявляет бизнес, включая целевые показатели точки (RPO) и времени (RTO) восстановления. Необходимо ли только резервное копирование данных или также послеаварийное восстановление?

Получив эту информацию, можно приступать к оценке параметров необходимого оборудования. Они включают количество ядер ЦП, объем памяти, а также требования к пропускной способности сетей WAN, LAN и SAN. Также потребуются достаточно быстрые СХД для хранения исходных данных и резервных копий, которые позволят поддерживать необходимую скорость резервного копирования.

Следующий шаг — само резервное копирование. При обработке данных Veeam использует Microsoft VSS, что позволяет создавать резервные копии ВМ Windows с учетом состояния приложений. Этот механизм не использует VMware Tools. Для надежной обработки данных с учетом состояния приложений необходима правильная работа компонентов «VSS Writer» на всех ВМ.

№1 Используйте текущие версии Veeam и vSphere

Последние версии Veeam Backup & Replication обеспечивают максимальную производительность при работе со средой VMware vSphere. Производительность Veeam Backup & Replication 9.5 намного выше, чем у более ранних версий, особенно в среде vSphere. Это достигается за счет таких нововведений, как служба брокера Veeam и методы обработки без использования VADP — режимы «Hot-Add», «Direct NFS» и резервное копирование с помощью аппаратных снимков.

Со стороны VMware в ESXi версии 6.x была улучшена консолидация снимков ВМ. Это обеспечивает более стабильную работу ВМ с высокой интенсивностью операций ввода-вывода при удалении снимка после резервного копирования.

Рекомендация. *Используйте улучшения в последних версиях Veeam Backup & Replication и vSphere.*

№2 Выбирайте оптимальный режим резервного копирования

Veeam Backup & Replication предлагает три различных режима передачи данных при резервном копировании ВМ vSphere. У всех режимов есть сильные и слабые стороны, и ни один из них не является наилучшим. Выбор одного из трех режимов зависит от требований и среды:

1. Сетевой режим или NBD.
2. Режим прямого доступа к хранилищу («Direct Storage Access»).
3. Режим виртуального устройства или «Hot-Add».

В свойствах каждого прокси-сервера можно выбрать нужный режим в разделе «Transport Mode», как показано на Рис. 1.

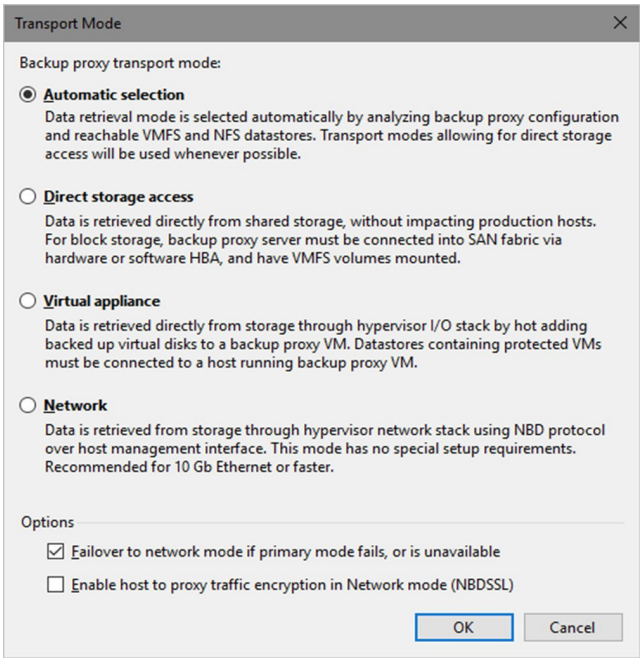

Рис. 1. Выбор режима передачи данных.

Сетевой режим или NBD — простейший способ резервного копирования данных VMware. Прокси-сервер Veeam использует порт управления на каждом ESXi-сервере для переноса данных резервного копирования. Это значительно упрощает установку и не требует дополнительной настройки ВМ или хранилища. Еще одним преимуществом данного режима является низкое воздействие на среду. По сравнению с режимом «Hot-Add» не требуется дополнительных операций по монтированию дисков, что позволяет экономить время. А в отличие от резервного копирования с помощью аппаратных снимков не происходит создания дополнительных аппаратных снимков интегрированных систем хранения. Координация ВМ и аппаратных снимков требует времени, поэтому сетевой режим может быть самым быстрым при инкрементальном резервном копировании в среде с большим количеством ВМ с низкой скоростью обновления данных.

Порт управления ESXi может стать «узким местом», особенно если используется интерфейс 1 Гбит. При использовании интерфейса 10 Гбит и выше проблем обычно не бывает.

Если вы используете ESXi 6.5: в этой версии VMware в обязательном порядке шифрует трафик резервного копирования с помощью NBD-SSL. До этого шифрование было опциональной настройкой. Это значительно сокращает скорость резервного копирования. В более поздних обновлениях VMware снова разрешает использовать незашифрованный трафик NBD. Начиная с версии Backup & Replication 9.5 Update 3, Veeam поддерживает незашифрованный трафик резервного копирования через режим NBD.

При использовании режима «Direct Storage Access» трафик резервного копирования поступает напрямую из системы хранения на прокси-сервер Veeam. В этом случае трафик не проходит через гипервизор ESXi, а используемый протокол зависит от среды хранения данных. Обычно это FibreChannel или iSCSI. «Direct Storage Access» обладает тем же преимуществом по сравнению с «Hot-Add», что и сетевой режим, а именно — отсутствием операции монтирования дисков. С другой стороны, оба режима используют VADP.

VADP — официальный API, разработанный VMware для резервного копирования виртуальных машин. Он оказывает некоторое влияние на производительность резервного копирования, из-за чего Veeam Backup & Replication не использует VADP в трех следующих конфигурациях:

- резервное копирование с помощью аппаратных снимков СХД;
- «Direct NFS» (аналогичен режиму «Direct Storage Access»);
- виртуальное устройство/«Hot-Add».

Отсутствие использования VADP приводит к заметному улучшению производительности резервного копирования, поэтому режим «Hot-Add» становится все более популярным. Но у этого режима есть и еще одно преимущество — в режиме «Hot-Add» прокси-сервер Veeam работает как дополнительная ВМ для резервного копирования. Он монтирует снимки ВМ и направляет трафик по обычной сети ВМ. Интерфейс управления ESXi при этом не используется. Это делает «Hot-Add» эффективной альтернативой в 1-гигабитных сетях, в которых невозможно использовать «Direct Storage Access».

Режим «Hot-Add» не рекомендуется использовать с хранилищами NFS. Для хранилищ NFS рекомендуется режим прямого доступа, а именно «Direct NFS». В пользовательском интерфейсе нет отдельной опции «Direct NFS», это одна из разновидностей режима «Direct Storage Access». Причина этой рекомендации состоит в том, что режим «Hot-Add» часто приводит к нестабильной работе ВМ, если она размещена не на одном ESXi-хосте с прокси-сервером Veeam. Подробная информация представлена в статье Базы знаний Veeam KB1681, в разделе «for environments with NFS datastores». Если вы все равно планируете использовать режим «Hot-Add» с хранилищами NFS, применяйте следующие правила и настройки:

- один прокси-сервер в режиме «Hot-Add» на ESXi-сервер;
- установите EnableSameHostHotAddMode = 1 в HKEY_LOCAL_MACHINE\SOFTWARE\Veeam\Veeam Backup and Replication.

Поскольку резервное копирование можно выполнять с различными настройками, удобно фиксировать результаты в таблице, чтобы потом выбрать наиболее подходящий вариант:

Mode	Operation	Time	Speed
Direct Storage Access	Full backup		
Direct Storage Access	Incremental backup		
Backup from Storage Snapshots	Full backup		
Backup from Storage Snapshots	Incremental backup		
Virtual Appliance	Full backup		
Virtual Appliance	Incremental backup		
Network	Full backup		
Network	Incremental backup		

Рекомендация. *Тестируйте режимы резервного копирования, чтобы выбрать наиболее подходящий для вашей среды.*

№3 Планируйте восстановление

После выбора оптимального режима резервного копирования важно рассмотреть методы восстановления. Veeam предлагает 57 сценариев восстановления ВМ, файлов и объектов приложений.

Во-первых, важно знать, что восстановление файлов и объектов приложений отличается от восстановления ВМ и дисков. Veeam восстанавливает файлы и объекты приложений (такие, как письма Microsoft Exchange или объекты Microsoft Active Directory) по сети. Под «сетью» имеется в виду подключение RPC (Windows) или SSH (Linux), по которому восстанавливаемые данные переносятся в ВМ.

Поскольку резервное копирование выполняется на основе снимка ВМ и на уровне блоков, восстановление ВМ или виртуальных дисков также происходит на уровне блоков. Для ВМ с «тонкими» или «толстыми» дисками могут применяться различные режимы восстановления. Режимы восстановления аналогичны режимам резервного копирования (т.е., «Direct Storage Access», «Hot Add» и NBD). Кроме того, доступна функциональность мгновенного восстановления ВМ, используемая совместно со Storage vMotion или технологией Quick Migration.

Режимы «Hot-Add» и NBD могут применяться для восстановления ВМ с «тонкими» и «толстыми» дисками. Как уже упоминалось, в версии 9.5 производительность режима «Hot-Add» при резервном копировании была улучшена. Также улучшена производительность этого режима при восстановлении ВМ и дисков. В большинстве сценариев рекомендуется иметь хотя бы один прокси-сервер для восстановления ВМ и дисков в режиме «Hot-Add».

Режим NBD обычно является самым медленным при восстановлении, т.к. он не может использовать всю пропускную способность сети.

Режим «Direct Storage Access» не имеет ограничений по использованию пропускной способности сети, но может восстанавливать только «толстые» диски. «Тонкие» диски будут на лету конвертироваться в «толстые». Режим «Direct Storage Access» при восстановлении использует VADP, поэтому обычно он не самый быстрый. Единственным исключением является режим «Direct NFS», при котором VADP не используется.

Для восстановления ВМ или виртуального диска не требуется переносить все данные. Если информация об измененных блоках данных на производственном хранилище верна, возможно восстановление на основе этой информации. Выбор этой опции может сократить время восстановления. Для этого при восстановлении включите настройку «Quick Rollback» (быстрый откат), как показано на рис. 2:

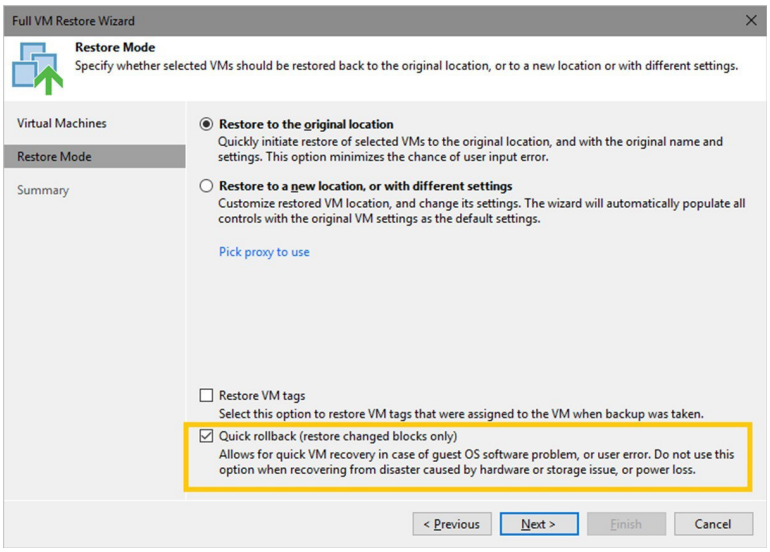

Рис. 2. Быстрый откат на основе информации об измененных блоках данных.

Мгновенное восстановление ВМ является альтернативой полному восстановлению ВМ. Эта функциональность позволяет мгновенно запустить ВМ прямо из репозитория резервных копий. Репозиторий выступает в роли хранилища NFS, подключенного к ESXi-хосту. Перенести данные ВМ из репозитория-хранилища NFS в производственную среду можно двумя способами:

- Veeam Quick Migration;
- VMware Storage VMotion.

Поскольку восстановление ВМ можно выполнять с различными настройками, удобно фиксировать результаты в таблице, чтобы потом выбрать наиболее подходящий вариант:

Mode	Operation	Time	Speed
Direct Storage Access	Full VM restore		
Direct Storage Access	Full VM restore CBT		
Virtual Appliance	Full VM restore		
Virtual Appliance	Full VM restore CBT		
Network	Full VM restore		
Network	Full VM restore CBT		
Instant VM recovery + Storage Vmotion	Full VM restore		
Instant VM recovery + Quick Migration	Full VM restore		

Рекомендация. *Планируйте восстановление и тестируйте его с различными режимами переноса данных, в зависимости от хранилищ. Если вы не используете хранилища NFS, рекомендуется развернуть по крайней мере один прокси-сервер с режимом «Hot-Add» в качестве запасного.*

№4 Установите VMware Tools

Во многих ситуациях Veeam Backup & Replication использует утилиты VMware Tools, установленные на ВМ. Без этих инструментов невозможно узнать, например, IP-адреса виртуальных машин или версию операционной системы. В результате этого обработка данных с учетом состояния приложений может завершиться с ошибкой.

Это происходит потому, что Veeam Backup & Replication не может определить IP-адрес ВМ, а без IP-адреса он не сможет подключиться к этой ВМ. VIX или vSphere Guest Operations API также не будет работать без VMware Tools (подробная информация о VIX представлена в рекомендации №10). На Рис. 3 показаны результаты теста, завершившегося с ошибкой из-за отсутствия VMware Tools.

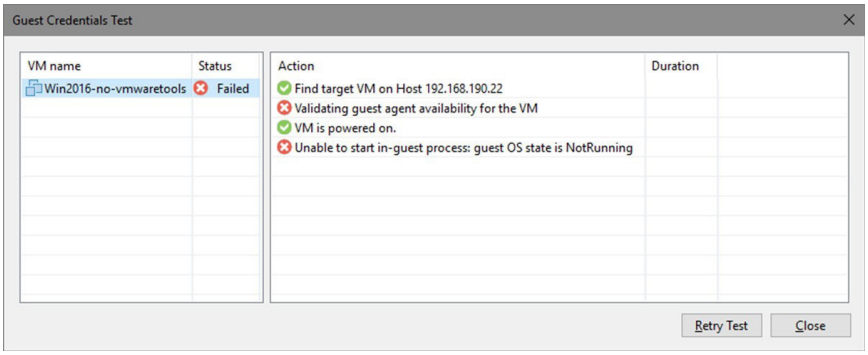

Рис. 3. Ошибки при тестировании обработки данных с учетом состояния приложений.

Еще один пример — тестирование SureBackup. Проверку «heartbeat» и пинги к этой ВМ также нельзя будет выполнить при отсутствии VMware Tools в гостевой ОС. Для VMware Tools есть правило №1: необходимо использовать последнее обновление.

Рекомендация. *Необходимо установить и вовремя обновлять VMware Tools.*

№5 Интегрируйте аппаратные снимки в концепцию доступности данных

Конечно, аппаратные снимки СХД уступают резервным копиям, но они могут помочь минимизировать потери данных во многих случаях. Veeam Backup & Replication предлагает интеграцию с СХД от многих поставщиков, что обеспечивает дополнительные возможности защиты данных.

Например, Veeam Backup & Replication может открыть аппаратный снимок и прямо из него восстановить файлы и объекты приложений. Благодаря этому можно создавать аппаратные снимки каждые 15 минут, без необходимости создавать обычные снимки состояния ВМ. Хотя создание аппаратного снимка каждые 15 минут не является настоящим резервным копированием, так как не соответствует правилу «3-2-1», оно помогает снизить показатели RPO.

Это иллюстрирует Рис. 4, на котором представлен Veeam Explorer™ для Storage Snapshots. В левой части показаны аппаратные снимки (т.е., тома LUN и снимок одного тома). В левой части представлены ВМ, содержащиеся в каждом аппаратном снимке. Из этого представления можно восстановить ВМ, с помощью «Instant VM Recovery», или ее отдельные файлы и объекты приложений. Представьте, что аппаратные снимки критически важных LUN создаются каждые 15 минут и через 4 часа удаляются. Это значит, что можно восстановить данные 15-минутной давности, а не вчерашние, из ночной резервной копии.

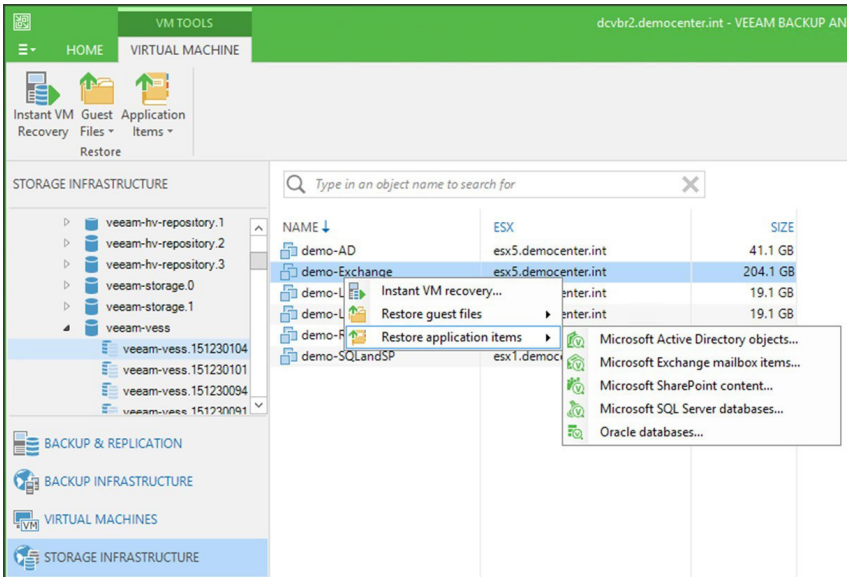

Рис. 4. Восстановление объектов приложений из аппаратного снимка.

Еще одно преимущество интеграции Veeam Backup & Replication с системами хранения данных — возможность резервного копирования больших ВМ с высокой интенсивностью транзакций без риска нарушения их работы при консолидации снимков VMware. Хотя в последних версиях vSphere эта проблема уже не так выражена, она остается основной причиной использования аппаратных снимков.

Кроме того, резервное копирование с помощью аппаратных снимков позволяет Veeam задействовать собственный механизм переноса данных, который способствует повышению производительности по сравнению с использованием VADP. Это особенно актуально для полного резервного копирования или резервного копирования данных с высокой скоростью обновления.

Рекомендация. *Используйте интеграцию с СХД, если ваша система поддерживается Veeam Backup & Replication.*

№6 Резервное копирование VMware vSAN

VMware vSAN становится все популярнее, однако имеет некоторые особенности, о которых не стоит забывать. VMware vSAN не использует традиционные протоколы систем хранения. Это означает, что невозможно использовать режим «Direct Storage Access» или резервное копирование с помощью аппаратных снимков.

Поддерживается сетевой режим и «Hot-Add». Используя режим «Hot-Add», Veeam Backup & Replication выполняет резервное копирование ВМ с учетом близости расположения к данным ВМ. Иными словами, резервное копирование выполняется через прокси-сервер, размещенный на хосте с максимальным количеством данных ВМ. Для правильной работы необходимо, чтобы на каждом ESXi-хосте был установлен прокси-сервер. Правило близости хоста к ВМ, на которой установлен прокси-сервер, предотвращает перенос ВМ на другие ESXi-хосты с помощью VMware Distributed Resource Scheduler (DRS).

Это помогает снизить объем трафика и уменьшить время задержки, а значит, сократить окно резервного копирования. Если ВМ находится на одном хосте, а прокси-сервер на другом, то это увеличивает объем трафика по сети, удлиняет время задержки и снижает скорость.

Veeam Backup & Replication сертифицирован как VMware-ready для vSAN в категории решений для защиты данных. Подробная информация представлена в статье Базы знаний VMware 2149874 и VMware vSAN HCL.

Рекомендация. *При использовании режима «Hot-Add» с VMware Virtual SAN необходимо установить прокси-сервер на каждый ESXi-хост.*

№7 Следите за состоянием инфраструктуры (vSphere)

В течение многих лет девизом Veeam было «он просто работает». Для большинства заказчиков подходят настройки по умолчанию, но для более крупномасштабных развертываний Veeam Backup & Replication рекомендуется составить подробный план.

vCenter — один из наиболее важных компонентов, необходимых для работы Veeam Backup & Replication. Если vCenter не работает, резервное копирование невозможно. Поэтому техническое обслуживание vCenter должно планироваться за пределами окна резервного копирования. Также рекомендуется отслеживать нагрузку на vCenter и количество подключений. Сеть между сервером резервного копирования Veeam и vCenter должна быть стабильной!

В зависимости от среды резервное копирование может добавлять нагрузку на производственное хранилище. Несколько ГБ в секунду не являются редкостью и могут увеличить время задержки операций ввода-вывода на традиционных дисковых массивах. Функция контроля ввода-вывода Veeam Backup & Replication регулирует скорость резервного копирования и восстановления (Рис. 5).

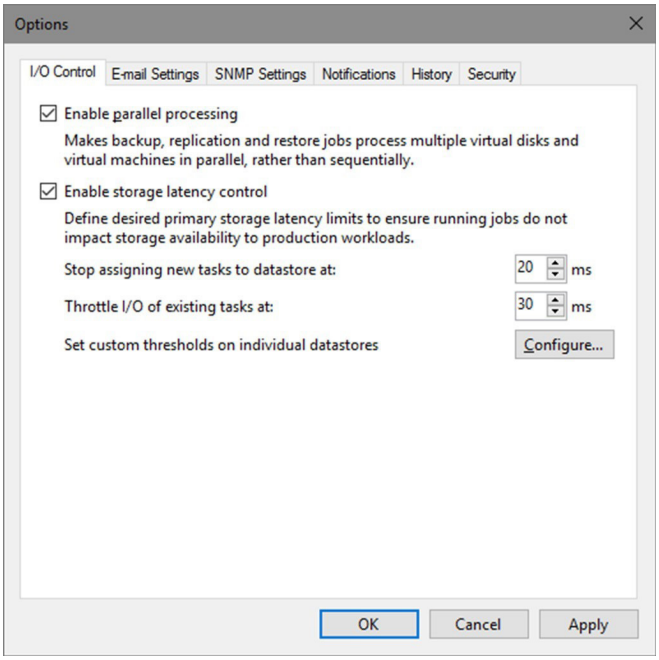

Рис. 5. Контроль времени задержки хранилища.

Функция контроля времени задержки хранилища регулирует выполнение заданий на основе сведений о задержке хранилища, полученных от vSphere. Это происходит в две стадии. Сначала Veeam перестает направлять новые задания резервного копирования на хранилище. Если время задержки все равно увеличивается, ограничивается скорость выполнения активных заданий. В итоге резервное копирование длится дольше, но с меньшей нагрузкой на работающие ВМ. Этот механизм позволяет выполнять резервное копирование в рабочее время с минимальной нагрузкой на ВМ, приложения и пользователей.

Функция контроля времени задержки отключает максимальное значение в 4 снимка ВМ на хранилище одновременно, принятое по умолчанию. Это также помогает повысить производительность.

Рекомендация. *Поскольку работа Veeam Backup & Replication зависит от vCenter, обеспечьте его эффективную работу. Отслеживайте нагрузку в рамках окна резервного копирования и вносите изменения, если требуется.*

№8 Безопасность

Veeam Backup & Replication использует vCenter для управления резервным копированием и восстановлением ВМ. С точки зрения безопасности всегда лучше использовать минимальное количество привилегий. VMware vCenter предлагает гранулярные права доступа для выполнения резервного копирования.

В документе о необходимых правах доступа представлена подробная информация о том, какие права доступа необходимы для каждого из режимов резервного копирования. Для разных режимов требуются различные права доступа. При использовании режима «Hot Add» правом безопасности является «удаление диска».

Соображения безопасности могут повлиять на выбор режима переноса данных. Также можно ограничить отдельные серверы резервного копирования (если у вас их несколько) определенными локациями или объектами vCenter.

Рекомендация. *Следуйте принципу минимальных привилегий.*

№9 Планируйте развертывание Veeam Backup & Replication с помощью Veeam ONE

Veeam Availability Suite™ содержит Veeam ONE™ —эффективный инструмент для планирования развертывания Veeam Backup & Replication.

Компонент Veeam ONE Monitor показывает текущий статус и актуальные проблемы среды vSphere. Проблемами, связанными с резервным копированием, могут быть, например, длительное время задержки хранилища или устаревшие, большие, многочисленные или неучтенные снимки ВМ.

Veeam ONE Reporter позволяет создать отчет о конфигурациях ВМ, отображающий потенциальные проблемы, которые могут помешать резервному копированию данных.

Типичные проблемы, показанные в отчете, это:

- не установлен пакет VMware Tools;
- старая версия оборудования ВМ (4.0 или более ранняя);
- диски, резервное копирование которых не может быть выполнено (например, независимые диски);
- менее чем 10% свободного пространства в хранилище;
- наличие «маппинга» устройств в ВМ.

Заблаговременное решение этих проблем поможет избежать ошибок при выполнении резервного копирования.

Рекомендация. *Используйте Veeam ONE для планирования развертывания Veeam Backup & Replication.*

№10 Резервное копирование с учетом состояния приложений с помощью VIX API

Рекомендация № 4 говорит о необходимости установки и своевременного обновления VMware Tools. Этот инструмент позволяет администратору Veeam выполнять резервное копирование ВМ Windows с учетом состояния приложений без прямого сетевого подключения к ВМ.

Предпочтительный метод выполнения резервного копирования с учетом состояния приложений — это подключение прокси-сервера приложений к ВМ через RPC. Это самый быстрый способ.

Если сегментация сети или брандмауеры не допускают прямого подключения к ВМ, Veeam может использовать VIX API или, в более новых версиях vSphere (6.5 и позже), vSphere Guest Operations API. На рис. 6 показано подключение через VIX (выделено оранжевым).

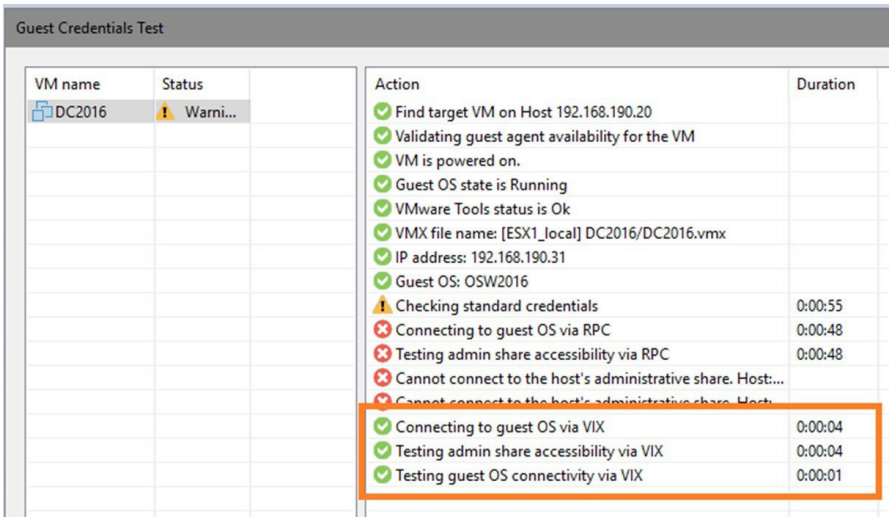

Рис. 6. Тестирование учетных данных через VIX API.

Для использования VIX или vSphere Guest Operations API необходима предварительная подготовка. Подробное описание требований представлено в статье Базы знаний Veeam KB 1788. Всего есть два требования:

- Учетная запись, используемая Veeam, должна принадлежать к группе локальных администраторов.
- Если учетная запись не озаглавлена «administrator», необходимо отключить Windows User Account Control (UAC).

VIX или vSphere Guest Operations API является резервным режимом на случай отказа RPC. Поэтому в среде, где большинство ВМ недоступно через RPC, резервное копирование займет больше времени, так как Veeam всегда сначала пытается задействовать RPC. Этот порядок можно изменить на обратный путем редактирования ключа регистра на сервере резервного копирования или прокси-сервере:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Veeam\Veeam Backup and Replication\
DWORD: InverseVssProtocolOrder
Value = 1
```

Для отключения (поведения по умолчанию) значение равно 0 (false).

Важно знать, что VIX или vSphere Guest Operations API имеет некоторые ограничения для операций восстановления. Этот метод позволяет восстанавливать файлы, но не объекты приложений. Это означает, что нельзя восстановить объекты Active Directory, Exchange и другие с помощью этого метода — для их восстановления потребуется сетевое подключение. Вторая особенность состоит в том, что перенос файлов по сети происходит намного медленнее.

Служба VeeamLogShipper, которая выполняет перенос журнала SQL, также может использовать VIX как резервный механизм, если она не может подключиться к репозиторию по сети. В большинстве сред это может занимать слишком много времени, поэтому рекомендуется выполнять перенос журнала SQL по сети.

Рекомендация. *Не забывайте об ограничениях VIX или vSphere Guest Operations API.*

Заключение

Сочетание Veeam Backup & Replication и VMware vSphere обычно работает без предварительной подготовки. Но благодаря выполнению некоторых рекомендаций качество работы может быть гораздо выше. Эти рекомендации просты, легко выполнимы и не требуют много времени.

Рекомендация. *Ознакомьтесь с полным руководством по лучшим практикам использования Veeam Backup & Replication, если вы планируете крупномасштабное или сложное развертывание.*

Об авторе

Ханнес Каспарик работает в ИТ-бизнесе с 2004 г. Сегодня Ханнес — сотрудник отдела Veeam по управлению развитием продуктов. В прошлом он управлял средами Linux и Windows, а также инфраструктурными сервисами, включая серверы, хранилища, сеть и брандмауеры.

О компании Veeam Software

Veeam® является лидером по разработке решений для резервного копирования, которые обеспечивают управление защитой облачных данных. Veeam Availability Platform™ — самое комплексное решение, которое позволяет успешно внедрить 5 стадий управления облачными данными. У Veeam свыше 355 000 заказчиков по всему миру, включая 82% компаний из списка Fortune 500 и 67% из списка Global 2 000. Показатели удовлетворенности заказчиков — самые высокие в отрасли и превышают средние значения в 3,5 раза. Глобальная экосистема Veeam включает 66 000 партнеров-реселлеров; компании Cisco, HPE, NetApp и Lenovo в качестве эксклюзивных реселлеров; а также свыше 23 500 поставщиков услуг и облачных сервисов. Офисы Veeam расположены в более чем 30 странах. Центральный офис находится в г. Бар, Швейцария. Подробная информация о компании представлена на https://www.veeam.com; следите за новостями на Twitter @veeam.

VEEAM

NEW

#1 Cloud Data Management

Veeam Availability Suite *9.5 Update 4*

The latest version of Veeam Availability Suite includes:

Cloud Tier

Unlimited capacity for long-term data retention by using native, cost effective object storage integration

Cloud Mobility

Easy portability and recovery to AWS, Azure and Azure Stack

Enterprise Application Support

Direct integration with critical enterprise applications including Oracle RMAN and SAP HANA

Data Governance Capabilities

Increased security and compliance including GDPR and malware prevention

vee.am/availabilitysuite