5 случаев, когда резервные копии VMware и Hyper-V могут вас подвести

Грег Шилдс (Greg Shields)

Специалист Microsoft MVP
и VMware vExpert

Что первым приходит вам в голову, когда вы слышите о защите виртуальных машин?

Многие ИТ-специалисты, вероятнее всего, подумают о технологии высокой доступности (High Availability, или HA).Каждый крупный поставщик платформ виртуализации предлагает собственную реализацию HA. И хотя для решения этой задачи могут использоваться различные приемы, вы получаете практически один и тот же результат: виртуальные машины защищены в случае отказа хоста.

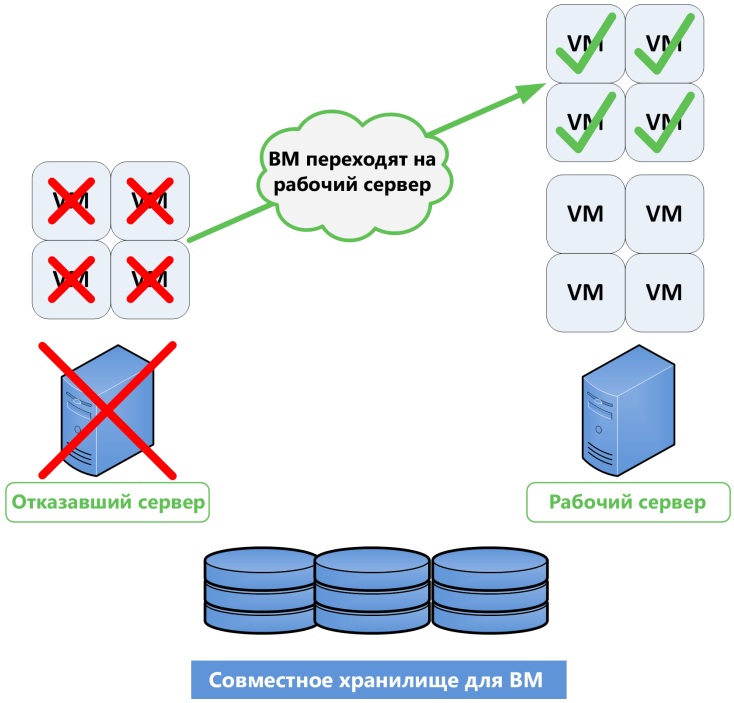

Рисунок 1. Технологии высокой доступности помогают защитить виртуальные машины.

В последние годы технологиям высокой доступности (см. рис. 1), таким как vMotion от VMware или Live Migration от Microsoft, уделялось значительное внимание. Одной из причин такой популярности является то, что эти технологии действительно помогают решить наболевшие проблемы.

Технологии, на которых основаны возможности HA, не могут не впечатлять. Уверенность в том, что в случае аварии хост можно с легкостью восстановить, позволяет многим администраторам виртуальных систем спокойно спать по ночам — они знают, что их виртуальные машины в безопасности.

Несмотря на то, что технологии высокой доступности имеют огромное значение для защиты виртуальных машин в определенных ситуациях, возможности этих технологий все же не безграничны. Высокая доступность может помочь вам в случае отказа хоста, а также, если вы приложите дополнительные усилия — и в случае отказа приложений. Но в конечном итоге высокая доступность ...

- *не поможет* в случае потери данных;
- *не поможет* в случае повреждения данных;
- *не даст ничего* в плане восстановления после аварии.

Множество причин отказа виртуальных машин

Ситуаций, в которых технологии высокой доступности действительно могут помочь, не так уж и много, если учитывать все возможные причины отказа виртуальных машин. Задумайтесь хотя бы на минуту о возможных рисках (которых, между прочим, огромное количество) — и вы снова перестанете спокойно спать по ночам. К отказу виртуальной машины может привести:

- повреждение или удаление данных;
- повреждение или удаление объектов приложений;
- выход из строя или повреждение ОС;
- случайное уничтожение объекта ВМ;
- повреждения вследствие ошибок взаимодействия между уровнями приложения;
- ошибки пользователей;
- ошибки администраторов;
- использование водной системы пожаротушения в ЦОД (кстати: это очень и очень плохо);
- а также любые другие аварии, возникшие по вине человека или в результате стихийных бедствий.

Некоторые причины отказа виртуальных машин могут показаться смешными. Но они призваны помочь вам распознать потенциальные опасности для работы виртуальных машин, исходящие из множества различных источников — как внешних, так и внутренних.

Еще один фактор в вышеприведенном списке возможных причин отказа заслуживает особого внимания. Чтобы защитить виртуальную машину, следует обеспечить сохранность не только ее содержимого — ОС, приложений и файлов — но и определяющих характеристик самой виртуальной машины. Эти характеристики могут быть представлены как объект виртуальной машины в пределах виртуальной платформы; к ним относятся записи реестра или атрибуты виртуальной машины, а также идентификатор MoRef (уникальный идентификатор экземпляра, известный также как instanceUUID).

Вне зависимости от среды (VMware vSphere или Microsoft Hyper-V), для успешной работы виртуальной машины необходима как функционирующая ОС, так и функционирующий объект виртуальной машины на виртуальной платформе. При выходе из строя одного из этих компонентов произойдет отказ виртуальной машины. Это вполне очевидно, однако многие средства резервного копирования были созданы без учета особенностей виртуализации. Действие таких традиционных средств направлено на защиту файлов, из которых состоит виртуальная машина, тогда как метаданные виртуальной машины внутри платформы виртуализации остаются без внимания.

Отчаянный поиск надежного решения при ненадежном инструменте для резервного копирования

Ниже представлен список проблем, с которыми вы можете столкнуться, если выполняете резервное копирование виртуальных машин с помощью традиционных инструментов, которыми пользовались годами. Вполне возможно, что эти инструменты неплохо работали с физическими серверами. Однако они не учитывают все особенности виртуальной среды, что может привести к целому ряду проблем.

Помните длинный список возможных причин отказа виртуальных машин, который может лишить вас сна? Этот список – всего лишь капля в море по сравнению с теми рисками, с которыми вы можете столкнуться из-за ненадежного решения для резервного копирования. Вот первые пять проблем, которые сразу приходят на ум:

- **Сбор данных с разных уровней инфраструктуры.** Файлы, из которых состоит виртуальная машина, — только часть общей картины, один из множества уровней стека виртуализованного ЦОД. Помимо него следует учитывать такие уровни как:серверное оборудованияе системы хранения данных, операционные системы и средства администрирования. То, что представляется как жесткий диск виртуальной машины на одном уровне, на другом уровне будет представлено каквиртуальный диск, причем гипервизор и устройства хранения будут работать с таким объектом по-разному. Средство резервного копирования, которое учитывает все особенности виртуализации, должно принимать во внимание специфику каждого уровня, чтобы обеспечить успешный сбор данных.
- **Проверка целостности резервной копии.** Если вы не можете получить гарантированно рабочую резервную копию, считайте, что у вас нет резервной копии. Многие средства резервного копирования предполагают наличие проверки целостности резервных копий, однако следует понимать, что такая проверка должна осуществляться как для данных резервной копии, так и для операционной системы и приложений внутри системы.
- **Сохранение целостности данных или VSS.** Решение для резервного копирования, созданное с учетом особенностей виртуализации, должно включать дополнительные функции мониторинга стабильности каждого уровня виртуальной среды. В том числе, оно должно обеспечивать надлежащее использование инструментов платформы виртуализации — VMware Tools или Hyper-V Integration Components — а также сложных операций инфраструктуры службы теневого копирования томов Windows (VSS).

- **Уведомление о проблеме.** Практически любое средство резервного копирования может уведомить вас об имеющихся проблемах, но всегда ли вы используете эту возможность? Если нет, вы никогда не узнаете, что собранные данные ненадежны.
- **Контроль за разрастанием виртуальной среды.** Последнее, и самое важное для виртуальной среды, — это дополнительные возможности, открывающие средству резервного копирования доступ к решению для управления платформой виртуализации. Только решение, которое учитывает особенности виртуализации, поможет обеспечить резервное копирование нужных виртуальных машин в растущей и меняющейся виртуальной среде.

Пять советов для надежной защиты виртуальных машин

Следует отметить, что вышеперечисленные проблемы чаще всего возникают в тех организациях, где используется принцип "настроил и забыл". И как правило, первая реакция при появлении проблем — "давайте найдем новое решение". Новсегда ли необходимо искать новое решение?

Конечно же, лучше всего использовать решение для резервного копирования, созданное с учетом особенностей виртуализации.

Ниже вы найдете пять советов, которые помогут вам сделать шаг вперед. Эти советы основаны на рекомендациях экспертов с многолетним опытом работы. Они помогут вам избежать ошибок при использовании решения для резервного копирования, которое у вас уже имеется.

Игнорируя эти советы, вы действуете на свой страх и риск. Они касаются ряда наиболее распространенных упущений, которые могутсвести на нет все ваши усилия по защите данных в виртуальной среде.

Совет №1. Учитывайте уровни.

А именно, уровни инфраструктуры. Как уже говорилось, виртуализация добавляет множество уровней между виртуальной машиной и местом хранения ее резервных копий. Фактически, чем больше уровней, тем лучше. Виртуальная машина взаимодействует с гипервизором, а гипервизор взаимодействует с хостом, который подключен к ресурсу для хранения данных виртуальной машины. С одной стороны, взаимодействие между этими уровнями позволяет оптимизировать работу ЦОД, но с другой стороны, оно же усложняет инфраструктуру, что может привести к ошибкам при проектировании и, как следствие, к появлению различных проблем.

Примером неудачного проектного решения может быть хранение производственных данных (таких как файлы дисков виртуальных машин) с данными резервных копий на одном и том же физическом носителе. Такая ситуация возможна при переходе с ленточных носителей резервных копий на дисковые носители. Лучшая рекомендация в этом случае — хранить данные резервных копий на другом физическом носителе, отличном от носителя, который вы используете для хранения данных производственных виртуальных машин. В этом случае при сбое производственной системы хранения резервные копии не будут утеряны.

РЕКОМЕНДЦИЯ: убедитесь, что резервные копии хранятся на отдельном носителе, а не в основном хранилище виртуальных машин.

Совет №2. Не тестируйте резервные копии.

Найдите кого-нибудь, кто будет тестировать их вместо вас. А еще лучше, воспользуйтесь автоматизированным средством для тестирования резервных копий. Учитывая то, что тестировать резервные копии нужно ежедневно, автоматизация дешевле. Кроме того, она надежнее, чем человек, который вручную выполняет эту важную операцию.

Выбирая решение для резервного копирования, также важно учитывать виды автоматизированного тестирования, которые это решение предлагает.

В то время как большинство средств резервного копирования на дисковые носители обеспечивают элементарную проверку целостности данных в резервных копиях, все же намного важнее убедиться, что резервные копии приложений виртуальной машины, операционной системы и объектов виртуализации (например, атрибутов) созданы правильно.

При переходе к резервному копированию на дисковые носители вы получаете больше возможностей для тестирования резервных копий. В отличие от резервных копий на ленточных носителях, резервные копии на дисковых носителях доступнее: дисковые системы всегда подключены и лучше обеспечивают возможность произвольного ввода-вывода. Хранилище резервных копий не всегда обладает уровнем производительности производственной системы хранения данных, однако резервные копии на дисковых носителях доступны для выполнения проверок на уровне виртуальной машины, ОС и приложений. Такие проверки, позволяют убедиться, что службы Active Directory, хранилища данных Exchange, ОС Windows и баз данных SQL работают корректно.

РЕКОМЕНДАЦИЯ: убедитесь, что для резервных копий предусмотрены комплексные проверки целостности данных и работоспособности служб, и что такие проверки автоматически выполняются для каждой резервной копии.

Совет №3. Контролируйте "заморозку".

«Заморозка» (quiescence) - один из важнейших аспектов резервных копий виртуальных машин. Мы уже говорили о дополнительных сложностях, которые виртуализация привносит в процедуру резервного копирования. И процесс "заморозки" в ходе резервного копирования крайне важен для обеспечения правильного сбора данных.

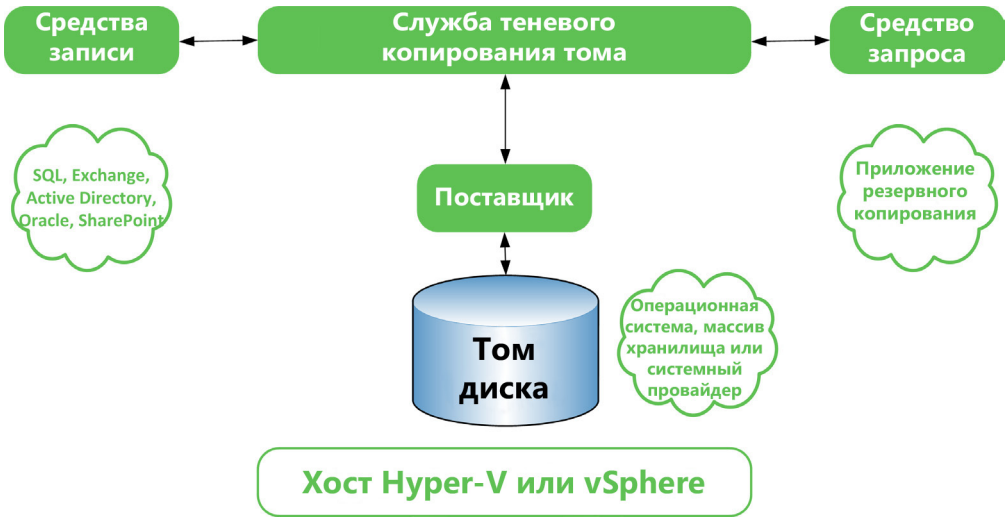

Рисунок 2. Роль VSS при создании резервных копий Windows

Большинство инструментов для защиты данных в среде Windows используют возможности собственных компонентов в сочетании со службой теневого копирования томов Windows (VSS). Эта служба, как показано на рисунке 2, требует четкой координации трех различных компонентов: VSS-редактора (VSS Writer), VSS-клиента (VSS Requestor) и VSS-провайдера (VSS Provider).

В роли VSS-клиента обычно выступает средство резервного копирования, которое управляет процессом резервного копирования. VSS-клиент координирует свои действия с VSS-провайдером (для взаимодействия с хранилищем) и с VSS -редактором (для работы с приложениями, установленными на виртуальной машине) .

На физическом компьютере эти три компонента работают согласованно для создания резервной копии. Отказ любого из трех компонентов помешает завершению резервного копирования или, что еще хуже, приведет к созданию резервной копии, из которой невозможно восстановить данные.

Поскольку программные и/или аппаратные компоненты должны работать вместе для использования преимуществ инфраструктуры VSS при создании резервной копии, критически важно сделать так, чтобы служба VSS работала корректно.

Если физические машины заменить виртуальными, координировать работу компонентов VSS станет еще труднее. Взаимодействие трех компонентов службы VSS (редактора, провайдера и клиента) при работе в среде vSphere или Hyper-V значительно усложняется.Для корректной работы службы VSS в среде vSphere необходимо координировать действия компонентов VSS с VMware Tools, установленными на виртуальной машине. В среде Hyper-V служба VSS добавляет новые уровни координации между VSS-редактором среды Hyper-V виртуального хоста и VSS-редактором внутри каждой виртуальной машины.

VSS-клиент также должен обеспечить корректную работу с приложениями в ходе резервного копирования, включая обрезку журнала транзакций для приложений с поддержкой VSS. Это критический компонент для успешной защиты данных виртуальной машины.

Служба VSS создана для обработки всех этих взаимосвязей, и обеспечение ее правильной работы в виртуальной среде — а также корректной работы с виртуальными машинами и их приложениями — становится ключевым требованием надежной защиты.

РЕКОМЕНДАЦИЯ: придерживайтесь верного подхода к VSS: доверяйте, но проверяйте.

Совет №4. Получайте уведомления о выполненных операциях.

Этот совет может показаться самым очевидным, однако опыт экспертов, участвовавших в создании данного документа, показывает, что на практике именно этот совет чаще всего забывается. Совет 4 очень простой: ваше средство резервного копирования вероятнее всего предоставляет возможности оповещения, благодаря которым вы сможете получать уведомления об успешных и неудачных операциях резервного копирования. Для уведомления администраторов могут использоваться такие простые средства, как электронная почта или протокол SNMP. Настройте эти оповещения.

Уделите несколько минут изучению функций оповещения, которые предлагает ваше решение для резервного копирования. Убедитесь, что уведомления будут высылаться как при успешных, так и при неудачных операциях резервного копирования.

Подтверждение того, что ваша система резервного копирования работает как нужно — основной индикатор успеха.

РЕКОМЕНДАЦИЯ: мониторы выполняют мониторинг лучше вас. Используйте их.

Совет №5. Не создавайте новые задания резервного копирования для новых виртуальных машин.

Если вы не поняли шутку, см. совет 2. «Правильный» инструмент для резервного копирования должен уметь работать с динамическойвиртуальной средой, которая непрерывно растет и меняется.

Рост и изменение виртуальной среды (в том числе, частного облака) вызваны тем, что виртуальные машины постоянно создаются и выводятся из эксплуатации.

Возможно, в вашей виртуальной среде и/или в частном облаке созданием виртуальных машин заняты не вы.Если вы не создаете виртуальные машины, но отвечаете за их защиту, откуда вы можете знать, нужно ли делать резервные копии для новых виртуальных машин или нет?

Правильный ответ — вы не можете этого знать без тщательного и постоянного мониторинга виртуальных машин или без средства резервного копирования, которое учитывает особенности платформы виртуализации. Средство резервного копирования, которое «знает» все о платформах виртуализации, может справиться с ростом количества виртуальных машин как в среде vSphere, так и в среде Hyper-V. Такой инструмент способен защитить как объект виртуальной машины, так и его содержимое. Подобное внимание к каждой составляющей виртуальной машины — именно то, что так нужно в динамической виртуальной среде и именно то, что совершенно необходимо для обеспечения надежной защиты виртуальных машин.

РЕКОМЕНДАЦИЯ: убедитесь, что средство резервного копирования выполняет операции для всех структурных компонентов виртуальной инфраструктуры — центров обработки данных, папок, кластеров и прочихобъектов — а не только для виртуальных машин.

Безопасных аварий!

Действительно, высокая доступность — это еще не все, и для защиты виртуальных машин придется выполнить ряд действий, для которых, в свою очередь, необходимо принять ряд решений.

Вы хотите заменить устаревшее средство резервного копирования или уже перешли на решение нового поколения, созданное специально для виртуальной среды? В любом случае, эти пять советов помогут вам сделать первые шаги по направлению к надежной защите виртуальных машин.

Об авторе

Грег Шилдс, Microsoft MVP и VMware vExpert, является независимым автором, докладчиком и ИТ-консультантом, а также партнером и главным технологом компании Concentrated Technology. За 15 лет работы в сфере информационных технологий Грег получил богатый опыт в области администрирования, разработки и архитектуры систем программного обеспечения.

О Veeam Software

Компания Veeam® Software, партнер VMware уровня Elite по программе VMware Technology Alliance Partner и ведущий партнер Microsoft по программе Microsoft Gold Certified Partner, занимается разработкой инновационных решений для управления виртуальными средами на платформах VMware vSphere и Microsoft Hyper-V. Veeam Backup & Replication™ является решением #1 для резервного копирования и репликации в виртуальной среде и обеспечивает надежную защиту данных средствами виртуализации (Virtualization-Powered Data Protection™). Решение Veeam ONE™ предоставляет эффективные и доступные инструменты для мониторинга в режиме реального времени, документирования и создания отчетов о работе виртуальной среды. Решения Veeam nworks расширяют возможности корпоративных систем мониторинга, позволяя с их помощью отслеживать состояние среды VMware. Veeam Management Pack™ предоставляет возможности расширенного мониторинга среды VMware напрямую из консоли Microsoft System Center, а Veeam Smart Plug-in™ обеспечивает расширенный мониторинг VMware средствами HP Operations Manager. Компания Veeam, активный член сообщества виртуализации, является спонсором образовательного портала Backup Academy, ежеквартальных обзоров V-index, ежегодного отчета Virtualization Data Protection Report, а также участвует в многочисленных отраслевых мероприятиях. Узнайте больше о компании Veeam на www.veeam.com.

VEEAM

#1 VM Backup

Veeam Backup & Replication

Резервное копирование | ***Репликация*** | ***Восстановление***

100% надежность | Лучшие RTOs и RPOs | Скорость и гибкость

НОВИНКА! Veeam Backup & Replication™ v6

Новые возможности усиливают лидерство в области резервного копирования виртуальных машин:

- **Масштабируемость корпоративного класса:** новая распределенная архитектура оптимизирует развертывание и обслуживание при установке в удаленных офисах/филиалах (ROBO) и при крупномасштабных установках.
- **Усовершенствованная репликация:** ускоряет репликацию до 10 раз, оптимизирует аварийное переключение на резервный ресурс и обеспечивает настоящий возврат на основной ресурс с разностной синхронизацией·
- **Поддержка нескольких гипервизоров:** отмеченная наградами защита Veeam распространяется на Hyper-V, что позволит защищать все свои ВМ — будь то VMware или Hyper-V— из одной консоли.
- **и многое другое!**

BEST OF vmworld 2011 GOLD AWARD NEW TECHNOLOGY | BEST OF vmworld 2010 BEST OF SHOW | BEST OF vmworld 2010 GOLD AWARD NEW TECHNOLOGY | 2010 Products of the Year GOLD | WINNER 2011 VIRTUALIZATION REVIEW | Products of the Year | TECHWORLD AWARDS

Узнайте больше:

http://www.veeam.com/ru/vmware-esx-backup.html