Резервное копирование данных

и основные модели его организации

Сергей СКЛАБОВСКИЙ,
менеджер по продукту провайдеров #CloudMTS и «ИТ-ГРАД» (входят в облачное направление МТС)

Актуальная статистика говорит об экспоненциальном росте объема цифровых данных. Безусловно, существенное влияние на это оказывает все более глубокое проникновение технологий. По данным IDC, в ближайшие годы основной объем информации будет генерироваться не пользователями, а компаниями. Бизнес уже сейчас становится не просто цифровым, а ориентированным на данные.

Правильный подход к данным и грамотная аналитика помогают компаниям находить новые точки роста и прогнозировать угрозы. Однако информация – не только «философский камень» развития, но и ключ к непрерывности бизнеса. Утрата или повреждение данных может привести к серьезным репутационным и финансовым издержкам. Последствия халатного отношения к информационной безопасности и организации непрерывной работы могут обусловить возникновение простоев бизнеса и многомиллионные убытки. Минимизировать подобные угрозы способны инструменты резервного копирования. Правильно подобранное и настроенное решение, а также грамотный подход повысят уровень сохранности корпоративных данных и элементов ИТ-инфраструктуры.

Организация резервного копирования

Современный рынок предлагает широкий спектр инструментов для резервного копирования данных. Среди них присутствуют как бесплатные продукты, ориентированные на частных лиц и представителей малого бизнеса, так и решения для крупных корпораций. В статье рассматриваются ключевые вопросы организации процесса резервного копирования в средних и крупных компаниях, популярные модели и схемы резервирования, представлен срез наиболее популярных бэкап-сервисов.

За основу примем несколько простых тезисов:

- резервное копирование не приносит дополнительную прибыль, однако при грамотной организации способно оградить бизнес от убытков;
- выбор сервиса резервного копирования и схема его реализации должны основываться на потребностях и возможностях компании.

Определение данных для резервирования

Одна из первых задач, с которыми вы столкнетесь, – определение данных, которые необходимо резервировать, а также степень оперативности восстановления последней или одной из предшествующих версий.

Единого рецепта здесь быть не может: каждый бизнес обладает собственным набором стратегически важной информации. Ниже приведен краткий чек-лист, с помощью которого без труда можно определить набор приоритетных данных.

- Базы данных, в том числе «1С», требуется резервировать в 100% случаев. Они могут пострадать не только из-за выхода из строя инфраструктуры, но и вследствие халатности персонала.
- Настройки серверов, пресеты ключевых программ и пользовательского ПО. В частности, если деятельность сотрудников компании сопряжена с использованием ПО, которое требует предварительной настройки, следует сохранять эту информацию. В экстренном случае можно оперативно восстановить конфигурацию.
- Копии стратегических приложений и веб-ресурсов.
- Бухгалтерские и юридические документы, таблицы, отчеты и прочая информация, без которой производственный процесс может встать.

Кроме того, следует определиться с частотой создания резервных копий, от которой будет зависеть выбор типа резервного

копирования. К примеру, громоздкие приложения, которые практически не подвергаются изменениям, имеет смысл бэкапить один-два раза в месяц. Текущие данные (БД, файлы пользователей и т. п.) требуется копировать гораздо чаще.

Помните о том, что процесс резервного копирования может создать существенную нагрузку на ИТ-инфраструктуру. Планируйте ресурсоемкие бэкапы на наименее нагруженные часы.

Модели резервного копирования

Перейдем к вариантам резервного копирования и рассмотрим их основные плюсы и минусы.

Full Backup, полное резервное копирование

Эта модель подразумевает создание полной копии исходных данных на регулярной основе. Технически это самый надежный подход к организации резервного копирования. Он позволяет максимально быстро восстановить утраченные данные. К минусам можно отнести низкую скорость создания копии, существенную нагрузку на сеть и высокую стоимость при большом объеме данных.

Инкрементное резервное копирование

За основу берется изначальная полная копия, а ежедневный инкрементный бэкап затрагивает только измененные данные. Как следствие, место в репозитории расходуется достаточно экономно. Однако у этого типа есть определенные недостатки. Поскольку инкременты создаются последовательно, каждый из них зависит от предыдущего. Повреждение одного делает всю последующую цепочку недоступной. Еще один минус: чем больше итераций прошло между изначальным полным бэкапом и инкрементом, тем дольше будет длиться восстановление. Однако стоит отметить, что инкрементальные копии создаются достаточно быстро и занимают относительно немного места в хранилище.

Дифференциальное резервное копирование

После создания полной копии в каждый последующий день создаются резервные копии, содержащие изменения относительно Full Backup. Плюсы – весьма надежный способ, обеспечивающий более высокую скорость восстановления, чем инкрементный подход, и более высокую скорость создания резервных копий, чем Full backup. К тому же дифференциальные копии не зависят от предыдущих: при повреждении промежуточной копии данные из последующих могут быть восстановлены. Главный недостаток – каждая новая копия занимает больше дискового пространства и выполняется дольше, чем предыдущая.

Обратное инкрементное копирование

Этот тип подразумевает, что каждая новая итерация резервного копирования будет создавать новую полную резервную копию, а место предыдущей РК будет заменено инкрементом. Плюс метода – высокая скорость восстановления самых свежих данных. Минусы – существенные требования к серверу РК и более длительное восстановление данных из старых копий.

Синтетическое резервное копирование

В качестве основы эта модель использует ранее подготовленные копии: Full Backup и инкрементную. С заданной периодичностью полная и инкрементные копии могут быть объединены в новую полную копию. Метод обладает высокой скоростью создания РК и восстановления утраченных данных, позволяет гибко управлять данными и существенно меньше нагружает сеть. Из недостатков – при повреждении промежуточных копий после «схлопывания» все последующие бэкапы также будут повреждены.

Правила и политики

Для надежного хранения резервных копий и обеспечения сохранности самих бэкапов при организации резервирования следует придерживаться правила «3-2-1» и выбранной схемы ротации. Наиболее критичные данные следует хранить в соответствии с правилом «3-2-1»: три копии в двух различных физических форматах, причем одна из копий должна храниться удаленно. Разберем каждый пункт подробнее.

В контексте этого правила число «три» обозначает количество копий, хранящихся в трех физически разных местах (не на одном ПК или сервере). Почему требуются именно три копии? Как правило, угрозы двум копиям оказываются зависимыми из-за логической организации резервного копирования.

Необходимость различия между физическими форматами обусловлена тем, что при таком подходе снижается вероятность одновременной потери всех копий.

Соответственно последний пункт – размещение бэкапов на удаленной площадке (вне офиса/основного ЦОД) – решает ту же задачу, что и первые два, но только через географическое распределение площадок хранения.

Необходимо ли следовать правилу «3-2-1» в 100% случаев? Конечно, нет. Все зависит от критичности, стоимости и вероятности угроз корпоративным данным. Помните: затраты на защиту не должны превышать ценность защищаемого объекта. При резервировании не очень ценных и критичных данных, а также в том случае, если угрозы маловероятны, реализовывать правило «3-2-1» можно лишь частично.

Рассмотрим две наиболее популярные схемы резервного копирования.

GFS («дед-отец-сын»)

В этом алгоритме резервное копирование состоит из трех ключевых шагов:

- «Grandfather» (дед) – полный бэкап на удаленный

и защищенный носитель. Делается редко, например один раз в месяц;
- «Father» (отец) – полное копирование, но на более быстрый по сравнению с пунктом выше носитель. Производится чаще, как правило, еженедельно;
- «Son» (сын) – дифференциальный или инкрементный ежедневный бэкап.

Ханойская башня (TOH)

Схема названа в честь известной математической головоломки. Из-за сложного уровня реализации применяется намного реже, чем GFS.
- На начальном этапе устанавливается интервал между выполнениями задач резервного копирования, например один день.
- Каждый второй интервал (первый, третий, пятый день и т. д.) – резервное копирование на первый выбранный носитель.
- Каждый четвертый интервал, когда не задействован первый носитель, – резервное копирование на второй носитель.
- Каждый восьмой интервал – на третий носитель и т. д.

Звучит сложно, однако многие современные решения могут автоматизировать реализацию этой схемы.

Способы организации резервной инфраструктуры

В зависимости от целей и бюджета резервного копирования возможен выбор из следующих вариантов.

Эксплуатация собственного ЦОД

Ресурсоемкая процедура построения системы резервного копирования в собственном дата-центре может быть оправдана следующими критериями: данные должны храниться строго в пределах компании, компания уже имеет собственный дата-центр, а также ресурсы (материальные и человеческие) для организации бэкапов. Этот подход подразумевает, что у вашей компании уже есть опыт администрирования собственной инфраструктуры, а мощности имеют достаточную степень резервирования.

Аренда площади в ЦОД

Такой вариант в отличие от предыдущего освобождает вас от выделения пространства, подведения необходимых коммуникаций и обеспечения безопасности в собственном помещении. Вопросы, связанные с охраной, пожарной безопасностью, непрерывным поступлением электроэнергии, владелец ЦОД полностью берет на себя.

Аренда инфраструктуры или сервисов у провайдера

Это один из наиболее простых и бюджетных вариантов организовать инфраструктуру для хранения резервных копий без капитальных затрат. Подрядчик берет на себя все задачи по администрированию вычислительных мощностей (IaaS) или непосредственно сервиса резервного копирования (BaaS).

Исходя из всего вышеперечисленного, наибольшее влияние на выбор способа оказывают параметры CAPEX и OPEX.

Кроме того, имеет смысл заранее определить значение RTO (Recovery Time Objective) и RPO (Recovery Point Objective). Первый показатель означает время, которое уйдет на восстановление данных после сбоя, а второй определяет длину периода, данные за который допустимо безвозвратно потерять. К примеру, веб-ресурс может иметь равно высокие RTO и RPO, а банк – равный RTO, но минимальный RPO.

Облачные BaaS-сервисы для резервного копирования

Термин BaaS расшифровывается как Backup as a Service – резервное копирование как услуга. Выбор BaaS – это соломоново решение. С одной стороны, оно экономически эффективно: исходя из задач, ресурсов и потребностей компании можно подобрать идеальное решение. С другой – нет необходимости строить собственную инфраструктуру резервного копирования, увеличивать штат ИТ-специалистов. Все, что вам потребуется, – обучить менеджерский состав обращению с сервисом. Рутинное взаимодействие с BaaS осуществляется через удобный пользовательский интерфейс, так что эта задача окажется не слишком сложной. Самый популярный на рынке стек решений, предлагаемых сервис-провайдерами, – инструменты Acronis Infoprotect, Veeam и Commvault.

Acronis Infoprotect

Простое, гибкое и бюджетное решение «все в одном» от Acronis позволяет создавать резервные копии приложений, серверов, рабочих станций, виртуальных машин и баз данных. Кроме того, решения Acronis обеспечивают защиту от криптомайнеров и программ-шифровальщиков. С помощью поведенческого анализа технология Acronis Active Protection обнаруживает нетипичную активность и блокирует любые процессы, связанные с попытками изменения или повреждения файлов: данные мгновенно сохраняются, а при повреждении автоматически восстанавливаются из резервной копии. Acronis Infoprotect также предоставляет возможность агентского резервирования. Для этого необходимо скачать агент с портала управления, установить его на объект резервного копирования и настроить политики.

Veeam

Программный комплекс Veeam для организации резервного копирования позволяет создавать в облаке резервные копии виртуальных машин, восстанавливать машины целиком или извлекать только отдельные файлы. Этот функционал сосредоточен в решении Veeam Backup & Replication. Кроме того, клиент может самостоятельно задавать сроки хранения данных и регулировать расписание задач резервного копирования. Для взаимодействия с сервисом используется

веб-портал, интегрированный с vCloud Director.

Если на площадке клиента уже установлен сервер Veeam B & R, с лицензиями Veeam Cloud Connect Backup он может использовать облако провайдера в качестве дополнительного хранилища резервных копий, тем самым обеспечивая соблюдение правила «3-2-1». В случае когда собственной системы резервного копирования нет, копирование с локальной площадки можно осуществлять с помощью Veeam Agent.

Commvault

Продвинутое решение для резервного копирования от Commvault позволяет создавать копии любых приложений, баз данных, крупных ИС корпоративного уровня вне зависимости от используемой ОС и платформы виртуализации. Защитить от потери данных можно как корпоративную инфраструктуру, так и облачные ресурсы.

Для восстановления данных не требуется взаимодействовать с провайдером облачных услуг: к услугам клиентов – удобная веб-консоль. С помощью всего одной программы-агента можно настроить хранение резервных копий сразу на нескольких облачных площадках.

Заключение

Представьте, что все информационные активы вашей компании – базы данных, файлы сотрудников, оцифрованная документация и многое другое исчезли в одночасье. Каков будет процент невосполнимых потерь?

Еще 10–15 лет назад организованную систему создания и хранения резервных копий могли позволить себе только компании ИТ-сферы и представители крупного бизнеса. Но настало время облаков – они дают возможность в мгновение ока разворачивать тестовые и продуктивные среды для ваших приложений и масштабировать мощности в пиковые часы и дни. Рынок решений для резервного копирования велик, и каждая компания может найти идеальный для себя инструмент. Крупным игрокам с серьезными запросами подойдут продукты Veeam и Commvault. Среднему бизнесу будет выгодно подключить BaaS на базе Acronis. Самое главное – иметь надежного партнера, который не позволит вашим данным сгинуть в недрах цифровой пучины. ■

Простота и гибкость облака

Компания NetApp, производитель программного обеспечения для управления данными в облаке, объявила об усовершенствовании ПО для управления данными NetApp ONTAP. NetApp также анонсировала улучшенный гибкий сервис NetApp Keystone Flex Subscription и новое решение NetApp SolidFire Enterprise SDS. Благодаря этим обновлениям компания помогает заказчикам по всему миру раскрыть потенциал облачных технологий. Теперь организации могут оптимизировать свою производительность и безопасность, сократить расходы, с легкостью перенести управление данными из локальных дата-центров в любое облако и использовать гибридную облачную инфраструктуру.

«Цифровая трансформация ускорилась до такой степени, что проекты, на реализацию которых раньше уходили годы, теперь требуют завершения в течение месяцев или даже недель, – заявил президент NetApp Цезарь Сернуда. – Благодаря инновационному ПО для управления данными NetApp теперь занимает уникальное положение на мировом рынке и помогает заказчикам быстро адаптироваться и осуществлять устойчивые преобразования в современном мире гибридных облаков. Мы облегчили процесс разработки приложений в облаке, перемещения приложений в облако, создания локальных облачных технологий».

Новые функции и возможности, которые представила компания NetApp

Расширенные возможности ПО NetApp ONTAP, которые обеспечивают большую консолидацию, более глубокую интеграцию в облако и постоянную доступность данных для повышения удобства, эффективности и защиты критически важных для бизнеса корпоративных приложений.

Обновление подписки NetApp Keystone Flex Subscription, обеспечивающей быстрый и гибкий путь к облачному центру обработки данных, основанной на принципе оплаты по мере роста, для получения локальных облачных сервисов. Подписка Keystone Flex Subscription также предлагает интеграцию в общедоступные облака, доступную через экосистему партнеров NetApp.

Новое решение NetApp SolidFire Enterprise SDS, которое обеспечивает простую и автоматизированную основу для частного облака с программным обеспечением NetApp Element в качестве автономной программно-определяемой системы хранения данных, которую можно использовать на любом оборудовании.