Интеллектуальная стратегия аварийного восстановления настольных компьютеров: модель «виртуальные компьютеры как услуга»

ТЕМАТИЧЕСКАЯ СТАТЬЯ

vmware®

Содержание

Краткий обзор

Руководители большинства организаций считают, что вероятность стихийных бедствий или длительных перебоев в энергоснабжении крайне низка и существующий план аварийного восстановления поможет предотвратить простой. Однако в действительности стихийные бедствия и аварии — далеко не редкость, а планы аварийного восстановления зачастую не обеспечивают ожидаемых результатов. Обычно во главу угла ставится безопасность серверов и сетевых компонентов, при этом настольные компьютеры остаются без какой-либо защиты. Это объясняется тем, что дублирование физических настольных компьютеров только для сохранения работоспособности в условиях чрезвычайной ситуации обходится слишком дорого. Как следствие, многие организации ничего не делают для устранения этого пробела в планах аварийного восстановления. Но если в случае выхода из строя настольных компьютеров сотрудники несколько дней не смогут работать, это повлечет за собой катастрофические последствия для бизнеса. Во избежание этого многие организации внедряют модель «виртуальные компьютеры как услуга», которая является доступным и удобным способом обеспечить высокую эффективность работы персонала и непрерывность бизнеса даже в случае стихийного бедствия.

Чрезвычайные ситуации больше не редкость

От катастроф не застрахован никто. Вспомним ураганы «Сэнди», «Айрин» и «Катрина». Если ваша организация находится в регионе, подверженном частому влиянию тропических штормов, ураганов, снежных бурь, землетрясений или экстремально высоких температур, то вероятность того, что в вашей компании наблюдаются (или вскоре будут наблюдаться) случаи перебоев в энергоснабжении или отсутствия сотрудников на рабочем месте по причине невозможности приехать в офис, довольно высока. Даже если непосредственно вас стихийное бедствие не коснется, на ваш бизнес могут негативно повлиять перебои в работе локального поставщика электроэнергии или отказ оборудования настольных компьютеров.

Мощный ураган «Сэнди» нанес организациям в Нью-Йорке ущерб в размере 6 миллиардов долларов.[1] Несмотря на то что «Сэнди» можно рассматривать как форс-мажорную ситуацию, недавний опрос, проведенный компанией CDW, показал, что более 25% корпоративных ИТ-систем за год простаивали 4 часа или более, а общая сумма убытков составила 1,7 миллиарда долларов.[2] Для отдельной организации стоимость нарушения рабочих процессов может измеряться тысячами долларов из расчета на одного сотрудника в день в связи со снижением эффективности работы и потерей возможностей для бизнеса.

Если персоналу для работы необходимы физические настольные компьютеры в офисе, но из-за погодных условий добраться до рабочего места невозможно или компьютеры просто не работают из-за перебоев в энергоснабжении, как сотрудники смогут получить доступ к своим приложениям и данным? Как в этом случае обеспечить непрерывность бизнеса?

Даже внутренняя инфраструктура виртуальных компьютеров и наличие электричества в офисе не станут гарантией того, что ваши сотрудники смогут выполнять рабочие задачи, если сервер, обеспечивающий работу этих виртуальных компьютеров, будет находиться в простаивающем ЦОД.

Аварийное восстановление настольных компьютеров — не самая легкая задача

Очевидно, что организациям необходимы планы аварийного восстановления для настольных компьютеров. Но создание отдельной среды аварийного восстановления настольных компьютеров в том виде, в каком она обычно представляется многим руководителям, связано со значительными капитальными и эксплуатационными расходами. Создание и обслуживание второго технического объекта и дублирование инфраструктуры настольных компьютеров — это задачи, которые требуют объема расходов, несопоставимого с прибылью многих компаний.

Кроме того, резервная среда должна полностью дублировать производственную инфраструктуру. Лучшей методикой в данном случае является проведение ежегодного тестирования системы аварийного восстановления для обеспечения ее работоспособности и доступности в любой момент. Согласно отчетам Gartner, на тестирование аварийного восстановления может тратиться до 150 000 долларов в год.[3]

Модель «виртуальные компьютеры как услуга»: страховка на случай аварийного восстановления настольных компьютеров

Модель предоставления виртуальных компьютеров как услуги все чаще называют интеллектуальной стратегией аварийного восстановления настольных компьютеров. Чтобы понять почему, необходимо сначала составить общее представление об этой модели. По сути, это облачная услуга по предоставлению конечным пользователям доступа к виртуальным компьютерам и приложениям на любом устройстве, включая планшеты, смартфоны, ноутбуки, ПК и «тонкие» клиенты, и в любой точке. Виртуальные компьютеры и приложения, предоставляемые из облака, работают как часть корпоративной ИТ-среды, хотя в действительности они запускаются в удаленном защищенном ЦОД. Вся инфраструктура, включая серверы, программное обеспечение, сеть и хранилище, находится в абсолютно надежных, превосходно защищенных и высокодоступных ЦОД поставщика услуг. При этом оплачивается только месячная подписка, стоимость которой зависит от числа и типа необходимых виртуальных компьютеров.

Модель «виртуальные компьютеры как услуга» идеально подходит для выполнения аварийного восстановления, так как в ее основе лежат соответствующие принципы. Поставщики услуг, использующие сетевую платформу «виртуальные компьютеры как услуга», могут без труда обеспечивать поддержку аварийного восстановления на базе одноименной модели для нескольких регионов и ЦОД. Это означает, что организация не только получает возможность работать с виртуальными компьютерами, расположенными в защищенном и высокодоступном ЦОД, который не затронут последствия аварии в вашем главном офисе, но и размещать свои виртуальные компьютеры в нескольких ЦОД поставщика услуг. Таким образом, в крайне маловероятном случае аварии в одном из ЦОД мирового уровня, ваши сотрудники смогут получить доступ к виртуальным компьютерам в другом ЦОД поставщика услуг.

Ниже приведен список причин, по которым модель «виртуальные компьютеры как услуга» является хорошим выбором для обеспечения аварийного восстановления настольных компьютеров.

- Виртуальные компьютеры, размещенные в облаке, доступны всегда, даже во время перебоев в энергоснабжении в офисе.
- Эффективность работы сотрудников не снижается; им потребуется только подключение к Интернету.
- Сотрудники могут работать где угодно и на любых устройствах, включая личные.
- ИТ-отделу организации не нужно обслуживать отдельную резервную среду или срочно выполнять подготовку среды аварийного восстановления в случае острой необходимости. Задачи ИТ-специалистов заключаются в разработке эталонного образа для восстановления, резервировании ресурсов и инициализации хранилища для виртуальных компьютеров и запуске процесса в нужный момент.
- По мере развития бизнеса подписку на услугу аварийного восстановления с использованием модели «виртуальные компьютеры как услуга» можно будет расширить всего лишь несколькими щелчками мыши.
- Отпадает необходимость в ежегодном тестировании системы аварийного восстановления, связанном с высокими расходами и значительными временными затратами.

Типичные сценарии аварийного восстановления с использованием модели «виртуальные компьютеры как услуга»

Как правило, аварийное восстановление на основе модели «виртуальные компьютеры как услуга» выполняется одним (или более) из следующих трех способов.

1. Защита для среды физических настольных компьютеров.
   При выборе этого сценария модель «виртуальные компьютеры как услуга» используется в качестве стратегии аварийного восстановления физических настольных компьютеров путем резервирования ресурсов в инфраструктуре поставщика услуг для всех или нескольких пользователей. В этом случае нужно только настроить учетную запись и инициализировать образы. При необходимости можно будет активировать виртуальные компьютеры, чтобы пользователи могли немедленно вернуться к работе.
2. Аварийное восстановление для инфраструктуры виртуальных компьютеров (VDI).
   Такой подход дает организации возможность работать с внутренней средой VDI, но применять модель «виртуальные компьютеры как услуга» в чрезвычайных ситуациях — при сбое ЦОД или сервера, обеспечивающего работу виртуальных компьютеров. Сотрудники смогут вернуться к выполнению рабочих задач всего через несколько минут.

3. Постоянное использование виртуальных компьютеров, предоставляемых как услуга. Поскольку в основе модели «виртуальные компьютеры как услуга» лежат принципы аварийного восстановления, что значительно упрощает работу ИТ-отделов и конечных пользователей (даже в отсутствие аварий), многие организации приняли решение перенести настольные компьютеры в облако на постоянной основе. Такой шаг обеспечивает заблаговременную защиту от стихийных бедствий или длительных простоев оборудования в основном офисе. В этом случае организации не потребуется отдельный план аварийного восстановления настольных компьютеров.

Эффективное решение по аварийному восстановлению на основе модели «виртуальные компьютеры как услуга» поддерживает различные подходы, благодаря чему можно подобрать сочетание, наиболее соответствующее потребностям вашего бизнеса. Приведем несколько примеров.

- «Горячее» или «холодное» аварийное восстановление
  - «Горячее» аварийное восстановление: немедленная доступность и постоянная готовность виртуальных компьютеров, размещенных в облаке. Эта модель подразумевает выделение и резервирование необходимых вашему бизнесу ресурсов, включая емкость хранилища и вычислительные ресурсы.
  - «Холодное» аварийное восстановление: несколько организаций совместно используют ресурсы инфраструктуры, например, для сотрудников, у которых нет необходимости в немедленном доступе к своим компьютерам, а требуется возобновление работы через определенное число часов. Хранилище выделяется для каждой компании отдельно.
- Использование выделенных или общих виртуальных компьютеров
  - Компании предоставляются полноценные виртуальные компьютеры с сохранением состояния под управлением ОС Windows 7 или Windows 8.
  - Используются общие сеансы виртуальных компьютеров с помощью службы удаленного подключения. Такая альтернатива помогает сократить объем дискового пространства и емкости хранилища, необходимый каждому пользователю, и свести расходы к минимуму. Многие организации используют для аварийного восстановления как общие, так и выделенные виртуальные компьютеры, предоставляемые как услуга.

Заключение

В современном мире, где работа может выполняться круглосуточно и без выходных, длительные простои недопустимы. Ураганы или неожиданные перебои в энергоснабжении не должны становиться причиной дорогостоящих перерывов в работе на несколько часов или дней. Если у вас нет эффективного плана аварийного восстановления для настольных компьютеров, задумайтесь о переходе к модели «виртуальные компьютеры как услуга». Это самый удобный, экономичный и надежный способ быстро вернуться к выполнению рабочих задач без снижения производительности. Предсказать, когда случится следующий шторм или крупная авария, невозможно, поэтому лучше принять меры защиты заранее. Дополнительные сведения о платформе VMware Horizon™ DaaS® и ее использовании для поддержки стратегии аварийного восстановления настольных компьютеров см. на веб-странице http://www.vmware.com/ru/products/daas.

---

1. Hurricane Sandy's Rising Costs («Рост убытков, причиненных ураганом "Сэнди"»), NY Times, 27 ноября 2012 г.
2. 2010 CDW Business Continuity Straw Poll: Plans Don't Align with Reality («Выборочный опрос CDW в 2010 г.: расхождение между планами и реальностью»)
3. Best Practices for Planning and Managing Disaster Recovery Testing («Лучшие методики, применяемые при составлении планов тестирования аварийного восстановления и управления ими»), Gartner, август 2011 г.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
125284, Россия, Москва, ул. Беговая, д. 3/1. Тел.: +7 (495) 212–2900 Факс: +7 (495) 212–2901 www.vmware.ru

01/14