

Акамова Надежда Владимировна

канд. пед. наук, доцент

Саранский кооперативный институт (филиал)

АНОО ВО Центросоюза РФ

«Российский университет кооперации»

г. Саранск, Республика Мордовия

ОБЕСПЕЧЕНИЕ КАТАСТРОФОУСТОЙЧИВОСТИ ДЛЯ ВИРТУАЛЬНОЙ ИНФРАСТРУКТУРЫ

Аннотация: в статье раскрывается понятие «виртуальная инфраструктура», рассматриваются технологии виртуализации, а также приводится пример построения концептуальной схемы работы VMware.

Ключевые слова: виртуальная инфраструктура, катастрофоустойчивость, VMware.

Успешное развитие информационной среды предприятия во многом зависит от целостности хранимых и обрабатываемых данных. Надежность вычислительной техники при этом является критическим фактором. Стоит учитывать, что надежность отдельных компонентов современных компьютеров достаточно велика, однако их количество в рамках современных корпоративных структур постоянно растет. Поэтому при планировании развития структур кластерных систем борьба за предотвращение потери данных и прерывание работы критических приложений в случае отказа одного из тысяч компонентов сохраняет свою актуальность [1].

Технология виртуализации содержит информацию о ряде возможностей повышения дохода и производительности, помимо простого преимущества безопасного разделения ресурсов. Клиенты VMware уже используют широкие возможности виртуализации для усовершенствования управления ИТ-ресурсами, обеспечения более высокого уровня обслуживания и ускорения ИТ-процессов. Для виртуализации ИТ-инфраструктуры был разработан специальный термин – виртуальная инфраструктура.

Катастрофоустойчивая система может состоять из двух систем виртуализации, функционирующих на одной серверной площадке. Обе системы являются активными. В каждой системе создается по одному кластеру VMware.

В каждый кластер добавляется сервер VMware Site Recovery Manager, управляющий процессами аварийного восстановления и реализующий функционал создания, тестирования и выполнения планов восстановления. Сервер VMware SRM устанавливается на отдельную виртуальную машину. Туда же устанавливается и СУБД MS SQL 2016 Express для этого VMware SRM сервера.

Схема работы VMware SRM строится по следующему принципу: файлы виртуальных машин реплицируются аппаратными средствами с основного массива на другой и, в случае сбоя, по сигналу администратора производиться запуск виртуальных машин из этих файлов на серверах другого кластера.

В нашем случае реализуется схема перекрестной защиты двух систем. Всего для двух кластеров защищается 10 виртуальных машин. В каждом кластере VM размещаются на выделенных томах. Тома перекрестно реплицируются между двумя дисковыми массивами. Сервер VMware SRM интегрируется с серверами VMware vCenter Server одного и второго кластера, что обеспечивает централизованное управление процессами аварийного восстановления, мониторинг их состояния, а также оповещение операторов в случае возникновения аварийных ситуаций.

Работа SRM основывается на репликации блоков данных уровня дисковых массивов. Репликация обеспечивается средствами программного обеспечения производителей систем хранения. Для интеграции с дисковыми массивами SRM использует программные адAPTERы репликации (SRA, Storage Replication Adapter), которые поставляются производителями дисковых массивов. Используя адаптер репликации, SRM проверяет наличие репликации LUN, на которых хранятся файлы защищаемых виртуальных машин; а также инициирует выполнение различных команд дисковыми массивами, таких как создание снапшотов, переключение режимов работы и т. п.

В каждом кластере создается своя группа защиты (Protection Group) и план аварийного восстановления. VMware SRM со стороны одного кластера посредством адаптера SRA определяет, какие LUN реплицируются, и позволяет создавать защищаемые группы (Protection Group) только для тех виртуальных машин, которые хранятся на реплицируемых LUN. При этом реплицируемый LUN находится в режиме «чтение-запись», а соответствующий LUN резервного сайта в режиме «только чтение».

В случае возникновения на основном сайте экстренной ситуации, требующей немедленного аварийного восстановления защищаемых виртуальных машин, оператор инициирует исполнение плана восстановления с помощью нажатия одной кнопки. VMware SRM прерывает репликацию, переводит резервный LUN в режим «чтение-запись» и выполняет все предопределенные шаги восстановления. Администратор контролирует выполнение шагов плана восстановления через vCenter и может в любой момент приостановить этот процесс. В результате все защищаемые виртуальные машины восстанавливаются даже при полном уничтожении одного из кластеров.

Благодаря отделению всей программной среды от исходной аппаратной инфраструктуры виртуализация позволяет объединить ряд серверов, инфраструктур хранения и сетей в единый пул ресурсов, динамически, безопасно и надежно распределляемый между приложениями по мере необходимости. С помощью этого инновационного решения организации могут создать вычислительную инфраструктуру с максимальной эффективностью, доступностью, автоматизацией и гибкостью, состоящую из недорогих серверов, соответствующих отраслевому стандарту.

Список литературы

1. Капулин Д.В. Разработка высоконадежных интегрированных информационных систем управления предприятием / Д.В. Капулин, Р.Ю. Царев, О.В. Дрозд [и др.]. – Красноярск: СФУ, 2015. – 184 с.

2. Виртуальная инфраструктура // Официальный сайт Компания БВ Информационные технологии (BW-IT.RU). – М., 2016 [Электронный ресурс]. – Режим доступа: <http://www.bw-it.ru>