СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ КОМПЬЮТЕРНОЙ СЕТИ

С 1998 г.
М.А. Копытов, Ю.П. Рогов

Общие проблемы и задачи сопровождения и поддержки системного программного обеспечения достаточно подробно изложены в [1]. Здесь же мы хотим остановиться на некоторых вопросах системного администрирования конкретной компьютерной сети.

Главная забота системного администратора состоит в поддержании компьютерной сети в рабочем состоянии. Это означает, что каждый зарегистрированный в сети пользователь (user) должен получать соответствующий сервис при использовании различных видов компьютеров и программного обеспечения.

Когда количество пользователей переходит за критическую черту (в каждом конкретном случае она своя), системному администратору приходится решать задачу минимизации своих временных и физических затрат на администрирование. Для этого производится концентрация различных сетевых служб на одном сервере, в одной базе данных, на одном дисковом устройстве, в одном общем файле.

К сожалению, в этом случае вся система в целом становится более уязвимой и менее защищенной от внешних и, особенно, внутренних злоумышленников - хакеров.

Кроме этого, если какой-либо из серверов начинает исполнять слишком много различных функций (NIS, DNS, email, файловый сервер и др.), качество и скорость выполнения заказов на эти функции резко снижаются. В этом случае начинают испытывать неудобства все пользователи сети, включая самого администратора.

Кстати, для того чтобы системный администратор лучше чувствовал проблемы рядового пользователя и быстрее реагировал на различные системные зависания, сбои и замедление реакции на выполнение своих задач, он не должен сам работать на самом мощном сервере, особом индивидуальном дисковом устройстве и в отдельном адресном (IP-addresses) пространстве.

Итак, после того как концентрация служб привела к перечисленным выше проблемам, приходится решать вопрос о распределении этих служб по различным серверам. Файловый сервер, как один из самых загруженных, не должен выполнять другие функции, кроме своих непосредственных. Эту задачу нам еще предстоит решить в ВЦ РАН, так как сервер, к сожалению, занят обслуживанием клиентов PC-NFS на персональных компьютерах, является NIS-сервером и сервером для бездисковых (diskless) рабочих станций. Но такие важные функции, как функции Web-сервера, DNS-сервера и почтового сервера выполняются на других рабочих станциях. После покупки новых дополнительных серверов и эти важные функции INTERNET будут перераспределяться.

Гетерогенность компьютерной сети, т.е. наличие разнородных вычислительных систем и разнообразных операционных систем, не облегчает задачи администрирования. Системному администратору приходится решать вопросы сопровождения сетевых приложений для программных систем DOS,Windows 3.x, Windows-95 на персональных компьютерах, для операционной системы OSF на станциях фирмы DEC, различных версий UNIX, в том числе Solaris-1 (SunOS) и Solaris-2 на рабочих станциях фирмы SUN. Остановимся на последних.

На первых, включенных в компьютерную сеть рабочих станциях фирмы SUN была установлена операционная система SunOS (версия 4.1.3) или Solaris-1. Было закуплено лицензионное программное обеспечение, в том числе так называемые SUN-компиляторы и графические пакеты под эту операционную систему.

Замена старой операционной системы на новую (Solaris-2) предполагает отказ от всех этих программных продуктов и переход на новые SPARC-компиляторы. Это потребует дополнительных средств и дополнительных усилий по их сопровождению. Сейчас на всех серверах локальной сети ВЦ РАН, обеспечивающих функции INTERNET, установлена операционная система Solaris-2, более надежная с точки зрения защиты от несанкционированного доступа. Но в минимальном объеме для использования имеющегося уже программного обеспечения предполагается сохранить и прежнюю версию этой операционной системы.

Несколько изменилось системное сопровождение персональных компьютеров с точки зрения их сетевых функций. Наряду с сетевым лицензионным программным обеспечением PC-NFS версии 4.0 для MS DOS в ВЦ РАН эксплуатируется и заново устанавливается PC-NFS версии 5.1, в том числе и для Windows 3.x. Несмотря на наличие лицензии на 25 установок, реально можно обеспечить функционирование гораздо большего числа персональных компьютеров в сети. Это осуществляется за счет специального мониторинга с использованием так называемого лицензионного сервера в сети.

Для Windows-95 и Windows-97 наличие установленного на персональном компьютере программного обеспечения PC-NFS необязательно, так как здесь имеется своя сетевая поддержка.

В настоящий момент в локальной сети ВЦ РАН (ЛВС ВЦ РАН) функционируют более пятидесяти персональных компьютеров.

После того как серверы, выполняющие различные функции в сети, стали в какой-то степени независимы друг от друга, т.е. перестали иметь общую базу данных по пользователям, хостам и пр., перед системным администратором встала задача синхронизации проводимых пользователями изменений и отслеживание этих изменений.

Приведем несколько примеров. С использованием аппарата периодического запуска программ (cron) производится сканирование домашних каталогов пользователей на наличие в них файла ~/.forward, который отвечает за переадресацию электронной почты. Вся эта информация собирается в одном файле, доступ к которому открыт и с файлового сервера, и с почтового. На почтовом сервере также периодически запускается командный файл, обрабатывающий полученную информацию, формирующий новое содержимое файла /etc/aliases и инициализирующий его командой newaliases.

Более простой способ отслеживания изменений на различных серверах сети состоит в модификации, там где это возможно, командных файлов, отвечающих за эти изменения. Модификация состоит либо в запрещении выполнения командного файла с переадресовкой в другой, либо в добавлении в него команд, сообщающих тем или иным способом (email, запись в файл) заранее выбранному пользователю о факте его выполнения.

Нам могут возразить, что все эти процедуры можно проделать гораздо проще и выполнять автоматически. Но для этого нужно открыть привилегированный доступ с одного сервера на другой, а это по соображениям безопасности нежелательно, тем более что задачи обеспечения безопасности и надежности системы являются наиболее важными для системного администратора [2,3].

Эти задачи близки по своему содержанию, но имеется ряд принципиальных отличий, существенным образом влияющих на методику решения этих задач.

Задача обеспечения надежности связана с изучением слабых мест в системе, выявлением ошибок в системных программах, с заменой одних элементов системы на другие, более надежные, а также с

совершенствованием программно-аппаратных средств, определяющих работу системы.

Поэтому системный администратор должен следить за развитием этих программно-аппаратных средств, отслеживать появление очередных версий используемых продуктов, инициировать их приобретение и производить их инсталляцию.

С другой стороны, обеспечение надежности предполагает организацию такой методики использования программно-аппаратных средств, при которой возможные отказы системы не приводили бы к длительным простоям и потере пользовательской и системной информации. Эту методику иногда называют системой высокой готовности.

Степень готовности системы к возобновлению работы после отказов и сбоев при минимальной потере информации может быть различной в зависимости от функциональных задач, решаемых системой.

Высокая готовность обеспечивается резервированием программно-аппаратных средств. Различают три вида резервирования: "горячее", "холодное", "теплое".

"Горячее" резервирование предполагает наряду с использованием основных программно-аппаратных средств постоянное функционирование дополнительных дублирующих средств, обеспечивающих сохранность информации и быстрое возобновление работы после отказов и сбоев основной системы.

При возникновении ситуации отказа при "горячем" резервировании система автоматически переходит на работу резервных средств, предварительно выполнив соответствующие процедуры восстановления информации.

"Холодное" резервирование обеспечивается хранящимся на складе, дополнительным резервным оборудованием, которое всегда можно ввести в строй после отказа основного, а также продуманной системой регулярного копирования информации.

"Горячее" резервирование обеспечивает возобновление работы системы в течение нескольких минут, "холодное" - нескольких часов и даже суток.

Реализация "холодного" и "горячего" резервирования требует значительных финансовых и прочих затрат.

Поскольку стоимость оборудования для академической системы, коей является информационно-вычислительная система ВЦ РАН, является решающим фактором, мы не можем реализовать ни "холодного", ни "горячего" резервирования. Наша методика обеспечения надежности работы системы связана с "теплым" резервированием.

Основные элементы этой методики следующие:

- файловые системы отображаются на физических устройствах, использующих RAID-технологию;
- ЛВС ВЦ РАН оснащена системой бесперебойного питания;
- осуществляется регулярное копирование пользовательской информации на магнитную ленту (back up);
- подготовлен и находится в "холодном" резерве на одном из серверов ЛВС сконфигурированный загрузочный вариант системы, зеркально повторяющий основной рабочий вариант.

В случае отказа главного сервера системы его зеркальный вариант должен стать основным. Время перезапуска системы с перекоммутацией физических устройств, но без глобального восстановления пользовательской информации с лент в этом случае составляет 1 ч.

Другой важной задачей, которую приходится решать системному администратору, является обеспечение безопасности системы. Между обеспечением надежности и безопасности имеется ряд отличий.

Прежде всего при обеспечении безопасности системы необходимо учитывать человеческий фактор, поскольку защищаться приходится от людей, случайным образом или умышленно проникающих незаконно в систему. Цели проникновения могут быть следующими:

- поиск и незаконное чтение чужой информации;
- порча информации или ее подмена;

- незаконное использование ресурсов системы;
- компьютерное хулиганство;
- вывод из строя системы.

Пятилетний опыт использования ЛВС ВЦ РАН позволил нам накопить некоторый опыт борьбы с компьютерными нарушителями и разного рода хакерами.

Однако в данной статье мы не собираемся подробно рассматривать конкретные мероприятия по повышению безопасности системы из соображений той же безопасности. Ограничимся лишь утверждением, что эти мероприятия направлены на децентрализацию серверных и административных функций.

И тут мы снова, с сожалением, должны констатировать, что некоторые мероприятия, связанные с повышением надежности и безопасности во многом противоречивы.

Повышение надежности часто требует концентрации системных функций, чтобы с наименьшими затратами можно было осуществить резервирование. Обеспечение безопасности, напротив, требует децентрализации, поскольку вероятность несанкционированного доступа в систему в этом случае уменьшается.

Таким образом, системному администратору постоянно приходится в своей работе сталкиваться с перечисленными выше проблемами и оптимально решать нелегкие задачи повышения безопасности, надежности и работоспособности компьютерной сети.

ЛИТЕРАТУРА

1. Байкова И.В., Копытов М.А., Кулагин М.В., Рогов Ю.П., Михайлов Г.М., Привезенцев Ю.А. Распределенные информационно - вычислительные системы. Вып. 1. Локальная сеть ВЦ РАН. М.: ВЦ РАН, 1995. 111с.
2. Байкова И.В., Копытов М.А., Кулагин М.В., Рогов Ю.П., Метелкин А.В., Михайлов Г.М., Плечов П.Ю. Распределенные информационно - вычислительные системы. Вып. 2. Инфраструктура и базовые средства локальной сети ВЦ РАН. М.: ВЦ РАН, 1996. 96с.
3. Евтушенко Ю.Г., Копытов М.А., Кулагин М.В., Михайлов Г.М., Рогов Ю.П. Локальная сеть ВЦ РАН и INTERNET //Информационные технологии и вычислительные системы. 1996, N3. с.43-52.