ГОСУДАРСТВЕННЫЙ НАУЧНЫЙ ЦЕНТР РОССИЙСКОЙ ФЕДЕРАЦИИ

ИНСТИТУТ ФИЗИКИ ВЫСОКИХ ЭНЕРГИЙ

ИФВЭ 2008–25
ОМВТ

А.С. Климов, В.В. Котляр, Е.В. Попова

ИСПОЛЬЗОВАНИЕ СВОБОДНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ОРГАНИЗАЦИИ СЕРВЕРА ЭЛЕКТРОННОЙ ПОЧТЫ С ПОВЫШЕННОЙ ОТКАЗОУСТОЙЧИВОСТЬЮ

Протвино 2008

УДК 004.056 М-24

Аннотация

Климов А.С., Котляр В.В., Попова Е.В. Использование свободного программного обеспечения для организации сервера электронной почты с повышенной отказоустойчивостью: Препринт ИФВЭ 2008 –25. – Протвино, 2008. – 8 с., 7 рис., библиогр.: 5.

В данной работе рассматриваются: способ организации сервера электронной почты с повышенной отказоустойчивостью, настройка кластерной системы из двух серверов, настройка HA Heartbeat, DRBD, OCFS2.

Abstract

Klimov A..S., Kotlyar V.V., Popova E.V. Free Software Usage for the Installation of a Fault-tolerance E-mail Server with High Availibility: IHEP Preprint 2008 –25. – Protvino, 2008. – p. 8, figs. 7, refs.: 5.

Organization of a fault-tolerance e-mail server with high availability, setup a cluster system for two servers, setup HA Heartbeat, DRBD, OCFS2 are described.

Введение

Установка и настройка систем с повышенной отказоустойчивостью является одной из часто решаемых задач в рамках сетевых инфраструктур. Существует достаточно большой перечень сервисов, используемых рядовыми пользователями в локальной сети или сети Internet, для которых требуется обеспечить повышенный уровень надежности и доступности, так как они используются в постоянной работе и любой простой или потеря данных являются критичными событиями. К такого рода сервисам и относится сервис электронной почты.

Описание сервиса электронной почты

Рассмотрим общую систему электронной почты масштаба одной организации. Данного рода система должна состоять из нескольких базовых сервисов, обеспечивающих прохождение электронной почты через сеть Internet и сеть Intranet (локальную компьютерную сеть организации). В процессе отправки и получения писем участвуют следующие серверы с базовыми сервисами (рис. 1):

- DNS-серверы, поддерживающие используемый домен имен в сети Internet, где каждому имени или группе имен ставится в соответствие так называемая MX (Mail Exchange) запись (одна или несколько), которая указывает имя реального сервера, на который и следует слать электронную почту для данного имени (адреса);
- MX-серверы, которые принимают всю входящую почту и обычно используются для отправки всей исходящей почты с целью уменьшения вероятности распространения сетевых почтовых вирусов. Так как через такие серверы проходят все электронные письма организации, там же обычно устанавливаются фильтры против электронного спама. Число писем в очередях на отправку может достигать нескольких тысяч. Электронное письмо находится в очереди до тех пор, пока не будет отправлено или удалено по истечении срока давности (например, 2 месяца);
- конечные почтовые серверы – именно они и являются последним пунктом в схеме получения почты внутри организации, и уже с них обычные пользователи имеют возможность забирать свои письма;

- антивирусные серверы или системы, участвующие в проверке электронной почты на вирусы. Эти системы устанавливаются в одной или нескольких точках прохождения электронного письма в зависимости от объема почтового трафика и производительности самой антивирусной системы.

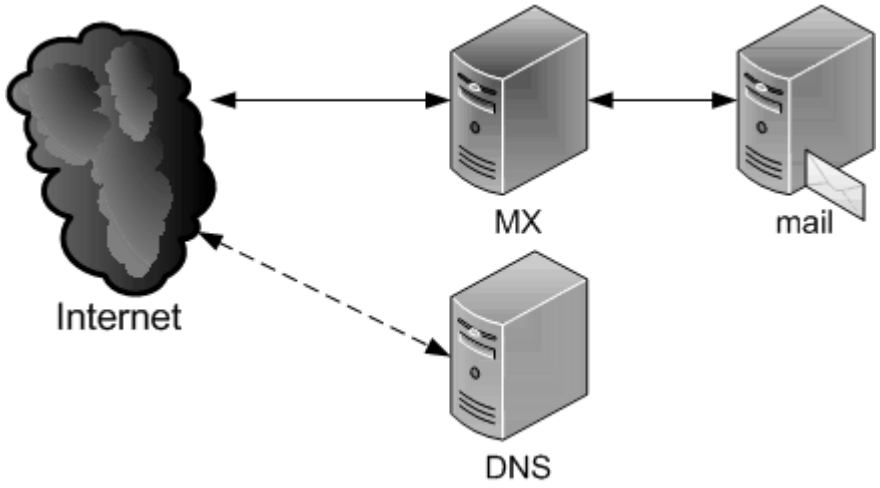


Рис. 1. Базовые сервисы электронной почты.

Все вышеизложенные сервисы могут иметь различные способы обеспечения безотказной работы и сохранности данных. В этой работе мы затронем только уровень, с которым работает непосредственно пользователь, т.е. сервер электронной почты большинства пользователей организации (теоретически любой пользователь может иметь свой собственный почтовый сервер).

Сервер электронной почты CommuniGate Pro и антивирусная система BitDefender

В качестве программного обеспечения для сервера электронной почты могут использоваться как промышленные, так и свободно распространяемые системы. Далее будет описано построение отказоустойчивой системы на базе сервера Communigate Pro и дополнения к нему – антивируса BitDefender. Следует заметить, что такие же принципы могут использоваться и для любых других программ (не обязательно почтовых систем).

Основанный на открытых стандартах сервер CommuniGate Pro является интегрированной платформой, в которой реализованы функции хранения и отправки электронной почты. Основные подсистемы CommuniGate Pro включают в себя [5]:

- управление идентификацией пользователей;
- управление хранением данных;
- передачу почты;
- среду для приложений реального времени;
- службы доступа к данным (www, imap, pop, wap);
- современные средства безопасности;
- многоуровневое администрирование;
- кластерные решения.

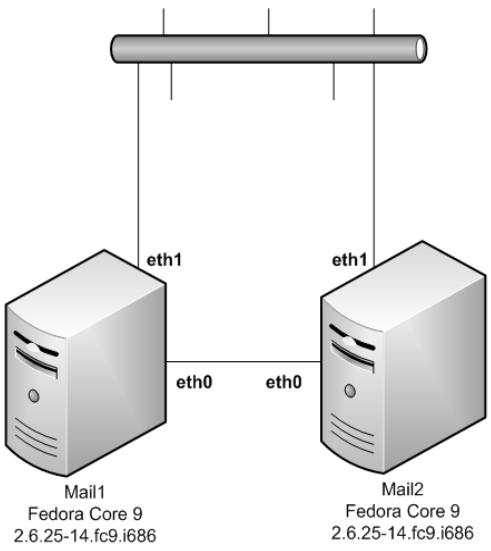
Использованное в нашей системе антивирусное ПО BitDefender Mail Protection for Enterprises [4] является хорошим решением для защиты от вирусов, спама и троянских программ. Этот продукт может быть интегрирован в почтовые серверы Sendmail, qmail, Courier, CommuniGate Pro. Кроме того, BitDefender SMTP Proxy может сканировать почту независимо от почтового сервера. Достоинствами этой антивирусной системы являются:

- доступный интерфейс для удаленного администрирования;
- простота внедрения и сопровождения;
- срочное реагирование при вирусных эпидемиях;
- сертифицированный антивирусный механизм;
- мощные технологии защиты от спама;
- управление пользователями и группами;
- интеллектуальные системы обновления.

Антивирусные механизмы защиты сертифицированы широко признанными фирмами, специализированными в антивирусном программном обеспечении: ICSA Labs, Virus Bulletin, CheckMark, CheckVir и TUV. BitDefender поддерживает более 80 различных типов архивов для обнаружения вирусов в почтовых приложениях. Антиспам-фильтр этого ПО поддерживает технологии эвристического анализа, bayesian, URL-фильтры, разрешающие и запрещающие списки.

Общее устройство системы

В зависимости от масштабов применения, т.е. от числа пользователей и интенсивности использования системы, возможны различные схемы её устройства. Мы ориентировались на уровень небольшого предприятия: 500-3000 человек. Предлагаемая схема устройства показана на рис. 2.




```
Filesystem      Size  Used Avail Use% Mounted on
/dev/md1         14G  490M   13G   4% /
/dev/md7         17G  346M   16G   3% /opt
/dev/md5        4.6G  2.5G  2.0G  56% /usr
/dev/md6        9.2G  167M  8.6G   2% /usr/local
/dev/md4         19G  173M   18G   1% /home
/dev/md3        4.6G  234M  4.2G   6% /var
/dev/md2        4.6G  144M  4.3G   4% /tmp
/dev/md0         471M   17M  430M   4% /boot
tmpfs           1013M     0 1013M   0% /dev/shm
/dev/drbd0       694G   78G  617G  12% /data
```

```
...
grep OCFS2 /boot/config-2.6.25-14.fc9.i686
CONFIG_OCFS2_FS=m
...
```

Рис. 2. Схема устройства системы.

Для повышения отказоустойчивости одновременно используются два сервера, работающие параллельно. Они имеют высокоскоростное подключение к компьютерной сети предприятия и высокоскоростное подключение между собой, что позволяет использовать ПО, обеспечивающее работу сервера в режиме повышенной отказоустойчивости.

Для обеспечения такого режима работы было использовано следующее дополнительное ПО:

- HA (High Availability) Heartbeat – постоянно доступная кластерная система, осуществляющая контроль за работой сервисов сервера электронной почты в рамках созданной кластерной системы из двух компьютеров;
- DRBD (Distributed Replicated Block Device) – система, позволяющая создавать RAID-массивы уровня 1 (зеркальные диски), используя сетевые соединения [3];
- OCFS2 (Oracle Cluster File System) – одна из файловых систем, рассчитанная на использование в кластерных системах и имеющая возможность учитывать конкурентные операции ввода/вывода над файлами.

Базовой операционной системой выбрана свободно распространяемая ОС – Linux Fedora Core 9.

Таким образом, была построена кластерная система из двух серверов с общим дисковым пространством, доступным одновременно с любого из членов кластера. Сам сервер электронной почты может работать только на одном из серверов и автоматически запускается на другом в случае отказа первичного компьютера. Второй же сервер используется для организации системы резервного копирования данных на магнитные ленты.

Установка и настройка DRBD

Общее устройство системы DRBD показано на рис. 3. На нем представлены два сервера кластерной системы, которые содержат стандартные компоненты ядра Linux: файловую систему, буферный кэш, планировщика дисковых операций, драйверы диска, TCP/IP стэк протокола и драйвер сетевой карты NIC (Network Interface Card). Стрелками обозначены потоки данных между этими компонентами.

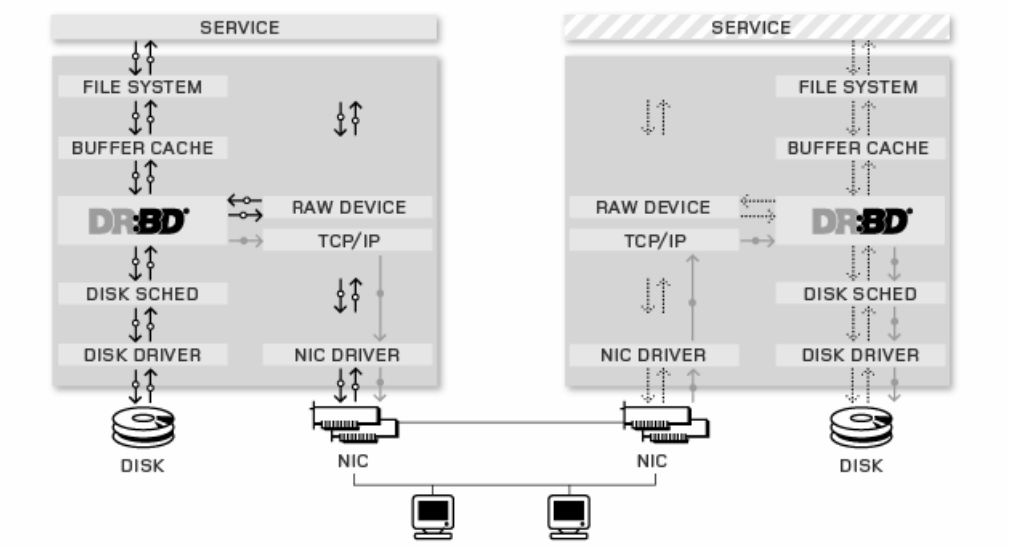


Рис. 3. Устройство системы DRBD.

Для обеспечения полной функциональной независимости двух серверов кластера и использования равномерной загрузки каждого из них был использован режим работы DRBD, когда оба сервера являются первичными – “dual-primary mode”. Для репликации данных был использован “Protocol C” – синхронный протокол репликации: локальные операции записи на сервере считаются полностью выполненными, когда будут подтверждены локальная и удаленная записи данных на диск, и поэтому выход из строя одного из узлов не влечет за собой потерю информации. Следует отметить, что при репликации данных происходит их верификация, позволяющая полностью исключить ошибки в передаче по сетевым каналам связи. Для такой верификации нами был использован алгоритм sha1 (криптографический алгоритм хэширования). Немаловажно также отметить то, что система позволяет осуществлять верификацию данных обоих серверов в рабочем режиме, т.е. без их останова. Процедура установки и пример конфигурационного файла показаны на рис. 4.

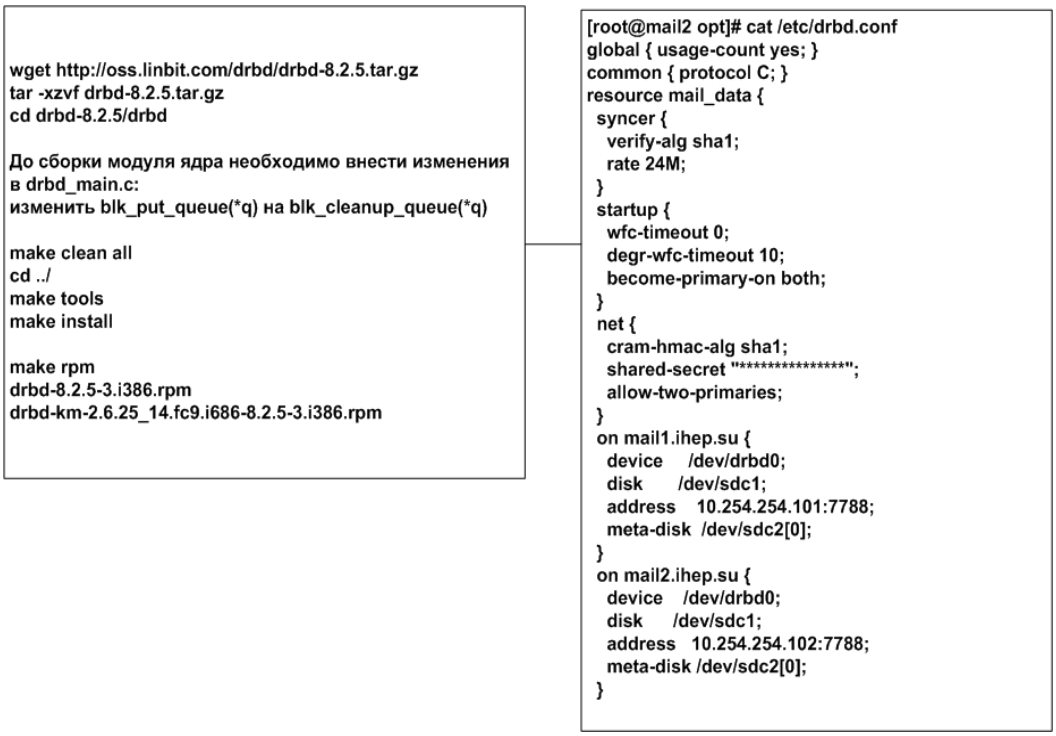


Рис. 4. Установка и настройка DRBD.

Использование файловой системы OCFS2

OCFS2 является симметричной разделяемой дисковой кластерной системой, позволяющей одновременно читать и писать данные всем членам кластера напрямую в дисковое хранилище [2]. К основным плюсам данной файловой системы относятся:

- варьируемый размер блока данных: от 512 байт до 4 Кбайт;
- пространственно-определенное распределение: отслеживание распределенного пространства в диапазонах блоков особенно эффективно при хранении больших файлов;
- гибкое распределение: поддерживаются неполные файлы и незаполненное пространство для увеличения производительности и эффективности хранения. Существующие файлы могут иметь «дыры» для большей эффективности;

- журналирование: поддерживаются режимы прямой и обратной записи журнальных данных, обеспечивающих целостность файловой системы в случае отказа питания или сбоя системы;
- платформонезависимость: поддерживается одновременное использование различными аппаратными платформами 32bit, 64bit (i86_64,ia64), 64bit PowerPC (системы отличаются способом хранения данных в памяти);
- встроенный распределенный менеджер блокировок кластерной системы;
- большие заголовки: заголовки файлов с размером в блок позволяют хранить маленькие файлы в этих же заголовках;
- большое число обслуживающих утилит, схожих по использованию с утилитами для широкораспространенной файловой системы EXT3.

Пример настройки OCFS2 приведен на рис. 5.

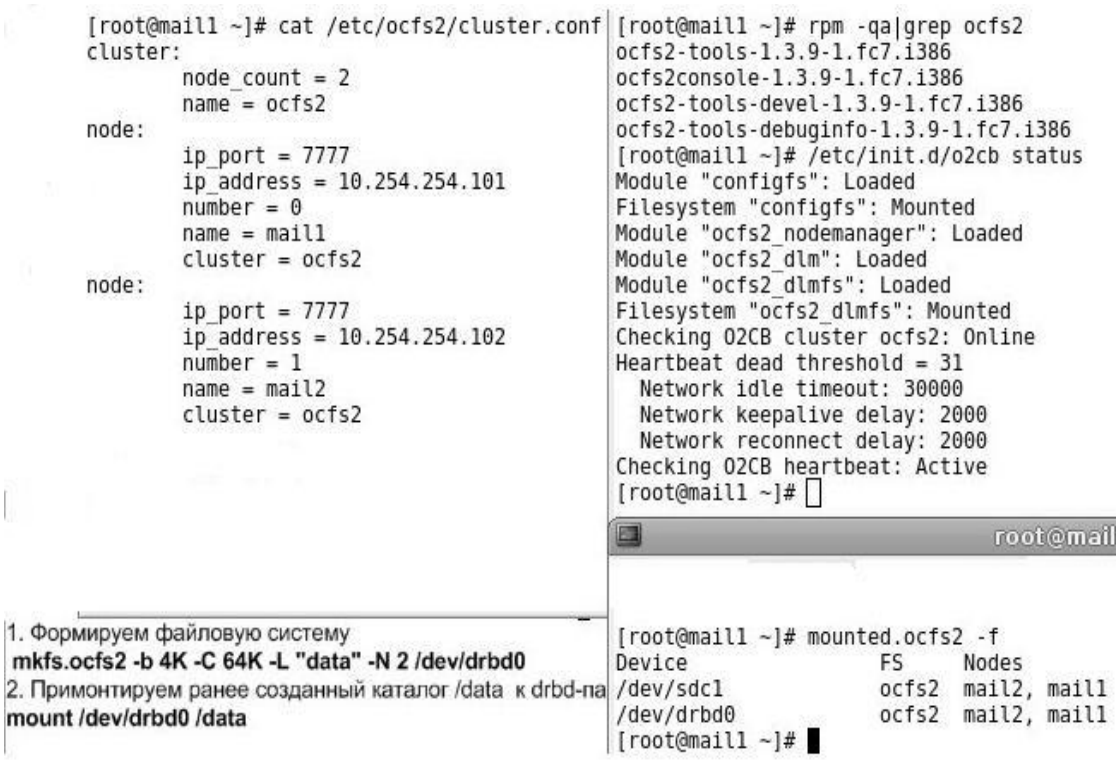


Рис. 5. Настройка OCFS2.

Настройка HA Heartbeat

Для обеспечения работы системы в режиме кластера было использовано программное обеспечение HA Heartbeat [1], которое обладает следующими свойствами:

- позволяет объединять группу компьютеров, которые совместно обеспечивают работу какого-либо сервиса;
- если один из компьютеров выходит из строя, другие выполняют его работу: это заключается в перехвате IP-адреса и перехвате сервиса;
- новые задачи начинают приходить на «перехвативший» компьютер.

Основное предназначение системы – обеспечить доступность, а не высокую производительность.

Примером обеспечения доступности сервиса может служить перехват функций по обеспечению доступа к данным дискового хранилища сервера А сервером В (см. рис. 6.) в случае выхода сервера А из строя.

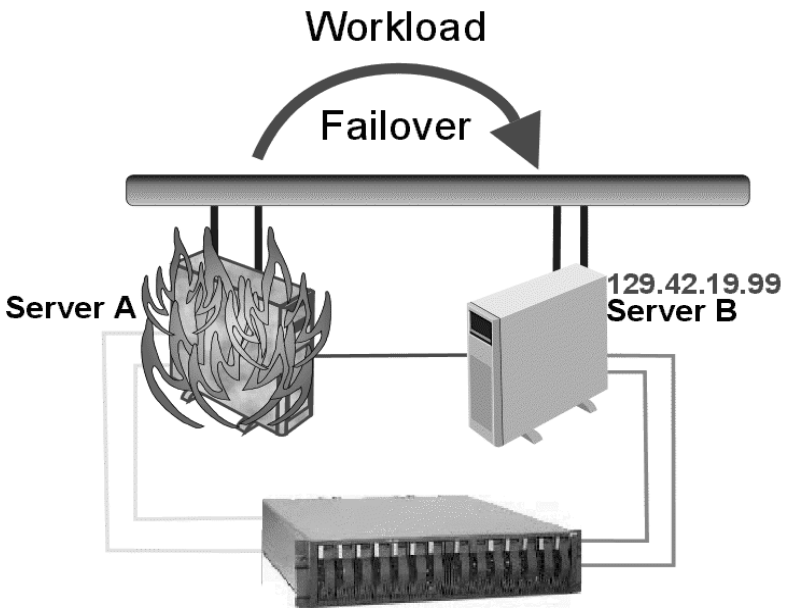


Рис. 6. Обеспечение обработки отказа в HA Heartbeat.

Когда оба сервера находятся в работе, можно распараллелить выполняемые ими функции, уменьшив таким образом нагрузку на каждый из членов кластерной системы. На рис. 7 представлены настройки ПО для работы в системе из двух серверов с общим (одним на кластер) сетевым именем.

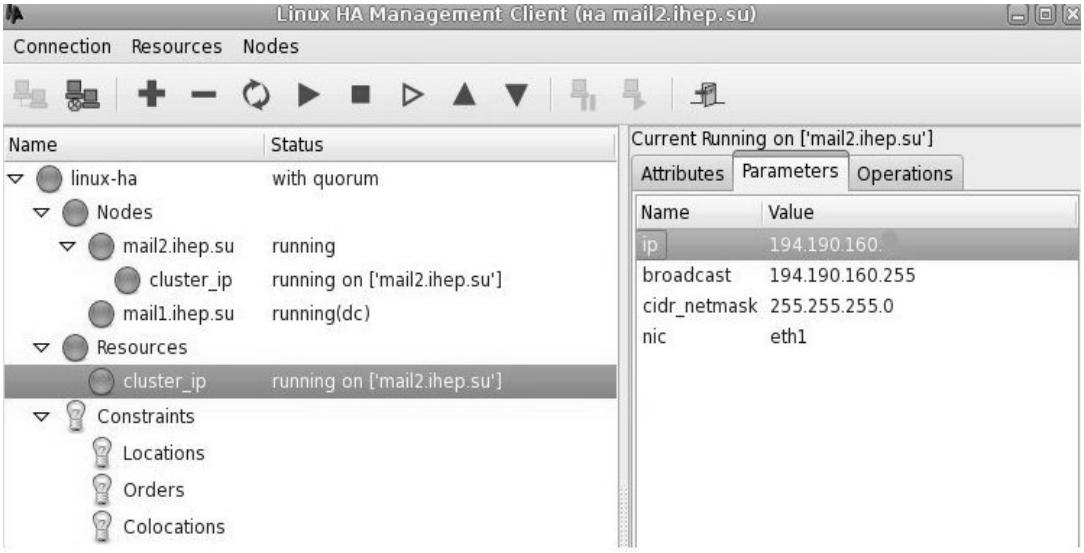


Рис.7. Настройка Linux HA Heartbeat.

В нашем случае на каждом из серверов установлено ПО, необходимое для работы сервиса электронной почты (CommuniGate Pro) и антивируса (BitDefender). При этом серверы используют общий кластерный диск для хранения настроек и файлов данных. Сами же сервисы запущены только на одном из серверов – том, который отвечает за работу кластерного сетевого адреса в текущий момент. Другой сервер в это же время используется для организации системы резервного копирования данных кластера на магнитные ленты.

Заключение

Сервис электронной почты в настоящее время является одним из главных сервисов в компьютерной сети. Он может быть построен на различных аппаратных и программных платформах, для каждой из которых существуют свои способы сделать данный сервис отказоустойчивым. Для свободно распространяемого программного обеспечения и операционной системы Linux это может быть кластерная система HA Heartbeat. Она в совокупности с другими средствами позволяет довольно легко создавать системы, устойчивые к отказам какой-либо из компонент, и может широко применяться практически вне зависимости от специфики самого сервиса. Привлекательным моментом является достаточно низкая стоимость при высокой надежности системы.

Описанная система успешно применяется в ИФВЭ для реализации службы e-mail с числом пользователей около 500 человек и средним количеством писем в день около 1500.

Список литературы

[1] The High Availability Linux Project,
http://www.linux-ha.org/

[2] The Oracle Cluster File System Project,
http://oss.oracle.com/projects/ocfs2/

[3] The Distributed Replicated Block Device Project,
http://www.drbd.org/

[4] BitDefender antivirus,
http://www.bitdefender.com/

[5] CommuniGate Pro mail system,
http://www.communigate.com/

Рукопись поступила 4 декабря 2008 г.

А.С. Климов, В.В. Котляр, Е.В. Попова
Использование свободного программного обеспечения для организации сервера электронной почты с повышенной отказоустойчивостью.

Редактор Л.Ф. Васильева.

Подписано к печати 08.12.2008. Формат 60 × 84/8. Офсетная печать.
Печ. л. 1,25. Уч.- изд. л. 1. Тираж 80. Заказ 100. Индекс 3649.

ГНЦ РФ Институт физики высоких энергий,
142281, Протвино Московской обл.

Индекс 3649

П Р Е П Р И Н Т 2008-25, ИФВЭ, 2008