

Министерство образования и науки Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г.ЧЕРНЫШЕВСКОГО»

Кафедра дискретной математики и
информационных технологий

Автоматизация администрирования сетей Linux в условиях предприятия

АВТОРЕФЕРАТ
бакалаврской работы

студента 4 курса 421 группы
направления 09.03.01 «Информатика и вычислительная техника»
факультета КНиИТ
Матвиенко Романа Геннадьевича

Научный руководитель

к. ф.-м.н., доцент

В.А. Поздняков

Зав. кафедрой

к. ф.-м.н., доцент

Л.Б. Тяпаев

Саратов 2016

ВВЕДЕНИЕ

Изначально автоматизация задач системного администрирования сводилась к написанию скриптов - небольших программ, написанных на так называемых сценарных языках. Скрипты позволяют минимизировать ручную работу администратора, повысить скорость решения задач и т.д. Однако при наличии большого парка техники, перед администратором снова встает вопрос ручных манипуляций - нужно запускать скрипты, или написания еще большего количества скриптов, что в итоге вырождается в огромную сложную систему, поддержка которой отнимает огромное количество времени, и решение возникающих ошибок в большинстве случаев требует неочевидного решения. Для решения подобных проблем было написано несколько систем управления конфигурациями - инструментов, которые позволяют администраторам упростить автоматизацию большинства задач настройки и поддержки парка техники. Из всех инструментов управления конфигурациями можно выделить 2 самых известных - это Puppet и Chef В выпускной квалификационной работе будет более подробно рассмотрено приложение Puppet и приведены несколько решений задач автоматизации, которые могут быть использованы в различных компаниях и предприятиях.

Puppet — кроссплатформенное клиент-серверное приложение, которое позволяет централизованно управлять конфигурацией операционных систем и программ, установленных на нескольких компьютерах. Написано на языке программирования Ruby. Отмечается как одно из самых актуальных средств конфигурационного управления по состоянию на 2014 год. Puppet позволяет просто настроить и впоследствии быстро управлять практически любой сетью на базе любой операционной системы Red Hat Enterprise Linux, CentOS, Fedora, Debian, Ubuntu, OpenSUSE, Solaris, BSD, Mac OS X и Microsoft Windows (через cygwin). Система Puppet достаточно популярна в среде IT-компаний, в частности, её используют Google, Fedora Project, Стэнфордский университет, Red Hat, Siemens IT Solution, SugarCRM.

Актуальным является автоматизация задач администрирования в предприятиях имеющих обширную IT-инфраструктуру.

В работе будут решены такие задачи, как:

- 1 Производство установки и первоначальной настройки Puppet
- 2 Реализация автоматического конфигурирования межсетевого экрана Netfilter средствами Puppet
- 3 Реализация автоматического развертывания Openvpn средствами Puppet
- 4 Реализация автоматического развертывания HAproxy средствами Puppet
- 5 Реализация автоматического развертывания Nginx средствами Puppet

Цель выпускной квалификационной работы - реализовать автоматизацию решения задач администрирования в сетях Linux при помощи кросс-платформенного клиент - серверного приложения Puppet.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

1 Puppet. Puppet является клиент-серверным приложением, в качестве клиентов выступают сервера или рабочие станции, на которых необходимо произвести развертывание либо конфигурирование каких либо программных средств. Puppet собирает информацию с клиентов при помощи утилиты `facter` - таким образом он получает специфичные значения конкретной машины и заносит их как переменные. После получения фактов от клиента Puppet-master компилирует каталог (список изменений, который должен быть выполнен на клиенте). После выполнения всех необходимых действий клиент отправляет серверу отчет о том, что было сделано[2].

2 IPTables. Проект `netfilter/iptables` был основан в 1998. Автором является Расти Расселл (`en:Rusty Russell`); он же автор проекта-предшественника `ipchains`. По мере развития проекта, в 1999 г. образовалась команда `Netfilter Core Team` (сокращено `coreteam`). Разработанный межсетевой экран получил официальное название `netfilter`. В марте 2000 г. был включен в ядро Linux 2.3. В августе 2003 руководителем `coreteam` стал Харальд Вельте (`Harald Welte`). В 2004 г. В системе `netfilter` пакеты пропускаются через цепочки. Цепочка является упорядоченным списком правил, а каждое правило может содержать критерии и действие или переход. Когда пакет проходит через цепочку, система `netfilter` по очереди проверяет, соответствует ли пакет всем критериям очередного правила, и если так, то выполняет действие (если критериев в правиле нет, то действие выполняется для всех пакетов, проходящих через правило). Вариантов возможных критериев очень много.

3 OpenVPN. При появлении в организации сорудников, работающих удаленно возникает необходимость обеспечения им защищенного доступа к различным корпоративным ресурсам. По соображениям безопасности доступ к этим ресурсам ограничен при помощи межсетевого экрана

(файервола) по портам и адресам IP. Ежедневную перенастройку доступа при изменении динамических IP сотрудников едва ли можно назвать разумным решением. Выход — это использование технологии виртуальных частных сетей Virtual Private Network (VPN) и ее свободной реализации OpenVPN. Эта реализация доступна практически для всех распространенных платформ, в том числе для планшетов и смартфонов. История развития OpenVPN насчитывает уже 12 лет (компания OpenVPN Technologies, Inc. была создана Francis Dinha и James Yona в 2002 году), так что это надежное и проверенное временем решение[10]. Для обеспечения безопасности управляющего канала и потока данных OpenVPN использует библиотеку OpenSSL. Это позволяет задействовать весь набор алгоритмов шифрования, доступных в данной библиотеке. Также может использоваться пакетная авторизация HMAC, для обеспечения большей безопасности, и аппаратное ускорение для улучшения производительности шифрования. Эта библиотека использует OpenSSL, а точнее протоколы SSLv3/TLSv1. OpenVPN используется в операционных системах Solaris, OpenBSD, FreeBSD, NetBSD, GNU/Linux, Apple Mac OS X, QNX, Microsoft Windows, Android.

4 HAProxy это бесплатное, очень быстрое и надёжное решение, предлагающее высокую доступность и балансировку нагрузки для TCP и HTTP-приложений, посредством распределения входящих запросов на несколько обслуживающих серверов. Программа написана на C и имеет репутацию быстрого, эффективного (в плане использования процессора и оперативной памяти) и стабильного решения. Её основная задача - повышение производительности серверной среды путем распределения рабочей нагрузки среди нескольких серверов (web, приложения, базы данных). HAProxy используется в ряде высоконагруженных веб-сайтов, включая Twitter, Instagram Github, Stack Overflow, Reddit, Tumblr и OpsWorks product из Amazon Web Services, W3C (W3C Validator), а также является составной частью облачной платформы Red Hat OpenShift и

балансировщиком по умолчанию в облачной платформе OpenStack. HAProxy является программой с открытым исходным кодом и распространяется в соответствии с GNU General Public License (GNU GPL v2). Производительность HAProxy: 2007 год - Типичные 1U сервера оснащённые двухъядерным процессором Opteron или Xeon обычно достигали производительности от 15 000 до 40 000 запросов/сек и не имели проблем с обслуживанием потока до 2 Гбит/с под ОС Linux. 2014 год - 1U сервера оснащённые Xeon E5 (2014 года) и 10 Гбит/с сетевой картой без проблем обрабатывают поток 40—60 Гбит/с, при этом подчёркивается, что ограничивающим фактором является пропускная способность сетевой карты. Даже на процессоре Intel Atom 1,6 ГГц (без воздушного охлаждения) HAProxy удалось обрабатывать поток до 1 Гбит/с. Расход памяти: 1 Гб ОЗУ хватает для обслуживания ~20 000—30 000 сессий.

5 nginx [engine x] — это HTTP-сервер и обратный прокси-сервер, почтовый прокси-сервер, а также TCP прокси-сервер общего назначения, изначально написанный Игорем Сысоевым. Уже длительное время он обслуживает серверы многих высоконагруженных российских сайтов, таких как Яндекс, Mail.Ru, ВКонтакте и Рамблер. Согласно статистике Netcraft nginx обслуживал или проксировал 21.43% самых нагруженных сайтов в апреле 2015 года. Вот некоторые примеры успешного внедрения nginx (тексты на английском языке): Netflix, Wordpress.com, FastMail.FM. У nginx есть один главный и несколько рабочих процессов. Основная задача главного процесса — чтение и проверка конфигурации и управление рабочими процессами. Рабочие процессы выполняют фактическую обработку запросов. nginx использует модель, основанную на событиях, и зависящие от операционной системы механизмы для эффективного распределения запросов между рабочими процессами. Количество рабочих процессов задаётся в конфигурационном файле и может быть фиксированным для данной конфигурации или автоматически

устанавливаться равным числу доступных процессорных ядер[6]. Как работают nginx и его модули, определяется в конфигурационном файле. По умолчанию, конфигурационный файл называется nginx.conf и расположен в каталоге /usr/local/nginx/conf, /etc/nginx или /usr/local/etc/nginx.

ЗАКЛЮЧЕНИЕ

В процессе написания выпускной квалификационной работы были решены следующие задачи:

- 1 Рассмотрен и изучен Puppet — приложения для автоматизации
- 2 Рассмотрено и изучено приложение HAProxy — балансировщик нагрузки
- 3 Рассмотрен и изучен Iptables — фаерволл
- 4 Рассмотрен и изучен NGinx — веб-сервер
- 5 Рассмотрен и изучен OpenVPN — клиент для построения частных сетей
- 6 Развернут тестовый стенд из 3х виртуальных машин, одна из которых является puppet-master'ом, оставшиеся 2 - клиенты
- 7 Реализована автоматическая установка вышеописанных приложений
 - а. 8. Реализовано централизованное конфигурирование виртуальных машин - клиентов

В различных организациях часто используются какие либо приложения из рассмотренных в работе, зачастую не одно. Результатом работы является получение модели организации, в которой реализована задача автоматизации поддержки и администрирования ИТ - инфраструктуры.

В ходе работы были получены следующие выводы:

- 1 Применение Puppet позволяет централизованно управлять конфигурацией серверов и их развертыванием, затрачивая на это минимально возможный временной интервал
- 2 Применение HAProxy повышает отказоустойчивость сервисов
- 3 Применение Iptables решает задачу сетевой безопасности компании
- 4 Применение OpenVPN решает задачу безопасного удаленного доступа к внутренним ресурсам компании

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

- 1 CyberForum [Электронный ресурс] / Powered by vBulletin® Version 3.8.7 PL3 Copyright ; vBulletin Solutions, Inc., некоммерческая организация. vBulletin®, 2000-. URL: <http://www.cyberforum.ru/> (дата обращения: 12.05.2015). Загл. с экрана. Последнее изменение страницы: 18:55, 30 апреля 2013 года. Яз. рус.
- 2 Хабрахабр [Электронный ресурс] / Руководство по установке и настройке OpenVPN / Хабрахабр (1/2) URL : <http://habrahabr.ru> Загл. с экрана. Последнее изменение страницы: 28 октября 2014 года. Яз. рус.
- 3 Википедия [Электронный ресурс] / Netfilter URL : <http://ru.wikipedia.org> Загл. с экрана. Последнее изменение страницы 30 ноября 2014 года. Яз. рус.
- 4 Википедия [Электронный ресурс] / Iptables URL : <http://ru.wikipedia.org> Загл. с экрана. Последнее изменение страницы 12 сентября 2011 года. Яз. рус.
- 5 otdocs.ru [Электронный ресурс] / Обзор возможностей веб-сервера Nginx URL : <http://otdocs.ru> Загл. с экрана. Последнее изменение страницы 30 марта 2016 года. Яз. рус.
- 6 Википедия [Электронный ресурс] / OpenVPN URL : <http://ru.wikipedia.org> Загл. с экрана. Последнее изменение страницы 12 декабря 2011 года. Яз. рус.
- 7 Хабрахабр [Электронный ресурс] / Топики / Избранное / Хабрацентр им. mblp / Хабрахабр URL : <http://habrahabr.ru> Загл. с экрана. Последнее изменение страницы 28 октября 2014. Яз. рус.
- 8 Википедия [Электронный ресурс] / HAProxy URL : <http://ru.wikipedia.org> Загл. с экрана. Последнее изменение страницы 01 декабря 2014. Яз. рус.

- 9 Хабрахабр [Электронный ресурс] /Puppet под нагрузкой / Блог компании Vadoo / Хабрахабр URL : <http://habrahabr.ru> Загл. с экрана. Последнее изменение страницы 28 октября 2014. Яз. рус.
- 10 dic.academic.ru [Электронный ресурс] Puppet URL : <http://dic.academic.ru> Загл. с экрана. Последнее изменение страницы 15 марта 2014. Яз. рус.
- 11 Википедия [Электронный ресурс] / Puppet URL : <http://ru.wikipedia.org> Загл. с экрана. Последнее изменение страницы 30 ноября 2014. Яз. рус.
- 12 <http://savepearlharbor.com> [Электронный ресурс] / Балансировка mysql | SavePearlHarbor URL : <http://savepearlharbor.com> Загл. с экрана. Последнее изменение страницы 12 апреля 2016. Яз. рус.
- 13 Хабрахабр [Электронный ресурс] / Как стать кукловодом или Puppet для начинающих / Хабрахабр URL : <http://habrahabr.ru> Загл. с экрана. Последнее изменение страницы 28 октября 2014. Яз. рус.
- 14 Георгий Курячий Кирилл Маслинский Операционная система Linux: Курс лекций. Учебное пособие / Г. В .Курячий, К. А. Маслинский — М. : ALT Linux; Издательство ДМК Пресс, 2010. — 348 с.