МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

**САНКТ-ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ
ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ**

В.А. Костеж
С.М. Платунова

Серверные технологии в вычислительных сетях Microsoft Windows Server® 2008.

Учебное пособие

Санкт-Петербург

2012

Костеж В.А., Платунова С.М. Серверные технологии в вычислительных сетях Microsoft Windows Server® 2008 – СПб: НИУ ИТМО, 2012. – 88 с.

В учебном пособии приводятся теоретические сведения, дополняющие материал лекций. Материал учебного пособия рекомендовано использовать во время самостоятельной работы над темой серверных технологий в гетерогенных вычислительных сетях. Материал необходимо дополнять сведениями из справочной системы конкретной версией сетевой операционной системы.

Пособие адресовано специалистам с высшим и средним профессиональным образованием, имеющим опыт работы в области IT технологий, обучающихся по направлению 230100 Информатика и вычислительная техника.

Рекомендовано к печати… Ученым советом факультета Академии ЛИМТУ, протокол № 6 от 23.12.2011

В 2009 году Университет стал победителем многоэтапного конкурса, в результате которого определены 12 ведущих университетов России, которым присвоена категория «Национальный исследовательский университет». Министерством образования и науки Российской Федерации была утверждена программа его развития на 2009–2018 годы. В 2011 году Университет получил наименование «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики»

СОДЕРЖАНИЕ

Введение

Учебно-методическое пособие предназначено для изучения основ Серверных технологий в вычислительных сетях на базе MS Windows Server® 2008. В нем содержится описание основных возможностей применения серверные технологии в вычислительных сетях, которые излагаются в виде теоретического материала и практических примеров.

Пособие следует использовать в качестве материалов для работы на аудиторных занятиях, а также в качестве справочного материала при выполнении самостоятельной работы.

Тема 1. Основы серверных технологий в вычислительных сетях

Классификация сетевых операционных систем, назначение и особенности архитектуры

Под вычислительной сетью будем понимать вычислительную сеть, в состав которой входят сетевые операционные системы.

В вычислительных сетях используются сетевые операционные системы, то есть операционные системы, способные осуществлять функции обмены информацией на основе принципов модели OSI.

Для классификации сетевых операционных систем существуют различные варианты критериев. Одним из вариантов критериев является – уровень и особенности реализации серверных решений.

Серверные решения – аппаратно-программный комплекс, адаптированный под выполнение компьютером функций сервера и содержащие в своем составе комплект программ для реализации соответствующего набора сервисов.

В данном Учебно-методическом пособии проведем классификацию сетевых операционных систем преимущественно по критериям производителей.

Microsoft Windows Server® 2008

Windows Server 2008® включает вариант Server Core, без оболочки Windows Explorer. Настройки выполняется

- при помощи интерфейса командной строки Windows,
- удалённо, подключением к серверу посредством Консоли управления.

Службы Active Directory интегрированы с традиционными протоколами, позволяют администратору централизованно настраивать

- параметры систем,

- учетные записи пользователей,
- приложения.

Доменные службы Active Directory (AD DS)

- хранят данные каталогов,
- управляют взаимодействием между пользователями и доменами,
- контролируют вход в домен,
- управляют процессом проверки подлинности,
- осуществляют поиск в каталоге,
- за счет интегрированных ролей поддерживают средства и технологии управления удостоверениями и доступом,
- позволяют централизованно управлять технологиями и учетными данными и предоставлять доступ к устройствам, приложениям и данным только уполномоченным пользователям.

Microsoft Windows Server® 2008 R2

Усовершенствованная версия Windows Server 2008, доступная только в 64-разрядном варианте.

Windows Server® 2008 R2 использует ядро Windows NT 6.1.

Отдельные особенности:

- улучшенная виртуализация;
- обновленная версия Active Directory;
- Internet Information Services 7.5.

Поддержка виртуализации осуществляется на базе компонентов:

- программы Live Migration,
- комплекса программ Cluster Shared Volumes (Failover Clustering),
- комплекса программ Hyper-V.

Обновленная версия Active Directory поддерживает функцию Корзина для удалённых объектов Active Directory.

В Internet Information Services 7.5:

- новый сервер FTP,
- расширения безопасности DNS,
- DirectAccess.

Windows Server® 2008 R2:

- содержит в своем составе Windows PowerShell 2.0;
- имеет возможность удаления GUI после установки;
- поддерживает iSCSI.

Классификацию Unix – систем можно провести по нескольким критериям, в первую очередь по назначению.

- Предустановленные в программно – аппаратные комплексы. Работают на специализированных аппаратных средствах. В этих

случаях сборка ядра осуществляется с целью минимизации потребляемых ресурсов.

- Операционные системы для специализированных серверов («тяжелых» серверов).

Для решения задач повышенной сложности создаются специализированные компьютеры со специализированными операционными системами с качественно улучшенной производительностью, скоростью обмена между элементами системы и устойчивость рабочих процессов.

Фирмы – производители: IBM, HP, Sun и другие. На подобных серверах осуществляется поддержка Unix – систем в качестве операционной среды. Для этих целей пользуются популярностью, в частности, 32- и 64-разрядные Red Hat Enterprise Linux и SUSE Enterprise Linux (Server и Advanced Server), Solaris (для Sun серверов).

- Операционные системы для серверов уровня ЛВС.

Для решения задач предоставления по сети ЛВС сервисов клиентским системам. Стабильность работы, безопасность и производительность – сильные стороны Unix – систем в указанной функциональной нише.

- Операционные системы для домашних компьютеров и решения офисных задач.

Для указанного класса задач важны удобный пользовательский интерфейс и поддержка заданного круга внешних устройств.

Для решения задач документооборота используют, в частности, пакет OpenOffice.org.

К особенностям архитектуры Unix-подобных операционных систем можно отнести следующее:

- многопользовательская сетевая операционная система,
- сетевая оконная графическая система X Window System,
- поддержка стандартов открытых систем,
- поддержка протоколов сети Internet,
- совместимость с файловыми системами DOS, MS Windows и другими,
- поддержка широкого круга аппаратных средств,
- возможность увеличения быстродействия за счет удаления части программных средств, в частности, графической оболочки,
- относительно малое количество созданных вирусов,
- возможность по ряду протоколов интегрироваться в локальные и глобальные сети с операционной средой,
- позволяет выполнять с использованием дополнительного программного обеспечения прикладные программы других ОС,
- обеспечивает использование дополнительных программных пакетов.

К активно распространяемым версиям Unix - подобных операционные системы можно отнести следующие.

- ALT Linux. Семейство операционных систем, включающий в себя подготовленные к эксплуатации программные решения для серверов и рабочих станций. Наиболее популярны:

ALT Linux 4.0 Desktop Professional (Сертифицирован ФСТЭК),
ALT Linux 4.0 Server Edition (сертификат ФСТЭК России),
ALT Linux 4.0 Server.

- ASPLinux. Предусмотрена возможность выбора варианта установки и использовать операционную систему в качестве:

- серверной платформы,
- офисной рабочей станции,
- мультимедийного домашнего компьютера.

Наиболее популярны:
ASPLinux 12 Carbon (обновления) (1DVD),
ASPLinux 12 Deluxe (BOX),
ASPLinux 12 Standard (BOX),
ASPLinux 12 Greenhorn (DVD),
ASPLinux 12 Express (DVD).

- CentOS. Основан на коммерческом Red Hat Enterprise Linux от компании Red Hat, и совместимый с ним.

CentOS используют исходный код Red Hat Enterprise Linux для создания клона.

CentOS использует up2date и Yellow Dog Updater Modified (yum) для скачивания и установки обновлений с репозитария CentOS Mirror Network (Red Hat Enterprise Linux и Fedora Core получают обновления с серверов Red Hat Network).

Наиболее популярны:
CentOS 5.4 для платформы i386 (1DVD)
CentOS 5.3 BOX

- Debian. Разработчики имеют опубликованные точные критерии качества программного обеспечения. Репутация самого надежного дистрибутива Linux в области использования на критически важных задачах, в качестве Internet-сервера.

Наиболее популярны:
Debian GNU/Linux 5.0r3 для платформы i386 (5DVD),
SimplyMEPIS 8.0 для платформы x86 (1CD),
Knoppix 5.3.1 (1DVD).

- Fedora. Создание спонсируется фирмой Red Hat. Проект служит для тестирования новых технологий, которые в дальнейшем включаются в продукты Red Hat.

Наиболее популярны:
Russian Fedora 11 (DVD-BOX)

Russian Fedora 11 для платформы i386 (1DVD)
Fedora 11 для платформы i386 (1DVD)

- FreeBSD. Система для построения сетевых серверов и сервисов. Предоставляет надёжные сетевые службы.

Наиболее популярны:
DragonFlyBSD 2.4 (1DVD + 2CD)
FreeBSD 7.2 для платформы i386 (1DVD)
FreeBSD 6.4 для платформы i386 (4DVD)
PC-BSD 7.0.2 для платформы i386 (1DVD)
Frenzy 1.1 (LiveCD)
FreeBSD 6.4 для платформы i386 (1DVD)
FreeSBIE 2.0 x86 (1 LIVE CD)

- Mandriva. Система предназначена для создания офисных рабочих станций и серверов.

Часть дистрибутивов сертифицированы ФСТЭК России:

- по 5 классу для СВТ («Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992),

- по 4 уровню контроля НДВ («Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999).

Сертифицированное ФСТЭК программное обеспечение рекомендуется к использованию государственными организациями, а также организациями, работающими с персональными данными граждан.

Наиболее популярны:
Mandriva One 2010 KDE (1CD)
Mandriva Free 2010 для платформы i586 (1DVD)
Mandriva 2009.1 Spring PowerPack (DVD-Box)

- RedHat.

Серверные версии:

Red Hat Enterprise Linux Advanced Platform - система для наиболее важных и критичных к времени простоя серверов. В Advanced Platform входят кластерные компоненты (Cluster Suite и GFS), адаптированные для работы в виртуальном окружении.

Red Hat Enterprise Linux - система для небольших серверов. Число одновременно запущенных гостевых систем ограничено четырьмя.

Клиентские версии:

Red Hat Enterprise Desktop - система для клиентских рабочих мест. Поддерживает системы с 1 процессором и 4 Gb оперативной памяти.

- SUSE. Ориентированы на персональные и сетевые компьютеры.

Наиболее популярны:

SUSE Linux Enterprise Server 11 для платформы i386 (2DVD)
SUSE Linux Enterprise Desktop 11 для платформы i386 (1DVD)
OpenSUSE 11.1 для платформы i586 (1DVD + 1CD)
OpenSUSE 11.0 (Box)

- Ubuntu. Поставляется с последними версиями GNOME и подборкой программного обеспечения для серверов и рабочих станций.

Наиболее популярны:
Ubuntu Server 9.10 (DVD-Box)
Ubuntu 9.10 (DVD-Box)
Ubuntu 9.10 для платформы i386 (1DVD)
Linux Mint 7 для платформы x86(1DVD)
Ubuntu Studio 8.10 для платформы x86 (1DVD)

Требования к аппаратным средствам ПК

Типичные требования к аппаратным средствам ПК.
FreeBSD 7.2 для платформы i386.
CPU: проц.Intel или AMD
HDD: 3GB минимум
RAM: 256 -минимум, 512-рекомендуется
Видео карты: NVIDIA,ATI, Intel i8xx и i9xx, SIS, Matrox, VIA
для 3D-decktop требуется наличие NVIDIA GeForce или более новых, ATIRadion 7000 или более новых
Звуковая карта: Sound Blaster-совместимые и AC97
Mandriva 2009.1 Spring PowerPack.
Любой процессор Intel®, AMD или VIA
Минимум 512Мб оперативной памяти, рекомендовано - 1Гб
Место на жестком диске: минимум 2 Гб, для полной установки рекомендуется 16 Гб,
Видеокарта: nVidia, ATI, Intel, SiS, Matrox, VIA.
Для 3-D стола - видеокарта с поддержкой аппаратного 3D-ускорения.
Звуковая карта — совместима с Sound Blaster, AC97 или HDA. Карты Creative Labs X-Fi пока не поддерживаются.
SATA, IDE, SCSI, SAS: большая часть контроллеров поддерживаются при отключении RAID, некоторые - с поддержкой RAID.

Лицензионные соглашения

Распространенной лицензией на свободной программное обеспечение является лицензия GPL (General Public License) созданная в рамках проекта GNU.

Основными идеями этой лицензии является:

- свобода использования программного обеспечение в любых целях,
- свобода изменять программное обеспечения в соответствии со своими потребностями (модификации исходных кодов),
- свобода распространения в исходном или модифицированном виде,
- запрещается закрытие исходных кодов после их модификации.

Создано несколько версий GPL (v1, v2,v3), а так же модификаций, главной попыткой которых было более четко определить рамки использования GPL в связке с другими лицензиями, а так же распространяемыми под ними продуктами.

Различные части дистрибутива программного обеспечения могут находиться под действием различных лицензий.

Юридическую силу имеют только документы, написанные на русском языке, оригинал GPL в нашей стране не действителен.

Если дистрибутив был приобретен в виде коробочной версии продукта или в составе программно-аппаратного комплекса, то рекомендуется сохранение сопутствующих документов и чека, подтверждающего факт купли продажи.

Достаточным подтверждением легальности использования программ для ПК считается заключённое лицензионное соглашение между правообладателем и пользователем. Дополнительно могут быть использованы счета, накладные, акты, документы, подтверждающие проведение платежа за ПО.

Ответственность за использование контрафактного софта

Программы и базы данных охраняются авторским правом (IV часть Гражданского кодекса РФ), программы для ПК охраняются как литературные произведения.

Автору принадлежат право авторства, право на имя, право на неприкосновенность произведения и иные личные неимущественные права, предусмотренные IV частью ГК РФ.

Исключительное право на программу может принадлежать как автору, так и иным гражданам и юридическим лицам. Обладатель исключительного права вправе использовать программу для ПК любым, не противоречащим законом способом, может распоряжаться программой по своему усмотрению, а также запрещать использование программы другим лицам, причем отсутствие запрета не является разрешением.

Использование программы без разрешения правообладателя (обладателя исключительных прав) является незаконным и влечет ответственность (гражданско-правовую, административную и уголовную).

Субъектами защиты исключительных прав признаются как сами правообладатели, так и лицензиаты - обладатели исключительных

лицензий на право пользования результатами интеллектуальной деятельности (ст.1254 ГК РФ)

Гражданско-правовая ответственность за использование контрафактного софта.

Участниками отношений, регулируемых гражданским законодательством (в том числе IV частью ГК) являются граждане и юридические лица. Гражданское законодательство регулирует отношения между лицами, осуществляющими предпринимательскую деятельность.

Гражданское законодательство предусматривает равенство, автономию воли и имущественную самостоятельность участников и не применяется к административным и иным властным отношениям.

Гражданско-правовая ответственность возникает в случае:

- когда правообладатель воспользовался установленными гражданским законодательством способами защиты своих прав,
- суд вынес решение в соответствии с требованиями правообладателя.

Административная ответственность за использование контрафактного софта

Для привлечения лица к административной ответственности необходима цель совершенного нарушения - извлечение дохода. Признак наличия цели извлечения доходов присутствует в том случае, если программы для ПК используются в коммерческой деятельности организации.

Необходимо учитывать, что юридические лица - коммерческие организации, согласно ст. 50 ГК РФ, основной целью своей деятельности имеют извлечение прибыли. Функционирование всех их подразделений, в конечном счете, ориентировано на извлечение прибыли, дохода.

К административной ответственности привлекаются не только граждане и юридические лица, но также и должностные лица.

Должностными лицами коммерческой организации признаются руководители и иные лица, выполняющие организационно-распорядительные или административно-хозяйственные функции. В каждом конкретном случае при привлечении к административной ответственности круг лиц устанавливается исходя из должностных инструкций и иных внутренних документов организации (приказов, доверенностей и т.п.).

Административная ответственность наступает при наличии умысла у нарушителя.

Юридическое лицо признается виновным в совершении административного правонарушения, если будет установлено, что у него имелись возможность для соблюдения правил и норм, за нарушение которых предусмотрена административная ответственность, но данным лицом не были приняты все зависящие от него меры по их соблюдению.

Дела могут возбуждаться как по заявлениям и сообщениям граждан и организаций, так и в результате обнаружения признаков правонарушения непосредственно работниками правоохранительных органов.

Уголовная ответственность за использование контрафактного софта.

Уголовная ответственность наступает только при наличии вины правонарушителя. К уголовной ответственности может быть привлечено только физическое лицо.

При нарушении авторских прав юридическим лицом уголовной ответственности может подлежать руководитель и иное ответственное лицо в зависимости от обстоятельств дела (например, системный администратор).

Первая часть ст.146 УК РФ предусматривает ответственность за деяния, в первую очередь посягающие на личные неимущественные права автора, в частности таким деянием может являться

- объявление себя автором чужого произведения,
- выпуск чужого произведения под своим именем,
- издание под своим именем произведения созданного в соавторстве без указания имен других авторов.

Вторая часть ст.146 УК РФ предусматривает ответственность за нарушение исключительных прав, в том числе приобретение, хранение, перевозка контрафактных экземпляров произведений с целью сбыта и совершенные в крупном размере.

Авторские права иностранных граждан и юридических лиц охраняются наравне с авторскими правами физических и юридических лиц в силу международных договоров или на основании принципа взаимности.

Организация вычислительной сети

На аппаратном уровне организация гетерогенной вычислительной сети осуществляется по стандартным процедурам и правилам.

На программном уровне предполагается сочетание разнородных операционных систем.

Наиболее типичные варианты:

1. Рабочие станции оснащены операционными системами типа Windows XX и Unix-подобными. В этом случае могут возникнуть проблемы сетевого взаимодействия с использованием протоколов различных уровней.
2. Существует сервер LDAP на базе соответствующего серверного варианта операционной системы Windows. Часть рабочих станций оснащены Unix-подобными операционными системами. В этом случае могут возникнуть проблемы корректного взаимоотношения внутри домена.

Контрольные вопросы

1. Основные особенности вычислительных сетей?
2. Программные средства вычислительных сетей?
3. Основные производители программных средств гетерогенных вычислительных сетей?
4. Классификация операционных систем Windows XX, используемых в вычислительных сетях?
5. Критерии классификации Unix-подобных операционных систем?
6. Области применения операционных систем Windows XX и Unix-подобных в вычислительных сетях?
7. Особенности архитектуры операционных систем вычислительных сетей?
8. Версии операционных систем вычислительных сетей?
9. Типичные требования к аппаратным средствам ПК операционных систем вычислительных сетей?
10. Особенности лицензирования операционных систем вычислительных сетей?

Тема 2. Инструментальные средства работы

Особенности интерфейса CLI

В Unix-подобных операционных системах в режиме без графической оболочки (режим CLI интерфейса) система запросит ввод логина сразу после завершения стартовых скриптов.

Как правило, загружается первая консоль – терминал.

В Unix-подобных операционных системах, вход конкретного пользователя в систему на конкретном терминале предопределяет для данного терминала права по запуску программ. У каждого пользователя есть уникальное имя (логин) и, при необходимости, пароль (при вводе пароля символы не отображаются).

В Unix-подобных операционных системах может быть несколько виртуальных консолей.

Для переключения между консолями зарезервированы специальные комбинации клавиш, например, Alt-F#.

При переключении от одной консоли к другой, происходит сохранение и восстановление вывода на экран. Программы, запускаемые на одной виртуальной консоли, не прекращают выполнение, при переключении на другую консоль.

Пример.

В конфигурации по умолчанию FreeBSD запускает восемь виртуальных консолей. Число и параметры виртуальных консолей задаются в файле /etc/ttys.

Вы можете использовать это файл для настройки виртуальных консолей FreeBSD. Любая не закомментированная строка в этом файле (строка, не начинающаяся с символа #), содержит настройки для одного терминала или виртуальной консоли.

Версия этого файла по умолчанию, поставляемая с FreeBSD, содержит настройки для девяти виртуальных консолей и включает восемь терминалов. Это строки, начинающиеся с ttyv.

За детальным описанием каждой колонки этого файла и всех опций, которые можно указать для настройки виртуальных консолей, обращайтесь к справочной странице ttys(5).

Особенности интерфейса GUI

В режиме GUI могут использоваться различные графические оболочки от простых менеджеров окон до интегрированных графических сред, типа KDE или GNOME.

В GNOME имеется

- панель (для запуска приложений и отображения их состояния),
- рабочий стол (где могут быть размещены данные и приложения),
- набор стандартных инструментов и приложений для рабочего стола,
- набор соглашений, облегчающих совместную работу и согласованность приложений.

KDE является простой в использовании графической оболочкой.

Совместно с KDE поставляется веб-браузер под названием Konqueror, который является в большинстве версий файловым менеджером.

Интерпретатор команд для текстового режима называют оболочкой (Shell).

Наиболее известные из них: sh, bash.

Оболочка bash использует несколько символов из числа 256 символов набора ASCII в специальных целях, либо для обозначения некоторых операций, либо для преобразования выражений.

В число таких символов входят символы:

` ~ ! @ # $ % ^ & * ( ) _ — [ ] { } : ; ' " / \ > <

а также символ с кодом 0, символ возврата каретки (генерируемый клавишей <Enter>) и пробел.

Символ \ (обратный слэш) можно назвать "символом отмены специального значения" для любого из специальных символов, который стоит сразу вслед за \.

Символы ' и " (одинарные и двойные кавычки) могут быть названы "символами цитирования". Любой из этих символов всегда используется в паре с его копией для обрамления какого-то выражения, совсем как в обычной прямой речи. Если какой-то текст взят в одинарные кавычки, то все символы внутри этих кавычек воспринимаются как литералы, никаким из них не придается специального значения.

Различие в использовании символов ' и " состоит в том, что внутри одинарных кавычек теряют специальное значение все символы, а внутри двойных кавычек - все специальные символы кроме $, ' и \ (знака доллара, одинарных кавычек и обратного слэша).

Оболочка предоставляет пользователю два специальных оператора для организации задания команд в командной строке: ; и &.

Оператор ;

Пользователь задает команды в командной строке по одной, имеется возможность задать в одной строке несколько команд, которые будут выполнены последовательно, одна за другой. Для этого используется специальный символ - оператор ;. Если не поставить этот разделитель команд, то последующая команда может быть воспринята как аргумент предыдущей.

Оператор & используется для того, чтобы организовать исполнение команд в фоновом режиме. Если поставить значок & после команды, то оболочка вернет управление пользователю сразу после запуска команды, не дожидаясь, пока выполнение команды завершится.

Команды бывают встроенные (код которых включен в код самой оболочки) и внешние (код которых расположен в отдельном файле на диске).

Для поиска внешней команды пользователь, в принципе, должен указать оболочке полный путь до соответствующего файла.

Когда программа запускается на выполнение, в ее распоряжение предоставляются три потока (или канала):

- стандартный ввод (standard input или stdin). По этому каналу данные передаются программе;
- стандартный вывод (standard output или stdout). По этому каналу программа выводит результаты своей работы;
- стандартный поток сообщений об ошибках (standard error или stderr). По этому каналу программы выдают информацию об ошибках.

По умолчанию входной поток связан с клавиатурой, а выходной поток и поток сообщений об ошибках направлены на терминал пользователя.

Использовать комбинацию клавиш <Ctrl>+<C> является в оболочке командой завершения работы запущенной программы.

Существуют специальные средства для перенаправления ввода/вывода.

Операторы >, < и >>

Для обозначения перенаправления используются символы ">", "<" и ">>". Чаще всего используется перенаправление вывода команды в файл.

Оператор > служит для перенаправления выходного потока. По отношению к входному потоку аналогичную функцию выполняет оператор <.

Особым вариантом перенаправления вывода является организация программного канала. Для этого две или несколько команд, таких, что вывод предыдущей служит вводом для следующей, соединяются символом вертикальной черты "|". При этом стандартный выходной поток команды, расположенной слева от символа |, направляется на стандартный ввод программы, расположенной справа от символа |.

Оболочка одновременно вызывает на выполнение все команды, включенные в конвейер, запуская для каждой из команд отдельный экземпляр оболочки. Каждая следующая команда выполняет свою операцию, ожидая данных от предыдущей команды и выдавая свои результаты на вход последующей.

Фильтры - это команды (или программы), которые воспринимают входной поток данных, производят над ним некоторые преобразования и выдают результат на стандартный вывод (откуда его можно перенаправить куда-то еще по желанию пользователя). К числу команд-фильтров относятся cat, more, less, wc, cmp, diff, grep, fgrep, egrep, tr, comm, pr, sed, поясним назначение некоторых из них.

grep, fgrep, egrep

Ищут во входном файле или данных со стандартного ввода строки, содержащие указанный шаблон, и выдают их на стандартный вывод

tr

Заменяет во входном потоке все встречающиеся символы, перечисленные в заданном перечне, на соответствующие символы из второго заданного перечня

comm

Сравнивает два файла по строкам и выдает на стандартный вывод 3 колонки: в одной— строки, которые встречаются только в 1 файле, во второй— строки, которые встречаются только во 2-ом файле: и в третьей— строки, имеющиеся в обоих файлах

pr

Форматирует для печати текстовый файл или содержимое стандартного ввода

sed

Строковый редактор, использующийся для выполнения некоторых преобразований над входным потоком данных.

tee

Направляет входной поток на стандартный вывод и в файл.

Параметры в оболочке. Именем (или идентификатором) параметра может быть слово, состоящее из алфавитных символов, цифр и знаков подчеркивания.

Параметр задан или установлен, если ему присвоено значение. Значением может быть и пустая строка. Чтобы вывести значение параметра, используют символ $ перед его именем.

Параметры разделяются на три класса:

- позиционные параметры,
- специальные параметры,
- переменные оболочки.

Имена (идентификаторы) позиционных параметров состоят из одной или более цифр.

Значениями позиционных параметров являются аргументы, которые были заданы при запуске оболочки.

Изменить значение позиционного параметра можно с помощью встроенной команды set. Значения этих параметров изменяются также на время выполнения оболочкой одной из функций.

Специальные параметры являются шаблонами с определенными правилами замены.

*

Заменяется позиционными параметрами, начиная с первого. Если замена производится внутри двойных кавычек, то этот параметр заменяется на одно единственное слово, составленное из всех позиционных параметров, разделенных первым символом специальной переменной IFS (о ней будет сказано ниже).

@

Заменяется позиционными параметрами, начиная с первого. Если замена производится внутри двойных кавычек, то каждый параметр заменяется отдельным словом.

#

Заменяется десятичным значением числа позиционных параметров

?

Заменяется статусом выхода последнего из выполнявшихся на переднем плане программных каналов

- (дефис)

Заменяется текущим набором значений флагов, установленных с помощью встроенной команды set или при запуске самой оболочки

$

Заменяется идентификатором процесса (PID) оболочки

!

Заменяется идентификатором процесса (PID) последней из выполняющихся фоновых (асинхронно выполнявшихся) команд

0

Заменяется именем оболочки или запускаемого скрипта.

_ (подчеркивание)

Заменяется последним аргументом предыдущей из выполнявшихся команд (если это параметр или переменная, то подставляется ее значение)

Переменная - это параметр, обозначаемый именем. Значения переменным присваиваются с помощью оператора =.

Если переменная задана, то ее можно удалить, используя встроенную команду оболочки unset.

Набор всех установленных переменных оболочки с присвоенными им значениями называется окружением (environment) или средой оболочки.

Переменная PS1 задает вид приглашения, которое выводится при ожидании ввода очередной команды пользователем.

Переменная PATH задает перечень путей к каталогам, в которых осуществляет поиск файлов в тех случаях, когда полный путь к файлу не задан в командной строке. Отдельные каталоги в этом перечне разделяются двоеточиями.

Для того, чтобы добавить каталог в этот список, нужно выполнить следующую команду:

PATH=$PATH:<имя нового каталога>.

При осуществлении поиска оболочка просматривает каталоги именно в том порядке, как они перечислены в переменной PATH.

Переменная IFS задает разделители полей (Internal Field Separator), которые используются при операции разделения слов при преобразованиях командной строки, выполняемых оболочкой перед тем, как запустить командную строку на исполнение.

Имя текущего каталога сохраняется в переменной окружения (с именем PWD), и значение этой переменной изменяется при каждом запуске программы cd.

Полное имя домашнего каталога пользователя, запустившего данный процесс, сохраняется в переменной HOME.

Оболочка, запуская на выполнение программу, передает часть переменных окружения.

Для того, чтобы переменная окружения передавалась запускаемому из оболочки процессу, ее нужно задавать с помощью специальной команды export.

Справочная система.

Важным источником информации является системный справочник (man).

Практически каждое приложение или утилита имеют соответствующую группу страниц, описывающую работу программы, опции и настройки.

Для просмотра этих страниц существует команда man:

man <команда или имя файла>

Команда или имя файла - это команда или имя конфигурационного файла, о которых необходимо получить информацию.

Содержимое системного справочника разделено на несколько разделов:

1. Пользовательские команды.
2. Системные вызовы и коды ошибок.
3. Функции стандартных библиотек.
4. Драйверы устройств.
5. Форматы файлов.
6. Развлечения и игры.
7. Дополнительная информация.
8. Команды системного администрирования.
9. Для разработчиков ядра.

В ряде случаев, необходимо явно указать раздел man, в котором нужно искать соответствующую страницу:

man <номер раздела> <команда или имя файла>

По традиции, в книгах и справках, конкретный раздел справочника указывается в скобках после команды.

При поиске команды по ключевым словам, встречающимся в ее описании, используя опции команды man.

В дополнение к страницам справочника, с программами может поставляться ипертекстовая документация в виде info файлов, которые могут быть просмотрены с помощью команды info.

Использование оболочек. Графический режим. Утилиты графических интерфейсов

KDE - графическая среда рабочего стола для UNIX-подобных операционных систем.

Построена на основе кросс-платформенного инструментария разработки пользовательского интерфейса Qt.

Работает преимущественно под UNIX-подобными операционными системами, которые используют графическую подсистему X Window.

В состав KDE входит набор интегрированных между собой программ, в том числе офисный пакет KOffice.

Стандартные пакеты

aRts — звуковой сервер (в KDE4 заменён на phonon).

kdelibs — основные библиотеки, требуются для сборки других пакетов.

kdepimlibs — библиотеки для PIM (для KDE4)

kdebase — рабочий стол и основные приложения.

kdeaccessibility — дополнительные программы для людей с ограниченными способностями (экранная лупа, синтезатор речи и т. д.).

kdeaddons — дополнительные модули и скрипты.

kdeadmin — инструменты графического администрирования.

kdeartwork — содержит дополнительные темы, экранные заставки, звуки, обои и различные стили оформления окон.

kdeedu — образовательное программное обеспечение.

kdegames — игры.

kdegraphics — ПО для работы с графикой.

kde-i18n — интернационализация; пакет для пользователей, которые хотят использовать в меню, справке и в приложениях языки, отличные от английского (в KDE4 заменён на kde-l10n).

kdemultimedia — ПО для работы с файлами (и устройствами) мультимедиа.

kdenetwork — инструменты для работы с сетью.

kdepim — персональный органайзер.

kdesdk — инструменты разработчика.

kdetoys — бесполезные «игрушки».

kdeutils — разнообразные утилиты.

kdeplasmoids — пакет дополнительных плазмойдов и тем plasma (для kde4.1)

kdewebdev — пакет программ для веб-разработчиков.

Основные программы:

Amarok — аудиоплеер;

Dolphin — файловый менеджер;

K3b — программа для записи CD- и DVD-дисков;

Konsole — эмулятор терминала;

Kontact — персональный информационный менеджер, включающий клиент электронной почты, адресную книгу, планирование задач, календарь, и многое другое;

Kopete — мультипротокольный клиент мгновенных сообщений;

Konqueror — веб-браузер, со множеством дополнительных возможностей;

KOffice — офисный пакет;

Gwenview — просмотрщик изображений;

Okular — универсальный просмотрщик файлов различных типов, в частности, PDF;

digiKam — программа для управления коллекциями фотографий;

KTorrent — Bittorrent-клиент;

Kdenlive — видеоредактор.

GNOME - графическая среда рабочего стола для Unix-подобных операционных систем.

В рамках проекта GNOME разрабатываются как приложения для конечных пользователей, так и набор инструментов для создания новых приложений, тесно интегрируемых в рабочую среду.

Файловый менеджер и панели

Файловый менеджер Nautilus обеспечивает отрисовку рабочего стола со значками на нём, а также работу с файлами и папками. Nautilus может работать в двух режимах: пространственном и режиме браузера.

В первом режиме каждая папка открывается в своём собственном окне, причём положение окон запоминается. Во втором режиме, перемещение по папкам производится в рамках одного окна, оснащённого панелями инструментов, деревом каталогов и другими элементами.

Программа GNOME Panel предоставляет панели для рабочего стола GNOME. По умолчанию GNOME имеет две панели, расположенные по верхнему и нижнему краям рабочего стола. Вместе с GNOME Panel поставляется набор апплетов — небольших приложений, которые встраиваются в панель для выполнения различных функций, например, отображения даты и времени, списка открытых окон или индикатора раскладки клавиатуры.

Основные приложения

GNOME Terminal — эмулятор терминала, предоставляющий доступ к командной оболочке UNIX для пользователя графической среды. GNOME Terminal поддерживает все типичные функции эмулятора терминала, а также цветной вывод и события от мыши.

gedit — текстовый редактор с поддержкой Юникода. Поддерживает использование вкладок для представления нескольких документов в одном окне, подсветку синтаксиса для ряда компьютерных языков, и другие возможности.

Приложение Yelp предназначено для просмотра документации, установленной в системе. Yelp позволяет просматривать как справку по приложениям GNOME, так и стандартные справочные материалы man и texinfo.

Evolution — приложение для управления электронной почтой, расписанием и адресной книгой.

Evolution поддерживает все основные почтовые протоколы.

Ekiga — приложение IP-телефонии и проведения видеоконференций.

Empathy — приложение мгновенного обмена сообщениями.

Totem — мультимедиа-проигрыватель среды GNOME.

Sound Juicer — приложение для извлечения звуковых дорожек с компакт-дисков.

Alacarte — редактор меню.

Brasero — программа для записи CD и DVD.

Bug Buddy — программа формирования и отправки отчётов об ошибках, возникающих в других приложениях GNOME.

Gconf-editor — программа редактирования настроек, хранящихся в GConf.

Gcalctool — калькулятор.

Gnome Games — набор игр.

GNOME Display Manager — дисплейный менеджер (графическая программа аутентификации пользователей среды).

GNOME Keyring Manager — программа управления конфиденциальными данными, хранящимися в зашифрованном виде в GNOME Keyring.

GNOME Screensaver — хранитель экрана.

GNOME System Monitor — монитор состояния системы.

Gucharmap — таблица символов Юникода.

File Roller — менеджер архивов.

Orca (итал.) — средство реабилитации (в том числе, экранный диктор).

Pessulus — программа для ограничения доступа к определённым функциям среды.

Sabayon — программа редактирования профилей пользователей (наборов настроек среды).

Seahorse — программа управления ключами шифрования.

Tomboy — программа создания заметок.

Vino — программа удалённого доступа к рабочему столу.

Графические утилиты администрирования

GNOME System Tools - комплект графических средств для администрирования UNIX-систем. В время в состав GNOME System Tools входят инструменты для настройки учётных записей пользователей системы, сетевых подключений, даты и времени, системных служб и общих сетевых ресурсов.

Контрольные вопросы

1. Варианты интерпретаторов команд?
2. Операторы организации задания команд?
3. Команды встроенные и внешние?
4. Потоки (канала) вводы/вывода?
5. Перенаправление ввода/вывода?
6. Команды - фильтры?

7. Классы параметров оболочки?
8. Изменение значений позиционного параметра?
9. Переменная PS1?
10. Переменная PATH?
11. Переменная HOME?
12. Особенности графического режима?
13. Особенности интерфейса Unix - подобных операционных систем?
14. Использование справочная система Unix - подобных операционных систем?

Тема 3. Файловые системы

Файловые системы содержатся в разделах.

Каждый раздел обозначается буквой от a до h (BSD) или цифрой (Linux). Каждый раздел может содержать только одну файловую систему.

Используется дисковое пространство под раздел подкачки (swap).

Корневой каталог обозначается символом "/".

Корневой каталог монтируется самым первым на этапе загрузки и содержит все необходимое, чтобы подготовить систему к загрузке в многопользовательский режим.

Корневой каталог также содержит точки монтирования всех других файловых систем.

Точкой монтирования называется каталог, который будет соответствовать корню смонтированной файловой системы.

Стандартные точки монтирования: /usr, /var, /tmp, /mnt и /cdrom.

В файле /etc/fstab указаны файловые системы и их точки монтирования. Большинство файловых систем, описанных в /etc/fstab, монтируются автоматически, если только для них не указана опция noauto.

Пример содержание основных директорий.

/ Корневой каталог файловой системы.

/bin Основные утилиты, необходимые для работы как в однопользовательском, так и в многопользовательском режимах.

/boot Программы и конфигурационные файлы, необходимые для нормальной загрузки операционной системы.

/boot/defaultsКонфигурационные файлы с настройками по умолчанию, используемые в процессе загрузки операционной системы.

/dev Файлы устройств.

/etc Основные конфигурационные файлы системы и скрипты.

/etc/defaults Основные конфигурационные файлы системы с настройками по умолчанию.

/etc/mail Конфигурационные файлы для систем обработки почты.
/etc/namedb Конфигурационные файлы для утилиты.
/etc/periodic Файлы сценариев, выполняемые ежедневно, еженедельно и ежемесячно.
/etc/ppp Конфигурационные файлы для утилиты ppp.
/mnt Пустой каталог, используемый системными администраторами как временная точка монтирования.
/proc Виртуальная файловая система, отображающая текущие процессы.
/rescue Статически собранные программы для восстановления после сбоев.
/root Домашний каталог пользователя root.
/sbin Системные утилиты и утилиты администрирования, необходимые для работы как в однопользовательском, так и в многопользовательском режимах.
/stand Программы, необходимые для работы в автономном режиме.
/tmp Временные файлы.
/usr Пользовательские утилиты и приложения.
/usr/bin Пользовательские утилиты и приложения общего назначения.
/usr/include Стандартные заголовочные файлы для языка C.
/usr/lib Файлы стандартных библиотек.
/usr/libdata Файлы данных для различных утилит.
/usr/libexec Системные утилиты.
/usr/local Локальные пользовательские приложения.
/usr/obj Архитектурно-зависимые файлы и каталоги, образующиеся в процессе сборки системы из исходных текстов в /usr/src.
/usr/ports Коллекция портов FreeBSD.
/usr/sbin Системные утилиты и утилиты администрирования (исполняемые пользователем).
/usr/share Архитектурно-независимые файлы.
/usr/src Исходные тексты программ.
/usr/X11R6 Утилиты, приложения и библиотеки X Window.
/var Файлы журналов.
/var/log Файлы системных журналов.
/var/mail Почтовые ящики пользователей.
/var/spool Файлы очередей печати, почты.
/var/tmp Временные файлы.

Монтирование файловых систем

Формат файла /etc/fstab, файловые системы перечисляются построчно:

- Имя устройства.

- Точка монтирования.
- Каталог (существующий), куда следует смонтировать файловую систему.
- Тип файловой системы.
- Опции. Значение опций в mount(8).
- Частота дампов. Утилита dump(8).
- Порядок проверки файловые системы.

Команда mount(8) используется для монтирования файловых систем.

mount <устройство> <точка-монтирования>

Примеры опций монтирования

-a Смонтировать все файловые системы, перечисленные в файле /etc/fstab. Исключение составляют помеченные как "noauto", перечисленные после опции -t и уже смонтированные.

-d Сделать все, кроме самого системного вызова mount. Эта опция полезна вместе с флагом -v для определения того, что на самом деле пытается сделать mount(8).

-f Монтировать поврежденный раздел (опасно!), или форсировать отмену всех запросов на запись при изменении режима монтирования с "чтение-запись" на "только чтение".

-r Монтировать файловую систему в режиме "только для чтения". То же самое, что и указание аргумента ro для опции -o.

-t <имя файловой системы> Монтировать файловую систему как систему указанного типа, или, в случае опции -a, только файловые системы данного типа.

-u Обновить опции монтирования для файловой системы.

-v Выдавать более подробную информацию.

-w Монтировать файловую систему в режиме "чтение-запись".

Команда umount(8) принимает в качестве параметра точку монтирования какой-либо файловой системы, имя устройства.

Права доступа

Многопользовательская среда предполагает наличие механизма регулирования прав доступа к любому ресурсу в системе.

Три типа прав доступа:

- чтение,
- запись,
- исполнение.

Права сгруппированы в три группы по три бита доступа.

Группы прав доступа:

- группа, определяющая права доступа для владельца элемента файловой системы,

- группа, определяющая права доступа для отдельной группы пользователей к элементу файловой системы,
- группа, определяющая права доступа для пользователей, не относящихся к первым двум группам.

Основные биты доступа:

- чтение,
- запись,
- выполнение.

Возможно численное представление сочетаний бит доступа:

0	Ничего не разрешено	---
1	Нельзя читать и писать, разрешено исполнять	--x
2	Нельзя читать и исполнять, разрешено писать	-w-
3	Нельзя читать, разрешено писать и исполнять	-wx
4	Разрешено читать, нельзя писать и исполнять	r--
5	Разрешено читать и исполнять, нельзя писать	r-x
6	Разрешено читать и писать, нельзя исполнять	rw-
7	Разрешено все	rwx

Для получения информации о правах на элементы файловой структуры используют команду ls(1) с опцией –l.

В выводимой информации первый символ обозначает тип элемента файловой системы (- файл, d директория, l ссылка…).

Следующие три символа задают права доступа для владельца элемента файловой системы.

Следующие три символа задают права доступа для отдельной группы пользователей к элементу файловой системы.

Следующие три символа задают права доступа для пользователей, не относящихся к первым двум группам к элементу файловой системы.

Каталоги также являются файлами. К ним применимы те же права на чтение, запись и выполнение. Для каталога бит исполнимый означает:

- можно зайти в каталог (с помощью команды cd),
- в данном каталоге можно получить доступ к файлам.

Если требуется получить список файлов в некотором каталоге, права доступа на него должные включать доступ на чтение. Для того, чтобы удалить из каталога какой-либо файл, имя которого известно, на этот каталог должны быть даны права на запись и на исполнение.

Существуют дополнительные права доступа, используемые в системных целях:

- setuid-бит на выполняемые файлы,
- sticky-бит на каталоги.

Символические обозначения в команде chmod, используют буквы для назначения прав на файлы и каталоги.

Символические выражения в команде chmod используют синтаксис (кто) (действие) (права), где существуют следующие значения:

(кто)	u	Пользователь (User)
(кто)	g	Группа (Group)
(кто)	o	Другие (Other)
(кто)	a	Все (All, "world")
(действие)	+	Добавление прав
(действие)	-	Удаление прав
(действие)	=	Явная установка прав
(права)	r	Чтение (Read)
(права)	w	Запись (Write)
(права)	x	Выполнение (Execute)
(права)	t	Sticky бит
(права)	s	SUID или SGID

Флаги обеспечивают дополнительный уровень защиты и контроля над файлами, но не могут применяться к каталогам.

Эти флаги добавляют дополнительные возможности контроля над файлами, обеспечивая (при определенных условиях) невозможность их удаления или изменения даже пользователю root.

Файловые флаги изменяются при помощи утилиты chflags(1) посредством простого интерфейса.

Некоторые флаги могут быть установлены или сняты с файлов только пользователем root. В остальных случаях эти флаги может установить владелец файла.

Дополнительные биты доступа setuid, setgid и sticky.

Реальный UID -- это идентификатор пользователя, запустившего процесс на выполнение. Действующий UID (EUID) -- это идентификатор пользователя, с которым выполняется процесс.

Бит setuid устанавливается добавлением цифры четыре перед численным представлением прав доступа. При наличии этого бита, в перечне прав доступа для владельца файла присутствует символ s, который заменил собой бит выполнения.

Бит setgid изменяет настройки прав для группы. При выполнении приложение с установленным битом setgid, то будут обеспечены права в соответствии с группой владельца файла, а не с группой пользователя, запустившего процесс. Чтобы установить на файл бит setgid, выполните команду chmod, добавив цифру два (2) перед численным представлением прав доступа. Бит отображается s в перечне прав доступа для группы:

Бит sticky, установленный на каталог, позволяет производить удаление файла только владельцу файла. Этот бит применяется для предотвращения удаления файлов в публичных каталогах, таких как /tmp, пользователями, не владеющими файлом. Добавление единицы (1) перед

численным представлением прав доступа. Отличительной особенностью бита sticky является наличие символа t в самом конце перечня прав.

Контрольные вопросы

1. Физическая организация файловой системы?
2. Логическая организация файловой системы?
3. Монтирование файловых систем?
4. Основные опции монтирования?
5. Основные биты доступа?
6. Символьное представление бит доступа?
7. Цифровое представление бит доступа?
8. Дополнительные биты доступа?
9. Изменение прав доступа?

Тема 4. Основы сетевого администрирования

Настройка карт сетевых интерфейсов

Сетевая карта должна определиться при загрузке.

Если драйвер вашей сетевой карты отсутствует, для ее использования потребуется загрузить подходящий драйвер.

Сетевая карта может быть настроена утилитами (например, sysinstall).

Для вывода информации о настройке сетевых интерфейсов системы используют команду ifconfig(8).

Для присвоения имени сетевой карте использует имя драйвера и порядковый номер, в котором карта обнаруживается при инициализации устройств.

Для настройки карты потребуются привилегии пользователя root. Настройка сетевой карты может быть выполнена из командной строки с помощью ifconfig(8) на сеанс.

Если вы настроили сетевую карту в процессе установки системы, некоторые строки, касающиеся сетевой карты, могут уже присутствовать в файлах конфигурации.

Как только вы внесены необходимые изменения необходимо перегрузите компьютер. Изменения настроек интерфейсов будут применены, кроме того будет проверена правильность настроек.

Как только система перезагрузится, проверьте сетевые интерфейсы.

Для проверки правильности настройки сетевой карты, попробуйте выполнить ping для самого интерфейса, а затем для другой машины в локальной сети.

Решение проблем с аппаратным и программным обеспечением всегда вызывает сложности, которые можно уменьшить, проверив сначала самые простые варианты:

- подключение сетевого кабеля,
- настройка сетевого сервиса,
- настройка брандмауэра,
- поддержка используемой сетевой карты.

Если карта работает, но производительность низка, может помочь чтение страницы справочника tuning(7). Проверьте также настройки сети, поскольку неправильные настройки могут стать причиной низкой скорости соединения.

Сообщение “No route to host” появляются, если система не в состоянии доставить пакеты к хосту назначения. Это может случиться, если не определен маршрут по умолчанию, или кабель не подключен. Проверьте вывод команды netstat -rn и убедитесь, что к соответствующему хосту есть работающий маршрут.

Сообщения “ping: sendto: Permission denied” зачастую появляются при неправильно настроенном брандмауэре. Если ipfw включен в ядре, но правила не определены, правило по умолчанию блокирует весь трафик, даже запросы ping.

Контрольные вопросы

1. Утилиты настройки сетевая карты?
2. Применение команды ifconfig?
3. Проверка сетевых настроек?
4. Использование команды ping?
5. Использование команды netstat -rn?

Тема 5. Настройка и администрирование серверов

Протокол передачи файлов (File Transfer Protocol, FTP) дает пользователям простой путь передачи файлов на и с FTP сервера.

Серверная программа FTP (ftpd), включена в базовую систему.

Наиболее важный шаг заключается в определении того, каким учетным записям будет позволено получать доступ к FTP серверу.

В обычной системе есть множество системных учетных записей, используемых различными даемонами, но пользователям должно быть запрещен вход с использованием этих учетных записей. В файле /etc/ftpusers находится список пользователей, которым запрещен доступ по FTP. По умолчанию он включает упомянутые системные учетные записи, но в него можно добавить и определенных пользователей, которым будет запрещен доступ по FTP.

Может понадобиться ограничить доступ определенных пользователей без полного запрета использования FTP. Это можно сделать через файл /etc/ftpchroot. В нем находится список пользователей и групп, к которым применяется ограничение доступа. На странице справочника ftpchroot(5) дана подробная информация.

Если вы захотите разрешить анонимный FTP доступ на сервер, в системе необходимо создать пользователя ftp.

Этот пользователь сможет входить на FTP сервер с именем пользователя ftp или anonymous, с любым паролем (существует соглашение об использовании почтового адреса пользователя в качестве пароля).

FTP сервер выполнит chroot(2) при входе пользователя anonymous для ограничения доступа только домашним каталогом пользователя ftp.

Существуют два текстовых файла, определяющих сообщение, отправляемое FTP клиентам. Содержимое файла /etc/ftpwelcome будет выведено пользователям перед приглашением на вход. После успешного входа будет выведено содержимое файла /etc/ftpmotd.

Путь к этому файлу задается относительно домашнего каталога пользователя, так что анонимным пользователям будет отправляться ~ftp/etc/ftpmotd.

Как только FTP сервер правильно настроен, он должен быть включен в /etc/inetd.conf. Все, что необходимо, это удалить символ комментария "#" из начала существующей строки ftpd. inetd должен перечитать конфигурацию после того, как этот файл настройки был изменен.

Теперь вы можете войти на FTP сервер любым клиентом ftp.

Если вам необходимо разрешить анонимную выгрузку файлов на FTP, права должны быть настроены таким образом, чтобы эти файлы не могли прочитать другие анонимные пользователи до их рассмотрения администратором.

Кроме поддержки многих прочих типов файловых систем, в ОС встроена поддержка сетевой файловой системы (Network File System), известной как NFS. NFS позволяет системе использовать каталоги и файлы совместно с другими машинами, посредством сети. Посредством NFS пользователи и программы могут получать доступ к файлам на удалённых системах точно так же, как если бы это были файлы на собственных дисках.

Вот некоторые из наиболее заметных преимуществ, которые даёт использование NFS:

- Отдельно взятые рабочие станции используют меньше собственного дискового пространства, так как совместно используемые данные могут храниться на одной отдельной машине и быть доступными для других машин в сети.

- Пользователям не нужно иметь домашние каталоги, отдельные для каждой машины в вашей сети. Домашние каталоги могут располагаться на сервере NFS и их можно сделать доступными отовсюду в сети.
- Устройства хранения информации, такие, как дискеты, приводы CD-ROM и устройства Zip®, могут использоваться другими машинами в сети. Это может привести к уменьшению переносимых устройств хранения информации в сети.

NFS строится из двух основных частей: сервера и одного или большего количества клиентов. Клиент обращается к данным, находящимся на сервере, в режиме удалённого доступа. Для того, чтобы это нормально функционировало, нужно настроить и запустить несколько процессов.

На сервере работают следующие даемоны:

Даемон	Описание
nfsd	Даемон NFS, обслуживающий запросы от клиентов NFS.
mountd	Даемон монтирования NFS, который выполняет запросы, передаваемые ему от nfsd(8).
rpcbind	Этот даемон позволяет клиентам NFS определить порт, используемый сервером NFS.

Клиент может запустить также даемон, называемый nfsiod. nfsiod обслуживает запросы, поступающие от сервера от сервера NFS. Он необязателен, увеличивает производительность, однако для нормальной и правильной работы не требуется. Для получения дополнительной информации обратитесь к разделу справочной системы о nfsiod(8).

Настройка NFS является достаточно незамысловатым процессом. Все процессы, которые должны быть запущены, могут быть запущены во время загрузки посредством нескольких модификаций в вашем файле /etc/rc.conf.

Проверьте на NFS-сервере в файле /etc/rc.conf соответствующие строки:

```
rpcbind_enable="YES"
nfs_server_enable="YES"
nfs_server_flags="-u -t -n 4"
mountd_flags="-r"
```

mountd запускается автоматически, если включена функция сервера NFS.

На клиенте убедитесь, что в файле /etc/rc.conf присутствует такой параметр: nfs_client_enable="YES"

Файл /etc/exports определяет, какие файловые системы на вашем сервере NFS будут экспортироваться (иногда их называют "совместно используемыми"). Каждая строка в /etc/exports задаёт файловую систему, которая будет экспортироваться и какие машины будут иметь к ней доступ. Кроме машин, имеющих доступ, могут задаваться другие параметры, влияющие на характеристики доступа. Имеется полный набор параметров, которые можно использовать, но здесь пойдёт речь лишь о некоторых из них. Описания остальных параметров можно найти на страницах справочной системы по exports(5).

Вот несколько примерных строк из файла /etc/exports:

В следующих примерах даётся общая идея того, как экспортировать файловые системы, хотя конкретные параметры могут отличаться в зависимости от ваших условий и конфигурации сети. К примеру, чтобы экспортировать каталог /cdrom для трёх машин, находящихся в том же самом домене, что и сервер (поэтому отсутствует доменное имя для каждой машины) или для которых имеются записи в файле /etc/hosts. Флаг -ro указывает на использование экспортируемой файловой системы в режиме только чтения. С этим флагом удалённая система не сможет никоим образом изменить экспортируемую файловую систему.

/cdrom -ro host1 host2 host3

В следующей строке экспортируется файловая система /home, которая становится доступной трем хостам, указанным по их IP-адресам. Это полезно, если у вас есть собственная сеть без настроенного сервера DNS. Как вариант, файл /etc/hosts может содержать внутренние имена хостов; пожалуйста, обратитесь к справочную систему по hosts(5) для получения дополнительной информации. Флаг -alldirs позволяет рассматривать подкаталоги в качестве точек монтирования. Другими словами, это не монтирование подкаталогов, но разрешение клиентам монтировать только каталоги, которые им требуются или нужны.

/home -alldirs 10.0.0.2 10.0.0.3 10.0.0.4

В строке, приведённой ниже, файловая система /a экспортируется таким образом, что она доступна двум клиентам из других доменов. Параметр -maproot=root позволяет пользователю root удалённой системы осуществлять запись на экспортируемую файловую систему как пользователь root. Если параметр -maproot=root не задан, то даже если пользователь имеет права доступа root на удалённой системе, он не сможет модифицировать файлы на экспортированной файловой системе.

/a -maproot=root host.example.com box.example.org

Для того, чтобы клиент смог обратиться к экспортированной файловой системе, он должен иметь права сделать это. Проверьте, что клиент указан в вашем файле /etc/exports.

В файле /etc/exports каждая строка содержит информацию об экспортировании для отдельной файловой системы для отдельно взятого

хоста. Удалённый хост может быть задан только один раз для каждой файловой системы, и может иметь только одну запись, используемую по умолчанию, для каждой локальной файловой системы. К примеру, предположим, что /usr является отдельной файловой системой. Следующий /etc/exports будет некорректен:

```
# Invalid when /usr is one file system
/usr/src   client
/usr/ports client
```

Одна файловая система, /usr, имеет две строки, задающие экспортирование для одного и того же хоста, client. Правильный формат в этом случае таков:

```
/usr/src /usr/ports  client
```

Свойства отдельной файловой системы, экспортируемой некоторому хосту, должны задаваться в одной строке. Строки без указания клиента воспринимаются как отдельный хост. Это ограничивает то, как вы можете экспортировать файловые системы, но для большинства это не проблема.

Ниже приведён пример правильного списка экспортирования, где /usr и /exports являются локальными файловыми системами:

```
# Экспортируем src и ports для client01 и client02, но
# только client01 имеет права пользователя root на них
/usr/src /usr/ports -maproot=root    client01
/usr/src /usr/ports         client02
#Клиентские машины имеют пользователя root и могут монтировать всё
# в каталоге /exports.  Кто угодно может монтировать /exports/obj в режиме чтения
/exports -alldirs -maproot=root      client01 client02
/exports/obj -ro
```

Даемон mountd должен быть проинформирован об изменении файла /etc/exports, чтобы изменения вступили в силу. Это может быть достигнуто посылкой сигнала HUP процессу mountd:

```
# kill -HUP `cat /var/run/mountd.pid`
```

или вызовом скрипта mountd подсистемы rc(8) с соответствующим параметром:

```
# /etc/rc.d/mountd reload
```

Как вариант, при перезагрузке FreeBSD всё настроится правильно. Хотя выполнять перезагрузку вовсе не обязательно. Выполнение следующих команд пользователем root запустит всё, что нужно.

На сервере NFS:

```
# rpcbind
# nfsd -u -t -n 4
# mountd -r
```

На клиенте NFS:

nfsiod -n 4

Теперь всё должно быть готово к реальному монтированию удалённой файловой системы. В приводимых примерах сервер будет носить имя server, а клиент будет носить имя client. Если вы только хотите временно смонтировать удалённую файловую систему, или всего лишь протестировать ваши настройки, то просто запустите команды, подобные приводимым здесь, работая как пользователь root на клиентской машине:

mount server:/home /mnt

По этой команде файловая система /home на сервере будет смонтирована в каталог /mnt на клиенте. Если всё настроено правильно, вы сможете войти в каталог /mnt на клиенте и увидеть файлы, находящиеся на сервере.

Если вы хотите автоматически монтировать удалённую файловую систему при каждой загрузке компьютера, добавьте файловую систему в /etc/fstab. Вот пример:

server:/home /mnt nfs rw 0 0

На страницах справочной системы по fstab(5) перечислены все доступные параметры.

У NFS есть много вариантов практического применения. Ниже приводится несколько наиболее широко распространённых способов её использования:

- Настройка несколько машин для совместного использования CDROM или других носителей.
- В больших сетях может оказаться более удобным настроить центральный сервер NFS, на котором размещаются все домашние каталоги пользователей.
- Несколько машин могут иметь общий каталог /usr/ports/distfiles. Таким образом, когда вам нужно будет установить порт на несколько машин, вы сможете быстро получить доступ к исходным текстам без их загрузки на каждой машине.

amd(8) (даемон автоматического монтирования) автоматически монтирует удалённую файловую систему, как только происходит обращение к файлу или каталогу в этой файловой системе. Кроме того, файловые системы, которые были неактивны некоторое время, будут автоматически размонтированы даемоном amd. Использование amd является простой альтернативой статическому монтированию, так как в последнем случае обычно всё должно быть описано в файле /etc/fstab.

amd работает, сам выступая как сервер NFS для каталогов /host и /net. Когда происходит обращение к файлу в одном из этих каталогов, amd ищет соответствующий удаленный ресурс для монтирования и автоматически его монтирует. /net используется для монтирования экспортируемой файловой системы по адресу IP, когда как каталог /host используется для монтирования ресурса по удаленному имени хоста.

Обращение к файлу в каталоге /host/foobar/usr укажет **amd** на выполнение попытки монтирования ресурса /usr, который находится на хосте foobar.

Вы можете посмотреть доступные для монтирования ресурсы отдалённого хоста командой showmount. К примеру, чтобы посмотреть ресурсы хоста с именем foobar, вы можете использовать:

```
% showmount -e foobar
Exports list on foobar:
/usr                10.10.10.0
/a              10.10.10.0
% cd /host/foobar/usr
```

Как видно из примера, showmount показывает /usr как экспортируемый ресурс. При переходе в каталог /host/foobar/usr даемон amd пытается разрешить имя хоста foobar и автоматически смонтировать требуемый ресурс.

amd может быть запущен из скриптов начальной загрузки, если поместить такую строку в файл /etc/rc.conf:

```
amd_enable="YES"
```

Кроме того, даемону amd могут быть переданы настроечные флаги через параметр amd_flags. По умолчанию amd_flags настроен следующим образом:

```
amd_flags="-a /.amd_mnt -l syslog /host /etc/amd.map /net /etc/amd.map"
```

Файл /etc/amd.map задает опции, используемые по умолчанию при монтировании экспортируемых ресурсов. В файле /etc/amd.conf заданы настройки некоторых более сложных возможностей amd.

Обратитесь к справочным страницам по amd(8) и amd.conf(5) для получения более полной информации.

Некоторые сетевые адаптеры имеют ограничения, которые могут привести к серьезным проблемам в сети, в частности, с NFS.

Проблема, которая возникает практически всегда при работе по сети систем с высокопроизводительными рабочими станциями, выпущенными такими производителями, как Silicon Graphics, Inc. и Sun Microsystems, Inc. Монтирование по протоколу NFS будет работать нормально, и некоторые операции также будут выполняться успешно, но неожиданно сервер окажется недоступным для клиент, хотя запросы к и от других систем будут продолжаться обрабатываться. Такое встречается с клиентскими системами, не зависимо от того, является ли клиент машиной или рабочей станцией. Во многих системах при возникновении этой проблемы нет способа корректно завершить работу клиента. Единственным выходом зачастую является холодная перезагрузка клиента, потому что ситуация с NFS не может быть разрешена.

Хотя "правильным" решением является установка более производительного и скоростного сетевого адаптера на систему, имеется

простое решение, приводящее к удовлетворительным результатам. Если система является сервером, укажите параметр -w=1024 на клиенте при монтировании. Если система является клиентом, то смонтируйте файловую систему NFS с параметром -r=1024. Эти параметры могут быть заданы в четвертом поле записи в файле fstab клиента при автоматическом монтировании, или при помощи параметра -o в команде mount(8) при монтировании вручную.

Нужно отметить, что имеется также другая проблема, ошибочно принимаемая за приведенную выше, когда серверы и клиенты NFS находятся в разных сетях. Если это тот самый случай, проверьте, что ваши маршрутизаторы пропускают нужную информацию UDP, в противном случае вы ничего не получите, что бы вы ни предпринимали.

В следующих примерах fastws является именем хоста (интерфейса) высокопроизводительной рабочей станции, а freebox является именем хоста (интерфейса) системы FreeBSD со слабым сетевым адаптером. Кроме того, /sharedfs будет являться экспортируемой через NFS файловой системой (обратитесь к страницам справочной системы по команде exports(5)), а /project будет точкой монтирования экспортируемой файловой системы на клиенте. В любом случае, отметьте, что для вашего приложения могут понадобиться дополнительные параметры, такие, как hard, soft или bg.

Пример системы FreeBSD (freebox) как клиента в файле /etc/fstab на машине freebox:

fastws:/sharedfs /project nfs rw,-r=1024 0 0

Команда, выдаваемая вручную на машине freebox:

mount -t nfs -o -r=1024 fastws:/sharedfs /project

Пример системы FreeBSD в качестве сервера в файле /etc/fstab на машине fastws:

freebox:/sharedfs /project nfs rw,-w=1024 0 0

Команда, выдаваемая вручную на машине fastws:

mount -t nfs -o -w=1024 freebox:/sharedfs /project

Практически все 16-разрядные сетевые адаптеры позволят работать без указанных выше ограничений на размер блоков при чтении и записи.

Для тех, кто интересуется, ниже описывается, что же происходит в при появлении этой ошибки, и объясняется, почему ее невозможно устранить. Как правило, NFS работает с "блоками" размером 8 килобайт (хотя отдельные фрагменты могут иметь меньшие размеры). Так, пакет Ethernet имеет максимальный размер около 1500 байт, то "блок" NFS разбивается на несколько пакетов Ethernet, хотя на более высоком уровне это все тот же единый блок, который должен быть принят, собран и подтвержден как один блок. Высокопроизводительные рабочие станции могут посылать пакеты, которые соответствуют одному блоку NFS, сразу друг за другом, насколько это позволяет делать стандарт. На слабых,

низкопроизводительных адаптерах пакеты, пришедшие позже, накладываются поверх ранее пришедших пакетов того же самого блока до того, как они могут быть переданы хосту и блок как единое целое не может быть собран или подтвержден. В результате рабочая станция входит в ситуацию тайм-аута и пытается повторить передачу, но уже с полным блоком в 8 КБ, и процесс будет повторяться снова, до бесконечности.

Задав размер блока меньше размера пакета Ethernet, мы достигаем того, что любой полностью полученный пакет Ethernet может быть подтвержден индивидуально, и избежим тупиковую ситуацию.

Наложение пакетов может все еще проявляться, когда высокопроизводительные рабочие станции сбрасывают данные на PC-систему, однако повторение этой ситуации не обязательно с более скоростными адаптерами с "блоками" NFS. Когда происходит наложение, затронутые блоки будут переданы снова, и скорее всего, они будут получены, собраны и подтверждены.

Samba это популярный пакет программ с открытыми исходными текстами, которая предоставляет файловые и принт-сервисы Microsoft® Windows® клиентам. Эти клиенты могут подключаться и использовать файловое пространство FreeBSD, как если бы это был локальный диск, или принтеры FreeBSD, как если бы это были локальные принтеры.

Пакет Samba должен быть включен в поставку FreeBSD. Если вы не установили Samba при первой установке системы, ее можно установить из порта или пакета net/samba3.

Файл настройки Samba по умолчанию устанавливается в /usr/local/etc/smb.conf.default. Этот файл необходимо скопировать в /usr/local/etc/smb.conf и отредактировать перед использованием Samba.

В файле smb.conf находится информация, необходимая для работы Samba, например определение принтеров и "общих каталогов", которые будут использоваться совместно с Windows клиентами. В пакет Samba входит программа с веб интерфейсом, называемая swat, которая дает простой способ редактирования файла smb.conf.

Программа веб администрирования Samba (Samba Web Administration Tool, SWAT) запускается как даемон из inetd. Следовательно, в /etc/inetd.conf необходимо снять комментарий перед тем, как использовать swat для настройки Samba:

swat stream tcp nowait/400 root /usr/local/sbin/swat

После изменения настроек inetd необходимо перечитать конфигурацию.

Как только swat был включен inetd.conf, вы можете использовать браузер для подключения к http://localhost:901. Сначала необходимо зарегистрироваться с системной учетной записью root.

После успешного входа на основную страницу настройки Samba, вы можете просмотреть документацию или начать настройку, нажав на кнопку Globals. Раздел Globals соответствует переменным, установленным в разделе [global] файла /usr/local/etc/smb.conf.

Независимо от того, используете ли вы swat, или редактируете /usr/local/etc/smb.conf непосредственно, первые директивы, которые вы скорее всего встретите при настройке Samba, будут следующими:

workgroup

Имя домена или рабочей группы для компьютеров, которые будут получать доступ к этому серверу.

netbios name

Устанавливает имя NetBIOS, под которым будет работать Samba сервер. По умолчанию оно устанавливается равным первому компоненту DNS имени хоста.

server string

Устанавливает строку, которая будет показана командой net view и некоторыми другими сетевыми инструментами, которые отображают строку описания сервера.

Две из наиболее важных настроек в /usr/local/etc/smb.conf отвечают за выбор модели безопасности и за формат паролей для клиентов. Эти параметры контролируются следующими директивами:

security

Два наиболее часто используемых параметра это security = share и security = user. Если имена пользователей для клиентов совпадают с их именами на компьютере, вы возможно захотите включить безопасность уровня пользователя (user). Это политика безопасности по умолчанию, она требует, чтобы клиент авторизовался перед доступом к совместно используемым ресурсам.

На уровне безопасности share клиенту не требуется входить на сервер перед подключением к ресурсу. Эта модель безопасности использовалась по умолчанию в старых версиях Samba.

passdb backend

Samba поддерживает несколько различных подсистем аутентификации. Вы можете аутентифицировать клиентов с помощью LDAP, NIS+, базы данных SQL, или через модифицированный файл паролей. Метод аутентификации по умолчанию smbpasswd, и здесь рассматривается только он.

Предполагая, что используется подсистема по умолчанию smbpasswd, необходимо создать файл /usr/local/private/smbpasswd, чтобы Samba могла аутентифицировать клиентов. Если вы хотите разрешить всем учетным записям UNIX® доступ с Windows клиентов, используйте следующую команду:

grep -v "^#" /etc/passwd | make_smbpasswd > /usr/local/private/smbpasswd

chmod 600 /usr/local/private/smbpasswd

Обратитесь к документации на Samba за дополнительной информацией о параметрах настройки. Основные настройки, рассмотренные здесь, достаточны для первого запуска Samba.

Для запуска Samba при загрузке системы, добавьте в /etc/rc.conf следующую строку:

samba_enable="YES"

Затем вы можете запустить Samba в любой момент, набрав:

/usr/local/etc/rc.d/samba.sh start

Starting SAMBA: removing stale tdbs :

Starting nmbd.

Starting smbd.

Samba состоит из трех отдельных даемонов. Вы можете видеть, что nmbd и smbd запускаются скриптом samba.sh. Если вы включили сервис разрешения имен winbind в smb.conf, то увидите также запуск даемона winbindd.

Вы можете остановить Samba в любой момент, набрав:

/usr/local/etc/rc.d/samba.sh stop

Samba это сложный программный набор с функциональностью, позволяющей полную интеграцию в сети Microsoft Windows. За дальнейшей информацией о функциях, выходящих за рамки описанной здесь базовой установки, обращайтесь к http://www.samba.org.

Network Information System (NIS/YP).

NIS разработан компанией Sun Microsystems для централизованного администрирования систем.

В настоящее время эти службы практически стали промышленным стандартом; все основные UNIX-подобные системы поддерживают NIS.

Это система клиент/сервер на основе вызовов RPC, которая позволяет группе машин в одном домене NIS совместно использовать общий набор конфигурационных файлов.

Системный администратор может настроить клиентскую систему NIS только с минимальной настроечной информацией, а затем добавлять, удалять и модифицировать настроечную информацию из одного места.

Имя домена NIS. Главный сервер NIS и все его клиенты (включая вторичные серверы), имеют доменное имя NIS. Как и в случае с именем домена Windows NT, имя домена NIS не имеет ничего общего с DNS.

rpcbind. Для обеспечения работы RPC (Remote Procedure Call, Удалённого Вызова Процедур, сетевого протокола, используемого NIS), должен быть запущен даемон rpcbind. Если даемон rpcbind не запущен, невозможно будет запустить сервер NIS, или работать как NIS-клиент.

ypbind. Связывает NIS-клиента с его NIS-сервером. Он определяет имя NIS-домена системы, и при помощи RPC подключается к серверу. ypbind является основой клиент-серверного взаимодействия в среде NIS; если на клиентской машине программа ypbind перестанет работать, то эта машина не сможет получить доступ к серверу NIS.

ypserv. Программа ypserv, которая должна запускаться только на серверах NIS: это и есть сервер NIS. Если ypserv(8) перестанет работать, то сервер не сможет отвечать на запросы NIS (к счастью, на этот случай предусмотрен вторичный сервер). Есть несколько реализаций NIS (к FreeBSD это не относится), в которых не производится попыток подключиться к другому серверу, если ранее используемый сервер перестал работать. Зачастую единственным средством, помогающим в этой ситуации, является перезапуск серверного процесса (или сервера полностью) или процесса ypbind на клиентской машине.

rpc.yppasswdd. Программа rpc.yppasswdd, другой процесс, который запускается только на главных NIS-серверах: это даемон, позволяющий клиентам NIS изменять свои пароли NIS. Если этот даемон не запущен, то пользователи должны будут входить на основной сервер NIS и там менять свои пароли.

В системе NIS существует три типа хостов:

- основные (master) серверы,
- вторичные (slave) серверы,
- клиентские машины.

Серверы выполняют роль централизованного хранилища информации о конфигурации хостов. Основные серверы хранят оригиналы этой информации, когда как вторичные серверы хранят ее копию для обеспечения избыточности. Клиенты связываются с серверами, чтобы предоставить им эту информацию.

Информация во многих файлах может совместно использоваться следующим образом. Файлы master.passwd, group и hosts используются совместно через NIS. Когда процессу, работающему на клиентской машине, требуется информация, как правило, находящаяся в этих файлах локально, то он делает запрос к серверу NIS, с которым связан.

Основной сервер NIS. Такой сервер, по аналогии с первичным контроллером домена, хранит файлы, используемые всеми клиентами NIS. Файлы passwd, group и различные другие файлы, используемые клиентами NIS, находятся на основном сервере.

Возможно использование одной машины в качестве сервера для более чем одного домена NIS. Однако, в этом введении такая ситуация не рассматривается, и предполагается менее масштабное использование NIS.

Вторичные серверы NIS. Похожие на вторичные контроллеры доменов, вторичные серверы NIS содержат копии оригинальных файлов данных NIS. Вторичные серверы NIS обеспечивают избыточность, что

нужно в критичных приложениях. Они также помогают распределять нагрузку на основной сервер: клиенты NIS всегда подключаются к тому серверу NIS, который ответил первым, в том числе и к вторичным серверам.

Клиенты NIS. Клиенты NIS, как и большинство рабочих станций, аутентифицируются на сервере NIS во время входа в систему.

Пример настройки NIS.

Имя домена NIS не должно быть использованного имени домена. Когда клиент рассылает запросы на получение информации, он включает в них имя домена NIS, частью которого является.

Таким способом многие сервера в сети могут указать, какой сервер на какой запрос должен отвечать.

Имя домена NIS должно быть уникальным в пределах вашей сети.

Оригинальные копии всей информации NIS хранится на единственной машине, которая называется главным сервером NIS.

Базы данных, которые используются для хранения информации, называются картами NIS.

Один сервер NIS может поддерживать одновременно несколько доменов, так что есть возможность иметь несколько таких каталогов, по одному на каждый обслуживаемый домен. Каждый домен будет иметь свой собственный независимый от других набор карт.

Основной и вторичный серверы обслуживают все запросы NIS с помощью ypserv.

ypserv отвечает за получение входящих запросов от клиентов NIS, распознавание запрашиваемого домена и отображение имени в путь к соответствующему файлы базы данных, а также передаче информации из базы данных обратно клиенту.

Настройка основного сервера NIS .

Добавить следующие строки в файл /etc/rc.conf

- nisdomainname="test-domain"
- В этой строке задается имя домена NIS, которое будет test-domain, еще до настройки сети (например, после перезагрузки).
- nis_server_enable="YES"
- Здесь указывается FreeBSD на запуск процессов серверов NIS, когда дело доходит до сетевых настроек.
- nis_yppasswdd_enable="YES"
- Здесь указывается на запуск даемона rpc.yppasswdd, который, как это отмечено выше, позволит пользователям менять свой пароль NIS с клиентской машины.

В зависимости от ваших настроек NIS, вам могут понадобиться дополнительные строки.

Запустить команду /etc/netstart, работая как администратор.

Произойдет настройка всего, при этом будут использоваться значения, заданные в файле /etc/rc.conf.

Карты NIS являются файлами баз данных, которые хранятся в каталоге /var/yp. Они генерируются из конфигурационных файлов, находящихся в каталоге /etc основного сервера NIS, за одним исключением: файл /etc/master.passwd. На это есть весомая причина, вам не нужно распространять пароли пользователя root и других административных пользователей на все серверы в домене NIS. По этой причине, прежде чем инициализировать карты NIS, вы должны сделать вот что:

```
# cp /etc/master.passwd /var/yp/master.passwd
# cd /var/yp
# vi master.passwd
```

Удалить все записи, касающиеся системных пользователей (bin, tty, kmem, games и так далее), а также записи, которые вы не хотите распространять клиентам NIS (например, root и другие пользователи с UID, равным 0 (администраторы)).

Проверьте, чтобы файл /var/yp/master.passwd был недоступен для записи ни для группы, ни для остальных пользователей. Воспользуйтесь командой chmod, если это нужно.

Скрипт ypsetup. При вызове программы ypinit передаем параметр -m. Для генерации карт NIS в предположении:

```
ellington# ypinit -m test-domain
Server Type: MASTER Domain: test-domain
Creating an YP server will require that you answer a few questions.
Questions will all be asked at the beginning of the procedure.
Do you want this procedure to quit on non-fatal errors? [y/n: n] n
Ok, please remember to go back and redo manually whatever fails.
If you don't, something might not work.
At this point, we have to construct a list of this domains YP servers.
rod.darktech.org is already known as master server.
Please continue to add any slave servers, one per line. When you are
done with the list, type a <control D>.
master server   :  ellington
next host to add:  coltrane
next host to add:  ^D
The current list of NIS servers looks like this:
ellington
coltrane
Is this correct?  [y/n: y] y
[..вывод при генерации карт..]
NIS Map update completed.
ellington has been setup as an YP master server without any errors.
```

Программа ypinit должна была создать файл /var/yp/Makefile из /var/yp/Makefile.dist. При создании этого файла предполагается, что вы работаете в окружении с единственным сервером NIS. Так как в домене test-domain имеется также и вторичный сервер, то вы должны отредактировать файл /var/yp/Makefile:

ellington# vi /var/yp/Makefile

Вы должны закомментировать строку, в которой указано

NOPUSH = "True"

(она уже не раскомментирована).

Настройка вторичного сервера NIS. Войдите на вторичный сервер и отредактируйте файл /etc/rc.conf.

При запуске программы ypinit должны использовать опцию -s. Применение опции -s требует также указание имени главного сервера NIS, так что наша команда должна выглядеть так:

```
coltrane# ypinit -s ellington test-domain
Server Type: SLAVE Domain: test-domain Master: ellington
Creating an YP server will require that you answer a few questions.
Questions will all be asked at the beginning of the procedure.
Do you want this procedure to quit on non-fatal errors? [y/n: n]  n
Ok, please remember to go back and redo manually whatever fails.
If you don't, something might not work.
There will be no further questions. The remainder of the procedure
should take a few minutes, to copy the databases from ellington.
Transferring netgroup...
ypxfr: Exiting: Map successfully transferred
Transferring netgroup.byuser...
ypxfr: Exiting: Map successfully transferred
Transferring netgroup.byhost...
ypxfr: Exiting: Map successfully transferred
Transferring master.passwd.byuid...
ypxfr: Exiting: Map successfully transferred
Transferring passwd.byuid...
ypxfr: Exiting: Map successfully transferred
Transferring passwd.byname...
ypxfr: Exiting: Map successfully transferred
Transferring group.bygid...
ypxfr: Exiting: Map successfully transferred
Transferring group.byname...
ypxfr: Exiting: Map successfully transferred
Transferring services.byname...
ypxfr: Exiting: Map successfully transferred
Transferring rpc.bynumber...
ypxfr: Exiting: Map successfully transferred
```

Transferring rpc.byname...
ypxfr: Exiting: Map successfully transferred
Transferring protocols.byname...
ypxfr: Exiting: Map successfully transferred
Transferring master.passwd.byname...
ypxfr: Exiting: Map successfully transferred
Transferring networks.byname...
ypxfr: Exiting: Map successfully transferred
Transferring networks.byaddr...
ypxfr: Exiting: Map successfully transferred
Transferring netid.byname...
ypxfr: Exiting: Map successfully transferred
Transferring hosts.byaddr...
ypxfr: Exiting: Map successfully transferred
Transferring protocols.bynumber...
ypxfr: Exiting: Map successfully transferred
Transferring ypservers...
ypxfr: Exiting: Map successfully transferred
Transferring hosts.byname...
ypxfr: Exiting: Map successfully transferred
coltrane has been setup as an YP slave server without any errors.
Don't forget to update map ypservers on ellington.

Каталог с именем /var/yp/test-domain. Копии карт главного сервера NIS должны быть в этом каталоге. Вы должны удостовериться, что этот каталог обновляется. Следующие строки в /etc/crontab вашего вторичного сервера должны это делать:

20 * * * * root /usr/libexec/ypxfr passwd.byname
21 * * * * root /usr/libexec/ypxfr passwd.byuid

Эти две строки заставляют вторичный сервер синхронизировать свои карты с картами главного сервера. Хотя эти строчки не обязательны, так как главный сервер делает попытки передать все изменения в своих картах NIS на свои вторичные серверы, но из-за того, что информация для входа в систему настолько жизненно важна для систем, зависящих от сервера, что выполнение регулярных обновлений является совсем не плохой идеей. Это ещё более важно в загруженных сетях, в которых обновления карт могут не всегда завершаться успешно.

Запустить команду /etc/netstart на вторичном сервере, по которой снова выполнится запуск сервера NIS.

Клиент NIS выполняет так называемую привязку к конкретному серверу NIS при помощи ypbind.

ypbind определяет домен, используемый в системе по умолчанию (тот, который устанавливается по команде domainname), и начинает широковещательную рассылку запросов RPC в локальной сети.

В этих запросах указано имя домена, к серверу которого ypbind пытается осуществить привязку.

Если сервер, который был настроен для обслуживания запрашиваемого домена, получит широковещательный запрос, он ответит ypbind, который, в свою очередь запомнит адрес сервера. Если имеется несколько серверов (например, главный и несколько вторичных), то ypbind будет использовать адрес первого ответившего. С этого момента клиентская система будет направлять все свои запросы NIS на этот сервер. Время от времени ypbind будет "пинать" сервер для проверки его работоспособности. Если на один из тестовых пакетов не удастся получить ответа за разумное время, то ypbind пометит этот домен как домен, с которым связка разорвана, и снова начнет процесс посылки широковещательных запросов в надежде найти другой сервер.

Настройка клиента NIS.

- Отредактируйте файл /etc/rc.conf, добавив туда следующие строки для того, чтобы задать имя домена NIS и запустить ypbind во время запуска сетевых служб:
- nisdomainname="test-domain"
- nis_client_enable="YES"
- Для импортирования всех возможных учётных записей от сервера NIS, удалите все записи пользователей из вашего файла /etc/master.passwd и воспользуйтесь командой vipw для добавления следующей строки в конец файла:
- +:::::::::

Эта строчка даст всем пользователям с корректной учетной записью в картах учетных баз пользователей доступ к этой системе.

Изменив эту строку, настроить ваш клиент NIS.

Вы должны оставить хотя бы одну локальную запись (то есть не импортировать ее через NIS) в вашем /etc/master.passwd и эта запись должна быть также членом группы wheel.

Если с NIS что-то случится, эта запись может использоваться для удаленного входа в систему, перехода в режим администратора и исправления неисправностей.

- Для импортирования всех возможных записей о группах с сервера NIS, добавьте в ваш файл /etc/group такую строчку:
- +:*::

После завершения выполнения этих шагов у вас должно получиться запустить команду ypcat passwd и увидеть карту учетных записей сервера NIS.

Любой пользователь, зная имя вашего домена, может выполнить запрос RPC к ypserv(8) и получить содержимое ваших карт NIS.

Для предотвращения такого неавторизованного обмена ypserv(8) поддерживает так называемую систему "securenets", которая может использоваться для ограничения доступа к некоторой группе хостов.

При запуске ypserv(8) будет пытаться загрузить информацию, касающуюся securenets, из файла /var/yp/securenets.

Имя каталога зависит от параметра, указанного вместе с опцией -p. Этот файл содержит записи, состоящие из указания сети и сетевой маски, разделенных пробелом. Строчки, начинающиеся со знака "#", считаются комментариями. Примерный файл securenets может иметь примерно такой вид:

```
# allow connections from local host -- mandatory
127.0.0.1     255.255.255.255
# allow connections from any host
# on the 192.168.128.0 network
192.168.128.0 255.255.255.0
# allow connections from any host
# between 10.0.0.0 to 10.0.15.255
# this includes the machines in the testlab
10.0.0.0      255.255.240.0
```

Если ypserv(8) получает запрос от адреса, который соответствует одному из этих правил, он будет отрабатывать запрос обычным образом. Если же адрес не подпадает ни под одно правило, запрос будет проигнорирован и в журнал будет записано предупреждающее сообщение. Если файл /var/yp/securenets не существует, ypserv будет обслуживать соединения от любого хоста.

Программа ypserv также поддерживает пакет программ TCP Wrapper от Wietse Venema. Это позволяет администратору для ограничения доступа вместо /var/yp/securenets использовать конфигурационные файлы TCP Wrapper.

Оба этих метода управления доступом обеспечивают некоторую безопасность, они, как основанные на проверке привилегированного порта, оба подвержены атакам типа "IP spoofing". Весь сетевой трафик, связанный с работой NIS, должен блокироваться вашим брандмауэром.

Серверы, использующие файл /var/yp/securenets, могут быть не в состоянии обслуживать старых клиентов NIS с древней реализацией протокола TCP/IP.

Некоторые из этих реализаций при рассылке широковещательных запросов устанавливают все биты машинной части адреса в ноль и/или не в состоянии определить маску подсети при вычислении адреса широковещательной рассылки.

Хотя некоторые из этих проблем могут быть решены изменением конфигурации клиента, другие могут привести к отказу от использования /var/yp/securenets.

Использование /var/yp/securenets на сервере с такой архаичной реализацией TCP/IP является весьма плохой идеей, и приведёт к потере работоспособности NIS в большой части вашей сети.

Использование пакета TCP Wrapper увеличит время отклика вашего сервера NIS. Дополнительной задержки может оказаться достаточно для возникновения тайм-аутов в клиентских программах, особенно в загруженных сетях или с медленными серверами NIS. Если одна или более ваших клиентских систем страдают от таких проблем, вы должны преобразовать такие клиентские системы во вторичные серверы NIS и сделать принудительную их привязку к самим себе.

Есть способ ограничить вход некоторых пользователей на этой машине, даже если они присутствуют в базе данных NIS.

Достаточно добавить -username в конец файла /etc/master.passwd на клиентской машине, где username является именем пользователя, которому вы хотите запретить вход. Рекомендуется сделать это с помощью утилиты vipw, так как vipw проверит ваши изменения в /etc/master.passwd, а также автоматически перестроит базу данных паролей по окончании редактирования.

Пример.

```
basie# vipw
[add -bill to the end, exit]
vipw: rebuilding the database...
vipw: done
basie# cat /etc/master.passwd
root:[password]:0:0::0:0:The super-user:/root:/bin/csh
toor:[password]:0:0::0:0:The other super-user:/root:/bin/sh
daemon:*:1:1::0:0:Owner of many system processes:/root:/sbin/nologin
operator:*:2:5::0:0:System &:/:/sbin/nologin
bin:*:3:7::0:0:Binaries Commands and Source,,,:/:/sbin/nologin
tty:*:4:65533::0:0:Tty Sandbox:/:/sbin/nologin
kmem:*:5:65533::0:0:KMem Sandbox:/:/sbin/nologin
games:*:7:13::0:0:Games pseudo-user:/usr/games:/sbin/nologin
news:*:8:8::0:0:News Subsystem:/:/sbin/nologin
man:*:9:9::0:0:Mister Man Pages:/usr/share/man:/sbin/nologin
bind:*:53:53::0:0:Bind Sandbox:/:/sbin/nologin
uucp:*:66:66::0:0:UUCP pseudo-user:/var/spool/uucppublic:/usr/libexec/uucp/uucico
xten:*:67:67::0:0:X-10 daemon:/usr/local/xten:/sbin/nologin
pop:*:68:6::0:0:Post Office Owner:/nonexistent:/sbin/nologin
nobody:*:65534:65534::0:0:Unprivileged user:/nonexistent:/sbin/nologin
+:::::::::
-bill
basie#
```

Сетевые группы. Отличие заключается в отсутствии числового идентификатора и возможности задать сетевую группу включением как пользователей, так и других сетевых групп.

Сетевые группы были разработаны для работы с большими, сложными сетями с сотнями пользователей и машин. С одной стороны, хорошо, если вам приходится с такой ситуацией. С другой стороны, эта сложность делает невозможным описание сетевых групп с помощью простых примеров. Пример, используемый в дальнейшем, демонстрирует эту проблему.

Ограничивая каждого пользователя по отдельности, придется добавить на каждой машине в файл passwd по одной строчке -user для каждого пользователя, которому запрещено входить на эту систему.

Использование сетевых групп дает несколько преимуществ:

- нет необходимости описывать по отдельности каждого пользователя;
- ставите в соответствие пользователю одну или несколько сетевых групп и разрешаете или запрещаете вход всем членам сетевой группы;
- при добавлении новой машины, достаточно определить ограничения на вход для сетевых групп;
- добавляется новый пользователь, достаточно добавить его к одной или большему числу сетевых групп.
- изменения независимы друг от друга;
- для разрешения или запрещения доступа к машинам вам нужно будет модифицировать единственный конфигурационный файл.

Инициализация карты NIS по имени netgroup.

Программа ypinit(8) по умолчанию этой карты не создаёт, хотя реализация NIS будет её поддерживает, как только она будет создана. Чтобы создать пустую карту

ellington# vi /var/yp/netgroup

и начните добавлять содержимое. Например, нам нужно по крайней мере четыре сетевых группы: сотрудники IT, практиканты IT, обычные сотрудники и интернатура.

```
IT_EMP (,alpha,test-domain)    (,beta,test-domain)
IT_APP  (,charlie,test-domain)  (,delta,test-domain)
USERS   (,echo,test-domain) (,foxtrott,test-domain) \
   (,golf,test-domain)
INTERNS (,able,test-domain) (,baker,test-domain)
```

IT_EMP, IT_APP и так далее являются именами сетевых групп. Несколько слов в скобках служат для добавления пользователей в группу. Три поля внутри группы обозначают следующее:

- Имя хоста или хостов, к которым применимы последующие записи. Если имя хоста не указано, то запись применяется ко

всем хостам. Если же указывается имя хоста, то вы получите мир темноты, ужаса и страшной путаницы.

- Имя учетной записи, которая принадлежит этой сетевой группе.
- Домен NIS для учетной записи. Вы можете импортировать в вашу сетевую группу учетные записи из других доменов NIS, если вы один из тех несчастных, имеющих более одного домена NIS.

Каждое из этих полей может содержать шаблоны, подробности даны в странице справочника по netgroup(5).

Не нужно использовать имена сетевых групп длиннее 8 символов, особенно если в вашем домене NIS имеются машины, работающие под управлением других операционных систем. Имена чувствительны к регистру; использование заглавных букв для имен сетевых групп облегчает распознавание пользователей, имен машин и сетевых групп.

Некоторые клиенты NIS не могут работать с сетевыми группами, включающими большое количество записей.

Активация и распространение вашей карты NIS:

ellington# cd /var/yp

ellington# make

Это приведет к созданию трех карт NIS netgroup, netgroup.byhost и netgroup.byuser. Воспользуйтесь утилитой ypcat(1) для проверки доступности ваших новых карт NIS:

ellington% ypcat -k netgroup

ellington% ypcat -k netgroup.byhost

ellington% ypcat -k netgroup.byuser

Вывод первой команды должен соответствовать содержимому файла /var/yp/netgroup. Вторая команда не выведет ничего, если вы не зададите сетевые группы, специфичные для хоста. Третья команда может использоваться пользователем для получения списка сетевых групп.

Настройка клиента. Чтобы настроить сервер war, достаточно запустить vipw(8) и заменить строку

+:::::::::

на

+@IT_EMP:::::::::

Теперь только данные, касающиеся пользователей, определенных в сетевой группе IT_EMP, импортируются в базу паролей машины war и только этим пользователям будет разрешен вход.

К сожалению, это ограничение также касается и функции ~ командного процессора и всех подпрограмм, выполняющих преобразование между именами пользователей и их числовыми ID. Другими словами, команда cd ~user работать не будет, команда ls -l будет выдавать числовые идентификаторы вместо имён пользователей, а find . -user joe -print работать откажется, выдавая сообщение “No such user”.

Чтобы это исправить, вам нужно будет выполнить импорт всех записей о пользователях без разрешения на вход на ваши серверы.

Это можно сделать, добавив еще одну строку в файл /etc/master.passwd. Эта строка должна содержать:

+:::::::::/sbin/nologin, что означает "Произвести импортирование всех записей с заменой командного процессора на /sbin/nologin в импортируемых записях". Вы можете заменить любое поле в строке с паролем, указав значение по умолчанию в вашем /etc/master.passwd.

Проверьте, что строка +:::::::::/sbin/nologin помещена после +@IT_EMP:::::::::. В противном случае все пользовательские записи, импортированные из NIS, будут иметь /sbin/nologin в качестве оболочки.

После этого изменения при появлении нового сотрудника IT вам будет достаточно изменять только одну карту NIS. Вы можете применить подобный метод для менее важных серверов, заменяя старую строку +::::::::: в их файлах /etc/master.passwd на нечто, подобное следующему:

```
+@IT_EMP:::::::::
+@IT_APP:::::::::
+:::::::::/sbin/nologin
```

Соответствующие строки для обычных рабочих станций могут иметь такой вид:

```
+@IT_EMP:::::::::
+@USERS:::::::::
+:::::::::/sbin/nologin
```

Возможность в NIS создавать сетевые группы из других сетевых групп может использоваться для предотвращения ситуаций. Одним из вариантов является создание сетевых групп на основе ролей. Вы можете создать сетевую группу с именем BIGSRV для задания ограничений на вход на важные серверы, другую сетевую группу с именем SMALLSRV для менее важных серверов и третью сетевую группу под названием USERBOX для обычных рабочих станций. Каждая из этих сетевых групп содержит сетевые группы, которым позволено входить на эти машины. Новые записи для вашей карты NIS сетевой группы должны выглядеть таким образом:

```
BIGSRV   IT_EMP  IT_APP
SMALLSRV  IT_EMP  IT_APP  ITINTERN
USERBOX   IT_EMP  ITINTERN USERS
```

Этот метод задания ограничений на вход работает весьма хорошо, если вы можете выделить группы машин с одинаковыми ограничениями. К сожалению, такая ситуация может быть исключением, но не правилом. В большинстве случаев вам нужна возможность определять ограничения на вход индивидуально для каждой машины.

Задание сетевых групп в зависимости от машин является другой возможностью, которой можно воспользоваться при изменении политики,

описанной выше. При таком развитии событий файл /etc/master.passwd на каждой машине содержит две строки, начинающиеся с "+". Первая из них добавляет сетевую группу с учётными записями, которым разрешено входить на эту машину, а вторая добавляет все оставшиеся учетные записи с /sbin/nologin в качестве командного процессора. Хорошей идеей является использование "ИМЕНИ МАШИНЫ" заглавными буквами для имени сетевой группы. Другими словами, строки должны иметь такой вид:

+*@BOXNAME*:::::::::

+:::::::::/sbin/nologin

Как только вы завершите эту работу для всех ваших машин, вам не нужно будет снова модифицировать локальные версии /etc/master.passwd. Все будущие изменения могут быть выполнены изменением карты NIS. Вот пример возможной карты сетевой группы для этого случая с некоторыми полезными дополнениями:

```
# Сначала определяем группы пользователей
IT_EMP    (,alpha,test-domain)    (,beta,test-domain)
IT_APP    (,charlie,test-domain)  (,delta,test-domain)
DEPT1     (,echo,test-domain)     (,foxtrott,test-domain)
DEPT2     (,golf,test-domain)     (,hotel,test-domain)
DEPT3     (,india,test-domain)    (,juliet,test-domain)
ITINTERN  (,kilo,test-domain)     (,lima,test-domain)
D_INTERNS (,able,test-domain)     (,baker,test-domain)
#
# Теперь задаем несколько групп на основе ролей
USERS     DEPT1   DEPT2     DEPT3
BIGSRV    IT_EMP  IT_APP
SMALLSRV  IT_EMP  IT_APP    ITINTERN
USERBOX   IT_EMP  ITINTERN  USERS
#
# И группы для специальных задач
# Открыть пользователям echo и golf доступ к антивирусной машине
SECURITY  IT_EMP  (,echo,test-domain)  (,golf,test-domain)
#
# Сетевые группы, специфичные для машин
# Наши главные серверы
WAR   BIGSRV
FAMINE    BIGSRV
# Пользователю india необходим доступ к этому серверу
POLLUTION  BIGSRV  (,india,test-domain)
#
# Этот очень важен и ему требуются большие ограничения доступа
DEATH     IT_EMP
#
```

```
# Антивирусная машина, упомянутая выше
ONE   SECURITY
#
# Ограничить машину единственным пользователем
TWO   (,hotel,test-domain)
# [...далее следуют другие группы]
```

Если вы используете какие-либо базы данных для управления учетными записями ваших пользователей, вы должны смочь создать первую часть карты с помощью инструментов построения отчетов вашей базы данных. В таком случае новые пользователи автоматически получат доступ к машинам.

И последнее замечание: Не всегда бывает разумно использовать сетевые группы на основе машин. Если в студенческих лабораториях вы используете несколько десятков или даже сотен одинаковых машин, то вам нужно использовать сетевые группы на основе ролей, а не основе машин, для того, чтобы размеры карты NIS оставались в разумных пределах.

Есть некоторые действия, которые нужно будет выполнять по-другому, если вы работаете с NIS.

- Каждый раз, когда вы собираетесь добавить пользователя в лаборатории, вы должны добавить его только на главном сервере NIS и обязательно перестроить карты NIS. Если вы забудете сделать это, то новый пользователь не сможет нигде войти, кроме как на главном сервере NIS. Например, если в лаборатории нам нужно добавить нового пользователя jsmith, мы делаем вот что:
- # pw useradd jsmith
- # cd /var/yp
- # make test-domain
- Вместо pw useradd jsmith вы можете также запустить команду adduser jsmith.
- Не помещайте административные учетные записи в карты NIS. Вам не нужно распространять административных пользователей и их пароли на машины, которые не должны иметь доступ к таким учётным записям.
- Сделайте главный и вторичные серверы NIS безопасными и минимизируйте их время простоя. Если кто-то либо взломает, либо просто отключит эти машины, то люди без права входа в лабораторию с легкостью получат доступ.

Это основное уязвимое место в любой централизованно администрируемой системе.

ypserv имеет встроенную поддержку для обслуживания клиентов NIS v1. Реализация NIS в отдельных ОС использует только протокол NIS v2, хотя другие реализации имеют поддержку протокола v1 для

совместимости со старыми системами. ypbind, поставляемые с такими системами, будут пытаться осуществить привязку к серверу NIS v1, даже если это им не нужно (и они будут постоянно рассылать широковещательные запросы в поиске такого сервера даже после получения ответа от сервера v2). Отметьте, что хотя имеется поддержка обычных клиентских вызовов, эта версия ypserv не отрабатывает запросы на передачу карт v1; следовательно, она не может использоваться в качестве главного или вторичного серверов вместе с другими серверами NIS, поддерживающими только протокол v1. К счастью, скорее всего, в настоящий момент такие серверы практически не используются.

Особое внимание следует уделить использованию ypserv в домене со многими серверами, когда серверные машины являются также клиентами NIS. Неплохо бы заставить серверы осуществить привязку к самим себе, запретив рассылку запросов на привязку и возможно, перекрестную привязку друг к другу. Если один сервер выйдет из строя, а другие будут зависеть от него, то в результате могут возникнуть странные ситуации. Постепенно все клиенты попадут в тайм-аут и попытаются привязаться к другим серверам, но полученная задержка может быть значительной, а странности останутся, так как серверы снова могут привязаться друг к другу.

Вы можете заставить хост выполнить привязку к конкретному серверу, запустив команду ypbind с флагом -S. Если вы не хотите делать это вручную каждый раз при перезагрузке вашего сервера NIS, то можете добавить в файл /etc/rc.conf такие строки:

```
nis_client_enable="YES"   # run client stuff as well
nis_client_flags="-S NIS domain,server"
```

Дополнительную информацию можно найти на странице справки по ypbind(8).

Одним из общих вопросов, которые возникают в начале работы с NIS, является вопрос совместимости форматов паролей. Если ваш сервер NIS использует пароли, зашифрованные алгоритмом DES, то он будет поддерживать только тех клиентов, что также используют DES. К примеру, если в вашей сети имеются клиенты NIS, использующие Solaris, то вам, скорее всего, необходимо использовать пароли с шифрованием по алгоритму DES.

Чтобы понять, какой формат используют ваши серверы и клиенты, загляните в файл /etc/login.conf. Если хост настроен на использование паролей, зашифрованных по алгоритму DES, то класс default будет содержать запись вроде следующей:

```
default:\
   :passwd_format=des:\
   :copyright=/etc/COPYRIGHT:\
   [Последующие строки опущены]
```

Другими возможными значениями для passwd_format являются blf и md5 (для паролей, шифруемых по стандартам Blowfish и MD5 соответственно).

Если вы внесли изменения в файл /etc/login.conf, то вам также нужно перестроить базу данных параметров входа в систему, что достигается запуском следующей команды пользователем root:

cap_mkdb /etc/login.conf

Формат паролей, которые уже находятся в файле /etc/master.passwd, не будет изменён до тех пор, пока пользователь не сменит свой пароль после перестроения базы данных параметров входа в систему.

После этого, чтобы удостовериться в том, что пароли зашифрованы в том формате, который выбран вами, нужно проверить, что строка crypt_default в /etc/auth.conf указывает предпочтение выбранного вами формата паролей. Для этого поместите выбранный формат первым в списке. Например, при использовании DES-шифрования паролей строка будет выглядеть так:

crypt_default = des blf md5

Выполнив вышеперечисленные шаги на каждом из серверов и клиентов NIS, работающих на FreeBSD, вы можете обеспечить их согласованность относительно используемого в вашей сети формата паролей. Если у вас возникли проблемы с аутентификацией клиента NIS, начать её решать определённо стоит отсюда. Запомните: если вы хотите использовать сервер NIS в гетерогенной сети, вам, наверное, нужно будет использовать DES на всех системах в силу того, что это минимальный общий стандарт.

Контрольные вопросы

1. Назначение протокола передачи файлов (File Transfer Protocol, FTP)?
2. Локальный запрет доступа по FTP?
3. Анонимный FTP доступ на сервер?
4. Настройка /etc/inetd.conf для FTP сервера?
5. Сетевая файловая система (Network File System)?
6. Настройка сервера и клиента NFS?
7. Администрирование Samba?
8. Администрирование NIS?

Тема 6. Серверы дистанционной регистрации

OpenSSH это набор сетевых инструментов, используемых для защищенного доступа к удаленным компьютерам. Он может быть использован в качестве непосредственной замены rlogin, rsh, rcp и telnet.

Кроме того, через SSH могут быть безопасно туннелированы и/или перенаправлены произвольные TCP/IP соединения. OpenSSH шифрует весь трафик, эффективно предотвращая кражу данных, перехват соединения и другие сетевые атаки.

OpenSSH в ряде ОС основан на SSH v1.2.12 со всеми последними исправлениями и обновлениями, совместим с протоколами SSH версий 1 и 2.

Обычно при использовании telnet(1) или rlogin(1) данные пересылаются по сети в незашифрованной форме. Перехватчик пакетов в любой точке сети между клиентом и сервером может похитить информацию о пользователе/пароле или данные, передаваемые через соединение. Для предотвращения этого OpenSSH предлагает различные методы шифрования.

Даемон sshd должен быть разрешен в процессе инсталляции. За запуск ответственна следующая строка в файле rc.conf:

sshd_enable="YES"

При следующей загрузке системы будет запущен sshd(8), даемон для OpenSSH. Вы можете также воспользоваться скриптом /etc/rc.d/sshd системы rc(8) для запуска OpenSSH:

/etc/rc.d/sshd start

SSH клиент

Утилита ssh(1) работает подобно rlogin(1).

ssh user@example.com

Host key not found from the list of known hosts.

Are you sure you want to continue connecting (yes/no)? yes

Host 'example.com' added to the list of known hosts.

user@example.com's password: *******

Вход продолжится так же, как если бы сессия была инициирована с использованием rlogin или telnet. SSH использует систему опознавательных ключей для проверки подлинности сервера при подключении клиента. Пользователю предлагается yes только при первом подключении. Дальнейшие попытки входа предваряются проверкой сохраненного ключа сервера. SSH клиент сообщит вам, если сохраненный ключ будет отличаться от только что полученного. Ключи серверов сохраняются в ~/.ssh/known_hosts, или в ~/.ssh/known_hosts2 для SSH v2.

По умолчанию современные серверы OpenSSH настроены на приём только соединений SSH v2. Клиент будет использовать версию 2 там, где это возможно, а затем версию 1. Также, клиент можно заставить использовать конкретную версию при помощи опций -1 и -2 для указания соответствующей версии протокола. Версия 1 поддерживается ради совместимости со старыми серверами.

Команда scp(1) работает подобно rcp(1); она копирует файл с удаленного компьютера, но делает это безопасным способом.

```
# scp user@example.com:/COPYRIGHT COPYRIGHT
user@example.com's password: *******
COPYRIGHT                     100% |*****************************|  4735
00:00
#
```

Поскольку в предыдущем примере ключ сервера уже был сохранен, в этом примере он проверяется при использовании scp(1).

Параметры, передаваемые scp(1), похожи на параметры cp(1), с файлом или файлами в качестве первого аргумента и приемником копирования во втором. Поскольку файлы файлы передаются по сети через SSH, один или более аргументов принимают форму user@host:<path_to_remote_file>.

Системные файлы настройки для даемона и клиента OpenSSH расположены в каталоге /etc/ssh.

Файл ssh_config используется для настройки клиента, а sshd_config для даемона.

Кроме того, параметры sshd_program (по умолчанию /usr/sbin/sshd), и sshd_flags rc.conf дают дополнительные возможности настройки.

Вместо использования паролей, с помощью ssh-keygen(1) можно создать ключи DSA или RSA, которыми пользователи могут аутентифицироваться:

```
% ssh-keygen -t dsa
Generating public/private dsa key pair.
Enter file in which to save the key (/home/user/.ssh/id_dsa):
Created directory '/home/user/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/user/.ssh/id_dsa.
Your public key has been saved in /home/user/.ssh/id_dsa.pub.
The key fingerprint is:
bb:48:db:f2:93:57:80:b6:aa:bc:f5:d5:ba:8f:79:17 user@host.example.com
```

ssh-keygen(1) создаст пару публичного и приватного ключей, используемых для аутентификации. Приватный ключ сохраняется в ~/.ssh/id_dsa или ~/.ssh/id_rsa, а публичный в ~/.ssh/id_dsa.pub или ~/.ssh/id_rsa.pub (для ключей DSA и RSA соответственно). Для включения аутентификации по ключам публичный ключ должен быть помещен в файл ~/.ssh/authorized_keys на удаленном компьютере.

Это позволяет соединяться с удаленным компьютером с помощью SSH-ключей вместо паролей.

Если при генерации ключей был использован пароль, каждый раз для при использовании приватного ключа он будет запрашиваться у пользователя. Для того, чтобы избежать непрерывного набора кодовой

фразы, можно использовать утилиту ssh-agent(1), как описано в разделе Разд. 14.11.7 ниже.

Параметры и имена файлов могут различаться для разных версий OpenSSH, установленных в системе, для решения проблем обратитесь к странице справочника ssh-keygen(1).

Утилиты ssh-agent(1) и ssh-add(1) позволяют сохранять ключи SSH в памяти, чтобы не набирать кодовые фразы при каждом использовании ключа.

Утилита ssh-agent(1) обеспечивает процесс аутентификации загруженными в нее секретными ключами; для этого утилита ssh-agent(1) должна запустить внешний процесс. В самом простом случае это может быть шелл-процесс; в чуть более продвинутом -- оконный менеджер.

Для использования ssh-agent(1) совместно с шеллом, ssh-agent(1) должен быть запущен с именем этого шелла в качестве аргумента. После этого в его память при помощи утилиты ssh-add(1) могут быть добавлены необходимые ключи; при этом будут запрошены соответствующие кодовые фразы. Добавленные ключи могут затем использоваться для ssh(1) на машины, на которых установлены соответствующие публичные ключи:

```
% ssh-agent csh
% ssh-add
Enter passphrase for /home/user/.ssh/id_dsa:
Identity added: /home/user/.ssh/id_dsa (/home/user/.ssh/id_dsa)
```

Для того чтобы использовать ssh-agent(1) в X11, вызов ssh-agent(1)должен быть помещен в файл ~/.xinitrc. Это обеспечит поддержкой ssh-agent(1) все программы, запущенные в X11. Файл ~/.xinitrc может выглядеть, например, так:

```
exec ssh-agent startxfce4
```

При этом будет запущен ssh-agent(1), который, в свою очередь, вызовет запуск XFCE, при каждом старте X11. После запуска X11, выполните команду ssh-add(1) для добавления ваших SSH-ключей.

OpenSSH поддерживает возможность создания туннеля для пропуска соединения по другому протоколу через защищенную сессию.

Следующая команда указывает ssh(1) создать туннель для telnet:

```
% ssh -2 -N -f -L 5023:localhost:23 user@foo.example.com
```

Команда ssh используется со следующими параметрами:

-2 Указывает ssh использовать версию 2 протокола (не используйте этот параметр, если работаете со старыми SSH серверами).

-N Означает использование в не-командном режиме, только для туннелирования. Если этот параметр опущен, ssh запустит обычную сессию.

-f Указывает ssh запускаться в фоновом режиме.

-L Означает локальный туннель в стиле localport:remotehost:remoteport.

user@foo.example.com

Удаленный сервер SSH.

Туннель SSH создается путем создания прослушивающего сокета на определенном порту localhost. Затем все принятые на локальном хосту/порту соединения переправляются на через SSH на определенный удаленный хост и порт.

В этом примере, порт 5023 на localhost перенаправляется на порт 23 на localhost удаленного компьютера. Поскольку 23 это порт telnet, будет создано защищенное соединение telnet через туннель SSH.

Этот метод можно использовать для любого числа небезопасных протоколов, таких как SMTP, POP3, FTP, и так далее.

Пример bспользование SSH для создания защищенного туннеля на SMTP

% ssh -2 -N -f -L 5025:localhost:25 user@mailserver.example.com

user@mailserver.example.com's password: *****

% telnet localhost 5025

Trying 127.0.0.1...

Connected to localhost.

Escape character is '^]'.

220 mailserver.example.com ESMTP

Этот метод можно использовать вместе с ssh-keygen(1) и дополнительными пользовательскими учётными записями для создания более удобного автоматического SSH туннелирования. Ключи могут быть использованы вместо паролей, и туннели могут запускаться от отдельных пользователей.

На работе находится SSH сервер, принимающий соединения снаружи. В этой же офисной сети находится почтовый сервер, поддерживающий протокол POP3. Сеть или сетевое соединение между вашим домом и офисом могут быть или не быть полностью доверяемыми. По этой причине вам потребуется проверять почту через защищенное соединение. Решение состоит в создании SSH соединения к офисному серверу SSH и туннелирование через него к почтовому серверу.

% ssh -2 -N -f -L 2110:mail.example.com:110 user@ssh-server.example.com

user@ssh-server.example.com's password: ******

Когда туннель включен и работает, вы можете настроить почтовый клиент для отправки запросов POP3 на localhost, порт 2110. Соединение будет безопасно переправлено через туннель на mail.example.com.

Некоторые сетевые администраторы устанавливают на брандмауэрах драконовские правила, фильтруя не только входящие соединения, но и исходящие. Вам может быть разрешен доступ к удаленным компьютерам только по портам 22 и 80, для SSH и просмотра сайтов.

Вам может потребоваться доступ к другому (возможно, не относящемуся к работе) сервису, такому как Ogg Vorbis для прослушивания музыки. Если этот сервер Ogg Vorbis выдает поток не с портов 22 или 80, вы не сможете получить к нему доступ.

Решение состоит в создании SSH соединения с компьютером вне брандмауэра и использование его для туннелирования сервера Ogg Vorbis.

% ssh -2 -N -f -L 8888:music.example.com:8000 user@unfirewalled-system.example.org

user@unfirewalled-system.example.org's password: *******

Клиентскую программу теперь можно настроить на localhost порт 8888, который будет перенаправлен на music.example.com порт 8000, успешно обойдя брандмауэр.

Зачастую хорошие результаты даёт ограничение того, какие именно пользователи и откуда могут регистрироваться в системе. Задание параметра AllowUsers является хорошим способом добиться этого. К примеру, для разрешения регистрации только пользователю root с машины 192.168.1.32, в файле /etc/ssh/sshd_config нужно указать нечто вроде следующего:

AllowUsers root@192.168.1.32

Для разрешения регистрации пользователя admin из любой точки, просто укажите имя пользователя: AllowUsers admin

Несколько пользователей должны перечислять в одной строке, как здесь:

AllowUsers root@192.168.1.32 admin

Замечание: Важно, чтобы бы перечислили всех пользователей, которые должны регистрироваться на этой машине; в противном случае они будут заблокированы.

После внесения изменений в /etc/ssh/sshd_config вы должны указать sshd(8) на повторную загрузку конфигурационных файлов, выполнив следующую команду:

/etc/rc.d/sshd reload

Машина может загружаться по сети и работать без наличия локального диска, используя файловые системы, монтируемые с сервера NFS.

Способы загрузки ядра по сети:

- PXE: Система Intel® Preboot eXecution Environment является формой загрузочного ПЗУ, встроенного в некоторые сетевые адаптеры или материнские платы. pxeboot(8) для получения более полной информации.
- Порт Etherboot (net/etherboot) генерирует код, который может применяться в ПЗУ для загрузки ядра по сети. Код может быть либо прошит в загрузочный PROM на сетевом адаптере, либо

загружен с локальной дискеты (или винчестера), или с работающей системы MS-DOS.

- Примерный скрипт (/usr/share/examples/diskless/clone_root) облегчает создание и поддержку корневой файловой системы рабочей станции на сервере. Скрипт, скорее всего, потребует некоторых настроек, но он позволит вам быстро начать работу.
- Стандартные файлы начального запуска системы, располагающиеся в /etc, распознают и поддерживают загрузку системы в бездисковом варианте.
- Подкачка, если она нужна, может выполняться через файл NFS либо на локальный диск.

Варианты полной настройки системы.

Корневая файловая система является копией стандартной корневой системы (обычно сервера), с некоторыми настроечными файлами, измененными кем-то специально для бездисковых операций или, возможно, для рабочей станции, которой она предназначена.

Части корневой файловой системы, которые должны быть доступны для записи, перекрываются файловыми системами md(4). Любые изменения будут потеряны при перезагрузках системы.

Ядро передается и загружается посредством Etherboot или PXE, и в некоторых ситуациях может быть использован любой из этих методов.

Настройка бездисковых рабочих станций относительно проста, но в то

Для выполнения успешной загрузки необходимо произвести несколько операций: компьютеру необходимо получить начальные параметры, такие как собственный IP адрес, имя исполняемого файла, корневой каталог. Для этого используются протоколы DHCP или BOOTP. DHCP это совместимое расширение BOOTP, используются те же номера портов и основной формат пакетов.

Возможна настройка системы для использования только BOOTP. Серверная программа bootpd(8) включена в основную систему.

У DHCP есть множество преимуществ над BOOTP (лучше файлы настройки, возможность использования PXE, плюс многие другие преимущества, не относящиеся непосредственно к бездисковым операциям), и мы в основном будем описывать настройку DHCP, с эквивалентными примерами для bootpd(8), когда это возможно.

Компьютеру требуется загрузить в локальную память одну или несколько программ. Используются TFTP или NFS. Выбор между TFTP или NFS производится во время компилирования в нескольких местах. Часто встречающаяся ошибка это указание имен файлов для другого протокола: TFTP обычно загружает все файлы с одного каталога сервера, и принимает имена файлов относительно этого каталога. NFS нужны абсолютные пути к файлам.

Необходимо инициализировать и выполнить возможные промежуточные программы загрузки и ядро. В этой области существует несколько важных вариаций:

- PXE загрузит pxeboot(8), являющийся модифицированной версией загрузчика третьей стадии FreeBSD. loader(8) получит большинство параметров, необходимых для старта системы, и оставит их в окружении ядра до контроля передачи. В этом случае возможно использование ядра GENERIC.
- Etherboot, непосредственно загрузит ядро, с меньшей подготовкой. Вам потребуется собрать ядро со специальными параметрами.
- PXE и Etherboot работают одинаково хорошо; тем не менее, поскольку ядро обычно позволяет loader(8) выполнить больше предварительной работы, метод PXE предпочтителен.

Если ваш BIOS и сетевые карты поддерживают PXE, используйте его.

Наконец, компьютеру требуется доступ к файловым системам. NFS используется во всех случаях. Страница справочника diskless(8).

Сервер ISC DHCP может обрабатывать как запросы BOOTP, так и запросы DHCP.

После установки ISC DHCP ему для работы требуется конфигурационный файл (обычно называемый /usr/local/etc/dhcpd.conf).

Пример.

```
default-lease-time 600;
max-lease-time 7200;
authoritative;
option domain-name "example.com";
option domain-name-servers 192.168.4.1;
option routers 192.168.4.1;
subnet 192.168.4.0 netmask 255.255.255.0 {
  use-host-decl-names on;
  option subnet-mask 255.255.255.0;
  option broadcast-address 192.168.4.255;

  host margaux {
    hardware ethernet 01:23:45:67:89:ab;
    fixed-address margaux.example.com;
    next-server 192.168.4.4;
    filename "/data/misc/kernel.diskless";
    option root-path "192.168.4.4:/data/misc/diskless";
  }
  host corbieres {
    hardware ethernet 00:02:b3:27:62:df;
    fixed-address corbieres.example.com;
```

```
    next-server 192.168.4.4;
    filename "pxeboot";
    option root-path "192.168.4.4:/data/misc/diskless";
  }
}
```

use-host-decl-names on

Параметр указывает dhcpd посылать значения деклараций host как имя хоста для бездисковой машины. Альтернативным способом было бы добавление option host-name *margaux* внутри объявлений host.

next-server 192.168.4.4

Директива next-server определяет сервер TFTP или NFS, используемый для получения загрузчика или файла ядра (по умолчанию используется тот же самый хост, на котором расположен сервер DHCP).

filename "/data/misc/kernel.diskless"

Директива filename определяет файл, который Etherboot или PXE будут загружать для следующего шага выполнения. Он должен быть указан в соответствии с используемым методом передачи. Etherboot может быть скомпилирован для использования NFS или TFTP. FreeBSD порт по умолчанию использует NFS. PXE использует TFTP, поэтому здесь применяются относительные пути файлов (это может зависеть от настроек TFTP сервера, но обычно довольно типично). Кроме того, PXE загружает pxeboot, а не ядро. Существуют другие интересные возможности, такие как загрузка pxeboot из каталога /boot FreeBSD CD-ROM (поскольку pxeboot(8) может загружать GENERIC ядро, это делает возможной загрузку с удаленного CD-ROM).

option root-path "192.168.4.4:/data/misc/diskless"

Параметр root-path определяет путь к корневой файловой системе, в обычной нотации NFS. При использовании PXE, можно оставить IP хоста отключенным, если параметр ядра BOOTP не используется. Затем NFS сервер может использоваться так же, как и TFTP.

Конфигурация с использованием bootpd , располагаться в /etc/bootptab.

Etherboot должен быть откомпилирован с нестандартной опцией NO_DHCP_SUPPORT для того, чтобы можно было использовать BOOTP, и что для работы PXE необходим DHCP.

```
.def100:\
  :hn:ht=1:sa=192.168.4.4:vm=rfc1048:\
  :sm=255.255.255.0:\
  :ds=192.168.4.1:\
  :gw=192.168.4.1:\
  :hd="/tftpboot":\
  :bf="/kernel.diskless":\
```

:rp="192.168.4.4:/data/misc/diskless":

margaux:ha=0123456789ab:tc=.def100

Изменить настройку Etherboot путем редактирования файла Config в каталоге исходных текстов Etherboot.

Для создания загрузочной дискеты, вставьте дискету в дисковод на машине, где установлен Etherboot, затем перейдите в каталог src в дереве Etherboot и наберите: gmake bin32/devicetype.fd0

devicetype зависит от типа адаптера Ethernet на бездисковой рабочей станции. Обратитесь к файлу NIC в том же самом каталоге для определения правильного значения для devicetype.

По умолчанию, pxeboot(8) загружает ядро через NFS. Он может быть скомпилирован для использования вместо него TFTP путем указания параметра LOADER_TFTP_SUPPORT в /etc/make.conf.

Есть два не документированных параметра make.conf, которые могут быть полезны для настройки бездискового компьютера с последовательной консолью: BOOT_PXELDR_PROBE_KEYBOARD, и BOOT_PXELDR_ALWAYS_SERIAL.

Для использования PXE при загрузке компьютера потребуется выбрать параметр Boot from network (загрузка по сети) в настройках BIOS, или нажать функциональную клавишу во время загрузки PC.

PXE или Etherboot, настроенные для использования TFTP - нужно включить tftpd на файловом сервере:

- Создайте каталог, файлы которого будет обслуживать tftpd, например, /tftpboot.
- Добавьте в ваш /etc/inetd.conf такую строчку:
- tftp dgram udp wait root /usr/libexec/tftpd tftpd -l -s /tftpboot
- Сообщите inetd о необходимости перечитать свой файл конфигурации. Файл /etc/rc.conf должен содержать строку inetd_enable="YES" для корректного исполнения команды
- # /etc/rc.d/inetd restart
- Поместить каталог tftpboot в любом месте на сервере.
- Проверить, что это местоположение указано как в inetd.conf, так и в dhcpd.conf.
- Включить NFS и экспортировать соответствующую файловую систему на сервере NFS.
- Добавьте следующее в /etc/rc.conf:
- nfs_server_enable="YES"
- Экспортируйте файловую систему, в которой расположен корневой каталог для бездисковой рабочей станции, добавив следующую строку в /etc/exports (подправьте точку

монтирования и замените margaux corbieres именами бездисковых рабочих станций):

- /data/misc -alldirs -ro margaux corbieres
- Заставьте mountd перечитать настроечный файл. На самом деле если вам потребовалось на первом шаге включить NFS в /etc/rc.conf, то вам нужно будет выполнить перезагрузку.
- # /etc/rc.d/mountd restart

При использовании Etherboot, потребуется создать конфигурационный файл ядра для бездискового клиента со следующими параметрами (вдобавок к обычным):

options BOOTP # Use BOOTP to obtain IP address/hostname

options BOOTP_NFSROOT # NFS mount root filesystem using BOOTP info

Вам может потребоваться использовать BOOTP_NFSV3, BOOT_COMPAT и BOOTP_WIRED_TO (посмотрите файл NOTES).

Эти имена параметров сложились исторически, и могут немного ввести в заблуждение, поскольку включают необязательное использование DHCP и BOOTP в ядре (возможно включение обязательного использования BOOTP или DHCP use).

При использовании PXE, сборка ядра с вышеприведенными параметрами не является совершенно необходимой (хотя желательна). Включение этих параметров приведет к выполнению большинства DHCP запросов во время загрузки ядра, с небольшим риском несоответствия новых значений и значений, полученных pxeboot(8) в некоторых особых случаях. Преимущество использования в том, что в качестве побочного эффекта будет установлено имя хоста. Иначе вам потребуется установить имя хоста другим методом, например в клиент-специфичном файле rc.conf.

Для включения возможности загрузки с Etherboot, в ядро необходимо включить устройство hints. Вам потребуется установить в файле конфигурации следующий параметр:

hints "GENERIC.hints"

Создать корневую файловую систему для бездисковых рабочих станций, в местоположении, заданном как root-path в dhcpd.conf.

Использование процедуры make world.

Этот метод установит новую систему в DESTDIR. Вполнить скрипт:

```
#!/bin/sh
export DESTDIR=/data/misc/diskless
mkdir -p ${DESTDIR}
cd /usr/src; make buildworld && make buildkernel
cd /usr/src/etc; make distribution
```

Настроить /etc/rc.conf и /etc/fstab, помещенные в DESTDIR, в соответствии с вашими потребностями.

Если это нужно, то файл подкачки, расположенный на сервере, можно использовать посредством NFS.

Подкачка через NFS.

На стадии загрузки ядро не поддерживает подкачку через NFS.

Подкачка должна быть разрешена при помощи загрузочных скриптов, монтирующих файловую систему, пригодную для записи и создающих на ней файл подкачки. Для создания файла подкачки выполнить следующие команды:

dd if=/dev/zero of=/path/to/swapfile bs=1k count=1 oseek=100000

Для активации этого файла подкачки следует добавить в файл rc.conf строку

swapfile=/path/to/swapfile

Если бездисковая рабочая станция настроена на запуск X, вам нужно подправить настроечный файл для XDM, который по умолчанию помещает протокол ошибок в /usr.

Если сервер с корневой файловой системой работает не под управлением FreeBSD, вам потребуется создать корневую файловую систему на машине FreeBSD, а затем скопировать ее в нужно место, при помощи tar или cpio.

В такой ситуации иногда возникают проблемы со специальными файлами в /dev из-за различной разрядности целых чисел для старшего/младшего чисел.

Решением этой проблемы является экспортирование каталога с постороннего сервера, монтирование его на конкретной машине и использование devfs(5) для создания файлов устройств прозрачно для пользователя.

Контрольные вопросы

1. Использование SSH?
2. Конфигурирование rc.conf?
3. Запуск скрипта /etc/rc.d/sshd?
4. Клиент SSH?
5. Утилита ssh?

Тема 7. Введение в Microsoft Windows Server® 2008

Microsoft Windows Server® 2008 – операционная система, которая помогает ИТ-специалистам полностью контролировать инфраструктуру, обеспечивая доступность и управляемость, что позволяет достичь более высокого уровня безопасности, надежности и устойчивости серверной

среды. ОС Windows Server® 2008 предоставляет пользователям, независимо от их местонахождения, доступ к полному набору сетевых услуг.

Редакции Windows Server® 2008

В семейство операционных систем Windows Server® 2008 входят несколько редакций. У каждой версии есть назначение, но все они поддерживают основные возможности, необходимые для решения задач, которые возникают в работе ИТ-систем и организаций любого размера:

- Windows Server® 2008 Foundation — это недорогое и экономичное техническое решение для бизнеса. Данная редакция предназначена для владельцев небольших компаний и ИТ-специалистов, занимающихся их поддержкой. Это недорогая, удобная в развертывании и надежная платформа, на которой можно запускать распространенные бизнес-приложения и обеспечивать общий доступ к информации и ресурсам.
- Windows Server® 2008 Standard — это самая надежная операционная система из семейства Windows Server на настоящее время. Эта система имеет встроенный веб-сервер и возможности виртуализации. Она поможет повысить надежность и гибкость серверной инфраструктуры при снижении расходов и экономии времени. Мощные инструменты обеспечивают более удобное управление серверами, упрощают настройку и управление. Надёжные средства безопасности этой операционной системы защищают сети и данные, что даёт возможность построить исключительно прочный фундамент для ИТ-среды бизнеса.
- Windows Server 2008® Enterprise — это мощная серверная платформа, обеспечивающая надежную поддержку для самых важных процессов и нагрузок. В этой редакции предусмотрены расширенные возможности виртуализации, экономии электроэнергии; улучшена управляемость; мобильные сотрудники могут проще получать доступ к ресурсам компании.
- Windows Server 2008 Datacenter является платформой корпоративного уровня для важнейших бизнес-приложений и крупномасштабной виртуализации на небольших или мощных серверах.

  Эта редакция отличается повышенной доступностью, улучшенным управлением электропитанием и встроенными решениями для мобильных сотрудников и работников филиалов. Эта редакция также включает неограниченные

лицензионные права на виртуальные системы, что позволяет значительно сократить затраты на инфраструктуру путем консолидации приложений. Данная редакция поддерживает от 2 до 64 процессоров.

- Windows Web Server 2008 представляет собой мощную платформу для веб-приложений и веб-служб. Эта редакция содержит службы Internet Information Services (IIS) и предназначена исключительно для интернет-серверов; в ней предусмотрены улучшенные средства администрирования и диагностики, позволяющие снизить затраты при использовании с несколькими популярными платформами разработки. Эта платформа поддерживает роли веб-сервера и DNS-сервера, обладает повышенной надежностью и масштабируемостью и обеспечивает управление в самых разных средах, от отдельного веб-сервера до фермы веб-серверов.
- Windows HPC Server 2008 принадлежит к следующему поколению высокопроизводительных вычислительных систем и предоставляет средства уровня промышленного предприятия для создания высокопроизводительной вычислительной среды. Средства масштабирования Windows HPC Server 2008 обеспечивают поддержку тысяч процессорных ядер и содержат консоли управления, помогающие выполнять проактивный мониторинг и поддерживать работоспособность и стабильность системы. Гибкость и широкие возможности взаимодействия, предоставляемые средствами планирования, обеспечивают интеграцию с высокопроизводительными вычислительными платформами на базе Windows и Linux и поддерживают приложения с сервис-ориентированной архитектурой (SOA) и пакетное выполнение приложений.
- Windows Server 2008 для систем на базе процессоров Itanium представляет собой платформу корпоративного уровня для важнейших бизнес-приложений. Эта платформа поддерживает крупные СУБД, бизнес-приложения и системы, разработанные на заказ, и отвечает всем потребностям растущего бизнеса. Для повышения доступности служит поддержка отказоустойчивых кластеров и возможности динамического аппаратного секционирования*. Поддерживается развертывание виртуальных экземпляров Windows Server (без ограничения их количества)**.

* Требуется серверное оборудование, поддерживающее такую функцию.

** Требуется технология виртуализации сторонних разработчиков. Виртуализация Hyper-VTM недоступна для систем на базе процессоров Itanium.

Роли, службы ролей и компоненты Windows Server 2008

Архитектура Windows Server 2008 отличается от предшествующих ОС. Готовя сервер к развёртыванию, вы устанавливаете и настраиваете следующие модули:

- **Роль сервера** — Связанный набор программ, позволяющий серверу выполнять определённую функцию по обслуживанию пользователей и других компьютеров. Сервер может быть выделен для одной роли, например, «Доменные службы Active Directory», а может выполнять и несколько ролей.
- **Служба роли** — Программа, обеспечивающая функциональность роли сервера. С каждой ролью сервера связана одна или несколько служб. Некоторые роли сервера, например DNS и DHCP, выполняют строго определённую функцию, которая устанавливается при установке роли. Другие роли, например, «Службы политики сети и доступа» и «Службы сертификации Active Directory», имеют несколько служб ролей, которые можно устанавливать по выбору.
- **Компонент** — Программный модуль, обеспечивающий дополнительную функциональность ОС. Компоненты, например, «BitLocker Drive Encryption» и «Windows Power Shell», устанавливаются и удаляются отдельно от ролей и служб ролей. На компьютере в зависимости от конфигурации может быть установлено несколько компонентов, а может не быть и ни одного.

Основные **роли** и связанные с ними **службы**, которые можно развёртывать на сервере Windows Server 2008:

DHCP-сервер — Предоставляет возможность централизованного управления IP-адресами. DHCP-серверы выдают динамические IP-адреса и назначают основные параметры TCP/IP другим компьютерам сети. Не включает дополнительных служб и ролей.

DNS-сервер. DNS — система разрешения имён, сопоставляющая имена компьютеров с их IP-адресами. Серверы DNS являются неотъемлемой частью системы разрешения имён в доменах Active Directory. Не включает дополнительных служб и ролей.

Веб-сервер (IIS) — Используется для размещения веб-сайтов и веб-приложений. Веб-сайты, размещённые на веб-сервере, могут включать как статическое, так и динамическое содержимое. Веб-приложения, размещённые на веб-сервере, могут создаваться с использованием ASP.NET и .NET Framework. При развёртывании веб-сервера можно управлять конфигурацией сервера при помощи модулей IIS и административных модулей.

Доменные службы Active Directory — Предоставляет функции хранения информации о пользователях, группах, компьютерах и других объектах сети, а так же делает эту информацию доступной пользователям и компьютерам. Контроллеры домена AD предоставляют сетевым пользователям и компьютерам доступ к разрешённым ресурсам сети.

Сервер приложений — Позволяет размещать на сервере распределённые приложения, написанные с использованием .NET Framework. Включает более десятка ролей и служб.

Службы Active Directory облегчённого доступа к каталогам — Предоставляет хранилище данных для приложений с поддержкой каталога, которым не требуются службы каталога AD DS и развёртывание на контроллерах домена. Не включает дополнительных служб ролей.

Службы UDDI — Предоставляет возможность общего доступа к информации о веб-службах, как в одной сети, так и между сетями. Включает следующие службы ролей: «База данных служб UDDI» и «Веб-приложение служб UDDI».

Службы печати — Предоставляет основные службы для управления сетевыми принтерами и драйверами печати. Включает следующие службы ролей: «Сервер печати», «Служба LDP» и «Печать через Интернет»

Службы политики сети и доступа — Предоставляет основные службы для управления маршрутизацией и удалённым доступом. Включает следующие службы ролей: «Сервер политики сети», «Службы маршрутизации и удалённого доступа», «Служба удалённого доступа», «Маршрутизация», «Центр регистрации работоспособности» и «Протокол авторизации учётных данных узла».

Службы развёртывания Windows — Предоставляет службы для развёртывания в сети компьютеров под управлением Windows. Включает

следующие службы ролей: «Сервер развёртывания» и «Транспортный сервер».

Службы сертификации Active Directory — Предоставляет функции выдачи и отзыва цифровых сертификатов пользователей, клиентских компьютеров и серверов. Включает следующие службы ролей: «Центр сертификации», «Служба подачи заявок в центр сертификации через Интернет», «Сетевой ответчик» и «Служба подачи заявок на сетевые устройства».

Службы терминалов — Предоставляет службы, позволяющие пользователям запускать Windows-приложения, установленные на удалённом сервере. Когда пользователь запускает приложение на сервере терминалов, запуск и обработка данных происходят на сервере, а по сети передаются только данные приложения. Включает следующие службы ролей: «Сервер терминалов», «Лицензирование служб терминалов», «Посредник сеансов служб терминалов», «Шлюз служб терминалов» и «Веб-доступ к службам терминалов».

Службы управления правами Active Directory — Предоставляет управляемый доступ к защищённым сообщениям электронной почты, документа, веб-страницам интрасети и файлам иных типов. Включает следующие службы ролей: «Сервер управления правами Active Directory» и «Поддержка федерации удостоверений».

Службы федерации Active Directory — Дополняет функции проверки подлинности и управления доступом AD DS, распространяя их на Интернет. Включает следующие службы ролей и подслужбы: «Служба федерации», «Прокси-агент службы федерации», «Веб-агенты», «Агент, поддерживающий утверждения» и «Агент Windows на основе маркеров».

Файловые службы — Предоставляет базовые службы для управления файлами, а также обеспечивает их доступность и репликацию в сети. Некоторым ролям сервера необходима файловая служба определённого типа. Включает следующие службы ролей и подслужбы: «Файловый сервер», «Распределённая файловая система DFS (Distributed File System)», «Пространства имён DFS», «Репликация DFS», «Диспетчер ресурсов файлового сервера», «Службы для NFS», «Служба поиска Windows», «Файловые службы Windows Server 2003», «Служба репликации файлов» и «Служба индексирования».

Факс-сервер — Обеспечивает централизованное управление отправкой и получением факсов в сети. Сервер факсов может действовать как шлюз

для отправки и получения факсов и позволяет управлять ресурсами факса, например, задачами и отчётами, а так же устройствами для отправки факсов, подключёнными к серверу и другим компьютерам сети. Не включает дополнительных служб ролей.

В таблице 1 приведено сравнение редакций Windows Server 2008 по доступности ролей сервера.

Таблица 1. Сравнение редакций по ролям сервера

Роль сервера	Datacenter	Enterprise	Standard	Foundation	Web	HPC	Itanium
DHCP-сервер	+	+	+	+	-	+	-
DNS-сервер	+	+	+	+	+	+	-
Hyper-V	+	+	+	-	-	+	-
Windows Server Update Services	+	+	+	+	-	+	-
Веб-сервер (IIS)	+	+	+	+	+	+	+
Доменные службы AD	+	+	+	+	-	+	-
Сервер приложений	+	+	+	+	-	-	+
Службы облегченного доступа к каталогам Active Directory	+	+	+	+	-	-	-
Службы печати	+	+	+	+	-	-	-
Службы политики сети и доступа	+	+	+[1]	+[2]	-	+[1]	-
Службы развёртывания Windows	+	+	+	+	-	+	-
Службы сертификации AD	+	+	+[3]	+[3]	-	+[3]	-
Службы терминалов	+	+	+[4]	+[5]	-	+[4]	-
Службы управления правами AD	+	+	+	+	-	-	-
Службы федерации AD	+	+	-	-	-	-	-
Файловые службы	+	+	+[6]	+[6]	-	+[6]	-
Факс-сервер	+	+	+	+	-	-	-

1 - не более 250 подключений RRAS, 50 подключений IAS и двух групп серверов IAS.

2 - не более 50 подключений RRAS, 10 подключений IAS.

3 - ограничение: можно создавать только центры сертификации, другие компоненты ADCS недоступны (NDES, служба сетевых ответчиков). Дополнительные сведения см. в документации о роли ADCS в сети TechNet.

4 - не более 250 подключений к удаленным рабочим столам.

5 - не более 50 подключений к удаленным рабочим столам.

6 - ограничение: один автономный корень DFS.

Системные требования

Для работы с Windows Server® 2008 компьютер должен удовлетворять требованиям, указанным в таблице 2*.

Таблица 2 Системные требования для Windows Server 2008

Компонент	Требование
Процессор	Минимум: 1 ГГц (процессор с архитектурой x86) или 1,4 ГГц (процессор с архитектурой x64). Для работы с Windows Server 2008 R2 for Itanium-Based Systems необходим процессор Intel Itanium 2.
Память	Минимальный объем: 512 МБ. Максимальный объем для (32-битных систем): 4 ГБ (Standard) или 64 ГБ (Enterprise and Datacenter) Максимальный объем для (64-битных систем): 8 ГБ (Foundation), 32 ГБ (Standard), 2 ТБ (Enterprise, Datacenter и Itanium-Based Systems).
Пространство на HDD	Минимальный объем для (32-битных систем): 20 ГБ. Минимальный объем для (64-битных систем): 32 ГБ. Foundation — 10 ГБ или более. На компьютерах, оснащенных более чем 16 ГБ ОЗУ, потребуется больше места на диске для файлов подкачки, спящего режима и дампа памяти.
Монитор	Монитор с разрешением Super VGA (800x600) или более высоким.
Прочее	Дисковод для DVD-дисков, клавиатура и мышь (Майкрософт) или совместимое указывающее устройство

*Фактические требования к системе зависят от конфигурации системы и от выбранных для установки приложений и компонентов. Производительность процессора зависит не только от его тактовой частоты, но и от числа ядер и объема кэша процессора. Необходимый объем свободного дискового пространства в системном разделе указан приблизительно. При установке по сети может потребоваться дополнительное место на диске.

Контрольные вопросы

1. Назвать редакции ОС Server 2008?

2. Назначения редакций ОС Server 2008?
3. Назвать роли ОС Server 2008?
4. Назначения ролей ОС Server 2008?
5. Системные требования ОС Server 2008?

Тема 8. Установка ролей Active Directory и DNS

Для этого необходимо установить роль «Доменные службы Active Directory. Т.к. начальная настройка завершена, можно закрыть консоль «Задачи начальной настройки», при этом откроется окно «Диспетчер сервера». «Диспетчер сервера» — это новый компонент операционной системы Windows Server® 2008, предоставляющий администраторам удобный интерфейс для установки и настройки ролей сервера и компонентов, которые являются частью Windows Server 2008, и управления ими. Диспетчер сервера запускается автоматически после выполнения задач, перечисленных в окне "Задачи начальной настройки". Если окно «Задачи начальной настройки» закрыто, «Диспетчер сервера» также запускается автоматически при входе администратора на сервер.

Чтобы добавить новую роль серверу, перейти по ссылке «Добавить роли» в разделе «Сводка по ролям» в Диспетчере сервера. Запуститися «Мастер добавления ролей» с перечнем всех доступных ролей данной редакции Windows Server® 2008.

Чтобы сделать сервер контроллером домена, поставить отметку на роли «Доменные службы Active Directory». По окончании установки доменной службы Active Directory было выдано сообщение, что служба установлена, но чтобы сделать сервер полностью функциональным контроллером домена, необходимо использовать «Мастер установки доменных служб Active Directory». Для этого необходимо в меню «Пуск» выбрать пункт «Выполнить…» и набрать в открывшемся окне команду «dcpromo».

После запуска «Мастера установки доменных служб Active Directory» сообщftncz о совместимости операционных систем в области обеспечения безопасности, и задатncz вопрос о создании домена в уже существующем лесу или в новом. Выбрать пункт «Создать новый домен в новом лесу». Далее дать название новому домену и Net BIOS-имя домена. Следующим шагом задать режим работы леса. Active Directory поддерживает несколько режимов работы леса:

Windows 2000 Этот режим предоставляет все возможности доменных служб Active Directory, доступные в операционной системе Windows Server 2000. Если контроллеры домена работают под управлением более поздних версий операционной системы Windows Server, на них могут

быть недоступны некоторые из дополнительных возможностей, поскольку лес будет работать в режиме Windows 2000.

Windows 2003 В этом режиме работы леса каталог поддерживает контроллеры домена, работающие под управлением Windows Server 2008 и Windows Server 2003. Контроллеры домена под управлением Windows Server 2000 и более ранних версий не поддерживаются. Домен, работающий в режиме Windows 2003, имеет доступ ко многим новым функциям Active Directory, включая универсальные группы, вложенность групп, преобразование типов групп и простое переименование контроллера домена.

Windows 2008 В этом режиме каталог поддерживает контроллеры домена, работающие только под управлением Windows Server 2008. Контроллеры домена под управлением Windows Server 2000 и Windows Server 2003 не поддерживаются. Однако взамен я получаю поддержку всех новейших возможностей Active Directory.

Выбрать наиболее продвинутый режим Windows 2008. После выбора режима работы леса предлагается сразу установить роль DNS-сервера. Последний вопрос – задание пароля для администратора режима восстановления служб каталогов. По окончании работы мастера установки доменных служб Active Directory сервер становится полноценным контроллером домена.

Контрольные вопросы

1. Назначение DNS-сервера?
2. Назначение Active Directory?

Тема 9. Установка роли DHCP-сервера

Для того чтобы установить роль DHCP-сервера, в «Диспетчере сервера» выбрать пункт «Добавить роли» и в запустившемся «Мастере добавления ролей» отметить роль «DHCP-сервер». При этом автоматически были определены все сетевые интерфейсы сервера, среди которых нужно отметить те, которые будут обслуживаться будущим DHCP-сервером. Отметить сетевой интерфейс. Далее указать имя родительского домена и IP-адрес основного DHCP-сервера. После необходимо указать настройки WINS-серверов.

WINS (Windows Internet Name Service) — это служба сопоставления NetBIOS-имён компьютеров с IP-адресами узлов. Обычно применяется на серверах, если в сети есть компьютеры под управлением операционной системы Windows 2000 и более ранних версий. В сети таковых

компьютеров не предвидится, поэтому и служба WINS на сервере применяться не будет. Поэтому оставить переключатель в положении «WINS не требуется для приложений в этой сети». Следующим шагом было необходимо указать диапазон IP-адресов, которые будут выдаваться в сети. В диалоговом окне «Добавление области» задать имя области, начальный IP-адрес, конечный IP-адрес и маска подсети (рисунок 3). Выбрать тип подсети «Проводной (срок действия аренды – х дней)». Следующим шагом нужно выбрать режим DHCP-сервера для IP-адресации шестой версии: отключить DHCPv6 режим без запоминания для этого сервера.

В последнем шаге нужно было указать учётные данные для авторизации DHCP-сервера в домене Active Directory. Обычно это учётная запись администратора домен. Перед завершением установки выдается сводная информация по заданным настройкам, чтобы свериться, что всё указано правильно. По завершении установки DHCP-сервера каждый клиент сети будет получать IP-адрес автоматически из заданной области. Чтобы проверить это, подключить клиентский компьютер с динамически назначенным IP-адресом к настроенной сети. И данный компьютер получит от DHCP-сервера первый свободный IP-адрес из заданного диапазона.

Присоединить компьютер в домен. Для этого сначала создать учётную запись нового пользователя на сервере в консоли «Active Directory – пользователи и компьютеры» и присвоить ему пароль. Затем на клиентской машине в Свойствах системы указать, что данный компьютер является членом домена. При этом выдан запрос на ввод имени и пароля пользователя имеющего права на присоединение к домену, т.е. администратора сети и домена. После ввода имени пользователя и пароля выдается сообщение о присоединении компьютера к домену и предложение перезагрузиться, чтобы изменения вступили в силу.

Чтобы повысить безопасность компьютеров в домене, необходимо, чтобы на них были установлены все обновления, распространяемые через систему Windows Update. Но чтобы не предоставлять при этом компьютерам доступа в интернет, требуется установить роль WSUS.

Контрольные вопросы

1. Назначение DHCP-сервера?
2. Назначение пула адресов?
3. Как работает клиент DHCP?

Тема 10. Установка роли WSUS-сервера

Windows Server Update Services (WSUS) — это сервер обновлений операционных систем и продуктов Microsoft®. Сервер обновлений синхронизируется с сайтом Microsoft®, скачивая обновления, которые могут быть распространены внутри корпоративной локальной сети. Это экономит внешний трафик компании и позволяет быстрее устанавливать исправления ошибок и уязвимостей в операционных системах Windows® на рабочих местах, а также позволяет централизованно управлять обновлениями серверов и рабочих станций.

Перед развертыванием серверов обновлений необходимо убедиться в том, что физический или виртуальный сервер поддерживает, по меньшей мере, минимальные системные требования. Эти требования предоставлены в таблице 3:

Таблица 3. Системные требования к серверу для развёртывания WSUS

Комплектующие	Минимальные требования	Рекомендуемые требования
Процессор	1 ГГц	1,5 ГГц или более мощный
Оперативная память	1 ГБ	2 ГБ
Видеоадаптер	Видеоадаптер с 16 МБ и аппаратным ускорением PCI/AGP	
Файл подкачки	Объем, в 1,5 раза превышающий объем физической памяти	
Сетевой адаптер	10 Мбит/с	100 Мбит/с
Подсистема ввода/вывода	Быстрый HDD ATA IDE или SCSI диск на 100 ГБ	
Свободное место	Не менее 1 ГБ свободного места в системном разделе	
	Не менее 2 ГБ свободного места в разделе, в котором будут храниться файлы базы данных	
	Не менее 20 ГБ свободного места в разделе, в котором будет храниться содержимое. Рекомендуется 30 ГБ свободного места	

Например, для нормальной работы сервера обновлений в организации с 25 000 рабочих мест на сервер обновлений достаточно выделить один отдельный физический сервер с процессором не менее Intel Core 2 Quad Q6600 2,4 ГГЦ и 4 ГБ оперативной памяти. А для распространения обновлений на 100 000 рабочих мест лучше всего применять сценарий из

двух идентичных серверов с процессорами Intel Core 2 6600 2,13 ГГЦ и 4 ГБ оперативной памяти объединив их в отказоустойчивый кластер. Для развертывания серверов обновлений не существует единственной рекомендуемой конфигурации оборудования. Все требования к оборудованию и базам данных зависят от того, как организация будет использовать WSUS-сервер. Также, при расчете аппаратной конфигурации для серверов обновлений, стоит руководствоваться количеством компьютеров в организации, частотой синхронизации с клиентскими компьютерами, количеством языков для обновлений клиентских систем, а также выбором между автономной установкой и созданием отказоустойчивых кластеров.

Для того чтобы сервер имел доступ к обновлениям, выпускаемым корпорацией Microsoft, он должен иметь доступ в Интернет. Для этого установить дополнительный сетевой интерфейс с подключением к глобальной сети.

Чтобы установить роль WSUS-сервера, в «Диспетчере сервера» выбрать пункт «Добавить роли» и в запустившемся «Мастере добавления ролей» отметил роль «Windows Server Update Services». При этом предупреждается, что для развёртывания данной роли требуются дополнительные службы ролей.

Среди дополнительных служб ролей видно, что требуется установить ещё и роль Веб-сервера (IIS). Согласиться с установкой всех необходимых служб ролей. Предоставляется краткая сводка по веб-серверу (IIS), и дальше предлагается выбрать службы ролей веб-сервера. Во время установки компонентов роли Windows Server Update Services автоматически запустится диалоговое окно «Мастер установки служб Windows Server Update Services 3.0 с пакетом обновления 2 (SP2)», при помощи которого нужно завершить установку сервера обновлений.

После принятия лицензионного соглашения сообщается, что на сервере не установлен «Распространяемый пакет средства Microsoft Report Viewer 2008». Без этого компонента не возможно будет использовать интерфейс администрирования Windows Server Update Services. И его следует установить после окончания установки WSUS. На следующей странице «Выбор источника обновлений» необходимо указать диск, который будет использоваться в качестве хранилища обновлений, обеспечивая их быструю загрузку на клиентские компьютеры. По умолчанию флажок «Хранить обновления локально» установлен и обновления будут храниться на сервере WSUS в указанном мной месте. Если же снять данный флажок, то клиентские компьютеры будут получать одобренные обновления, подключаясь, непосредственно, к центру обновлений Microsoft.

На следующей странице «Параметры базы данных» необходимо выбрать базу данных, которая будет использоваться WSUS-сервером. На

этом этапе можно выбрать внутреннюю базу данных Windows, которая выбрана по умолчанию, или базу данных SQL сервера на локальном или удаленном компьютере. Оставить установленный по умолчанию вариант «Внутренней базы данных Windows». На странице «Выбор веб-узла» нужно указать веб-сайт, предназначенный для использования сервера WSUS. Если на данном сервере будет расположен только стандартный сайт сервера обновлений, находящийся на порту 80, достаточно установить переключатель на опции «Использовать существующий веб-узел IIS по умолчанию». На последней странице выдается сводная информация о выставленных настройках. Если всё верно, начинается сам процесс установки.

По окончании установки WSUS автоматически запускается диалоговое окно «Мастер настройки Windows Server Update Services», при помощи которого можно указать первоначальные настройки для данного сервера. При помощи данного мастера можно настроить сетевое подключение, выбрать языки и продукты, предназначенные для обновлений, а также настроить синхронизацию. Данный мастер предлагает завершить первоначальную настройку всего лишь за 8 шагов.

На первом шаге предлагается повысить качество, надежность и производительность программного обеспечения корпорации Microsoft, приняв свое участие в программе улучшения качества Центра обновлений Microsoft. Это означает, что WSUS-сервер будет отправлять в корпорацию Microsoft такие сведения как количество компьютеров организации, которые подключены к серверу WSUS, информацию об удачных и неудачных обновлениях компьютеров и прочую информацию. На втором шаге нужно выбрать источник обновлений для текущего сервера. Если данный сервер является единственным в организации, то нужно установить переключатель на опцию «Синхронизовать с центром обновления Майкрософт» и никакой дополнительной информации заполнять не нужно. Если же данный сервер не является единственным и в организации еще присутствует вышестоящий WSUS-сервер, необходимо установить флажок на опции «Синхронизовать с другим сервером Windows Server Update Services», указать в соответствующих текстовых полях имя сервера и порт, который данный сервер будет использовать для взаимодействия с вышестоящим сервером. Также, при необходимости, если для синхронизации серверы будут использовать порт 443, нужно установить флажок «Использовать SSL при синхронизации данных об обновлениях». Так как в данном примере WSUS-сервер является единственным сервером обновлений в организации, установить переключатель на опции «Синхронизовать с центром обновления Майкрософт» и нажать на кнопку «Далее».

На третьем шаге страница «Настройки прокси-сервера» позволяет при необходимости задать параметры подключения сервера к прокси-серверу.

Если сервер имеет сетевой интерфейс с прямым доступом в сеть Интернет, поэтому никаких изменений не вносить. На следующей странице, для загрузки и сохранения информации о прокси-сервере, необходимо нажать на кнопку «Начать подключение». Во время подключения будет доступна кнопка «Остановить подключение». Если во время подключения будут обнаружены какие-либо проблемы, можно воспользоваться данной кнопкой, исправить ошибки в настройках подключения, после чего заново возобновить подключение. Если подключение завершилось удачно, кнопка «Далее» становится доступна.

Следующим шагом предоставляется возможность выбора подмножества языков, которые будут загружаться на WSUS-сервер из центра обновлений Microsoft.

Выбирая только обновления для конкретных языков, можно сэкономить как время загрузки обновлений и сетевой трафик, так и пространство на жестком диске, который был указан на этапе установки сервера обновлений. Здесь стоит быть предельно внимательным, так как если не выбрать какой-то определенный язык, то подчиненные клиенты не смогут получать полный набор обновлений.

Следующим этапом настройки серверов обновлений является выбор продуктов, для которых будут загружаться обновления. На этой странице все продукты корпорации Microsoft сгруппированы иерархически, то есть по семействам. Соответственно, можно выбрать как всю линейку продуктов, например, Exchange, так и конкретный продукт (например, Exchange Server 2010). Если установить флажок на верхнем уровне, то также автоматически выбираются все элементы более низких уровней. По умолчанию выбраны уровни «Office» и «Windows».

На шестом шаге предоставляется возможность выбора классов обновлений, которые необходимо устанавливать. Можно выбрать как все существующие классы, так и строго определенные. В перечне присутствуют такие классы обновлений, как:

- Драйверы
- Критические обновления
- Накопительные пакеты обновления
- Обновления определений
- Обновления системы безопасности
- Обновления
- Пакеты новых функций
- Пакеты обновления
- Средства

По умолчанию выбраны классы «Критические обновления», «Обновления определений», а также «Обновления системы безопасности».

Предпоследним шагом, который необходимо настроить, является настройка выполнения синхронизации обновлений. Здесь, на странице «Настройка расписания синхронизации» предстоит выбрать, нужно ли выполнять синхронизацию вручную или автоматически. По умолчанию переключатель установлен на опции «Синхронизация вручную». Это означает, что в этом случае придется каждый раз для синхронизации WSUS-сервера с центром обновлений Microsoft запускать процесс вручную непосредственно из консоли администрирования WSUS. Если выбрать «Автоматическая синхронизация», то через указанные интервалы времени сервер будет автоматически производить синхронизацию. Можно выбрать от 1 до 24 синхронизации за 1 день, частота синхронизации может изменяться от одной синхронизации за день, до одной за один час. Стоит помнить, что фактическое время начала синхронизации может определяться со случайной задержкой до 30 минут после указанного времени.

На заключительной странице мастера настройки Windows Server Update Services можно запустить первоначальную синхронизацию с центром обновлений Microsoft или вышестоящим сервером обновлений.

Настройка клиентских компьютеров WSUS

По умолчанию на серверах WSUS созданы две группы: «Все компьютеры» и «Неназначенные компьютеры», куда изначально входят все клиентские компьютеры, подключенные к WSUS-серверу. Группы можно создавать вручную, образовывая так называемую иерархию. Количество групп может быть не ограниченным.

В большинстве случаев принято назначать клиентские компьютеры в группы компьютеров со стороны клиента, а именно средствами групповых политик. Данный способ позволяет автоматически назначать все настройки клиентам, которые добавляются в сеть. Прежде чем переходить к процедуре назначения компьютера в группу компьютеров средствами групповых политик, требуется рассмотреть параметры групповой политики, доступные для управления клиентскими компьютерами Windows Server Update Services:

- Включить рекомендуемые обновления через автоматическое обновление. Используя этот параметр групповой политики, можно определить, будет ли на клиентском компьютере служба автоматического обновления Windows доставлять обновления, которые помечены как важные и рекомендуемые из Центра обновления Windows. В том случае, если отключить данный параметр, то будут доставляться только важные обновления;

- Включить уведомление о наличии программ. Этот параметр позволяет отображать подробные расширенные уведомления от службы центра обновления Майкрософт пользователям, что ускоряет установку и использование дополнительных приложений;
- Задержка перезагрузки при запланированных установках. При помощи этого параметра можно указать промежуток времени, в течение которого операционная система будет ожидать перед плановой перезагрузкой. Данный параметр применяется для службы автоматического обновления только в том случае, если установка обновлений настроена по расписанию, в противном случае придется выполнять перезагрузку в ручном режиме. Если данный параметр политики отключен, то перед перезагрузкой компьютер будет ожидать 15 минут, если же включить данный параметр, то промежуток времени будет изменен до 5 минут;
- Настройка автоматического обновления. Данный параметр групповой политики позволяет определить, как именно клиентский компьютер будет получать обновления для операционной системы и приложений. Если включить данный параметр, то нужно будет выбрать один из четырех параметров, которые выполняют те же функции, что и параметры, расположенные в раскрывающемся списке «Важные обновления» в окне настроек параметров центра обновления Windows. Если выбрать параметр «2 – уведомление о загрузке и установке», то при обнаружении операционной системой новых обновлений, в области уведомлений будет отображаться значок, свидетельствующий о том, что можно загрузить и установить обновления. После того как будут выбраны обновления, необходимые для загрузки, они будут загружены в фоновом режиме и нужно будет их установить. Данный вариант приемлем для персонала, тестирующего обновления, а также для некоторых домашних пользователей, но его ни в коем случае не стоит выбирать для пользователей в организации, так как следить за состоянием своей операционной системы будет от силы один из десяти пользователей. Если установить параметр «3 – авт. загрузка и уведом. об устан», что равносильно значению «Загружать обновления, но решение об установке принимается мной» в графическом пользовательском интерфейсе, то после того как операционная система обнаружит новые обновления, она их автоматически загрузит на компьютер в фоновом режиме и пользователю нужно будет только

установить загруженные обновления. Выбрав параметр «4 – авт. загрузка и установка по расписанию», обновления будут автоматически загружены и установлены в указанное в данном параметре время, причем, если для завершения установки понадобится перезагрузить компьютер, он будет перезагружен в автоматическом режиме. Параметр под номером 5 разрешает локальным администраторам выбирать режим вывода уведомлений об обновлениях и их установке;

- Не выполнять автоматическую перезагрузку при автоматической установке обновлений, если в системе работают пользователи. Этот параметр групповой политики позволяет для завершения установки обновлений по расписанию запретить автоматическую перезагрузку компьютера, тем самым, дав пользователям возможность перезагружать систему автоматически при первом входе в систему;
- Не задавать по умолчанию параметр «Установить обновления и завершить работу» в диалоговом окне «Завершение работы Windows». Используя текущий параметр, можно определить, будет ли в диалоговом окне завершения работы операционной системы по умолчанию отображаться команда «Установить обновления и завершить работу». В том случае, когда завершение установки обновления требует перезагрузки, отображается именно эта команда, но если включить данный параметр групповой политики, то в диалоговом окне завершения работы операционной системы будет установлена по умолчанию та команда, которая задана в настройках операционной системы;
- Не отображать параметр «Установить обновления и завершить работу» в диалоговом окне «Завершение работы Windows». Если на компьютере есть обновления, которые будут установлены после перезагрузки компьютера, то команда «Завершить работу» меняется на «Установить обновления и завершить работу». При включенном параметре команда «Завершение работы» всегда будет иметь такое название даже в том случае, если на компьютере присутствуют обновления, которые будут установлены после перезагрузки или выключения компьютера;
- Перенос запланированных автоматических установок обновлений. Данный параметр групповой политики позволяет указать период ожидания после загрузки операционной системы до выполнения

пропущенной ранее установки обновлений по расписанию. По умолчанию пропущенная установка обновлений по расписанию выполняется через одну минуту после загрузки системы, при отключении данного параметра, система будет ждать до следующей установки по расписанию. Если же включить данный параметр, то можно указать период времени, в течение которого операционная система будет ждать до выполнения установки пропущенных обновлений;

- Повторный запрос для перезагрузки при запланированных установках. Периодически практически у каждого пользователя случаются такие ситуации, когда он загружает и устанавливает обновления, но не хочет перезагружать компьютер для завершения установки некоторых обновлений. В этом случае каждые 10 минут выскакивает предупреждающее приглашения с предложением перезагрузить компьютер, которое может действовать некоторым людям на нервы. При помощи этого параметра можно определить период времени, через который пользователь увидит запрос для перезагрузки компьютера;
- Разрешить пользователям, не являющимся администраторами, получать уведомления об обновлениях. По умолчанию, в том случае если не выбрана установка обновлений по расписанию, только локальные администраторы компьютеров могут получать уведомления об обновлениях. Если же требуется дать наряду с локальными администраторами обычным пользователям возможность получать уведомления, а также устанавливать важные, рекомендуемые и необязательные обновления, то нужно воспользоваться текущим параметром групповой политики, причем, для установки обновлений пользователи даже не увидят диалогового окна UAC;
- Разрешить клиенту присоединение к целевой группе. Именно при помощи этого параметра можно назначить клиентский компьютер в группу компьютеров сервера Windows Server Update Services. Если группа не указана, а пользователь подключается к WSUS-серверу, то можно найти этот компьютер в группе «Неназначенные компьютеры». Если же нужно поместить пользователя не в одну группу, а в несколько, то необходимо разделить группы точками с запятой;
- Разрешить немедленную установку автоматических обновлений. Помимо обновлений, которые для завершения установки требуют перезагрузку компьютера, есть и такие обновления, которые могут

устанавливаться в работающей операционной системе без всяких перезагрузок компьютера. При помощи текущего параметра групповой политики можно задать службе автоматического обновления немедленную установку обновлений без прерывания каких-либо служб операционной системы или ее перезагрузки;

- Разрешить прием обновлений с подписью из службы обновлений Майкрософт в интрасети. Если помимо обновлений от серверов Microsoft, мой WSUS-сервер распространяет обновления, разработанные другими компаниями, которые подписаны сертификатом, расположенным в хранилище «Доверенные издатели» на локальном компьютере, то данный параметр групповой политики позволит пользователям устанавливать такие обновления. Если же данный параметр отключен, то на клиентские компьютеры будут распространяться только обновления для продуктов компании Microsoft®;
- Разрешить управлению электропитанием центра обновления Windows выводить систему из спящего режима для установки запланированных обновлений. Если в организации обновления устанавливаются автоматически по расписанию, то целесообразно устанавливать время расписания установки обновлений на ночь и не выключать полностью компьютеры, а переводить их в режим гибернации. Данный параметр групповой политики позволяет для установки обновлений переводить компьютер в обычный режим для установки обновлений;
- Указать размещение службы обновлений Майкрософт в интрасети. По умолчанию, клиентские компьютеры не знают, установлен ли в организации WSUS-сервер. Используя этот параметр групповой политики, можно указать путь к WSUS-серверу, который будет служить внутренним сайтом служб обновлений в организации. Здесь необходимо указать два параметра, а именно имя сервера, на котором будет выполняться поиск и загрузка обновлений, а также сервер, на котором будет выполняться статистика. В большинстве случаев это один и тот же сервер;
- Частота поиска автоматических обновлений. При помощи текущего параметра групповой политики можно указать промежуток времени между поиском новых обновлений на WSUS-сервере. По умолчанию доступные обновления проверяются с интервалом в 22 часа. Если включить данный параметр, то можно указать время ожидания в часах

путем вычитания от 0 до 20% от установленного времени. Данную политику указывать бессмысленно в том случае, если настроен параметр групповой политики «Настройка автоматического обновления»;

- Запретить использование любых средств Центра обновления Windows. Данный параметр групповой политики доступен только в разделе конфигурации пользователя и позволяет полностью запретить доступ к центру обновления Windows®. Не рекомендовано использовать данный параметр в производственной среде.

Теперь, чтобы назначить на контроллере домена клиентские компьютеры в группу компьютеров, требуется открыть оснастку «Управление групповой политикой», создать объект GPO «Клиенты WSUS» и привязать его к подразделению с клиентами домена Diplom. В контекстном меню объекта выбрать пункт «Изменить». В открывшейся оснастке «Редактор управления групповыми политиками» перейти в узел «Конфигурация компьютера» \ «Политики» \ «Административные шаблоны» \ «Компоненты Windows» \ «Центр обновления Windows».

На панели сведений выбрать политику «Указать размещение службы обновлений Майкрософт в сети» и дважды щелкнуть по ней, чтобы открыть диалоговое окно параметра групповой политики. В отобразившемся диалоговом окне выбрать опцию «Включить» и в текстовом поле «Укажите службу обновлений в интрасети для поиска обновлений» ввести имя WSUS-сервера. А в текстовом поле «Укажите сервер статистики в интрасети» ввести адрес сервера статистики, «http://W2k8-Diplom», и нажать на кнопку «ОК».

На панели сведений открыть политику «Разрешить клиенту присоединение к целевой группе», установить переключатель на опции «Включить» и в текстовом поле «Имя целевой группы для данного компьютера» ввести название группы компьютеров, на которые распространяется групповая политика. После того как изменения были внесены, нажать на кнопку «ОК»На панели сведений открыть политику «Не отображать параметр «Установить обновления и завершить работу» в диалоговом окне «Завершение работы Windows»» и установить переключатель опции на «Включить».

На панели сведений открыть политику «Настройка автоматического обновления», установить переключатель на опцию «Включить». В раскрывающемся списке выбрать опцию «4 – Автоматическая загрузка и установка по расписанию» и установить в соответствующих полях дни недели и время для установки обновлений по расписанию.

На панели сведений открыть политику «Включить уведомления о наличии программ» и установить переключатель на опцию «Включить». Так же на панели сведений открыть политику «Включить рекомендуемые

обновления через автоматическое обновление» и установить переключатель на опцию «Включить». И последней политикой открыть «Не выполнять автоматическую перезагрузку при автоматической установке обновлений, если в системе работают пользователи» и установить переключатель на опцию «Включить». Нажать на кнопку «ОК» и закрыть оснастку «Редактор управления групповыми политиками». Применить обновление групповых политик с помощью команды «gpupdate /force».

Контрольные вопросы

1. Назначение WSUS -сервера?
2. Назначение Веб-сервера (IIS)?
3. В чем заключается настройка клиента WSUS?

В 2009 году Университет стал победителем многоэтапного конкурса, в результате которого определены 12 ведущих университетов России, которым присвоена категория «Национальный исследовательский университет». Министерством образования и науки Российской Федерации была утверждена программа его развития на 2009–2018 годы. В 2011 году Университет получил наименование «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики»

КАФЕДРА АППАРАТНО-ПРОГРАММНЫХ КОМПЛЕКСОВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

Кафедра Аппаратно-программных комплексов вычислительной техники осуществляет переподготовку и повышение квалификации специалистов с широким спектром образовательных программ по следующим направлениям:

- Системный инженер - специалист по эксплуатации аппаратно-программных комплексов вычислительной техники
- Системный администратор - специалист по эксплуатации компьютерных сетей и сопровождению программ 1С:Предприятие
- Обслуживание, диагностика и ремонт персональных компьютеров
- Администрирование вычислительных сетей
- Конфигурирование, администрирование и программирование в среде 1С:

На кафедре ведется подготовка магистров по направлению 230100 «Информатика и вычислительная техника»:
магистерская программа – «Системное администрирование аппаратно-программных комплексов и сетей», 230100.68.13.

Кафедра является выпускающей по направлению 230100 «Информатика и вычислительная техника» на факультете ВиЗО.

Владимир Александрович Костеж
Светлана Михайловна Платунова

Серверные технологии в вычислительных сетях на базе MS Windows Server 2008

Учебно-методическое пособие
по изучению дисциплины
«Администрирование вычислительных сетей»

В авторской редакции
Редакционно-издательский отдел НИУ ИТМО
Зав. РИО Н.Ф. Гусарова
Лицензия ИД № 00408 от 05.11.99
Подписано к печати
Заказ №
Тираж 100
Отпечатано на ризографе

Редакционно-издательский отдел
Санкт-Петербургского национального
исследовательского университета
информационных технологий, механики
и оптики
197101, Санкт-Петербург, Кронверкский пр., 49