МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра космического приборостроения и систем связи

УТВЕРЖДАЮ
Проректор по учебной работе
_____ О.Г. Локтионова
«___» _____ 2017 г.

ИЗУЧЕНИЕ ТИПОВ СЕРВЕРОВ И ИХ СПЕЦИФИКА ОБСЛУЖИВАНИЯ

Методические указания по выполнению лабораторной работы №2 для студентов, обучающихся по направлению подготовки 11.03.02 «Инфокоммуникационные технологии и системы связи»
по дисциплине: «Основы построения инфокоммуникационных систем и сетей», часть 1

Курск 2017

2

УДК 621.391

Составители: А.В. Хмелевская, А.Н. Шевцов

Рецензент
Доктор технических наук, старший научный сотрудник,
профессор кафедры *В.Г. Андронов*

Изучение типов серверов и их специфика обслуживания: методические указания по выполнению лабораторной работы №2 по дисциплине: «Основы построения инфокоммуникационных систем и сетей», ч. 1 / Юго-Зап. гос. ун-т; сост.: А.В. Хмелевская, А.Н. Шевцов. – Курск, 2017. – 13 с.: – Библиогр.: с. 13.

Методические указания по выполнению практической работы содержат краткие теоретические сведения о типах серверов и их специфике обслуживания.

Методические указания полностью соответствуют требованиям типовой программы, утвержденной УМО по направлению подготовки 10.05.02 «Информационная безопасность телекоммуникационных систем», а также рабочей программе дисциплины: «Сети и системы передачи информации».

Предназначены для студентов, обучающихся по направлению подготовки 10.05.02, очной формы обучения.

Текст печатается в авторской редакции

Подписано в печать 15.12.17 . Формат 60x841/16.
Усл. печ. л. 1,51 .Уч.-изд. л.1,37.Тираж 100 экз. Заказ.3241Бесплатно
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94

1 Цель работы

Целью данной лабораторной работы является ознакомление с основными типами серверов и спецификой их обслуживания**.**

2 Краткие теоретические сведения

2.1 Специфика обслуживания сервера

Техническое обслуживание серверов и сопутствующего оборудования - важное условие качественной и стабильной работы информационных систем. Именно от него зависит сохранность информации и ее защищенность от несанкционированного доступа.

Полное комплексное обслуживание серверов включает в себя множество операций. В первую очередь оно предполагает собственно монтаж, настройку и обслуживание серверов и серверного оборудования.

Перед тем как осуществить монтаж серверного оборудования, подвергаются серьезному анализу все требования, которые имеются к технике. И на их основе выбирается именно тот вид оснащения и конфигурация системы, которые уместны в данном конкретном случае.

Потом осуществляется установка серверного оборудования, его конфигурирование. Затем его подключают и производят запуск. Устанавливается, тестируется, настраивается и начинает использоваться необходимое программное обеспечение.

Когда все необходимые операции будут произведены, в постоянном режиме обслуживания сервера производится:

- непрерывный мониторинг состояния системы и отдельных ее сервисов;
- осуществляется поддержка ее работоспособности;
- осуществляется проверка основного и резервного электропитания;
- необходимо достаточно часто проверять и заменять аккумуляторы;
- работу устройств ввода/вывода, к которым относятся клавиатура, мышь, монитор, свитчи для их подключения к системным блокам, провода и разъемы;
- регулярно следует осматривать кабели на предмет

внешних повреждений;

- проверке также подвергается уровень нагрева тепловыделяющих компонентов аппаратуры;

- и работа систем вентиляции и кондиционирования - в данном случае крайне важно, чтобы не было никаких помех для охлаждения оснащения.

В операции по обслуживанию сервера также входит ремонт оснащения и замена комплектующих в том случае, если нагрузка на сервер будет повышаться.

Также осуществляется проверка правильности настройки сервера, обеспечение хорошей их работы с помощью частой проверки программных и аппаратных составляющих. Особое внимание уделяется управлению правом доступа к секретной информации и периодическое резервное копирование. В связи с этим происходит постоянная проверка работоспособности и износа оборудования резервного копирования.

Одной из целей выполняемых работ по обслуживанию серверов являются защита данных как от внешних опасностей, к примеру, от несанкционированного доступа и вредоносных программ, именуемых вирусами, так и от внутренних, к которым относятся сбои в работе программного обеспечения.

Помимо прочих вышеуказанных процедур при осуществлении обслуживания серверов, обязательных для совершения, также важно проводить периодическую чистку серверов.

В течение определенного времени в серверном корпусе и блоках питания собирается грязь и пыль, от которой крайне важно своевременно избавляться. В противном случае вы можете столкнуться с крайне неприятной ситуацией - перегревом системы. Также крайне важной процедурой является осмотр рабочей способности вентиляторов. Если не совершать вышеуказанные процедуры своевременно, в результате может существенно замедлиться работа серверного оснащения или оно даже придет в негодность. Для того чтобы подобная проблема не возникала, вам следует периодически осуществлять проводить проверку и чистку сервера.

Помимо прочих процедур, в перечень услуг, предоставляемых компаниями, занимающимися обслуживанием серверов, также включены работы:

- по диагностике и аудиту оснащения.

Вряд ли для кого-то будет секретом тот факт, что по истечении определенного промежутка времени системы начинают работать медленнее, что становится заметно без определенных замеров времени. В задачи аудита входит повышение производительности систем и произведение перенастройки и модернизации серверного оснащения. Постоянный контроль помогает осуществить диагностику на ранних этапах возникновения неполадок. Благодаря этому не возникают различные критические ситуации при работе системы.

К операциям по обслуживанию сервера причисляют обновление ОС (операционных систем), программ и контрольной панели.

В связи с этим специалист, занимающийся обслуживанием серверов, периодически осуществляет проверку наличия последних обновлений ПО. Важным направлением работы специалиста, занимающегося обслуживанием серверов, является:

- поддержка и администрирование корпоративной почты.

К примеру, он будет заниматься образованием и изменением учетных записей почты, обеспечением ее приватности.

Благодаря обслуживанию серверов становится возможной проверка сроков окончания лицензий. Чтобы определить, насколько хорошо будет работать сервер, специалист проверяет его скорость работы, целостность, приходящуюся на него среднюю и пиковую нагрузку, систему дублирования, резервирования и т. д.

В обслуживание серверов входит:

- оптимизация интернет-трафика, которая предполагает ее фильтрацию;

- осуществляется проверка суммарного внешнего трафика, выясняется, какие порты являются открытыми, заполняются устройства массовой памяти.

2.2 Удаленное администрирование серверов

Он включает в себя управление учетными записями и соответствующими сетевыми ресурсами. Данный вид работ предполагает обслуживание специализированных серверных ролей,

к которым относятся Active Directory, Exchange Server, ISA, SQL и другие.

2.3 Организация файл-сервера предприятия на базе Free BSD или Linux

Для централизованного хранения данных, необходимых для работы предприятия, используется файловый сервер. Как правило, это выделенный компьютер, работающий под серверной операционной системой и имеющий быструю и надежную дисковую подсистему. Помимо хранения и организации доступа к документам, файловый сервер решает такую важную задачу, как разграничение прав доступа пользователей к информации. Каждый сотрудник может просматривать или вносить изменения только в те документы, на которые он имеет соответствующие права.

2.4 Хранение всех данных в одном месте сильно упрощает управление правами доступа пользователей

Если в локальной сети присутствуют рабочие станции под управлением операционных систем семейства Windows, что характерно для большинства предприятий, то для общего доступа к файлам и принтерам используется протокол SMB.

Использование серверных продуктов от Microsoft не всегда может оказаться оправданным по экономическим соображениям. Тем более, когда есть альтернатива.

Экономичным и в то же время производительным и надежным решением может выступить операционная система Free BSD или Linux.

Для организации доступа к данным используется свободная реализация SMB протокола - Samba. Установка Samba позволяет использовать компьютер на базе Free BSD или Linux в качестве члена домена либо контроллера домена (PDC) в Windows сети. Так же Samba может стать частью домена Active Directory. Для того чтобы обеспечить общую

систему безопасности Active Directory, используется протокол Kerberos. Поддержка данного протокола в FreeBSD может быть быть реализована при помощи программы heimdal.

Таким образом возможна организация сети предприятия, в которой клиентские машины работают под управлением Windows, в то время как для серверов используют Free BSD или Linux системы. Несмотря на то, что у некоторых специалистов подобная идея может вызвать сомнение, совместную работу Windows и UNIX систем в одной сети настроить можно. Причем сложность подобного решения вовсе не так высока, как это может показаться на первый взгляд. Вместе с тем, настроить и в дальнейшем обслуживать сервер Linux / Free BSD будет более выгодно силами компаний профессионально занимающихся обслуживанием серверов.

Доступность веб-интерфейсов настройки печати и доступа к файлам, а также возможность настройки при помощи ACL управления правами доступа при помощи стандартного инструментария Windows делают администрирование подобной системы достаточно несложным. С текущим обслуживанием сервера может справиться любой сотрудник, имеющий минимальные навыки работы в операционных системах, схожих с UNIX. Опытный администратор или специализированная компания, предоставляющая услуги по обслуживанию серверов Linux / Free BSD понадобится только на этапе проектирования и внедрения системы, а также при внесении достаточно сложных изменений.

К преимуществам серверов, работающих под управлением Free BSD или Linux систем, можно отнести:

- высокую производительность;
- возможность гибкой настройки практически под любые задачи;
- и высокую стабильность.

Системы Free BSD и Linux отличаются большой гибкостью настройки. Их можно адаптировать практические под любые задачи. На работающем сервере будут исполняться только те процессы, которые необходимы, что экономит системные ресурсы и снижает вероятность возникновения программного сбоя.

Обслуживание файлового сервера на основе Free BSD с

установленной Samba может осуществляться путем внесения изменений в файл конфигурации smb.conf, который после инсталляции Samba должен находиться по адресу /usr/local/etc/smb.conf. Его можно создать либо воспользоваться образцом smb.conf.sample, куда вносятся все необходимые изменения. Для облегчения процесса настройки Samba можно использовать веб-интерфейс SWAT. К преимуществам его использования, помимо графического интерфейса, можно отнести хорошую систему справки по всем параметрам настройки.

Порой возникает ситуация, когда руководителю или ответственному сотруднику необходимо изменить права доступа к отдельным файлам и папкам. Если администратор отсутствует, это может оказаться затруднительным. Ведь далеко не все пользователи имеют навыки работы в Free BSD или Linux системах. Для того чтобы организовать возможность настройки прав доступа к файлам и каталогам при помощи проводника Windows, можно использовать списки доступа ACL (Access Control Lists). Поддержка ACL реализована в большинстве актуальных версий Free BSD или Linux на уровне ядра – все, что необходимо, – это включить ее для выбранных файловых систем.

Нередко, помимо хранения и предоставления доступа к документам, файл-сервер выполняет и некоторые другие функции. Достаточно часто файловый сервер является и сервером печати, то есть организует возможность работать с принтерами для всех рабочих станций сети предприятия. В случае при обслуживании сервера с установленной операционной системы Free BSD используется система печати CUPS. Для упрощения процедуры настройки доступен веб-интерфейс.

Кроме того, именно на файл-сервер обычно ложится организация резервного копирования. Собранные в одном месте данные, без которых работа предприятия в нормальном режиме попросту невозможна, очень уязвимы.

Причин повреждения данных может быть множество – это аппаратная неисправность, проблемы с электропитанием, воздействия вредоносного ПО или пожар,

но все они могут принести предприятию значительные убытки. Для того чтобы предотвратить потерю данных, необходимо при выполнении регулярного обслуживания сервера делать резервные копии всех важных документов и хранить их в надежном, желательно удаленном от сервера месте.

Существует три основных типа серверов удалённого доступа:

- серверы удаленного управления;
- серверы удаленных узлов;
- терминальные серверы.

Серверы удаленных узлов выступают в роли маршрутизаторов, или шлюзов, выполняя лишь транспортный сервис, тем самым соединяя клиентов с центральной сетью. Обслуживание серверов происходит при использовании протоколов IP, IPX или NetBIOS.

Серверы удаленного управления помогают обеспечить транспортный сервис, а также способны запускать от имени клиента различные приложения на компьютерах, подсоединённых к центральной сети, на экране удаленного компьютера создают образ графической среды этого приложения. Как правило, серверы удалённого управления работают с системой Windows.

Терминальные серверы работают аналогично, но при использовании многотерминальных операционных систем, таких как Unix, VAX VMS, IBM VM.

Терминальный сервер обеспечивает клиентов вычислительными ресурсами: память, процессорное время и пр. С технической стороны вопроса терминальный сервер - это мощный компьютер высокой производительности, который способен обслужить одновременно несколько пользователей. Расположение терминального сервера для работы не имеет значения - он может находиться как в соседней комнате, так и в другой стране.

Доступ к серверу и обслуживание сервера обеспечивают специальные терминальные клиенты - программы, которые в течение работы воспроизводят данные по работе сервера.

2.5 Обслуживание сервера контроллера доменов

Для того чтобы повысить эффективность любой ИТ-

инфраструктуры, очень важно правильно выполнить все необходимые настройки на базе вашей операционной

Качественная настройка и обслуживание сервера включает в себя:

- настройку всех основных служб для работы сети;
- таких как контроллер домена;
- сервер баз данных;
- файл-сервер;
- почтовый и прокси-серверы и т. д.

Сервер терминалов достаточно часто используется при совместной работе в программе 1С. Это позволяет не только значительно повысить производительность программного обеспечения 1С, но и обеспечить высокую надежность программы и возможный удаленный доступ к 1С через Интернет. При необходимости в некоторой степени экономить интернет-траффик при полном контроле доступа в глобальную сеть в офисе хорошим решением становится установка интернет-шлюза и прокси-сервера и дальнейшее обслуживание северов этих типов. При настройке ограничения доступа в глобальную сеть Интернет появляется возможность намного эффективнее использовать рабочее время ваших сотрудников.

При установке важно убедиться в том, что сервер, на который устанавливается Active Directory, имеет специальный раздел с файловой системой NTFS. Также перед установкой важно убедиться в том, что служба DNS правильно настроена. Обратите внимание на то, что сервер может вести себя по-разному, что следует учитывать при обслуживании сервера, в зависимости от версии и выпуска установленной операционной системы, а также прав и разрешений учетной записи и настроек меню.

Какое же оборудование может понадобиться для установки сервера на предприятии?

К нему относятся:

- коммутаторы;
- маршрутизаторы;
- принт-серверы и прочее.

А для того чтобы оборудование не выходило из

строя, требуется своевременное обслуживание сервера.

Благодаря своевременному обслуживанию сервера появляется возможность значительно увеличить срок его службы, а также избежать его внезапного выхода из строя. Оперативно устранять ошибки в программной части сервера возможно даже при удаленном обслуживании сервера. Если вы являетесь владельцем малого или среднего бизнеса и используете на фирме небольшое количество серверов, то чаще всего содержать в штате высококвалифицированного, а, следовательно, и высокооплачиваемого специалиста для настроек и обслуживания сервера довольно часто экономически нецелесообразно. Поэтому обслуживание серверов логичнее и более экономически выгодно поручить компании, которая специализируется по данному профилю.

2.6 Обслуживание серверов windows 2003 и windows 2008

Сегодня практически каждая компания старается оборудовать свой офис различными видами оргтехники, первое место среди которой занимает компьютер. Компьютеризировать офис - это всего лишь пол дела, надо научиться грамотно обслуживать дорогостоящую технику. Корректная настройка позволяет повысить эффективность деятельности хозяйствующего субъекта. Столь популярные на сегодняшний день автоматизированные системы и программные продукты, позволяющие облегчить ведение учета и контроля за теми или иными процессами. Но для их полноценного функционирования необходимо создание определенных условий, в частности это касается операционной системы и набора дополнительных программных модулей. На сегодняшний день многие компании для повышения эффективности ИТ-инфраструктуры устанавливают и настраивают сервера именно на базе операционной системы Windows Server.

Обслуживание компьютеров, обслуживание сервера windows 2003 или обслуживание сервера windows 2008 считается одной из важных расходных статей для любой компании.

Обслуживание техники заключается не только в поддержке оборудования в рабочем состоянии, но и в эффективных борьбы с вредоносными программами, обновлении базы данных, переустановке операционной системы и пр.

Сегодня сервера - это надёжное обеспечение как на аппаратном, так и на программном уровне. Однако не стоит забывать, что своевременное обслуживание сервера windows 2003 и обслуживание сервера windows 2008 позволит увеличить его работоспособность и значительно продлить срок службы. Обслуживание сервера windows 2003 и обслуживание сервера windows 2008 возможное в виде удаленного обслуживания указанных серверов позволит оперативно исправлять большое количество ошибок в программной части серверов.

Качественная настройка и обслуживание сервера windows 2008, windows 2003 подразумевает комплексную настройку основных служб для работы внутренней сети предприятия, те. подключение интернет-шлюза, файл-сервера, сервера баз данных, почтового сервера, DNS, DHCP, VPN и пр.

Данная система предназначена для серверного использования, в домашних условиях её применяют крайне редко. Конечно, при большом желании и грамотном обслуживании сервера windows 2003, вполне возможно использовать и на домашнем ПК эту операционную систему, но лучше для таких целей предназначены другие операционные системы.

Ещё одна операционная система от компании Microsoft, которая отлично подходит для использования на предприятии - Windows Server 2008.

Гибкая и надёжная операционная система Windows Server 2008 включает в свой состав новые технологии, к примеру, режим Server Core, командная оболочка Windows PowerShell и др. Модернизированные сетевые технологии Windows Server 2008 повышают управляемость и доступность серверной инфраструктуры. Качественное и выгодное обслуживание сервера windows 2008 разрешает сэкономить время и значительно сократить затраты.

Если обслуживание сервера windows 2008 проводится качественно, то данная ОС позволяет реализовать заложенный в ней потенциал, существенно улучшая и расширяя возможности по администрированию, диагностике, управлению службами и сервисами.

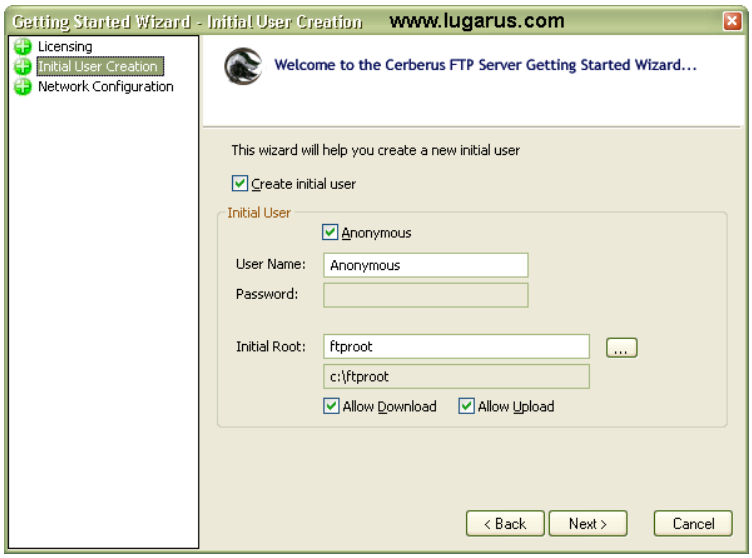
Значительно повысить эффективность использования оборудования и улучшить доступность серверов помогает встроенная технология виртуализации Windows Server 2008. Кроме того, Windows Server 2008 считается самым защищённым из всех аналогичных продуктов. Повышенную безопасность операционной системе гарантируют защита сетевого доступа, контроллер домена только для чтения и федеративные службы управления правами. Обслуживание сервера windows 2008 на предприятии позволяет полностью обезопасить бизнес в целом.

Стоит отметить, что серверы Windows Server 2008 могут быть использованы в качестве терминального сервера в том случае, если это редакции Standard, Enterprise и Datacenter, содержащие службы Terminal Services. Обслуживание сервера windows 2008 подразумевает обеспечение каждого пользователя лицензией Windows CAL, а также отдельной клиентской лицензией на доступ к серверу терминалов.

3 Задание на лабораторную работу

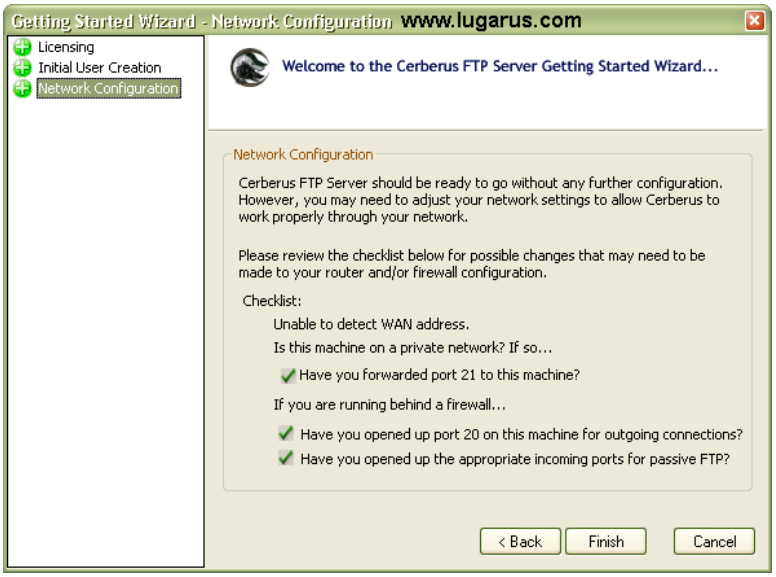
1. Установить программу Cerberus FTP Server, предназначенную для запуска FTPсервера.
2. Выбрать тип лицензии: для бизнеса или домашнего использования. Выбирайте Personal Use.

3. Создать аккаунт по умолчанию. Обычно это anonymous, т.е. любой человек, зная ip-адрес вашего сервера, сможет войти на него. Для анонима можно не задавать пароль.

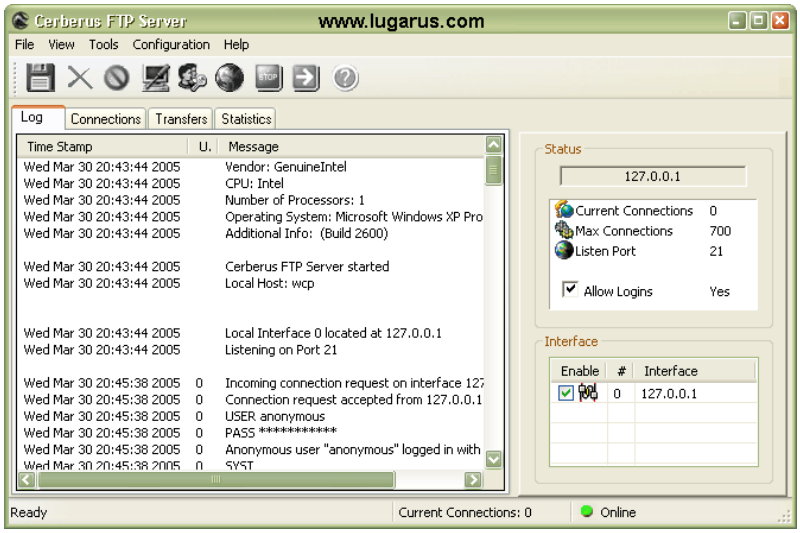


Initial Root - это корневая папка FTP сервера, к которой впоследствии вы сможете добавить другие доступные пользователям папки.

3. Последняя опция дает возможность включить определение IP-адреса FTP для того, чтобы сервер был доступен не только из локальной сети, но и из внешнего интернета. Так же эта настройка открывает 21-й порт для обмена данными. Если у вас установлен файрвол (а он обязательно должен быть установлен!), то разрешите в нем использование этого порта.



Все, нажимаем кнопку Finish и наш FTP переходит в режим Online, готовясь принять первых посетителей. О режиме работы сервера сигнализирует зеленый или красный индикатор в статусной строке главного окна сервера:



На вкладке LOG отображаются все серверные сообщения о подключениях к FTP, передвижениях по каталогам, запросах на download/upload и прочее... Вкладка CONNECTIONS показывает

всех подключенных в данный момент пользователей. Список обновляется в режиме реального времени. Если кликнуть на любом пользователе правой кнопкой, то можно получить 2 команды управления подключением: Terminate User (принудительно выбросить пользователя с вашего FTP) и Block Address (блокировать данный IP-адрес, чтобы какой-нибудь хулиган не смог попасть на сервер). На вкладке TRANSFERS видны производимые с файлами операции: процент скачивания/закачивания, прошедшее и оставшееся время, имя пользователя, имя файла и пр. И, наконец, на вкладке STATISTICS отображается сводная информация о работе FTP сервера: общее число подключений, число подключений в данный момент, количество удачно/неудачно скаченных с сервера и закаченных на него файлов.

Дефолтовый-то аккаунт мы создали, но никакие каталоги для него еще недоступны, посетители при входе на FTP будут видеть только пустую папку ftproot.

Для определения параметров аккаунта выберите в меню "Configuration - User Management" или нажмите на панели инструментов кнопку с изображением человечков:

Разберемся с настройками аккаунта для анонима. - Отключение аккаунта производится простым снятием галочки в окошке "Cerberus User Accounts- Property". - Там же можно задать пароль, дважды кликнув по слову "Password". - Simultaneous Logins - число одновременных заходов для данного аккаунта. Выставьте необходимое значение или оставьте Unlimited по умолчанию. Чем

больше посетителей входят одновременно на ваш сервер, тем больше ресурсов они будут потреблять. Представьте себе, что получится, если 10 человек будут одновременно качать к себе 10 фильмов? А 50 человек? Лично мне было бы жалко мой жесткий диск :) - Simple Directories - быстрое отключение всех виртуальных каталогов. В этом случае пользователи снова увидят лишь пустой каталог ftproot

Теперь научимся подключать каталоги. В окошке "Virtual Root Directory for" жмем на кнопку "...", выбираем нужный каталог (который, кстати, может быть расположен на любом подключенном носителе: CD, другой раздел жесткого диска, FDD и пр.), затем кнопку "Add" - выбранный каталог добавлен в дерево ftproot. Теперь настроим для него права (permissions): скачивание, закачка на сервер, переименование, удаление, создание каталогов, отображение скрытых файлов. Комбинация прав может быть любой для каждого каталога и каждой группы пользователей.

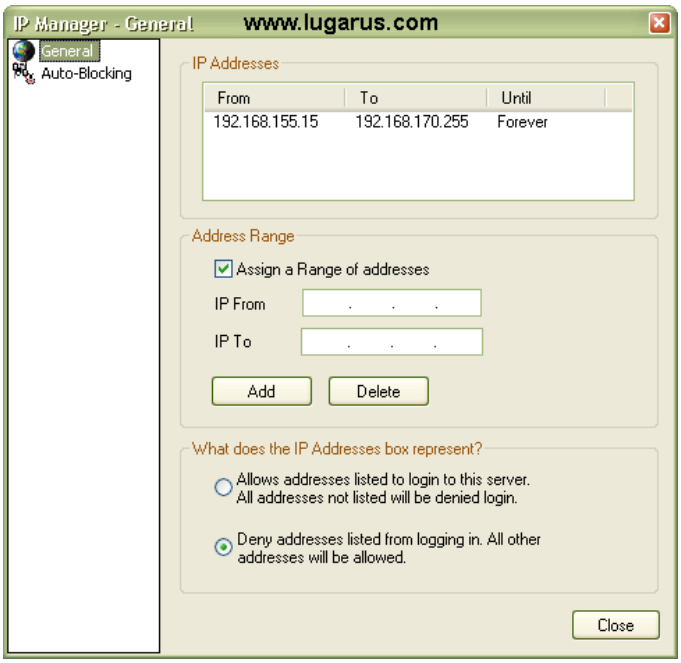
Кстати, еще немного о пользователях. Может быть, у вас есть информация, которой можно поделиться лишь с избранными? Легко! Создайте для них отдельный паролированный аккаунт. Делается это нажатием кнопки "New":

Обратите внимание, что здесь произошли некоторые изменения по сравнению с анонимным логином, а именно: - название группы является так же логином, который нужно будет ввести в FTP-клиенте для корректного подключения к серверу - задан пароль для группы special - число одновременных подключений ограничено 5 логинами - отключена возможность

анонимного подключения именно для этой группы! Не забывайте снимать галочку, если создаете особые группы, иначе любой гость без ввода пароля сможет увидеть ваши секретные данные :)

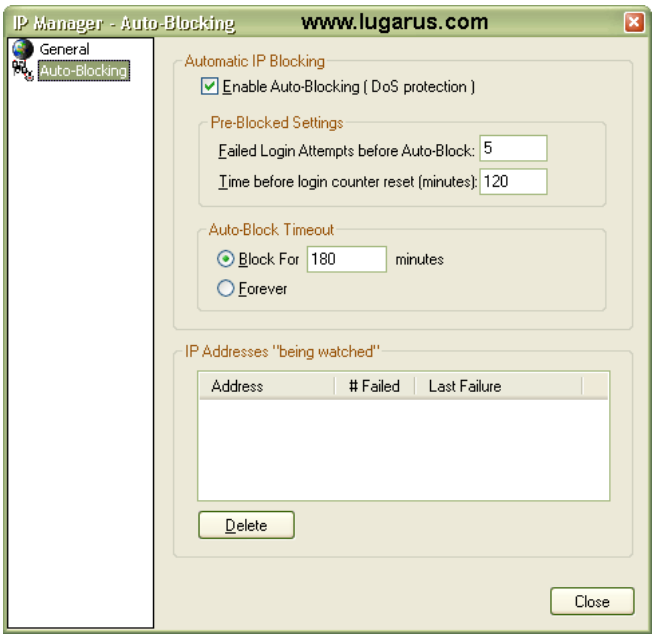
Опции"NT Users" мы касаться не будем, она дает возможность использовать учетные записи компьютеров для подключения к FTP. Оставим эту возможность отключенной.

Сервер запущен, пользователи оповещены, вы наблюдаете за операциями, ощущая себя великим и могучим :) Все довольны... Но что делать, если вдруг объявится какой-нибудь доморощенный кулхацер, смыслом никчемной жизни которого является процесс устраивания подлянок другим? Если он вдруг начнет устраивать ддос-атаку на ваш FTP или просто будет хулиганить в публичных каталогах, закачивания вам массу никчемных файлов, вирусов и пр. ? Каждый раз кликать по его нику и делать "Terminate User" - рука устанет. Для таких случаев Cerberus предоставляет в наше несколько инструментов:

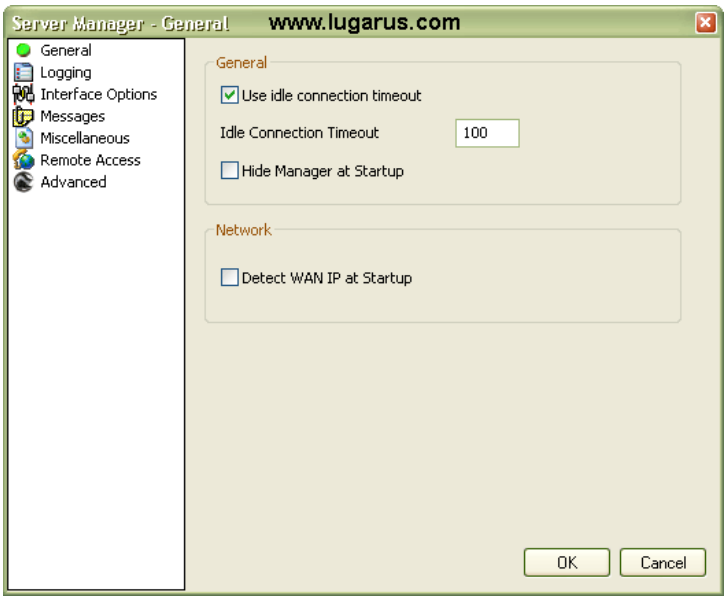


На вкладке General можно четко разграничить возможность доступа к серверу, добавляя целые диапазоны IP-адресов в "черный" или "белый" списки: deny / allow. Но можно указать и конкретный IP-адрес, если снять галочку с опции "Assign a Range of addresses".

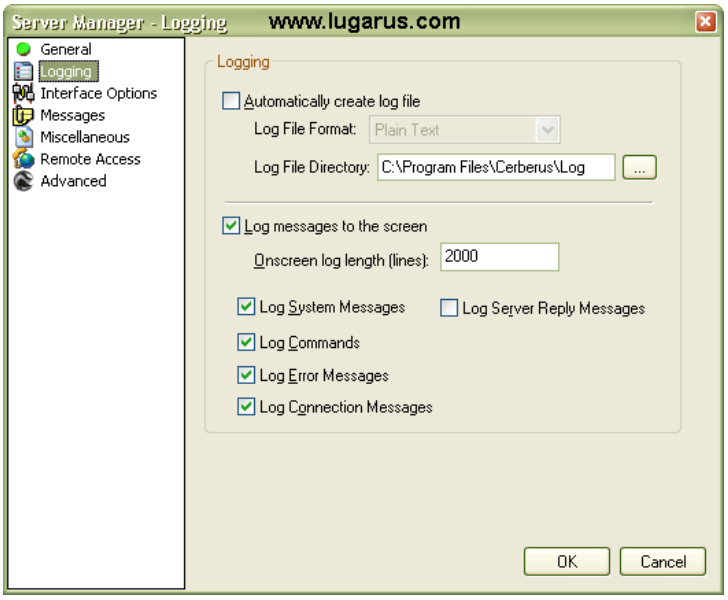
Вкладка "Auto-Blocking" более интересна:

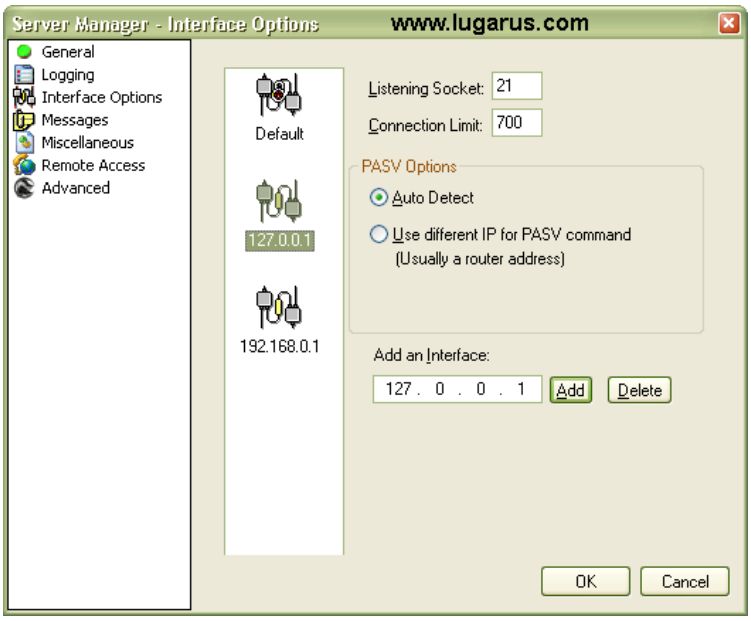


"Enable Auto-Blocking (DoS Protection)" - рекомендую сразу же включить эту опцию, будет только лучше. Ее цель: определять и блокировать подозрительные подключения. Наример, кто-то долго и безостановочно пытается подключиться к вашему FTP в надежде методом перебора найти логин/пароль для какой-либо группы пользователей? Установите значение "Failed Login Attempts before Auto-Block" (число неудачных попыток логина перед автоблокировкой) "5" и через это число попыток наглому пользователю будет блокирован доступ к серверу. Время и режим блокировки определите чуть ниже: блокировать на XX минут или навсегда. Все блокированные адреса помещаются в окно "IP addresses (being watched)", откуда ошибочно блокированный адрес можно удалить кнопкой "Delete".



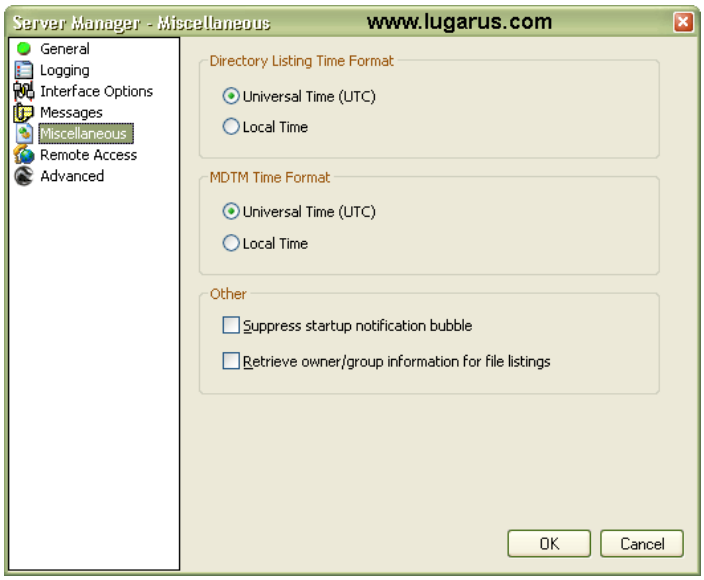
"Use idle connection time" - по истечении указанного времени неактивные пользователи будут отключены от сервера



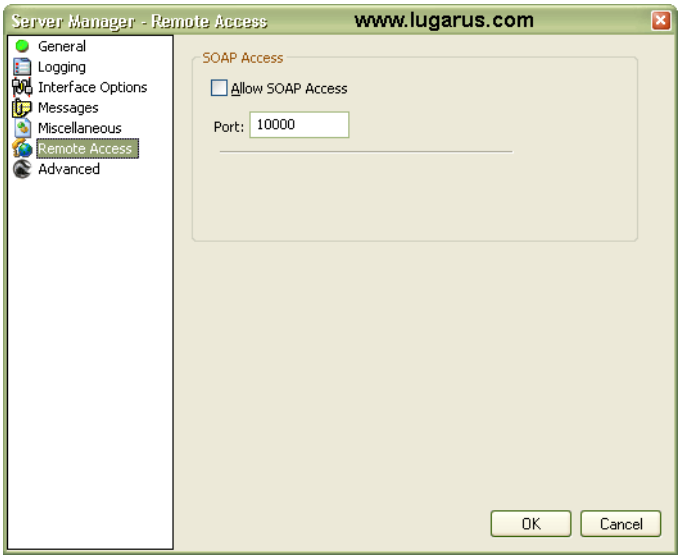


Здесь можно настроить дополнительные интерфейсы сервера. Напрммер, если у вас есть реальный IP и вы хотите сделать свой FTP доступным из внешнего интернета, то можете создать новый интерфейс, наример, 194.146.135.129. Для локальной же сети можно включить отдельный интерфейс 10.10.10.10. Дефолтовый интерфейс 127.0.0.1 будет пригоден для тестирования сервера в пределах одного компьютера. Переключение или включение дополнительных интерфейсов можно производить в главном окне сервера - "Interface".

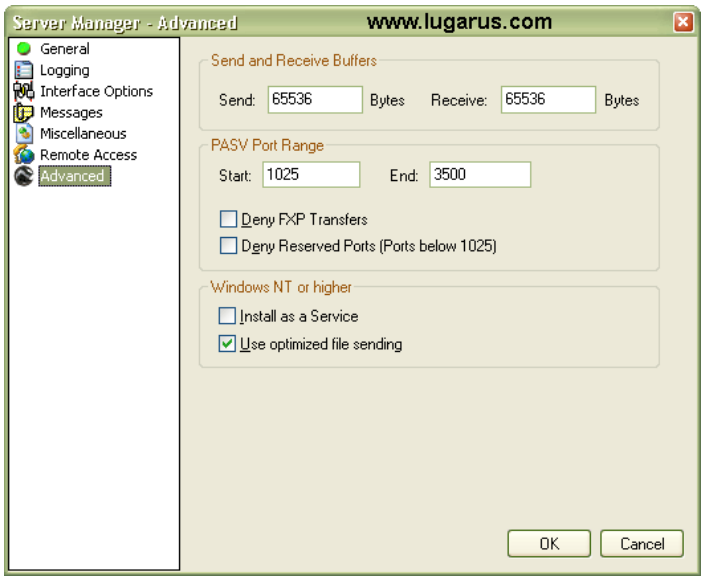
Это сообщения вашего сервера, которые выдаются пользователю при подключении и отключении от FTP.



Укажите, какое время использовать при отображении каталогов: мировое или локальное, которое сейчас установлено на вашем компьютере. Здесь же можно подавить вывод информационных стартовых сообщений.



Возможность удаленного администрирования сервера.



Определение размеров буферов приема-передачи, установка FTP сервера как системного сервиса (чтобы мог стартовать одновременно с операционной системой), запрет на передачу файлов "сервер-сервер" (Deny FXP Transfers - некоторые клиенты умеют делать такую передачу)

4 Содержание отчета

Лабораторная работа рассчитана на 2 часа для очной и 3 часа для заочной форм обучения направления подготовки 11.03.02 и выполняется в 1-й контрольной точке.

Отчет по работе должен включать:

- цель работы;
- краткие теоретические сведения;
- исходные данные работы;
- порядок выполнения работы;
- основные полученные результаты;
- выводы по работе с анализом полученных результатов;
- ответы на контрольные вопросы.

Минимальный балл за практическую работу составляет 0.5 балла (выполнил работу, но не защитил). Максимальный балл – 4 (выполнил работу и защитил без замечаний).

Примерные критерии оценки качества отчётов по лабораторной работе:

– оформление отчёта не соответствует предъявляемым требованиям – минус 0,5 балла;

– полученные экспериментальные материалы не обработаны (осциллограммы, спектрограммы и т. п.) – минус 0.5 балла;

– выводы не соответствуют результатам работы – минус 0,5 балла;

– работа защищена не вовремя (после окончания 1й контрольной точки) – минус 0.5 балла.

5 Контрольные вопросы

1. Раскройте понятие сервера.
2. Назовите известные типы серверов?
3. Перечислите операционные системы для серверов?
4. Можно ли открывать файлы на редактирование по FTP-протоколу?
5. Какие операции с файлами позволяет выполнять FTP-протокол?
6. Какие операции с файлами позволяет выполнять HTTP-протокол?
7. Можно ли разграничить доступ к файлам через HTTP протокол?
8. Что такое LOGIN, NIC, PASSWORD? Что требуется для указания доступа черезFTP протокол?
9. Перечислите программы, которые являются FTP или HTTP серверами?
10. Какие программы позволяют сохранять данные в виде web-страницы?

6 Список использованных источников

1. Основы построения телекоммуникационных систем и сетей [Текст] : учебник / под ред.: В. Н. Гордиенко, В. И. Крухмалева. - 2-е изд., испр. - М. : Горячая линия - Телеком, 2008. - 424 с.

2. Проектирование и техническая эксплуатация цифровых телекоммуникационных систем и сетей [Текст] : учебное пособие / Е. Б. Алексеев [и др.] ; под ред. В. Н. Гордиенко и М. С. Тверецкого. - Москва : Горячая линия-Телеком, 2014. - 391 с.

3. Крук, Б. И. Телекоммуникационные системы и сети [Текст] : учебное пособие / Б. И. Крук, В. Н. Попантонопуло, В. П. Шувалов ; под ред. В. П. Шувалова. - 4-е изд., испр. и доп. - Москва : Горячая линия - Телеком. Т. 1 : Современные технологии. - 2013. - 620 с.

4. Пескова, С. А. Сети и телекоммуникации [Текст] : учебное пособие / С. А. Пескова, А. В. Кузин, А. Н. Волков. - 2-е изд., стер. - М. : Академия, 2007. - 352 с.

5. Основы построения систем и сетей передачи информации [Текст] : учебное пособие / В. В. Ломовицкий [и др.]. - М. : Горячая линия - Телеком, 2005. - 382 с.

6. Шарипов, Ю. К. Отечественные телекоммуникационные системы [Текст] : учебное пособие / Ю. К. Шарипов, В. К. Кобляков. - 3-е изд., перераб. и доп. - М. : Логос, 2005. - 832 с.

7. Пятибратов, А. П. Вычислительные системы, сети и телекоммуникации [Электронный ресурс] : учебник / А. П. Пятибратов, Л. Гудыно, А. Кириченко. - 4-е изд., перераб. и доп. - Москва : Финансы и статистика, 2013. - 736 с. // Режим доступа - http://biblioclub.ru/index.php?page=book&id=220195