Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Локтионова Оксана Геннадьевна
Должность: проректор по учебной работе
Дата подписания: 17.01.2024 12:33:07
Уникальный программный ключ:
0b817ca911e6668abb13a5d426d39e5f1c11eabbf73e943df4a4851fda56d089

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

Кафедра вычислительной техники

УТВЕРЖДАЮ
Проректор по учебной работе
_____ О.Г. Локтионова
«20» 09 2022 г.

АДМИНИСТРИРОВАНИЕ ОПЕРАЦИОННЫХ СИСТЕМ

Методические указания к выполнению практических заданий для студентов направления подготовки 09.04.01 Информатика и вычислительная техника

Курск 2022

УДК 004

Составитель Д.О. Бобынцев

Рецензент: к.т.н., доцент Ватутин Э.И.

Администрирование операционных систем: методические указания к выполнению практических заданий / Юго-Зап. гос. ун-т; сост.: Д.О. Бобынцев. Курск, 2022. 34 с. Библиогр.: с. 34.

Содержит методические указания к выполнению практических заданий по дисциплине «Администрирование операционных систем». Указывается порядок выполнения работ, контрольные вопросы. Предназначено для студентов направления подготовки «Информатика и вычислительная техника».

Текст печатается в авторской редакции

Подписано в печать . Формат 60х84 1/16.
Усл.печ. л. 1,98. Уч.-изд. л. 1,79. Тираж 100 экз. Заказ Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

Содержание

Для выполнения данного курса работ Вам понадобится виртуальная машина с установленной серверной операционной системой Ред ОС 7.3 на базе ОС Linux. Для создания машины рекомендуем пользоваться бесплатной платформой Oracle VM Virtual Box. Поскольку в список известных операционных систем у этой платформы не входит Ред ОС, выбирайте тип операционной системы на этапе создания Other Linix соответствующей разрядности. Виртуальный жёсткий диск создавайте на том физическом диске, где для него будет достаточно места в соответствии с его объёмом!

Скачать образ операционной системы Ред ОС Вы можете с официального сайта http://red-soft.ru/ Не забудьте указать на этапе установки, что Вам нужна серверная версия с графическим интерфейсом, иначе по умолчанию будет установленная версия для рабочей станции, а также провести базовую настройку, в частности, задать пароль верховного администратора root, и создать одну простую учётную запись с правами администратора для обычного входа в систему (можно без пароля).

Настройка межсетевого экрана

Цель работы: получение практических навыков настройки средств сетевой защиты, используемых в операционной системе Ред ОС.

Базовые понятия брандмауэра

Демон (фоновая служебная программа) firewalld управляет группами правил при помощи так называемых зон. Зоны – это, по сути, наборы правил, которые управляют трафиком на основе уровня доверия к той или иной сети. Зоны присваиваются сетевым интерфейсам и управляют поведением брандмауэра.

Компьютеры, которые часто подключаются к разным сетям (например, ноутбуки) могут использовать зоны, чтобы изменять наборы правил в зависимости от среды. К примеру, при подключении к общественной сети W-iFi брандмауэр может применять более строгие правила, а в домашней сети ослаблять ограничения.

В firewalld существуют следующие зоны:

- drop: самый низкий уровень доверия сети. Весь входящий трафик сбрасывается без ответа, поддерживаются только исходящие соединения.
- block: эта зона похожа на предыдущую, но при этом входящие запросы сбрасываются с сообщением icmp-host-prohibited или icmp6-adm-prohibited.
- public: эта зона представляет публичную сеть, которой нельзя доверять, однако поддерживает входящие соединения в индивидуальном порядке.
- external: зона внешних сетей. Поддерживает маскировку NAT, благодаря чему внутренняя сеть остается закрытой, но с возможностью получения доступа.
- internal: обратная сторона зоны external, внутренние сети. Компьютерам в этой зоне можно доверять. Доступны дополнительные сервисы.
- dmz: используется для компьютеров, расположенных в DMZ (изолированных компьютеров, которые не будут иметь доступа к остальной части сети); поддерживает только некоторые входящие соединения.
- work: зона рабочей сети. Большинству машин в сети можно доверять. Доступны дополнительные сервисы.
- home: зона домашней сети. Окружению можно доверять, но поддерживаются только определённые пользователем входящие соединения.
- trusted: всем машинам в сети можно доверять.

Правила firewalld бывают постоянными и временными. Если в наборе появляется или изменяется какое-либо правило, текущее поведение брандмауэра изменяется сразу. Однако после перезагрузки все изменения будут утрачены, если их не сохранить.

Большинство команд firewall-cmd может использовать флаг –permanent, который сохранит правило, после чего оно будет использоваться на постоянной основе.

Чтобы включить брандмауэр, для начала нужно включить демон. Unit-файл systemd называется firewalld.service. Чтобы запустить демон, введите:

sudo systemctl start firewalld.service

Убедитесь, что сервис запущен:

firewall-cmd --state

Теперь брандмауэр запущен и работает, согласно конфигурации по умолчанию.

На данный момент сервис включен, но не будет запускаться автоматически вместе с сервером. Чтобы случайно не заблокировать себя на собственном сервере, сначала создайте набор правил, а затем настройте автозапуск.

Стоит сделать небольшое замечание по поводу GUI-интерфейса, он очень удобен, но совершенно не гибок в отличие от способа, если бы мы конфигурировали МЭ через консольные команды. Об этом прямо говорит справка при открытии GUI.

Чтобы узнать, какая зона используется по умолчанию, введите:

firewall-cmd --get-default-zone

На данный момент firewalld не получал никаких инструкций относительно других зон, кроме того, к другим зонам не привязан ни один интерфейс, поэтому сейчас зона public является зоной по умолчанию, а также единственной активной зоной. Чтобы получить список активных зон, введите:

firewall-cmd --get-active-zones

Вы увидите, что к зоне public привязаны сетевые интерфейсы. Интерфейсы, привязанные к зоне, работают согласно правилам этой зоны. *Покажите результат преподавателю.* Чтобы узнать, какие правила использует зона по умолчанию, введите:

firewall-cmd --list-all

Покажите результат преподавателю.

Итак, теперь вы знаете, что:

1) public является зоной по умолчанию и единственной активной зоной;
2) к ней привязаны интерфейсы;
3) она поддерживает трафик DHCP (присваивание IP-адресов) и SSH (удаленное администрирование).

Теперь следует ознакомиться с другими зонами. Чтобы получить список всех доступных зон, введите:

firewall-cmd --get-zones

Покажите результат преподавателю.

Чтобы получить параметры конкретной зоны, добавьте в команду флаг --zone=.

firewall-cmd --zone=home --list-all

Чтобы вывести определения всех доступных зон, добавьте опцию --list-all-zones. Для более удобного просмотра вывод можно передать в пейджер:

firewall-cmd --list-all-zones | less

Покажите результат преподавателю.

Изначально все сетевые интерфейсы привязаны к зоне по умолчанию. Чтобы перевести интерфейс в другую зону на одну сессию, используйте опции --zone= и --change-interface=.

Выберите наименование активного интерфейса и наберите:

sudo firewall-cmd --zone=home --change-interface= <наименование интерфейса>

Если получен результат success, перевод прошёл успешно.

Примечание: При переводе интерфейса в другую зону нужно учитывать, что это может повлиять на работу некоторых сервисов. К примеру, зона home поддерживает SSH, поэтому соединения этого сервиса не будут сброшены. Но некоторые зоны сбрасывают все соединения, включая SSH, и тогда вы можете случайно заблокировать себе доступ к собственному серверу.

Чтобы убедиться, что интерфейс привязан к новой зоне, введите:

firewall-cmd --get-active-zones

Покажите результат преподавателю.

После перезагрузки брандмауэра интерфейс будет снова привязан к зоне по умолчанию. Проверьте и *окажите результат преподавателю:*

sudo systemctl restart firewalld.service

Если в настройках интерфейса не указана никакая другая зона, после перезапуска брандмауэра интерфейс будет снова привязан к зоне по умолчанию. В РЕД ОС такие конфигурации хранятся в каталоге /etc/sysconfig/network-scripts, в файлах формата ifcfg-interface.

Чтобы определить зону интерфейса, откройте конфигурационный файл этого интерфейса, например:

sudo nano /etc/sysconfig/network-scripts/ifcfg-enp0s3

В конец файла добавьте переменную ZONE= и в качестве значения укажите другую зону, например, home:

Содержимое файла:

```
. . .
 DNS1=2001:4860:4860::8844
 DNS2=2001:4860:4860::8888
 DNS3=8.8.8.8
 ZONE=home
```

Сохраните и закройте файл.

Чтобы обновить настройки, перезапустите сетевой сервис и брандмауэр:

```
sudo systemctl restart network.service
sudo systemctl restart firewalld.service
```

После перезапуска указанный Вами интерфейс будет привязан к зоне home. *Покажите результат преподавателю.*

```
firewall-cmd --get-active-zones
```

Также Вы можете выбрать другую зону по умолчанию. Для этого используется параметр --set-default-zone=. После этого все интерфейсы будут привязаны к другой зоне:

```
sudo firewall-cmd --set-default-zone=home
```

Проще всего добавить сервис или порт в зону, которую использует брандмауэр. Просмотрите доступные сервисы и *покажите результат преподавателю*:

```
firewall-cmd --get-services
```

Примечание: Больше информации о каждом конкретном сервисе можно найти в файлах .xml в каталоге /usr/lib/firewalld/services. К пример, сведения о сервисе SSH хранятся в /usr/lib/firewalld/services/ssh.xml и выглядят так:

```
<?xml version="1.0"
encoding="utf-8"?>
<service>
<short>SSH</short>
<description>Secure
Shell (SSH) is a protocol for logging into and executing commands on
remote machines. It provides secure encrypted communications. If you
```

plan on accessing your machine remotely via SSH over a firewalled

interface, enable this option. You need the openssh-server package installed for this option to be useful.</description>

<port

protocol="tcp" port="22"/>

</service>

Чтобы включить поддержку сервиса в той или иной зоне, используйте опцию --add-service=. Указать целевую зону можно с помощью опции --zone=. По умолчанию эти изменения будут работать в течение одной сессии. Чтобы сохранить изменения и использовать их на постоянной основе, добавьте флаг --permanent.

Например, чтобы запустить веб-сервер для обслуживания трафика HTTP, для начала нужно включить поддержку этого трафика в зоне public на одну сессию:

sudo firewall-cmd --zone=public --add-service=http

Если сервис нужно добавить в зону по умолчанию, флаг --zone= можно опустить.

Убедитесь, что операция выполнена успешно, и *покажите результат преподавателю*:

firewall-cmd --zone=public --list-services

Протестируйте работу сервиса и брандмауэра. Если всё работает правильно, можно изменить постоянный набор правил и добавить в него правило для поддержки этого сервиса.

sudo firewall-cmd --zone=public --permanent --add-service=http

Чтобы просмотреть список постоянных правил, введите:

sudo firewall-cmd --zone=public --permanent --list-services

Покажите результат преподавателю.

Теперь зона public поддерживает HTTP и порт 80 на постоянной основе. Если веб-сервер может обслуживать трафик SSL/TLS, вы также можете добавить сервис https (для одной сессии или в набор постоянных правил):

sudo firewall-cmd --zone=public --add-service=https

sudo firewall-cmd --zone=public --permanent --add-service=https

Что делать, если нужный сервис недоступен? Брандмауэр firewalld по умолчанию включает в себя многие наиболее распространённые сервисы. Однако некоторым приложениям

необходимы сервисы, поддержка которых отсутствует в firewalld. В таком случае вы можете поступить двумя способами.

Способ 1: Настройка порта

Проще всего в такой ситуации открыть порт приложения в необходимой зоне брандмауэра. Нужно просто указать порт или диапазон портов и протокол.

Например, приложение, которое использует порт 5000 и протокол TCP, нужно добавить в зону public. Чтобы включить поддержку приложения на одну сессию, используйте параметр --add-port= и укажите протокол tcp или udp.

sudo firewall-cmd --zone=public --add-port=5000/tcp

Убедитесь, что операция прошла успешно:

firewall-cmd --list-ports

5000/tcp

Также можно указать последовательный диапазон портов, отделив первый и последний порт диапазона с помощью тире. Например, если приложение использует UDP-порты 4990-4999, чтобы добавить их в зону public, нужно ввести:

sudo firewall-cmd --zone=public --add-port=4990-4999/udp

После тестирования можно добавить эти правила в постоянные настройки брандмауэра.

sudo firewall-cmd --zone=public --permanent --add-port=5000/tcp

sudo firewall-cmd --zone=public --permanent --add-port=4990-4999/udp

sudo firewall-cmd --zone=public --permanent --list-ports

success

success

4990-4999/udp 5000/tcp

Способ 2: Определение сервиса

Добавлять порты в зоны просто, но, если у вас много таких приложений, в результате будет сложно отследить, для чего предназначен тот или иной порт. Чтобы избежать такой ситуации, можно вместо портов определить сервисы.

Сервисы – это просто наборы портов с определённым именем и описанием. С помощью сервисов проще управлять настройками, но сами по себе они сложнее, чем порты.

Для начала нужно скопировать существующий сценарий из каталога /usr/lib/firewalld/services в каталог /etc/firewalld/services (здесь брандмауэр ищет нестандартные настройки).

Например, можно скопировать определение сервиса SSH и использовать его для определения условного сервиса example. Имя сценария должно совпадать с именем сервиса и иметь расширение .xml.

sudo cp /usr/lib/firewalld/services/service.xml /etc/firewalld/services/example.xml

Откорректируйте скопированный файл.

sudo nano /etc/firewalld/services/example.xml

В файле находится определение SSH:

<?xml version="1.0"
encoding="utf-8"?>
<service>
<short>SSH</short>
<description>Secure Shell (SSH) is a protocol for logging into and executing commands on remote machines. It provides secure encrypted communications. If you plan on accessing your machine remotely via SSH over a firewalled interface, enable this option. You need the openssh-server package installed for this option to be useful.</description>
<port protocol="tcp" port="22"/>
</service>

Большую часть определения сервиса составляют метаданные. Изменить краткое имя сервиса можно в тегах. Это человекочитаемое имя сервиса. Также нужно добавить описание сервиса. Единственное изменение, которое повлияет на работу сервиса – это изменение номера порта и протокола.

Вернёмся к сервису example; допустим, он требует открыть TCP- порт 7777 и UDP- порт 8888. Определение будет выглядеть так:

<?xml version="1.0"
encoding="utf-8"?>
<service>
<short>Example Service</short>

<description>This is just an example service. It probably shouldn't be used on a real system.</description>

<port protocol="tcp" port="7777"/>

<port protocol="udp" port="8888"/>

</service>

Сохраните и закройте файл.

Перезапустите брандмауэр:

sudo firewall-cmd --reload

Теперь сервис появится в списке доступных сервисов:

firewall-cmd

--get-services

RH-Satellite-6 amanda-client bacula bacula-client

dhcp dhcpv6 dhcpv6-client dns example ftp high-availability http

https imaps ipp ipp-client ipsec kerberos kpasswd ldap ldaps libvirt

libvirt-tls mdns mountd ms-wbt mysql nfs ntp openvpn pmcd pmproxy

pmwebapi pmwebapis pop3s postgresql proxy-dhcp radius rpc-bind samba

samba-client smtp ssh telnet tftp tftp-client transmission-client

vnc-server wbem-https

Брандмауэр предоставляет много предопределенных зон, которых в большинстве случаев достаточно для работы. Но в некоторых ситуациях возникает необходимость создать пользовательскую зону. Например, для веб-сервера можно создать зону publicweb, а для DNS-сервиса – зону privateDNS. Создавая зону, нужно добавить её в постоянные настройки брандмауэра.

Попробуйте создать зоны publicweb и privateDNS:

sudo firewall-cmd --permanent --new-zone=publicweb

sudo firewall-cmd --permanent --new-zone=privateDNS

Убедитесь, что зоны существуют:

sudo firewall-cmd --permanent --get-zones

Покажите результат преподавателю.

В текущей сессии новые зоны не будут доступны:

firewall-cmd --get-zones

Чтобы получить доступ к новым зонам, нужно перезапустить брандмауэр:

sudo firewall-cmd --reload

firewall-cmd --get-zones

Покажите результат преподавателю

Теперь вы можете присвоить новым зонам требуемые сервисы и порты. К примеру, в зону publicweb можно добавить SSH, HTTP и HTTPS.

sudo firewall-cmd --zone=publicweb --add-service=ssh

sudo firewall-cmd --zone=publicweb --add-service=http

sudo firewall-cmd --zone=publicweb --add-service=https

firewall-cmd --zone=publicweb --list-all

Покажите результат преподавателю.

В зону privateDNS можно добавить DNS:

sudo firewall-cmd --zone=privateDNS --add-service=dns

firewall-cmd --zone=privateDNS --list-all

Покажите результат преподавателю.

Затем можно привязать сетевые интерфейсы к новым зонам:

sudo firewall-cmd --zone=publicweb --change-interface=eth0

sudo firewall-cmd --zone=privateDNS --change-interface=eth1

Теперь можно протестировать настройку. Если всё работает правильно, вы можете добавить эти правила в постоянные настройки.

sudo firewall-cmd --zone=publicweb --permanent --add-service=ssh

sudo firewall-cmd --zone=publicweb --permanent --add-service=http

sudo firewall-cmd --zone=publicweb --permanent --add-service=https

sudo firewall-cmd --zone=privateDNS --permanent --add-service=dns

После этого можно настроить сетевые интерфейсы для автоматического подключения к правильной зоне.

К примеру, eth0 будет привязан к publicweb:

sudo nano /etc/sysconfig/network-scripts/ifcfg-eth0

Содержимое файла:

. . .

IPV6_AUTOCONF=no

DNS1=2001:4860:4860::8844

DNS2=2001:4860:4860::8888

DNS3=8.8.8.8

ZONE=publicweb

А интерфейс eth1 будет привязан к privateDNS:

sudo nano /etc/sysconfig/network-scripts/ifcfg-eth1

Содержимое файла:

. . .

NETMASK=255.255.0.0

DEFROUTE='no'

NM_CONTROLLED='yes'

ZONE=privateDNS

Перезапустите сетевые сервисы и брандмауэр:

sudo systemctl restart network

sudo systemctl restart firewalld

Проверьте зоны:

firewall-cmd --get-active-zones

privateDNS

interfaces: eth1

publicweb

interfaces: eth0

Убедитесь, что в зонах работают нужные сервисы:

firewall-cmd --zone=publicweb --list-services

http htpps ssh

firewall-cmd --zone=privateDNS --list-services

dns

Покажите результат проверки преподавателю.

Пользовательские зоны полностью готовы к работе. Вы можете сделать любую из них зоной по умолчанию. Например:

sudo firewall-cmd --set-default-zone=publicweb

Теперь, когда Вы проверили все настройки и убедились, что все правила работают должным образом, Вы можете настроить автозапуск брандмауэра. Для этого введите:

sudo systemctl enable firewalld

Теперь брандмауэр будет запускаться вместе с сервером. Брандмауэр firewalld – очень гибкий инструмент. Зоны позволяют быстро изменять политику брандмауэра.

Контрольные вопросы

1. Что такое демон в UNIX-системах?
2. Каким образом брандмауэр Ред ОС управляет правилами?
3. Что подразумевается под зоной в брандмауэре?
4. Какие виды зон использует брандмауэр?
5. Что нужно сделать, чтобы правило использовалось на постоянной основе?
6. Как добавить сервис или порт в зону?
7. Что подразумевается под сервисом и портом?
8. Как создать пользовательскую зону?

Организация домена IPA

Цель работы: получение навыков создания домена на основе сервера FreeIPA в операционной системе Ред ОС.

Теоретический материал

Домен IPA (FreeIPA) – это интегрированное решение идентификации и авторизации для РЕД ОС. Сервер FreeIPA обеспечивает централизованную аутентификацию, авторизацию и предоставление учетной информации путем хранения данных о пользователе, группах, хостах и других объектах, необходимых для управления аспектами безопасности компьютерной сети.

FreeIPA построена на основе хорошо известных Open Source компонентов и стандартных протоколов с очень сильной ориентацией на простоту управления и автоматизацию задач установки и настройки.

Несколько FreeIPA-серверов можно легко настроить в домене FreeIPA, чтобы обеспечить избыточность и масштабируемость. 389 Directory Server является основным хранилищем данных и предоставляет полный LDAPv3 мульти-мастер инфраструктуры каталогов. Аутентификация с использованием единого входа осуществляется через MIT Kerberos KDC. Возможности аутентификации дополняются интегрированным центром сертификации на основе проекта Dogtag. При желании можно управлять именами доменов с помощью интегрированного сервера DNS.

Управление полностью централизовано и управляется через веб-интерфейс или инструмент командной строки.

Зачем использовать домен IPA? Для обеспечения эффективности, соблюдения и снижения рисков организациям необходимо централизованно управлять и сопоставлять важную информацию о безопасности, включая:

1) идентификацию (машин, пользователей, виртуальных машин, групп, учетных данных для проверки подлинности);
2) политики (управление доступом на основе хоста, правил sudo, пользовательских карт SELINUX);

3) SSO - технология единого доступа к различным сервисам и ресурсам.

Домен на основе IPA сфокусирован на том, чтобы информация о пользователе, политиках и аудите была легко централизованной, совместимой и управляемой. Так же, имеет возможность взаимодействовать с Windows доменами и многое другое.

Для развёртывания домена IPA имеется ряд рекомендаций. DNS преднамеренно отображается первым, поскольку DNS играет важную роль в функциях управления идентификацией, особенно Kerberos.

IPA всегда должен иметь собственный основной домен, например example.ru или ipa.example.ru, который не должен использоваться совместно с другой системой управления идентификацией на основе Kerberos, поскольку в противном случае на уровне системы Kerberos будут возникать конфликты. Например, если IPA и Active Directory используют один и тот же домен, доверительные отношения никогда не будут возможны, а также автоматическое обнаружение клиентского сервера через DNS SRV-записи.

Избегайте коллизий имен. Настоятельно рекомендуется не использовать доменное имя, которое не делегировано Вам, даже в частной сети. Например, Вы не должны использовать доменное имя example.ru, если у Вас нет действительного делегирования для него в общедоступном дереве DNS. Если это правило не соблюдается, доменное имя будет разрешено по-разному в зависимости от конфигурации сети. В результате сетевые ресурсы станут недоступными. Использование доменных имен, которые не делегированы Вам, также затрудняет развертывание и обслуживание DNSSEC. Дополнительную информацию об этой проблеме можно найти в FAQ ICANN по вопросам коллизий доменных имен.

Клиентские машины не обязательно должны находиться в том же домене, что и IPA-серверы. Например, IPA может быть доменом ipa.example.ru и иметь клиентов в домене clients.example.ru, просто нужно иметь четкое сопоставление между доменом DNS и областью Kerberos. Стандартным методом для создания

сопоставления являются записи TXT DNS. (IPA DNS добавляет их автоматически.)

Не называйте свой домен .local! Он зарезервирован для автоматически конфигурируемых сетей.

Если нужно получить доступ к ресурсам в уже существующей среде (Windows AD), то необходимо внести изменения в процесс разрешения хостов на linux-машине. Отредактируйте /etc/nsswitch.conf. Изначально интересующий нас раздел содержит следующие записи:

hosts: files mdns4_minimal [NOTFOUND=return] dns

Соответственно, в этом режиме сначала производится поиск в файле /etc/hosts, затем запрос идет к mdns, после чего возвращается ответ "не найдено". Mdns кэширует данные и работает с демоном Avahi. Модифицируйте эту "схему" к классическому виду:

hosts: files dns

Домен Active Directory – сложная система. Он включает в себя логически структурированный набор ресурсов (машины, пользователи, службы и т. Д.), которые принадлежат потенциально нескольким доменам DNS. Несколько доменов DNS могут быть частью одного домена AD (где домен AD по определению совпадает с областью AD Kerberos). Несколько доменов AD можно объединить в лес. Самый первый домен AD, созданный в лесу, называется лесной корневой домен. Верхнее имя основного домена DNS домена AD используется как имя домена Kerberos AD.

Домен IPA тоже представляет собой сложную систему. Он включает в себя логически структурированный набор ресурсов (машины, пользователи, службы и т. Д.), которые принадлежат потенциально нескольким доменам DNS. В отличие от Active Directory, у нас есть один домен / область IPA для развертывания, а для Active Directory этот единственный домен IPA выглядит как отдельный лес Active Directory. Active Directory считает основной домен DNS, используемый в качестве основы для области Kerberos IPA, как корневой домен леса для домена IPA (например, корневой домен леса для Active Directory).

Домен IPA может быть размещен в любом домене DNS, который не имеет прямого совпадения с любым доменом в лесу Active Directory. Он может быть, например, ipa.example.ru, если эта

зона DNS не занята каким-либо другим доменом AD в том же лесу. Или может быть ipa.ad.example.ru, если нет перекрытий на одном уровне зоны DNS.

Доверие между двумя лесами Active Directory всегда устанавливается как доверие между корневыми доменами этих лесов. Если домен IPA использует ipa.ad.example.ru в качестве основной зоны DNS, мы будем говорить об установлении доверительного отношения к лесу между лесом Active Directory ad.example.ru и доменом IPA ipa.ad.example.ru. Если существует несколько зон DNS, принадлежащих домену IPA, рекомендуется размещать записи kerberos указывающие на имя области IPA в каждом из них для правильного обнаружения сетевых ресурсов клиентами IPA.

Домен IPA может обслуживаться либо интегрированной службой DNS, либо внешней службой. Рекомендуется использовать интегрированную службу DNS. При использовании интегрированной службы DNS пакет bind-dyndb-ldap должен быть установлен перед разворачиванием IPA сервера.

При использовании внешнего сервера имен возможно использование функций управления идентификацией или доверия, однако конфигурация будет намного сложнее и подвержена ошибкам.

Когда Вы начинаете устанавливать сервер IPA, Вы всегда определяете имя области Kerberos для этой установки. При выборе названия области выполните следующие правила:

1. Имя области не должно конфликтовать с любым другим существующим именем области Kerberos (например, имя, используемое Active Directory).
2. Имя области должно быть верхним регистром (EXAMPLE.RU) основного DNS-имени домена (example.ru).
3. Клиенты IPA из разных доменов DNS (example.net, example.org, example.com) могут быть объединены в единую область Kerberos (EXAMPLE.RU)
4. Одна установка IPA всегда представляет собой единую область Kerberos.

ВАЖНО:

Невозможно изменить основной домен и область IPA после установки. Продумайте его тщательно. Не ожидайте перехода от лабораторной / промежуточной среды к рабочей среде (например, сменить lab.example.ru на ipa.example.ru)

Серверы и клиенты IPA могут распространяться в разных географических точках. Механизм местоположения DNS позволяет разделить топологию на отдельные области, называемые местоположениями. Клиенты, использующие записи DNS SRV (например, SSSD) в одном месте, используют близлежащие серверы IPA.

При планировании развертывания важно иметь в виду, что функции DNS в IPA требуют, по крайней мере, одного DNS-сервера в каждом месте. Если это необходимо, можно использовать несколько DNS-представлений на внешних DNS-серверах вместо развертывания DNS-сервера для каждого местоположения, но такие настройки обычно менее устойчивы.

Когда выполнена настройка PKI, хосты и службы IPA могут получать подписанные сертификаты от IPA CA (корневой сертификат). Затем сертификаты могут использоваться для аутентификации или проверки подлинности в настроенных службах.

В настоящее время существует 3 типа настройки среды сертификатов IPA:

1. Без смешивания – IPA просто устанавливается с собственной службой PKI и самозаверяющим сертификатом CA.
2. Внешний CA – IPA установлен с собственной PKI, но сертификат CA подписан внешним центром сертификации (служба сертификации Active Directory или другая пользовательская служба сертификации). Для этого требуется, чтобы внешний ЦС (центр сертификации) разрешил субцентры.
3. Установка без CA – IPA не настраивает собственный ЦС, но использует подписанные сертификаты хоста из внешнего ЦС.

ВАЖНО

После установки невозможно изменить базу данных сертификата IPA. Продумайте это тщательно. По умолчанию используется O = $ REALM

Настоятельно рекомендуется избегать развертывания других приложений или служб на виртуальной машине IPA по нескольким основным причинам:

1. Причины производительности - сервер IPA может быть ресурсозатратным для машины, особенно когда количество объектов LDAP велико.
2. Стабильность - IPA интегрирована в систему, и если стороннее приложение меняет конфигурацию или службы IPA, домен может сломаться
3. Легче перенести сервер IPA на более новую платформу

IPA работает в реплицированной среде с несколькими мастерами. Количество серверов зависит от нескольких факторов:

1. Сколько записей в системе?
2. Сколько у Вас разных географически распределенных центров обработки данных?
3. Насколько активны приложения и клиенты в отношении аутентификации и поиска LDAP.

Как правило, рекомендуется иметь по меньшей мере 2-3 реплики в каждом центре обработки данных. В каждом центре обработки данных должна быть по крайней мере одна реплика с дополнительными службами IPA, такими как PKI или DNS, если они используются. Обратите внимание, что не рекомендуется иметь более 4 реплик в одном месте. В следующем примере показана рекомендуемая инфраструктура (рис. 1):

У каждого клиента для отказоустойчивости должно быть, как минимум, два DNS сервера, настроенных в /etc/resolv.conf. Обновите конфигурацию resolv.conf и DHCPd.

Для каждого клиента, использующего ipa-client-install, требуется доступ к порту 443 (HTTPS) на сервере IPA. Это связано с тем, что после регистрации клиент загружает собственные ключи SSH и выполняет несколько операций. IPI CLI также использует тот же порт для связи с ведущим IPA. Таким образом, требуется доступ к HTTPS (443) с клиентской стороны.

Чтобы настроить доверительные отношения, необходимо правильно настроить DNS, IPA должен иметь собственный первичный DNS-домен, и соответствующую ему область Kerberos. DNS-домен и область Kerberos должны отличаться от домена DNS Active Directory.

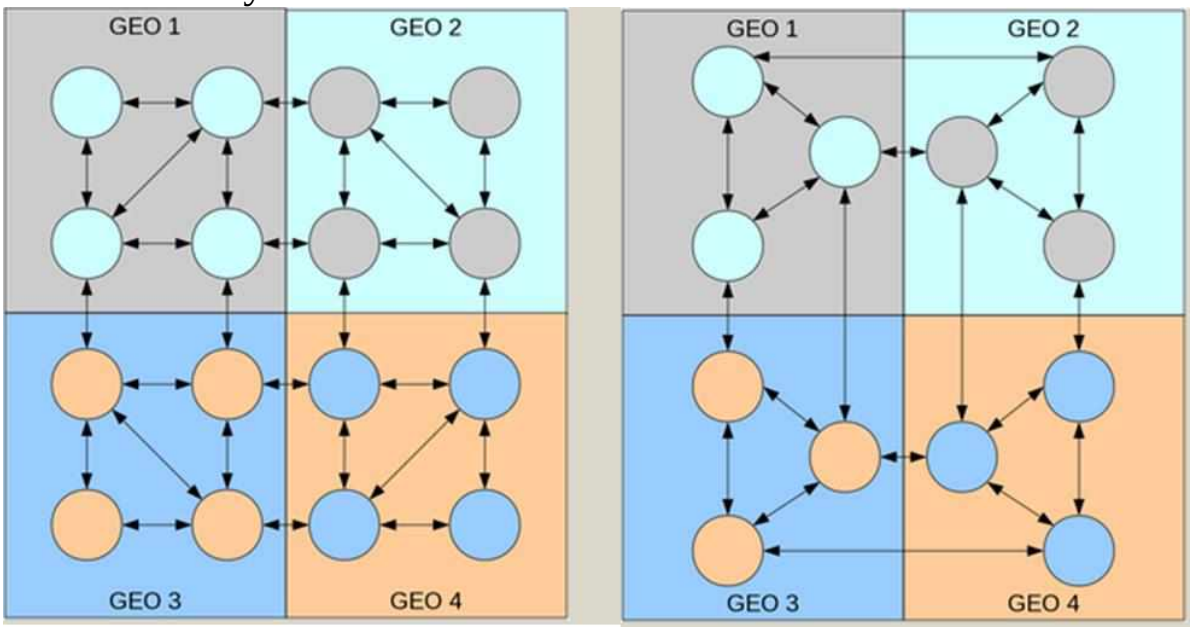

Рисунок 1 – Рекомендуемая инфраструктура реплик

Ещё одним важным требованием является стек IPv6. Рекомендуемым способом для современных сетевых приложений является только открытие сокетов IPv6 для прослушивания, поскольку IPv4 и IPv6 используют один и тот же диапазон локальных портов. IPA использует Samba как часть интеграции с Active Directory, а Samba требует включенного стека IPv6 на машине.

НЕ используйте ipv6.disable = 1 в командной строке ядра: он отключает весь стек IPv6 и ломает Samba.

Если необходимо, добавьте ipv6.disable_ipv6 = 1, это будет поддерживать функциональность стека IPv6, но не будет назначать адреса IPv6 для ваших сетевых устройств. Это рекомендуемый подход для случаев, когда вы не используете сети IPv6.

Добавление следующих строк в /etc/sysctl.d/ipv6.conf, позволит не назначать адреса IPv6 для определенного сетевого интерфейса:

net.ipv6.conf.all.disable_ipv6 = 1

Отключение «все» не применяется к интерфейсам, которые уже используются, когда применяются параметры sysctl.

net.ipv6.conf.<интерфейс0>.disable_ipv6 = 1

где interface0 – Ваш специализированный интерфейс. Обратите внимание, что все, что нам нужно, это то, чтобы стек IPv6 был включен на уровне ядра, это рекомендуется для разработки сетевых приложений уже давно.

Из-за CVE-2014-3566 протокол протокола Secure Socket Layer версии 3 (SSLv3) должен быть отключен в модуле mod_nss. Вы можете сделать это, выполнив следующие шаги:

Отредактируйте файл/etc/httpd/conf.d/nss.conf и установите параметр NSSProtocol (для обратной совместимости) и TLSv1.1.

NSSProtocol TLSv1.0, TLSv1.1

Перезапустите httpd-службу.

service httpd restart

Выполнение работы

Перед установкой настройте сетевой адаптер и сделайте IP-адрес сервера статическим. Он никогда не должен изменяться! Если есть необходимость, пропишите в файле /etc/chrony.conf сервера времени перед стандартными.

Назначьте имя серверу формата Ваше_имя.шифр_группы.ru. Используйте полное доменное имя. Имя серверу можно назначить командой

hostnamectl set-hostname <имя>

Установите IPA сервер. Если Вы используете РЕД ОС версии 7.1 или 7.2, выполните команду:

yum -y install bind bind-dyndb-ldap ipa-server ipa-server-dns ipa-server-trust-ad

Если Вы используете РЕД ОС 7.3 и старше, выполните команду:

dnf -y install bind bind-dyndb-ldap ipa-server ipa-server-dns ipa-server-trust-ad

После установки, убедитесь, что используется Java OpenJDK версии 8:

java -version

Если используется Java 11, то необходимо переключиться на 8-ую версию. Для этого выполните команды:

update-alternatives --config java

update-alternatives --config jre_openjdk

в каждой выберите нужную версию, указав ее порядковый номер. После чего нажмите Enter.

Есть два варианта настройки, интерактивный и автоматический.

ВАЖНО!

Невозможно изменить конфигурацию после создания домена, и невозможно перенести его из одной конфигурации в другую. Крайне важно, чтобы требования были рассмотрены до начала процесса установки.

Если каждая машина в домене будет клиентом IPA, добавьте адрес сервера IPA в конфигурацию DHCP.

Примечание: сценарий ipa-replica-install включает в себя утилиту ipa-replica-conncheck, которая проверяет статус требуемых портов. Вы также можете запускать ipa-replica-conncheck отдельно для устранения неполадок.

После установки сервера, выполните интерактивную настройку. Воспользуйтесь командой ipa-server-install --mkhomedir

Помимо аутентификации, IPA может управлять DNS-записями для хостов. Это может облегчить настройку и управление хостами. Поэтому в процессе настройки Вы увидите следующее сообщение:

Do you want to configure integrated DNS (BIND)? [no]:

[no] означает, что при нажатии Enter установщик примет Ваш ответ "Нет", и конфигурация DNS будет пропущена. Чтобы выполнить её, наберите yes и нажмите Enter.

Далее нужно указать имя хоста сервера, доменное имя и пространство Kerberos.

Server host name [<имя хоста>]:

Нажмите Enter и увидите следующее сообщение:

Please confirm the domain name [<имя домена>]:

Установщик автоматически выделил в созданном Вами имени хоста имя домена. Подтвердите его.

Please provide a realm name [<имя пространства Kerberos>]:

Подтвердите пространство Kerberos. Затем создайте пароль для менеджера каталогов LDAP и пароль администратора IPA,

который будет использоваться при аутентификации в IPA в качестве администратора.

Добавляем ретранслятор службы имен (DNS relay). Этот шаг необязателен, и необходим в том случае, если у Вас предполагается использовать внешний сервер для обработки запросов службы имен DNS. Учитываете, что по-умолчанию, сервер IPA предполагает, что будет пользоваться собственным сервером имен, который развертывает локально.

Do you want to configure DNS forwarders? [yes]:

Выбирайте [yes] (да), в случае, если присутствует внешний ретранслятор службы имен, иначе, выбирайте [no] – нет. Далее впишите дополнительные реверс зоны, если они нужны.

Do you want to configure these servers as DNS forwarders?

Инициируем создание обратной зоны для службы имен.

Do you want to configure the reverse zone? [yes]:

Подтвердите конфигурацию. После этого запустится программа установки.

Continue to configure the system with these values? [no]: yes

Убедитесь, что сервер IPA работает:

kinit admin

ipa user-find admin

Покажите результаты преподавателю.

Ввод компьютера-клиента Ред ОС в домен IPA

Если возможности Вашего компьютера позволяют запустить одновременно две виртуальные машины с серверной и клиентской операционной системой Ред ОС, Вы можете попробовать добавить клиентскую машину в домен, создав виртуальную сеть между ними. Для этого в клиентской машине необходимо перед стартом включить второй сетевой адаптер с типом подключения Внутренняя сеть, а после загрузки операционной системы настроить сетевое подключение адаптера на статический IP-адрес из той же подсети, что и адрес сервера, а также указать, что DNS-сервером для этого подключения является Ваш сервер.

Когда настройки внутренней сети будут выполнены, оставьте на сервере активным только подключение со статическим IP. Проверьте из клиентской машины командой ping IP-адрес

доступность статического IP сервера. Если прозвон успешный, задайте клиенту имя. Он должен быть в области домена IPA сервера. Например, если ваш домен example.ru, то хостнейм клиента должен быть - client.example.ru

hostnamectl set-hostname client.example.ru

Пропишите настройки DNS и домен в создаваемом клиенте, укажите в качестве DNS ваш IPA сервер и опцию для того, чтобы по DHCP не принимался DNS адрес.

Для этого, используйте утилиту «Сетевые соединения», расположенную в «Меню» → «Параметры» → «Сетевые соединения» в графическом окружении Cinnamon или «Система» → «Параметры» → «Сетевые соединения» в графическом окружении Mate. Выберите ваше активное подключение, нажмите кнопку «Изменить», перейдите на вкладку «Параметры IPv4», поменяйте «Метод» на «Вручную», в поле «Дополнительные серверы DNS» напишите адрес IPA-сервера (например, 172.16.0.11), в поле «Дополнительные поисковые домены» введите поисковый домен (например, example.ru), нажмите применить и переподключитесь к сети.

Проверьте заданные настройки в файле /etc/resolv.conf

cat /etc/resolv.conf

search example.ru

nameserver 172.16.0.11

Так же выполните команду:

dig SRV _ldap._tcp. example.ru

в выводе нужно удостоверится, что SRV запись берется из DNS контроллера домена.

Установите ipa-client (в РЕД ОС 7.2 установлен по умолчанию):

для РЕД ОС версии 7.1 или 7.2:

yum -y install ipa-client

для РЕД ОС версии 7.3 и старше:

dnf -y install ipa-client

Настройте клиента.

Впишите в команду данные для вашей сети:

ipa-client-install --mkhomedir --enable-dns-updates

Скрипт установки должен автоматически найти настройки на ipa сервере, вывести их и спросить подтверждение для найденных параметров:

Continue to configure the system with these values? [no]:

Ответьте yes.

Затем введите имя администратора. Можно просто использовать администратора по умолчанию IPA, который был создан при установке сервера:

User authorized to enroll computers: admin

Введите пароль администратора IPA, который был установлен во время настройки сервера IPA.

После этого клиент IPA подготовит систему.

Если установка прошла успешно, в конце вывода вы увидите:

Client configuration complete.

The ipa-client-install command was successful

После этого хост должен появиться в веб-интерфейсе ipa сервера. Откройте веб-браузер на сервере, наберите в адресной строке полное доменное имя сервера. В результате должен открыться интерфейс такого вида (рис. 2):

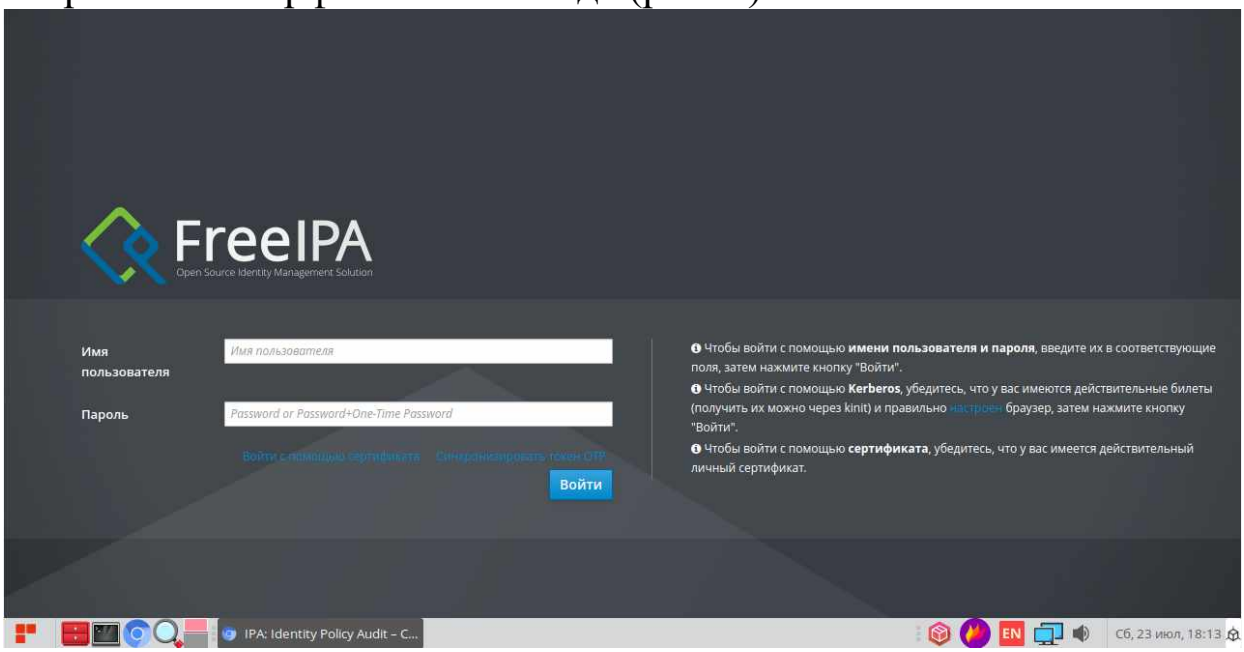

Рисунок 2 – Веб-интерфейс сервера IPA

Введите имя пользователя admin и пароль администратора IPA. В результате откроется графическая панель управления пользователями, группами и компьютерами. Проверьте наличие клиентской машины во вкладке Узлы. После этого вернитесь на

вкладку Пользователи и в разделе Активные пользователи добавьте новую учётную запись со своими именем и фамилией. ID группы оставьте пустым. Определите пароль для пользователя.

После этого проверьте в клиентской машине командой ping <полное имя IPA сервера>, что DNS-сервер отзывается, и происходит разрешение имён. Затем попробуйте получить билет Kerberos на созданного пользователя командой kinit <логин>. Если имя будет распознано, вы получите запрос пароля пользователя, при успешной авторизации – требование сменить его. После смены пароля снова получить билет. Если получение пройдёт успешно, терминал не выдаст никаких дополнительных сообщений.

Перезагрузите клиентскую машину и попробуйте войти под вновь созданной учётной записью. *Покажите результат преподавателю, а также учётную запись в веб-интерфейсе сервера IPA.*

Контрольные вопросы

1. Перечислите рекомендации для развёртывания домена IPA.
2. Почему нельзя называть домен именем .local?
3. В чём отличие домена IPA от домена Active Directory?
4. Что такое лес?
5. Что такое доверительные отношения?
6. Что такое Kerberos?
7. Каких правил необходимо придерживаться при определении имени Kerberos?
8. Можно ли изменить основной домен и область Kerberos после установки?
9. Какие типы среды сертификатов IPA Вы знаете?
10. Почему рекомендуется избегать развертывания других приложений или служб на виртуальной машине IPA?
11. От каких факторов зависит необходимое количество реплик серверов IPA?

Настройка домена Samba

Цель работы: научиться настраивать домен на основе программного пакета Samba в составе серверной операционной системы Ред ОС.

Установка Samba DC

Samba может выступать в роли контроллера домена и сервиса Active Directory. Если у вас уже установлен домен IPA, для выполнения этой работы необходимо создать новую виртуальную машину и установить на неё сервер Ред ОС заново.

Для установки выполните обновление РЕД ОС:

для РЕД ОС версии 7.1 или 7.2:

yum clean all && yum update

для РЕД ОС версии 7.3 и старше:

dnf makecache && dnf update

Установите необходимые пакеты. Если вы используете РЕД ОС версии 7.1 или 7.2, выполните команду:

yum install samba-client*.x86_64 samba-common.noarch samba-common*x86_64 samba-dc*.x86_64 samba-libs*.x86_64 samba-winbind*.x86_64 -y

Если вы используете РЕД ОС версии 7.3 и старше, выполните команду:

dnf install samba-client*.x86_64 samba-common.noarch samba-common*x86_64 samba-dc*.x86_64 samba-libs*.x86_64 samba-winbind*.x86_64 -y

Проверьте Samba на наличие kerberos heimdal (при использовании MIT Kerberos возможна некорректная работа samba с kerberos) см. ссылку

https://wiki.samba.org/index.php/Running_a_Samba_AD_DC_with_MIT_Kerberos_KDC

В том случае, если следующая команда выдаёт "HAVE_LIBKADM5SRV_MIT", тогда нужно установить Samba с поддержкой Kerberos Heimdal.

smbd -b | grep HAVE_LIBKADM5SRV_MIT

HAVE_LIBKADM5SRV_MIT

Переименуйте используемые по умолчанию конфигурационные файлы samba и kerberos:

mv /etc/krb5.conf /etc/krb5.conf.bak

mv /etc/samba/smb.conf /etc/samba/smb.conf.bak

Команда проверки установленной версии samba:

smbd -V

На время настройки сервиса переведите selinux в режим уведомлений. Для этого измените содержимое конфигурационного файла:

nano /etc/selinux/config

Заменив текст SELINUX=enforcing на SELINUX=permissive

Выполните:

setenforce 0

Не забудьте включить selinux после завершения настройки.

Присвойте серверу статический ip-адрес, а также назначьте имя. Имя должно определять область домена. Например, если Ваш домен skynet.murom, то hostname сервера может быть вида: dc1.skynet.murom. Тогда короткое имя будет dc1. *Сформируйте имя следующего формата: <Ваше_имя><Ваша фамилия>.ru*

Команда назначения имени серверу:

hostnamectl set-hostname <имя_сервера>

Укажите в файле /etc/hosts соответствие ip-адреса сервера с его полным и коротким именем:

nano /etc/hosts

<IP-адрес> <полное имя> <короткое имя>

В настройках сетевого адаптера пропишите поисковый домен в соответствии со сформированным именем, а в качестве dns-адреса укажите ip-адрес создаваемого Samba DC сервера.

Перезагрузите сетевой интерфейс для применения настроек:

systemctl restart NetworkManager

Проверьте resolv.conf выполнив:

cat /etc/resolv.conf

В консоли должно отображаться следующее:

Generated by NetworkManager

search <доменное имя>

nameserver <IP сервера>

Опишем некоторые настройки для тестового домена:

1. use-rfc2307 - параметр добавляет POSIX атрибуты (UID / GID) на схеме AD. Он понадобится при аутентификации клиентов Linux, BSD, or OS X (в том числе на локальной машине) в дополнение к Microsoft Windows.
2. interactive - параметр заставляет сценарий резерва запускаться в интерактивном режиме.
3. realm - указывает на DNS-имя домена в верхнем регистре, которое настроено в hosts, в нашем тесте realm: skynet.murom
4. Domain - доменное имя сервера.
5. Server Rules(роли сервера): dc - (Domen controller)
6. DNS backend (SAMBA_INTERNAL, BIND9_FLATFILE, BIND9_DLZ, NONE) - указывает кто, будет в роли DNS сервера. SAMBA_INTERNAL – внутренний DNS самбы.
7. DNS forwarder IP address. Данный параметр позволяет указать IP-адрес DNS-сервера, на который будут перенаправлены dns запросы, в случае, когда сервер Samba не сможет их разрешить.

Для запуска конфигурирования выполните команду:

samba-tool domain provision --use-rfc2307 --interactive

Конфигурирование запустится после того, как Вы ответите на все вопросы конфигуратора. После запуска автоматического конфигурирования, Samba сама создаст файлы конфигурации. Настройки Samba находятся в файле /etc/samba/smb.conf.

Начиная с версии 3.3.0, появился модуль acl_xattr, позволяющий Samba корректно обрабатывать Windows ACL (Access Control List). Для полноценной поддержки прав доступа к файлам используйте модуль acl_xattr. Для этого добавьте в smb.conf в раздел [global] следующие параметры:

vfs objects = acl_xattr

map acl inherit = yes

store dos attributes = yes

Для обновления записей в DNS добавьте два параметра в раздел [global]:

allow dns updates = nonsecure

nsupdate command = /usr/bin/nsupdate -g

Если при автоконфигурировании не был указан dns-форвардинг, то его можно включить, добавив в секцию [global] dns адрес, который используется в вашей локальной сети.

В секцию [global] добавьте поддержку расширения схемы AD

dsdb:schema update allowed = true

После внесения изменений в файл /etc/samba/smb.conf выполните команду проверки testparm. Предупреждение "rlimit_max: increasing rlimit_max (1024) to minimum Windows limit (16384)" отображается в связи с тем, что в Linux по умолчанию установлен лимит на 1024 одновременно открытых файлов, а в Windows он 16384. Чтобы убрать предупреждение добавьте в конец файла /etc/security/limits.conf строки:

* - nofile 16384

root - nofile 16384

Для применения настроек перезагрузите сервер. Скопируйте настройки Kerberos, которые создались после настройки samba в /etc

cp /var/lib/samba/private/krb5.conf /etc/

Добавляем в /etc/krb5.conf время жизни билета керберос - в секцию [libdefaults]:

nano /etc/krb5.conf

ticket_lifetime = 24h

forwardable = yes

Запуск и добавление в автозапуск сервиса samba:

systemctl enable samba --now

Проверка статуса:

systemctl status samba

Не запускайте службу winbindd вручную на контроллере домена Samba Active Directory (AD). Служба запускается автоматически как подпроцесс процесса samba.

Проверяем запущенные процессы:

ps ax | egrep "samba|smbd|nmbd|winbindd"

Проверьте, может ли служба Winbindd подключаться к контроллеру домена:

wbinfo --ping-dc

Посмотреть список пользователей и групп в домене можно следующими командами:

wbinfo -u
wbinfo -g

Для службы Samba, в отличие от IPA, нет собственного графического интерфейса, поэтому при необходимости графической оболочки администрирования необходимо использовать средства удалённого администрирования RSAT. Сведения об их установке Вы можете найти здесь: https://wiki.samba.org/index.php/Installing_RSAT. Ввод компьютера Windows в домен Samba выполняется так же, как в домен Active Directory.

Контрольные вопросы

1. Что такое ActiveDirectory?
2. Что представляет собой подразделение в Active Directory?
3. Какие виды групп пользователей существуют в Active Directory?
4. Какова область действия локальной доменной группы?
5. Кто может входить в локальную доменную группу?
6. Чем отличается глобальная группа от универсальной?
7. Что означает понятие контроллер домена?
8. Сколько должно быть контроллеров домена?
9. Что такое репликация?
10. Что понимается под доверительными отношениями?

Список литературы

1. Кобылянский, В. Г. Операционные системы, среды и оболочки : учебное пособие / В. Г. Кобылянский. – Новосибирск : Новосибирский государственный технический университет, 2018. – 80 с. – URL: https://biblioclub.ru/index.php?page=book&id=576354 (дата обращения: 07.03.2022). – Режим доступа: по подписке. – Текст : электронный.
2. Курячий, Г.В. Операционная система Linux : учебник / Г.В. Курячий, К.А. Маслинский. – 2-е изд., исправ. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 451 с. - URL: https://biblioclub.ru/index.php?page=book&id=578058 (дата обращения: 02.02.2021). – Режим доступа: по подписке. – Текст : электронный.
3. Куль, Т. П. Операционные системы : учебное пособие / Т. П. Куль. – Минск : РИПО, 2019. – 312 с. - URL: https://biblioclub.ru/index.php?page=book&id=599951 (дата обращения: 05.03.2022). Режим доступа: по подписке. – Текст : электронный.
4. Основы администрирования информационных систем : учебное пособие / Д. О. Бобынцев, А. Л. Марухленко, Л. О. Марухленко [и др.]. – Москва ; Берлин : Директ-Медиа, 2021. – 201 с. - :URL: https://biblioclub.ru/index.php?page=book&id=598955 (дата обращения: 05.03.2022). – Режим доступа: по подписке. – Текст : электронный.