Мне понадобилось настроить авторизацию доменный учетных записей Active Directory по ssh на linux сервер. В моем случае это будет система CentOS 7. Данная возможность будет очень удобна для организаций с внедренной доменной структурой Windows. С помощью групп доступа в AD вы сможете централизованно управлять доступом к linux серверам.

Если у вас есть желание научиться работать с роутерами микротик и стать специалистом в этой области, рекомендую по программе, основанной на информации из официального курса **MikroTik Certified Network Associate**. Курс стоящий, все подробности читайте по ссылке. Есть бесплатные курсы.

Содержание:

Подготовка сервера

Если у вас еще нет готового сервера, то можете воспользоваться моими материалами на эту тему — установка и настройка centos 7. Так же рекомендую настроить iptables для корректной работы сервера с доменом windows. Далее я не буду касаться этого вопроса, мы просто отключим фаерволл, потому что его настройка не тема этой статьи.

Информационная таблица

xs.local	название домена
10.1.3.4	ip адрес контроллера домена

xs-winsrv.xs.local	полное имя контроллера домена
xs-centos7-test	имя сервера centos, который вводим в домен
administrator	учетная запись администратора домена
gr_linux_adm	группа в AD, для которой разрешено подключение к серверам по ssh
lin-user	учетная запись в AD для проверки подключений по ssh

Выключаем firewalld:

```
# systemctl stop firewalld && systemctl disable firewalld
```

> Перед дальнейшей настройкой, убедитесь, что с вашего сервера centos вы без проблем пингуете и резолвите контроллер домена по полному имени. Если есть какие-то проблемы, исправьте это либо указанием нужного dns сервера, либо правкой файла hosts.

Настроим синхронизацию времени с контроллером домена. Это важно, у вас должно быть одинаковое время с контроллером домена. Проверьте его и убедитесь, что стоят одинаковые часовые пояса.

Устанавливаем утилиту для синхронизации времени **chrony**:

```
# yum install chrony
```

Добавляем в конфиг */etc/chrony.conf* адрес контроллера домена. И делаем его единственным сервером для синхронизации, остальные удаляем.

```
server xs-winsrv.xs.local iburst
```

Сохраняем конфиг, запускаем chrony и добавляем в автозагрузку.

```
# systemctl start chronyd && systemctl enable chronyd
```

Проверим, что с синхронизацией.

```
# cat /var/log/messages | grep chronyd
Jul 12 17:58:38 xs-centos7-test chronyd[10620]: chronyd version 2.1.1 starting (+CMDMON +NTP +REFCLOCK +RTC +PRIVDROP +DEBUG
+ASYNCDNS +IPV6 +SECHASH)
Jul 12 17:58:38 xs-centos7-test chronyd[10620]: Frequency 0.000 +/- 1000000.000 ppm read from /var/lib/chrony/drift
Jul 12 17:02:54 xs-centos7-test chronyd[10620]: Selected source 10.1.3.4
Jul 12 17:02:54 xs-centos7-test chronyd[10620]: System clock wrong by -3348.457170 seconds, adjustment started
Jul 12 17:02:54 xs-centos7-test chronyd[10620]: System clock was stepped by -3348.457170 seconds
```

Все в порядке. Синхронизировали время с контроллером домена. По логу видно, что время на сервере убежало вперед на 56 минут, но мы это исправили.

Подключение CentOS 7 к домену

Устанавливаем софт, который нам понадобится, для корректного ввода centos в домен windows.

```
# yum install realmd sssd oddjob oddjob-mkhomedir adcli samba-common samba-common-tools
```

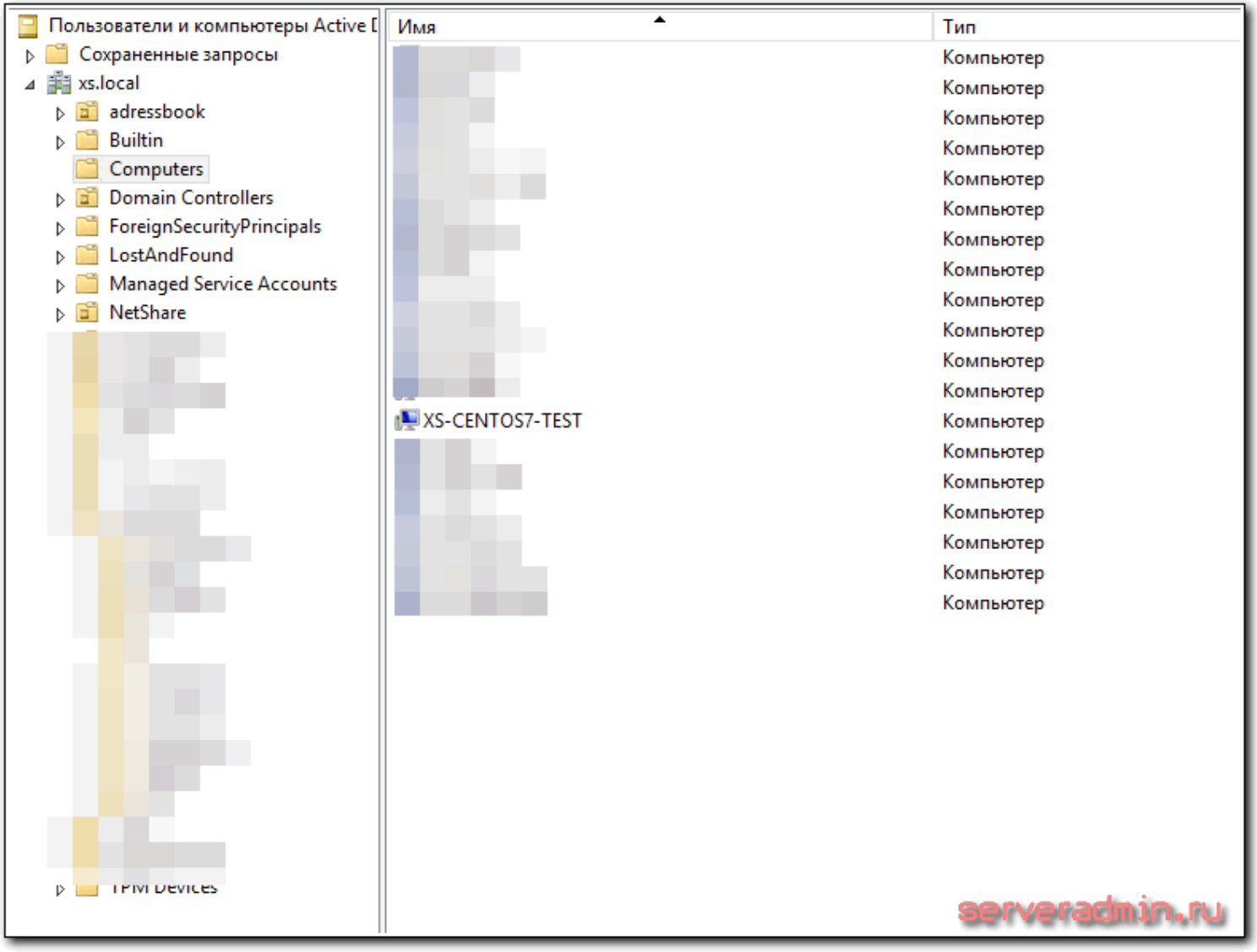
Вводим Centos 7 в домен:

```
# realm discover XS.LOCAL
xs.local
  type: kerberos
  realm-name: XS.LOCAL
  domain-name: xs.local
  configured: no
  server-software: active-directory
  client-software: sssd
  required-package: oddjob
  required-package: oddjob-mkhomedir
  required-package: sssd
```

```
  required-package: adcli
  required-package: samba-common-tools
```

```
# realm join -U administrator XS.LOCAL
Password for administrator:
```

Если не получили никакой ошибки, значит все прошло нормально. Можно зайти на контроллер домена и проверить, появился ли наш linux сервер в домене.


Пользователи и компьютеры Active D
Сохраненные запросы
xs.local
adressbook
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
LostAndFound
Managed Service Accounts
NetShare
Имя
Тип
Компьютер
XS-CENTOS7-TEST
serveradmin.ru

Изменим немного конфиг **sssd** для того, чтобы не нужно было вводить полное имя домена при логине, а только username.

```
# mcedit /etc/sssd/sssd.conf
```

```
use_fully_qualified_names = False
```

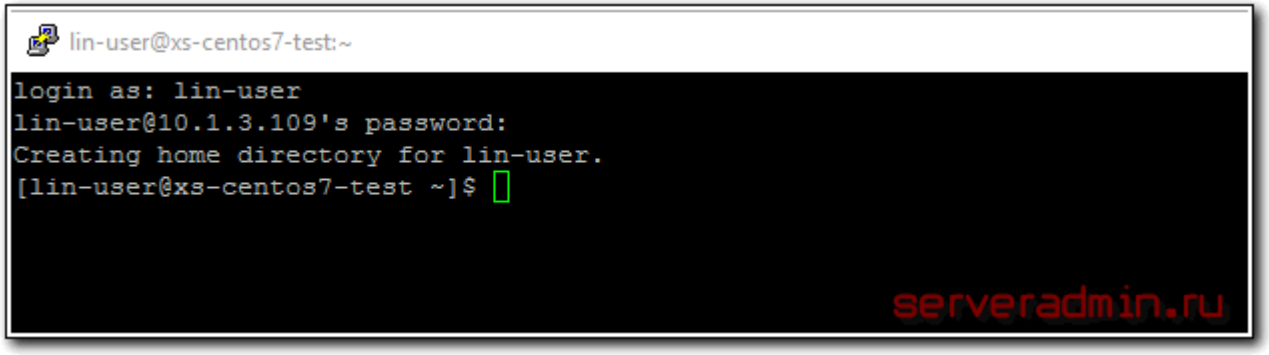
Разрешаем доменным пользователям создавать домашние директории:

```
# authconfig --enablemkhomedir --enablesssdauth --updateall
```

Запускаем службу sssd и добавляем в автозагрузку:

```
# systemctl enable sssd.service && systemctl restart sssd
```

Проверяем авторизацию по ssh, подключившись по любой доменной учетной записи.



Для пользователя будет создана домашняя директория */home/lin-user@xs.local*.

Ограничение доступа ssh по группам и пользователям домена

На текущий момент подключиться к серверу может любой пользователь домена. Исправим это и разрешим подключаться только пользователям из группы **gr_linux_adm**. Для этого правим конфиг */etc/sssd/sssd.conf*, добавляя туда новые параметры.

```
# mcedit /etc/sssd/sssd.conf
```

```
access_provider = simple
simple_allow_users = user55@xs.local
simple_allow_groups = gr_linux_adm@xs.local
```

Обращаю внимание, что параметр access_provider у вас уже будет установлен в другое значение. Надо это изменить. Вы можете добавить разрешение как для конкретного пользователя, так и для целых групп. Сохраняйте конфиг и перезапускайте sssd.

```
# systemctl restart sssd
```

Теперь подключиться по ssh к серверу сможет только пользователь домена user55 и все члены группы gr_linux_adm.

Для разбора полетов и решения проблем нужно использовать лог файл — */var/log/secure*. Вот пример успешного подключения:

```
Jul 12 18:10:44 xs-centos7-test sshd[4163]: pam_sss(sshd:auth): authentication success; logname= uid=0 euid=0 tty=ssh ruser=
rhost=10.1.3.221 user=lin-user
Jul 12 18:10:44 xs-centos7-test sshd[4163]: Accepted password for lin-user from 10.1.3.221 port 51063 ssh2
Jul 12 18:10:45 xs-centos7-test sshd[4163]: pam_unix(sshd:session): session opened for user lin-user by (uid=0)
```

А вот кусок лога подключения доменного пользователя, для которого доступ по ssh закрыт.

```
Jul 12 18:08:28 xs-centos7-test sshd[4059]: pam_sss(sshd:auth): authentication success; logname= uid=0 euid=0 tty=ssh ruser=
rhost=10.1.3.221 user=vzap
Jul 12 18:08:28 xs-centos7-test sshd[4059]: pam_sss(sshd:account): Access denied for user vzap: 6 (Permission denied)
Jul 12 18:08:28 xs-centos7-test sshd[4059]: Failed password for vzap from 10.1.3.221 port 51057 ssh2
Jul 12 18:08:28 xs-centos7-test sshd[4059]: fatal: Access denied for user vzap by PAM account configuration [preauth]
```

Здесь видно, что идентификация пользователя прошла корректно, но доступ к серверу запрещен.

Ограничение доступа к sudo по доменным группам

Ограничение доступа к ssh по группам и пользователям настроили, теперь надо разрешить доменным учетным записям получать права суперпользователя в системе. Сейчас у них нет такой возможности.

```
[sudo] password for lin-user:
lin-user is not in the sudoers file. This incident will be reported.
```

Создаем новый файл в директории */etc/sudoers.d*.

```
# mcedit /etc/sudoers.d/xs
```

```
%gr_linux_adm@xs.local ALL=(ALL) ALL
```

> Обращаю внимание, что имя данного файла не должно содержать точки. Я сначала не знал об этом и сделал файл с именем xs.local и долго не мог понять, почему не работает. Когда изменил имя файла, все заработало.

Выставляем минимальные права на файл:

```
# chmod 0440 /etc/sudoers.d/xs
```

Теперь вы можете зайти в систему доменной учетной записью из группы gr_linux_adm и получить полные права в системе.

Реализовать то же самое можно было через настройки sssd. В его конфиге можно было указать группы, которым разрешен доступ к sudo. Но в целом это не принципиально. Так, как сделал я, мне показалось проще. Не нужно использовать полные имена объектов в AD, в которых легко запутаться, особенно тем, кто не очень в этом ориентируется. Мне же понадобились только конечные имена групп. Более подробно об этом можно почитать в руководстве redhat. Ссылку приведу в конце.

Заключение

На этом все. Я рассмотрел наиболее типовую ситуацию, которая может быть полезной при использовании структуры AD совместно с linux серверами. При написании статьи использовал официальные руководства:

- Deployment, Configuration and Administration of Red Hat Enterprise Linux 6
- sssd.conf — Linux man page

Почему-то из руководства по RHEL 7 раздел, посвещенный SSSD убрали, хотя в 5 и 6 есть. Может просто я не заметил, так как структура сильно поменялась. Люблю я CentOS в первую очередь за отличную документацию Redhat. Там есть подробное описание практически всего, с чем приходилось сталкиваться. Надо только не лениться в английском языке разбираться.

Онлайн курсы по Mikrotik

Если у вас есть желание научиться работать с роутерами микротик и стать специалистом в этой области, рекомендую пройти курсы по программе, основанной на информации из официального курса **MikroTik Certified Network Associate**. Помимо официальной программы, в курсах будут лабораторные работы, в которых вы на практике сможете проверить и закрепить полученные знания. Все подробности на сайте . Стоимость обучения весьма демократична, хорошая возможность получить новые знания в актуальной на сегодняшний день предметной области. Особенности курсов:

- Знания, ориентированные на практику;
- Реальные ситуации и задачи;
- Лучшее из международных программ.

Помогла статья? Есть возможность отблагодарить автора