Интеграция CentOS 7 (8) с ADDS и настройка файлового сервера Samba

**Входные данные**

* Файловый сервер (samba-sssd-srv.fdsdn.corp) на CentOS 7 (8) с ip address – 192.168.0.109;
* ADDS сервер (adds.fdsdn.corp) на Windows Server 2016 с ip address – 192.168.0.120, домен – fdsdn.corp.

Подготовка для присоединения сервера к домену fdsdn.corp

Важной частью для удачного присоединения linux сервера к домену является правильно настроенный hostname сервера.

# hostnamectl set-hostname samba-sssd-srv.fdsdn.corp

Проверить правильность настройки hostname можно таким образом:

# hostname -s

samba-sssd-srv

# hostname -f

samba-sssd-srv.fdsdn.corp

Не менее важной частью является настройка правильного DNS т.е. того, кто обслуживает домен AD. В нашем случает DNS установлен на контролере домена. Указать ip address DNS сервера можно с помощью **nmtui** или вручную изменить конфигурационный файл на linux сервере (**/etc/sysconfig/network-scripts/ifcfg-ens33**), где **ifcfg-ens33** файл конфигурации определенного сетевого интерфейса.

После проделанных настроек нужно удостовериться, что контроллер домена доступен с linux сервера по имени т.е. банально, сделать ping.

Далее важной частью является синхронизация времени linux сервера и контроллера домена т.к. для протокола Kerberos это очень важно. Для синхронизации времени в CentOS 8 используется chronyd. В нашем случае добавляем строчку в конфигурационный файл chronyd (**/etc/chrony.conf**), а настроенные по-умолчанию pools удаляем или комментируем (не забываем перезапустить chronyd):

server adds.fdsdn.corp iburst

Посмотреть успешную синхронизацию можно с помощью команды:

# timedatectl

Local time: Sun 2020-08-30 12:40:57 MSK

Universal time: Sun 2020-08-30 09:40:57 UTC

RTC time: Sun 2020-08-30 09:40:58

Time zone: Europe/Moscow (MSK, +0300)

**System clock synchronized: yes**

NTP service: active

RTC in local TZ: no

Или с помощью log файла:

# tail -n 10 /var/log/messages | grep chronyd

Aug 30 12:37:57 samba-srv chronyd[4264]: chronyd version 3.5 starting (+CMDMON +NTP +REFCLOCK +RTC +PRIVDROP +SCFILTER +SIGND +ASYNCDNS +SECHASH +IPV6 +DEBUG)

Aug 30 12:37:57 samba-srv chronyd[4264]: Frequency 8.798 +/- 0.055 ppm read from /var/lib/chrony/drift

Aug 30 12:37:57 samba-srv chronyd[4264]: Using right/UTC timezone to obtain leap second data

**Aug 30 12:38:01 samba-srv chronyd[4264]: Selected source 192.168.0.120**

Aug 30 12:38:01 samba-srv chronyd[4264]: System clock TAI offset set to 37 seconds

Также можно проверить какой источник выбран:

# chronyc sources

210 Number of sources = 1

MS Name/IP address Stratum Poll Reach LastRx Last sample

===============================================================================

^\* adds.fdsdn.corp 3 7 377 111 +29us[ +81us] +/- 175ms

**Примечание:**

Бывает возникает проблема, при которой не происходит синхронизации времени linux сервера с контроллером домена на Windows Server. Если ip связность между linux и ADDS в порядке, и firewall не препятствует то скорее всего контроллер домена не отвечает на запросы синхронизации. Чтобы заставить Windows Server отвечать на ntp запросы нужно проделать такие действия в CMD (тезисно):

> net stop w32time

> w32tm /config /reliable:yes

> net start w32time

Нужно заметить, что при присоединении linux к домену с помощью sssd происходит динамическое создание DNS записи (в отличии от winbind). Тем не менее, после присоединения, лучше зайти на DNS для домена и убедиться в этом. Если необходимо, то создать вручную, т.к. это довольно-таки важный момент.

Присоединение CentOS 7 (8) в ADDS (sssd) на Windows Server 2016

В системы CentOS 7 (8) realmd установлен, но если нет, то устанавливаем:

# yum install realmd

Для CentOS 8:

# dnf install realmd

Выводим информацию о домене:

# realm discover fdsdn.corp

fdsdn.corp

type: kerberos

realm-name: FDSDN.CORP

domain-name: fdsdn.corp

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

или так (уточняем, что нас интересует домен active directory):

# realm discover fdsdn.corp --server-software=active-directory

fdsdn.corp

type: kerberos

realm-name: FDSDN.CORP

domain-name: fdsdn.corp

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

Устанавливаем то, что необходимо (показано в выводе):

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

Для CentOS 8:

# dnf install oddjob oddjob-mkhomedir sssd adcli samba-common-tools \

krb5-workstation authselect-compat

Что мы установили? Краткое описание:

* realmd: управляет регистрацией и членством в доменах Active Directory;
* samba-common-tools: общие инструменты для серверов и клиентов;
* oddjob: Это сервис D-bus, который выполняет odd задания для клиентов;
* oddjob-mkhomedir: используется со службами odd заданий для создания домашних каталогов для учетных записей AD, если это необходимо;
* sssd: Непосредственно, сам The System Security Services daemon (sssd) демон;
* adcli: инструменты для присоединения и управления доменами AD.

Присоединение к домену:

# realm join fdsdn.corp -v -U denysb

Кстати, если нужно сразу определить компьютер в определенный OU, то можно присоединить так:

# realm join -v -U denysb \

--computer-ou=OU=Linux\_servers,DC=FDSDN,DC=CORP fdsdn.corp

Вывести информацию по домену, в котором состоит сервер:

# realm list

fdsdn.corp

type: kerberos

realm-name: FDSDN.CORP

domain-name: fdsdn.corp

configured: kerberos-member

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

login-formats: %U@fdsdn.corp

login-policy: allow-realm-logins

Что делает данная команда? Ответ – присоединяет данный компьютер к домену AD. Но что она делает более детально? Ответы ниже.

Она создает конфигурационный файл /etc/sssd/sssd.conf такого вида:

[sssd]

domains = fdsdn.corp

config\_file\_version = 2

services = nss, pam

[domain/fdsdn.corp]

ad\_domain = fdsdn.corp

krb5\_realm = FDSDN.CORP

realmd\_tags = manages-system joined-with-samba

cache\_credentials = True

id\_provider = ad

krb5\_store\_password\_if\_offline = True

default\_shell = /bin/bash

ldap\_id\_mapping = True

use\_fully\_qualified\_names = True

fallback\_homedir = /home/%u@%d

access\_provider = ad

При этом изменяет конфигурационный файл /etc/nsswitch.conf и конфигурационные файлы PAM (/etc/pam.d/\*). По сути, выполняет команды по настройке аутентификации ОС (выполнять команды ниже не нужно):

В CentOS 7 для NSS (nsswitch.conf):

# authconfig --enablesssd –update

В CentOS 7 для PAM:

# authconfig --enablesssdauth --update

В CentOS 7 для автоматического создания домашних каталогов:

# authconfig --enablemkhomedir –update

В CentOS 8 для NSS, PAM и автоматического создания домашних каталогов:

# authselect select sssd with-mkhomedir

Сама работа sssd с NSS и PAM происходит за счет строчки в конфигурационном файле sssd.conf:

services = nss, pam

Далее для CentOS 8 нужно, все таки, ввести такие команды (на всякий случай):

# authselect select sssd  
# authselect select sssd with-mkhomedir

Проверка, того, что ОС знает о доменных пользователях:

#id denysb@fdsdn.corp

Далее можно зайти локально или с помощью ssh и убедиться, что работает доменная аутентификация. При этом создаются домашние каталоги.

**Заметка**.

Если вы получили ошибку:

”realm: Couldn’t join realm: Joining the domain FDSDN.CORP failed“

просто перезагрузите realmd и попробуйте заново.

**Заметка**.

Как-то возникла проблема с тем, что библиотеке ldb "мешал" файл (тоже библиотека) /usr/lib64/ldb/modules/ldb/paged\_results.so. Решение – удалить данный файл и перезапустить демон sssd.

**Заметка**.

При действии GPO на учетные записи возникает ошибка, говорящая о том, что определенный контейнер не может быть прочитан или отсутствует атрибут. Данную ошибку можно исправить с помощью добавления строчки в /etc/sssd/sssd.conf такого содержания (доменный в контекст):

ad\_gpo\_ignore\_unreadable = True

Таким образом полностью конфигурационный файл sssd.conf выглядит так:

[sssd]

domains = fdsdn.corp

config\_file\_version = 2

services = nss, pam

[domain/fdsdn.corp]

ad\_domain = fdsdn.corp

krb5\_realm = FDSDN.CORP

realmd\_tags = manages-system joined-with-samba

cache\_credentials = True

id\_provider = ad

krb5\_store\_password\_if\_offline = True

default\_shell = /bin/bash

ldap\_id\_mapping = True

use\_fully\_qualified\_names = True

fallback\_homedir = /home/%u@%d

access\_provider = ad

**ad\_gpo\_ignore\_unreadable = True**

**Настройка sudo.**

Как было изложено выше мы можем попасть на сервер по ssh из-под доменных учетных записей. Теперь осталось дать данному пользователю права sudo.

Создаем файл **/etc/sudoers.d/fdsdn** (без точек, а то работать не будет) и делаем там запись:

%ssh\_users@fdsdn.corp ALL=(ALL) ALL

%Domain\ Admins@fdsdn.corp ALL=(ALL) ALL

Таким образом мы дали права на sudo пользователям в группе **Domain Admins** и для примера еще пользователям входящие в группу **ssh\_users**.

Выставляем минимальные права на файл:

~# chmod 0440 /etc/sudoers.d/fdsdn

Кстати, можно заметить, что формат записи групп в sudo несколько отличаются от того, как при присоединении компьютера к домену с помощью winbind.

**Дать доступ к серверу определенным группам.**

После того, как мы присоединили данный компьютер к домену, можно дать доступ к нему (компьютеру) только определенным группам.

Первый способ изменить конфигурационный файл sssd.conf вручную. “Говорим” sssd использовать Simple Access Provider. Изменяем строчки в файле sssd.conf:

access\_provider = simple

simple\_allow\_groups = domain admins,smb\_users,ssh\_users,rdp\_users

Таким образом файл sssd.conf будет иметь вид:

[sssd]

domains = fdsdn.corp

config\_file\_version = 2

services = nss, pam

[domain/fdsdn.corp]

ad\_domain = fdsdn.corp

krb5\_realm = FDSDN.CORP

realmd\_tags = manages-system joined-with-samba

cache\_credentials = True

id\_provider = ad

krb5\_store\_password\_if\_offline = True

default\_shell = /bin/bash

ldap\_id\_mapping = True

use\_fully\_qualified\_names = True

fallback\_homedir = /home/%u@%d

**#access\_provider = ad**

**access\_provider = simple**

**simple\_allow\_groups = Domain Admins, smb\_users, ssh\_users, rdp\_users**

ad\_gpo\_ignore\_unreadable = True

После этого надо перезапустить sssd:

# systemctl restart sssd.service

Второй способ заключается в том, чтобы использовать команду realm при этом файл sssd.conf **не трогаем**.Его самостоятельно изменить команда realm:

# realm deny --all

# realm permit -g 'Domain Admins' 'smb\_users'

# realm permit -g 'Domain Admins' 'smb\_users' 'ssh\_users' 'rdp\_users'

# realm list

fdsdn.corp

type: kerberos

realm-name: FDSDN.CORP

domain-name: fdsdn.corp

configured: kerberos-member

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

login-formats: %U@fdsdn.corp

login-policy: allow-permitted-logins

permitted-logins:

**permitted-groups: Domain Admins, smb\_users, ssh\_users, rdp\_users**

А вот как данная команда изменила sssd.conf:

[sssd]

domains = fdsdn.corp

config\_file\_version = 2

services = nss, pam

[domain/fdsdn.corp]

ad\_domain = fdsdn.corp

krb5\_realm = FDSDN.CORP

realmd\_tags = manages-system joined-with-samba

cache\_credentials = True

id\_provider = ad

krb5\_store\_password\_if\_offline = True

default\_shell = /bin/bash

ldap\_id\_mapping = True

use\_fully\_qualified\_names = True

fallback\_homedir = /home/%u@%d

**access\_provider = simple**

ad\_gpo\_ignore\_unreadable = True

**simple\_allow\_groups = Domain Admins, smb\_users, ssh\_users, rdp\_users**

Опциональные настройки

**Формат домашней директории.**

Опция fallback\_homedir устанавливает формат домашней директории, если она не определена в AD. Можно добавить строчку override\_homedir, которая всегда будет использовать заданный формат, даже если дериктория определена в AD:

override\_homedir = /home/%u@%d

**Автоматическое обновление компьютерной учетной записи.**

Если установлен adcli (а мы его установили), то sssd будет самостоятельно обновлять /etc/krb5.keytab файл. Т.е. Демон sssd каждый день проверяет устарел ли пароль компьютерной учетки, и если он устарел, то обновляет. По-умолчанию, пароль обновляется раз в 30 дней, но можно это изменить (например, раз в 60 дней), хотя без надобности, лучше оставить значение по-умолчанию:

ad\_maximum\_machine\_account\_password\_age = 60

**Динамическое обновление DNS.**

Можно включить динамические обновления в ДНС:

dyndns\_update = true

dyndns\_refresh\_interval = 43200

dyndns\_update\_ptr = true

dyndns\_ttl = 3600

Покинуть домен

Покинуть т.е. отсоединиться от домена:

# realm leave fdsdn.corp

с удаление учетной записи компьютера на контролере домена:

# realm leave fdsdn.corp --remove

Настройка Samba с доменной аутентификацией

**ОЧЕНЬ ВАЖНО.**

С Samba сервером присоединённом к домену с помощью sssd есть один большой недостаток. Данный сервер работает только с клиентами Windows. С клиентами linux – **не работает!** Если нужно настроить Samba сервер с работой для linux клиентов, то нужно данный сервер заводить в домен с помощью winbind.

Более подробно настройка с разными ACL была рассмотрена в статье касающейся winbind. Тут мы будем настраивать, используя extended POSIX ACLs.

**Настройка samba share используя Extended POSIX ACLs**

Начнем с входных данных. У нас есть три группы (rdp\_users, smb\_users, ssh\_users), в которые входят определенные пользователи. Пользователи каждой группы имеют доступ только к своим шарам (rdp-users-folder, smb-users-folder, ssh-users-folder). Для этого содаем необходимые директории:

~# mkdir /samba-shares

Теперь нужно сделать необходимые права. К директории rdp-users-folder имеют доступ только пользователи группы rdp\_users, к smb-users-folder – только smb\_users, а к ssh-users-folder – только ssh\_users. Группе “Domain Admins” сделаем полные права. Будем использовать “extendet acl”.

Дадим права на директорию /samba-shares группе “Domain Admins” полные права, а “Domain Users” на чтение и выполнение (значит, что могут заходить в папку). Это делается для того, чтобы у всех в домене был доступ к “начальной” шаре. Кроме того, “включим” наследования только для “Domain Admins”, чтобы права только для аминов были наследованы и другим директориям.

~# setfacl -m group::--- /samba-shares

~# setfacl -m default:group::--- /samba-shares

~# setfacl -m other::--- /samba-shares

~# setfacl -m default:other::--- /samba-shares

~# setfacl -m group:"FDSDN\Domain Admins":rwx /samba-shares

~# setfacl -m group:"FDSDN\Domain Users":r-x /samba-shares

~# setfacl -m default:group:"FDSDN\Domain Admins":rwx /samba-shares

~# getfacl /samba-shares/

getfacl: Removing leading '/' from absolute path names

# file: samba-shares/

# owner: root

# group: root

user::rwx

group::---

group:domain\040admins@fdsdn.corp:rwx

group:domain\040users@fdsdn.corp:r-x

mask::rwx

other::---

default:user::rwx

default:group::---

default:group:domain\040admins@fdsdn.corp:rwx

default:mask::rwx

default:other::---

Далее создадим оставшиеся директории и дадим только необходимые правила тем директория, которые находятся внутри директории /samba-shares.

~# mkdir -p /samba-shares/{rdp-users-folder,smb-users-folder,ssh-users-folder}

~# setfacl -m group:"FDSDN\rdp\_users":rwx /samba-shares/rdp-users-folder

~# setfacl -m default:group:"FDSDN\rdp\_users":rwx /samba-shares/rdp-users-folder

~# getfacl /samba-shares/rdp-users-folder/

getfacl: Removing leading '/' from absolute path names

# file: samba-shares/rdp-users-folder/

# owner: root

# group: root

user::rwx

group::---

group:domain\040admins@fdsdn.corp:rwx

group:rdp\_users@fdsdn.corp:rwx

mask::rwx

other::---

default:user::rwx

default:group::---

default:group:domain\040admins@fdsdn.corp:rwx

default:group:rdp\_users@fdsdn.corp:rwx

default:mask::rwx

default:other::---

~# setfacl -m group:"FDSDN\smb\_users":rwx /samba-shares/smb-users-folder

~# setfacl -m default:group:"FDSDN\smb\_users":rwx /samba-shares/smb-users-folder

~# getfacl /samba-shares/smb-users-folder/

~# getfacl /samba-shares/smb-users-folder/

getfacl: Removing leading '/' from absolute path names

# file: samba-shares/smb-users-folder/

# owner: root

# group: root

user::rwx

group::---

group:domain\040admins@fdsdn.corp:rwx

group:smb\_users@fdsdn.corp:rwx

mask::rwx

other::---

default:user::rwx

default:group::---

default:group:domain\040admins@fdsdn.corp:rwx

default:group:smb\_users@fdsdn.corp:rwx

default:mask::rwx

default:other::---

~# setfacl -m group:"FDSDN\ssh\_users":rwx /samba-shares/ssh-users-folder

~# setfacl -m default:group:"FDSDN\ssh\_users":rwx /samba-shares/ssh-users-folder

~# getfacl /samba-shares/ssh-users-folder/

getfacl: Removing leading '/' from absolute path names

# file: samba-shares/ssh-users-folder/

# owner: root

# group: root

user::rwx

group::---

group:domain\040admins@fdsdn.corp:rwx

group:ssh\_users@fdsdn.corp:rwx

mask::rwx

other::---

default:user::rwx

default:group::---

default:group:domain\040admins@fdsdn.corp:rwx

default:group:ssh\_users@fdsdn.corp:rwx

default:mask::rwx

default:other::---

Далее устанавливаем сам Samba сервер:

Для CentOS 7:

~# yum install samba

Для CentOS 8:

~# dnf install samba

Конфигурационный файл /etc/samba/smb.conf приводим к такому виду:

[global]

**workgroup = FDSDN**

server string = File Server sssd

log file = /var/log/samba/log.%m

log level = 3

max log size = 500

**security = ads**

encrypt passwords = yes

passdb backend = tdbsam

**realm = FDSDN.CORP**

load printers = no

cups options = raw

printcap name = /dev/null

[samba-shares]

path = /samba-shares

read only = no

inherit acls = yes

hide unreadable = yes

access based share enum = yes

Настройка “access based share enum = yes” нужна для того, чтобы при монтировании шары (/samba-srv/samba-shares) на клиентском ПК были видны только те директории, на которые для залогиненного пользователя есть права хотя бы на чтение. Т.е., например, если пользователь smbuser1 смонтирует данную шару, то несмотря на то, что в этой шаре есть три директории он увидит только одну (“smb-users-folder”).