ООО «Базальт СПО»
Общество с ограниченной ответственностью
«Базальт свободное программное обеспечение»
127015, г. Москва, ул. Бутырская, д. 75, офис 307
Тел./факс: +7 495 123-4799

ОГРН 1157746734837
ИНН 7714350892
КПП 77140100

РУКОВОДСТВО ДЛЯ ИНТЕГРАТОРА

РАЗРАБОТКА ОТКРЫТОЙ БИБЛИОТЕКИ ДЛЯ УПРАВЛЕНИЯ ДОМЕННОЙ ИНФРАСТРУКТУРОЙ НА ОСНОВЕ СЛУЖБЫ КАТАЛОГОВ SAMBA

Москва 2023

Содержание

1. Схема стенда

В настоящем документе приводится общая информация по разворачиванию ПО.

Схема стенда представлена на Рис. 1. Состав технических и программных средств стенда приведён в табл. 1.

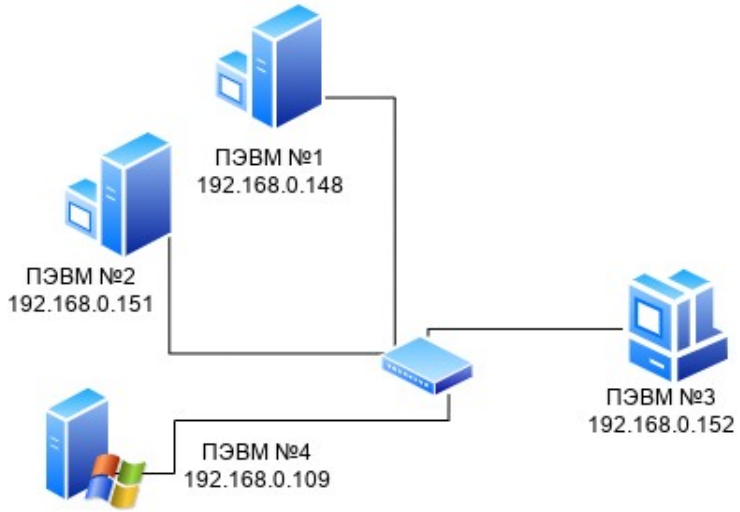

Рис. 1. Схема стенда

Таблица 1. Состав технических и программных средств стенда

№ ПЭВМ	Программная среда	Описание
1	ОС Альт Сервер 10	Контроллер домена (DC)
2	ОС Альт Сервер 10	Сервер LDAP
3	ОС Альт (Рабочая станция 10, Рабочая станция K 10, Образование 10)	Машина с libdomain
5	ОС Microsoft Windows Server	Сервер Active Directory

Параметры домена:

- домен AD – domain.alt;
- сервер AD (ОС ALT) – dc1.domain.alt (192.168.0.148);
- сервер LDAP (ОС ALT) – dc2.domain.alt (192.168.0.151);
- рабочая станция 1 (ОС ALT) – host-01.domain.alt (192.168.0.152);
- рабочая станция 4 (ОС Windows) – PK1.domain.alt (192.168.0.109);

- имя пользователя-администратора – Administrator;
- пароль администратора – Pa$$word.

  Примечание. На текущий момент библиотека поддерживает только протокол IPv4.

2. Контроллер домена (Samba AD DC)

2.1. Установка ОС «Альт Сервер» 10.x

Ссылка для скачивания ОС: https://www.basealt.ru/alt-server/download.

Инструкция по установке ОС: https://docs.altlinux.org/ru-RU/alt-server/10.1/html/alt-server/install-distro.html

2.2. Разворачивание сервера Samba AD DC

Все действия выполняются на узле dc1.domain.alt (192.168.0.148).

Для установки Samba AD DC выполняются следующие шаги:

1. Установить пакеты task-samba-dc и libsasl2-plugin-gssapi (нужен для работы библиотеки libdomain):

```
# apt-get install task-samba-dc libsasl2-plugin-gssapi
```

2. Остановить конфликтующие службы krb5kdc и slapd, а также bind:

```
# for service in smb nmb krb5kdc slapd bind; do chkconfig $service
off; service $service stop; done
```

3. Очистить базы и конфигурацию Samba:

```
# rm -f /etc/samba/smb.conf
# rm -rf /var/lib/samba
# rm -rf /var/cache/samba
# mkdir -p /var/lib/samba/sysvol
```

4. Установить имя домена. Имя домена, для разворачиваемого DC, должно состоять минимум из двух компонентов, разделённых точкой. При этом должно быть установлено правильное имя узла и домена для сервера. Для этого в файл `/etc/sysconfig/network` необходимо добавить строку:

```
HOSTNAME=dc1.domain.alt
```

И выполнить команды:

```
# hostnamectl set-hostname dc1.domain.alt
# domainname domain.alt
```

5. Для корректного функционирования домена в файле `/etc/resolv.conf` должна присутствовать строка:

```
nameserver 127.0.0.1
```

Если этой строки в файле `/etc/resolv.conf` нет, то в конец файла `/etc/resolvconf.conf` следует добавить строку:

```
name_servers='127.0.0.1'
```

и перезапустить сервис resolvconf:

```
# resolvconf -u
```

6. Создать домен domain.alt с паролем администратора Pa$$word:

```
# samba-tool domain provision --realm=domain.alt --domain=domain
--adminpass='Pa$$word' --dns-backend=SAMBA_INTERNAL --option="dns
forwarder=8.8.8.8" --server-role=dc
```

где

- --realm – область Kerberos (LDAP), и DNS имя домена;
- --domain – имя домена (имя рабочей группы);
- --adminpass – пароль основного администратора домена;
- --server-role – тип серверной роли.

Примечание. Пароль администратора должен быть не менее 7 символов и содержать символы как минимум трёх групп из четырёх возможных: латинских букв в верхнем и нижнем регистрах, чисел и других небуквенно-цифровых символов. Пароль не полностью соответствующий требованиям это одна из причин завершения развертывания домена ошибкой.

7. Запустить службы:

```
# systemctl enable --now samba
```

8. Настроить Kerberos. В момент создания домена Samba конфигурирует шаблон файла krb5.conf для домена в каталоге /var/lib/samba/private/. Заменить этим файлом файл, находящийся в каталоге /etc/:

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

9. Проверить работоспособность домена:

- просмотр общей информации о домене:

```
# samba-tool domain info 127.0.0.1
Forest           : domain.alt
Domain           : domain.alt
Netbios domain   : DOMAIN
```

```
DC name            : dc1.domain.alt
DC netbios name    : DC1
Server site        : Default-First-Site-Name
Client site        : Default-First-Site-Name
```

- убедиться в наличии nameserver 127.0.0.1 в `/etc/resolv.conf`:

```
# host domain.alt
domain.alt has address 192.168.0.148
```

- проверить имена хостов:

```
# host -t SRV _kerberos._udp.domain.alt.
_kerberos._udp.domain.alt has SRV record 0 0 88 dc1.domain.alt.
# host -t SRV _ldap._tcp.domain.alt.
_ldap._tcp.domain.alt has SRV record 0 100 389 dc1.domain.alt.
# host -t A dc1.domain.alt.
dc1.domain.alt has address 192.168.0.148
```

- проверка Kerberos (имя домена должно быть в верхнем регистре):

```
# kinit administrator@DOMAIN.ALT
```

Примечание. Если имена не находятся, необходимо проверить выключение службы named.

10. Создать и разблокировать пользователя ivanov в домене:

```
# samba-tool user create ivanov --given-name='Иван Иванов' --mail-
address='ivanov@domain.alt'
# samba-tool user setexpiry ivanov --noexpiry
```

2.3. Настройка сервера LDAP

Все действия выполняются на узле (192.168.0.151).

Для установки и настройки сервера LDAP выполняются следующие шаги:

1. Установить пакеты openldap-servers openldap-clients:

```
# apt-get install openldap-servers openldap-clients
```

2. Создать скрипт генерации сертификатов `generate_cert.sh` со следующим содержимым:

```
#!/bin/bash
set -euxo pipefail
```

```
CERT_PATH="${1:-/var/lib/samba/private/tls}"

# Генерация ключа CA с использованием RSA, длина ключа 4096 бит
openssl genrsa -out "${CERT_PATH}/ca.key" 4096
# Генерация root сертификата, со сроком действия 1 год. Необходимо
указать CN, это должно быть полное доменное имя домена в верхнем
регистре.
openssl req -new -x509 -nodes -days 365 -key "${CERT_PATH}/ca.key"
-out "${CERT_PATH}/ca.pem" -subj "/O=Test Inc/OU=Samba CA
Cert/CN=domain.alt"
# Генерация ключа
openssl genrsa -out "${CERT_PATH}/dc0.domain.alt.key" 4096
# Запрос сертификата CSR
openssl req -new -sha256 -key "${CERT_PATH}/dc0.domain.alt.key" -
subj "/O=Test Inc/OU=Samba CA Cert/CN=dc0.domain.alt" -out "$
{CERT_PATH}/dc0.domain.alt.csr"
# Подпись сертификата
openssl x509 -req -in "${CERT_PATH}/dc0.domain.alt.csr" -CA "$
{CERT_PATH}/ca.pem" -CAkey "${CERT_PATH}/ca.key" -CAcreateserial -
out "${CERT_PATH}/dc0.domain.alt.pem" -days 365
# Проверка сертификата
openssl verify -CAfile "${CERT_PATH}/ca.pem"
"${CERT_PATH}/dc0.domain.alt.pem"
```

3. Запустить скрипт генерации сертификатов:

```
# chmod +x generate_cert.sh
# mkdir -p /certs && ./generate_cert.sh /certs
```

4. Создать файл конфигурации OpenLDAP `slapd.conf` со следующим содержимым:

```
#
# See slapd.conf(5) for details on configuration options.
#

# [ GLOBAL SETTINGS ]

# Default schemas
```

```
include /etc/openldap/schema/core.schema
include /etc/openldap/schema/cosine.schema
include /etc/openldap/schema/inetorgperson.schema
include /etc/openldap/schema/openldap.schema
include /etc/openldap/schema/nis.schema
# Password policy
include /etc/openldap/schema/ppolicy.schema

# ALT Domain schemas
include /etc/openldap/schema/samba4.schema

# Set pid file
pidfile /tmp/slapd.pid

#
# Loading MDB database and Sync Provider
# See slapo-syncprov(5) and slapd.backends(5) for more details.
#
moduleload back_mdb.la
moduleload syncprov.la
moduleload ppolicy.la

database mdb
suffix "dc=domain,dc=alt"
rootdn "cn=admin,dc=domain,dc=alt"
rootpw password

overlay ppolicy
ppolicy_default "cn=default,ou=policies,dc=domain,dc=alt"
ppolicy_use_lockout

directory /tmp/ldap

# This option configures one or more hashes to be used in
generation of user passwords
# {CLEARTEXT} indicates that the new password should be added to
userPassword as clear text.
```

```
password-hash {CLEARTEXT}

# SASL Auth

#
# SASL Users authenticate against the following
# meta DNs in the LDAP tree:
#
# With a SASL Realm:
# uid=<username>,cn=<realm>,cn=<mechanism>,cn=auth
#
# Without a SASL Realm:
# uid=<username>,cn=<mechanism>,cn=auth
#
# Map the meta DN to a real dn using authz-regexp.
#
# See slapauth(8) for more details on SASL authentication.
#

authz-regexp
  uid=admin,cn=[^,]*,cn=auth
  cn=admin,dc=domain,dc=alt

authz-regexp
  uid=([^,]*),cn=[^,]*,cn=auth
  uid=$1,ou=people,dc=domain,dc=alt

TLSCACertificateFile /certs/ca.pem
TLSCertificateFile /certs/dc0.domain.alt.pem
TLSCertificateKeyFile /certs/dc0.domain.alt.key
```

5. Создать файл тестовых данных `domain.alt.ldif` со следующим содержимым:

```
dn: dc=domain,dc=alt
objectClass: organization
objectClass: dcObject
dc: domain
```

```
o: alt

dn: ou=users,dc=domain,dc=alt
objectClass: top
objectClass: organizationalUnit
ou: users
description: Central location for users

dn: ou=groups,dc=domain,dc=alt
objectClass: top
objectClass: organizationalUnit
ou: groups
description: Central location for groups

dn: ou=equipment,dc=domain,dc=alt
objectClass: top
objectClass: organizationalUnit
ou: equipment
description: Central location for computers

dn: ou=policies,dc=domain,dc=alt
objectClass: top
objectClass: organizationalUnit
ou: policies
description: Central location for policies

dn: cn=default,ou=policies,dc=domain,dc=alt
cn: default
objectClass: organizationalRole
objectClass: pwdPolicy
pwdAttribute: userPassword
pwdMinLength: 12
pwdCheckQuality: 2
pwdMaxFailure: 10
pwdLockout: TRUE
pwdLockoutDuration: 600
```

```
pwdInHistory: 5
pwdMustChange: TRUE

dn: ou=test_delete_ou,dc=domain,dc=alt
objectClass: top
objectClass: organizationalUnit
ou: test_delete_ou
description: OU for deletion testing

dn: ou=test_rename_ou,dc=domain,dc=alt
objectClass: top
objectClass: organizationalUnit
ou: test_rename_ou
description: OU for rename testing

dn: ou=test_mod_ou,dc=domain,dc=alt
objectClass: top
objectClass: organizationalUnit
ou: test_mod_ou
description: OU for modififcation testing

dn: cn=test_delete_group,ou=groups,dc=domain,dc=alt
objectClass: top
objectClass: posixGroup
cn: test_delete_group
gidNumber: 0

dn: cn=test_rename_group,ou=groups,dc=domain,dc=alt
objectClass: top
objectClass: posixGroup
cn: test_rename_group
gidNumber: 1

dn: cn=test_mod_group,ou=groups,dc=domain,dc=alt
objectClass: top
objectClass: posixGroup
cn: test_mod_group
```

```
gidNumber: 1

dn: cn=test_delete_user,ou=users,dc=domain,dc=alt
uid: test_delete_user
gecos: test_delete_user
objectClass: top
objectClass: account
objectClass: posixAccount
objectClass: shadowAccount
userPassword: {SSHA}RsAMqOI3647qg1gAZF3x2BKBnp0sEVfa
shadowLastChange: 15140
shadowMin: 0
shadowMax: 99999
shadowWarning: 7
loginShell: /bin/false
uidNumber: 801
gidNumber: 801
homeDirectory: /home/test_delete_user

dn: cn=test_mod_user,ou=users,dc=domain,dc=alt
uid: test_mod_user
gecos: test_mod_user
objectClass: top
objectClass: account
objectClass: posixAccount
objectClass: shadowAccount
userPassword: {SSHA}RsAMqOI3647qg1gAZF3x2BKBnp0sEVfa
shadowLastChange: 15140
shadowMin: 0
shadowMax: 99999
shadowWarning: 7
loginShell: /bin/false
uidNumber: 801
gidNumber: 801
homeDirectory: /home/test_mod_user
```

```
dn: cn=test_rename_user,ou=users,dc=domain,dc=alt
uid: test_rename_user
gecos: test_rename_user
objectClass: top
objectClass: account
objectClass: posixAccount
objectClass: shadowAccount
userPassword: {SSHA}RsAMqOI3647qg1gAZF3x2BKBnp0sEVfa
shadowLastChange: 15140
shadowMin: 0
shadowMax: 99999
shadowWarning: 7
loginShell: /bin/false
uidNumber: 801
gidNumber: 801
homeDirectory: /home/test_rename_user

dn: cn=test_search_user,ou=users,dc=domain,dc=alt
uid: test_search_user
gecos: test_search_user
objectClass: top
objectClass: account
objectClass: posixAccount
objectClass: shadowAccount
userPassword: {SSHA}RsAMqOI3647qg1gAZF3x2BKBnp0sEVfa
shadowLastChange: 15140
shadowMin: 0
shadowMax: 99999
shadowWarning: 7
loginShell: /bin/false
uidNumber: 801
gidNumber: 801
homeDirectory: /home/test_search_user

dn: cn=test_block_user,ou=users,dc=domain,dc=alt
uid: test_block_user
```

```
gecos: test_block_user
objectClass: top
objectClass: account
objectClass: posixAccount
objectClass: shadowAccount
userPassword: {SSHA}gVK8WC9YyFT1gMsQHTGCgT3sSv5zYWx0
shadowLastChange: 15140
shadowMin: 0
shadowMax: 99999
shadowWarning: 7
loginShell: /bin/false
uidNumber: 801
gidNumber: 801
homeDirectory: /home/test_block_user

dn: cn=test_rename_computer,ou=equipment,dc=domain,dc=alt
objectClass: top
objectClass: device
cn: test_rename_computer
description: Some brand of computer
seeAlso: dc=domain,dc=alt
serialnumber: 1-77-23-13
l: Room 17
owner: cn=john smith,ou=people,dc=domain,dc=alt
ou: equipment

dn: cn=test_mod_computer,ou=equipment,dc=domain,dc=alt
objectClass: top
objectClass: device
cn: test_mod_computer
description: Some brand of computer
seeAlso: dc=domain,dc=alt
serialnumber: 1-77-23-17
l: Room 17
owner: cn=john smith,ou=people,dc=domain,dc=alt
ou: equipment
```

```
dn: cn=test_delete_computer,ou=equipment,dc=domain,dc=alt
objectClass: top
objectClass: device
cn: test_delete_computer
description: Some brand of computer
seeAlso: dc=domain,dc=alt
serialnumber: 1-77-23-18
l: Room 17
owner: cn=john smith,ou=people,dc=domain,dc=alt
ou: equipment
```

6. Создать скрипт заполнения OpenLDAP тестовыми данными `start-ldap.sh` со следующим содержимым:

```
#!/bin/bash

mkdir /tmp/ldap

slapd -d any -h "ldap://0.0.0.0:3890/ ldaps://0.0.0.0:6360" -f
./slapd.conf 2>&1 > /tmp/slapd.log &

i=0
while [ $i -le 15 ]
do
if ldapadd -x -f ./domain.alt.ldif -H ldap://127.0.0.1:3890 -D
"cn=admin,dc=domain,dc=alt" -w password ; then
break
else
sleep 2
i=$(( $i + 1 ))
fi
done

if [ $? -ne 0 ]; then
echo "Error while configuring slapd service!"
cat /tmp/slapd.log
```

```
exit 1
fi
```

7. Запустить скрипт:

```
# chmod +x start-ldap.sh
# ./start-ldap.sh
```

2.4. Настройка узла с libdomain

Все действия выполняются на узле (192.168.0.152).

Для установки libdomain на машину с ОС «Альт» следует установить пакеты libdomain libdomain-tests:

```
# apt-get install libdomain libdomain-tests
```

2.5. Тестирование libdomain

Для тестов samba/AD нужно указать переменные:

- LDAP_SERVER=ldap://dc0.domain.alt:389
- LDAPS_SERVER=ldaps://dc0.domain.alt:636
- LDAP_CA_CERT=/certs/ca.pem
- DIRECTORY_TYPE=AD
- VALID_CONFIG_FILE=/<путь к файлу>/config.ini

Для тестов OpenLDAP нужно указать переменные:

- LDAP_SERVER=ldap://<ipv4 хоста>:3890
- LDAPS_SERVER=ldaps://dc0.domain.alt:6360
- LDAP_CA_CERT=/certs/ca.pem
- DIRECTORY_TYPE=OpenLDAP
- VALID_CONFIG_FILE=/<путь к файлу>/config.ini