cepces-test

Предусловия

Стенд:

- Клиент с ALT (в качестве клиента AD)
- Windows Server 2012R2 (в качестве сервера AD)

Настройка Windows AD на Windows Server

Настройка AD DS

В данном тест-кейсе используется Windows Server 2012R2, hostname: **addc.windows.testdomain**, пароль администратора домена `$Password1`.

1. Изменить имя машины:
    1. Правой кнопкой на **Пуск** → **Система** → Раздел **Имя компьютера**, имя домена и параметры рабочей группы **Изменить параметры** → На вкладке **Имя компьютера** нажать кнопку **Изменить** → В поле **Имя компьютера** ввести `addc` → Перезагрузить систему.
2. Добавить роль AD:
    1. Открыть диспетчер серверов.
    2. **Управление** → **Добавить роли и компоненты**.
    3. На этапе **Перед началом работы**, **Тип установки** и **Выбор сервера** всё оставить по умолчанию и нажать **Далее**.
    4. На этапе **Роли сервера** выбрать роль **Доменные службы Active Directory** (В открывшемся окне нажать **Добавить компоненты**) и нажать **Далее**.
    5. На этапе **Компоненты**, **AD DS** всё оставить по умолчанию и нажать **Далее**.
    6. На этапе **Подтверждение** всё оставить по умолчанию и нажать **Установить** → **Дождаться окончания установки** и нажать **Закрыть**.
    б3. Нажать на значок **Уведомление** (восклицательный желтый знак).
    1. В открывшемся списке выбрать **Доменные службы Active Directory** → Нажать **Повысить роль этого сервера до уровня контроллера домена**.
    2. На этапе **Конфигурация развертывания** выбрать **Добавить новый лес** и в поле **Имя корневого домена** ввести `windows.testdomain` и нажать **Далее**.
    3. На этапе **Параметры контроллера домена** ввести **Пароль** и **Подтверждение пароля для режима восстановления служб каталогов** и нажать **Далее**.
    4. На оставшихся этапах всё оставить по умолчанию. На последнем этапе нажать **Установить**.
    5. После окончания установки перезагрузить систему.
3. Так же нужно заменить логин администратора на английский (если он на русском):
    1. Открыть диспетчер серверов.
    2. Нажать **Средства** → **Active Directory - домены и доверие**.
    3. В открывшемся окне кликнуть правой кнопкой мыши на созданный ранее домен → **Управление**.
    4. В открывшемся окне выбрать созданный домен → **Users** → Выбрать пользователя **Администратор**.
    5. В открывшемся окне во вкладке **Учетная запись** в поле **Имя входа пользователя** ввести `Admin`, во всплывающем списке (правее поля) выбрать `@windows.testdomain`, в поле **Имя входа пользователя (пред-Windows 2000)** ввести `Admin` и нажать **ОК**.

Настройка Службы сертификации

1. Запустить **Диспетчер серверов** – **Управление** – **Добавить роли и компоненты**.
2. В окне **Мастера добавления ролей** нажать **Далее**.
3. Выбрать тип установки **Установка ролей или компонентов** и нажать **Далее**.
4. В окне выбора целевого сервера нажать **Далее**, если выбран единственный добавленный в диспетчере сервер.
5. В следующем окне выбрать роль **Службы сертификатов Active Directory**, в открывшемся окне нажать **Добавить компоненты**, и нажать **Далее**.
6. Пропустить шаг добавления компонентов, а также информацию о службе сертификатов, нажав **Далее**.
7. На этапе **Выбор служб ролей** выбрать для установки:

    1. **Центр сертификации**
    2. **Веб-служба политик регистрации сертификатов**
    3. **Веб-служба регистрации сертификатов**
8. Нажать **Далее**.
9. На этапах **Роль веб-сервера (IIS)**, **Выбор служб ролей** нажимать **Далее**.
10. На этапе **Подтверждение установки компонентов** отметить чекбокс **Автоматический перезапуск конечного сервера, если требуется**.
11. Нажать **Установить**.
12. Нажать на значок **Уведомление** (восклицательный желтый знак).
13. Выбрать **Настроить службы сертификатов Active Directory**.
14. На этапе **Учетные данные** нажать **Далее**.
15. На этапе **Службы ролей** отметить чекбокс **Центр сертификации**
16. Нажать **Далее**.
17. На этапе **Вариант установки** выбрать **ЦС предприятия**, нажать **Далее**.
18. На этапе **Тип ЦС** выбрать **Корневой ЦС**, нажать **Далее**.
19. На этапах **Закрытый ключ**, **Шифрования для ЦС** нажать **Далее**.
20. На этапе **Имя ЦС** убедиться, что указано **Общее имя для этого ЦС** как `windows-ADDC-CA`, нажать **Далее**.
21. На этапах **Срок действия**, **База данных ЦС**, нажать **Далее**.
22. На этапе **Подтверждение** нажать **Настроить**.
23. Нажать **Закрыть**.
24. При запросе **Вы хотите настроить дополнительные службы ролей?** нажать **Да**.
25. На этапе **Учетные данные** нажать **Далее**.
26. На этапе **Службы ролей** отметить следующие чекбоксы:
    1. **Веб-служба регистрации сертификатов**
    2. **Веб-служба политик регистрации сертификатов**
27. Нажать **Далее**.
28. На этапах **ЦС для CES**, **Тип проверки подлинности для службы CES** нажимать **Далее**.
29. На этапе Учетная запись службы CES выбрать **Использовать встроенное удостоверение пула приложений**, нажать **Далее**.
30. На этапе **Тип проверки подлинности для службы CEP** нажать **Далее**.
31. На этапе **Сертификат сервера** выбрать **Выбрать и назначить сертификат для SSL позже** и нажать **Далее**.
32. На этапе **Подтверждение** нажать **Настроить**.
33. Нажать **Закрыть**.
34. Перезагрузить сервер для применения настроек.

Настройка автоматической регистрации сертификата сервера

1. На компьютере, на котором установлен AD DS, открыть **Windows PowerShell**, ввести `mmc` и нажать клавишу `ВВОД`. Откроется консоль управления (MMC).
2. В меню **Файл** выбрать **Добавить или удалить оснастку**. Откроется диалоговое окно **Добавление или удаление оснастки**.
3. В **доступных оснастках** прокрутить вниз и дважды щёлкнуть **Редактор управления групповыми политиками**. Откроется диалоговое **окно выбора объекта** групповой политики.
4. В **объекте групповой политики** нажать кнопку **Обзор**. Откроется диалоговое окно **Поиск объекта групповой политики**.
5. В **доменах, подразделениях и связанных объектах** групповой политики выбрать **Default Domain Policy** и нажать кнопку **ОК**.
6. Нажмите кнопку **Готово**, а затем — кнопку **ОК**.
7. Дважды щёлкнуть на **Политика Default Domain Policy**. В консоли развернуть следующий путь: **Конфигурация компьютера** → **Политики** → **Windows Параметры** → **Параметры безопасности** → **Политики открытого ключа**.
8. Щёлкнуть **Политики открытого ключа**. На панели подробностей дважды щёлкнуть параметр **Клиент службы сертификации: автоматическая регистрация**. Откроется диалоговое окно **Свойства**. Настроить следующие элементы:
    1. В окне **Модель конфигурации** выбрать параметр **Включено**.

2. Выбрать **Обновлять сертификаты с истекшим сроком действия или в состоянии ожидания и удалять отозванные сертификаты**.
3. Выбрать **Обновлять сертификаты и удалять отозванные сертификаты**.

9. Нажать кнопку **ОК**.
10. Перезагрузить систему сервера для применения настроек.

Настройка общего каталога на сервере

1. Создать на сервере папку `C:\Share`.
2. Перейти в свойства данной папки.
3. Перейти на вкладку **Доступ**.
4. Нажать **Общий доступ**.
5. Добавить группу **Все**.
6. Изменить права группы **Все** на **Чтение и запись**.
7. Нажать **Поделиться**.
8. Нажать **Готово**.

Настройка сервера IIS

1. На сервере открыть **Диспетчер служб IIS**.
2. Выбрать **ADDC (Windows\Admin)**.
3. Выбрать **Сертификаты сервера** двойным кликом.
4. На правой панели выбрать **Создать сертификат домена**.
5. Указать следующие настройки:
   1. Полное имя: `addc.windows.testdomain`
   2. Организация: `windows`
   3. Подразделение: `windows`
   4. Город: `windows`
   5. Област, край: `windows`
   6. Страна или регион: **RU**
6. Нажать **Далее**.
7. В окне **Локальный центр сертификации** нажать **Выбрать** и выбрать **windows-ADDC-CA**.
8. Задать понятное имя как: `SSLCertificate`
9. Нажать **Готово**.
10. Раскрыть дерево, выбрать путь **сайты → Default Web Site**.
11. Нажать на правой панели **Привязки**.
12. Выбрать **https**.
13. Нажать **Изменить**.
14. Выбрать SSL-сертификат **SSLCertificate**.
15. Нажать **Вид**.
16. Выбрать вкладку **Состав**.
17. Нажать **Копировать в файл**.
18. Нажимать **Далее** до окна с выбором указания файла.
19. Нажать **Обзор**, выбрать путь: `C:\Share\windowsad.cer`.
20. Нажать **Далее**, затем **Готово**.
21. Скопировать аналогично сертификат **windows-ADDC-CA** как `C:\Share\windowsad-root.cer`
22. На правой панели нажать кнопку **Перезапустить**.

Настройка клиентов

Ввести клиентов ALT в данный домен с применением групповых политик:

```
# apt-get install -y task-auth-ad-sssd pwgen alterator-gpupdate && \
DOMAINNAME="windows.testdomain" && \
SERVERIP=<AD SERVER IP> && hostname=$(pwgen -1 -A) && \
hostnamectl set-hostname $hostname.${DOMAINNAME} && \
echo -e "name_servers=${SERVERIP}\nsearch_domains=${DOMAINNAME}" >> /etc/resolvconf.conf && \
```

```
reboot

# system-auth write ad "windows.testdomain" "$(hostname --short)" "WINDOWS" Admin '$Password1' --gpo && \
reboot
```

Настроить общий каталог (ввести пароль администратора домена):

```
# mkdir -p /mnt/adshare && mount -v -t cifs -o user=Admin //addc.windows.testdomain/share /mnt/adshare && l
/mnt/adshare
```

Установить сертификат для IIS:

```
# cp /mnt/adshare/windowsad.cer /etc/pki/ca-trust/source/anchors/ && \
update-ca-trust && \
trust  list | grep windows
```

Вывод:

```
label: addc.windows.testdomain
```

Установить корневой сертификат CA:

```
# cp /mnt/adshare/windowsad-root.cer /etc/pki/ca-trust/source/anchors/ && \
update-ca-trust && \
trust  list | grep windows-addc-ca -i
```

Установленные пакеты на клиентах ALT:

```
# apt-get install -y cepces cepces-certmonger python3-module-cepces samba-gpupdate
```

Создать папку для хранения будущих запросов:

```
# mkdir -p /etc/pki/trust/anchors
```

Настроить `cepces` по умолчанию:

```
# sed -i "s/^server=.*/server=addc.windows.testdomain/" /etc/cepces/cepces.conf && grep 'server='
/etc/cepces/cepces.conf
```

Шаги

Шаг 1

Описание

Убедиться, что **cepces** зарегистрирован в **certmonger** на клиенте:

```
# getcert list-cas -c cepces
```

Ожидаемый результат

Вывод:

```
CA 'cepces':
        is-default: no
        ca-type: EXTERNAL
        helper-location: /usr/libexec/certmonger/cepces-submit
```

Шаг 2

Описание

Выполнить команду:

```
# samba-gpupdate --rsop
```

Ожидаемый результат

Присутствует запрос на сертификат

```
. . . . .
  CSE: gp_cert_auto_enroll_ext
  -----------------------------------------
    Policy Type: Auto Enrollment Policy
    -----------------------------------------
    [ windows-ADDC-CA ] =
      [ CA Certificate ] =
-----BEGIN CERTIFICATE-----
MIIDeTCCAmGgAwIBAgIQEVQMb91+MIFOi+qNlMEj8TANBgkqhkiG9w0BAQUFADBP
MRowGAYKCZImiZPyLGQBGRYKdGVzdGRvbWFpbjEXMBUGCgmSJomT8ixkARkWB3dp
bmRvd3MxGDAWBgNVBAMTD3dpbmRvd3MtQUREQy1DQTAeFw0yMzExMTMxNzI1NDla
Fw0yODExMTMxNzM1NDhaME8xGjAYBgoJkiaJk/IsZAEZFgp0ZXN0ZG9tYWluMRcw
FQYKCZImiZPyLGQBGRYHd2luZG93czEYMBYGA1UEAxMPd2luZG93cy1BRERDLUNB
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA8+z3fCd4iEgpUJhaw1xd
xTMLbmP98f9CCM9Z7kO6C5SOF/GKvvWWj/2kmzYhKJN/poMbDL+jEc58VetThvYL
DYVxkuucJNYu6aFD3H7t1mW7A/zMQomNmvZoz4kKtbUwUyITYl0jHlZyiNjKJLgY
k2qdvAOz3sZR+6muawnOSNd53ETbplVkSJQDgl+HsDrDiW/Bv2BEAwA06tH8PV4p
QiIF+EnWnxTIFb8J6rcySO/2ZSqC+yBJBFcNx+8tAaiqRngGJiOpTT3To/Ztiej1
q9oeXe60ZCelazu9ng0yu21Cg7R9ReQbMbcmbjES7wNSvtCo/F6p2ST9f4IRAzQo
4wIDAQABo1EwTzALBgNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4E
FgQUEJnKq+DRRWHpaNstEWXS/9ABUPQwEAYJKwYBBAGCNxUBBAMCAQAwDQYJKoZI
hvcNAQEFBQADggEBACEOCu/l1oeA/qSUue2SAz2e8p+Xi0bqpULt082X4+A1Fg4R
5JAei5nmsb9/bMflqMJQBCIXUwgZDYpx9sQHO5HVUfbrBX/m3XLV84NmbWRULqvZ
nqcnKXfuizSpdpEYauFic8JV7vQXvl57OzxztKmHz4gmDurJHaEyWJLllCLSVpnq
GH8WW0QvzVMC1rcwTBCxl/zIk0Oh2IOEyq7l39X5JJL84YixldENGofCziqnoWJ+
jhLKQHfoTY0odSR/Y/ppTCHVPkUb7XWVgdqNSCJF93XqoapMnt9+PSXtwo37i2uz
yFYV55jGtvu49vh+pliarupKFkcnXOP28eVO7kc=
-----END CERTIFICATE-----
      [ Auto Enrollment Server ] = addc.windows.testdomain
      [ Templates ] =
        [ Machine ]
. . . . .
```

Фактический результат

Ошибка:

```
Traceback (most recent call last):
  File "/usr/lib64/python3/site-packages/samba/gp/gpclass.py", line 764, in site_dn_for_machine
    site_name = c.netr_DsRGetSiteName(hostname)
samba.WERROREror: (1210, 'WERR_INVALID_COMPUTERNAME')

During handling of the above exception, another exception occurred:

Traceback (most recent call last):
  File "/usr/sbin/samba-gpupdate", line 131, in <module>
    rsop(lp, creds, store, gp_extensions, username, opts.target)
  File "/usr/lib64/python3/site-packages/samba/gp/gpclass.py", line 1041, in rsop
    gpos = get_gpo_list(dc_hostname, creds, lp, username)
  File "/usr/lib64/python3/site-packages/samba/gp/gpclass.py", line 869, in get_gpo_list
    site_dn = site_dn_for_machine(samdb, dc_hostname, lp, creds, username)
  File "/usr/lib64/python3/site-packages/samba/gp/gpclass.py", line 772, in site_dn_for_machine
    raise ldb.LdbError(ldb.ERR_NO_SUCH_OBJECT,
_ldb.LdbError: (32, 'site_dn_for_machine: no result')
```

В Sisyphus не воспроизводится:

```
# samba-gpupdate --rsop
Resultant Set of Policy
Computer Policy

GPO: Default Domain Policy
================================================================================================================
================================================================================
  CSE: gp_access_ext
  ----------------------------------------------------------------------------------------------------
  ----------------------------------------------------------------------------------------------------
  CSE: gp_krb_ext
  ----------------------------------------------------------------------------------------------------
  ----------------------------------------------------------------------------------------------------
  CSE: gp_scripts_ext
  ----------------------------------------------------------------------------------------------------
  ----------------------------------------------------------------------------------------------------
  CSE: gp_sudoers_ext
  ----------------------------------------------------------------------------------------------------
  ----------------------------------------------------------------------------------------------------
  CSE: vgp_sudoers_ext
  ----------------------------------------------------------------------------------------------------
  ----------------------------------------------------------------------------------------------------
  CSE: gp_centrify_sudoers_ext
  ----------------------------------------------------------------------------------------------------
  ----------------------------------------------------------------------------------------------------
  CSE: gp_centrify_crontab_ext
  ----------------------------------------------------------------------------------------------------
  ----------------------------------------------------------------------------------------------------
  CSE: gp_smb_conf_ext
  ----------------------------------------------------------------------------------------------------
  ----------------------------------------------------------------------------------------------------
  CSE: gp_msgs_ext
  ----------------------------------------------------------------------------------------------------
  ----------------------------------------------------------------------------------------------------
  CSE: vgp_symlink_ext
  ----------------------------------------------------------------------------------------------------
  ----------------------------------------------------------------------------------------------------
  CSE: vgp_files_ext
  ----------------------------------------------------------------------------------------------------
  ----------------------------------------------------------------------------------------------------
  CSE: vgp_openssh_ext
  ----------------------------------------------------------------------------------------------------
  ----------------------------------------------------------------------------------------------------
  CSE: vgp_motd_ext
  ----------------------------------------------------------------------------------------------------
  ----------------------------------------------------------------------------------------------------
  CSE: vgp_issue_ext
  ----------------------------------------------------------------------------------------------------
  ----------------------------------------------------------------------------------------------------
  CSE: vgp_startup_scripts_ext
  ----------------------------------------------------------------------------------------------------
  ----------------------------------------------------------------------------------------------------
  CSE: vgp_access_ext
  ----------------------------------------------------------------------------------------------------
  ----------------------------------------------------------------------------------------------------
  CSE: gp_gnome_settings_ext
  ----------------------------------------------------------------------------------------------------
  ----------------------------------------------------------------------------------------------------
  CSE: gp_cert_auto_enroll_ext
  ----------------------------------------------------------------------------------------------------
    Policy Type: Auto Enrollment Policy
    ------------------------------------------------------------------------------------------------
    [ windows-ADDC-CA ] =
      [ CA Certificate ] =
-----BEGIN CERTIFICATE-----
```

```
MIIDeTCCAmGgAwIBAgIQUNKQIlp1fapMct66eokryjANBgkqhkiG9w0BAQUFADBP
MRowGAYKCZImiZPyLGQBGRYKdGVzdGRvbWFpbjEXMBUGCgmSJomT8ixkARkWB3dp
bmRvd3MxGDAWBgNVBAMTD3dpbmRvd3MtQUREQy1DQTAeFw0yNDAzMjkxNDQxMjla
Fw0yOTAzMjkxNDUxMjlaME8xGjAYBgoJkiaJk/IsZAEZFgp0ZXN0ZG9tYWluMRcw
FQYKCZImiZPyLGQBGRYHd2luZG93czEYMBYGA1UEAxMPd2luZG93cy1BRERDLUNB
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAm9WbqR+cW2o9Mgv81Pne
Us2YiRT8fcGPLJBZIwIInZT4PR2unJWnAMLIZ31pI13d25gErkP3X53Fj1sk8nLY
eST+hD51XSOCh2ZW4PcZ+yGvqUdUdQS+47K2ZZmVt091WpzrgGMMajI1td3hhPV2
IHCaqwaBbBUgnykDVYiUGVsUohK/M3suI0TSYVzLZdQeHZh5Lv2JmXKof+UcE4Tv
p5Jz5m0ZPwBckTXA7IdDeAsBuI+jUaKmbiy8TgFAsSqA5QXVK1qxLLAW7wZWc6pd
tI4N1SK2PFeyYdyS0FzZ0pqSAfPlSdQ0R2nAgBiDMDFDhFaupeNU7mQPH0x1kqaK
2wIDAQABo1EwTzALBgNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4E
FgQUhJ8W6Tf6xLdpo2BhzFU4axPMHWEwEAYJKwYBBAGCNxUBBAMCAQAwDQYJKoZI
hvcNAQEFBQADggEBAIkiC4T/83v90R6c17GOixflXZCU+mclbLE86gzbddYcZ1wn
hV45jYmioVtgvtF2IRG6rHL8hvdm88yqjuFtTUX65puL2iu40wsSikHVwPjJC02s
Xu9r6Wada56oiMi7xoyxFRmkWPWBJrwkumdqYIxSTQyp9z0qE5iznHw6e+8RKTPW
WbR2XE5gsOUOJWN98iMavTn5kNdoZwHnrPjEgWvMsEKN9vXXVSmHp9Zlt4tqUpAu
DSBPI9fBgCWhhQUt5uPLs86kwPweHhSEYScxSYEiw/WnFLFZauwEHgkDb/sM7YPc
G1HZops+F7CWWJ6qgR1SMwS2m9+4ATP91YeJ2YI=
-----END CERTIFICATE-----
      [ Auto Enrollment Server ] =           addc.windows.testdomain
      [ Templates ] =

    ----------------------------------------------------------------------------------------------------
  ----------------------------------------------------------------------------------------------------
  CSE: gp_firefox_ext
  ----------------------------------------------------------------------------------------------------
  ----------------------------------------------------------------------------------------------------
  CSE: gp_chromium_ext
  ----------------------------------------------------------------------------------------------------
  ----------------------------------------------------------------------------------------------------
  CSE: gp_chrome_ext
  ----------------------------------------------------------------------------------------------------
  ----------------------------------------------------------------------------------------------------
  CSE: gp_firewalld_ext
  ----------------------------------------------------------------------------------------------------
  ----------------------------------------------------------------------------------------------------
====================================================================================================
================================================================================
```