Настройка 2ФА на РЕД ОС 7.3 в домене Windows с помощью Рутокен ЭЦП

Описание стенда

Сервер:

ОС: Windows server 2019

доменное имя: server.astradomain.ad

ip: 10.0.2.15

Клиент:

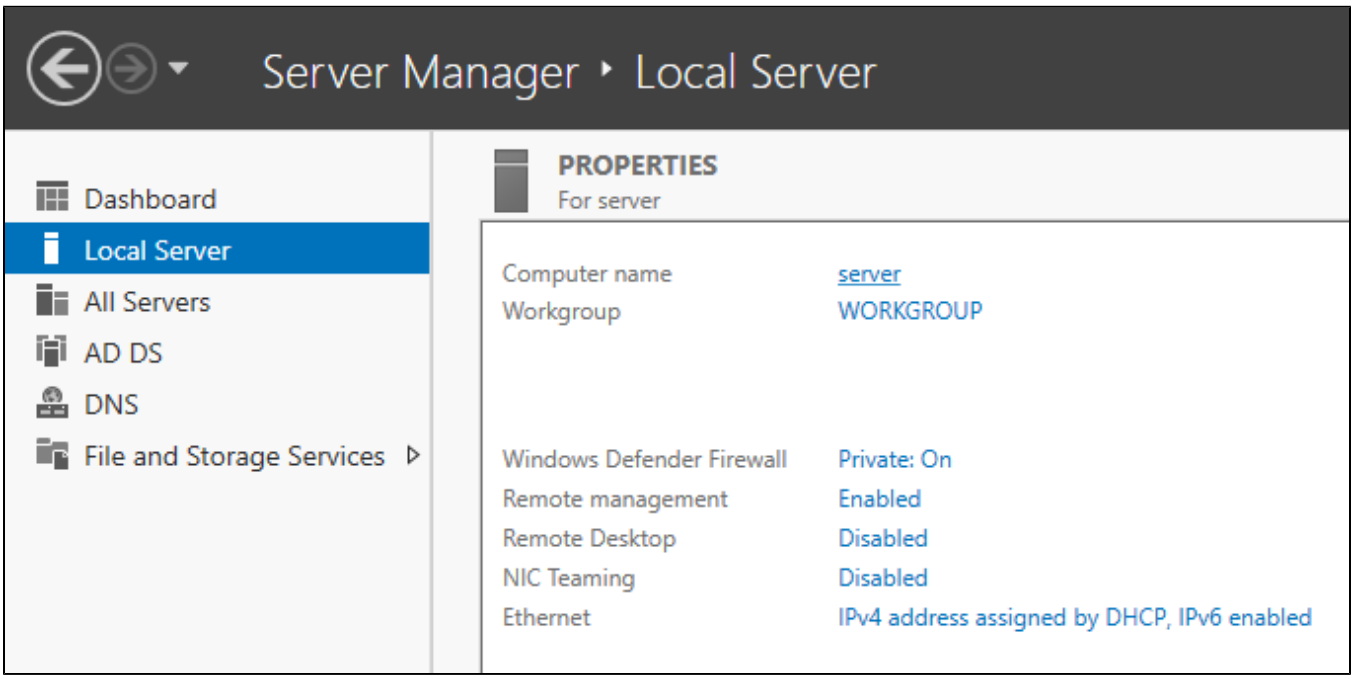
ОС: РЕД ОС

Настройка сервера

Установка сервиса Active Directory

При необходимости измените имя сервера. Это необходимо сделать до выполнения его настройки.

Имя сервера можно задать в окне менеджера сервера:



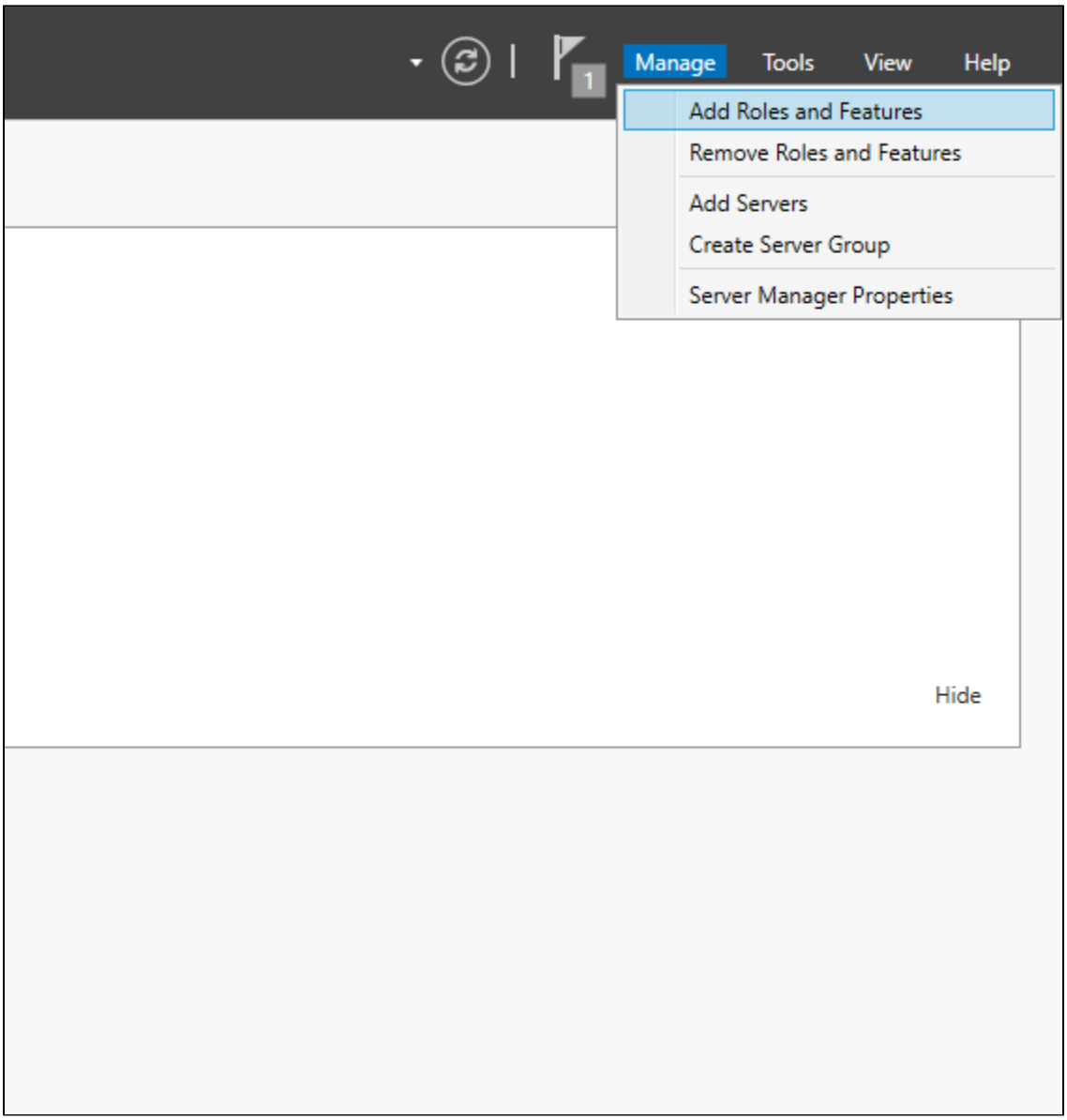
Процедура установки состоит из следующих шагов:

1. Добавление сервисов.
2. Настройка домена.
3. Добавление новых пользователей.
4. Установка центра сертификации Active Directory.

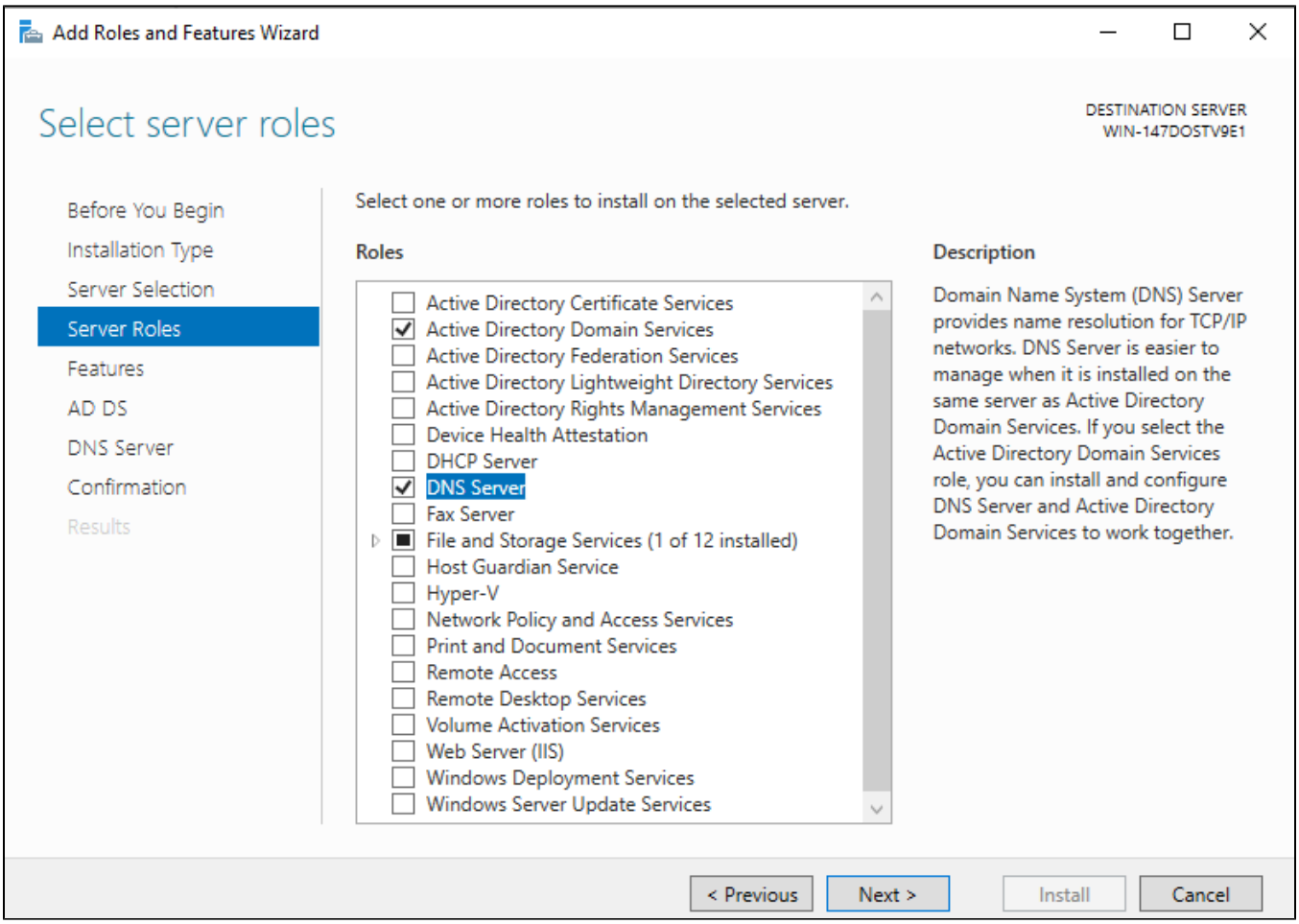
Шаг 1. Добавление необходимых сервисов

Добавьте на сервер сервисы **Active Dirrectory** и **DNS**:

1. Откройте окно для добавления ролей в менеджере сервера:



2. В окне для выбора сервисов установите галочки **Active Directory Domain Services** и **DNS Server**:



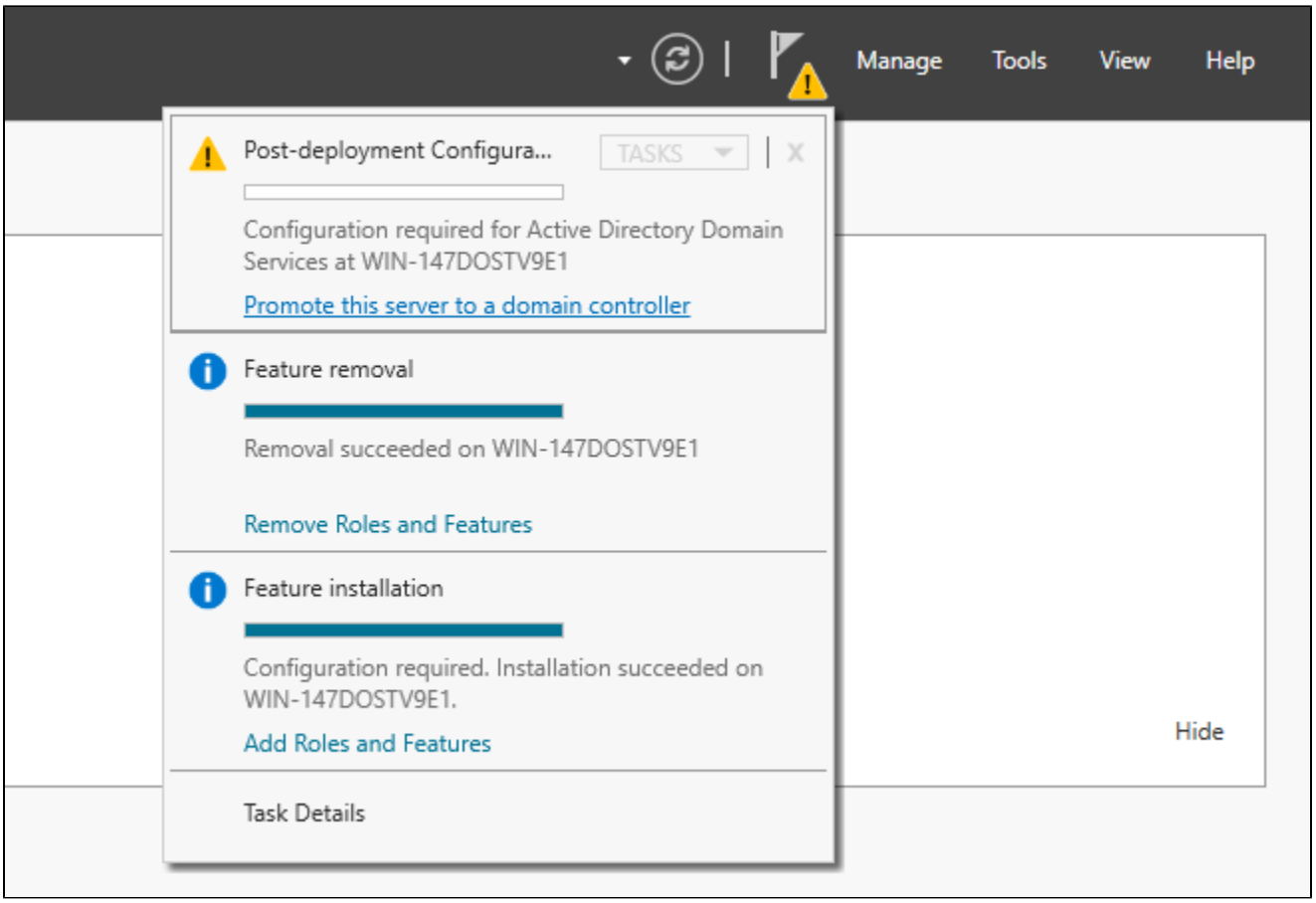
3. Нажмите **Next**.

4. Во всех остальных пунктах даём согласие на установку.

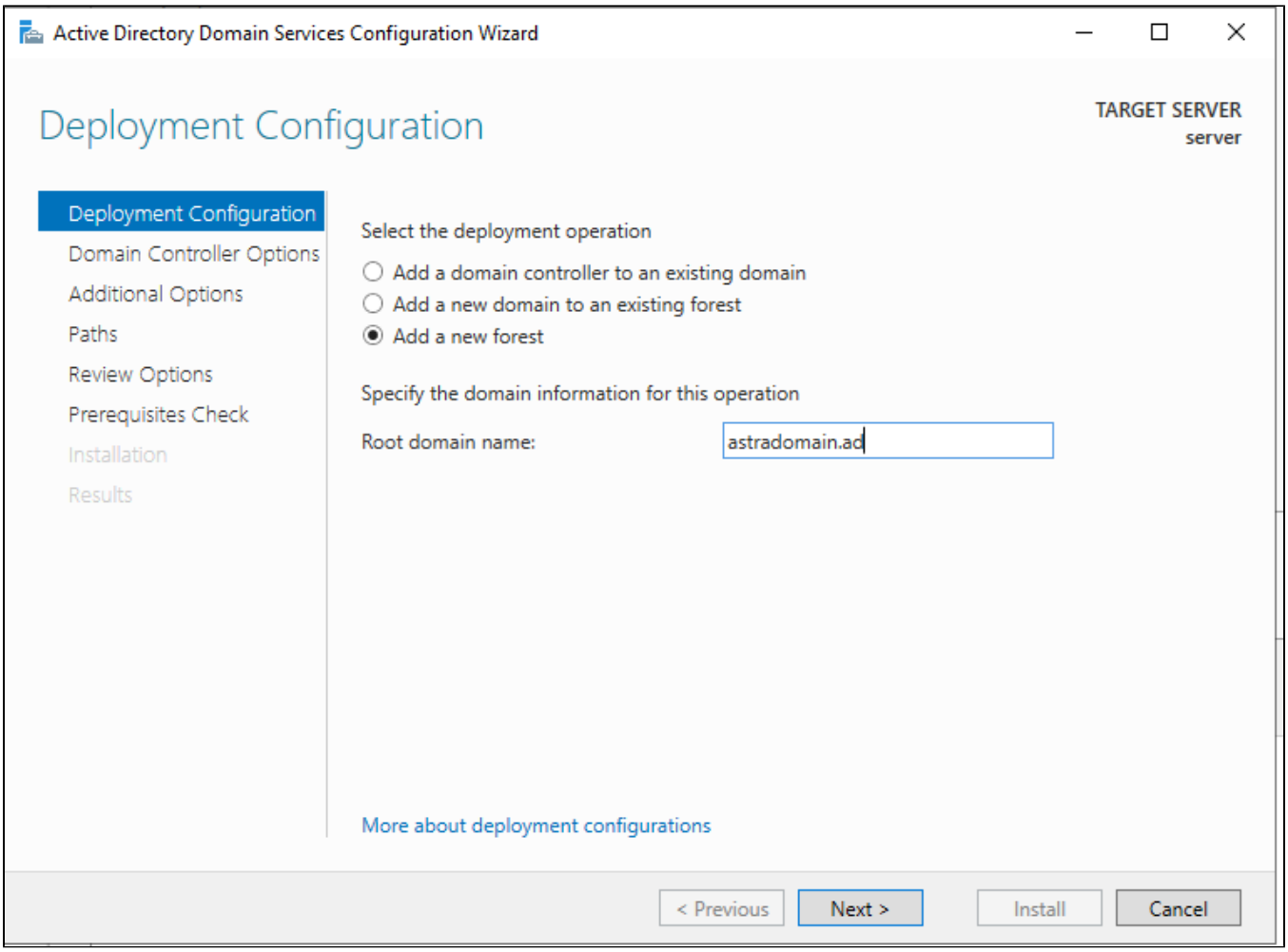
Шаг 2. Настройка домена

После завершения установки сервисов вам надо перейти к настройке домена:

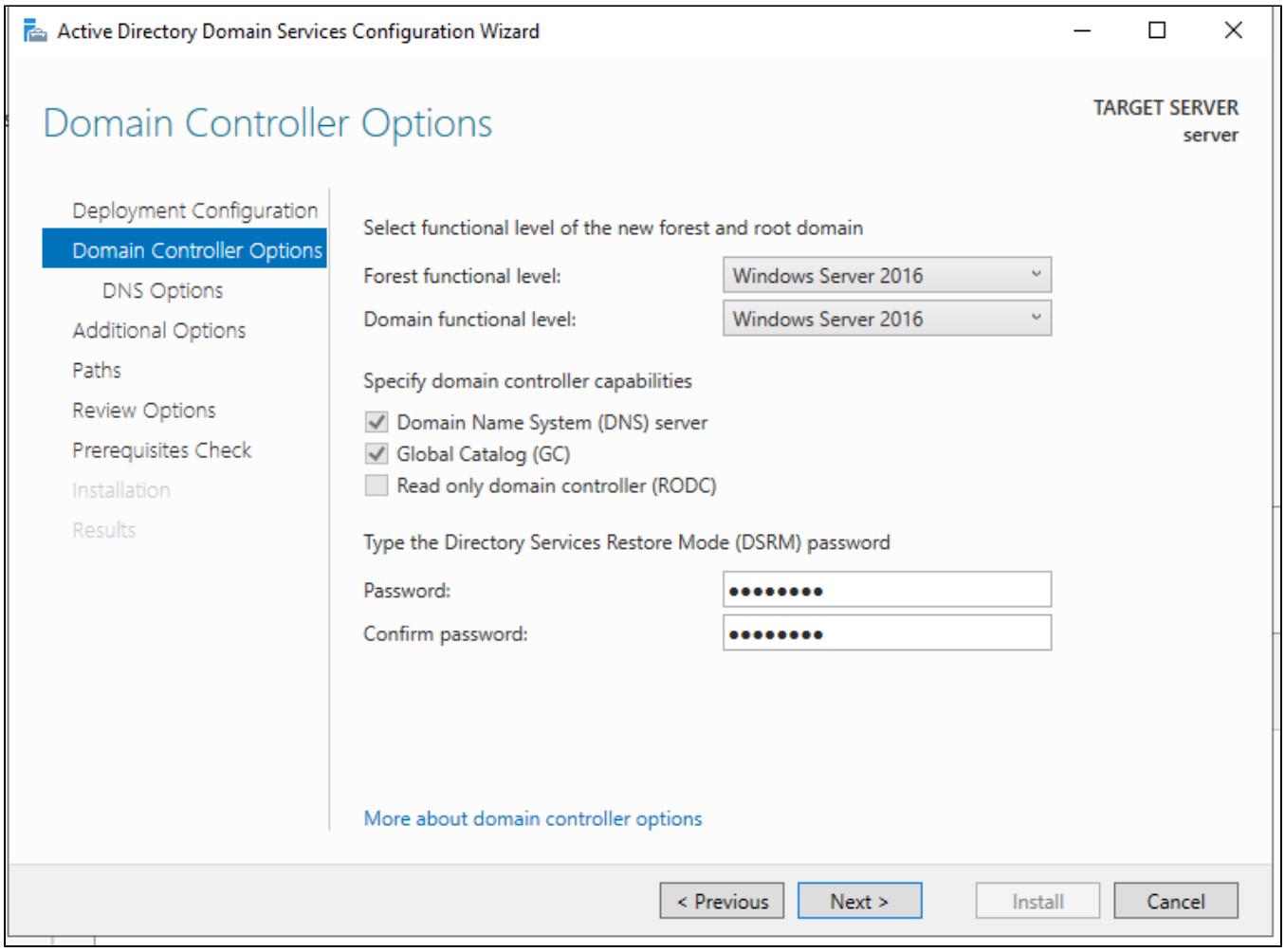
1. Откройте меню уведомлений и выберите пункт "Promote this server to a domain controller":



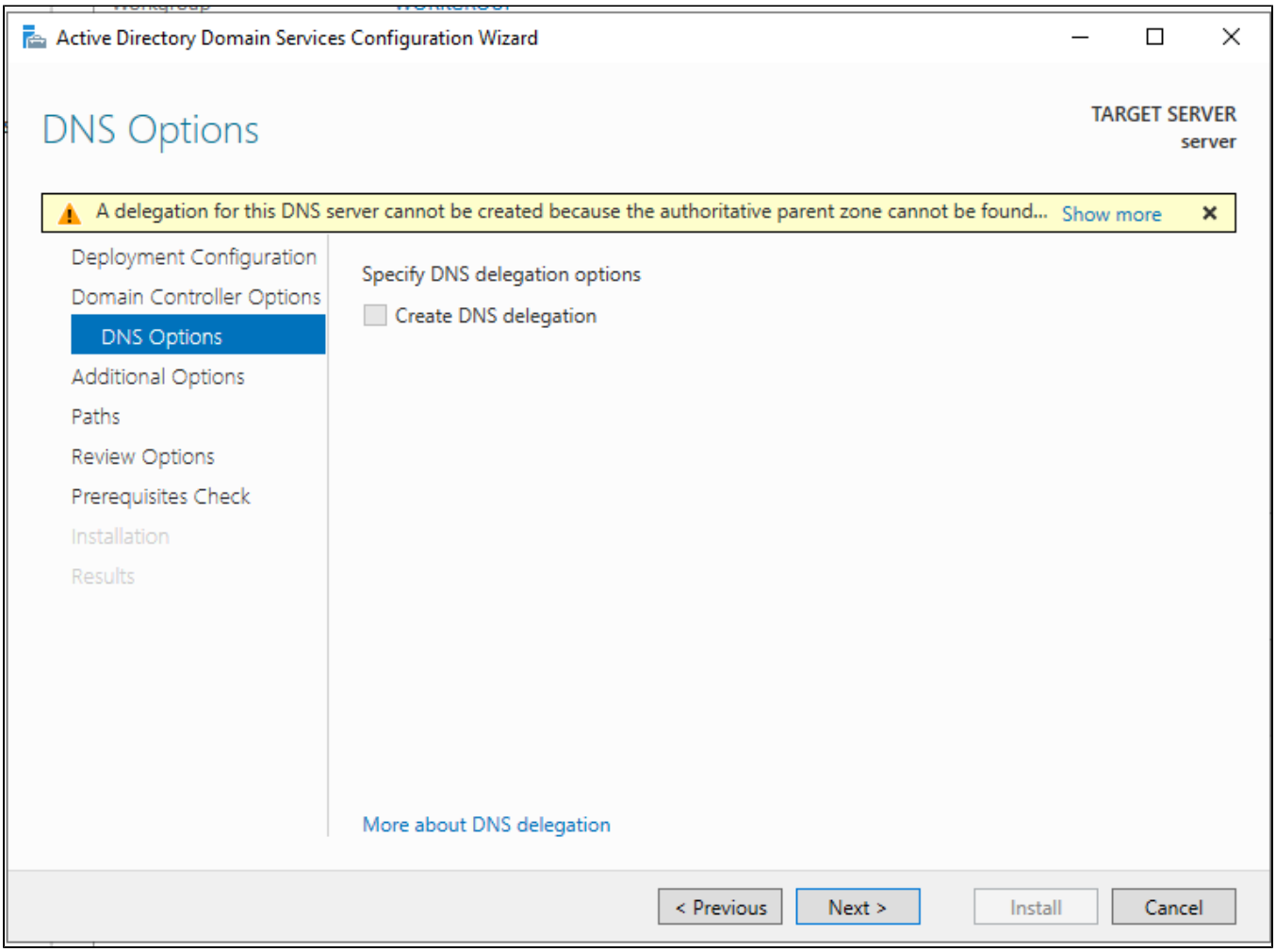
2. На вкладке **Deployment Configuration** выберите опцию для создания нового домена и укажите его название:



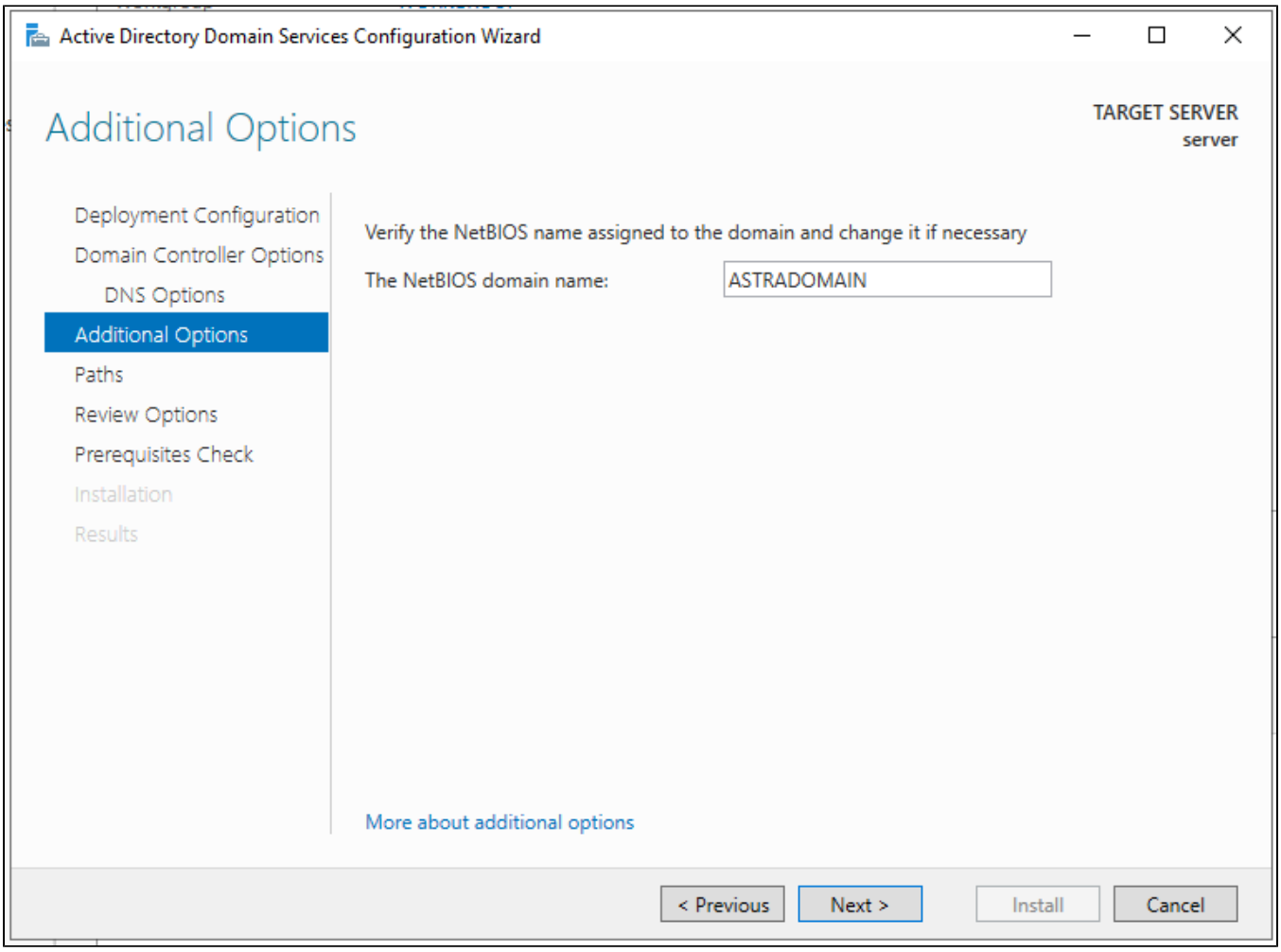
3. Введите пароль сброса:

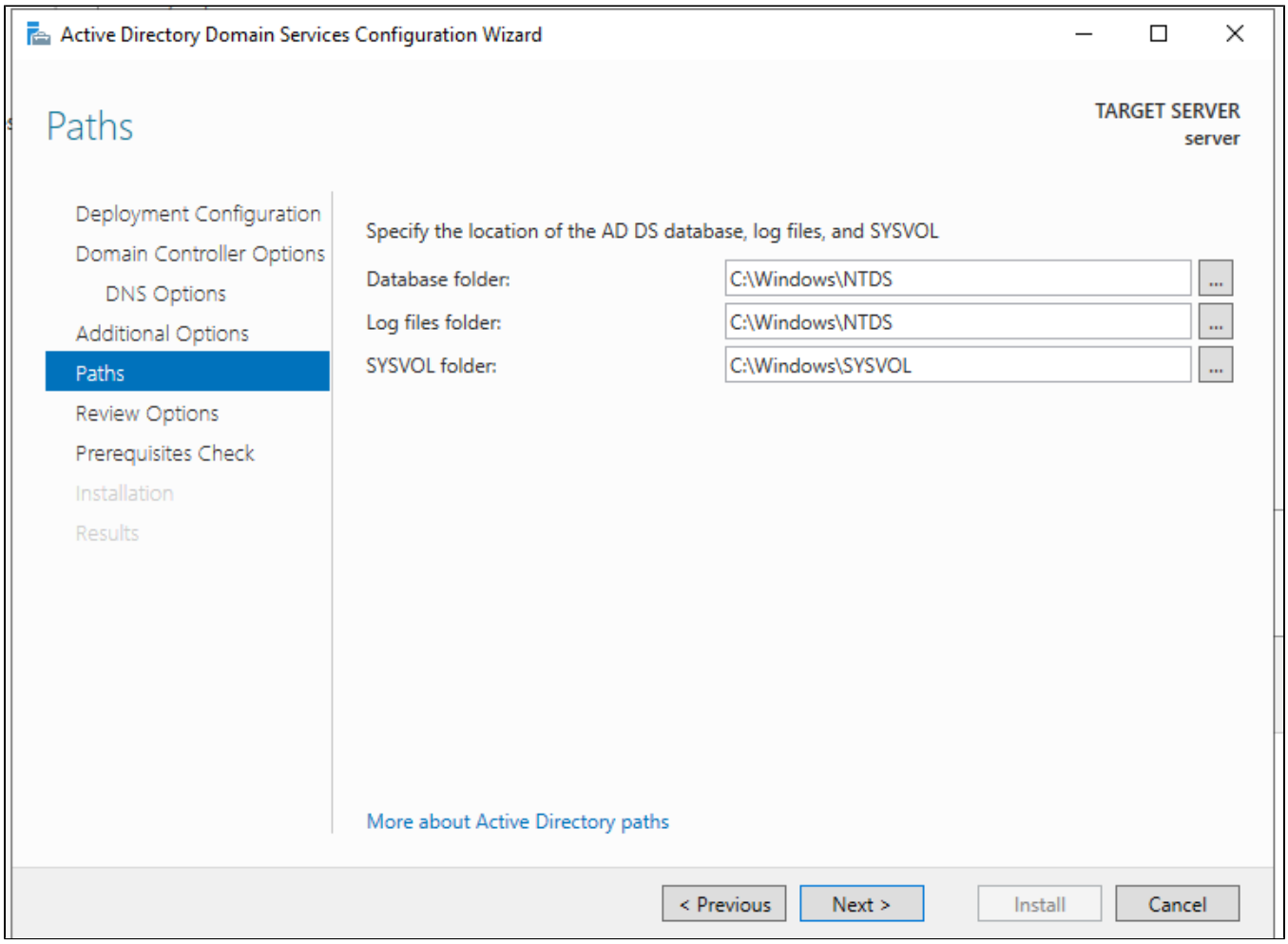


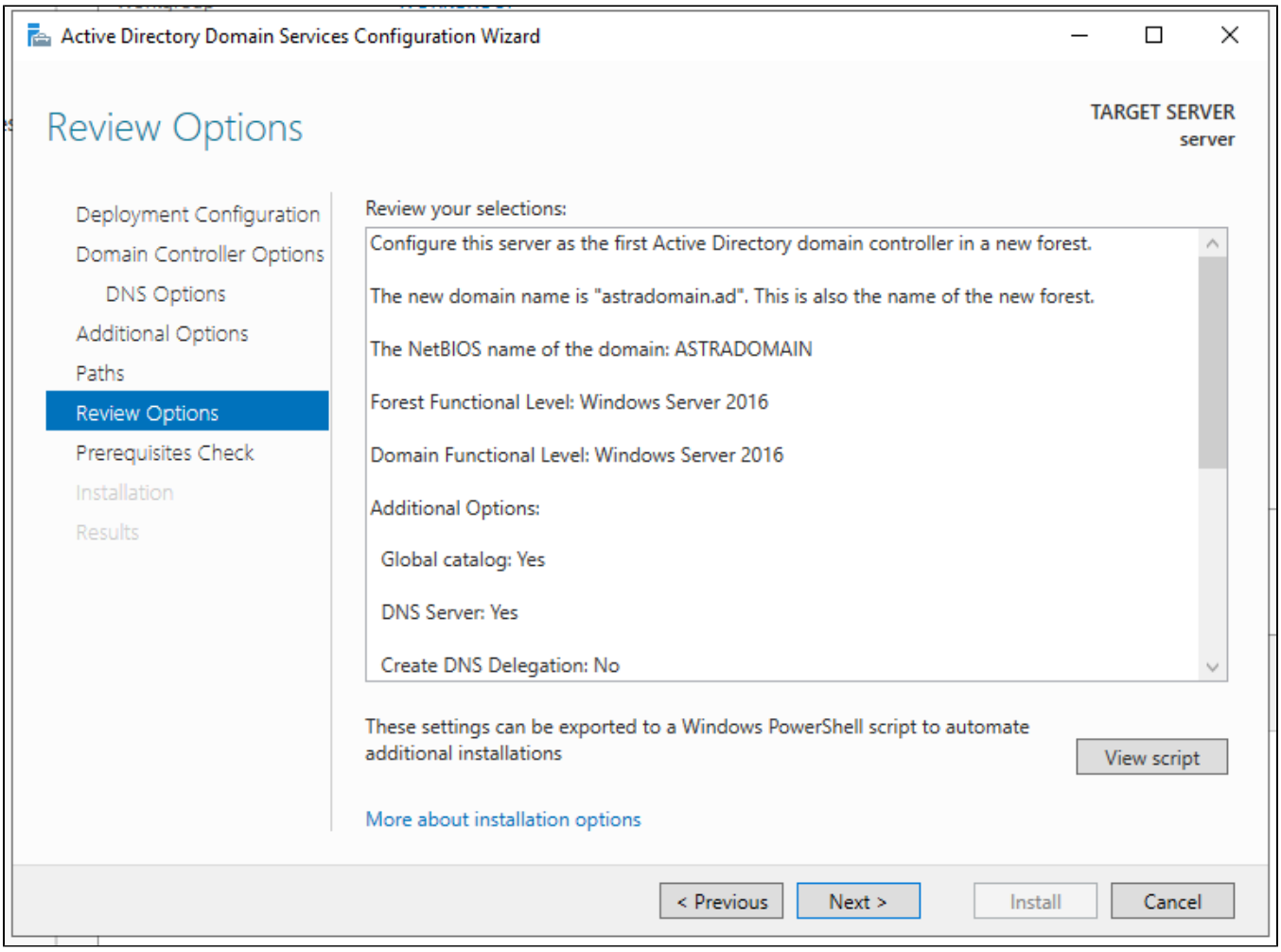
4. На вкладке **DNC Options** ничего не меняйте, т.к. сервер сам является DNS сервером:



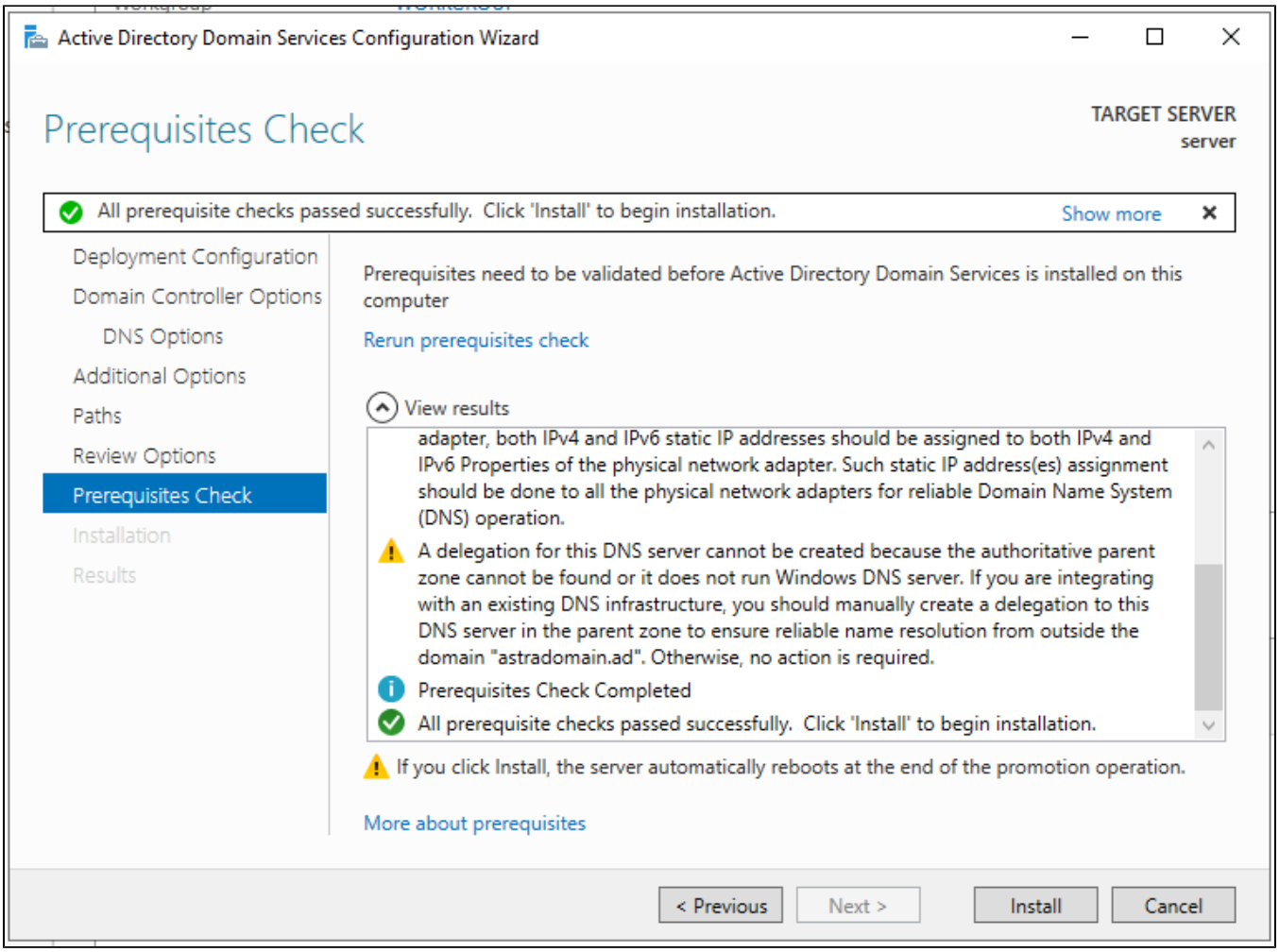
5. На следующих трёх вкладках также оставьте всё как есть:


Active Directory Domain Services Configuration Wizard
Additional Options
TARGET SERVER
server
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Verify the NetBIOS name assigned to the domain and change it if necessary
The NetBIOS domain name:
ASTRADOMAIN
More about additional options
< Previous
Next >
Install
Cancel


Active Directory Domain Services Configuration Wizard
Paths
TARGET SERVER
server
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Specify the location of the AD DS database, log files, and SYSVOL
Database folder:
C:\Windows\NTDS
Log files folder:
C:\Windows\NTDS
SYSVOL folder:
C:\Windows\SYSVOL
More about Active Directory paths
< Previous
Next >
Install
Cancel



6. Перед запуском процесса установки ознакомьтесь с уведомлениями об ошибках. Если необходимо, устраните возникшие проблемы. В нашем случае уведомления не являются критичными:

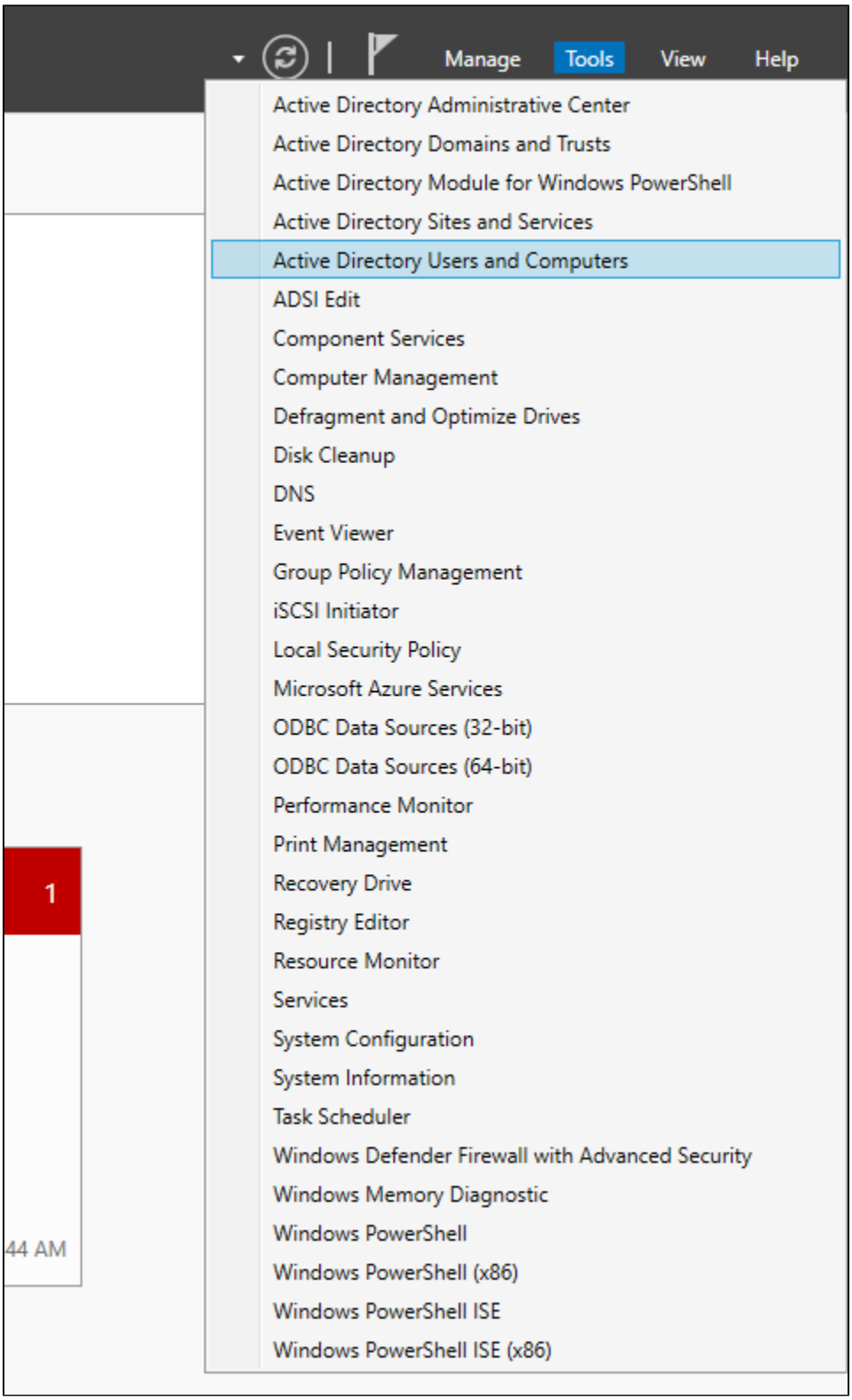


После установки Active Directory сервер перезагрузится. Если настройка прошла успешно, то на экране отобразится окно для входа в аккаунт доменного пользователя.

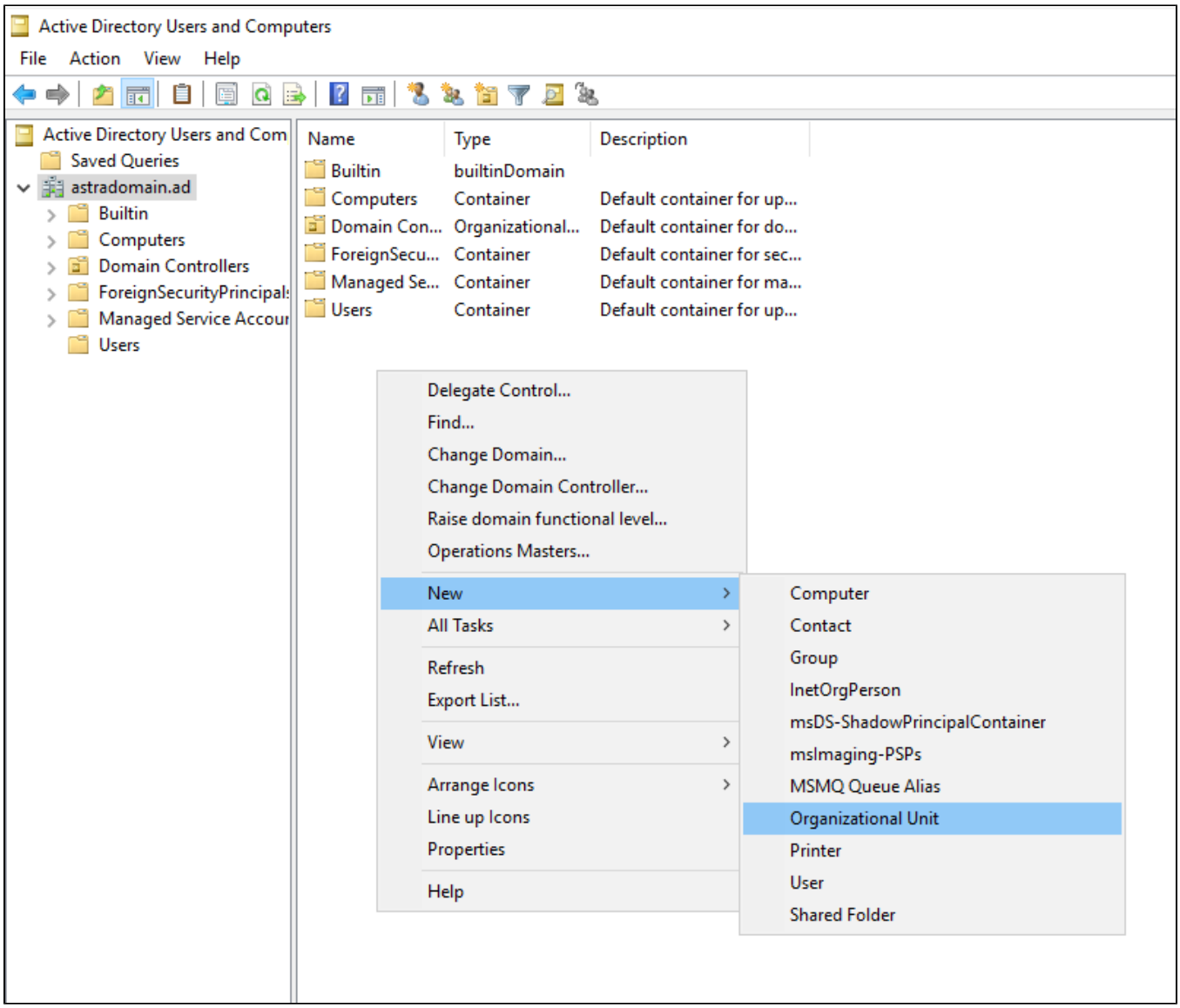
Шаг 3. Добавление новых пользователей

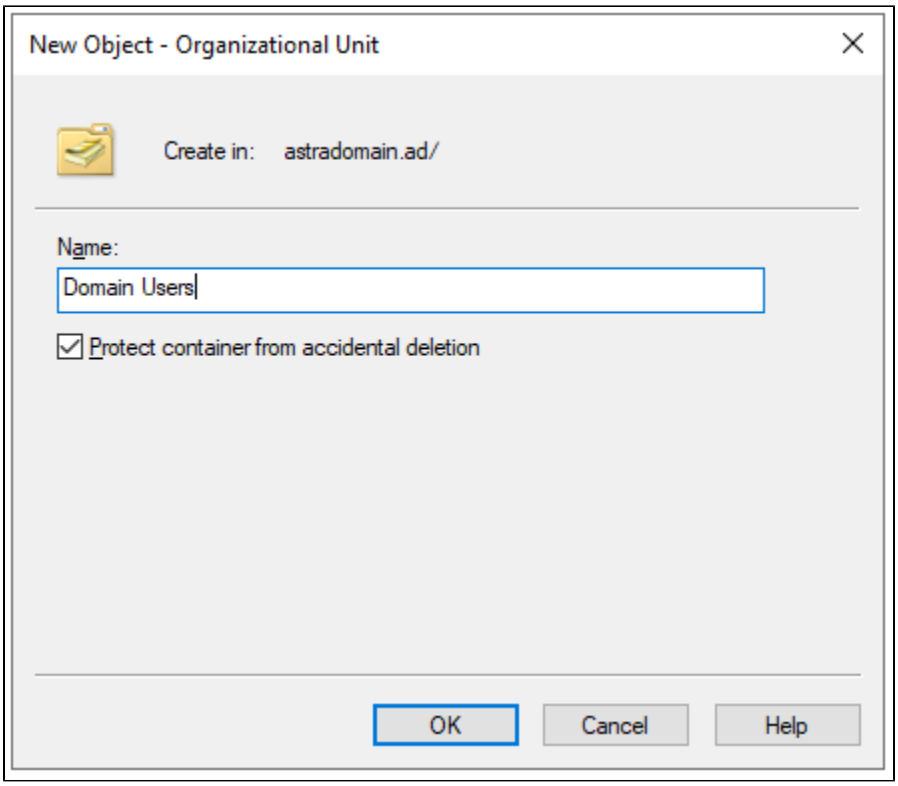
Чтобы добавить новых пользователей:

1. Откройте утилиту управления пользователями и компьютерами домена:

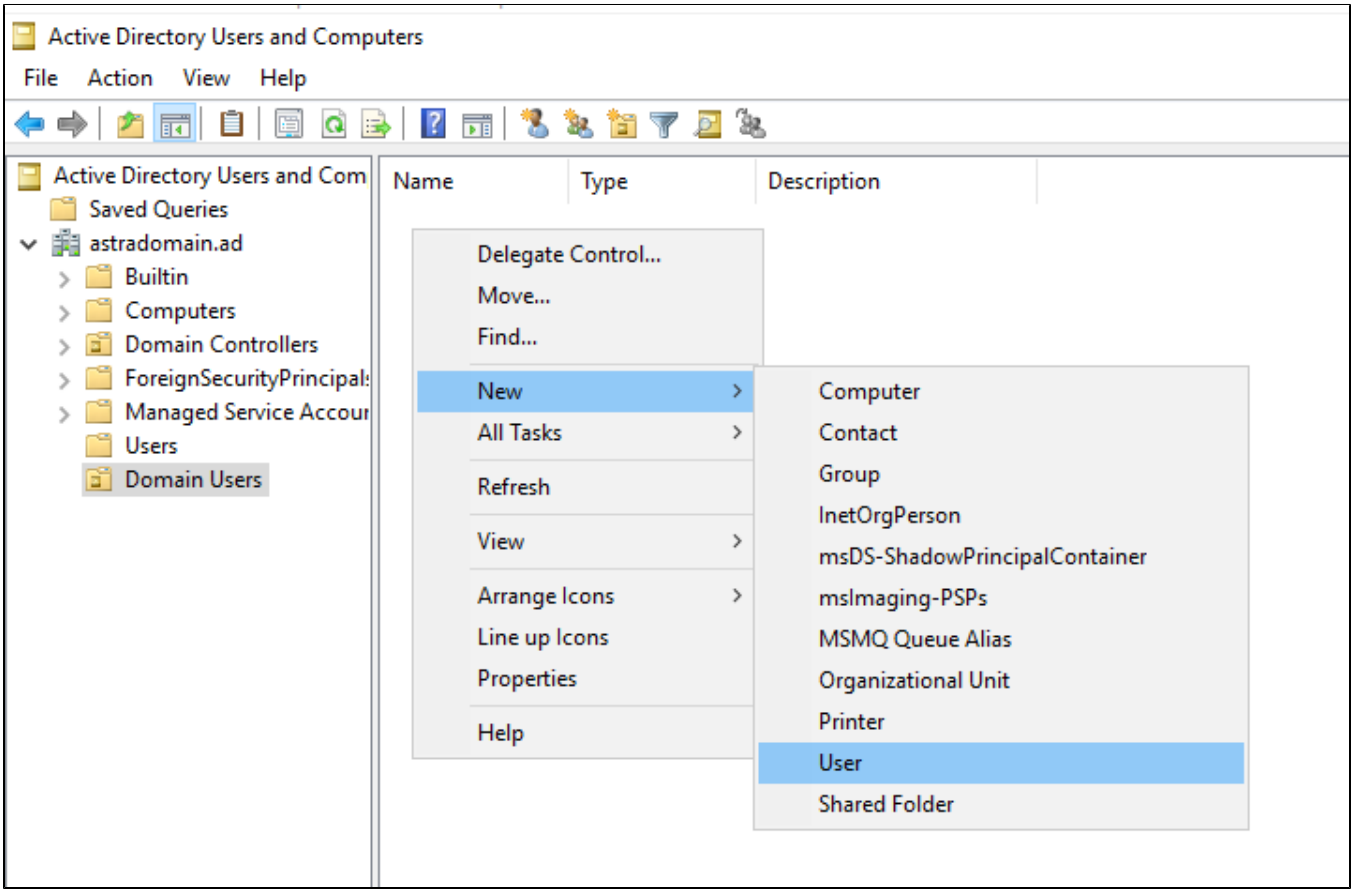


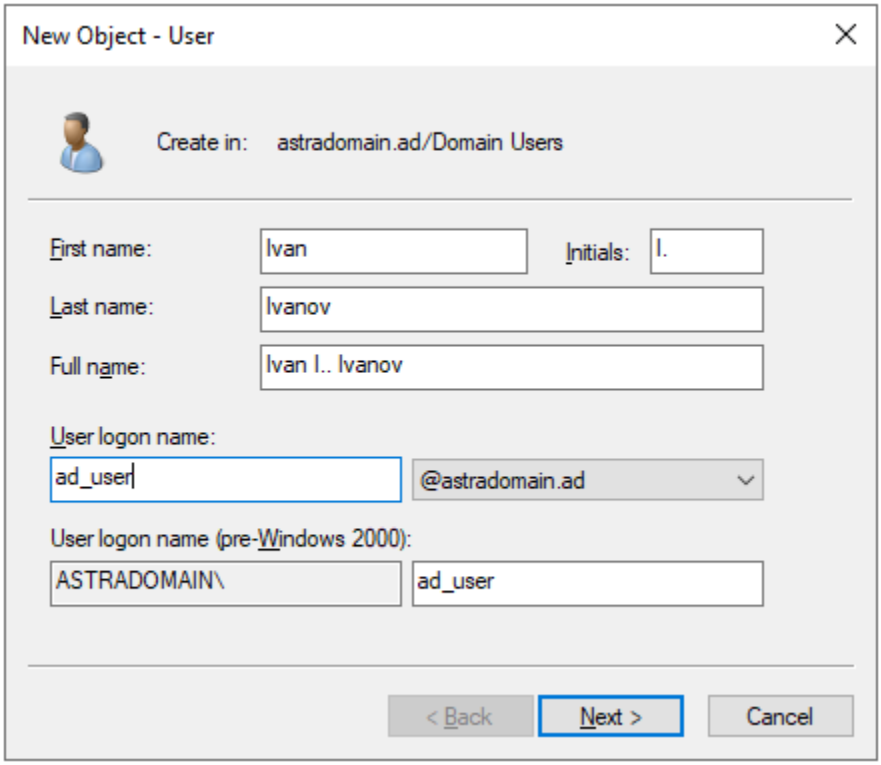
2. Для удобства создайте отдельную директорию Domain Users, в которой будете создавать доменных пользователей:

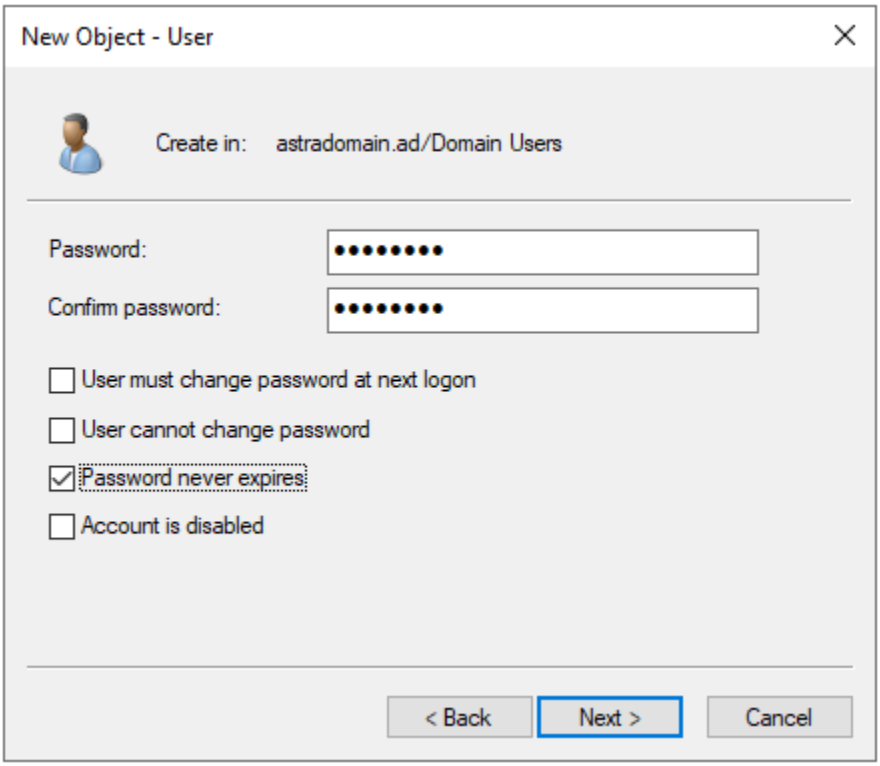

Active Directory Users and Computers
File
Action
View
Help
Active Directory Users and Com
Saved Queries
astradomain.ad
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipal
Managed Service Accour
Users
Name
Type
Description
Builtin
builtinDomain
Computers
Container
Default container for up...
Domain Con...
Organizational...
Default container for do...
ForeignSecu...
Container
Default container for sec...
Managed Se...
Container
Default container for ma...
Users
Container
Default container for up...
Delegate Control...
Find...
Change Domain...
Change Domain Controller...
Raise domain functional level...
Operations Masters...
New
All Tasks
Refresh
Export List...
View
Arrange Icons
Line up Icons
Properties
Help
Computer
Contact
Group
InetOrgPerson
msDS-ShadowPrincipalContainer
mslmaging-PSPs
MSMQ Queue Alias
Organizational Unit
Printer
User
Shared Folder

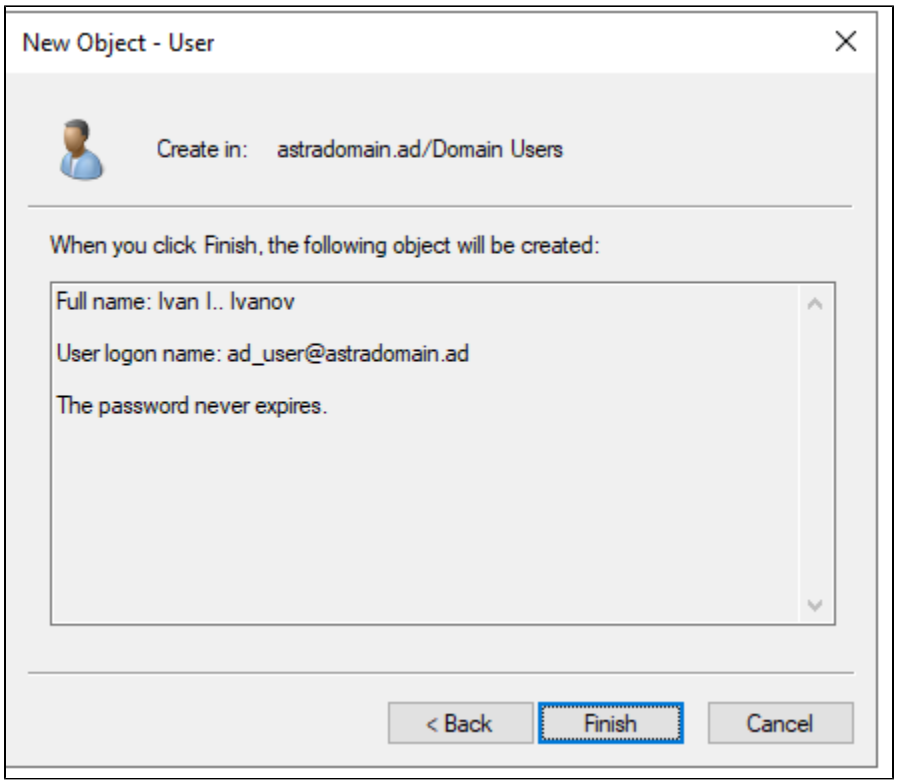


3. Добавьте нового пользователя User:




New Object - User
Create in: astradomain.ad/Domain Users
First name:
Ivan
Initials:
I.
Last name:
Ivanov
Full name:
Ivan I.. Ivanov
User logon name:
ad_user
@astradomain.ad
User logon name (pre-Windows 2000):
ASTRADOMAIN\
ad_user
< Back
Next >
Cancel


New Object - User
Create in: astradomain.ad/Domain Users
Password:
Confirm password:
User must change password at next logon
User cannot change password
Password never expires
Account is disabled
< Back
Next >
Cancel



4. Аналогичным образом добавьте остальных пользователей, которые должны быть в домене.

Шаг 4. Установка центра сертификации Active Directory

Перед процедурой установите драйверы для работы с Рутокеном на сервер, ссылка на актуальную версию: https://www.rutoken.ru/support/download/windows/

После этого можно приступить к настройке центра сертификации и выдаче сертификатов для пользователей. Это можно сделать по данной инструкции.

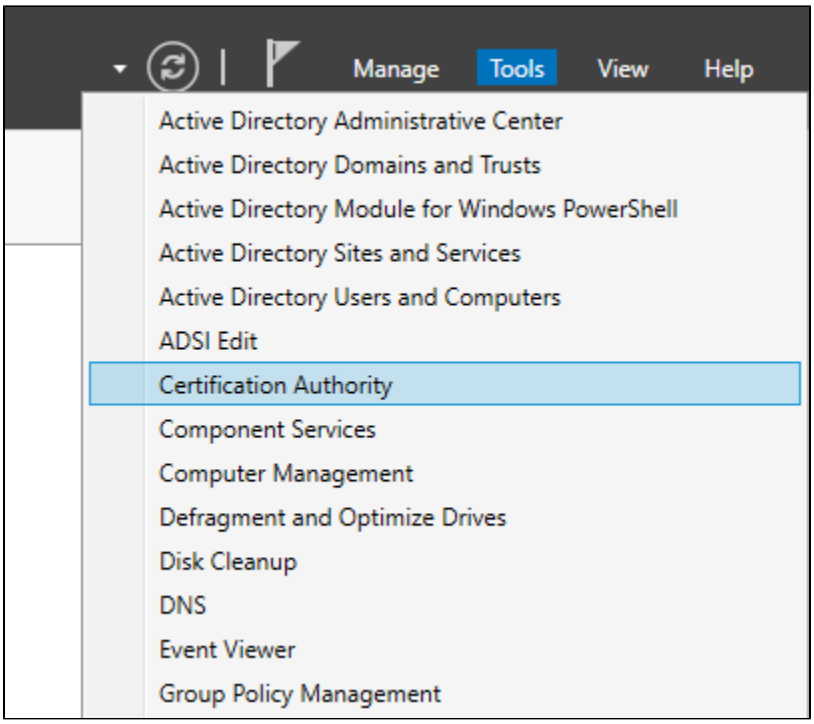
Настройку авторизации с помощью сертификатов можно реализовать по этой инструкции.

Для аутентификации пользователя через linux машины необходимы:

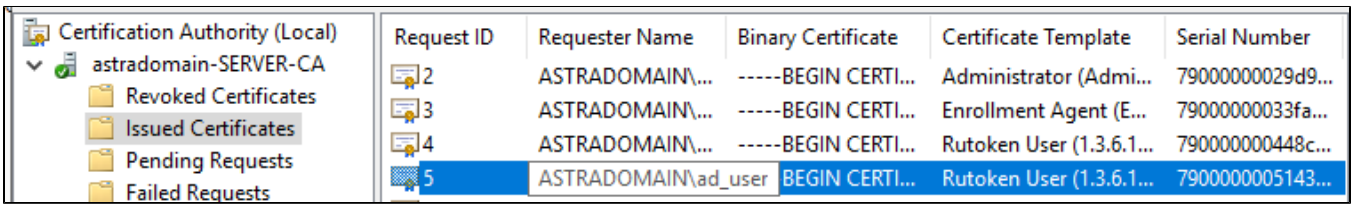
- токен с ключами и сертификатов;
- корневой сертификат УЦ (его необходимо отправить пользователям).

Чтобы получить корневой центр УЦ:

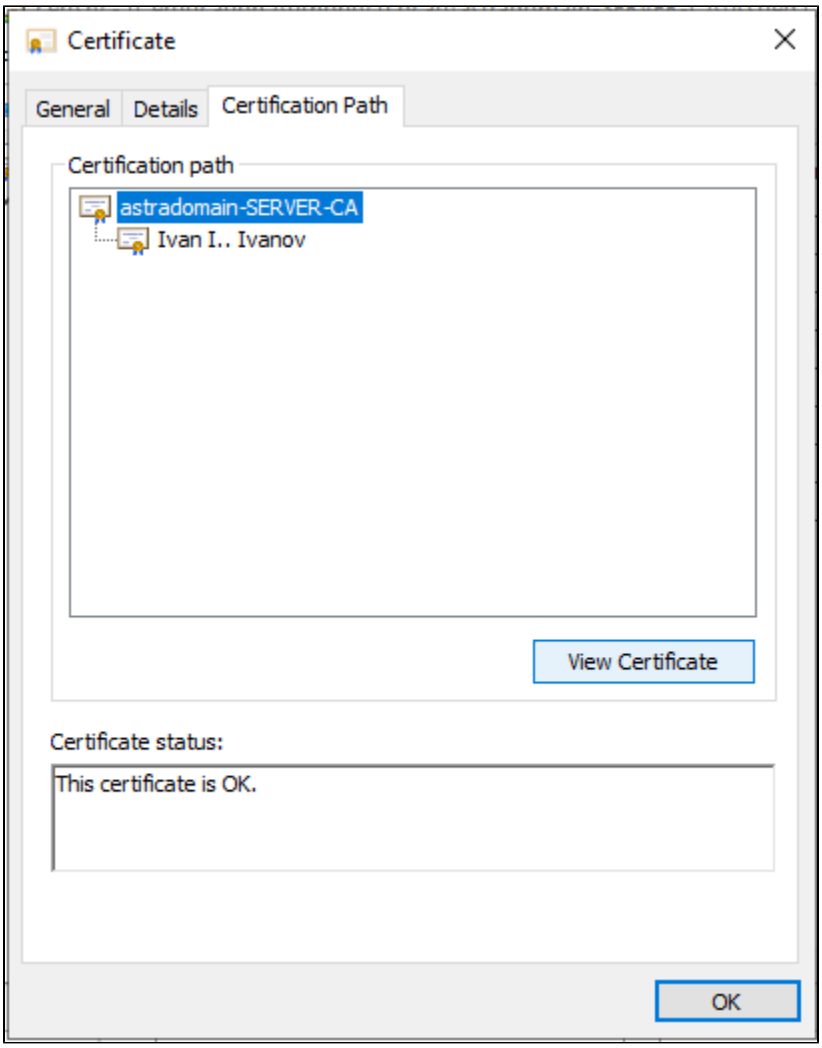
1. Выберите пункт меню **Tools** и подпункт **Certification Authority**.



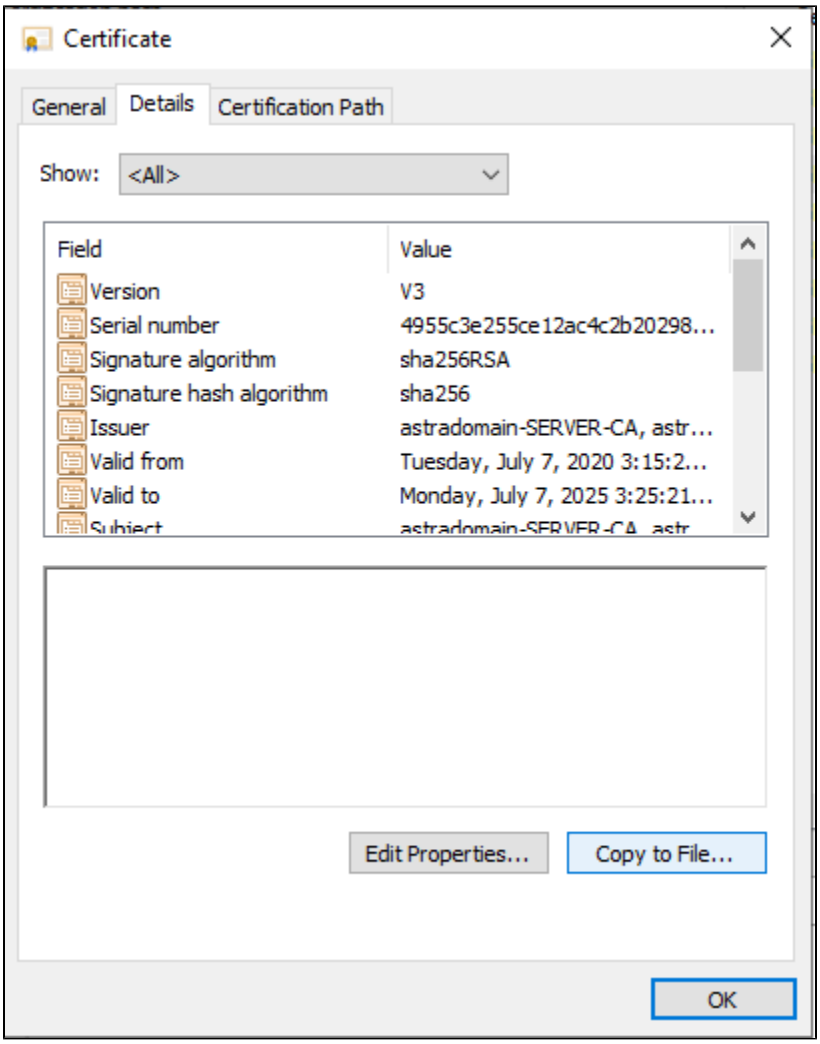
2. Два раза щёлкните по строке с сертификатом.



3. В окне сертификата на вкладке **Certification Path** щёлкните по имени сертификата и нажмите **View Certificate**.



4. Нажмите **Copy to File** и сохраните сертификат в формате BASE64.



Настройка клиента РЕД ОС

Добавление пользователя в sudo

Отредактируйте файл /etc/sudoers

```
su

sudo nano /etc/sudoers
```

И добавьте в него строчку user ALL=(ALL) ALL

Далее залогиньтесь под пользователем и продолжите работу из-под него.

```
su user
```

Далее установите следующие пакеты:

```
sudo dnf update

sudo dnf upgrade

sudo dnf install ccid opensc pam_pkcs11 gdm-plugin-smartcard p11-kit join-to-domain

sudo dnf install -y realmd PackageKit

sudo dnf install -y krb5-workstation

sudo dnf install -y nss-tools opensc krb5-pkinit
```

Загрузите модуль librtpkcs11ecp.so и установите:

```
sudo rpm -i librtpkcs11ecp-X.X.X.X-X.x86_64.rpm
```

Настройка DNS

Через консоль

Измените имя клиента в нашем домене astradomain.ad на client

```
sudo hostnamectl set-hostname client.astradomain.ad
```

Узнайте название вашего соединения. Они могут отличаться.

```
CON_NAME="enp0s3"
```

Название интерфейса, которое использует ваше соединение.

```
INT_NAME="Ethernet"
```

Адрес dns сервера

```
DNS_SERVER_IP=10.0.2.15
```

Отключите соединение

```
sudo nmcli con down "$CON_NAME"
```

Настройте сетевую карту соединения — по умолчанию $INT_NAME

```
sudo nmcli con mod "$CON_NAME" connection.interface-name $INT_NAME
```

Настройте DNS — вместо DNS_SERVER_IP указать IP-адрес сервера DNS. При необходимости укажите адрес локального сервера DNS.

```
sudo nmcli con mod "$CON_NAME" ipv4.dns "$DNS_SERVER_IP 10.0.2.15"

sudo nmcli con mod "$CON_NAME" ipv4.ignore-auto-dns yes
```

Включите сетевое соединение

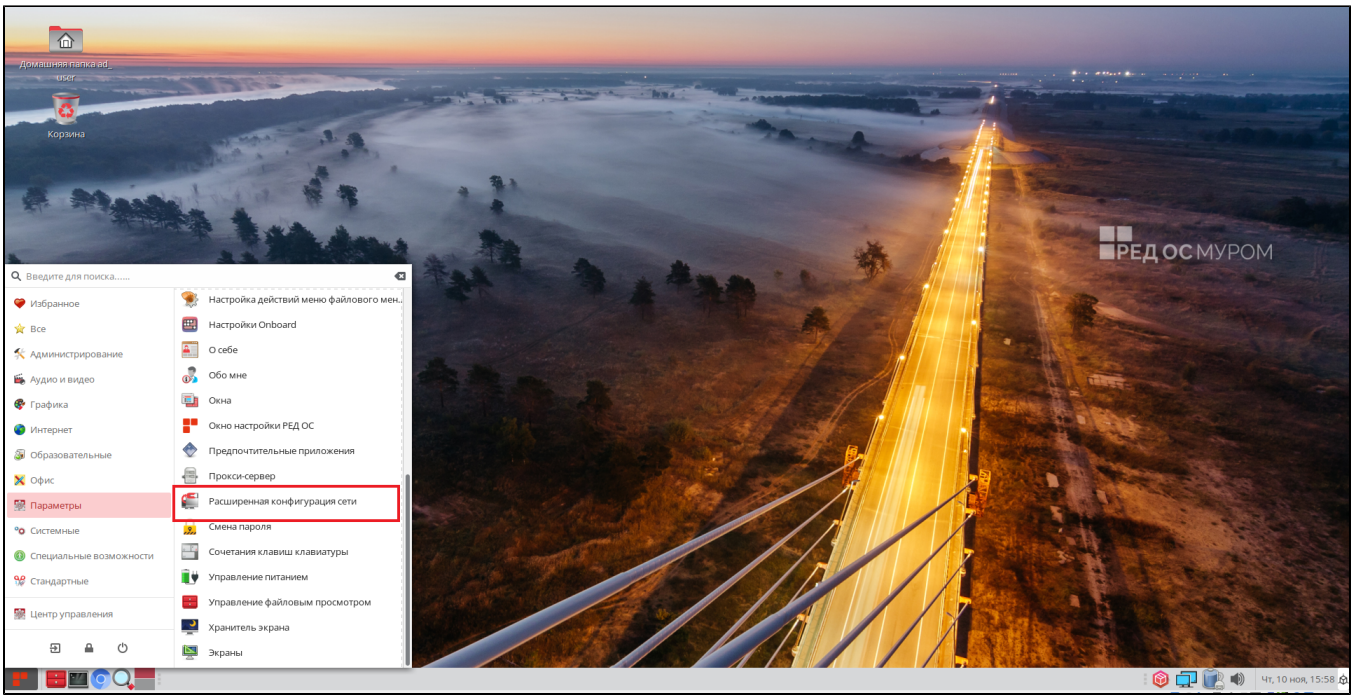
```
sudo nmcli con up "$CON_NAME"
```

Вводите компьютер в домен

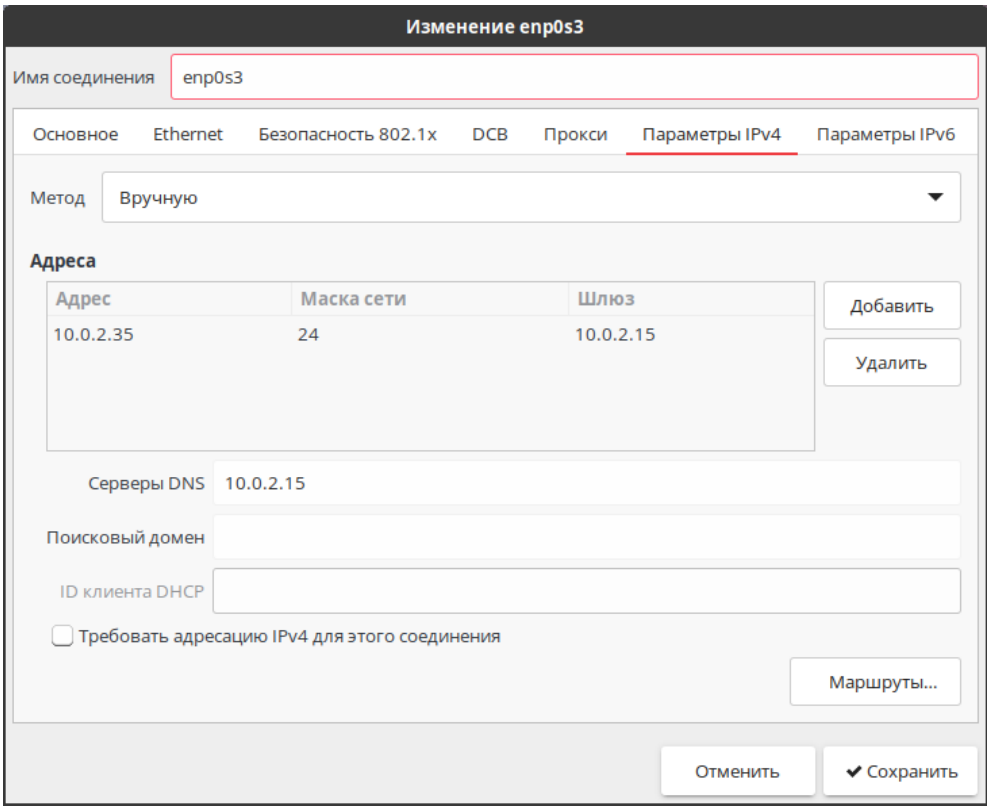
```
sudo join-to-domain.sh
```

Через графический интерфейс

Откройте **Главное меню** — **Параметры** — **Расширенная конфигурация сети**.

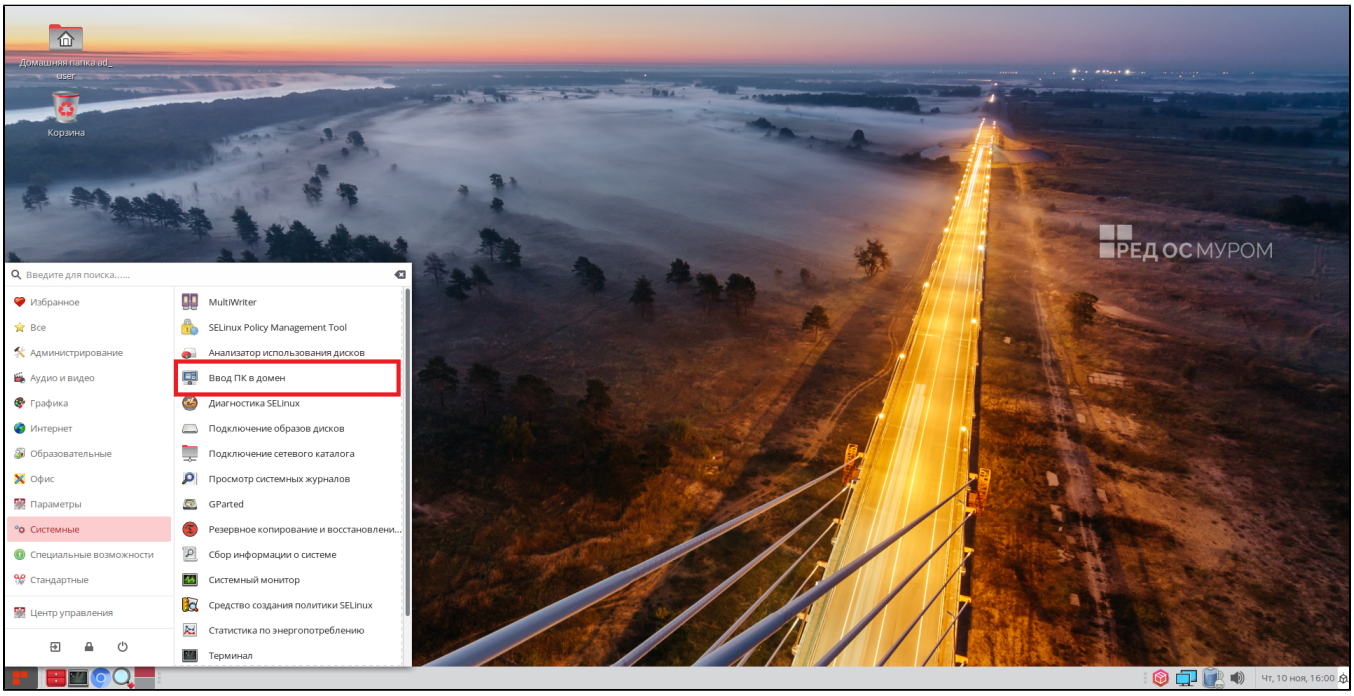


Выберите своё соединение, и на вкладке **Параметры IPv4** введите IP клиента (так как на сервере не установлен DHSP) и DNS.

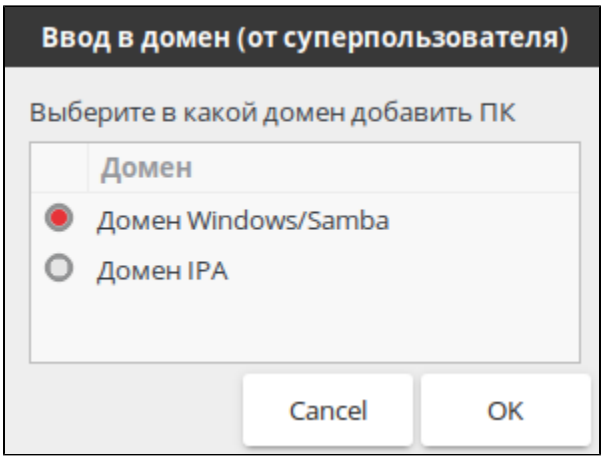


Обязательно перезагрузите компьютер.

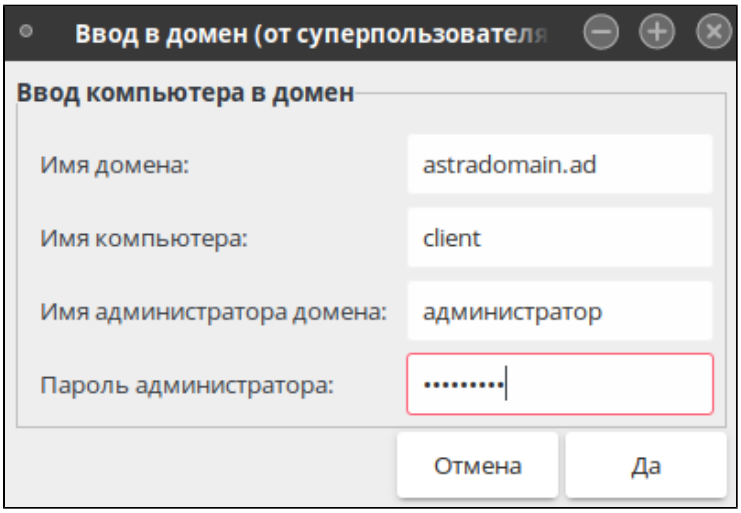
После перезагрузки, откройте **Главное меню** — **Системные** — **Ввод ПК в домен**.



Выберите параметр «**Домен Windows/Samba**»



Далее необходимо ввести параметры для ввода компьютера в домен.



Обязательно перезагрузите компьютер.

Узнаем какие пакеты ещё необходимы для подключения к домену

```
realm discover astradomain.ad
```

Список необходимых для работы пакетов будет выведен в следующем формате:

```
required-package: pkg1
required-package: pkg2
required-package: pkg3
```

Установите отсутствующие пакеты:

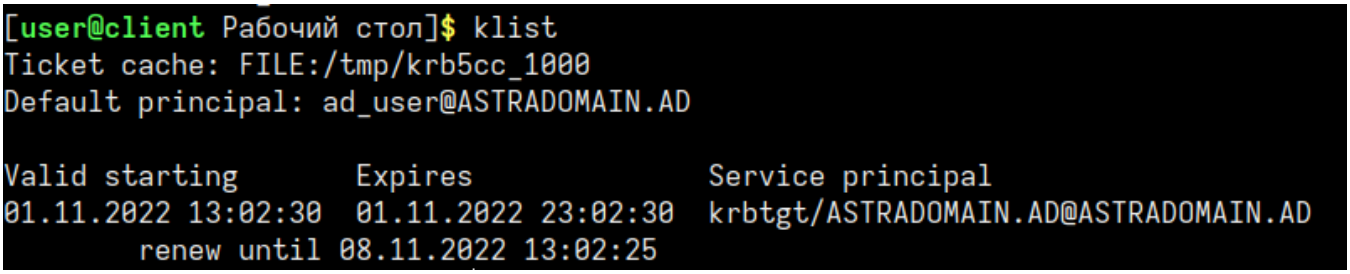
```
sudo dnf install -y pkg1 pkg2 pkg3 ...
```

Если в домене есть пользователь ad_user, к которому можно подключиться с помощью пароля, то можно осуществить проверку настройки получив тикет для него

```
kinit ad_user@ASTRADOMAIN.AD
```

Проверка получения тикета осуществляется командой

```
klist
```



Удаление тикета

```
kdestroy
```

Проверка аутентификации под пользователем в домене без Рутокена

```
su ad_user@astradomain.ad
```

Залогиньтесь локальным пользователем для дальнейшей настройки:

```
su user
```

Настройка клиента для аутентификации в домене с помощью Рутокена

При необходимости удалите старую базу и создайте новую:

```
sudo rm -fr /etc/pki/nssdb

sudo mkdir /etc/pam_pkcs11/nssdb

sudo chmod 777 /etc/pam_pkcs11/nssdb

sudo certutil -N -d /etc/pam_pkcs11/nssdb --empty-password

sudo modutil -dbdir /etc/pam_pkcs11/nssdb -add "Rutoken PKCS11" -libfile /usr/lib64/librtpkcs11ecp.so
```

Установите корневой сертификат в /etc/pki/ca-trust/source/anchors/.

Следующая команда используется из директории, в которой находится корневой сертификат:

```
sudo cp ca_cert.cer /etc/pki/ca-trust/source/anchors/

sudo update-ca-trust force-enable

sudo update-ca-trust extract

sudo certutil -d /etc/pam_pkcs11/nssdb -A -n 'AD-ROOT' -t CT,CT,CT -a -i /etc/pki/ca-trust/source/anchors
/ca_cert.cer
```

Проверьте, что сертификат виден на токене и в базе данных. Система должна запросить PIN-код Рутокена и выдать сертификат с карточки с правами u,u,u и корневого сервера.

```
sudo certutil -L -d /etc/pam_pkcs11/nssdb -h all

Certificate Nickname Trust Attributes
SSL,S/MIME,JAR/XPI

Enter Password or Pin for "Rutoken ECP <no label>":
AD-ROOT CT,C,C
Rutoken ECP <no label>:te-Rutoken-0329dc84-5937-4b1e-adaf-5cbfe977cda0_E u,u,u
```

Добавьте модуль Рутокен к p11-kit

```
sudo nano /usr/share/p11-kit/modules/Rutoken.module
```

Добавить в файл следующий текст:

```
module:/usr/lib64/librtpkcs11ecp.so
```

Сделайте модуль Рутокен по умолчанию для p11-tools

```
sudo modutil -default "Rutoken PKCS11" -dbdir /etc/pam_pkcs11/nssdb -mechanisms RSA:DSA:RC4:DES
```

Отредактируйте pam_pkcs11

```
sudo nano /etc/pam_pkcs11/pam_pkcs11.conf
```

```
pam_pkcs11 {
  nullok = false;
  debug = true;
  use_first_pass = false;
  use_authtok = false;
  card_only = false;
  wait_for_card = false;
  use_pkcs11_module = rutokenecp;

  # Aktiv Rutoken ECP
  pkcs11_module rutokenecp {
    module = /usr/lib64/librtpkcs11ecp.so;
    slot_num = 0;
    support_thread = true;
    ca_dir = /etc/pam_pkcs11/cacerts;
    crl_dir = /etc/pam_pkcs11/crls;
    cert_policy = signature;
  }

  use_mappers = ms;

  mapper_search_path = /usr/lib64/pam_pkcs11;

  mapper ms {
  debug = false;
  module = internal;
  ignorecase = true;
  ignoredomain = true;
  domain = "ASTRADOMAIN.AD";
 }
}
```

Настройте PAM стандартным средством RHEL authselect.

```
sudo authselect select sssd with-smartcard with-mkhomedir --force
```

Общий вид /etc/pam.d/system-auth:

```
sudo nano /etc/pam.d/system-auth
```

```
auth        required                                    pam_env.so
auth        required                                    pam_faildelay.so delay=2000000
auth        [default=1 ignore=ignore success=ok]        pam_usertype.so isregular
auth        [default=2 ignore=ignore success=ok]        pam_localuser.so
auth        [success=done authinfo_unavail=ignore ignore=ignore default=die] pam_sss.so try_cert_auth
auth        sufficient                                  pam_unix.so nullok try_first_pass
auth        [default=1 ignore=ignore success=ok]        pam_usertype.so isregular
auth        sufficient                                  pam_sss.so forward_pass
auth        required                                    pam_deny.so

account     required                                    pam_unix.so
account     sufficient                                  pam_localuser.so
account     sufficient                                  pam_usertype.so issystem
account     [default=bad success=ok user_unknown=ignore] pam_sss.so
account     required                                    pam_permit.so

password    requisite                                   pam_pwquality.so try_first_pass local_users_only
password    sufficient                                  pam_unix.so sha512 shadow nullok try_first_pass
use_authtok
password    sufficient                                  pam_sss.so use_authtok
password    required                                    pam_deny.so

session     optional                                    pam_keyinit.so revoke
session     required                                    pam_limits.so
-session    optional                                    pam_systemd.so
session     optional                                    pam_oddjob_mkhomedir.so umask=0077
session     [success=1 default=ignore]                  pam_succeed_if.so service in crond quiet use_uid
session     required                                    pam_unix.so
session     optional                                    pam_sss.so
```

Общий вид /etc/pam.d/password-auth:

```
sudo nano /etc/pam.d/password-auth
```

```
auth        required                                    pam_env.so
auth        required                                    pam_faildelay.so delay=2000000
auth        [default=1 ignore=ignore success=ok]        pam_usertype.so isregular
auth        [default=1 ignore=ignore success=ok]        pam_localuser.so
auth        [success=done authinfo_unavail=ignore ignore=ignore default=die] pam_sss.so try_cert_auth
auth        sufficient                                  pam_unix.so nullok try_first_pass
auth        [default=1 ignore=ignore success=ok]        pam_usertype.so isregular
auth        sufficient                                  pam_sss.so forward_pass
auth        required                                    pam_deny.so

account     required                                    pam_unix.so
account     sufficient                                  pam_localuser.so
account     sufficient                                  pam_usertype.so issystem
account     [default=bad success=ok user_unknown=ignore] pam_sss.so
account     required                                    pam_permit.so

password    requisite                                   pam_pwquality.so try_first_pass local_users_only
password    sufficient                                  pam_unix.so sha512 shadow nullok try_first_pass
use_authtok
password    sufficient                                  pam_sss.so use_authtok
password    required                                    pam_deny.so

session     optional                                    pam_keyinit.so revoke
session     required                                    pam_limits.so
-session    optional                                    pam_systemd.so
session     optional                                    pam_oddjob_mkhomedir.so umask=0077
session     [success=1 default=ignore]                  pam_succeed_if.so service in crond quiet use_uid
session     required                                    pam_unix.so
session     optional                                    pam_sss.so
```

Настройте SSSD

Для того, чтобы аутентификация корректно работала на лок скрине. В настройках sssd нужно указать название сервиса, использующегося при аутентификации через лок скрин, чтобы сделать его доверенным. У каждой графической оболочки свое название данного сервиса. Узнать название вашей графической оболочки можно с помощью команды:

Название графической оболочки

```
echo $XDG_CURRENT_DESKTOP
```

Вот список соответствий названий графических оболочек и сервиса, используемого лок скрином. Данный список не является полным.

MATE → mate-screensaver
X-Cinnamon → cinnamon-screensaver
fly → <Отсутствует>
KDE → kde
GNOME → xdg-screensaver

Сконфигурируем SSSD. Для этого отредактируем файл **/etc/sssd/sssd.conf**.

```
sudo nano /etc/sssd/sssd.conf
```

Общий вид /etc/sssd/sssd.conf:

```
[sssd]
domains = astradomain.ad
config_file_version = 2
services = nss, pam

[domain/astradomain.ad]
ad_domain = astradomain.ad
ad_server = WIN-HAFG0T1O90S.astradomain.ad
krb5_realm = ASTRADOMAIN.AD
case_sensitive = Preserving
realmd_tags = manages-system joined-with-samba

#   ,
cache_credentials = True

id_provider = ad
access_provider = ad
krb5_store_password_if_offline = True
default_shell = /bin/bash
ldap_id_mapping = True
ad_gpo_access_control = disabled

# /
use_fully_qualified_names = False

#
fallback_homedir = /home/%u@%d

#  access_provider = simple         .
#access_provider = simple
#simple_allow_users = user1@example.com, user2@example.com
#simple_allow_groups = group@example.com

# /    , (id  getent)      enumerate = true
enumerate = false

#  ignore_group_members           ,    OU
#    TRUE,          ldap      .
# ignore_group_members = True

#         ,    .
# true -     .   .
#ldap_referrals = false

# /   DNS,    sssd  "TSIG error with server: tsig verify failure",   dyndns_update = false
#dyndns_update = true
#dyndns_refresh_interval = 43200
#dyndns_update_ptr = true
#dyndns_ttl = 3600

#[nss]
#   nss_sss    (    ) Default: 120
#entry_cache_timeout = 15
#    ,        . Default: 60
#get_domains_timeout = 10

[pam]
pam_cert_auth = True
debug_level = 10
pam_cert_db_path = /etc/pki/ca-trust/source/anchors/ca_cert.cer
pam_p11_allowed_services = +mate-screensaver

[certmap/files/ms]
matchrule = <SAN:ntPrincipalName>.*@domain
maprule =({subject_nt_principal.short_name})
```

Измените конфиг Kerberos

```
sudo nano /etc/krb5.conf
```

Общий вид файла:

```
includedir /etc/krb5.conf.d/


[logging]

    default = FILE:/var/log/krb5libs.log

    kdc = FILE:/var/log/krb5kdc.log

    admin_server = FILE:/var/log/kadmind.log


[libdefaults]

#    dns_lookup_realm = false  #   kerberos-   DNS

    dns_lookup_kdc = true #   kerberos-   DNS

    ticket_lifetime = 24h

    renew_lifetime = 7d

    forwardable = true

    rdns = false

#    spake_preauth_groups = edwards25519

    default_ccache_name = FILE:/tmp/krb5cc_%{uid}

    default_realm = ASTRADOMAIN.AD

    pkinit_kdc_hostname = WIN-HAFG0T1O90S.ASTRADOMAIN.AD

    pkinit_anchors = DIR:/etc/pki/ca-trust/source/anchors/

    pkinit_identities = PKCS11:librtpkcs11ecp.so

    pkinit_eku_checking = none

    canonicalize = True

default_tgs_enctypes = aes256-cts-hmac-sha1-96 aes128-cts-hmac-sha1-96 RC4-HMAC DES-CBC-CRC DES3-CBC-SHA1 DES-
CBC-MD5
default_tkt_enctypes = aes256-cts-hmac-sha1-96 aes128-cts-hmac-sha1-96 RC4-HMAC DES-CBC-CRC DES3-CBC-SHA1 DES-
CBC-MD5
preferred_enctypes = aes256-cts-hmac-sha1-96 aes128-cts-hmac-sha1-96 RC4-HMAC DES-CBC-CRC DES3-CBC-SHA1 DES-CBC-
MD5

[realms]

ASTRADOMAIN.AD = {

    kdc = WIN-HAFG0T1O90S.astradomain.ad # Primary Domain Controller


    admin_server = WIN-HAFG0T1O90S.astradomain.ad # Primary Domain Controller

    default_domain = astradomain.ad # Domain name

}
```

```
[domain_realm]

.astradomain.ad = ASTRADOMAIN.AD

astradomain.ad = ASTRADOMAIN.AD


[appdefaults]

        pam = {

                debug = true

        }
```

Обязательно перезагрузите компьютер.

Проверьте аутентификацию после перезагрузки.