# Настройка 2ФА на рабочих станциях Linux 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:**

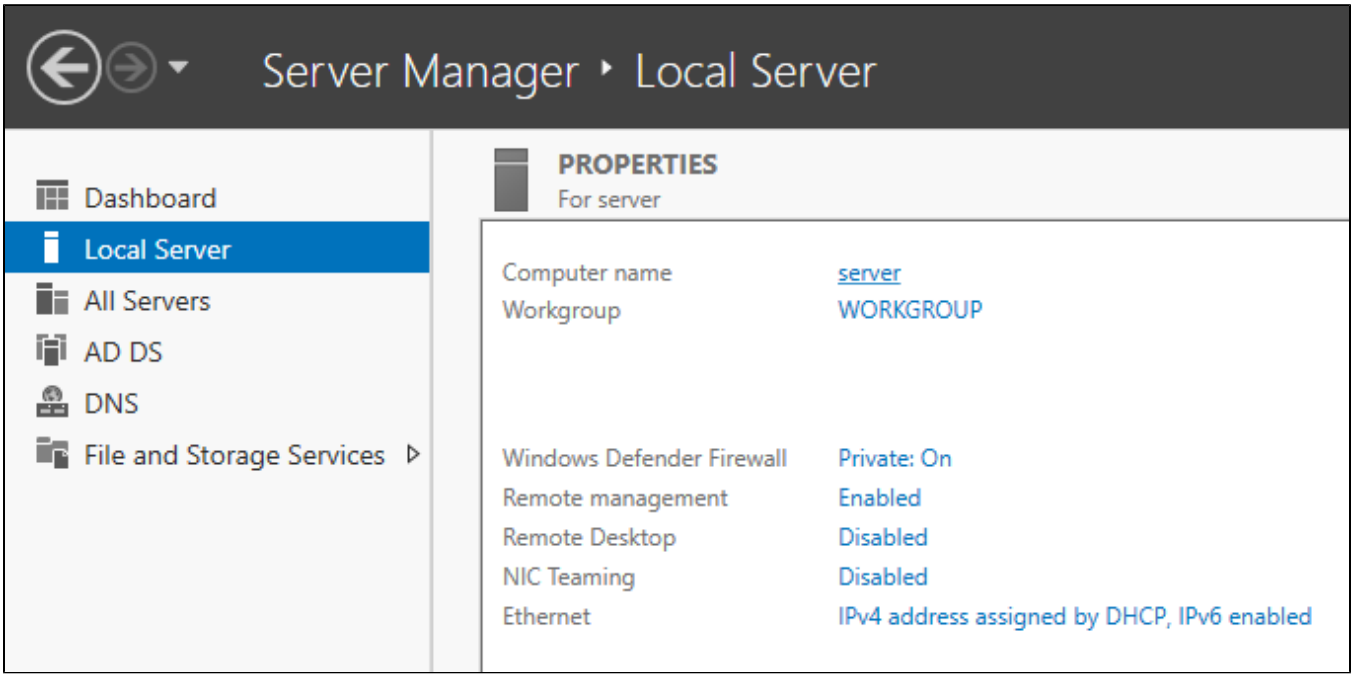
ОС: РЕД ОС \ Астра Линукс \ ALT Linux \ Ubuntu

доменное имя: redos.astradomain.ad \ smolensk.astradomain.ad \ orel.astradomain.ad \ ubuntu.astradomain.ad

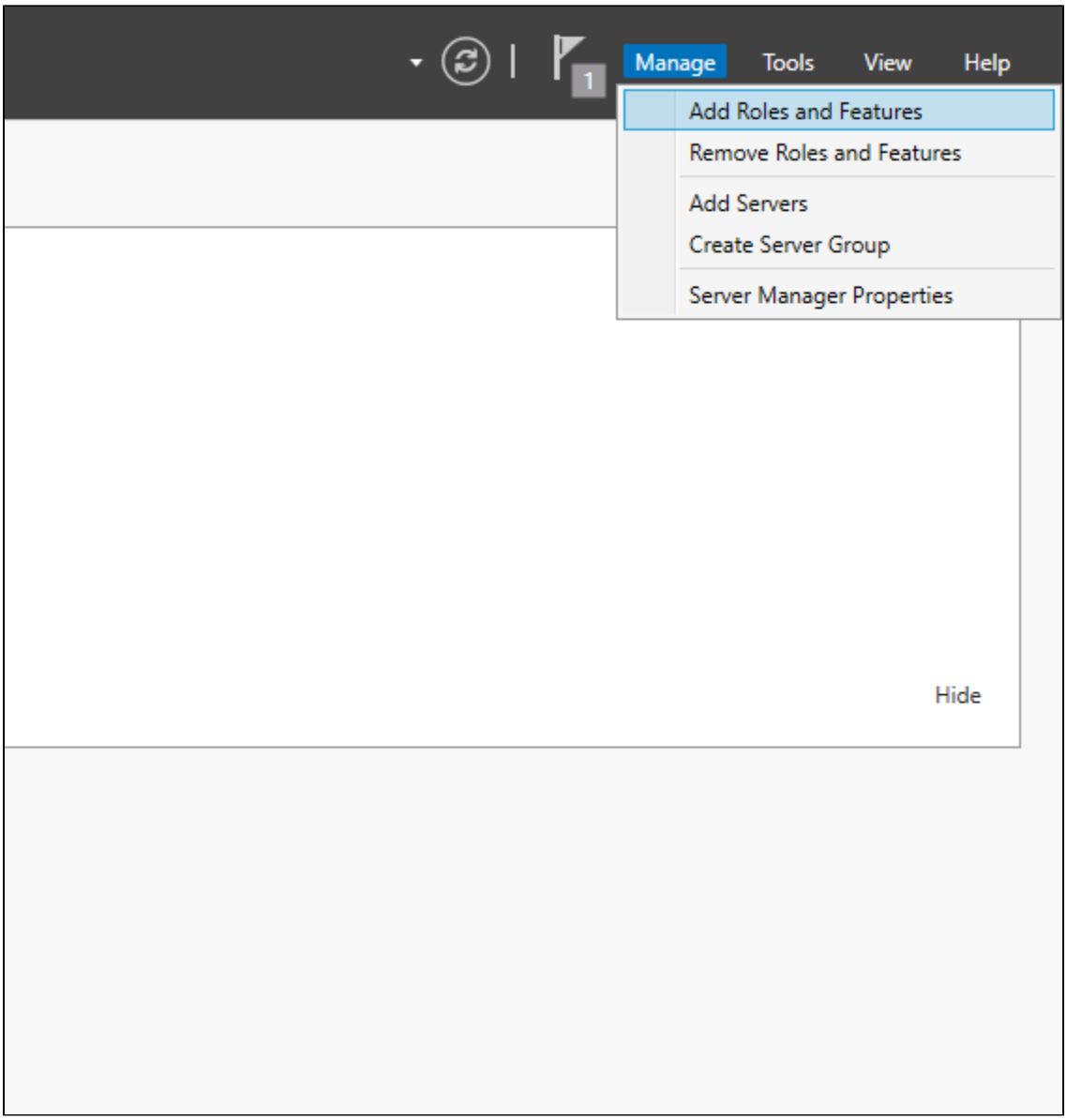
## Настройка сервера

### Установка сервиса Active Directory

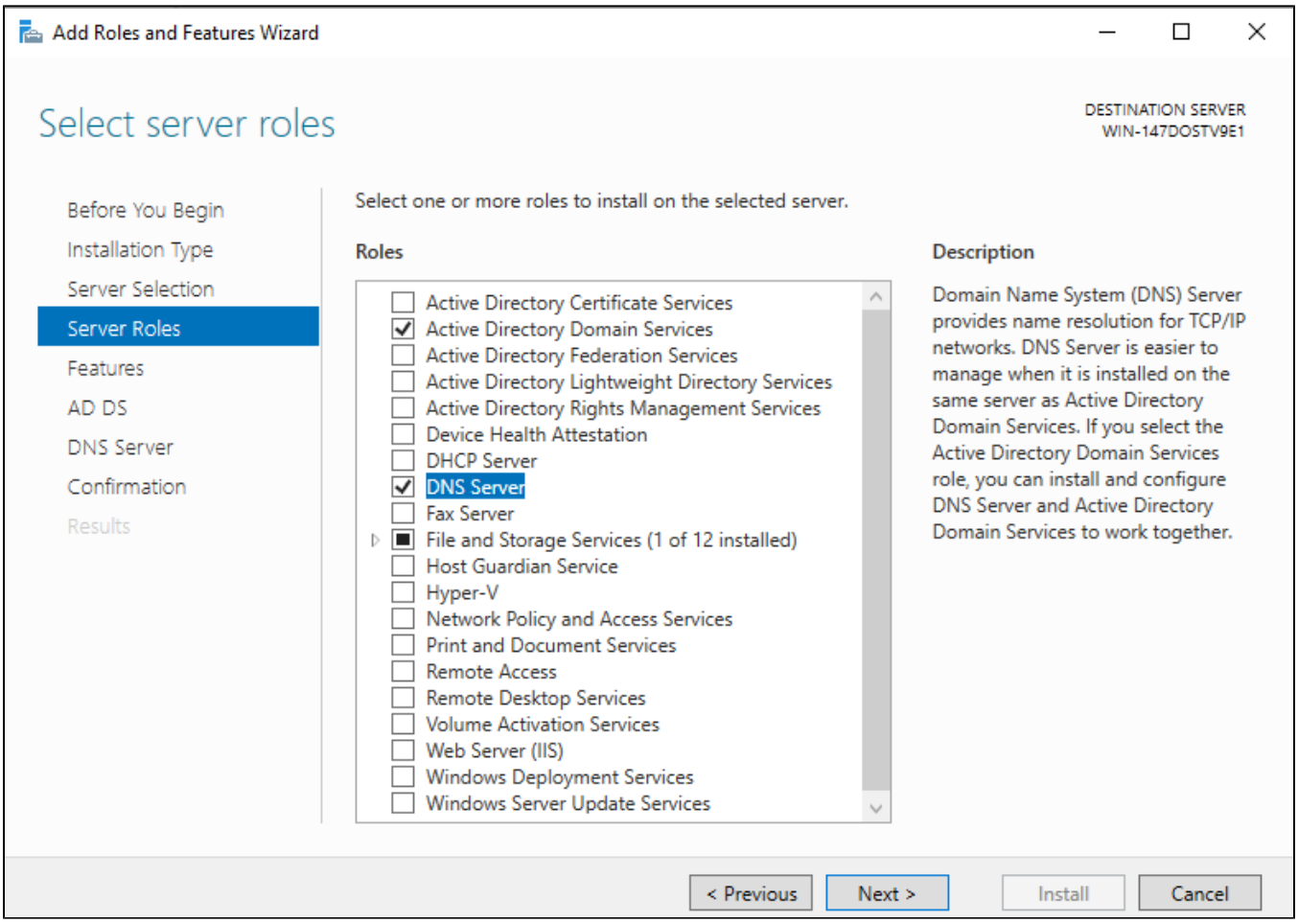
Измените имя сервера, если это необходимо. Его можно задать в окне менеджера сервера:




Добавим службу Active Dirrectory и DNS на сервер. Для этого откроем окно добавления ролей в менеджере сервера:

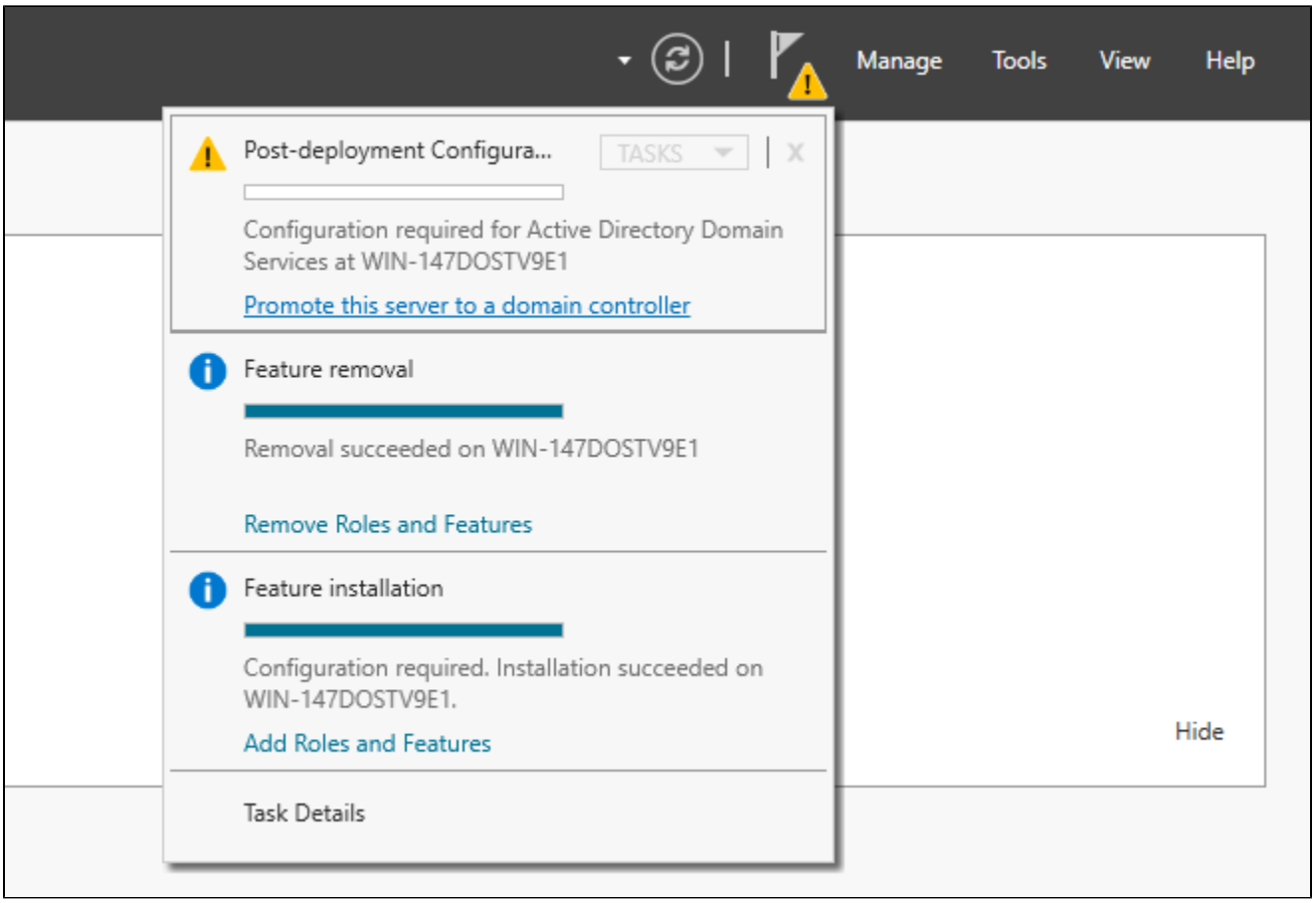



В окне для выбора сервисов установим галочки "Active Directory Domain Services" и "DNS Server":

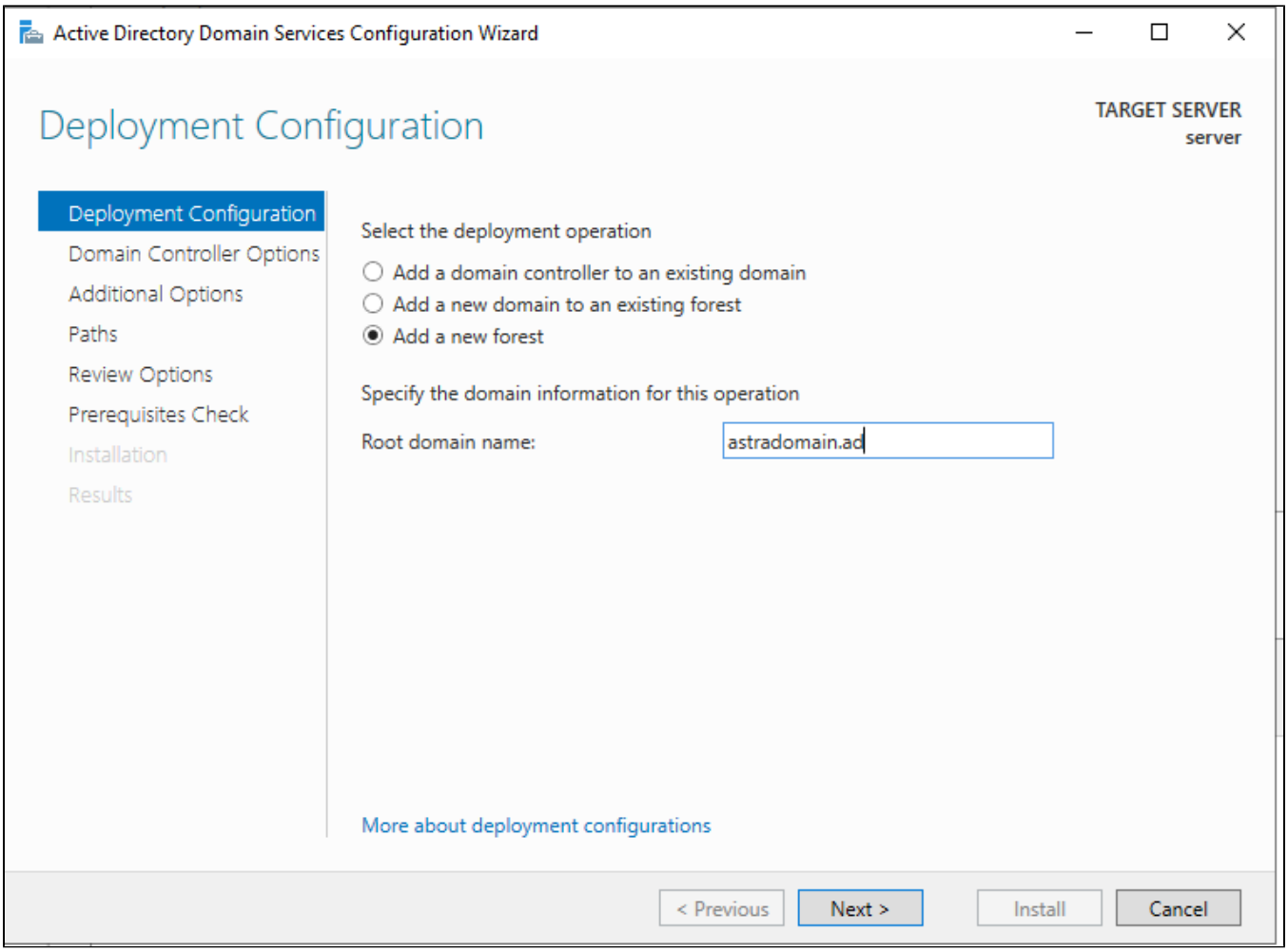



Во всех остальных пунктах даем согласие на установку.

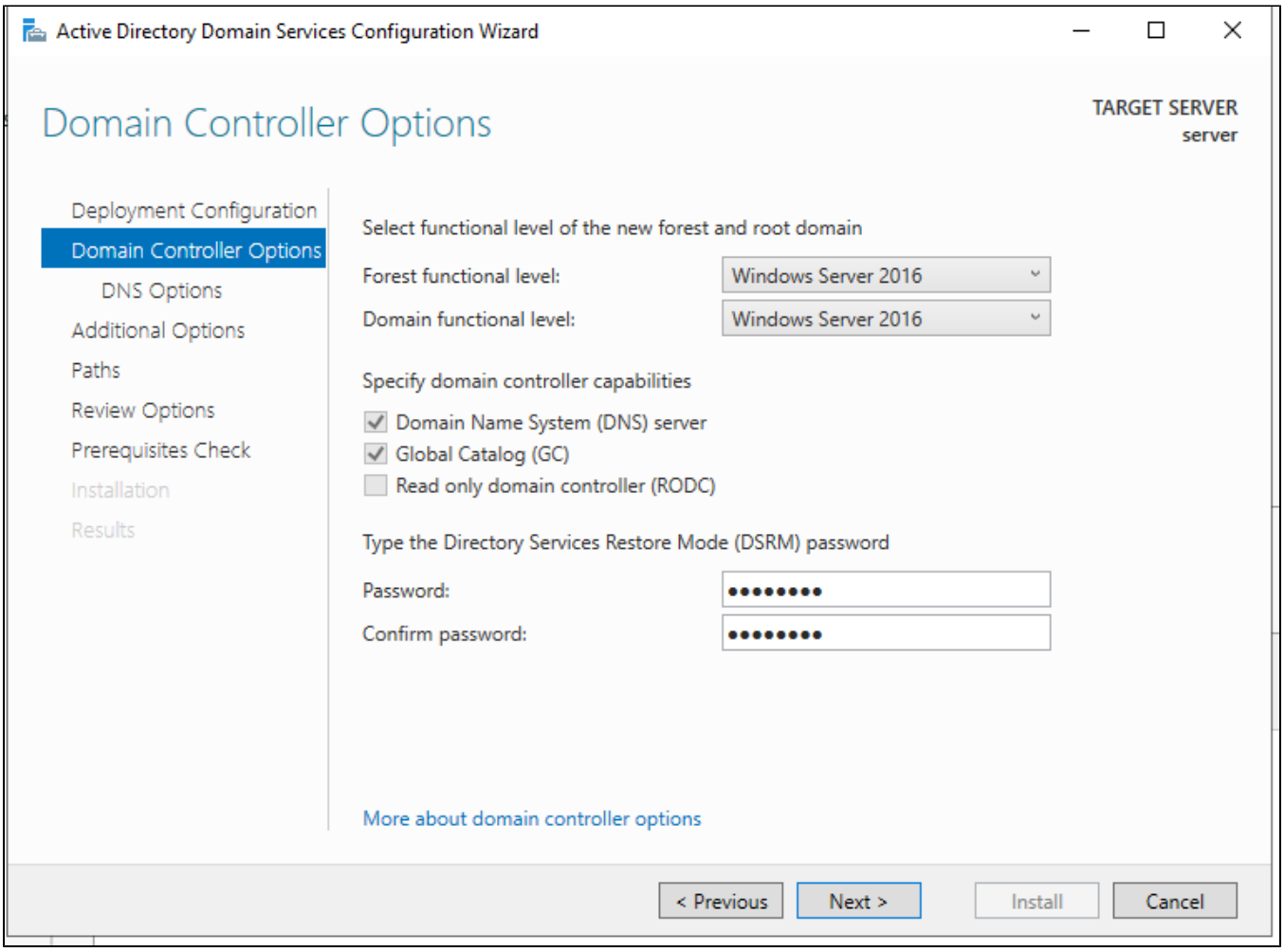
После завершения установки сервисов вам надо перейти к настройке домена. Для этого откройте меню уведомлений и выберите пункт "Promote this server to a domain controller":



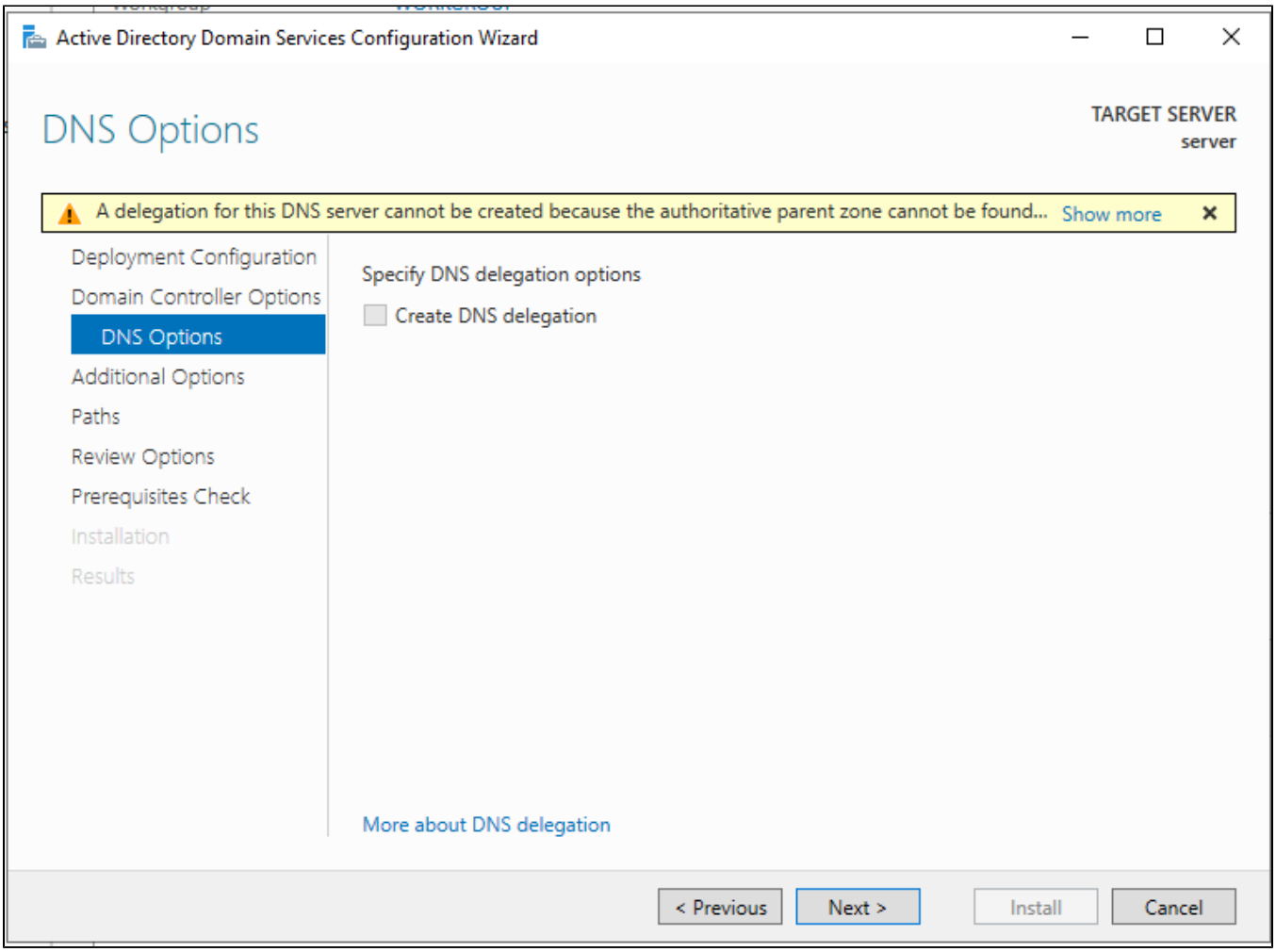

На первой вкладке укажите опцию для создания нового домена и укажите его название:



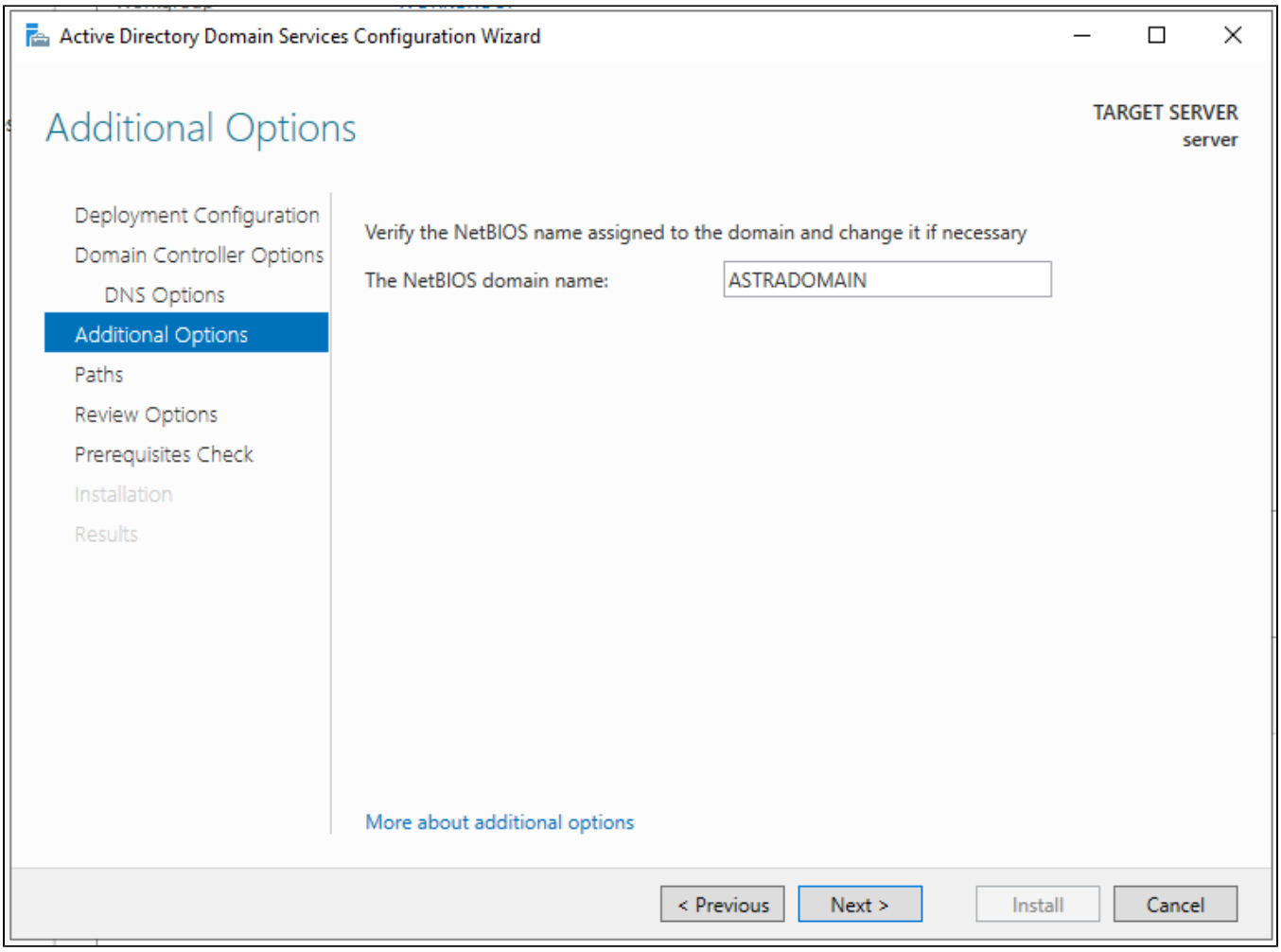

Введите пароль сброса:

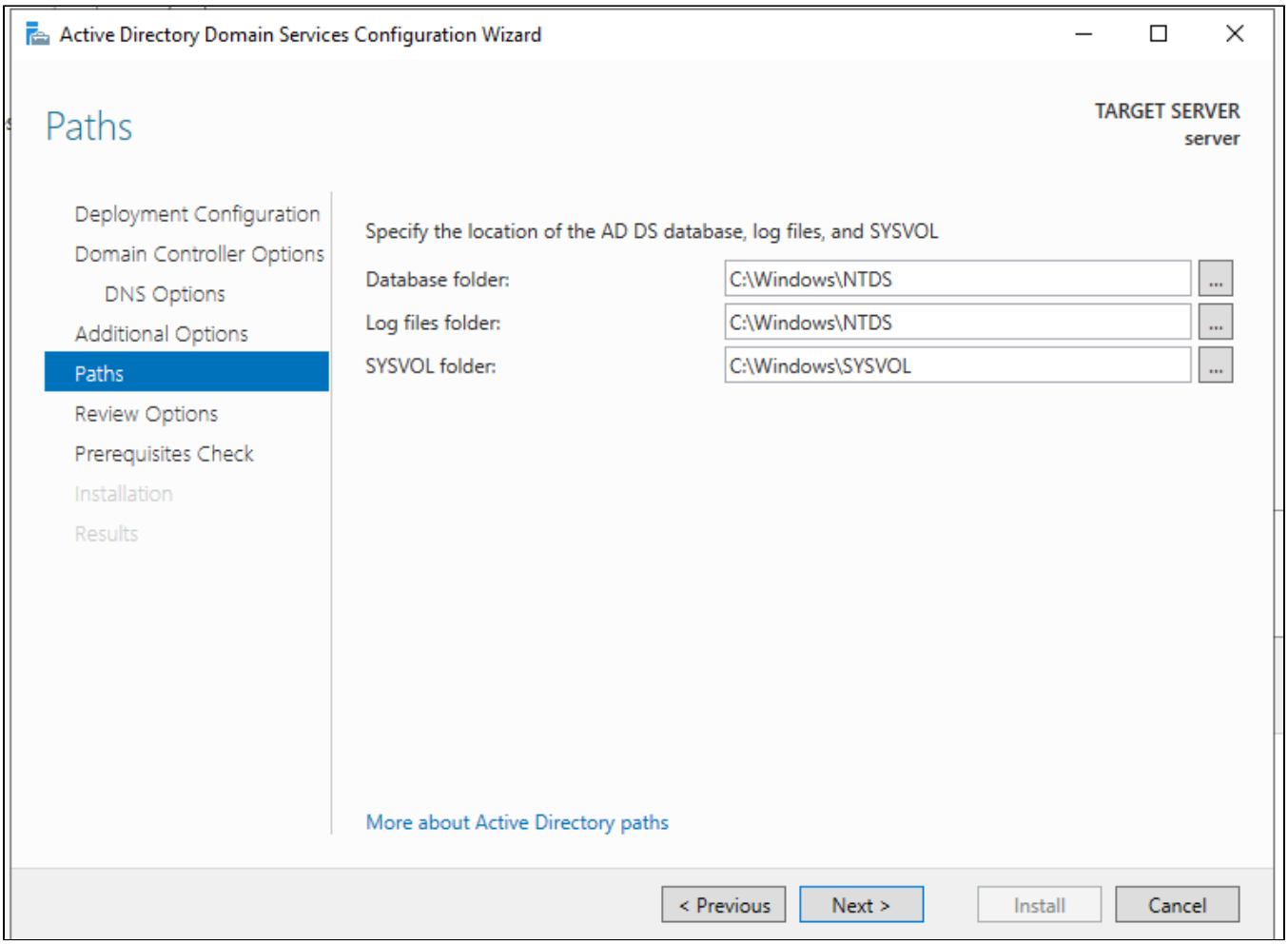


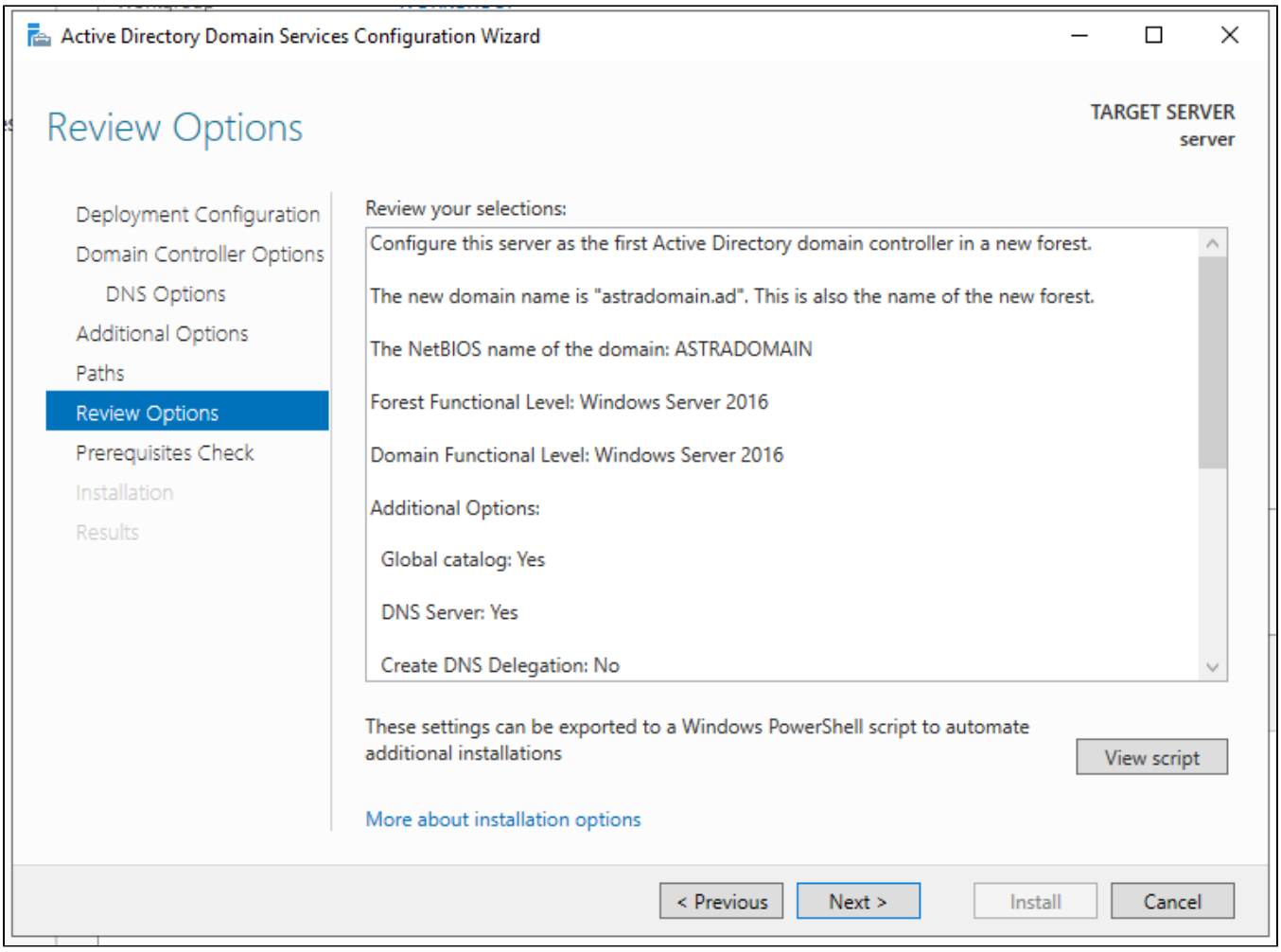

На следующей вкладке оставляем все как есть., т.к. наш сервер сам является DNS сервером:



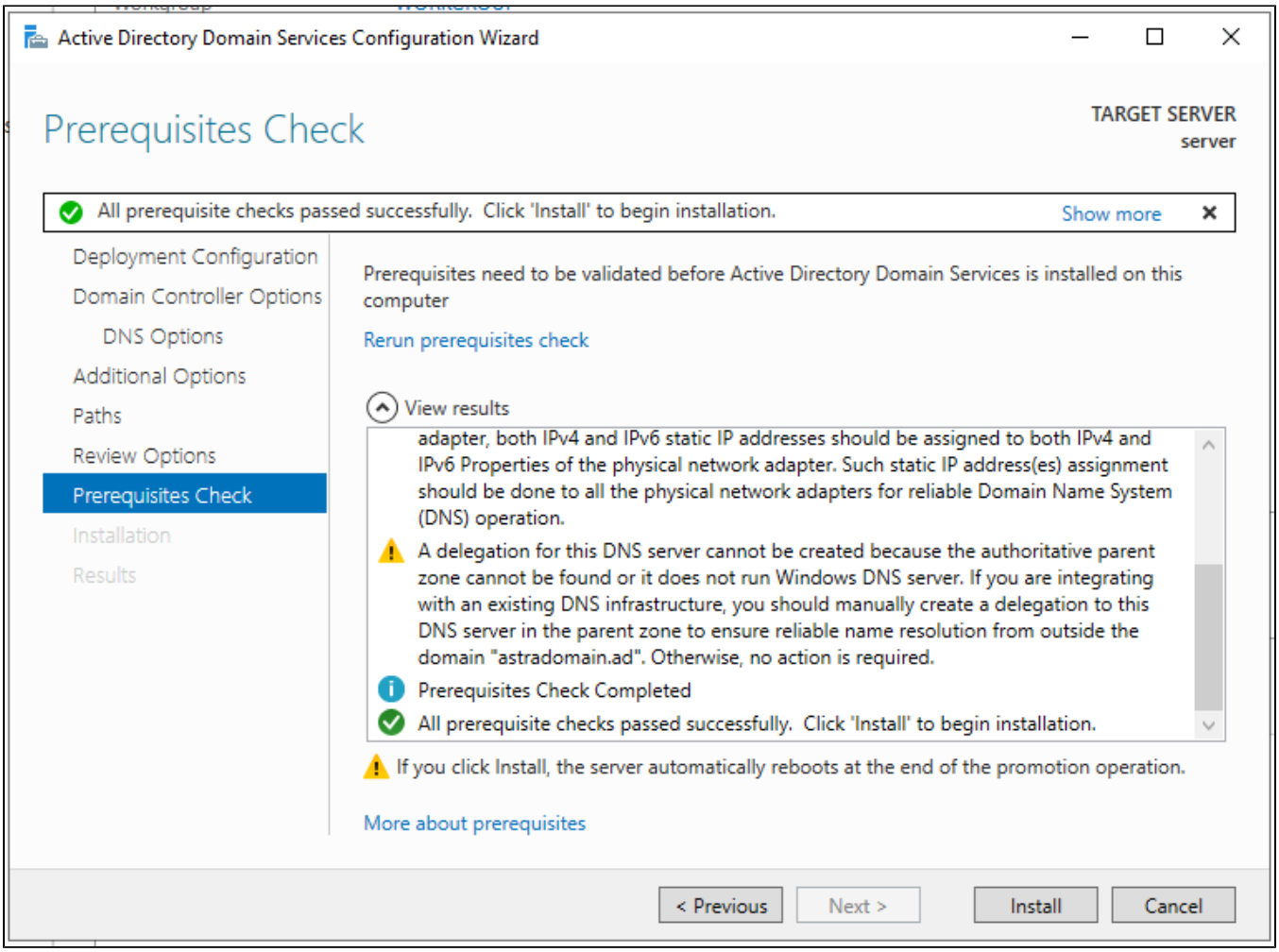

На следующих трёх вкладках также оставляем все как есть:


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



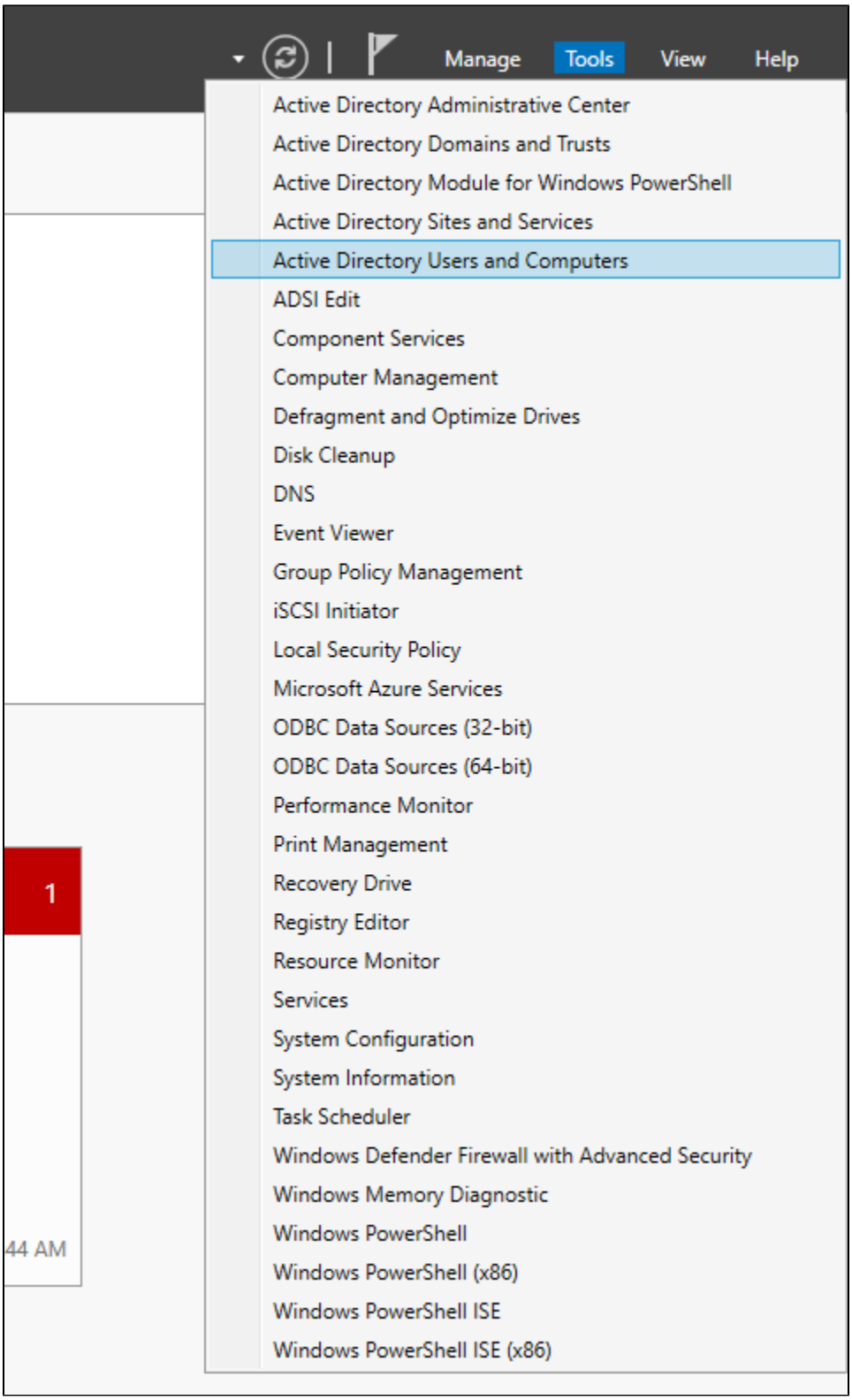

Перед запуском процесса установки ознакомимся с уведомлениями об ошибках.. И если необходимо, устраняем возникшие проблемы. В нашем случае уведомления не являются критичными:



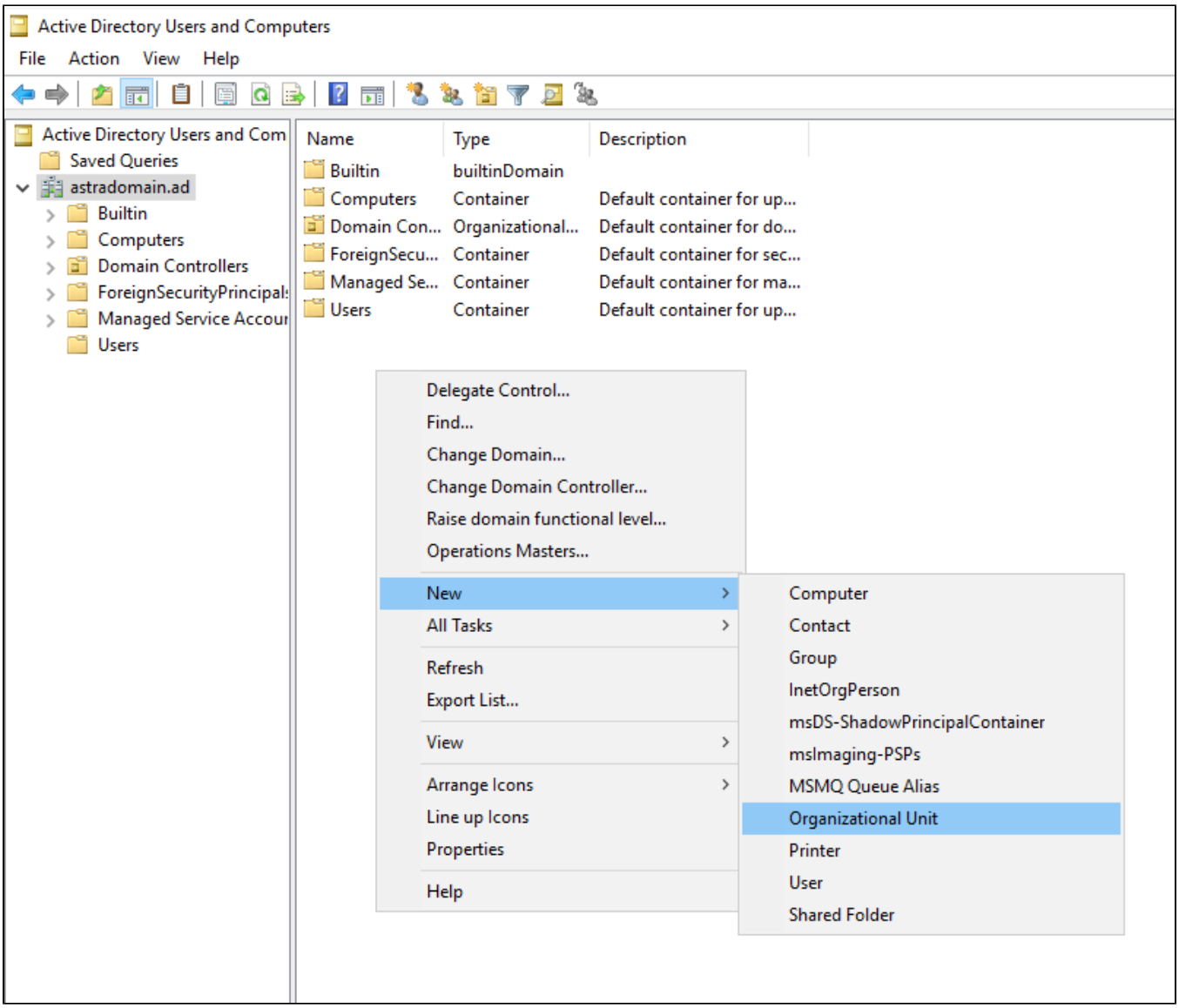

После установки Active Directory сервер перезагрузится. Если настройка прошла успешно, то нас попросят войти в аккаунт на этот раз доменного пользователя:

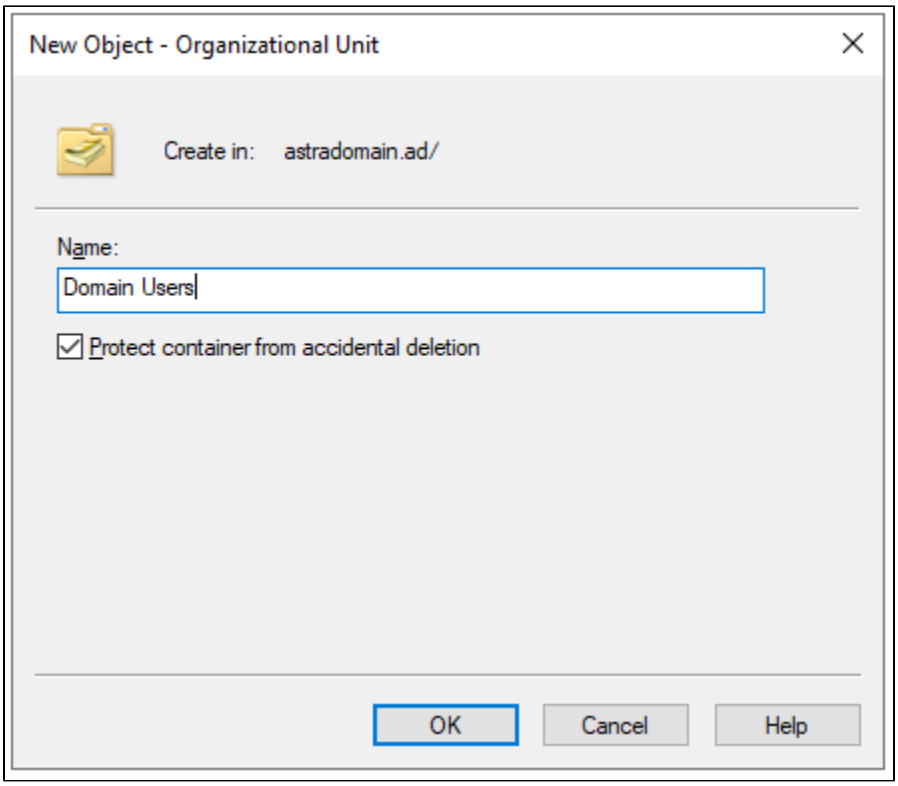
## Добавление новых пользователей:

Откроем утилиту управления пользователями и компьютерами домена:

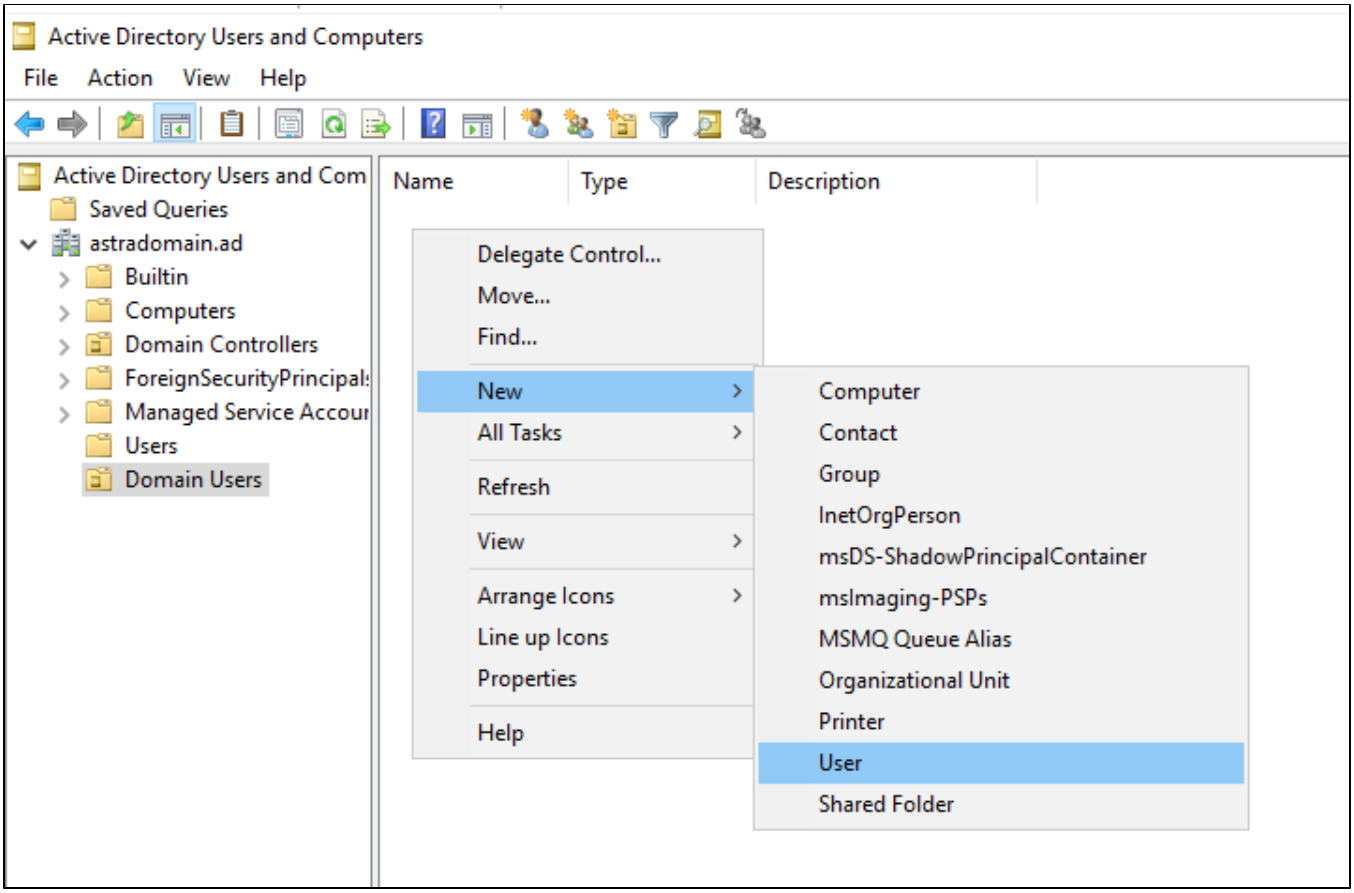


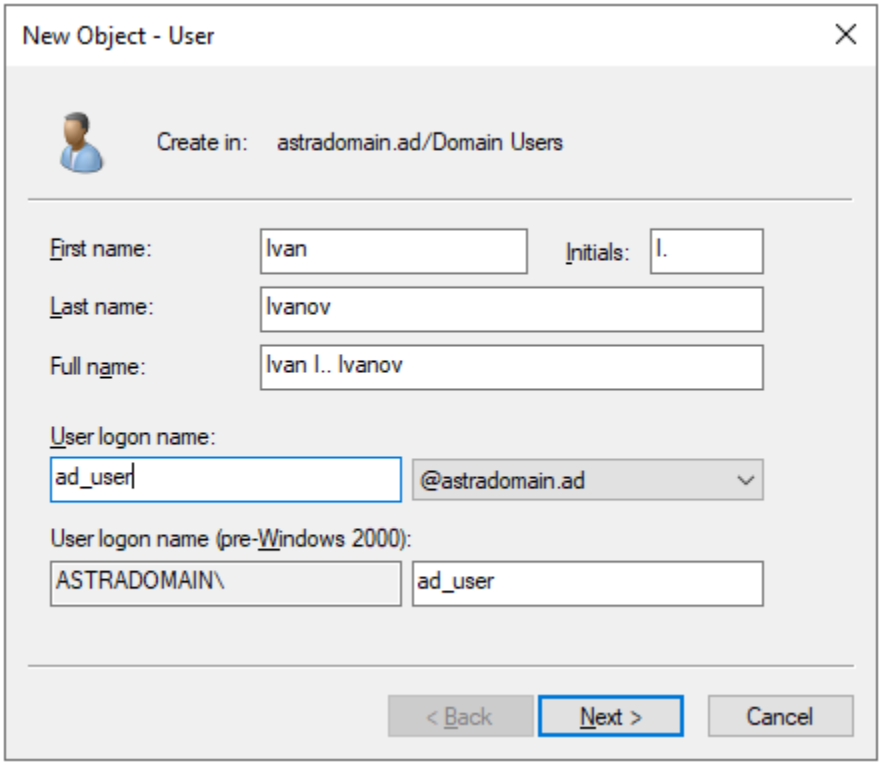

Для удобства можно создать отдельную дирректорию Domain Users, где будем создавать доменных пользователей:

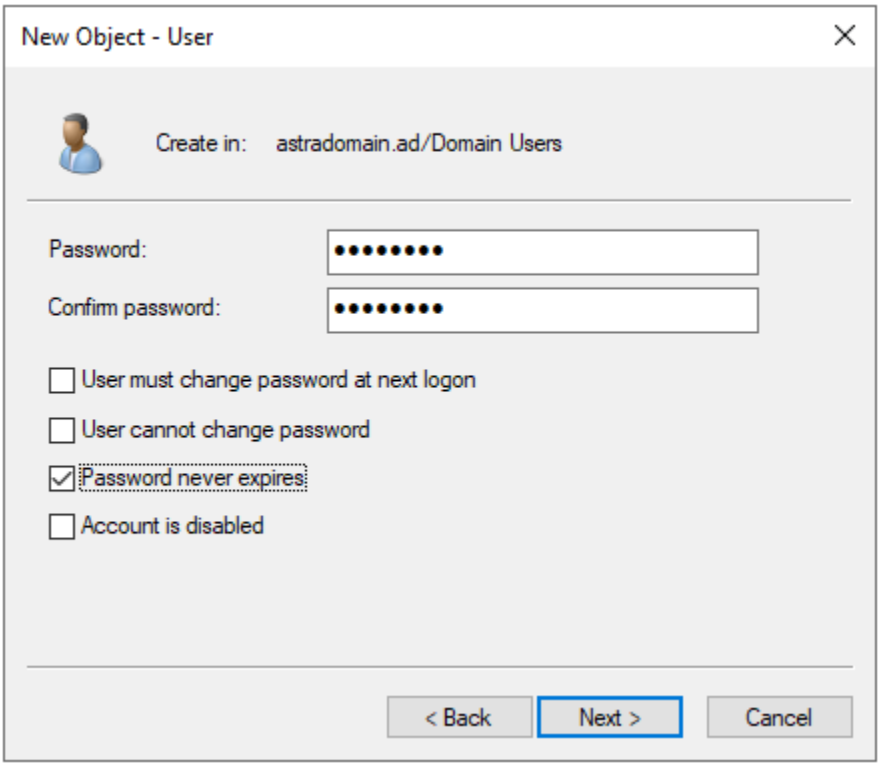

Active Directory Users and Computers
File
Action
View
Help
Active Directory Users and Com
Saved Queries
astradomain.ad
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipal
Managed Service Accour
Users
Name
Type
Description
Builtin
builtinDomain
Computers
Container
Default container for up...
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

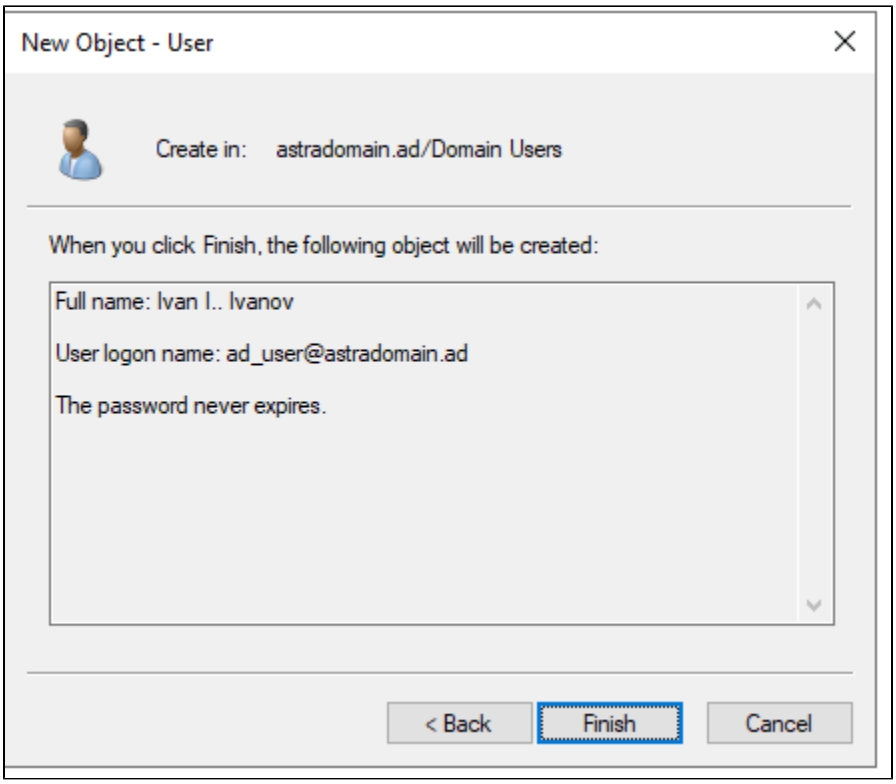



Добавим нового пользователя user:




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




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

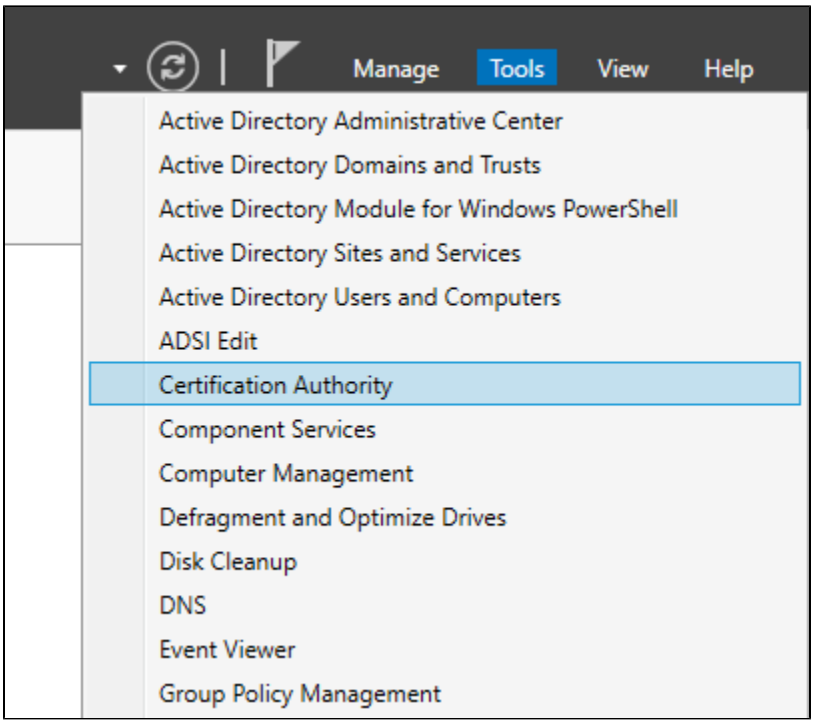
## Установка центра сертификации Active Directory:

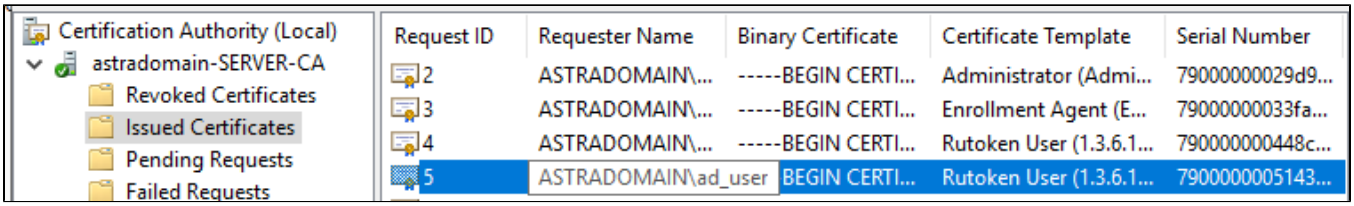
Установите драйверы для работы с Рутокеном на сервер. Их можно получить тут. После этого можно приступить к настройке центра сертификации и выдачи сертификатов для пользователей. Это можно сделать по данной инструкции. Настройку авторизации с помощью сертификатов можно воспроизвести по этой инструкции.

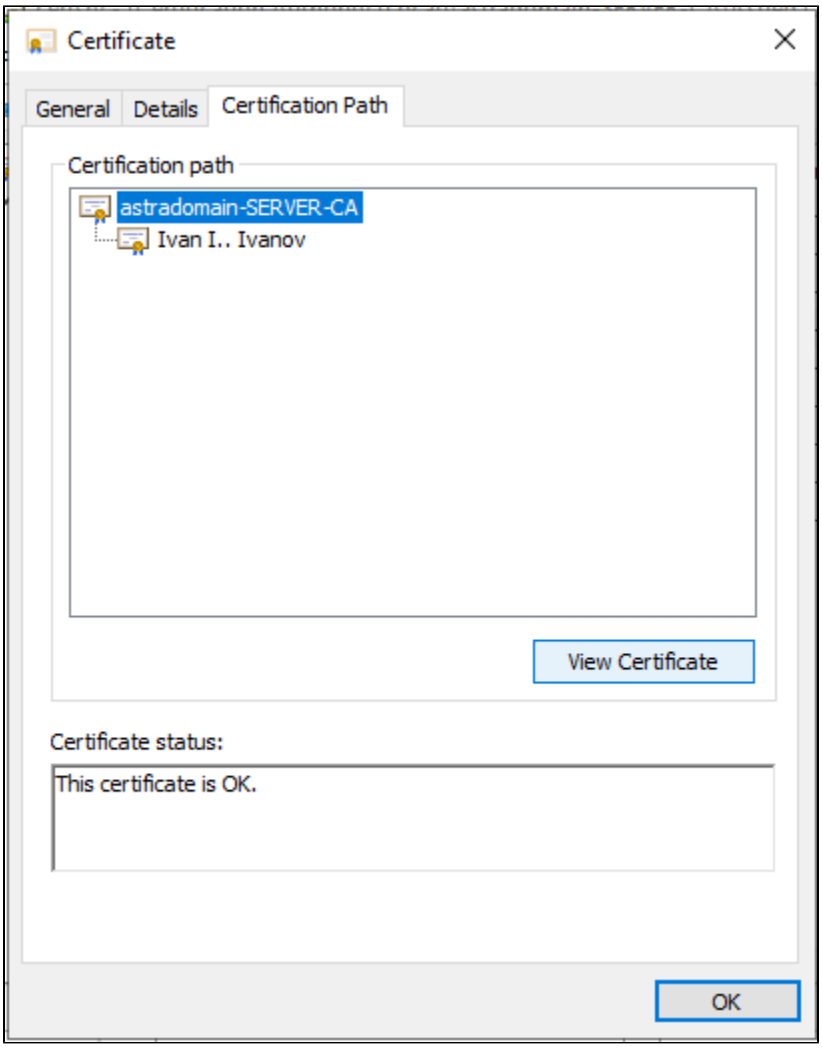
Для пользователей Linux

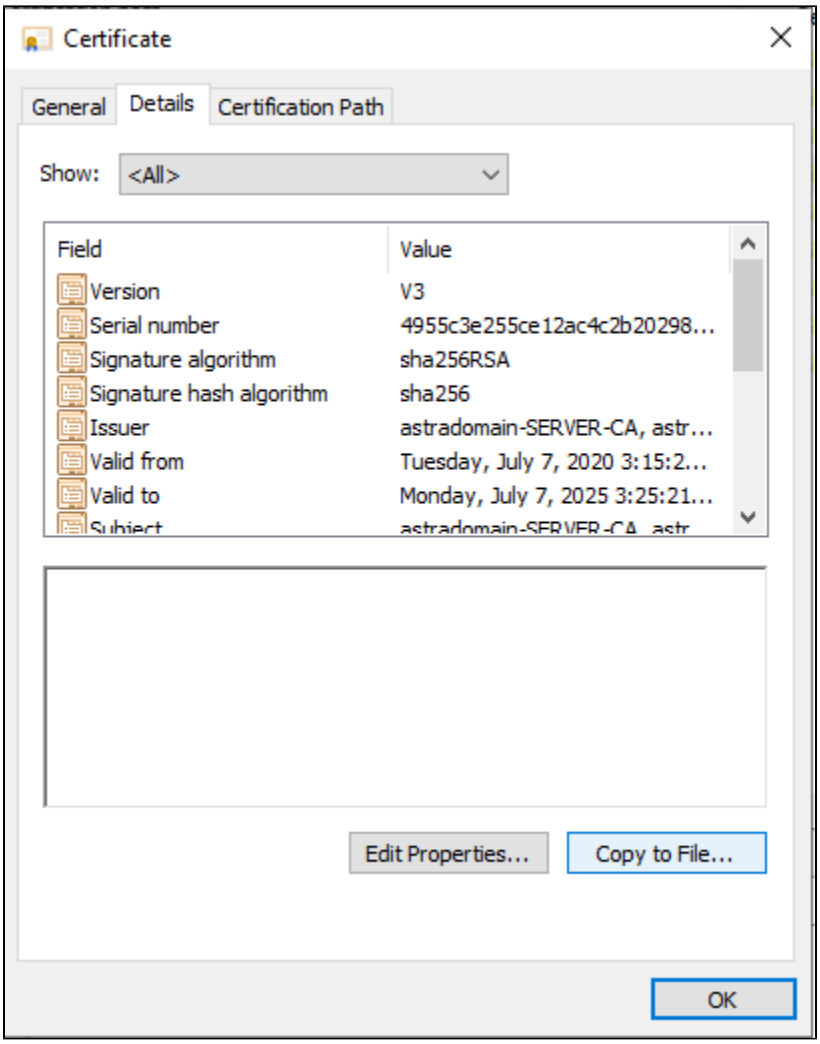
Для аутентификации пользователей через linux машины. Помимо токенов с ключами и сертификатов пользователей, вам также необходимо направить им корневой сертификат УЦ.

Его можно получить здесь:


Manage
Tools
View
Help
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
ADSI Edit
Certification Authority
Component Services
Computer Management
Defragment and Optimize Drives
Disk Cleanup
DNS
Event Viewer
Group Policy Management


Certification Authority (Local)
astradomain-SERVER-CA
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests
Request ID
Requester Name
Binary Certificate
Certificate Template
Serial Number
2 ASTRADOMAIN\... -----BEGIN CERTI... Administrator (Admi... 79000000029d9...
3 ASTRADOMAIN\... -----BEGIN CERTI... Enrollment Agent (E... 79000000033fa...
4 ASTRADOMAIN\... -----BEGIN CERTI... Rutoken User (1.3.6.1... 790000000448c...
5 ASTRADOMAIN\ad_user BEGIN CERTI... Rutoken User (1.3.6.1... 7900000005143...


Certificate
General
Details
Certification Path
Certification path
astradomain-SERVER-CA
Ivan I.. Ivanov
View Certificate
Certificate status:
This certificate is OK.
OK




# Настройка клиента Linux

## Настройка подключения к домену

Astra Linux Smolensk

Для Astra Linux Smolensk чтобы подключиться к домену (не настраивая двухфакторную аутентификацию), можно воспользоваться следующей инструкцией.

Если во время выполнения инструкции панель "Настройки клиента Active Directory" не будет запускаться, то введите в командной строке следующую команду:

**доступ к X11 для root**

```
xhost +SI:localuser:root
```

Она предоставит пользователю root доступ к графическому интерфейсу среды.

В первую очередь настроим подключение к домену. Это можно сделать с помощью следующей последовательности команд:

Настройка DNS

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

#


##########################################################
###  .   DNS  ###
##########################################################
#    .
CON_NAME="  1"
#  ,
INT_NAME="eth0"
#  dns
DNS_SERVER_IP=10.0.2.37
#
sudo nmcli con down "$CON_NAME"

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

#  DNS -  DNS_SERVER_IP  IP-  DNS.       DNS.      DNS     FreeIPA.     IP
sudo nmcli con mod "$CON_NAME" ipv4.dns "$DNS_SERVER_IP 8.8.8.8"
sudo nmcli con mod "$CON_NAME" ipv4.ignore-auto-dns yes

#
sudo nmcli con up "$CON_NAME"

#
ping server.astradomain.ad

##########################################################
#############    #############
##########################################################
#       yum
sudo yum install -y realmd PackageKit

#       apt-get
sudo apt-get install -y realmd packagekit

#
realm discover astradomain.ad

#
# required-package: pkg1
# required-package: pkg2
# required-package: pkg3
# ...

#
#       yum
sudo yum install -y pkg1 pkg2 pkg3 ...

#       apt-get
sudo apt-get install -y pkg1 pkg2 pkg3 ...


##########################################################
#################    ##################
##########################################################
# c
#  user       .
sudo realm join astradomain.ad --user=user

#   krb5-workstation
```

```
#       yum
sudo yum install -y krb5-workstation

#       apt-get
sudo apt-get install -y krb5-user

#   Alt linux
sudo apt-get install -y krb5-workstation

#      user,       ,
kinit user@ASTRADOMAIN.AD

#
klist

#
kdestroy
```

## Настройка автоматического создания домашней директории

Когда доменный пользователь аутентифицируется в системе необходимо чтобы для него автоматически создавался домашний каталог.

Это можно сделать в настройках pam. Для этого в файле

**/etc/pam.d/common-session** для систем основанных на Debian

**/etc/pam.d/system-auth** для систем основанных на Red Hat

**/etc/pam.d/system-auth-sss-only** для пользователей Alt linux

активируем модуль pam_mkhomedir.so, после pam_sss.so. Содержимое файла будет выглядеть следующем образом:

**Настройка автоматического создания каталога**

```
...
session optional pam_sss.so
session required pam_mkhomedir.so skel=/etc/skel/ umask=0022
...
```

## Проверка аутентификации под пользователем в домене без Рутокена

Если в домене есть пользователь user, под которым можно аутентифицироваться без смарт-карты, то можно проверить предыдущую надстройку аутентифицируясь под ним. Для начала можно попробовать аутентифицироваться через командную строку:

**Настройка автоматического создания каталога**

```
su user@astradomain.ad
```

```
[lo1ol@redosclie home]$ su user1@astradomain.ad
Пароль:
[user1@astradomain.ad@redosclie home]$ klist
Ticket cache: KEYRING:persistent:1907601108:krb_ccache_wXFsUEB
Default principal: user1@ASTRADOMAIN.AD

Valid starting       Expires              Service principal
08.07.2020 10:07:21  08.07.2020 20:07:21  krbtgt/ASTRADOMAIN.AD@ASTRADOMAIN.AD
        renew until 15.07.2020 10:07:21
[user1@astradomain.ad@redosclie home]$
```

# Настройка клиента для аутентификации в домене с помощью Рутокена

## Упрощенная настройка

Для упрощенной настройки можно воспользоваться утилитой для работы с токенами. Описание упрощенной настройки можно прочитать тут.

## Ручная настройка

### Установка необходимых пакетов для работу:

**Установка libnss3-tools**

```
#       yum
sudo yum install -y nss-tools opensc krb5-pkinit

#       apt-get
sudo apt-get install -y libnss3-tools opensc krb5-pkinit
```

Для ручной настройки также потребуется установить библиотеку **librtpkcs11ecp**. Ее можно получить тут.  Установим данную библиотеку.

**Установка библиотеки pkcs11**

```
#       red hat
sudo rpm -i librtpkcs11ecp-2.0.5.1-1.x86_64.rpm
#    Debian
sudo dpkg -i librtpkcs11ecp-2.0.5.1-1.x86_64.deb
```

### Добавление корневого сертификата и сертификатов токена в БД

Инициализируем БД:

**Установка libnss3-tools**

```
mkdir /etc/pki/nssdb
sudo certutil -N -d /etc/pki/nssdb --empty-password
```

Добавление корневого сертификата в БД:

**Установка libnss3-tools**

```
sudo certutil -d /etc/pki/nssdb -A -n 'CA-ROOT-CERT' -t CT,CT,CT -a -i /path/to/ca_cert.pem
```

Добавление сертификатов с Рутокена:

**Добавление сертификатов с Рутокена**

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

Проверку того, что сертификаты добавились в БД можно осуществить с помощью команды

**Добавление сертификатов с Рутокена**

```
#   pcscd  ,
sudo systemctl restart pcscd

#
sudo certutil -L -d /etc/pki/nssdb -h all
```

```
[lo1ol@redosclie ~]$ sudo certutil -L -d /etc/pki/nssdb -h all

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

Enter Password or Pin for "Rutoken ECP <no label>":
CA-ROOT-CERT                                                 CT,C,C
Rutoken ECP <no label>:te-RutokenUser-066f9fe7-7542-4d4d-8973-f4a412b09c9d_E u,u,u
[lo1ol@redosclie ~]$
```

## Настройка 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**. Он должен выглядеть примерно следующим образом:

**/etc/sssd/sssd.conf**

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

[domain/astradomain.ad]
ad_domain = astradomain.ad
krb5_realm = ASTRADOMAIN.AD
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
fallback_homedir = /home/%u@%d
access_provider = ad

#
use_fully_qualified_names = False

#   Astra Linux
ad_gpo_access_control = permissive

#     -
[pam]
pam_cert_auth = True
#   ,   .   ,
pam_p11_allowed_services = +<service_name>
```

Перезапустим сервис SSSD

**перезапуск сервиса sssd**

```
sudo systemctl restart sssd
```

## Настройка Kerberos

Скопируем корневой сертификат в директорию **/etc/pki/tls/certs/**.

**Копирование корневого сертификата**

```
sudo cp /path/to/ca_cert.pem /etc/pki/tls/certs/
#     /etc/pki/tls/certs/
sudo chmod 777 /etc/pki/tls/certs/
```

Для настройки Kerberos изменим содержимое файла **/etc/krb5.conf**. Секция [libdefaults] должна содержать следующее:

**/etc/krb5.conf**

```
...
[libdefaults]
...
#         .pem
    pkinit_anchors = DIR:/etc/pki/tls/certs/
#  KDC
    pkinit_kdc_hostname = server.astradomain.ad
#   EKU
    pkinit_eku_checking = kpServerAuth
    default_ccache_name = KEYRING:persistent:%{uid}
#
    default_realm = ASTRADOMAIN.AD
#
    pkinit_identities = PKCS11:librtpkcs11ecp.so
#    AD
    canonicalize = True
...
```

Проверка настройки с помощью получения тикета для пользователя user, который аутентифицируется по Рутокену

**получение тикета для пользователя user**

```
#  .     -
kinit user

#
klist

#
kdestroy
```

```
[lo1ol@redosclie ~]$ kinit user
Rutoken ECP <no label>           PIN:
[lo1ol@redosclie ~]$ klist
Ticket cache: KEYRING:persistent:1000:1000
Default principal: user@ASTRADOMAIN.AD

Valid starting       Expires              Service principal
08.07.2020 11:12:20  08.07.2020 21:12:20  krbtgt/ASTRADOMAIN.AD@ASTRADOMAIN.AD
        renew until 15.07.2020 11:12:17
[lo1ol@redosclie ~]$ kdestroy
```

## Попытка аутентификации по смарт-карте

Попробуйте аутентифицироваться под доменным пользователем user по смарт-карте в системе:

**Аутентфиикация пользователя user**

```
su user
```

```
[lo1ol@redosclie ~]$ su user
PIN for Rutoken ECP <no label>
[user@redosclie lo1ol]$
```

Если аутентификация не прошла успешно, то попробуйте изменить конфигурацию pam модулей, иначе можете пропустить данную часть

## Настройка pam модулей

Для аутентификации пользователя в системе с помощью смарт-карты необходимо изменить содержимое pam модулей

### Для систем основанных на Debian

Файл **/etc/pam.d/common-auth** должен содержать следующие строки:

**Настройка автоматического создания каталога**

```
...
auth [success=2 default=ignore] pam_sss.so forward_pass
auth [success=1 default=ignore] pam_unix.so try_first_pass nullok_secure
...
```

### Для систем основанных на Red Hat

Файл **/etc/pam.d/system-auth** должен содержать следующие строки:

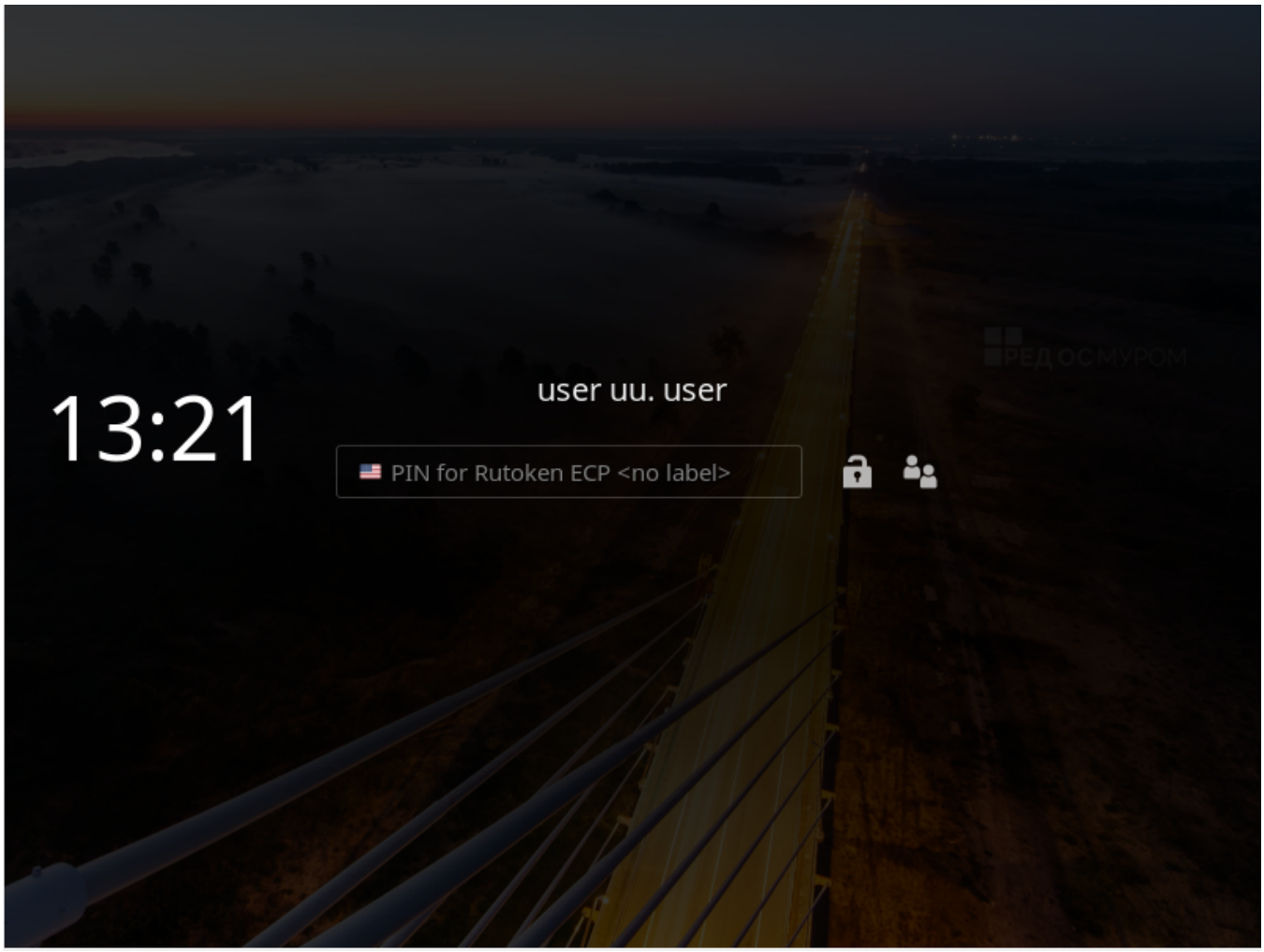
**Настройка автоматического создания каталога**

```
...
auth        [default=1 ignore=ignore success=ok]         pam_localuser.so
auth        sufficient                                   pam_unix.so nullok try_first_pass
auth        requisite                                    pam_succeed_if.so uid >= 1000 quiet_success
auth        sufficient                                   pam_sss.so forward_pass
...
```

## Аутентфикация через гритер

Проверьте аутентификацию через гритер  через лок скрин.

Ср, 11:28
ru
user uu. user
PIN for Rutoken ECP <no label>
Отмена
Разблокировать
РЕД ОС МУРОМ




Для пользователей Astra Linux предложение ввода ПИН-кода не отображается. В поле ввода пароля просто введите ПИН-код от Рутокена:

Вход в smolensk.astradomain.ad
вт, 14 июл. 2020, 16:58 MSK
Имя:
user
Пароль:
Тип сессии
Меню
En

Компьютер smolensk.astradomain.ad
16 : 57
14
Вт.
Введите пароль
Сессии...
********
EN
CapsLock Выкл.