

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:

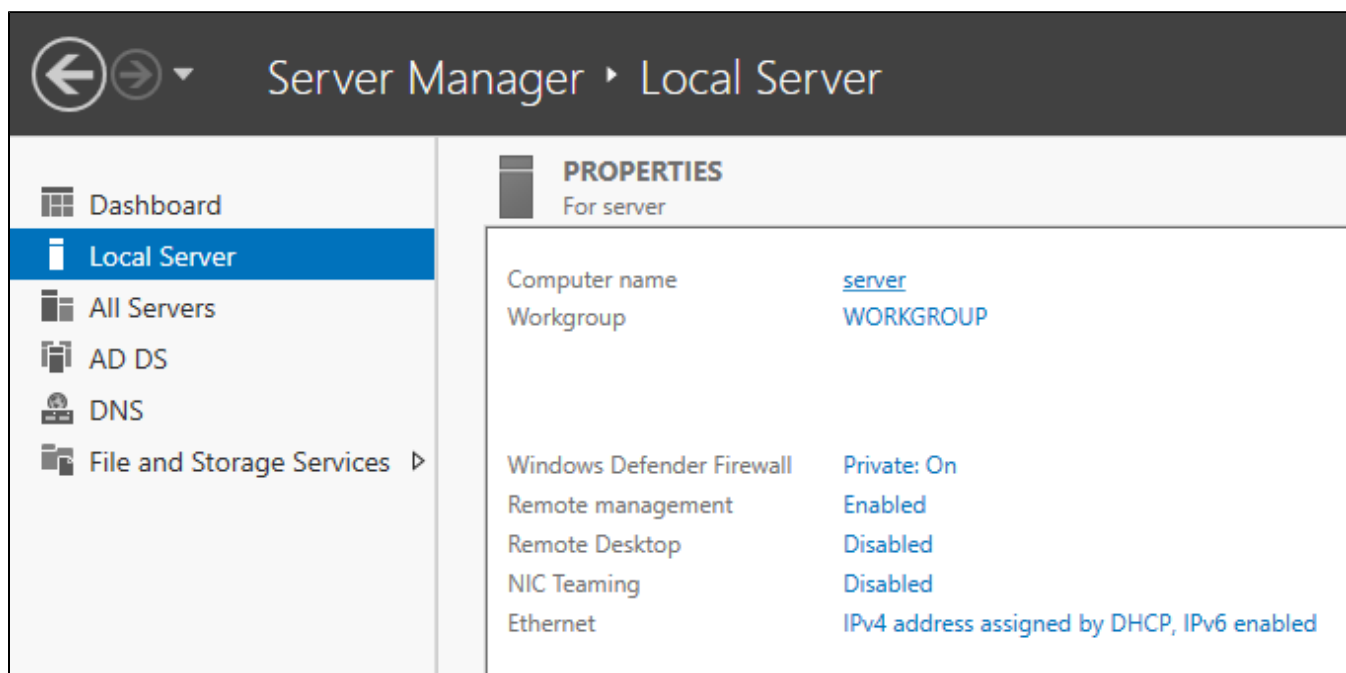
ОС: РЕД ОС \ Астра Линукс \ ALT Linux \ Ubuntu

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

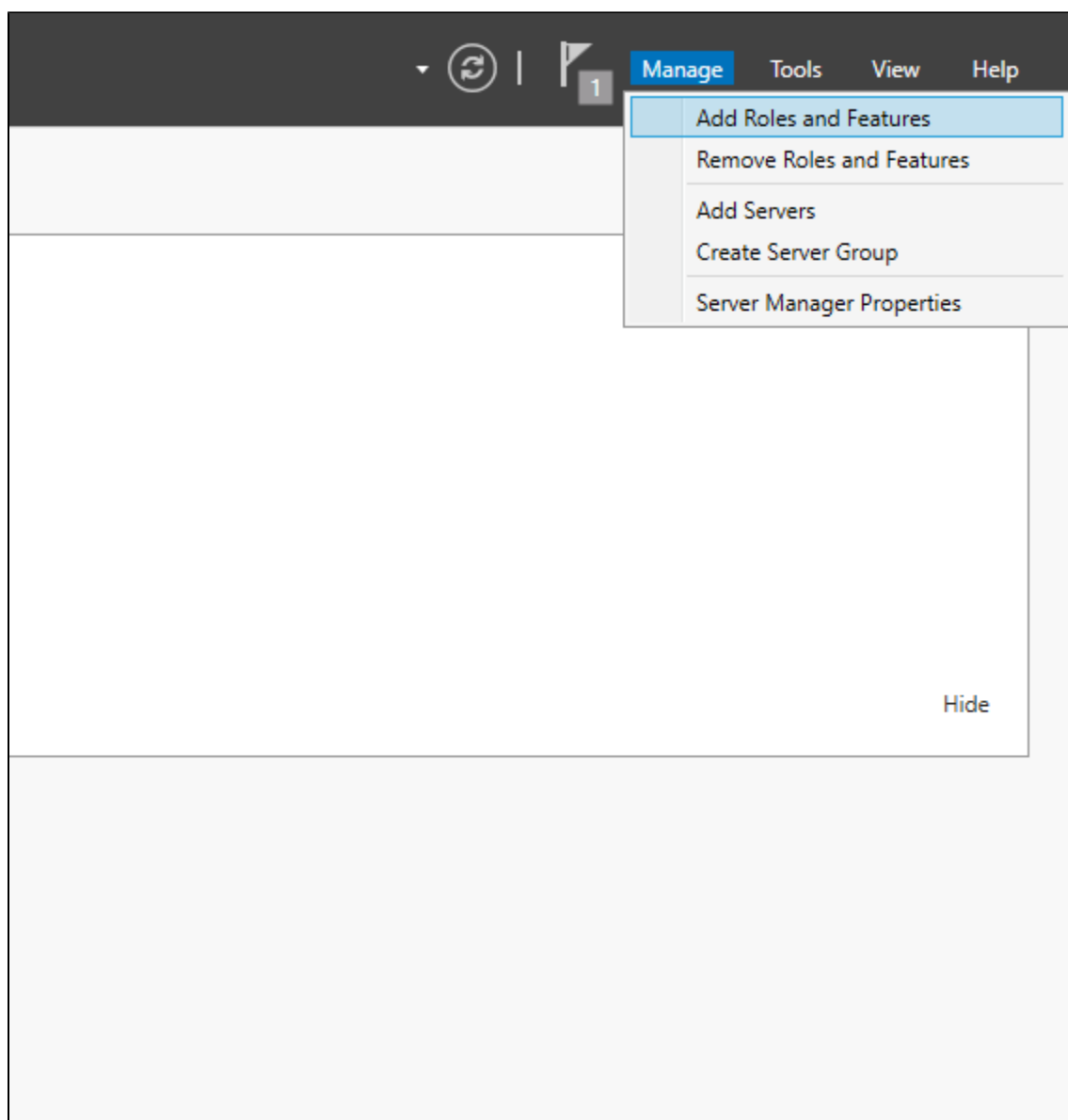
Настройка сервера

Установка сервиса Active Directory

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



Добавим службу Active Directory 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":

Add Roles and Features Wizard

Before You Begin

Installation Type

Server Selection

Server Roles

Features

AD DS

DNS Server

Confirmation

Results

Select one or more roles to install on the selected server.

Roles

☐ Active Directory Certificate Services
☒ Active Directory Domain Services
☐ Active Directory Federation Services
☐ Active Directory Lightweight Directory Services
☐ Active Directory Rights Management Services
☐ Device Health Attestation
☐ DHCP Server
☒ **DNS Server**
☐ Fax Server

▶

File and Storage Services (1 of 12 installed)

☐ Host Guardian Service
☐ Hyper-V
☐ Network Policy and Access Services
☐ Print and Document Services
☐ Remote Access
☐ Remote Desktop Services
☐ Volume Activation Services
☐ Web Server (IIS)
☐ Windows Deployment Services
☐ Windows Server Update Services

Description

Domain Name System (DNS) Server provides name resolution for TCP/IP networks. DNS Server is easier to manage when it is installed on the same server as Active Directory Domain Services. If you select the Active Directory Domain Services role, you can install and configure DNS Server and Active Directory Domain Services to work together.

< Previous

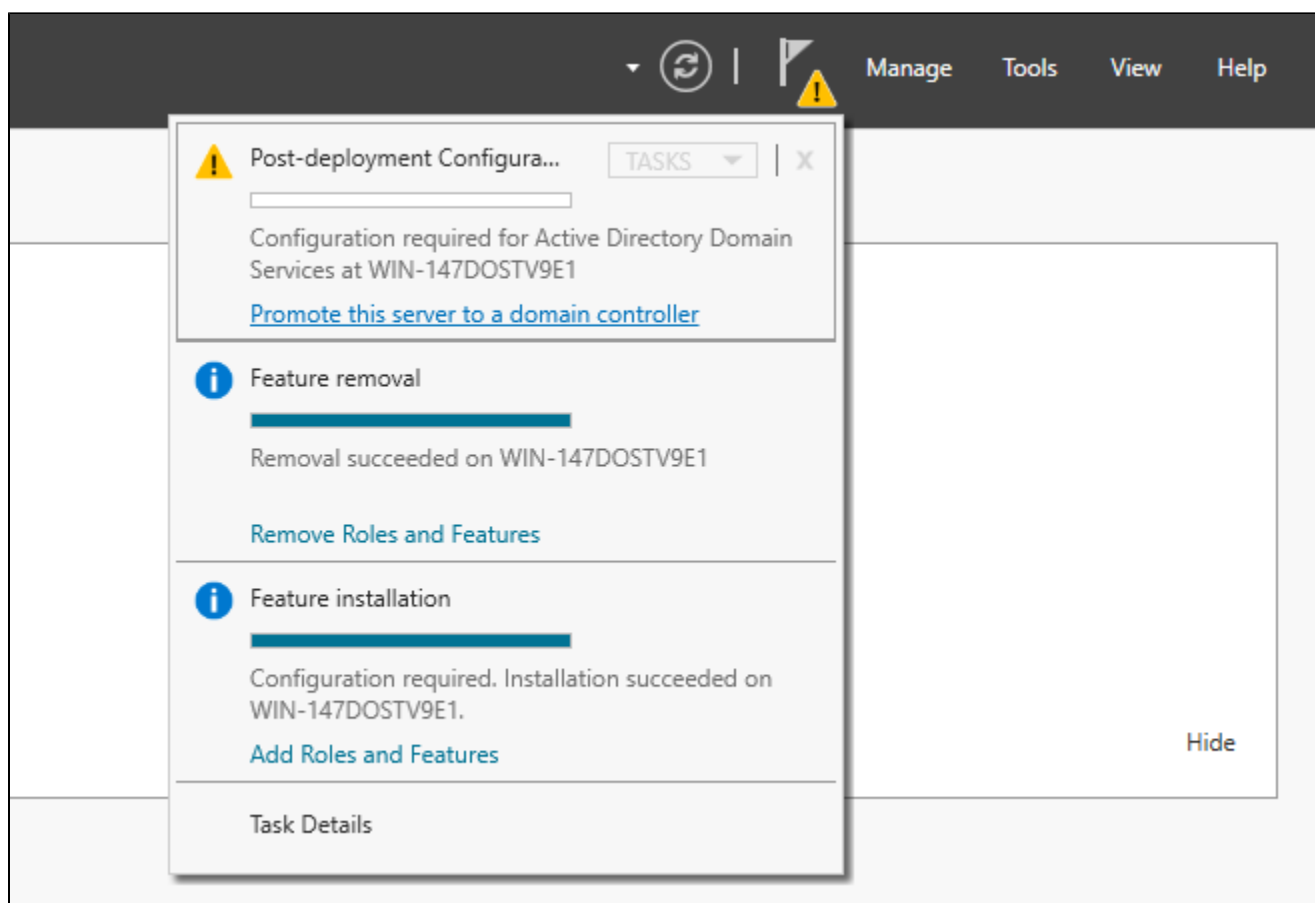
Next >

Install

Cancel

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:

Active Directory Domain Services Configuration Wizard

Deployment Configuration

TARGET SERVER
server

Deployment Configuration

Domain Controller Options

Additional Options

Paths

Review Options

Prerequisites Check

Installation

Results

Select the deployment operation

☐ Add a domain controller to an existing domain

☐ Add a new domain to an existing forest

☒ Add a new forest

Specify the domain information for this operation

Root domain name:

[More about deployment configurations](#)

< Previous

Next >

Install

Cancel

Введите пароль сброса:

Active Directory Domain Services Configuration Wizard

Domain Controller Options

TARGET SERVER
server

Deployment Configuration

Domain Controller Options

DNS Options

Additional Options

Paths

Review Options

Prerequisites Check

Installation

Results

Select functional level of the new forest and root domain

Forest functional level: Windows Server 2016

Domain functional level: Windows Server 2016

Specify domain controller capabilities

☒ Domain Name System (DNS) server

☒ Global Catalog (GC)

☐ Read only domain controller (RODC)

Type the Directory Services Restore Mode (DSRM) password

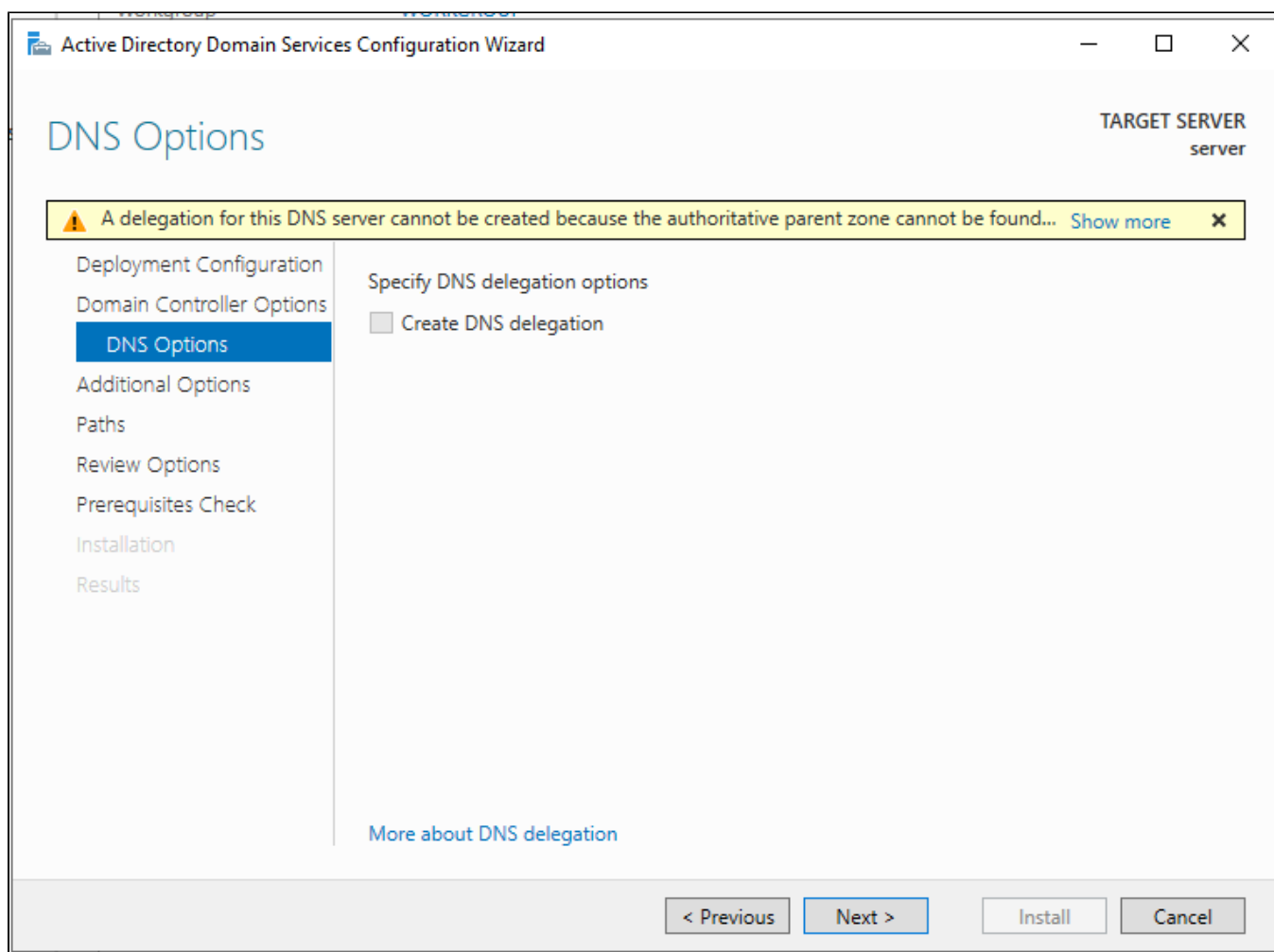
Password:

Confirm password:

[More about domain controller options](#)

< Previous Next > Install Cancel

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



На следующих трёх вкладках также оставляем все как есть:

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:

[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

...

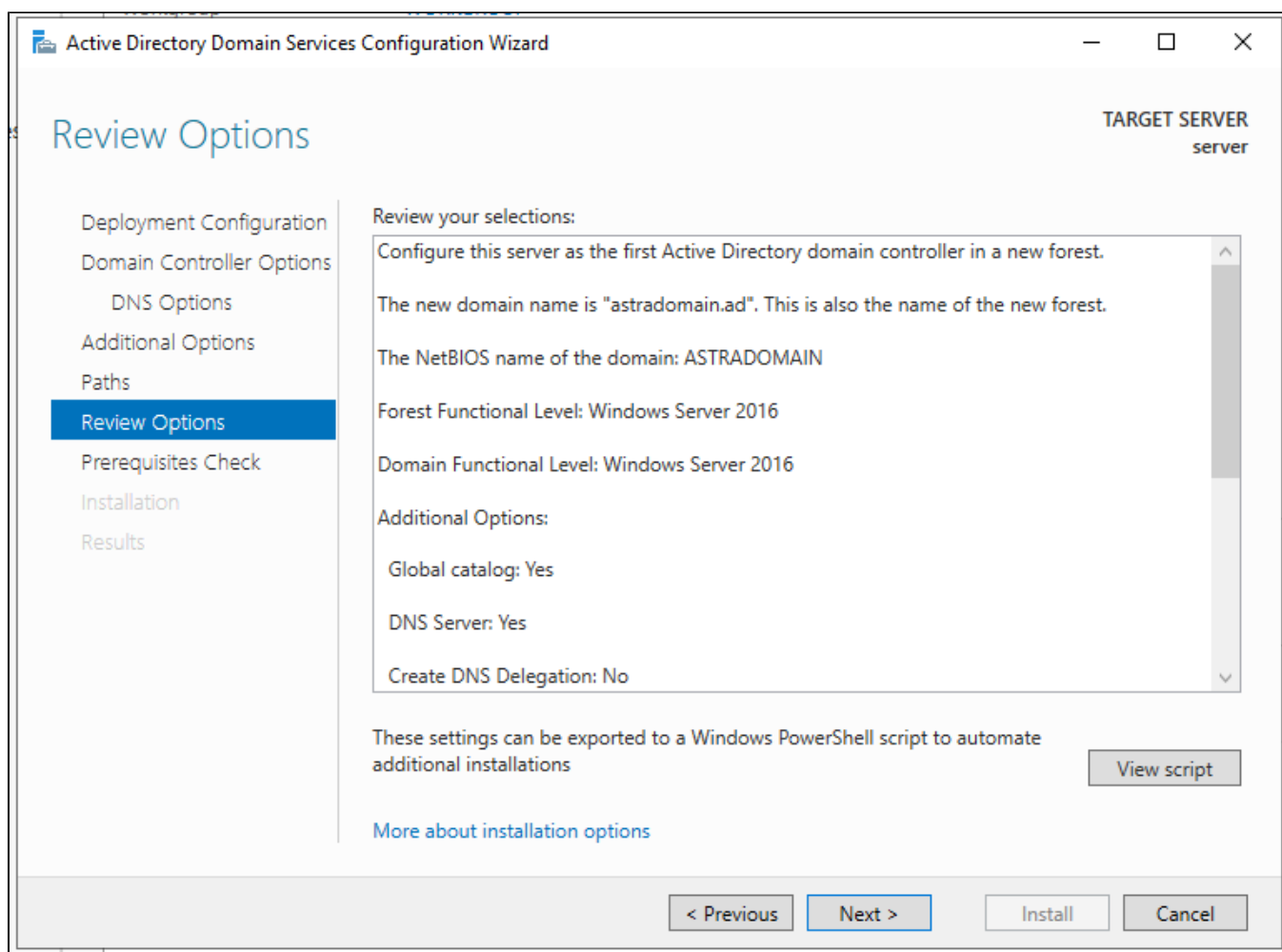
[More about Active Directory paths](#)

< Previous

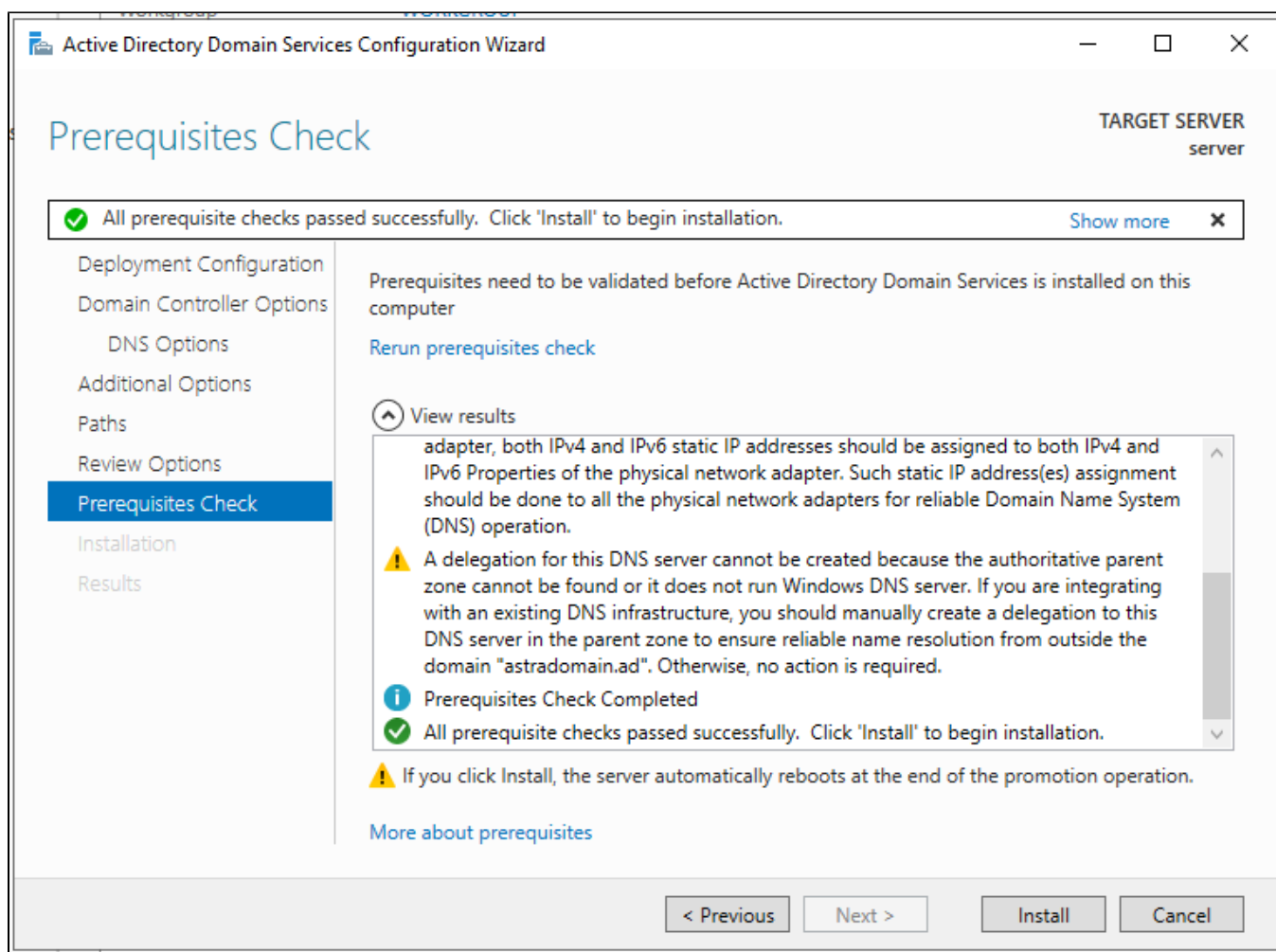
Next >

Install

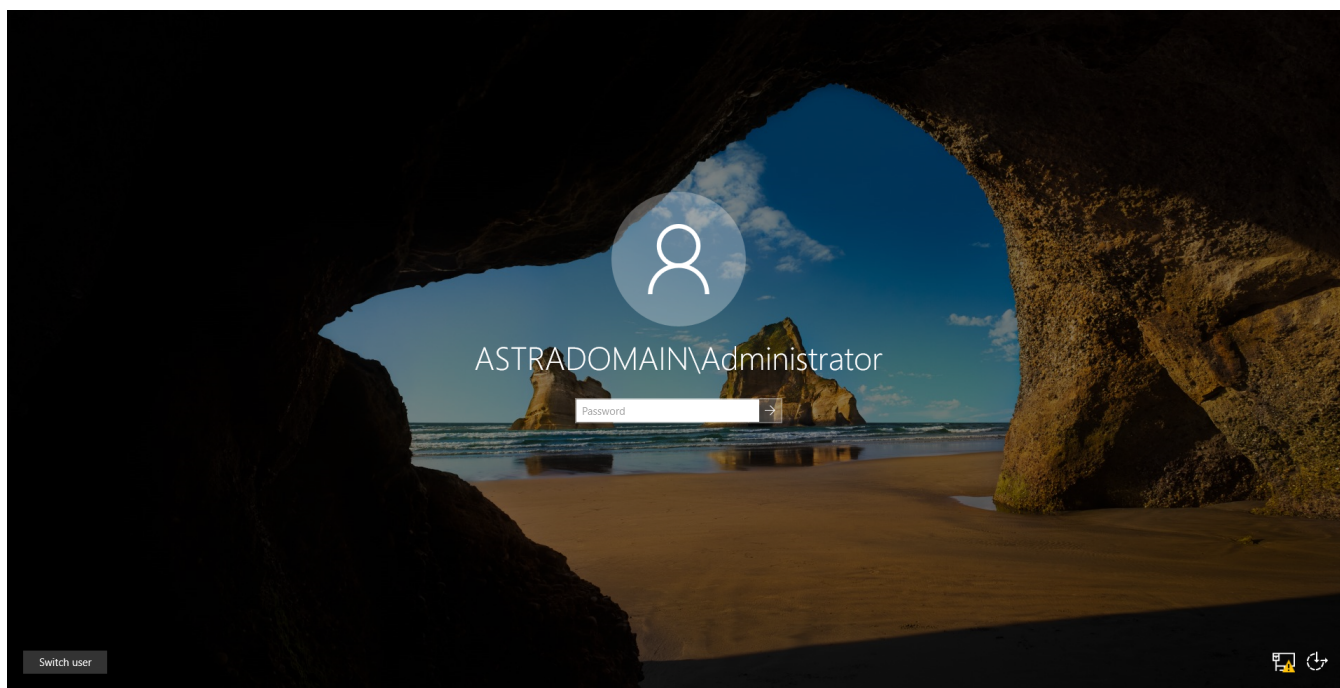
Cancel



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

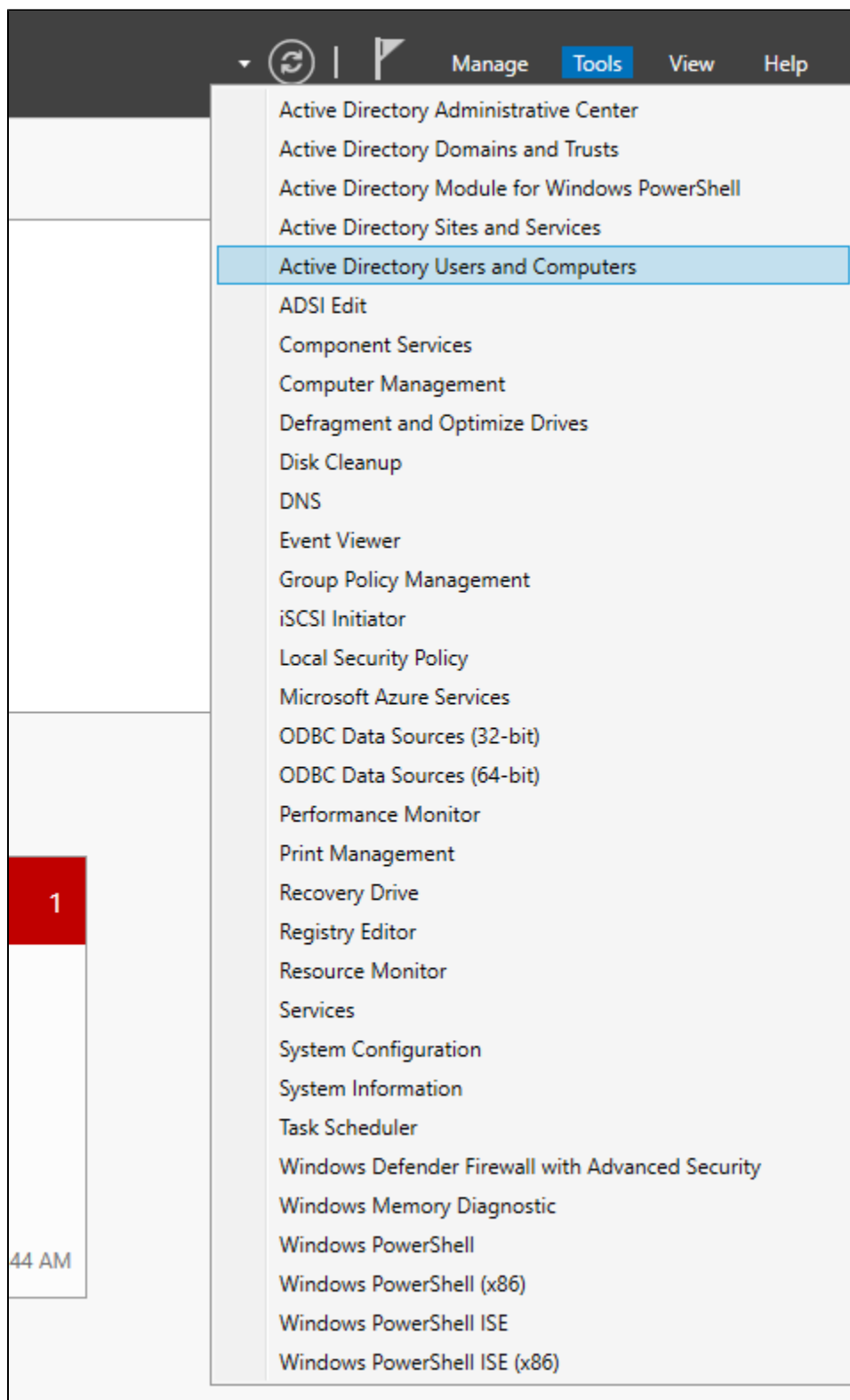


После установки Active Directory сервер перезагрузится. Если настройка прошла успешно, то нас попросят войти в аккаунт на этот раз доменного пользователя:



Добавление новых пользователей:

Откроем утилиту управления пользователями и компьютерами домена:



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

Active Directory Users and Computers

FileActionViewHelp

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

msImaging-PSPs

MSMQ Queue Alias

Organizational Unit

Printer

User

Shared Folder

New Object - Organizational Unit

Create in: astradomain.ad/

Name:

☒ Protect container from accidental deletion

OK Cancel Help

Добавим нового пользователя user:

Active Directory Users and Computers

File Action View Help

Active Directory Users and Computers

- Active Directory Users and Computers
 - Saved Queries
 - astradomain.ad
 - Builtin
 - Computers
 - Domain Controllers
 - ForeignSecurityPrincipals
 - Managed Service Accounts
 - Users
 - Domain Users

Name	Type	Description
Delegate Control...		
Move...		
Find...		
New		Computer
All Tasks		Contact
Refresh		Group
View		InetOrgPerson
Arrange Icons		msDS-ShadowPrincipalContainer
Line up Icons		msImaging-PSPs
Properties		MSMQ Queue Alias
Help		Organizational Unit
		Printer
		User
		Shared Folder

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

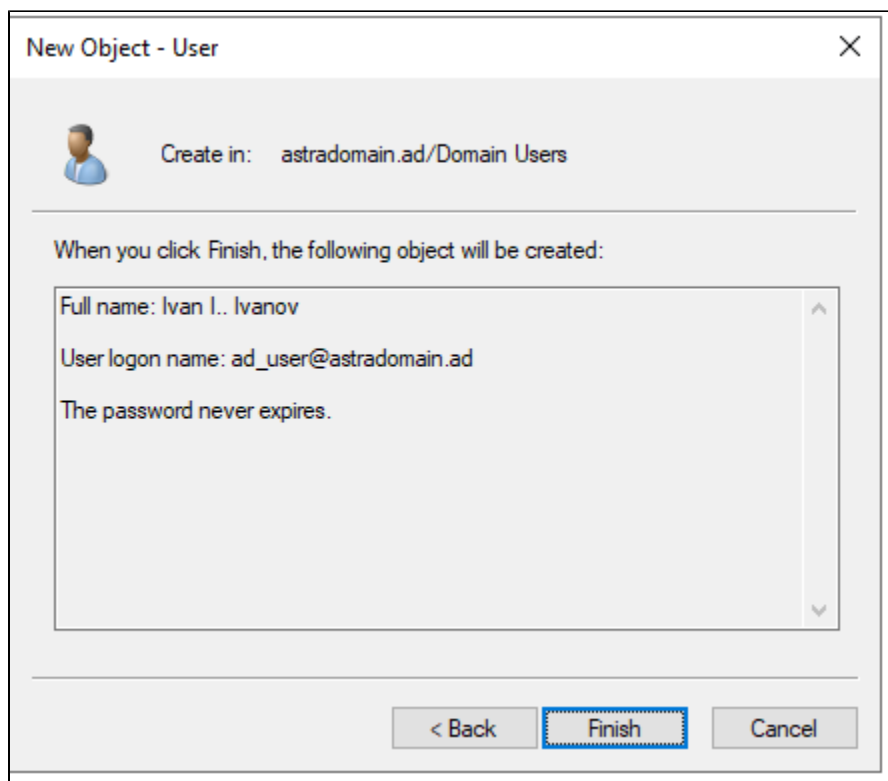
☒ Password never expires

☐ Account is disabled

< Back

Next >

Cancel



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

Установка центра сертификации Active Directory:

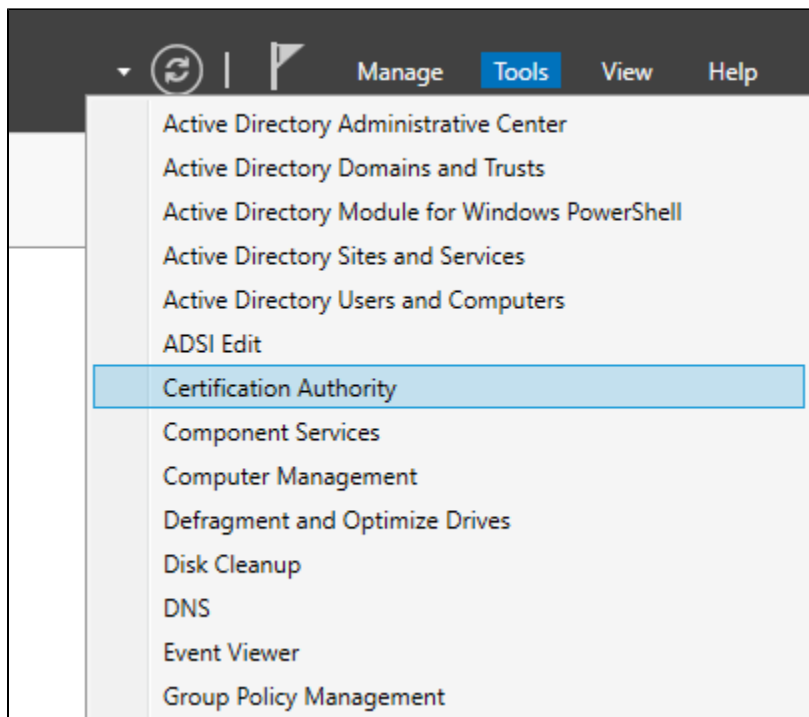
Установите драйверы для работы с Рутокеном на сервер. Их можно получить [тут](#). После этого можно приступить к настройке центра сертификации и выдачи сертификатов для пользователей. Это можно сделать по [данной инструкции](#). Настройку авторизации с помощью сертификатов можно воспроизвести по [этой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

Для пользователей Linux

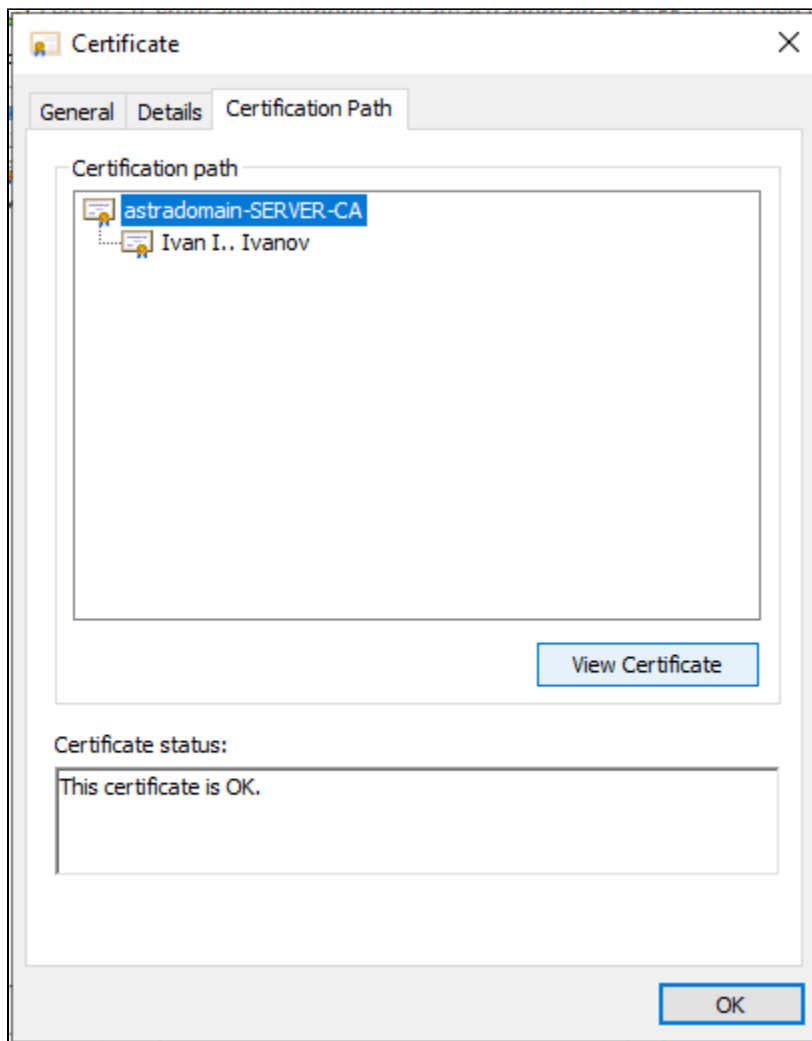


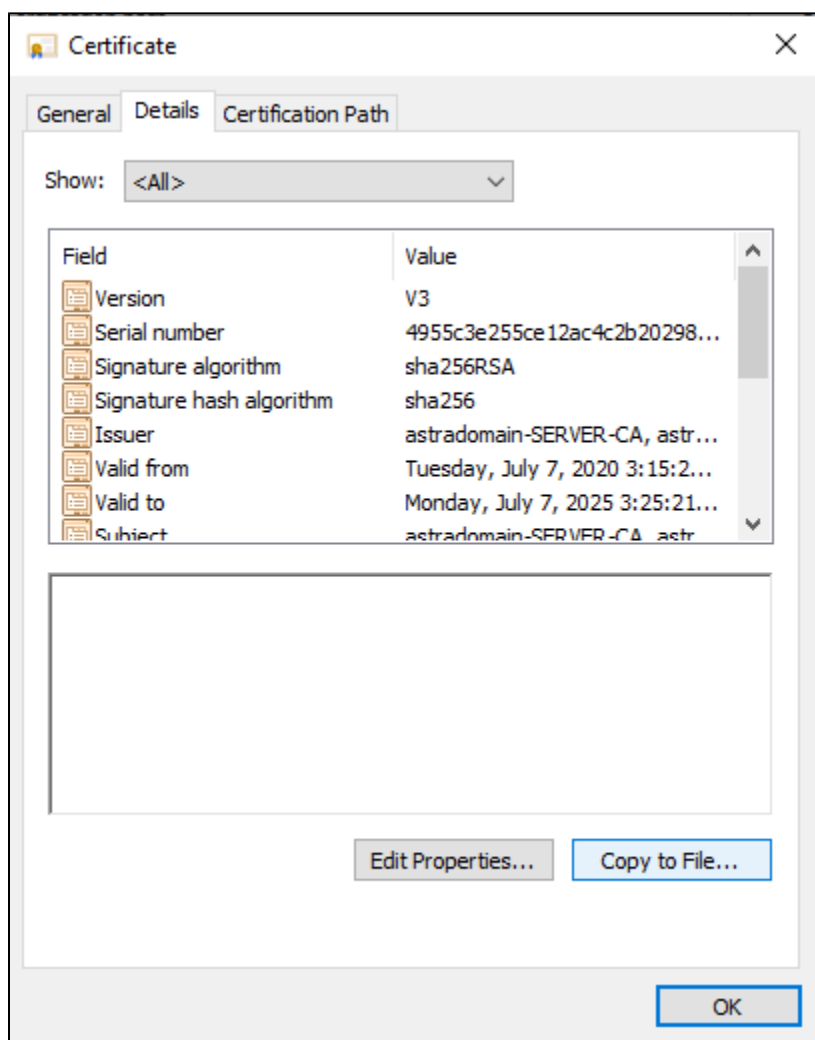
Для аутентификации пользователей через linux машины. Помимо токенов с ключами и сертификатов пользователей, вам также необходимо направить им корневой сертификат УЦ.

Его можно получить здесь:



Certification Authority (Local)		Request ID	Requester Name	Binary Certificate	Certificate Template	Serial Number
astradomain-SERVER-CA	Revoked Certificates	2	ASTRADOMAIN\...	-----BEGIN CERTI...	Administrator (Admi...	79000000029d9...
	Issued Certificates	3	ASTRADOMAIN\...	-----BEGIN CERTI...	Enrollment Agent (E...	790000000033fa...
	Pending Requests	4	ASTRADOMAIN\...	-----BEGIN CERTI...	Rutoken User (1.3.6.1...	7900000000448c...
	Failed Requests	5	ASTRADOMAIN\ad_user	BEGIN CERTI...	Rutoken User (1.3.6.1...	79000000005143...





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 следующим 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
```

```
[lolol@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 работы:

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

```
# pcsd ,
sudo systemctl restart pcsd

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

```
[lolol@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

```
[lolol@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/sss/sss.conf**. Он должен выглядеть примерно следующим образом:

/etc/sss/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
#   ECU
#   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
```

```
[lolol@redosclie ~]$ kinit user
Rutoken ECP <no label>          PIN:
[lolol@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
[lolol@redosclie ~]$ kdestroy
```

Попытка аутентификации по смарт-карте

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

Аутентификация пользователя user

```
su user
```

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

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
...
```

Аутентификация через гритер

Проверьте аутентификацию через гритер через лок скрин.

Ср, 11:28



ru ▾



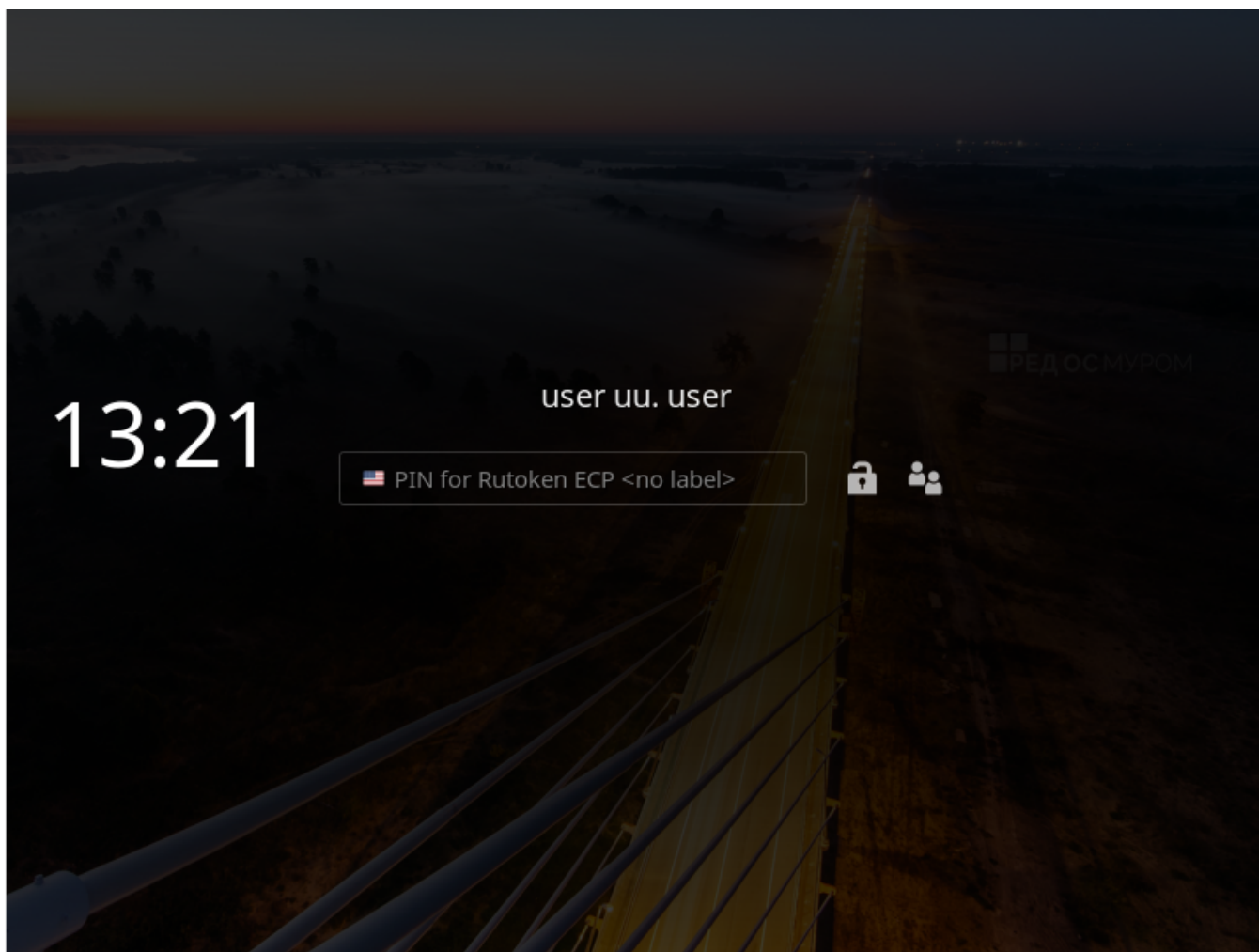
user uu. user

PIN for Rutoken ECP <no label>

Отмена

Разблокировать





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.

Сессии...

Введите пароль





EN

CapsLock Выкл.

