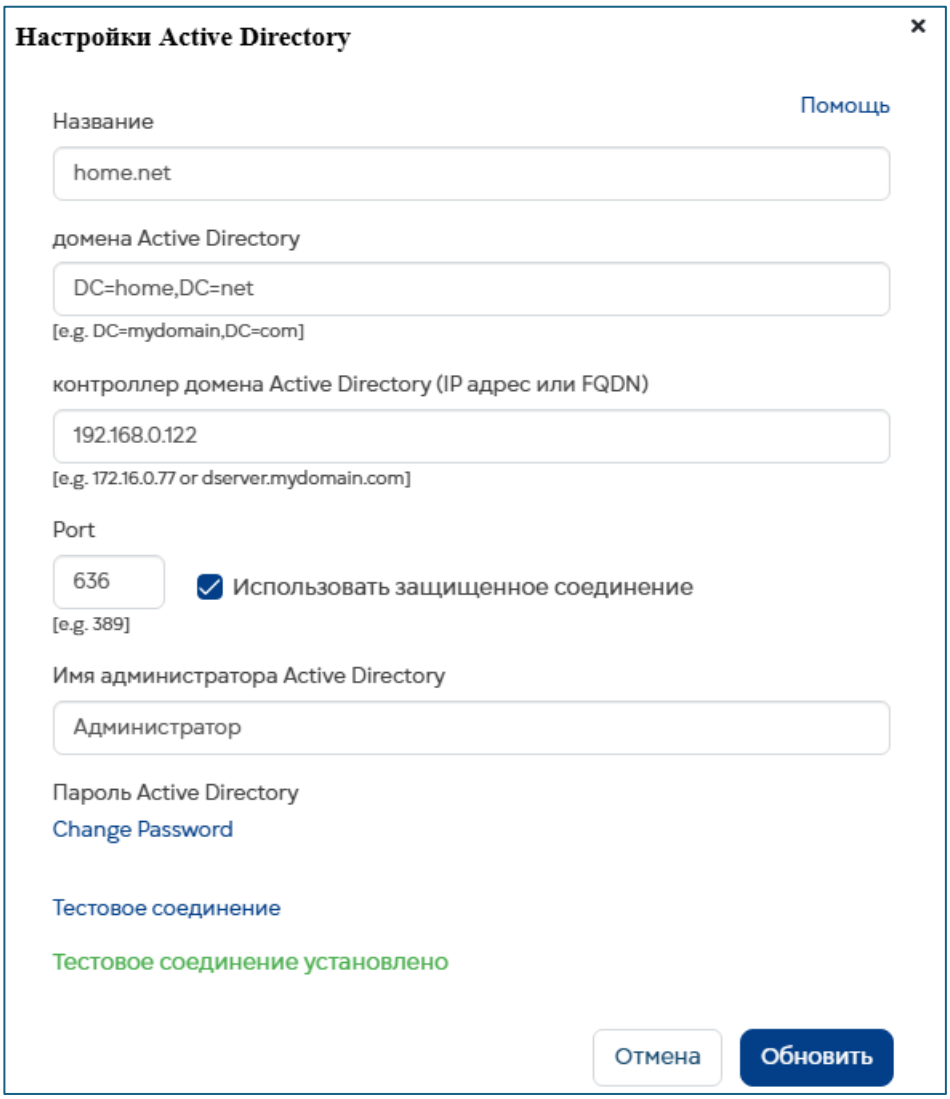
Использовать защищенное соединение при подключении к Active Directory



Для успешной синхронизации с Active Directory с использованием защищенного соединения необходимо сделать предварительные настройки LDAPS:

Настройка LDAPS на контроллере домена Windows Server

1. Исходные данные

Для примера используется следующая конфигурация:

Параметр	Значение
Домен	home.net
Контроллер домена	dc1.home.net
IP-адрес DC	192.168.0.122
Тестовый компьютер	192.168.0.159
LDAPS	TCP 636
Центр сертификации	home-DC1-CA
Шаблон сертификата	«Проверка подлинности домена»

Цель настройки — обеспечить подключение к Active Directory через **LDAPS (LDAP over SSL/TLS)** по порту **636**.

2. Первичная проверка порта LDAPS

Перед настройкой сертификата необходимо проверить доступность TCP-порта 636 с компьютера, который будет подключаться к контроллеру домена.

На компьютере 192.168.0.159 открыть **PowerShell от имени администратора** и выполнить:

```
Test-NetConnection dc1.home.net -Port 636
```

Необходимо проверить параметр:

TcpTestSucceeded : True

Если значение True, TCP-порт 636 доступен.

Важно: успешная проверка TCP 636 ещё не означает, что LDAPS полностью работает. Необходимо также проверить TLS-соединение и сертификат контроллера.

3. Проверка наличия сертификата на контроллере домена

На контроллере dc1.home.net открыть PowerShell от имени администратора и выполнить:

```
Get-ChildItem Cert:\LocalMachine\My
```

Необходимо проверить наличие сертификата, предназначенного для использования контроллером домена.

Если подходящий сертификат отсутствует, необходимо установить и настроить **Службы сертификатов Active Directory (AD CS)**.

4. Установка Служб сертификатов Active Directory

На контроллере домена открыть:

Диспетчер серверов → Управление → Добавить роли и компоненты

или:

Server Manager → Manage → Add Roles and Features

Тип установки

Выбрать:

Установка ролей или компонентов

Role-based or feature-based installation

Нажать **Далее**.

Выбор сервера

Выбрать контроллер домена:

dc1.home.net

Нажать **Далее**.

5. Выбор роли AD CS

В списке ролей установить флажок:

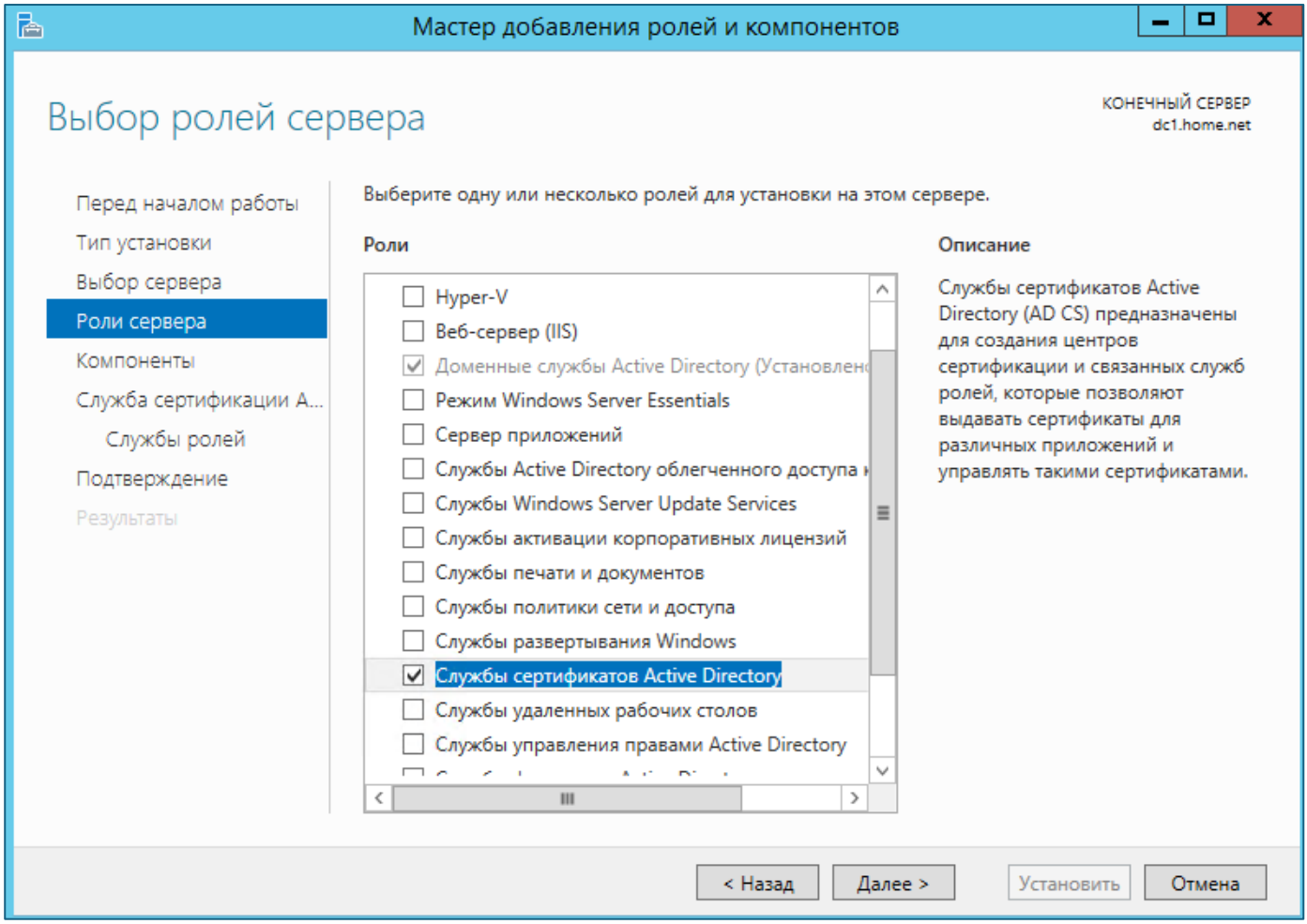
Службы сертификатов Active Directory

или:

Active Directory Certificate Services

При появлении запроса на добавление необходимых компонентов подтвердить установку.

Нажать **Далее**.



6. Выбор службы роли

На странице **Службы ролей** выбрать:

☑ **Центр сертификации**

или:

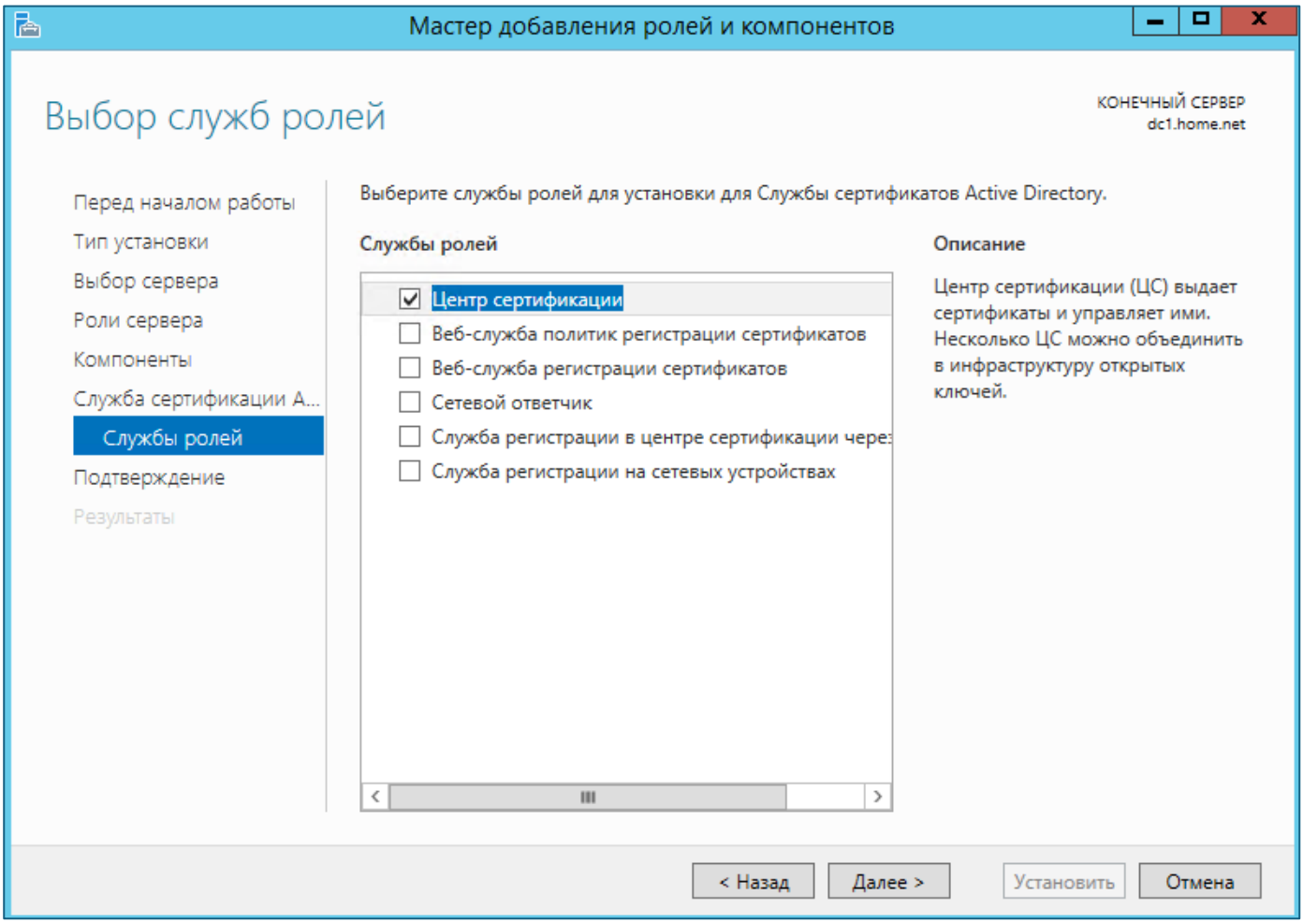
Certification Authority

Для данной настройки остальные службы AD CS устанавливать не требуется.

Необходимо нажать:

Далее → Установить

После завершения установки перейти к настройке AD CS.



7. Настройка центра сертификации

В **Диспетчере серверов** открыть уведомление и выбрать:

Настроить службы сертификатов Active Directory на сервере назначения

или:

Configure Active Directory Certificate Services on the destination server

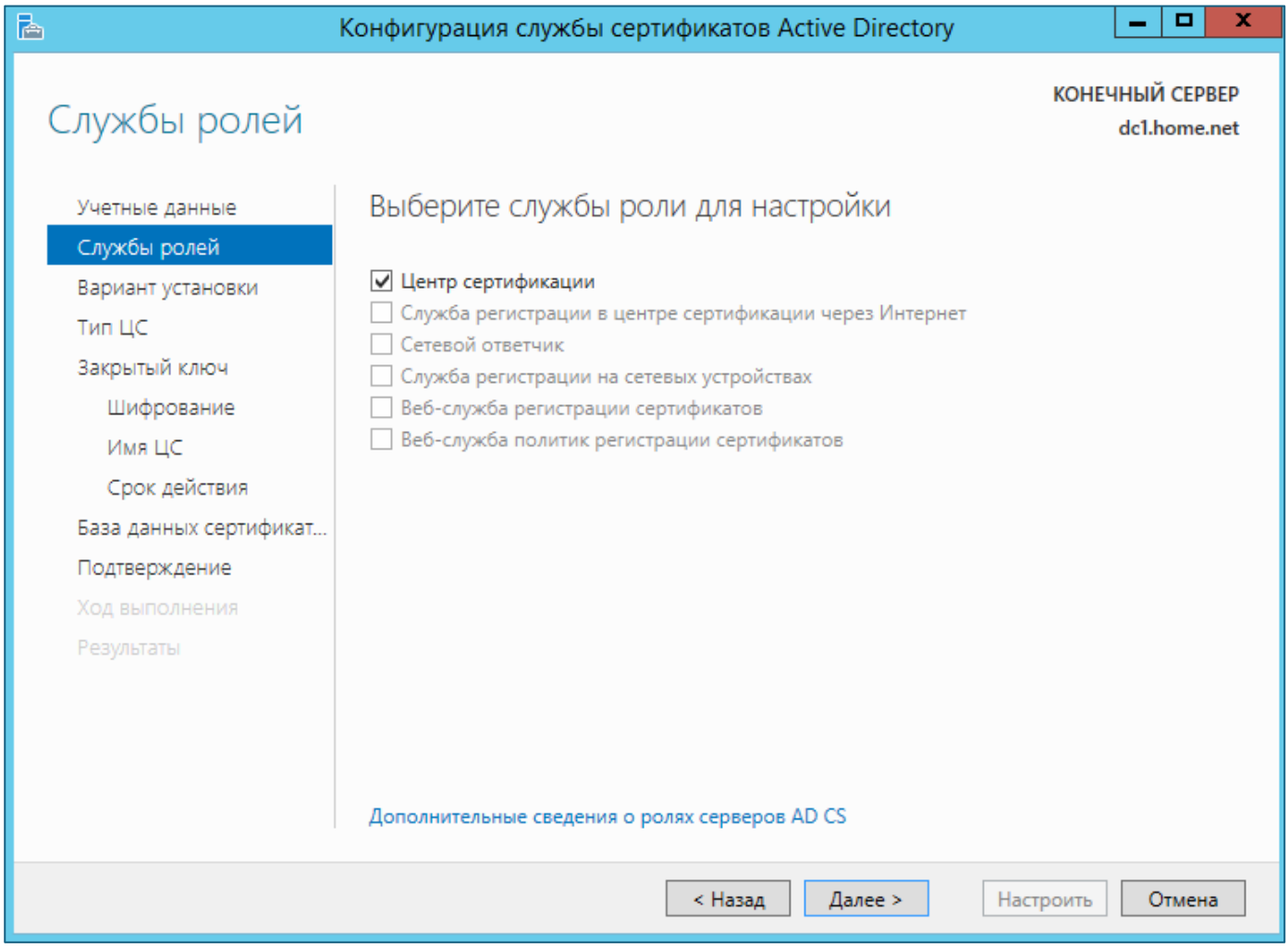
Откроется мастер настройки AD CS.

8. Выбор службы роли

На странице выбора служб ролей оставить:

☑ **Центр сертификации**

Нажать **Далее**.



9. Выбор типа установки CA

Поскольку центр сертификации должен использоваться в существующем домене Active Directory, выбрать:

Корпоративный центр сертификации

или:

Enterprise CA

Нажать **Далее**.

10. Выбор типа центра сертификации

Если в инфраструктуре ещё отсутствует собственный центр сертификации, выбрать:

Корневой центр сертификации

или:

Root CA

Нажать **Далее**.

11. Создание закрытого ключа

Выбрать:

Создать новый закрытый ключ

или:

Create a new private key

Параметры криптографии оставить рекомендованными мастером, если нет специальных требований.

Нажать **Далее**.

12. Имя центра сертификации

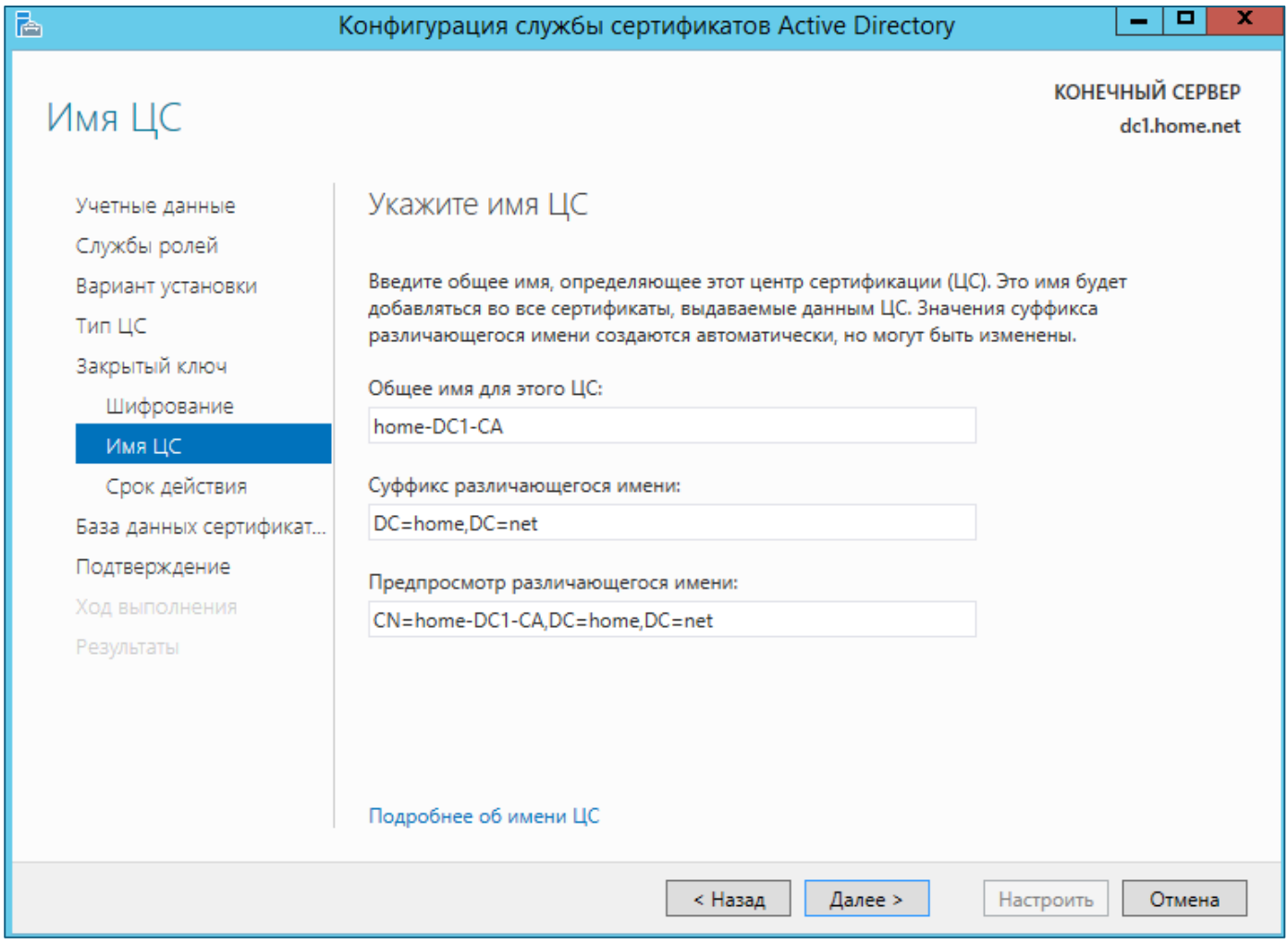
В качестве имени центра сертификации можно использовать:

home-DC1-CA

После настройки конфигурация CA будет иметь вид:

dc1.home.net\home-DC1-CA

Завершить работу мастера настройки.



13. Проверка работы службы Certification Authority

После настройки AD CS необходимо проверить состояние службы.

На контроллере домена выполнить:

```
Get-Service CertSvc
```

Необходимо получить:

Status Name DisplayName

------ ---- -----------

Running CertSvc Службы сертификации Active Directory

Если служба находится в состоянии Running, центр сертификации запущен.

14. Проверка конфигурации CA

Для определения имени настроенного центра сертификации выполнить:

```
certutil -getconfig
```

Необходимо получить строку вида:

Строка настройки: "dc1.home.net\home-DC1-CA"

15. Запрос сертификата для контроллера домена

Для получения сертификата необходимо использовать хранилище сертификатов локального компьютера.

На dc1.home.net выполнить:

```
certlm.msc
```

Откроется оснастка:

Сертификаты — локальный компьютер

или:

Certificates - Local Computer

Перейти:

Личное → Сертификаты

или:

Personal → Certificates

16. Запуск запроса нового сертификата

В разделе **Сертификаты** нажать правой кнопкой мыши:

Все задачи → Запросить новый сертификат

или:

All Tasks → Request New Certificate

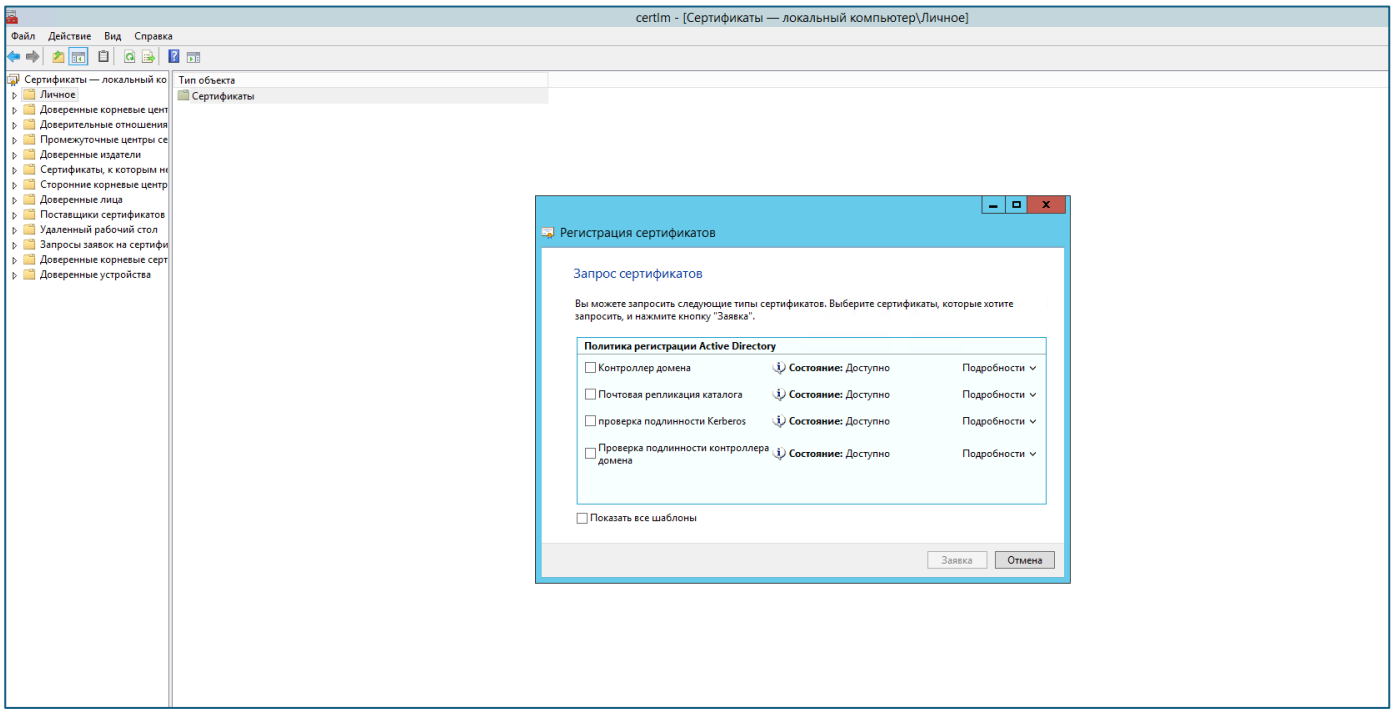
В мастере выбрать:

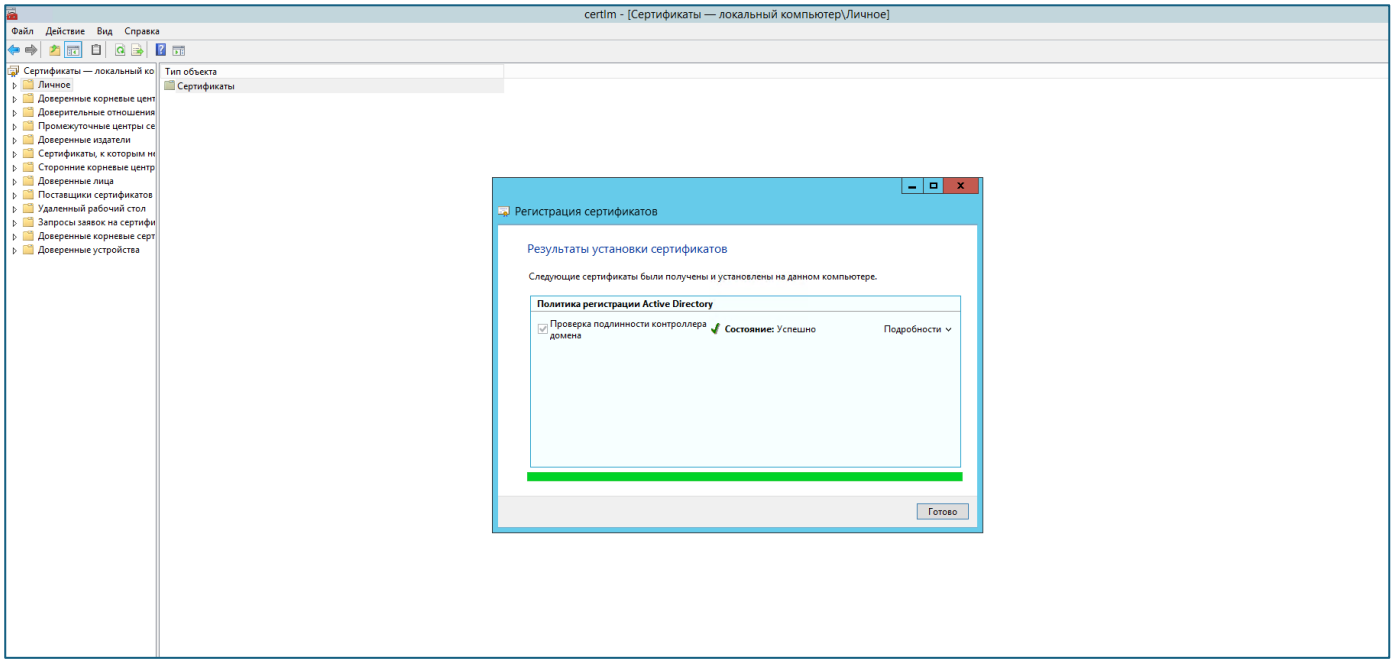
Политика регистрации Active Directory

или:

Active Directory Enrollment Policy

Нажать **Далее**.





17. Выбор шаблона сертификата

В списке доступных шаблонов необходимо выбрать:

Проверка подлинности домена

или:

Domain Controller Authentication

Данный сертификат предназначен для аутентификации контроллера домена и может использоваться для LDAPS.

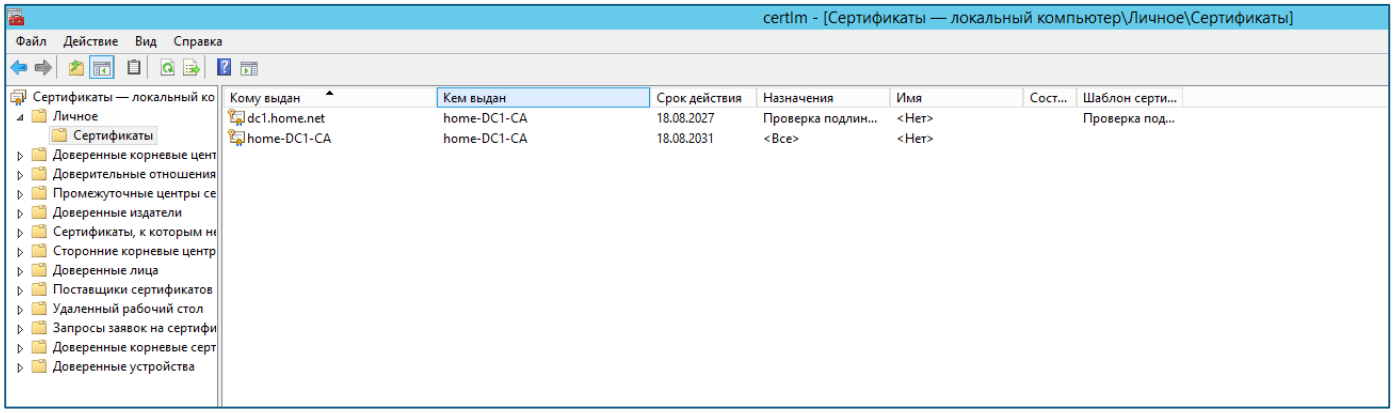
Нажать:

Зарегистрировать / Enroll

После успешной регистрации сертификат должен появиться в:

Личное → Сертификаты

локального компьютера.



18. Проверка сертификата

На контроллере домена выполнить:

```
Get-ChildItem Cert:\LocalMachine\My |
Format-List Subject,Issuer,NotBefore,NotAfter,Thumbprint,EnhancedKeyUsageList
```

Необходимо найти сертификат, выданный центром:

CN=home-DC1-CA, DC=home, DC=net

Для LDAPS сертификат должен иметь назначение:

Server Authentication

OID:

1.3.6.1.5.5.7.3.1

19. Проверка имени контроллера в сертификате

Необходимо проверить, что сертификат содержит DNS-имя контроллера:

dc1.home.net

Для этого найти сертификат по отпечатку:

```
Get-ChildItem Cert:\LocalMachine\My |
Where-Object Thumbprint -eq "63D11439E23B581CB841C422F9ADAA35B98FB48C" |
Format-List Subject,Issuer,DnsNameList,HasPrivateKey,EnhancedKeyUsageList
```

В результате необходимо убедиться в наличии:

DnsNameList : {dc1.home.net}

HasPrivateKey : True

Также необходимо убедиться, что в EnhancedKeyUsageList присутствует:

Проверка подлинности сервера

или:

Server Authentication

20. Проверка LDAPS через TLS

После установки подходящего сертификата необходимо проверить TLS-соединение с компьютера 192.168.0.159.

OpenSSL для этого не требуется.

На компьютере 159 выполнить одной строкой:

```
$tcp=New-Object System.Net.Sockets.TcpClient("dc1.home.net",636); $ssl=New-Object
System.Net.Security.SslStream($tcp.GetStream(),$false,({$true}));
$ssl.AuthenticateAsClient("dc1.home.net"); $ssl.RemoteCertificate | Format-List
Subject,Issuer,NotBefore,NotAfter,Thumbprint
```

Если TLS работает корректно, команда должна выполниться **без ошибки**, а в результате должен отображаться сертификат, выданный:

home-DC1-CA

21. Проверка TCP-порта 636

Дополнительно необходимо выполнить:

```
Test-NetConnection dc1.home.net -Port 636
```

Ожидаемый результат:

TcpTestSucceeded : True

22. Проверка подключения к Active Directory через LDAPS

Для проверки непосредственно LDAP-подключения необходимо выполнить:

```
$cred = New-Object System.Net.NetworkCredential("Администратор","ПАРОЛЬ","HOME")
$entry = New-Object System.DirectoryServices.DirectoryEntry(
    "LDAP://dc1.home.net/DC=home,DC=net",
    $cred.UserName,
    $cred.Password,
    [System.DirectoryServices.AuthenticationTypes]::SecureSocketsLayer
```

)

```
$entry.NativeObject
```

Команда должна завершиться **без ошибки**.

Данная проверка подтверждает подключение к Active Directory с использованием SSL.

23. Итоговая проверка

После выполнения всех этапов необходимо убедиться в следующем:

Проверка	Ожидаемый результат
AD CS установлен	Да
CertSvc	Running
CA	home-DC1-CA
Сертификат DC	Есть
DNS сертификата	dc1.home.net
Закрытый ключ	True
Server Authentication	Есть
TCP 636	True
TLS handshake	Успешный
LDAPS DirectoryEntry	Без ошибки

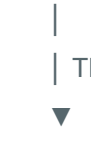
Итог

После выполнения описанных действий контроллер домена dc1.home.net должен предоставлять доступ к Active Directory через **LDAPS на TCP-порту 636**.

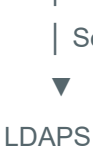
Рабочая схема:

Компьютер 159

dc1.home.net



Сертификат dc1.home.net



LDAPS

Active Directory

home.net

Примечание: для рабочей инфраструктуры с несколькими контроллерами домена аналогичный сертификат необходимо обеспечить на каждом DC, который должен принимать LDAPS-подключения.