SafeDNS AD Agent environment configuration

The manual below describes the whole process of the preparation, configuration, and installation of the Agent under the Active Directory environment. The user operating system used is Windows 11 while the server version OS: Windows Server 2019 Standard.

Prerequisites: fresh installed Windows Server 2019 Standard, fresh installed Windows 11

Important Notice:

I: If the Active Directory is already installed and configured, while the Group Policy Management is not configured, please proceed with the installation of the Group Policy Management.

II: If the Active Directory and Group Policy Management are already installed and configured, please proceed to step 3 - Creating Users/Groups.

III: If the Active Directory and Group Policy Management are already installed and configured and Users/Groups exist, please proceed to step 4 - MSI File Preparation on the Server

Installing Agent in the AD environment without AD functionality

If you need to set up the Agent in the AD environment without using the AD functionality (e.g. adding AD users to SafeDNS Dashboard), you need the special build of the .msi file.

To get the special .msi build, please follow these steps:

1. Send the request for the .msi file to the Support (support@safedns.com) or your SafeDNS Manager.
   The request should contain username, password and PIN code.
   PIN code is required to enter the Agent GUI. If PIN is not provided, it will be generated randomly.
2. Wait until the .msi file is created and sent to you.

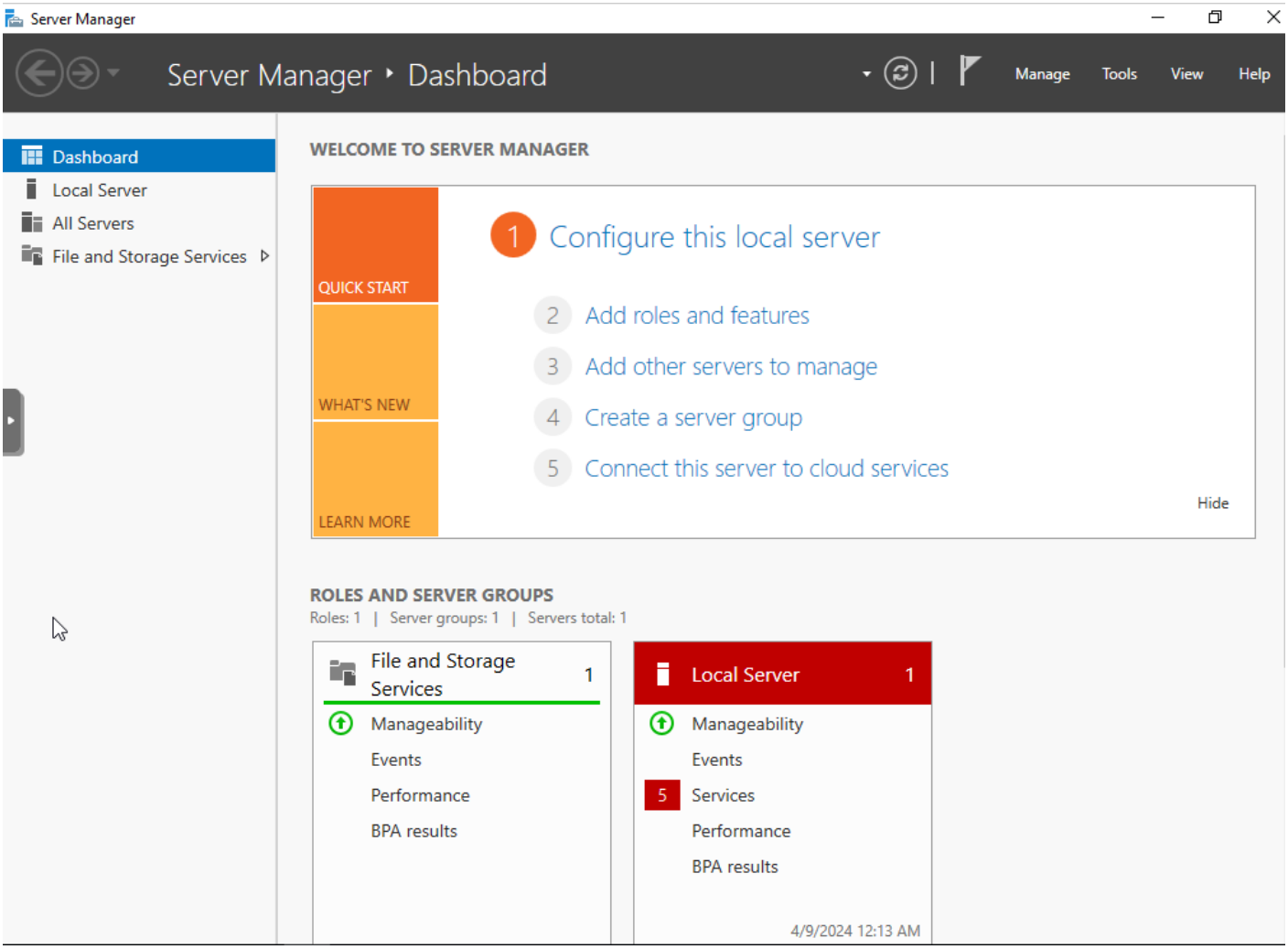
3. Upload the .msi file to the server and hosted in the folder that is available on the network to the end-user computer - we recommend setting the access level to Everyone.
4. Add the .msi file to the following path using the Group Policy Management console: **Computer Configuration > Policies > Software Settings > Software Installation**

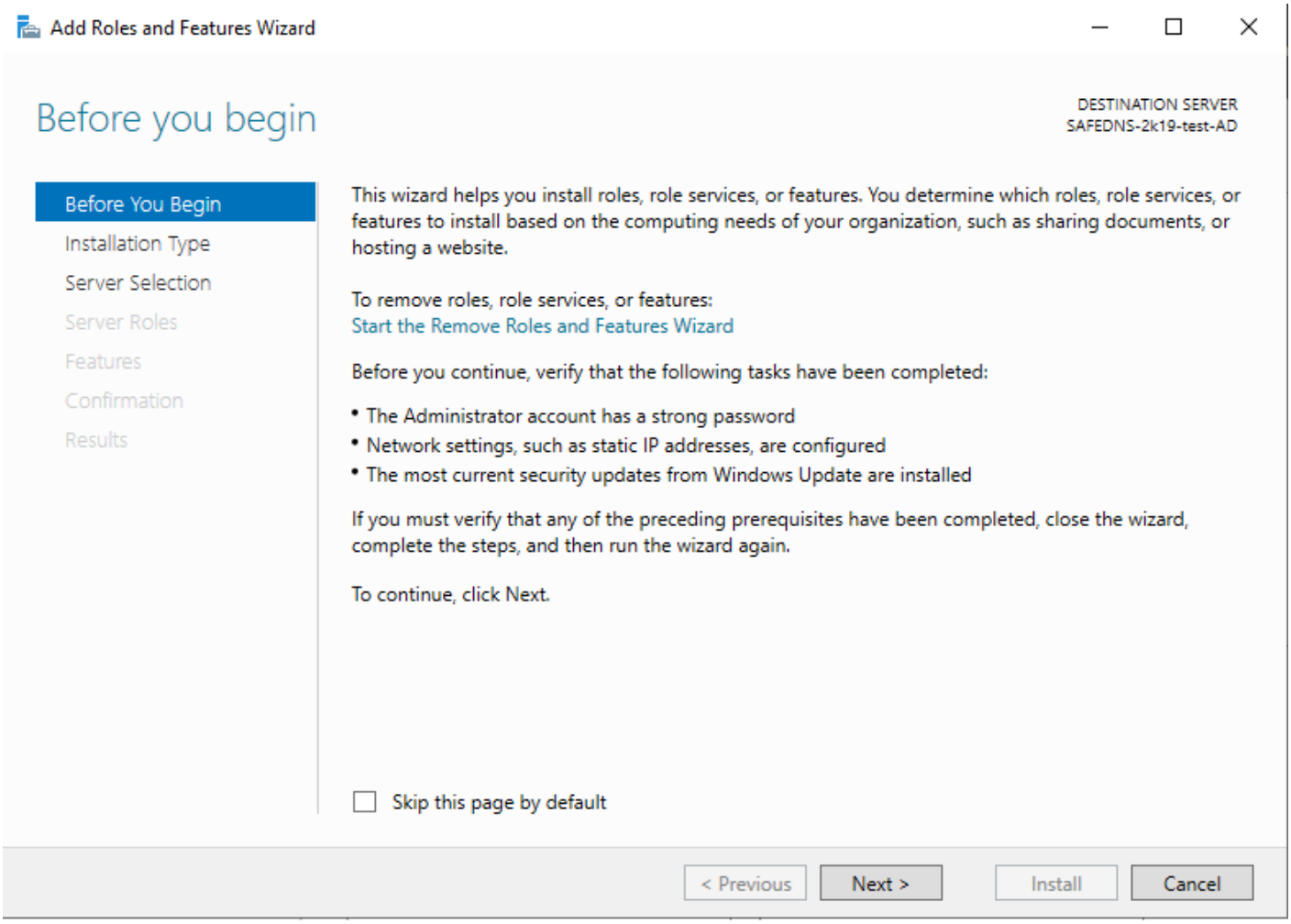
The .msi file installation will start after the end-user computer restart.
The installation can be forced by running the following command on the end-user computer: gpupdate /force

> This process for the NOAD agent installation follows exactly the same steps as described below. The only difference is that the NOAD agent uses credentials instead of an AD key and has the AD module disabled using the /noad key.

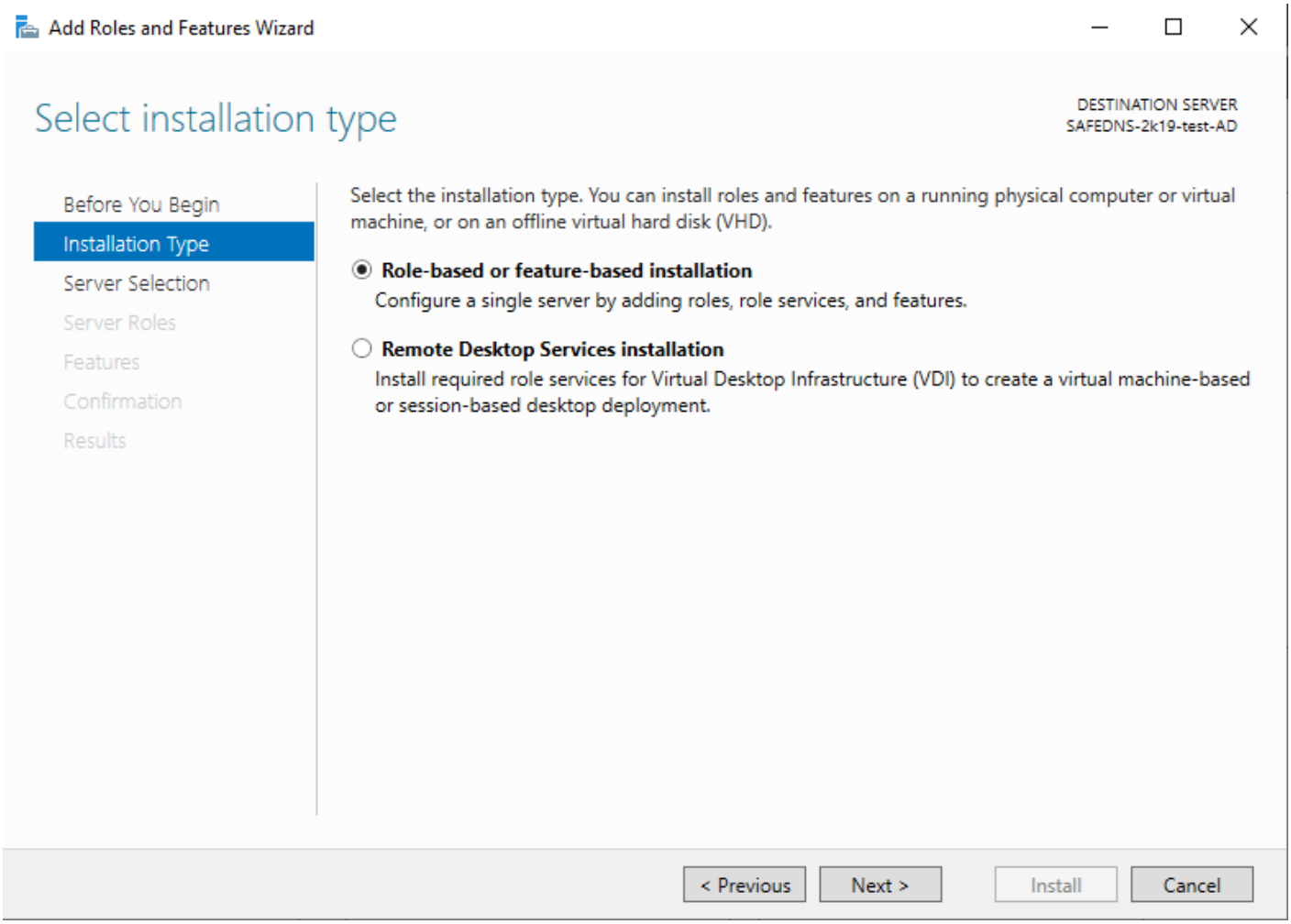
1. Server installation Part. Installation of the Roles and Features.

Start the Server Manager and initiate the installation of the Roles:

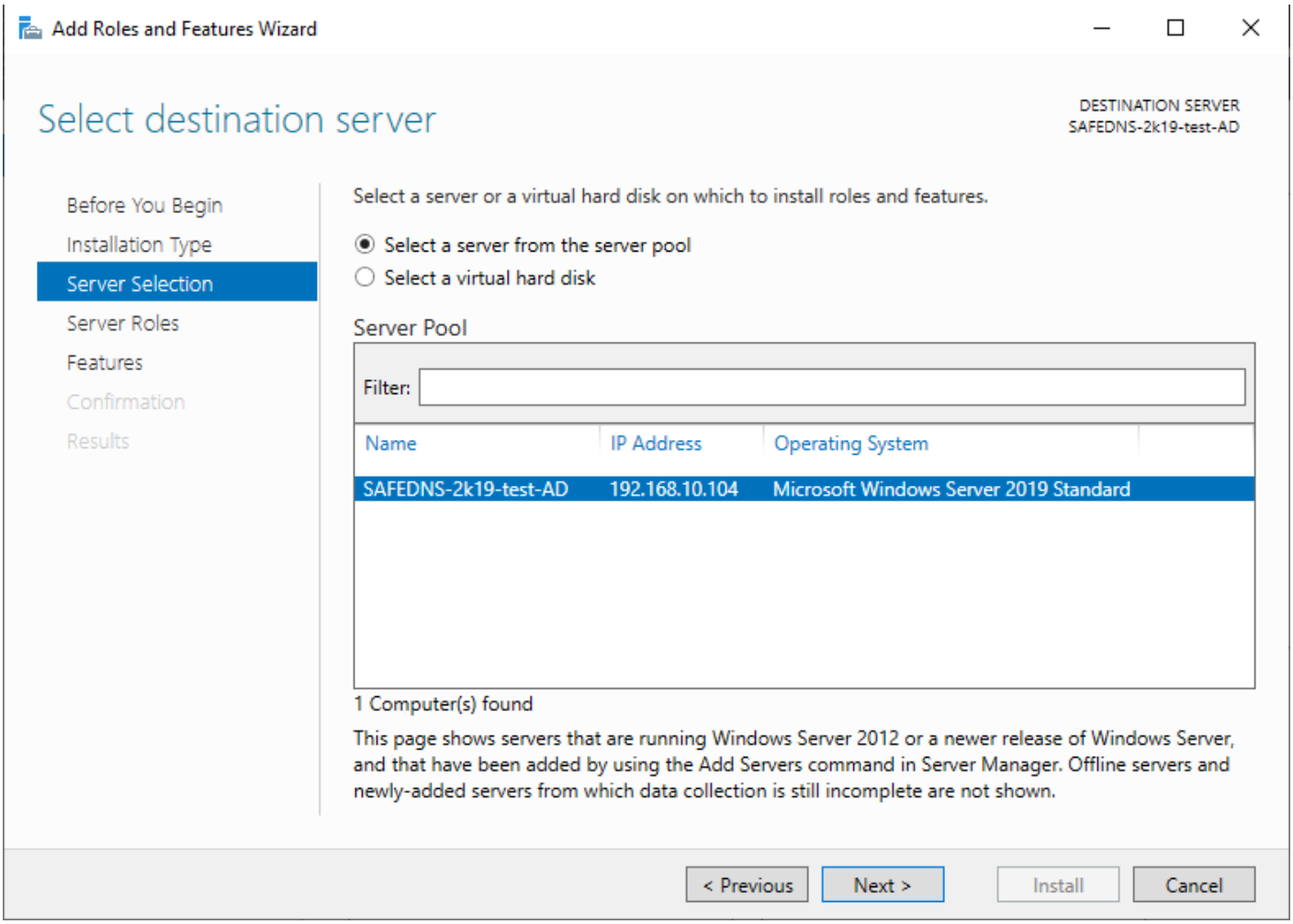

Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Services
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud services
Hide
ROLES AND SERVER GROUPS
Roles: 1 | Server groups: 1 | Servers total: 1
File and Storage Services 1
Manageability
Events
Performance
BPA results
Local Server 1
Manageability
Events
5 Services
Performance
BPA results
4/9/2024 12:13 AM



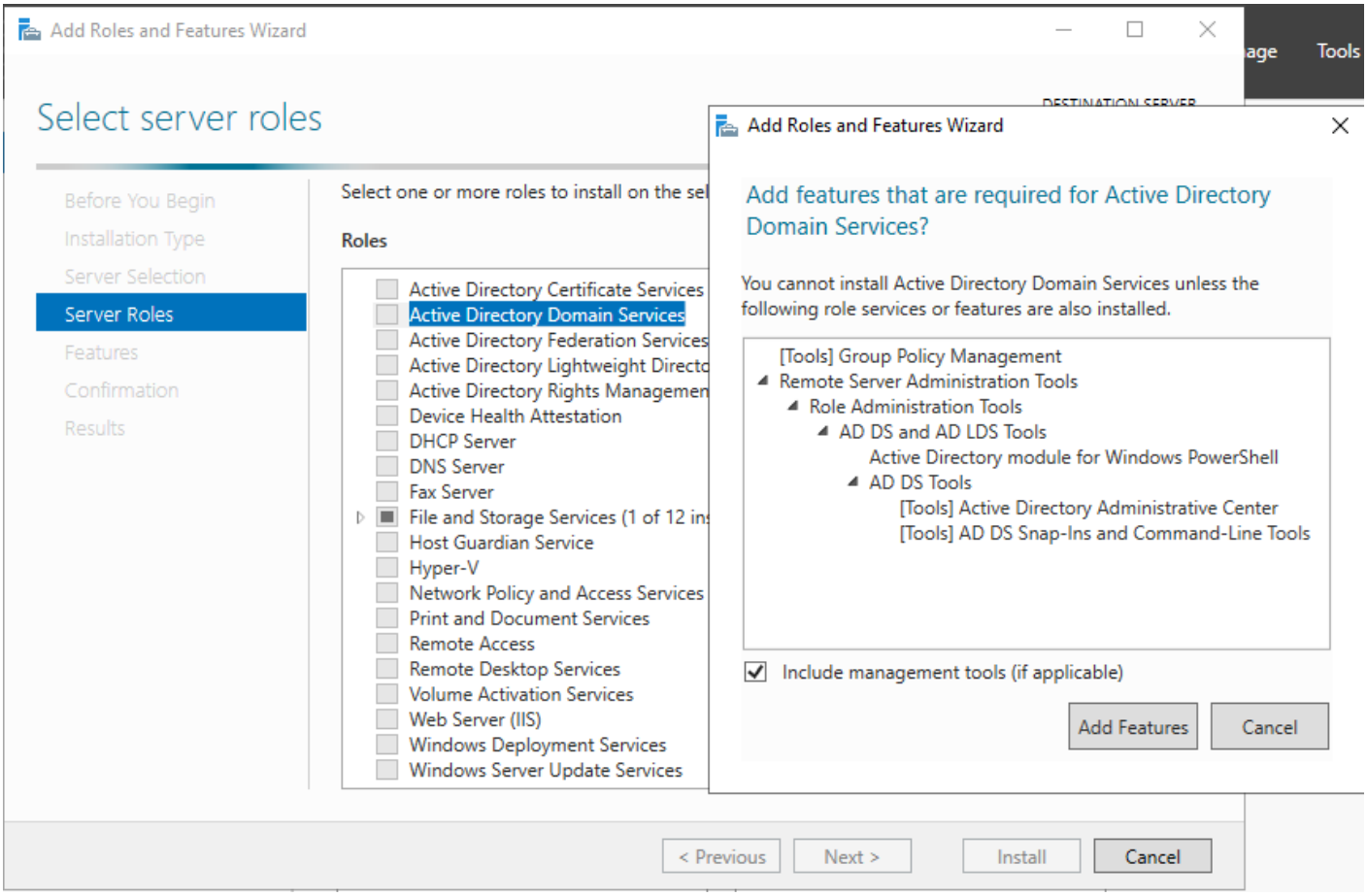
Selecting Role-based or feature-based installation:



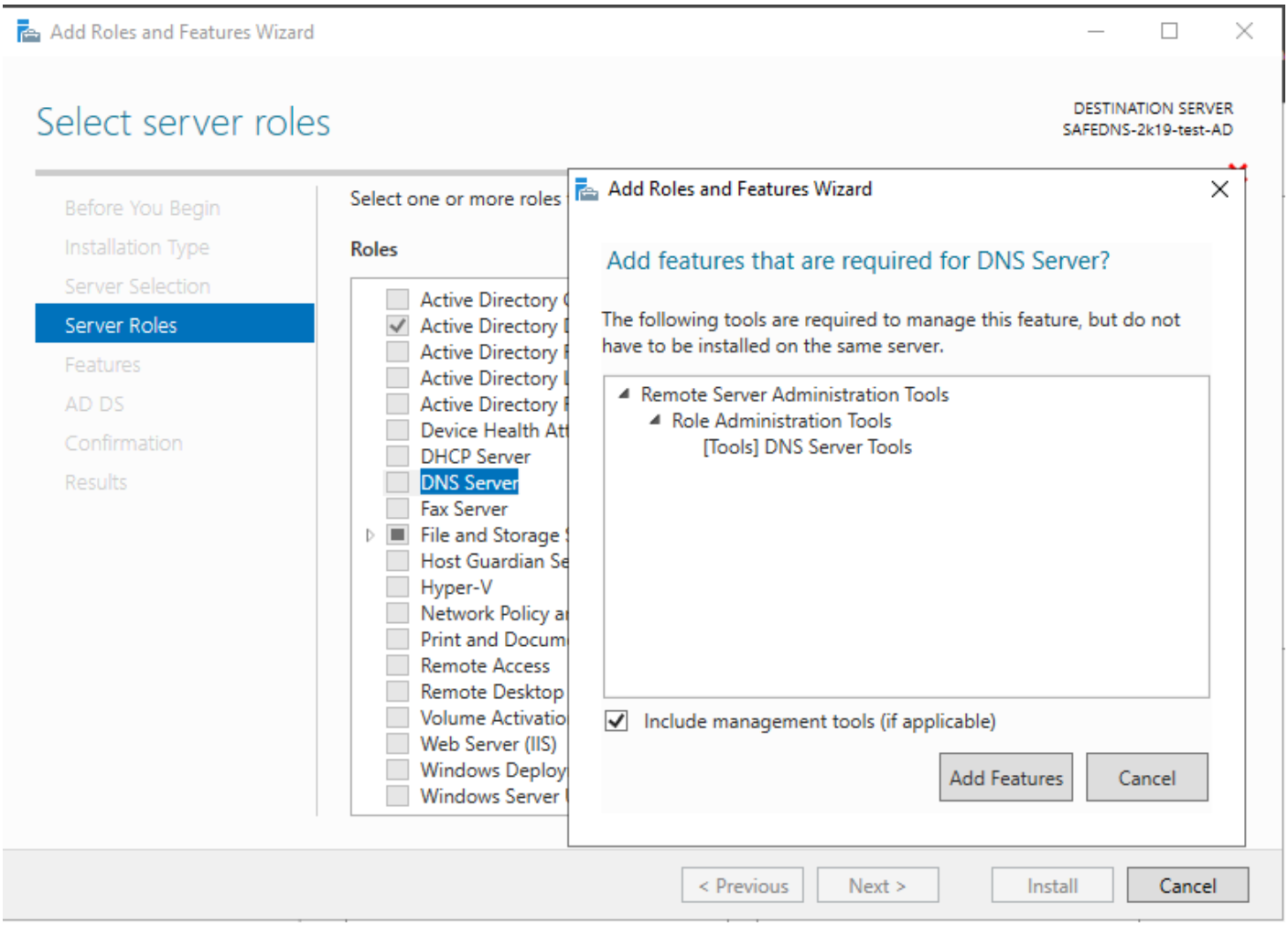
Selecting the local server from the Server Pool:



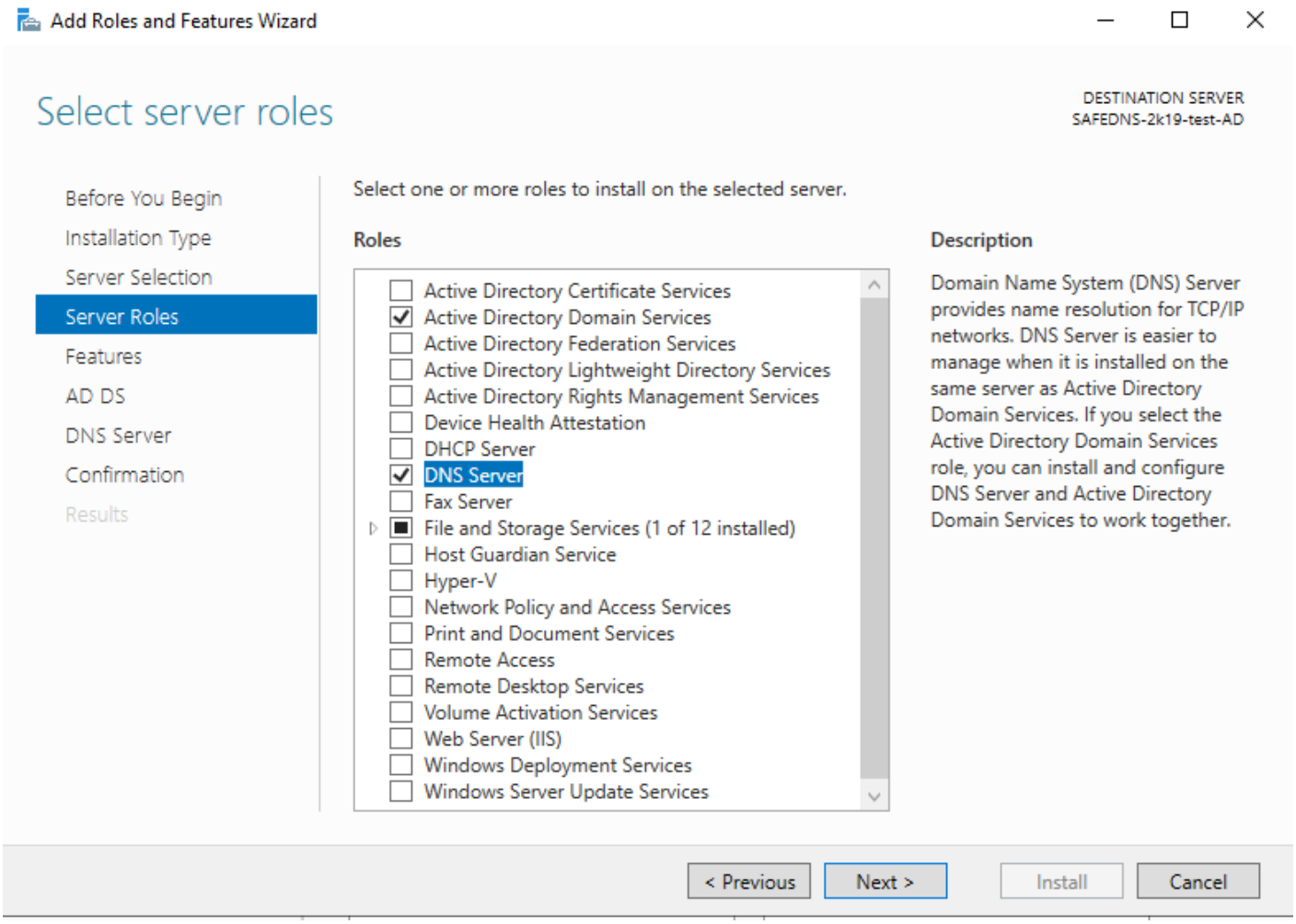
Selecting the Active Directory Domain Services role and in the small window taping the Add Features button:



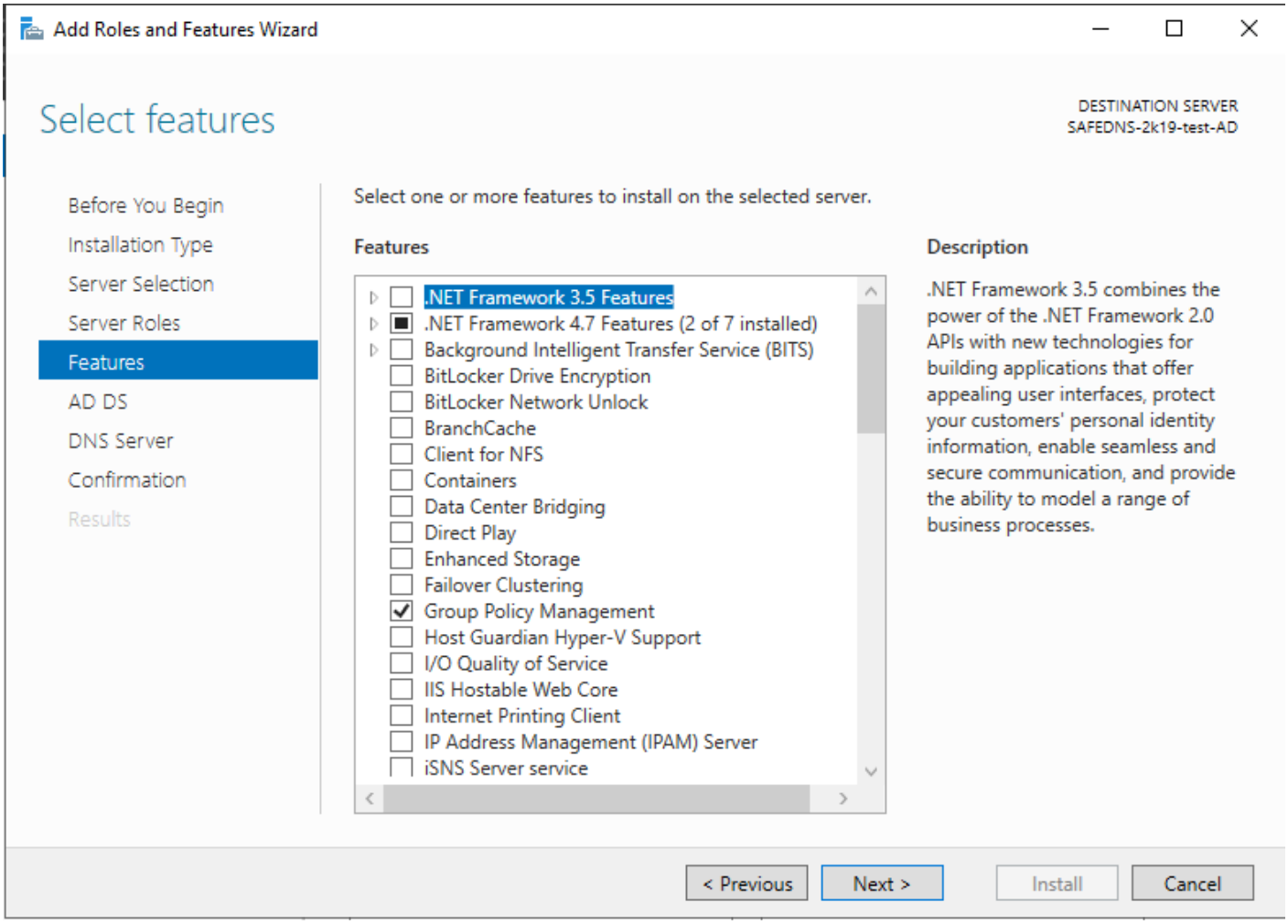
The next step is to select the Role of the DNS Server, accepting the proposed Features list:



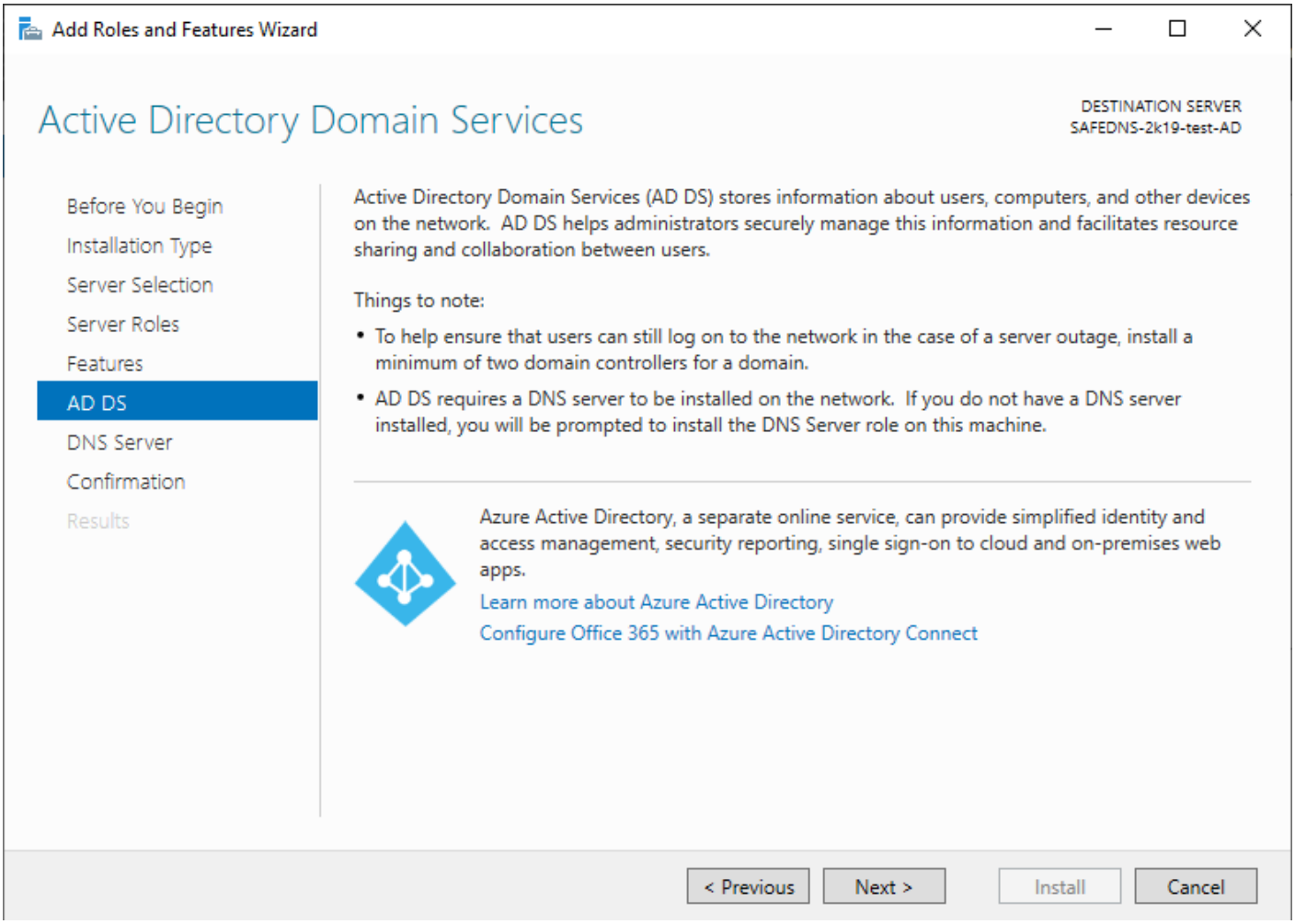
Accept the selected before Roles and tap the Next button:



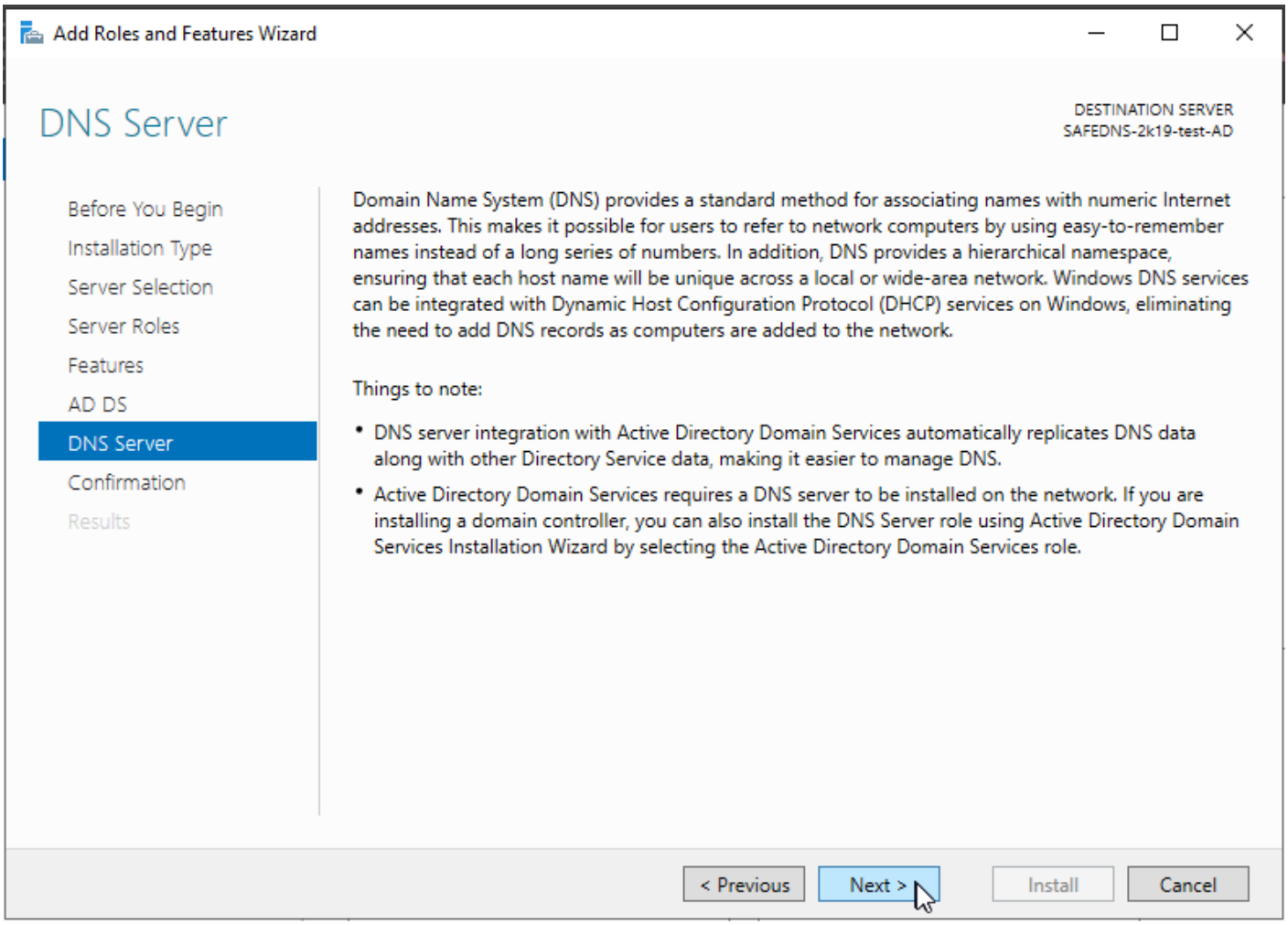
Select the Group Policy Management feature:



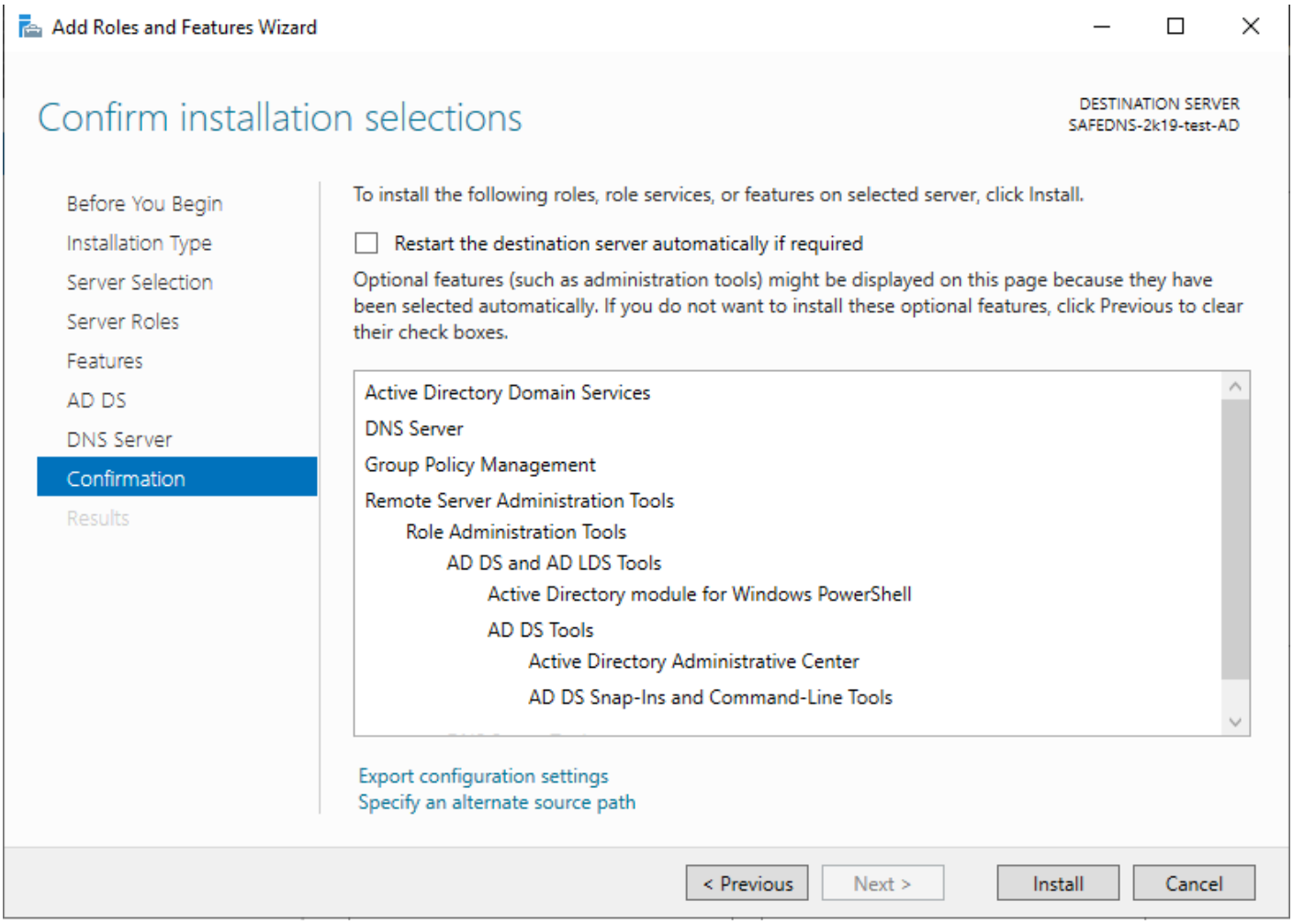
Brief information about Azure Active Directory Domain Services(promo):



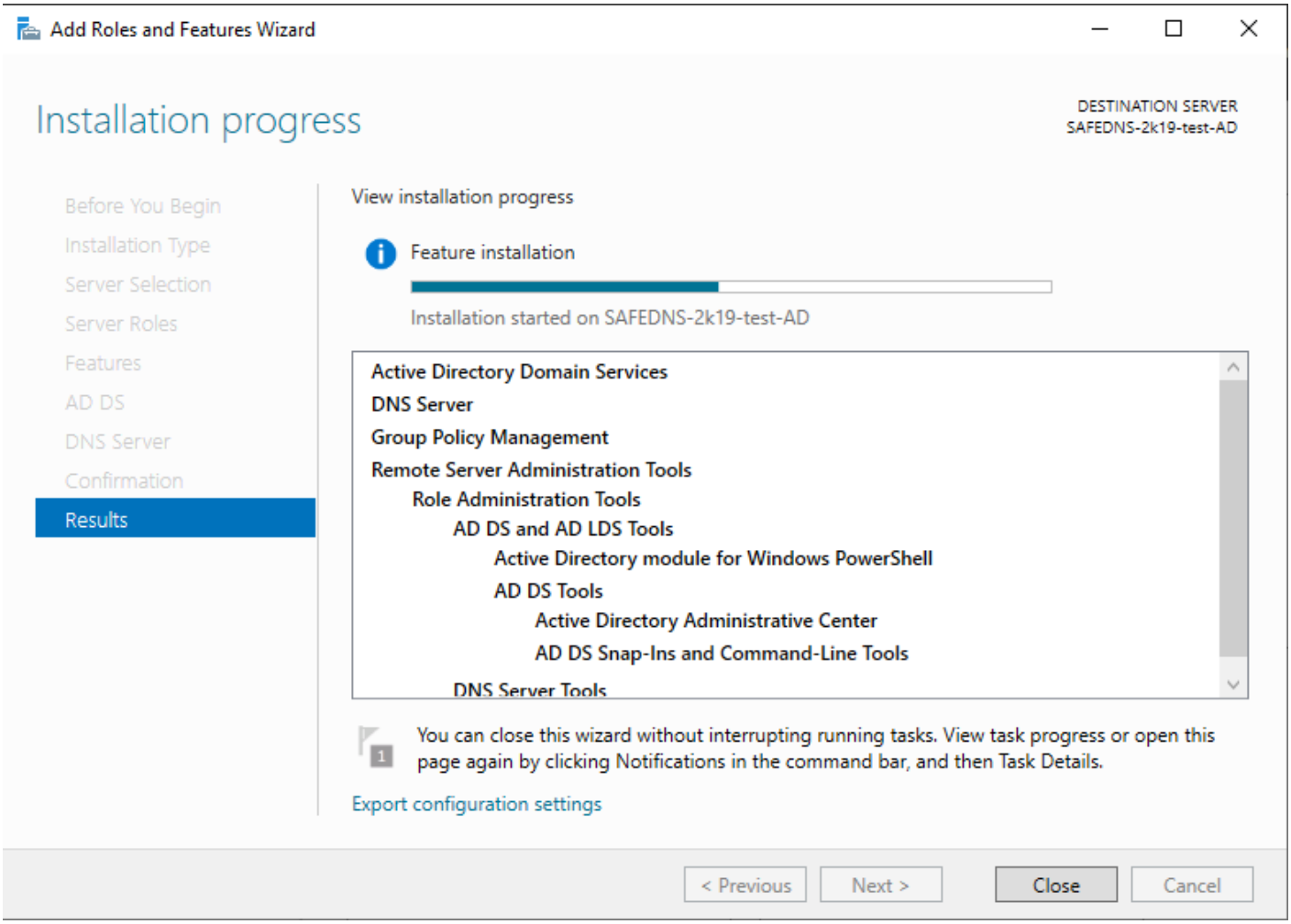
Brief information about installing DNS server:



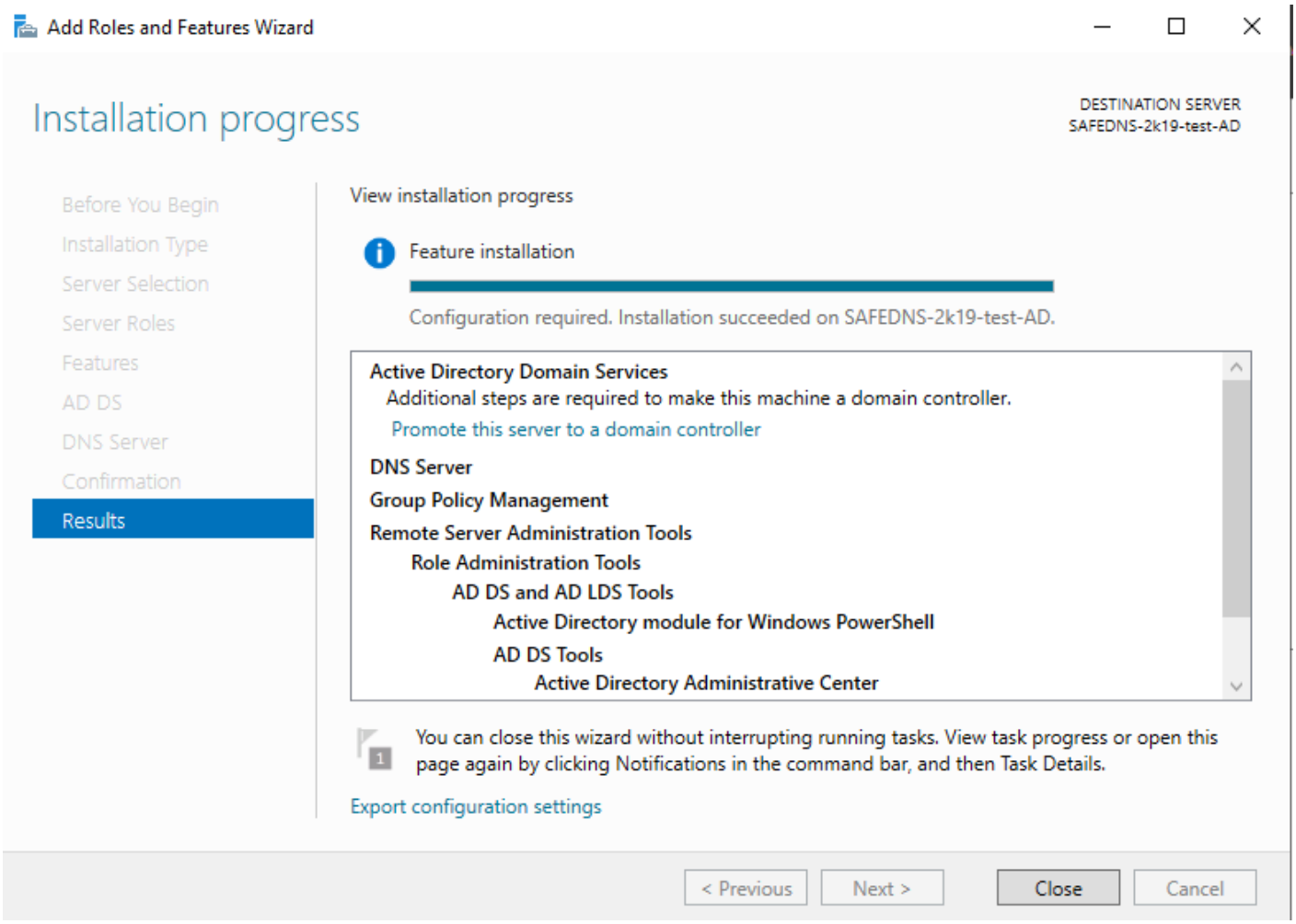
The summary with the list of installing Roles and Features:



The installtion process begins:



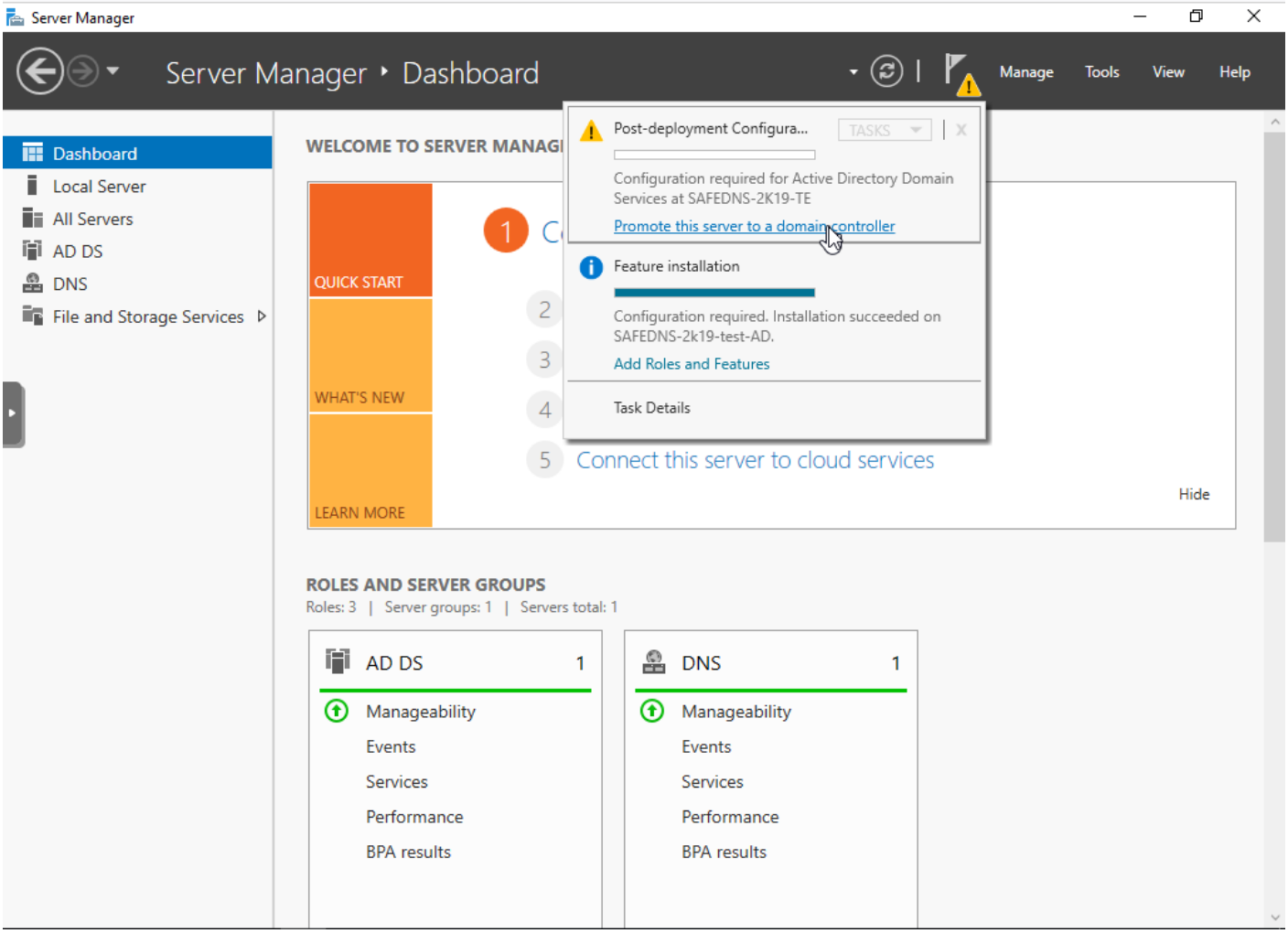
Once installed, the wizard shows the results of the installation:



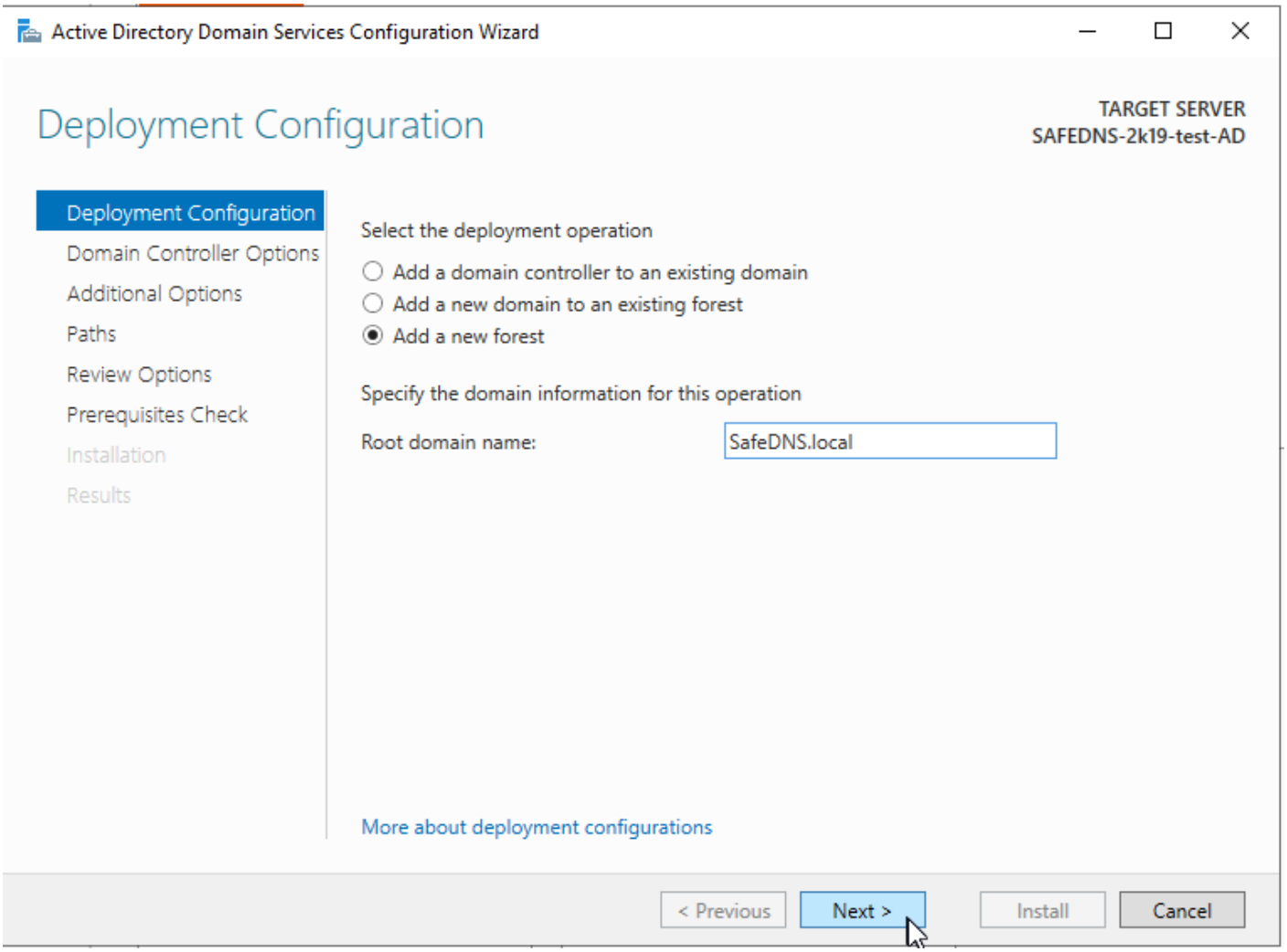
We are set with the installation of the Roles & Features. Please close the window.

2. Active Directory Configuration process.

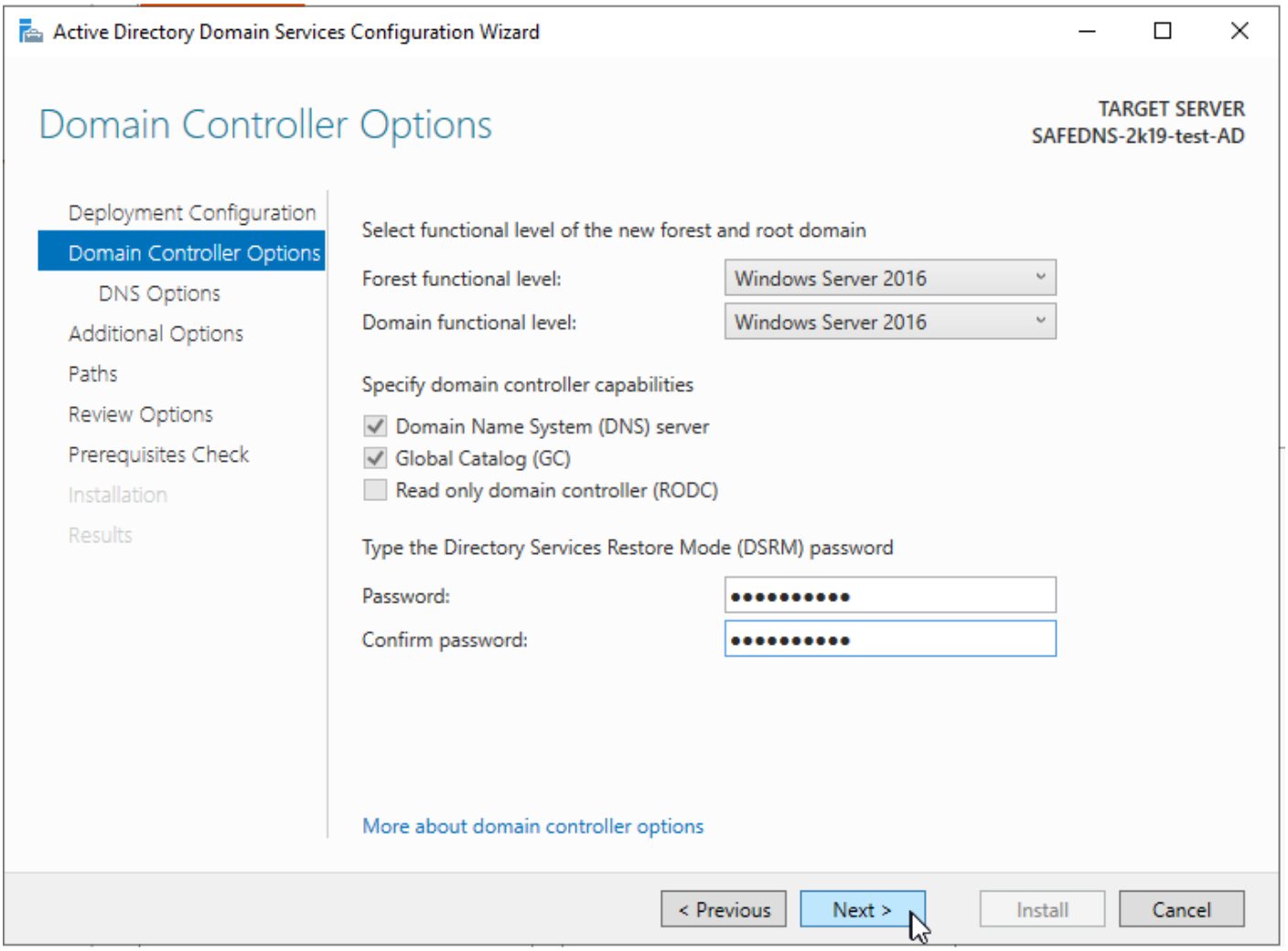
Start the Server Management and promote the server as a domain controller:



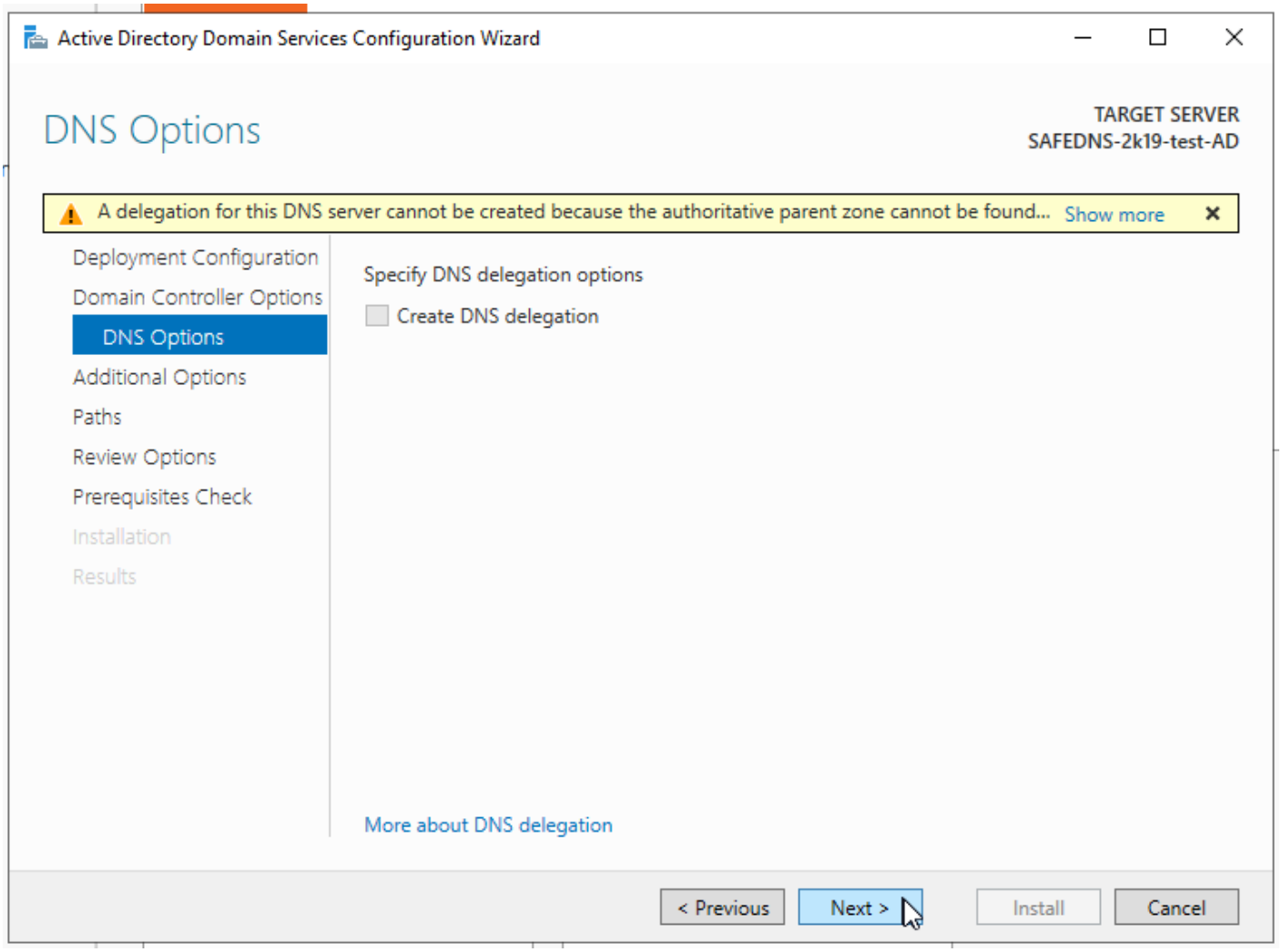
Creating a new forest and name it accordingly:



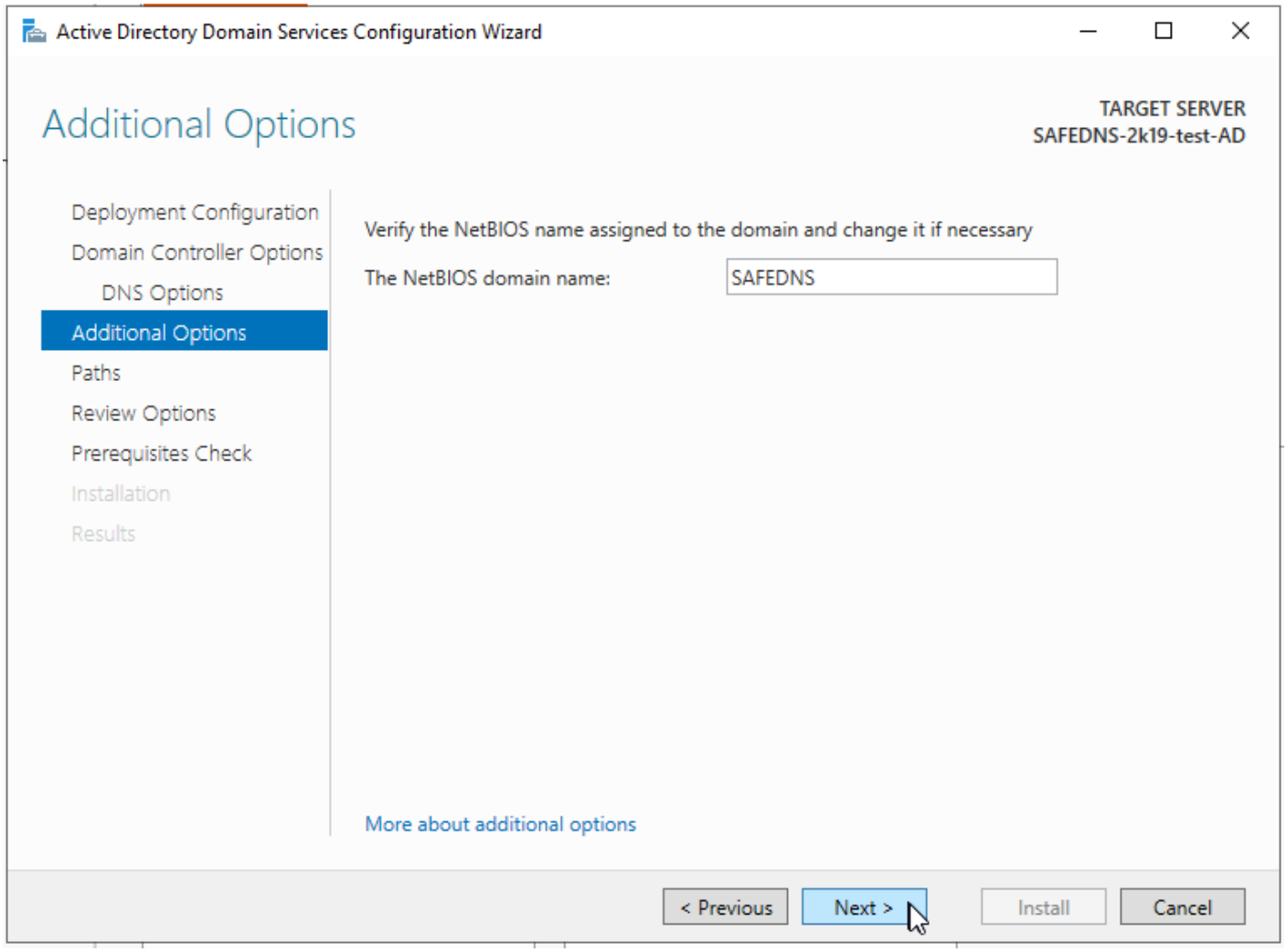
Leaving the options by default. Please set the DSRM password:



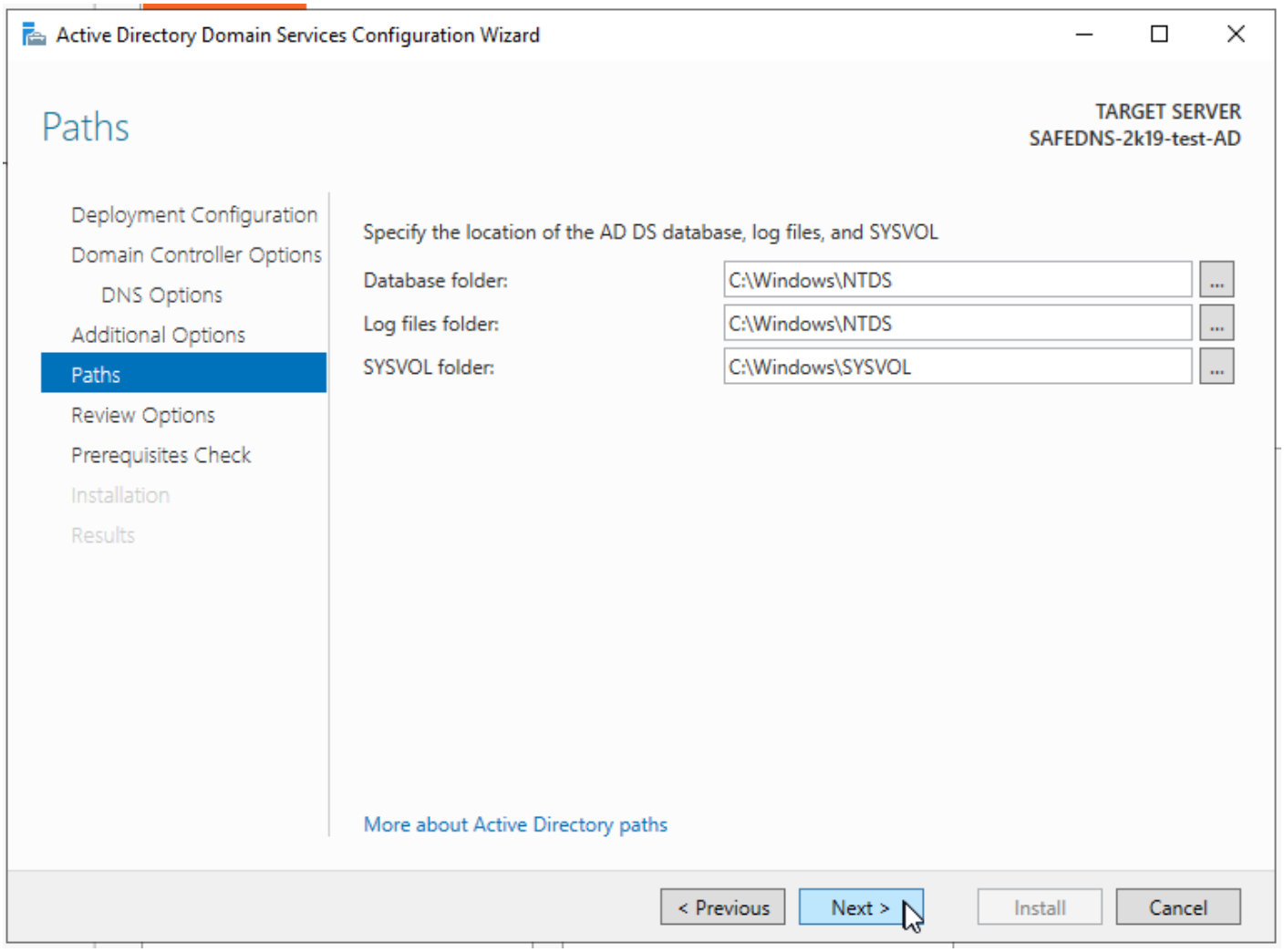
Configure the delegation options (if there is a need for that):



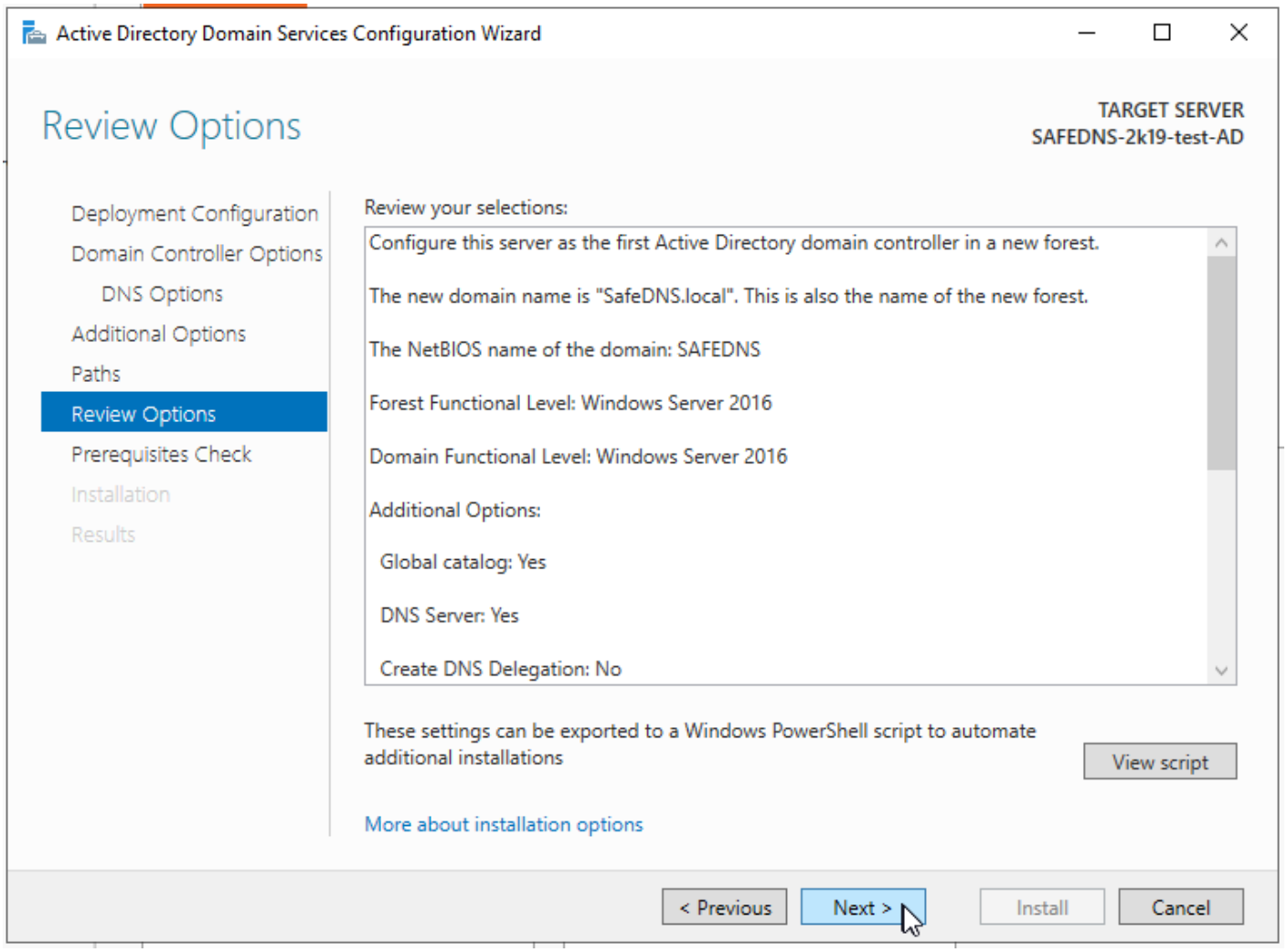
Configure the NETBIOS name:



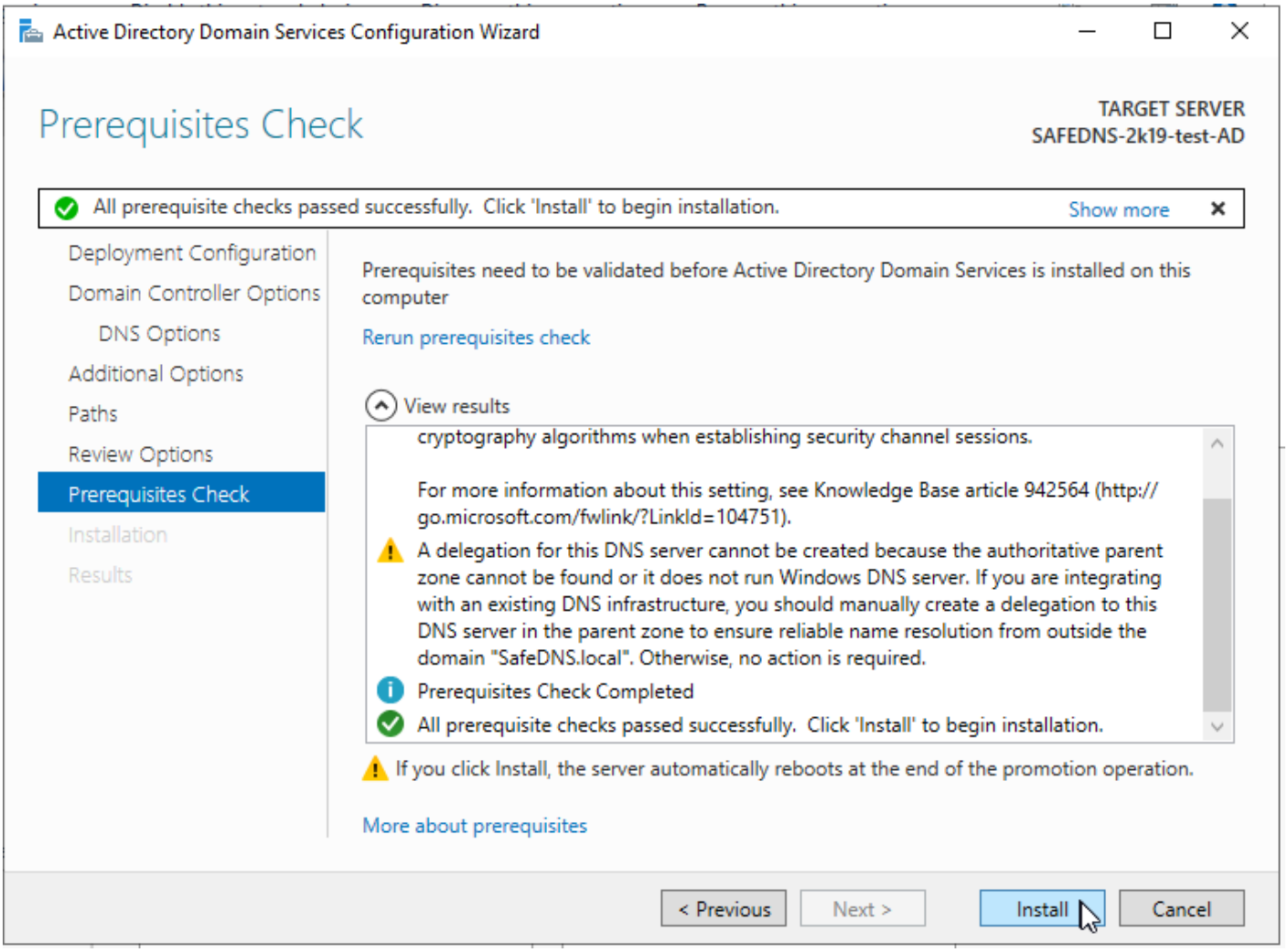
Configuring the system folders:



The preview of the installing options:



Prerequisites check and install:

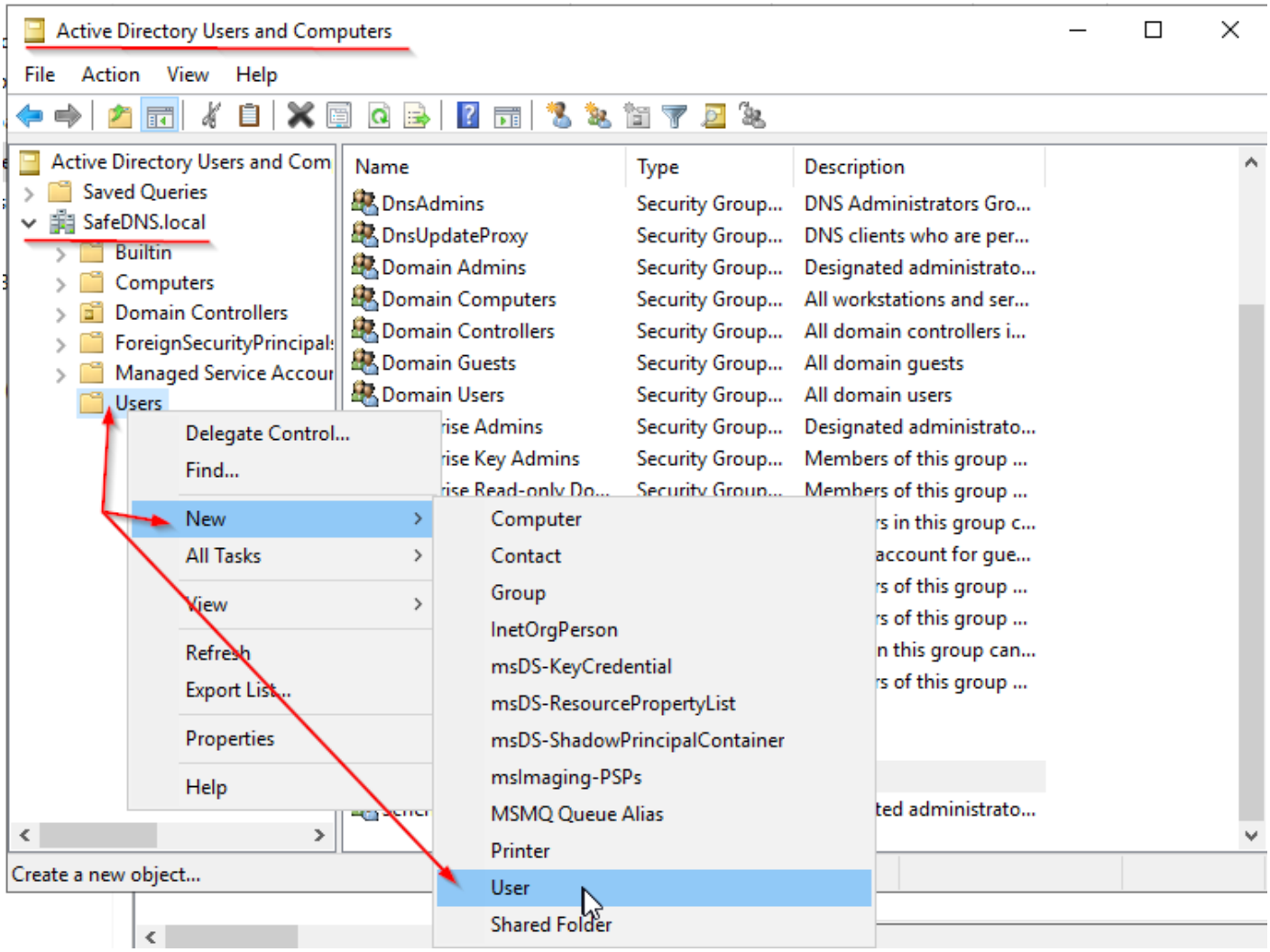


3. Creating User/Groups on the AD.

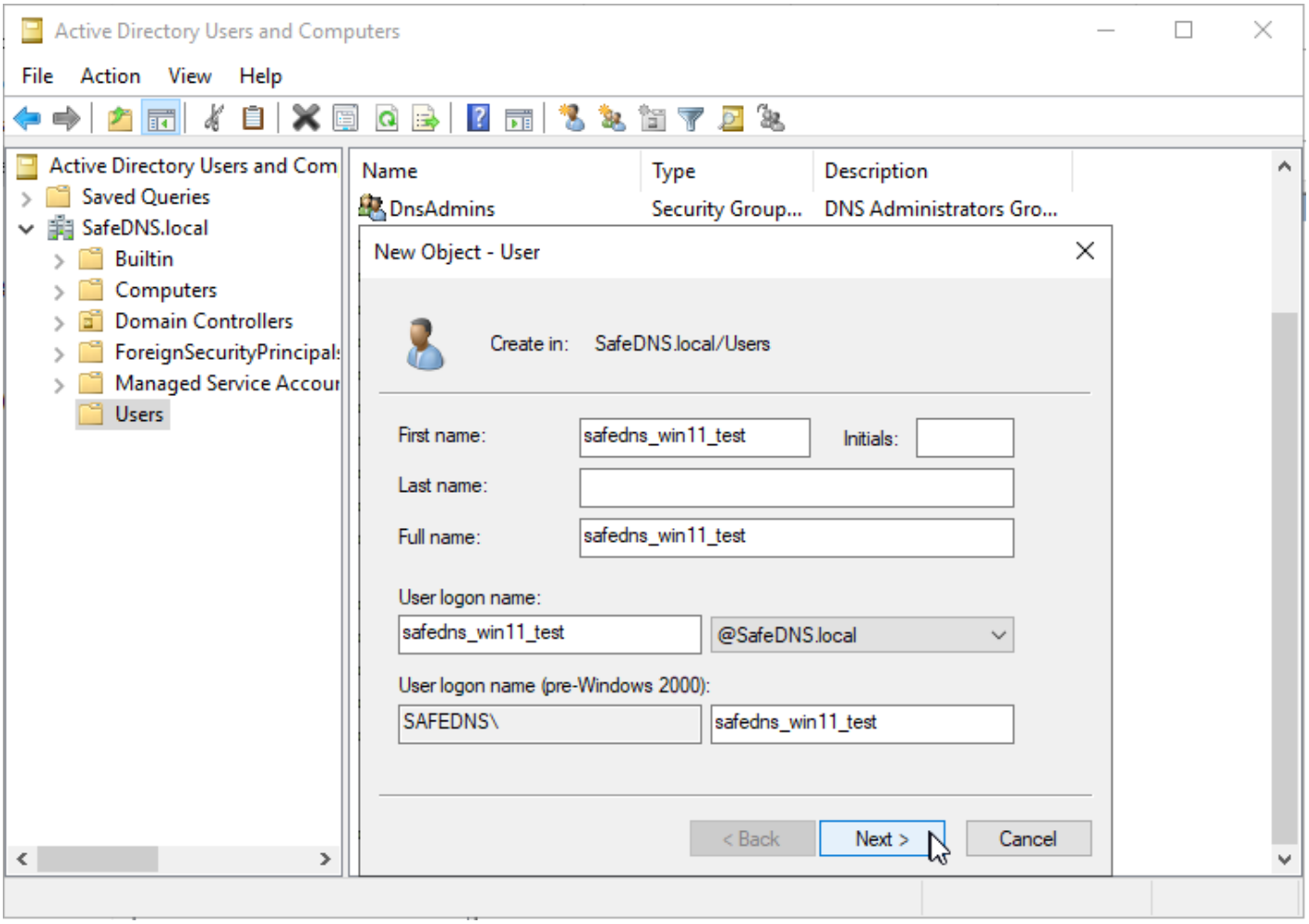
The new group and user should be created for the Agent Software delivery to the end-user computers. The application installation starts immediately after first user logon to the computer.

3.1. Creating a new user.

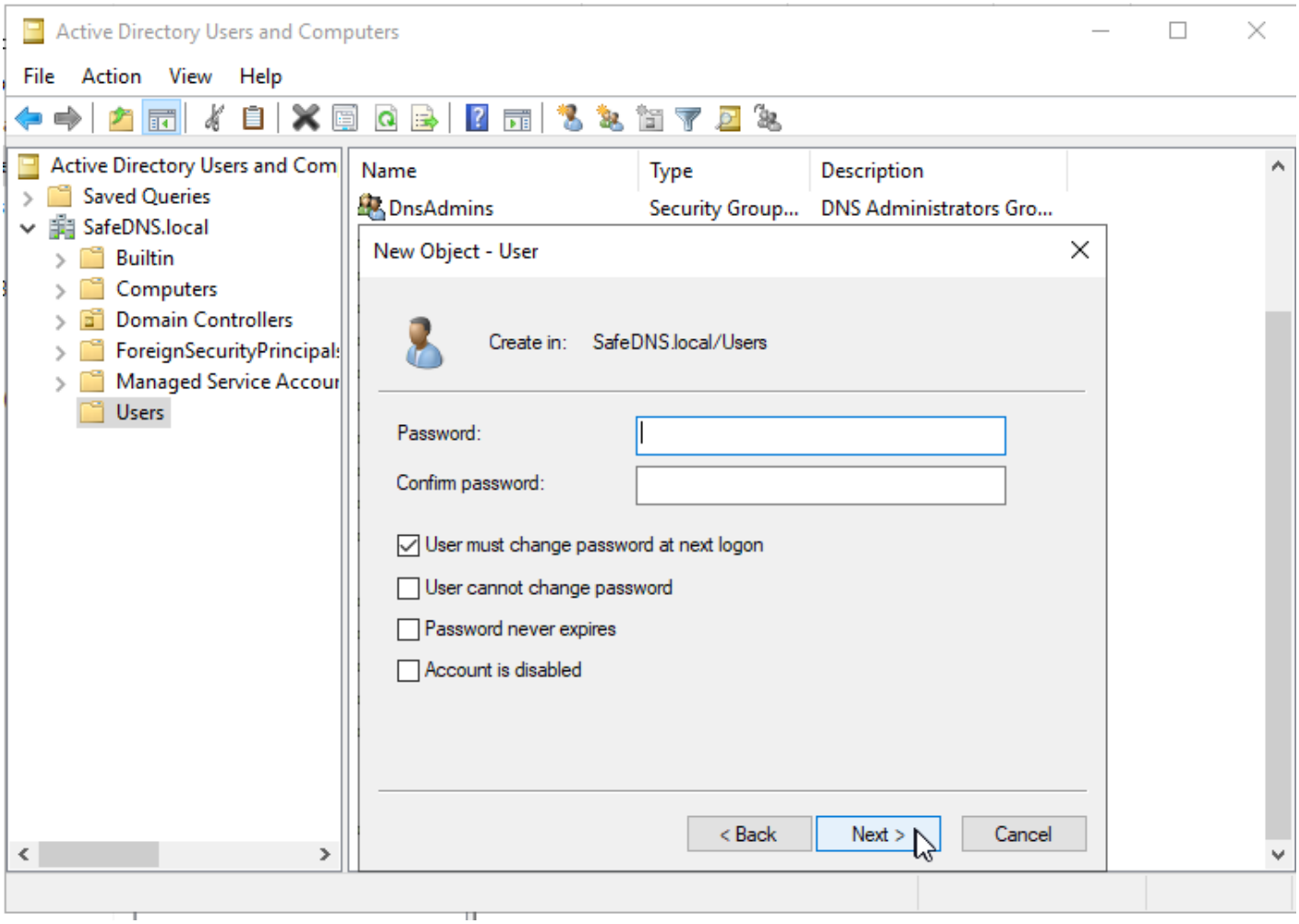
Open the Active Directory Users and Computers, select the recently created domain, then Users => New => User:



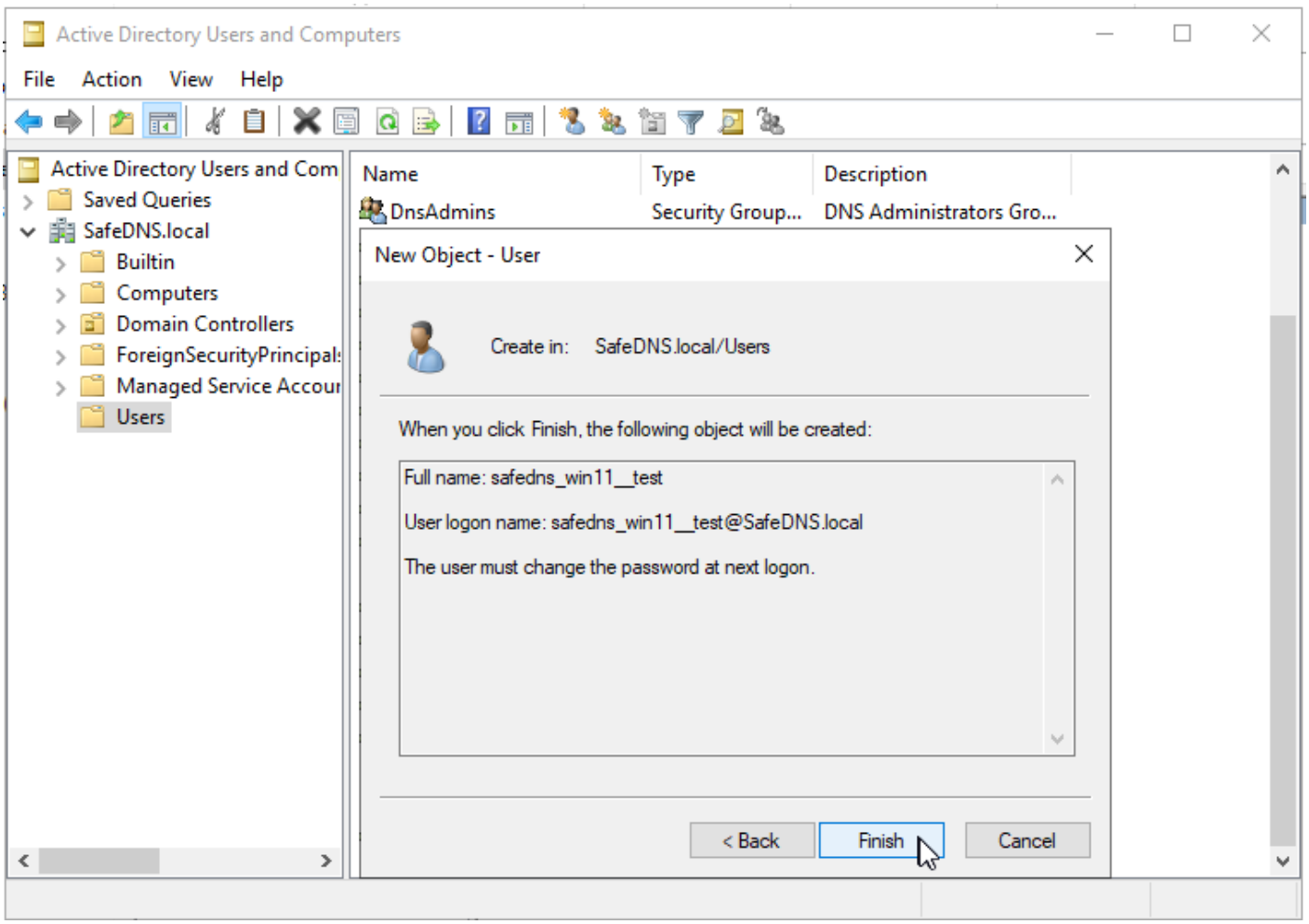
Setting the username:


Active Directory Users and Computers
File Action View Help
Active Directory Users and Com
Saved Queries
SafeDNS.local
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accour
Users
Name
Type
Description
DnsAdmins
Security Group...
DNS Administrators Gro...
New Object - User
Create in: SafeDNS.local/Users
First name:
safedns_win11_test
Initials:
Last name:
Full name:
safedns_win11_test
User logon name:
safedns_win11_test
@SafeDNS.local
User logon name (pre-Windows 2000):
SAFEDNS\
safedns_win11_test
< Back
Next >
Cancel

Password:



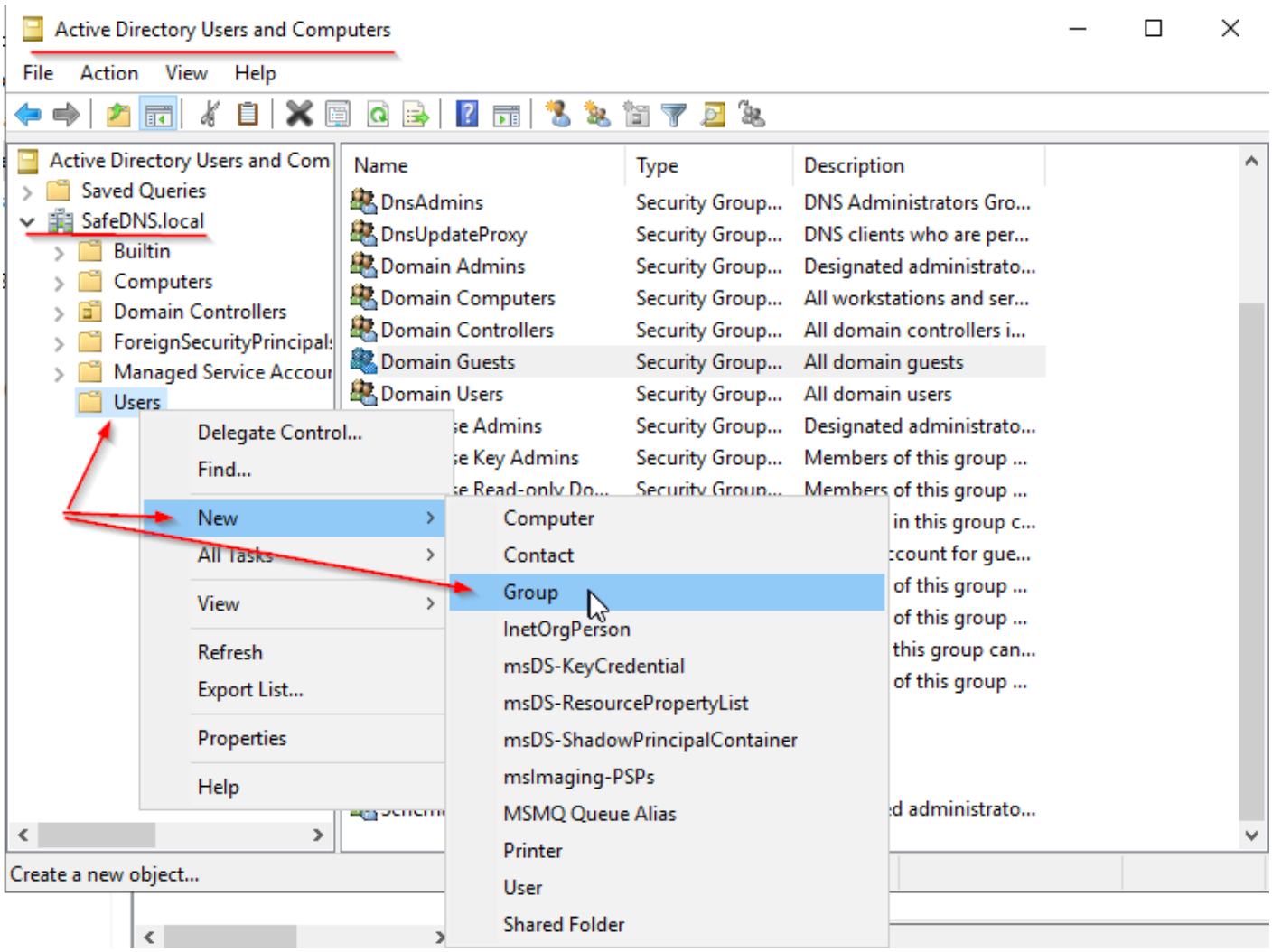
Reviewing the object(User) summary and finishing the process:



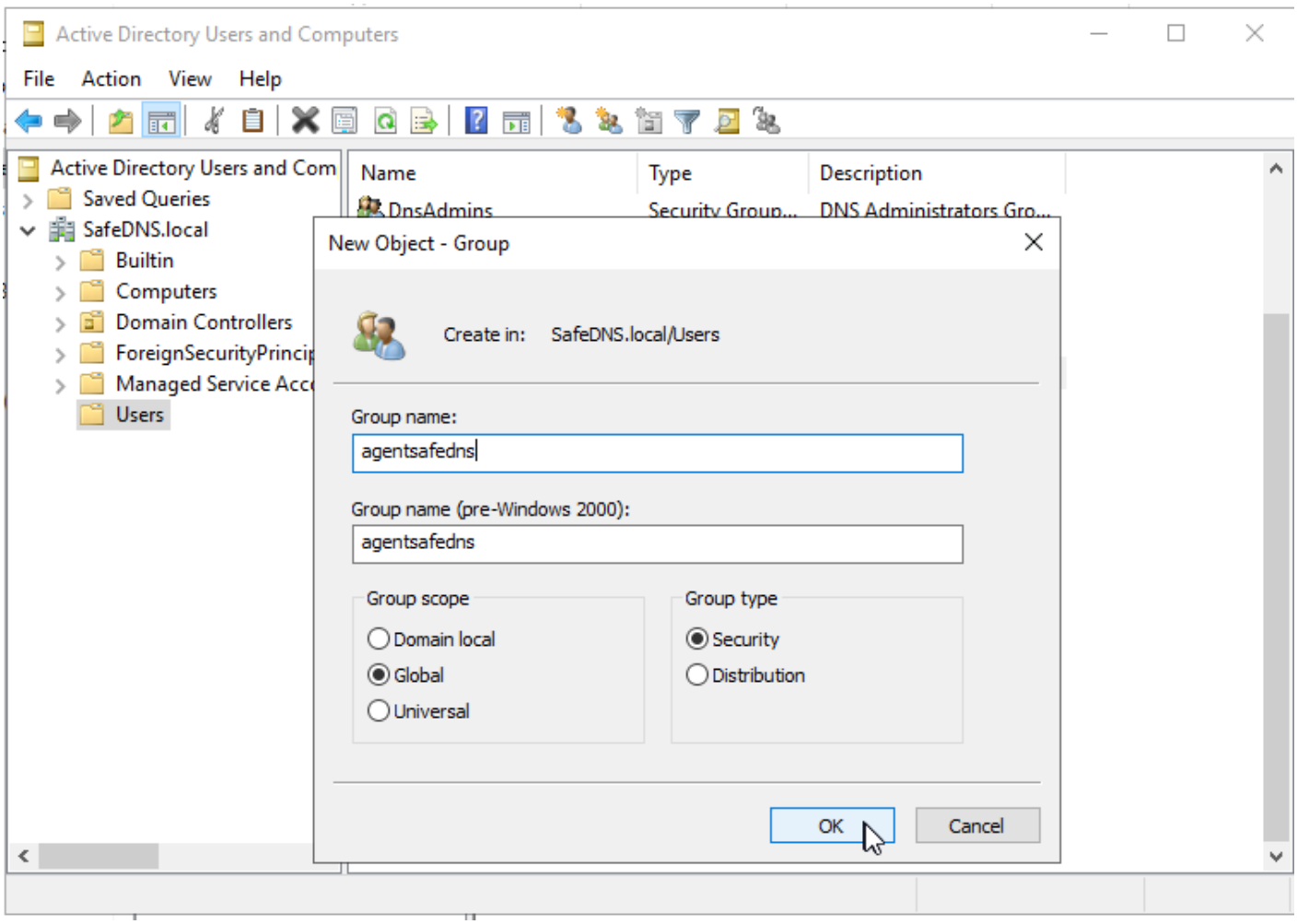
3.2. Creating of the User Group.

Users can be part of one group within the AD environment. The application can be applied to a group of users optimizing the configuration and management of the Application Rollout.

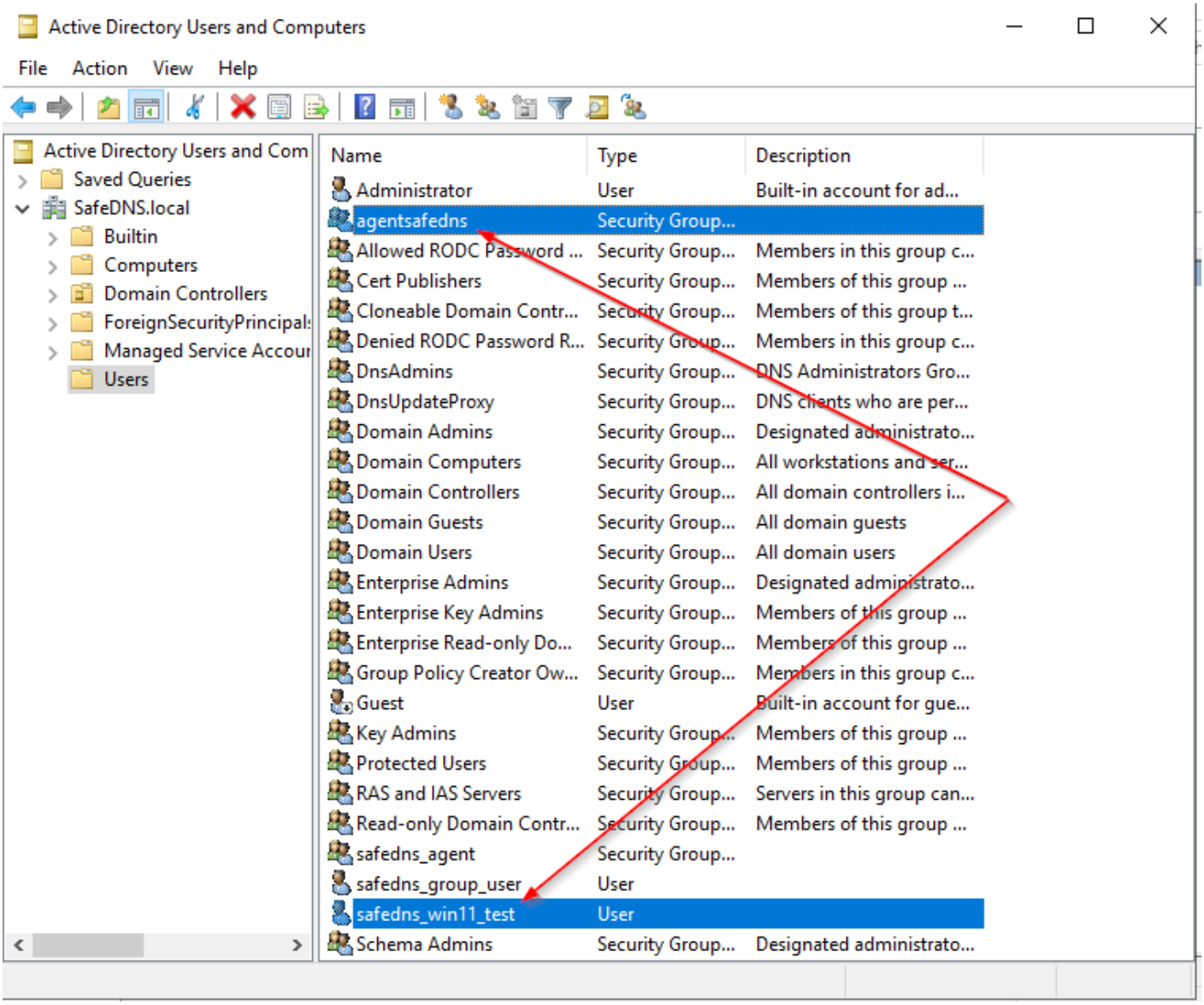
Active Directory Users and Computers, Selecting our domain, and then tap on the Users => New => Group:



Entering the data of the Group and tap OK:

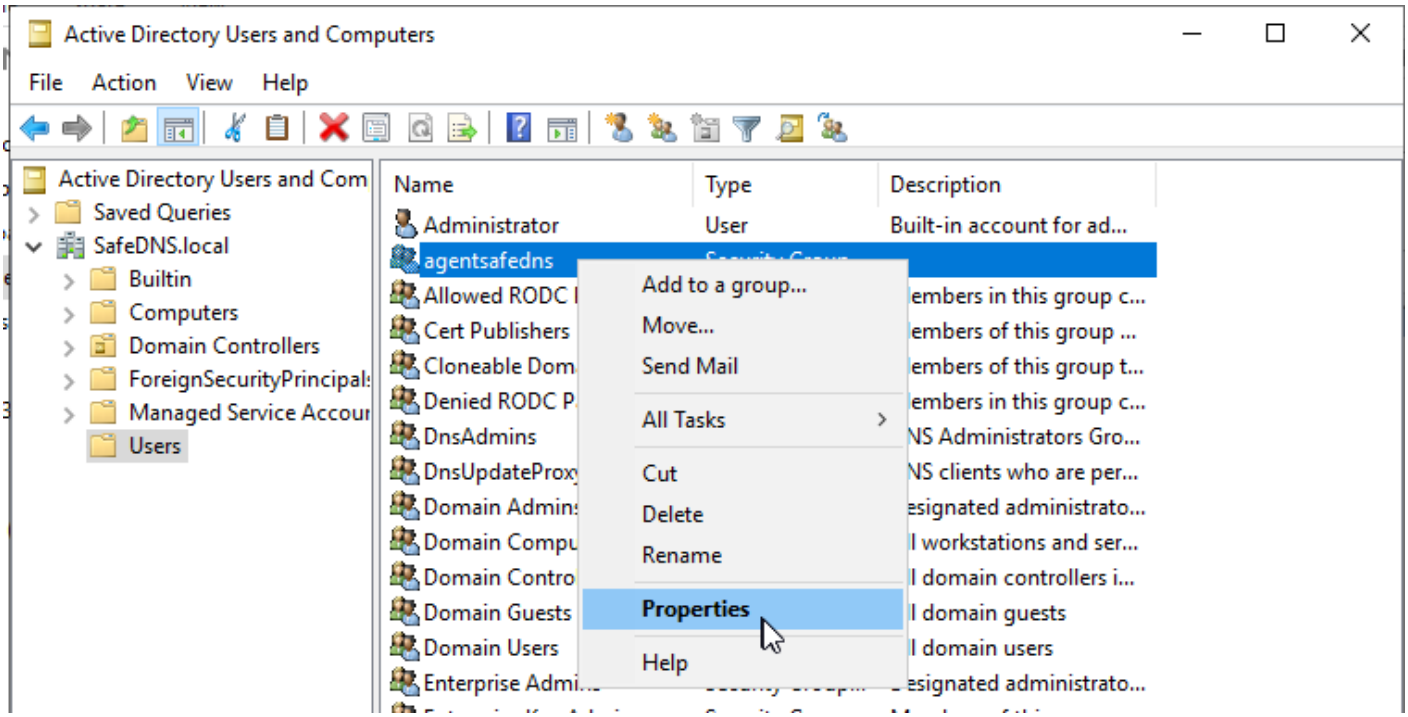


Please check that User and group has been created:

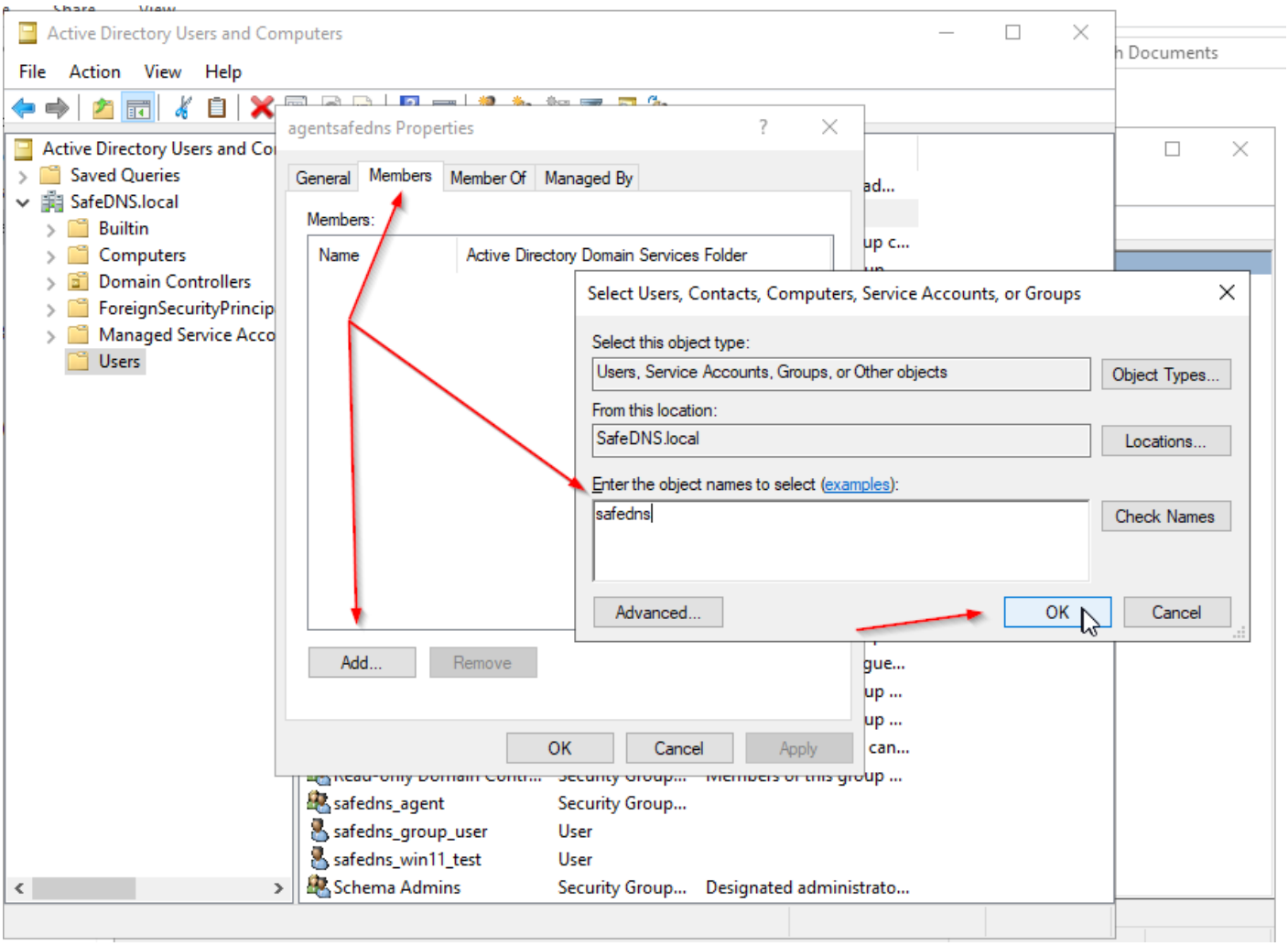


3.3. User added to the group.

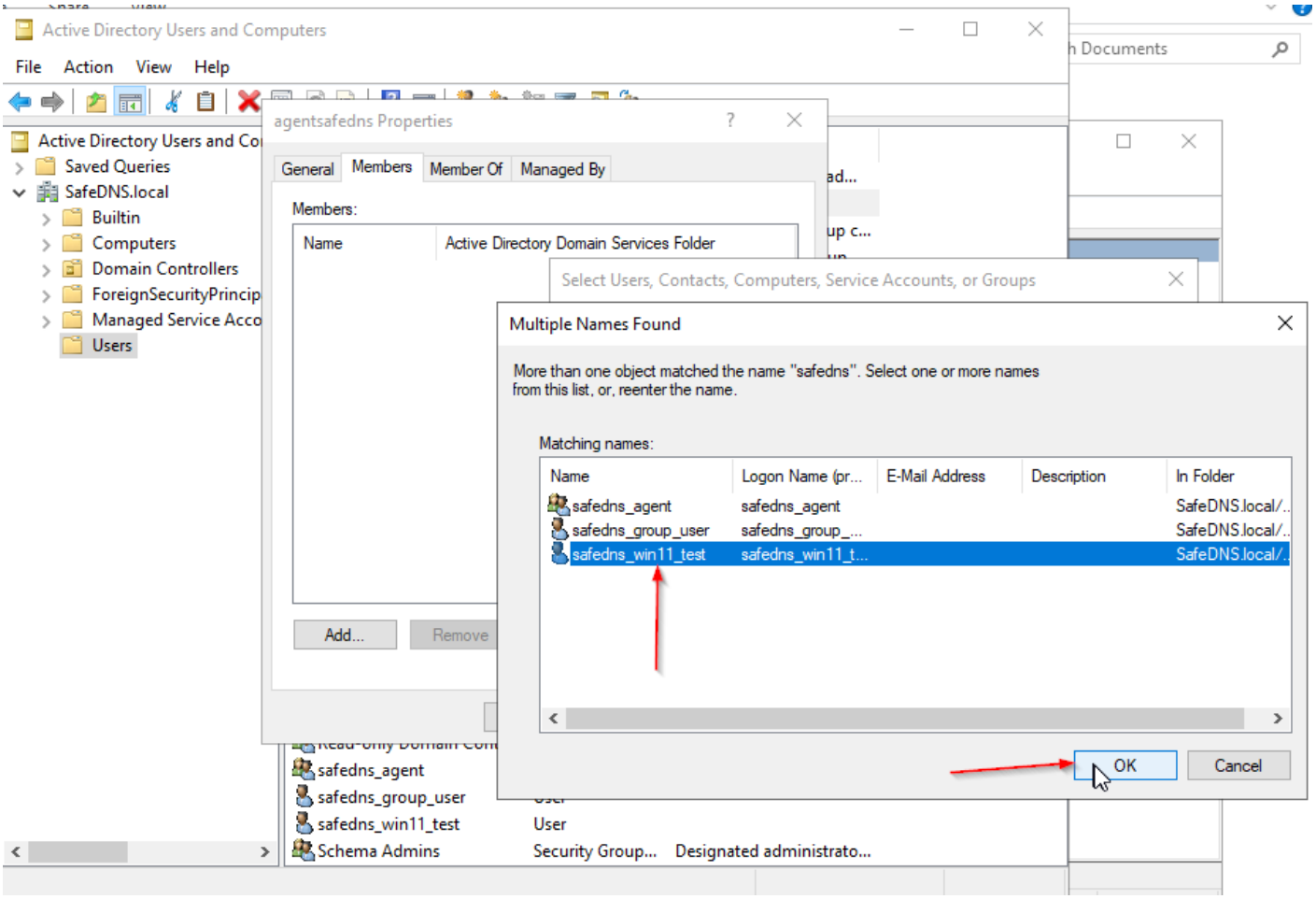
Select the group and in the context menu tap the Properties:



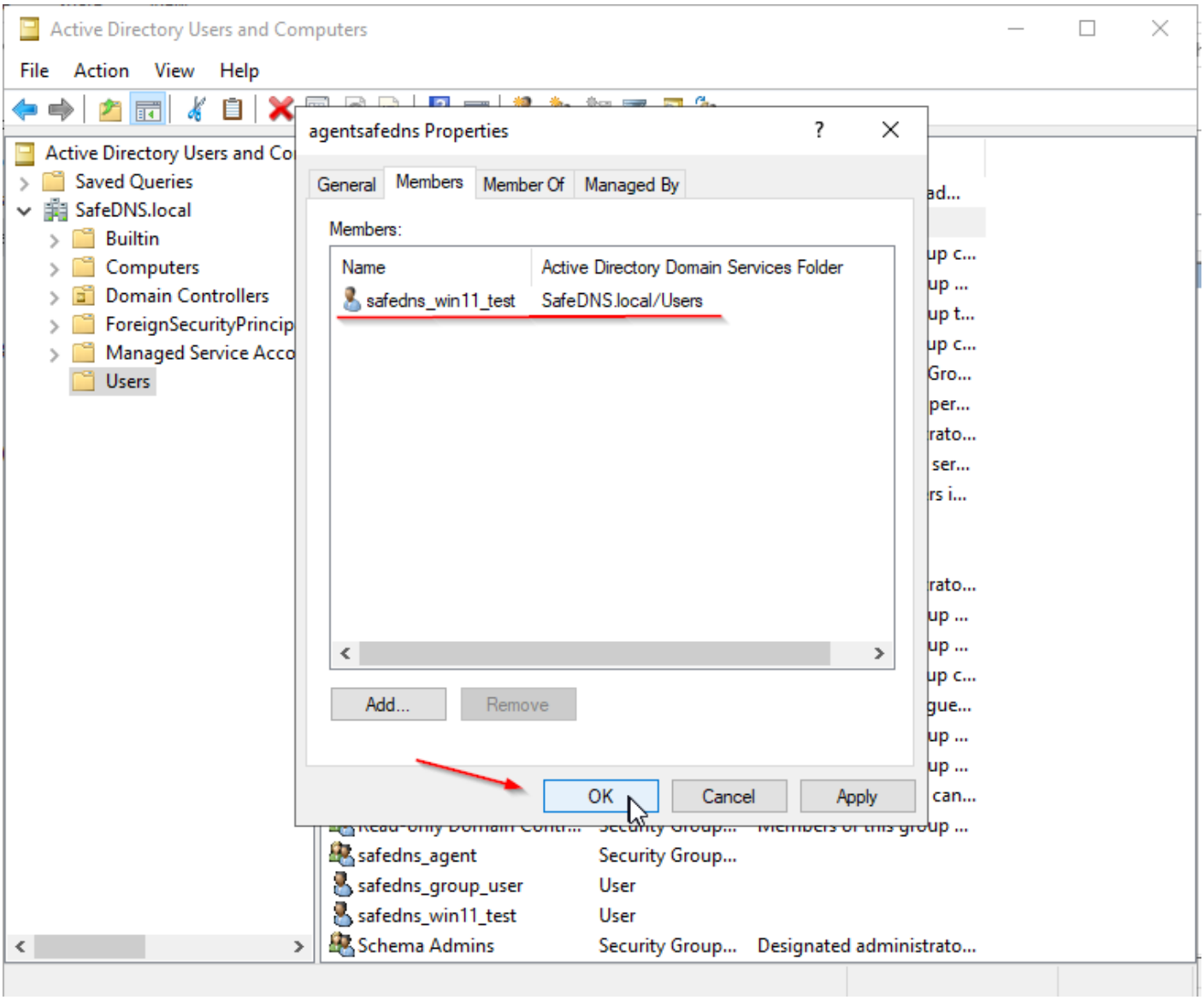
On the appeared window select Members and tap the Add button. Enter the username in the search field and press OK:



Select the user safedns_win11_test and tap OK button:



Check the result and press OK button:



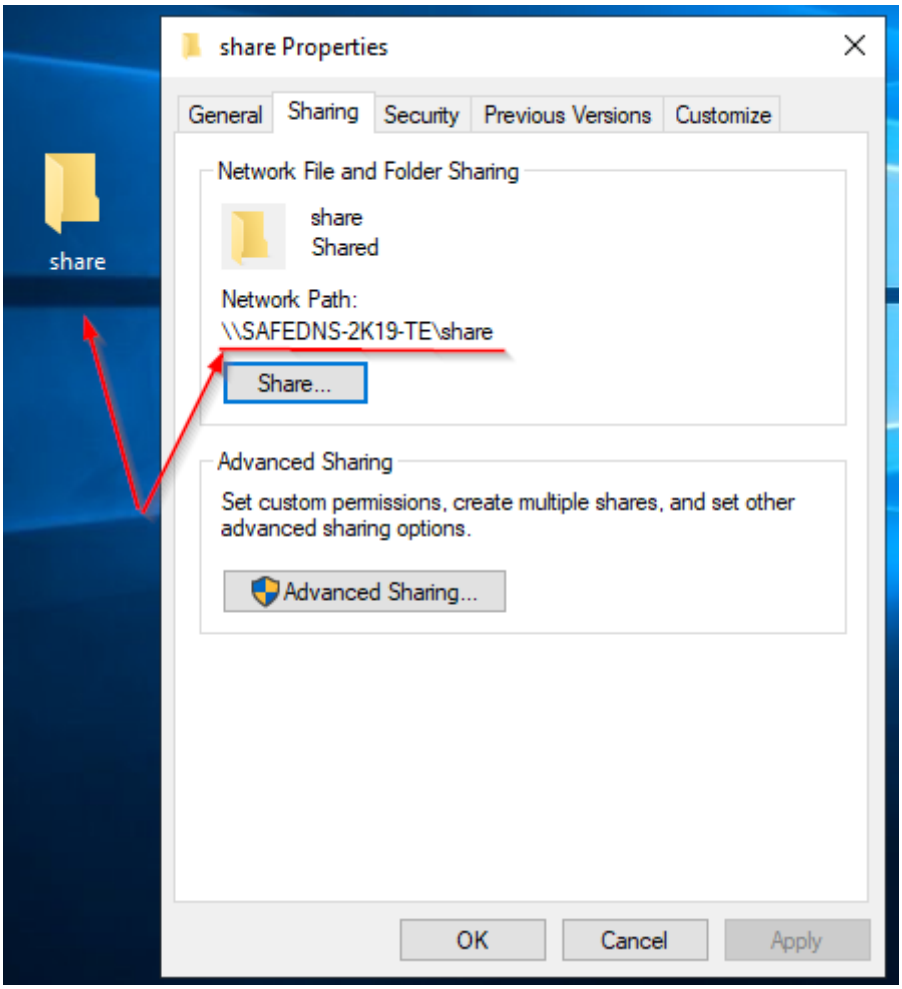
The user creation part is over, now we need to configure GPO.

4. MSI file Preparation on the server.

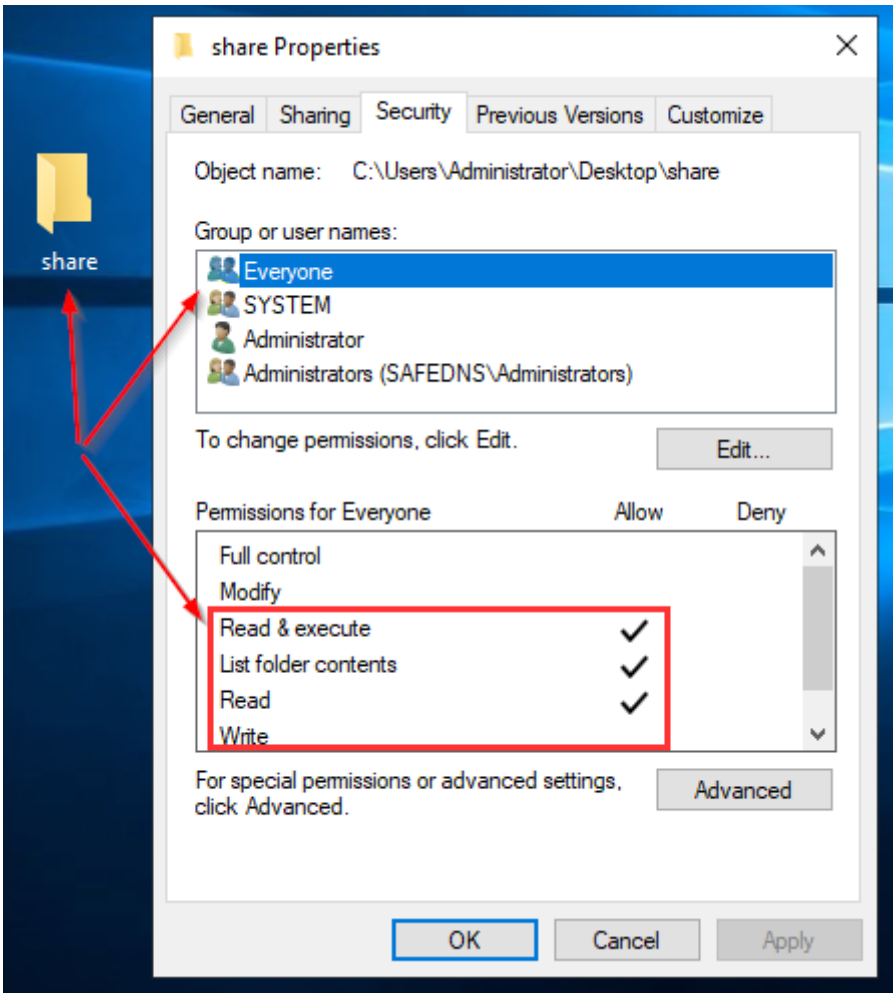
The MSI Agent package should be prepared and copied to the folder on the Active Directory Server.

> The MSI Agent package is prepared by SafeDNS. Our technical team generates and inserts your personal identification token into the package.

The folder with the Agent package should be avalable from the client's computer.



The folder permissions should be the following. User Everyone should have access to the read&execute:

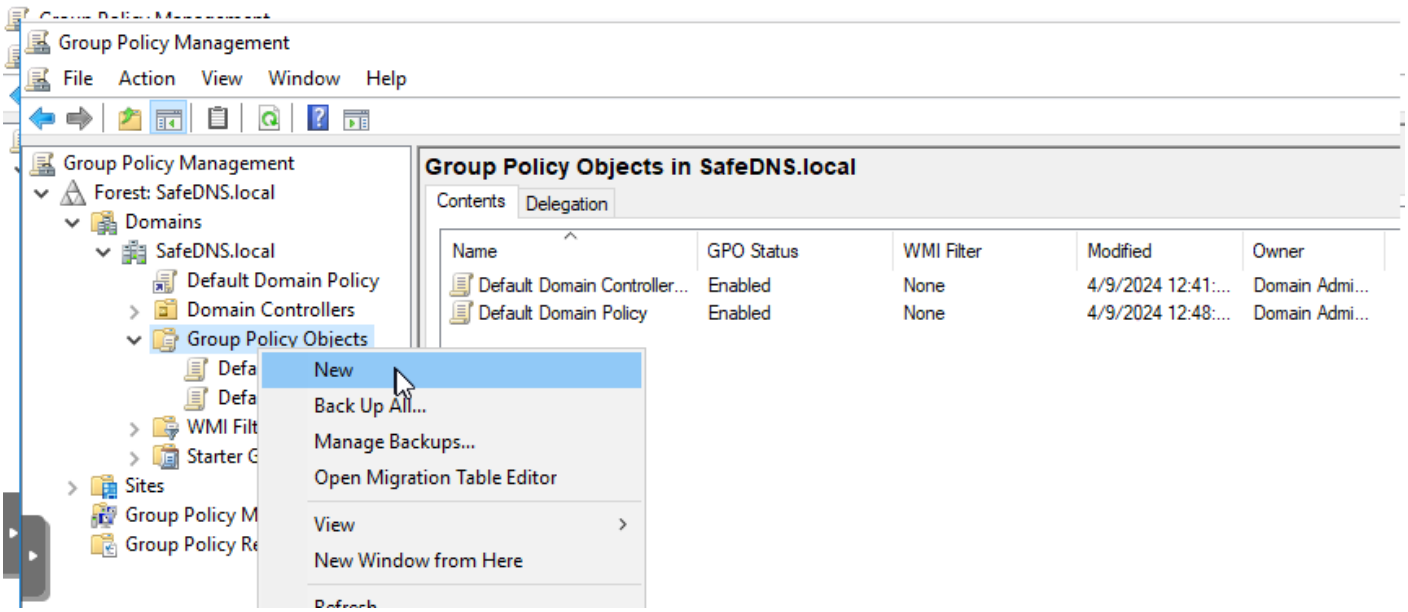


The preparation of the file process is over.

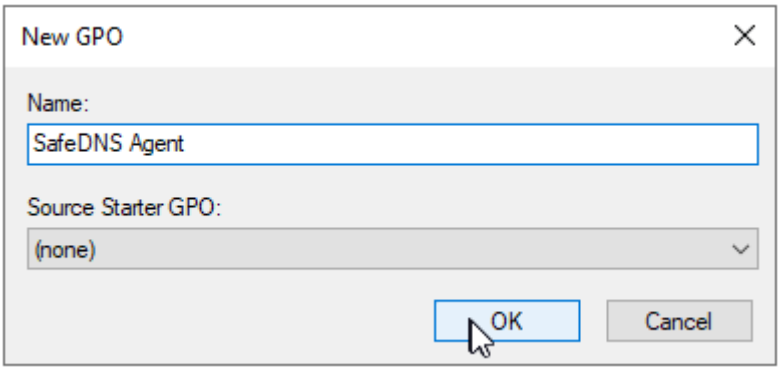
5. Group Policy Configuration.

Open the Group Policy Management console

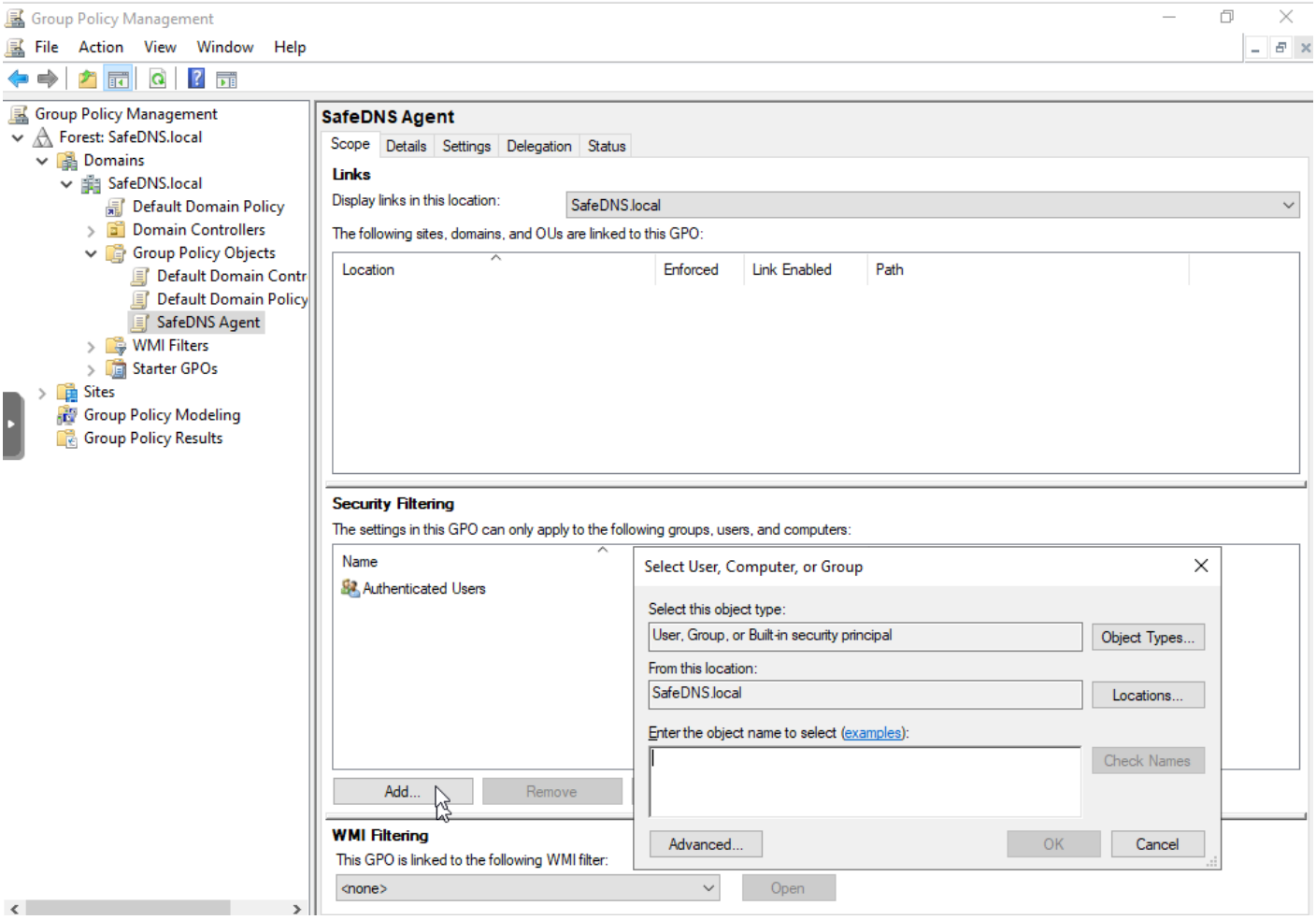
Select the current domain, then Group Policy Objects and open the context menu => New



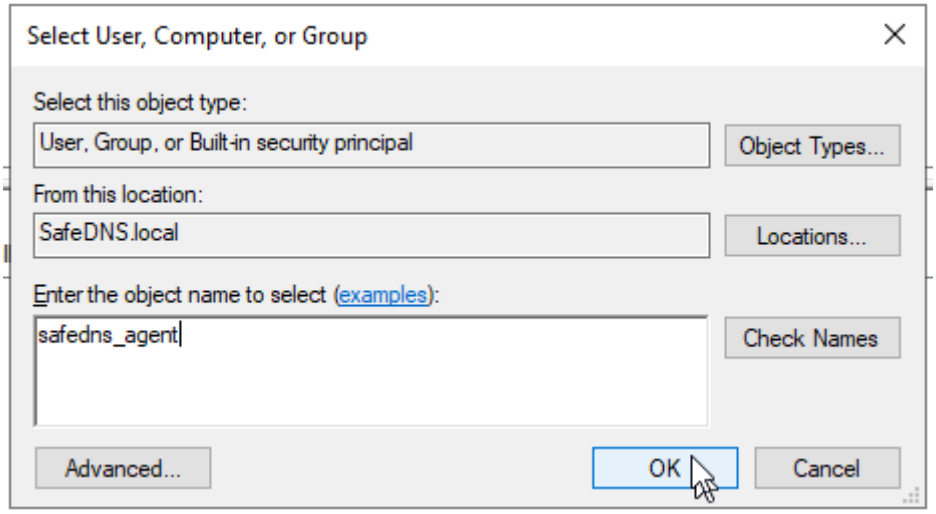
Please name the Group Policy accordingly:



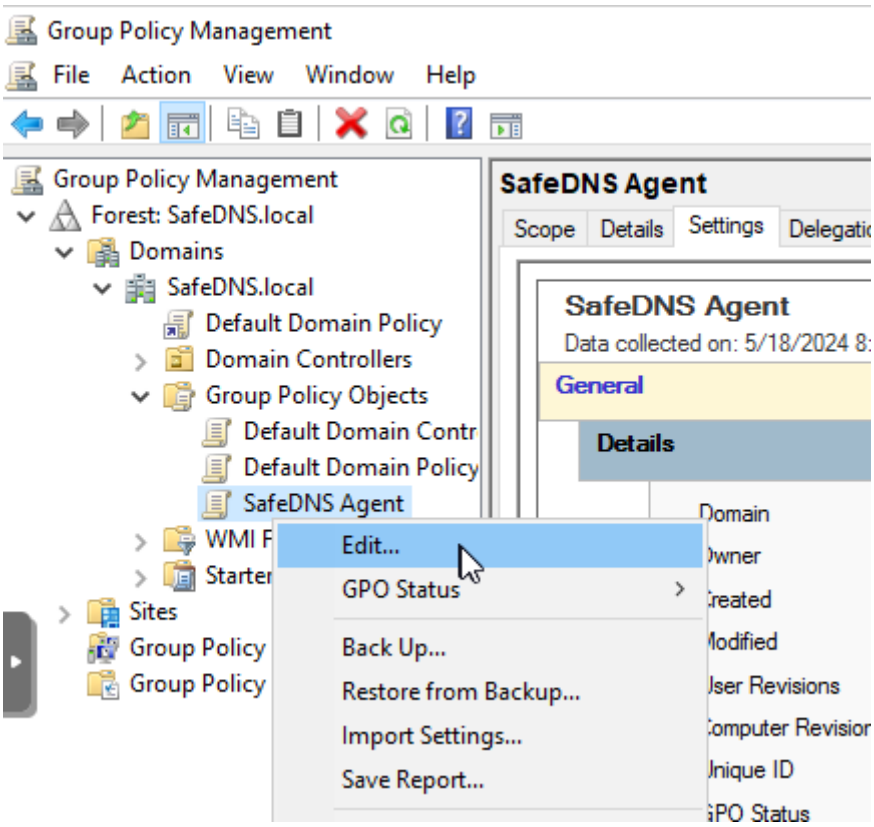
Once the policy is created, please set the User/Group applied the GPO installation:



In the appeared window select the Group safedns_agent - with the user safedns_win11_test:



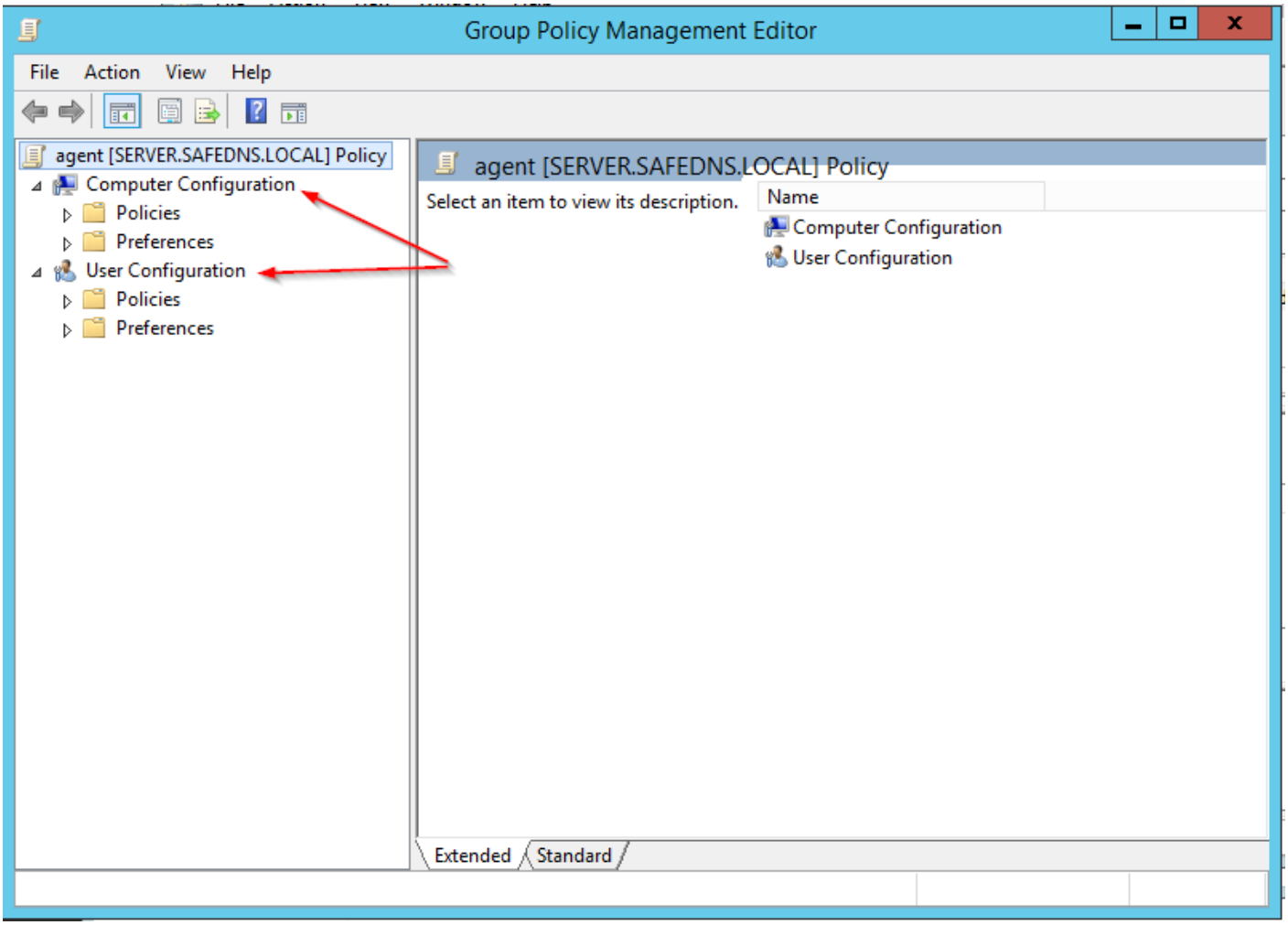
Once the GPO is created, tap the context menu of the object and click on Edit button:



Important notice: There are 2 possible ways of the MSI package installation:

1. Installation Policy applied to the computer - Computer Configuration

2. Installation Policy applied to the user - User configuration

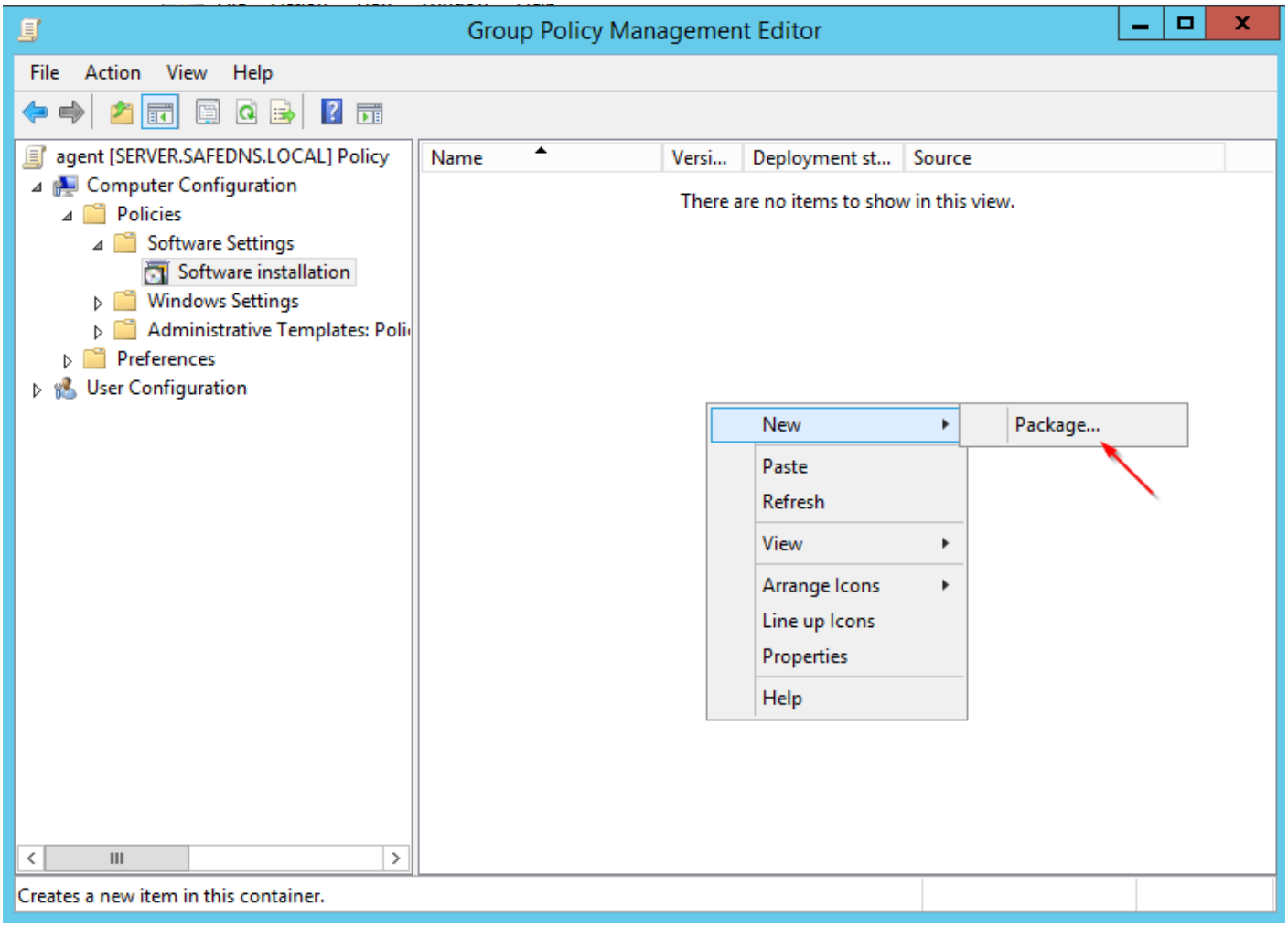


It is recommended to use Computer Configuration - the software installation will start without user interaction and the user can not stop/close installation.

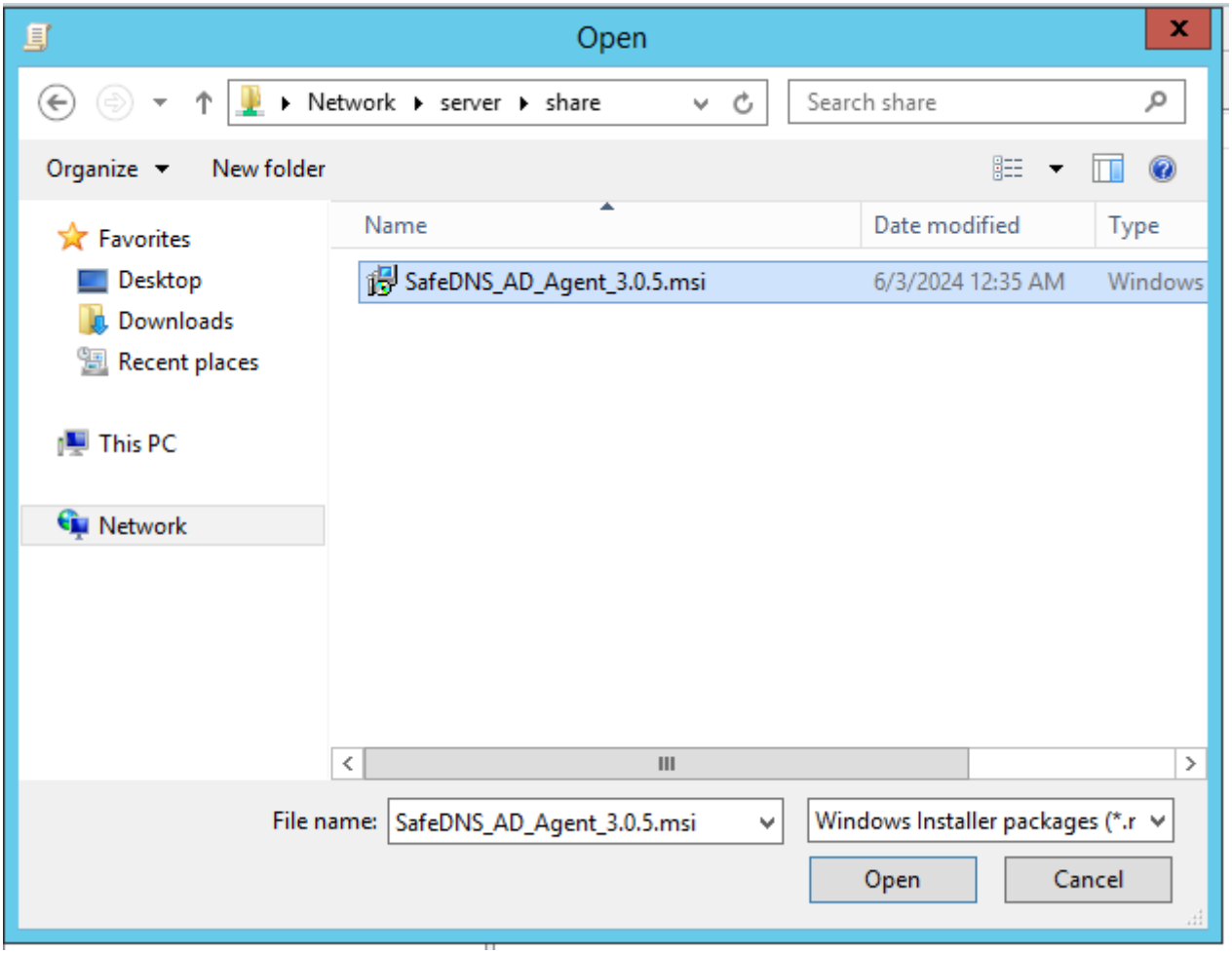
The second option - User Configuration requires user actions on the computer to start the package installation and will require Administrator credentials.

In the Group Policy Management Editor select Computer Configuration then Policies => Software Settings => Software Installation.

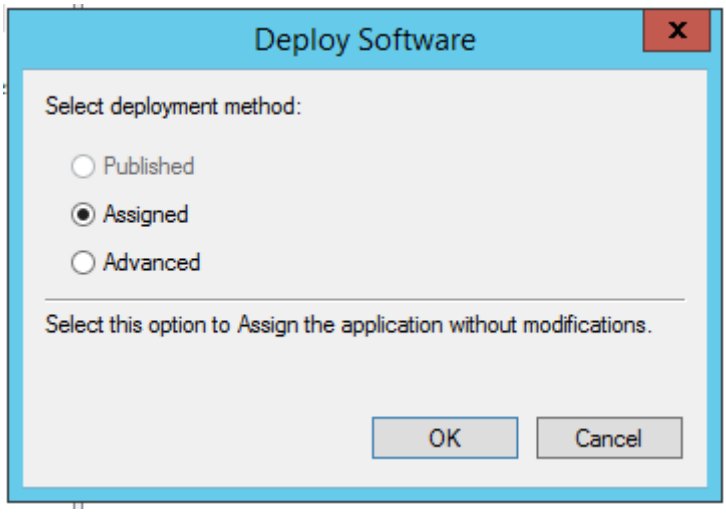
Tap the context menu button and select New=>Package:



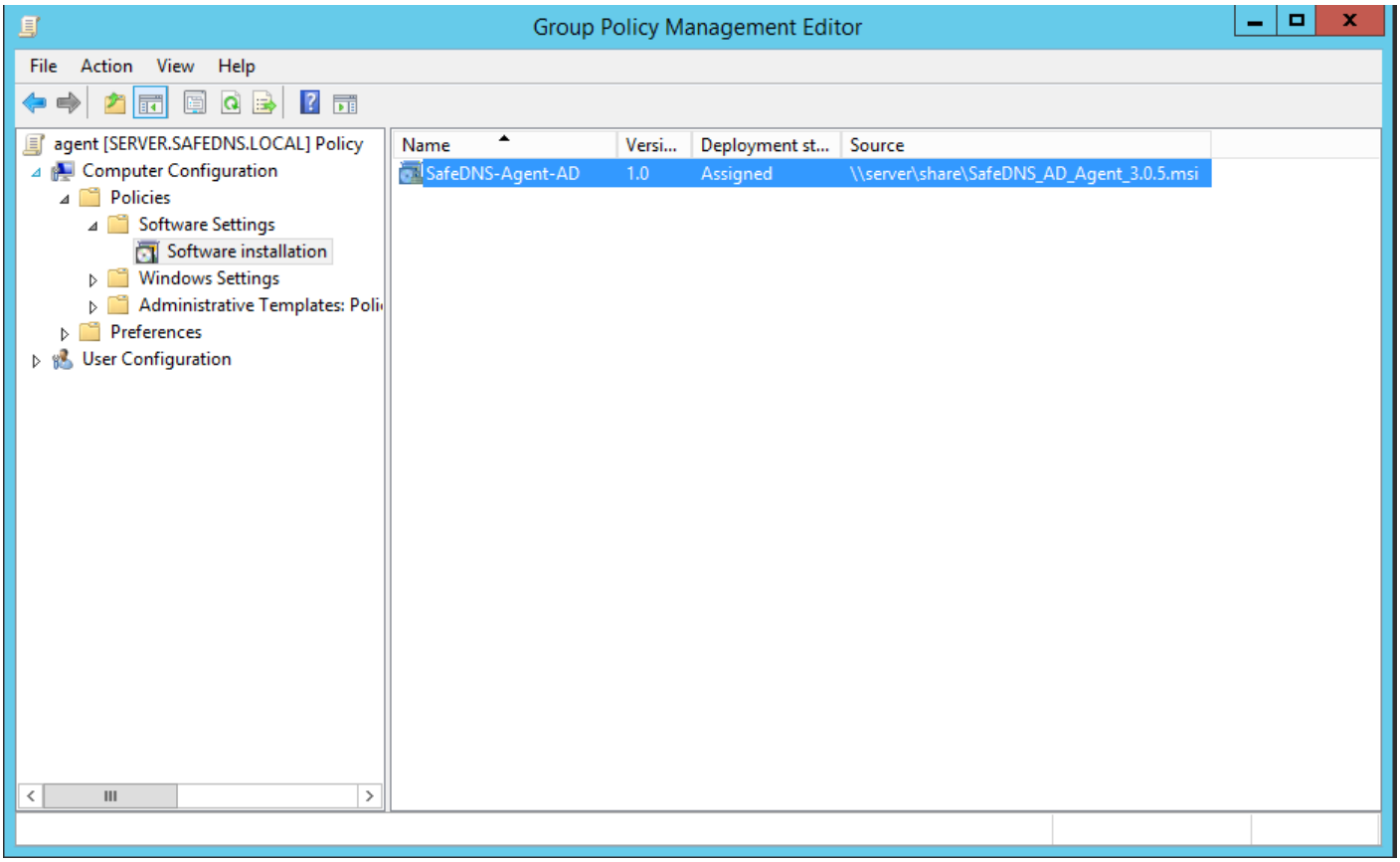
Select the SafeDNS Agent installation package. The path should be the following: \\server\share\SafeDNS_AD_Agent_3.0.5.msi



Select the Assigned deploy method:



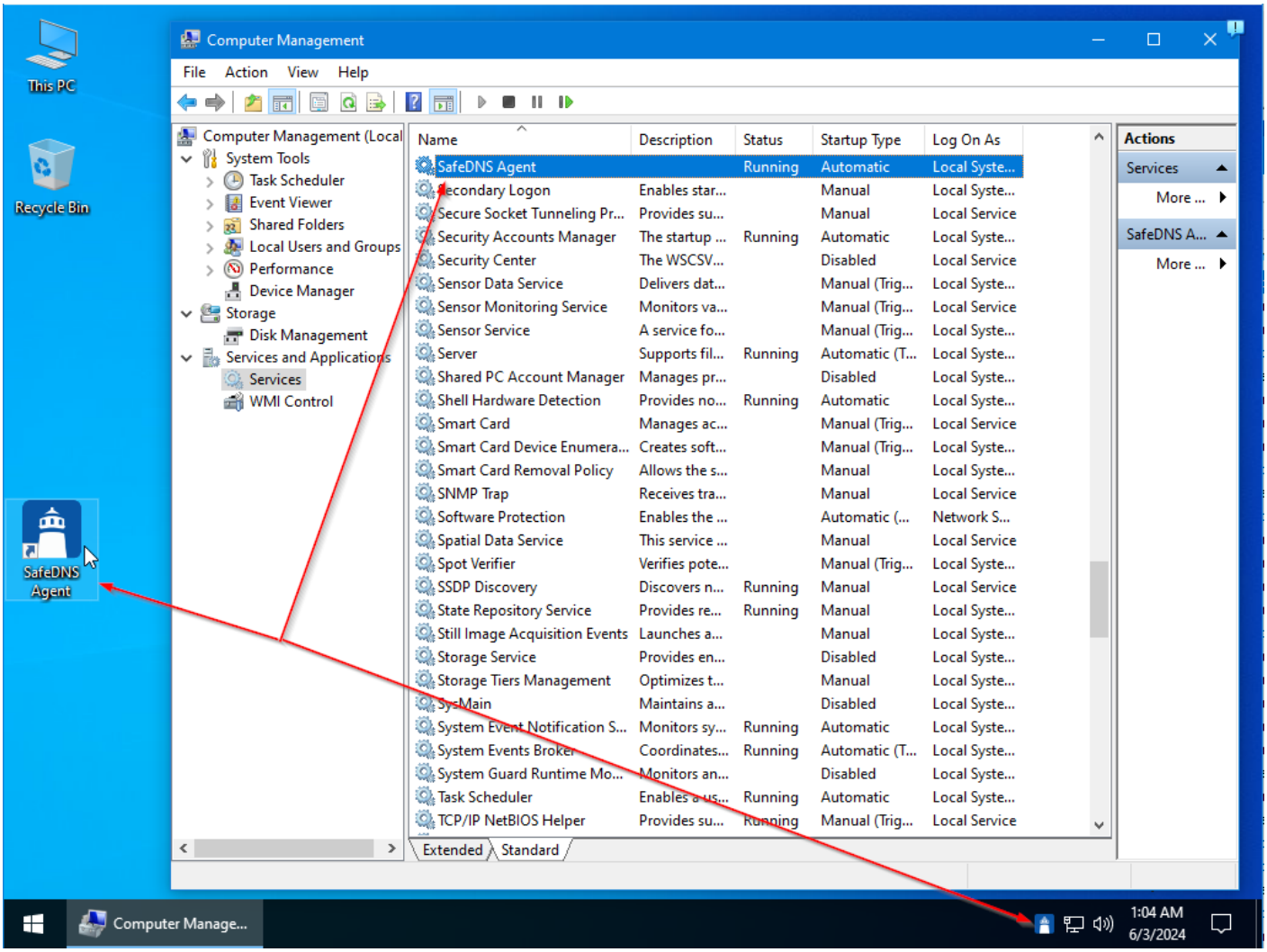
Once the Application package is added, the new record should appear in the list:



> The installation is finished, the Agent should be installed after the next login to the computer.

Depending on the MSI package settings, after the installation the following objects should appear:

1. SafeDNS Agen icon on the Desktop
2. SafeDNS Agent service
3. SafeDNS icon on the system tray



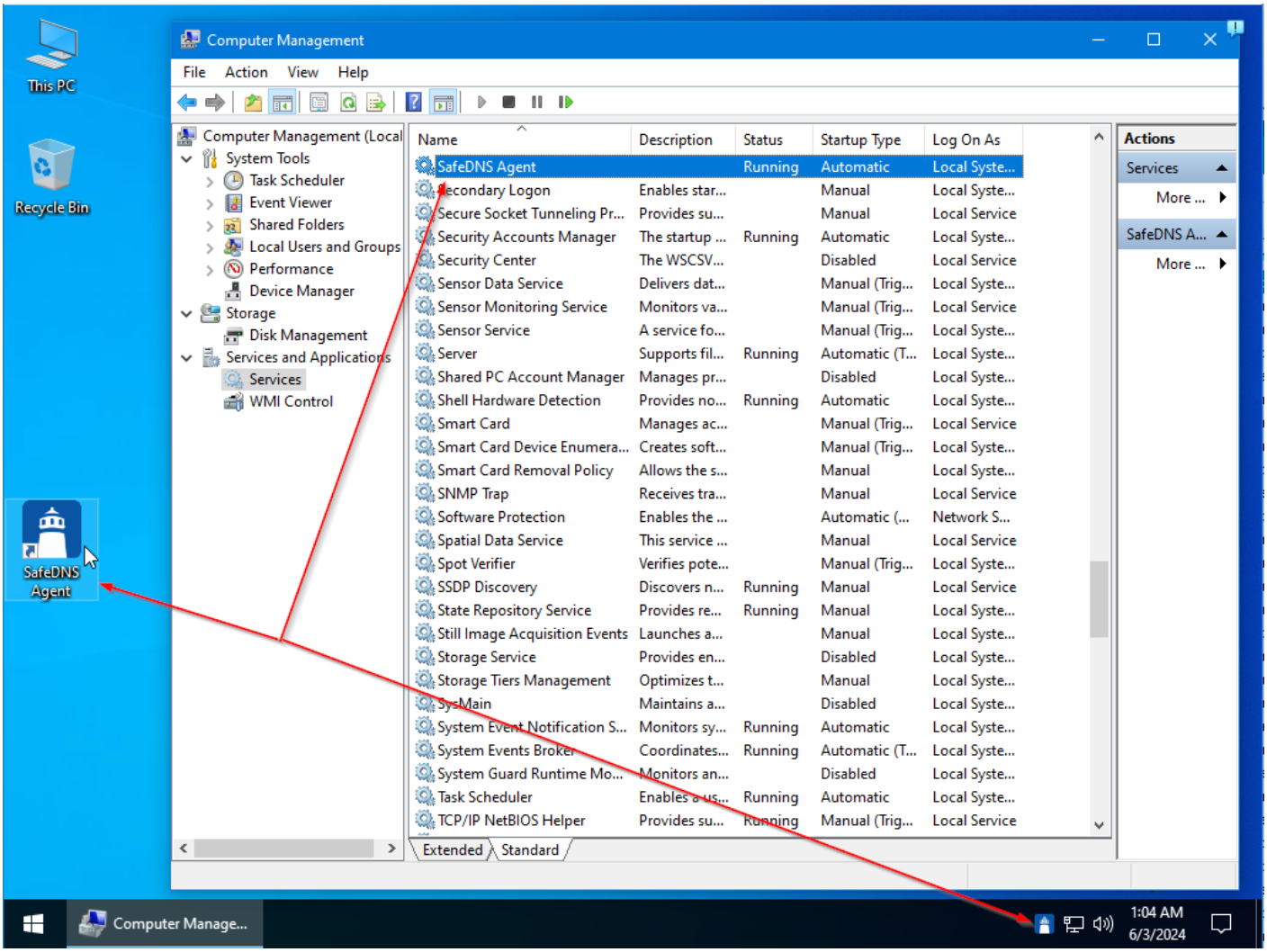
If there is a need to start the MSI package installation before restarting/new login please start the CMD command line and run the following command:

gpupdate /force

This command will initiate the installation process:

```
C:\Windows\system32\cmd.exe - gpupdate /force
Microsoft Windows [Version 10.0.19045.2486]
(c) Microsoft Corporation. All rights reserved.

C:\Users\supertest>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.

Certain Computer policies are enabled that can only run during startup.

OK to restart? (Y/N)
```

Once the computer restarted, the applicaation will appear on the Desktop, the service created and the icon appeared in the system tray:



Revision #8
Created 1 July 2024 22:19:47 by Mark Woodman
Updated 27 September 2024 07:39:22 by Mickaël Gauthier