ACTIVE DIRECTORY

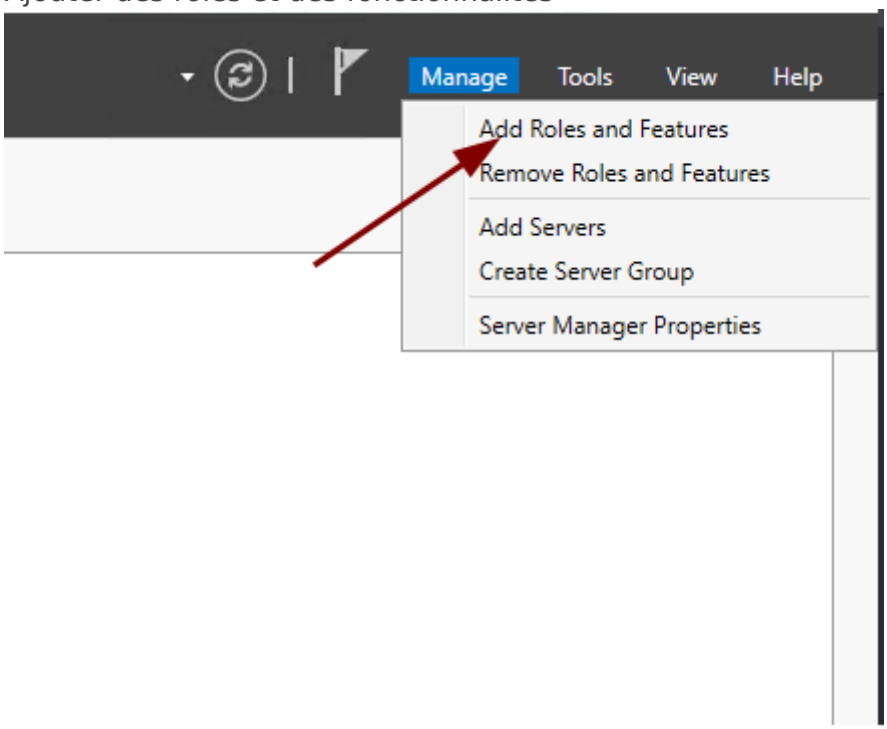
- INSTALLATION
- UTILISATEUR ET GROUPES
    - CREATION ET GESTION DES OU
- Ajouter PfSense à l'active directory
- Ajouter machine linux a l'AD
    - Ajout d'une machine linux a l'ad

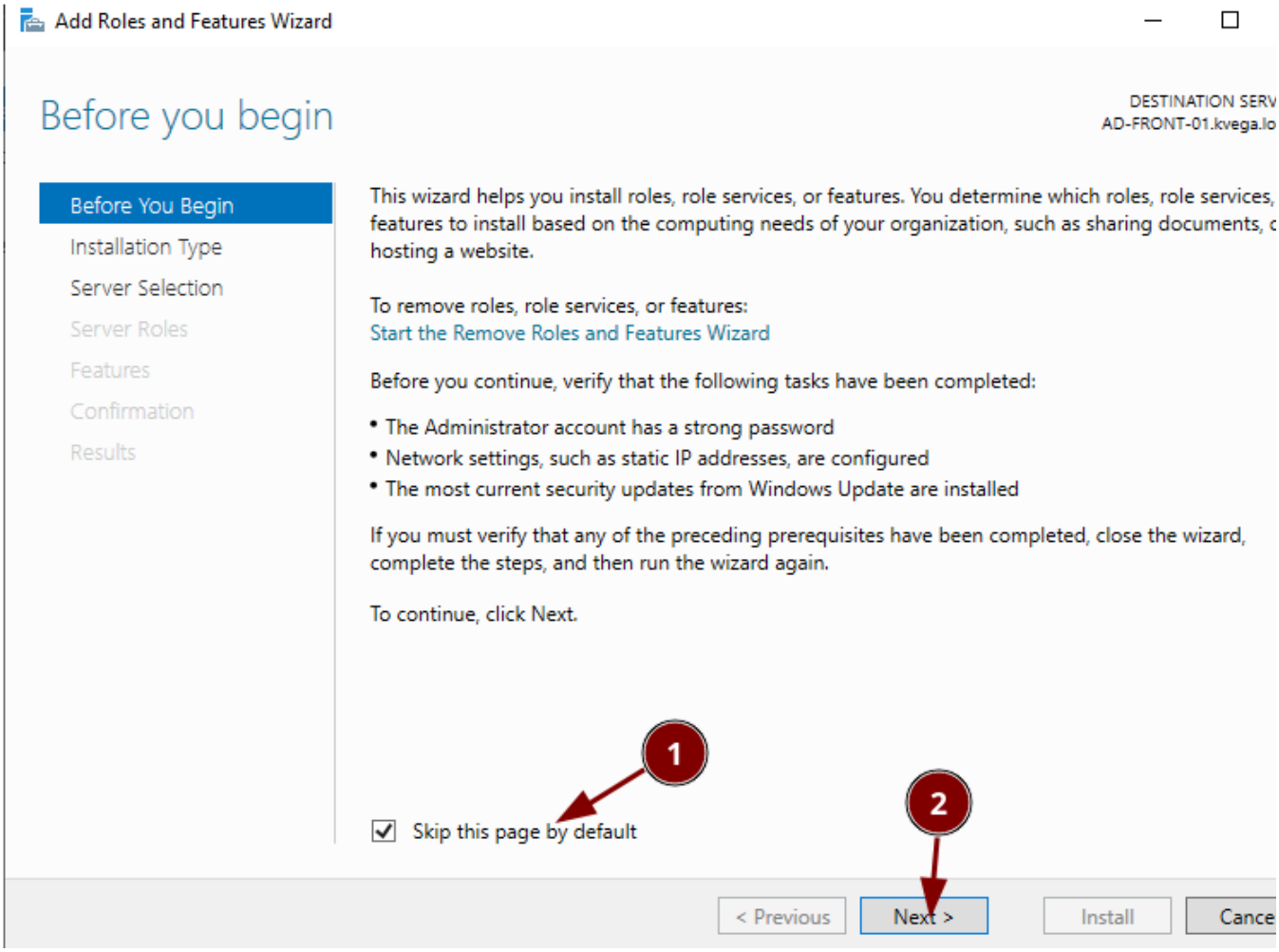
INSTALLATION

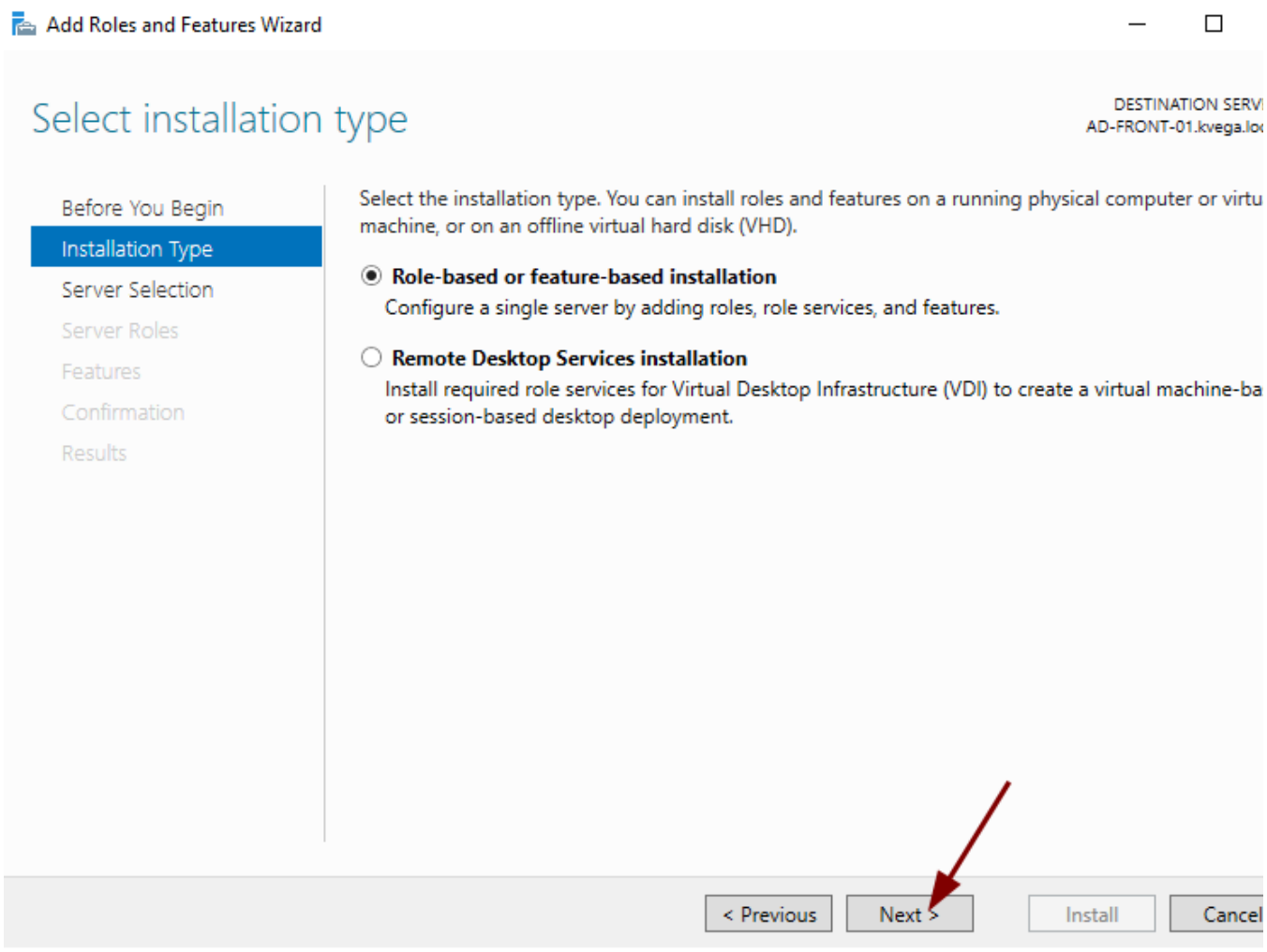
Installation d’un active Directory

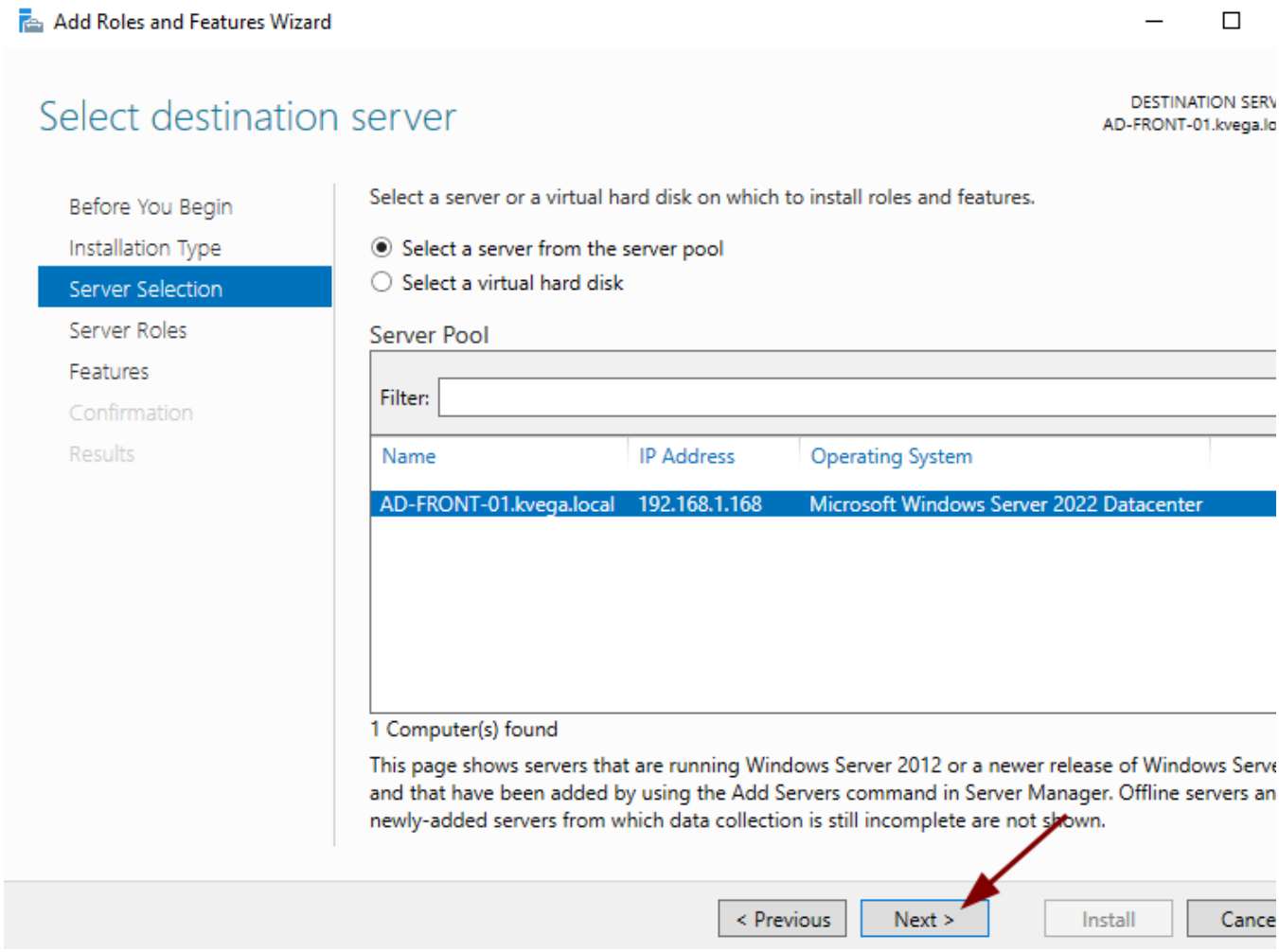
Installation Manuelle:

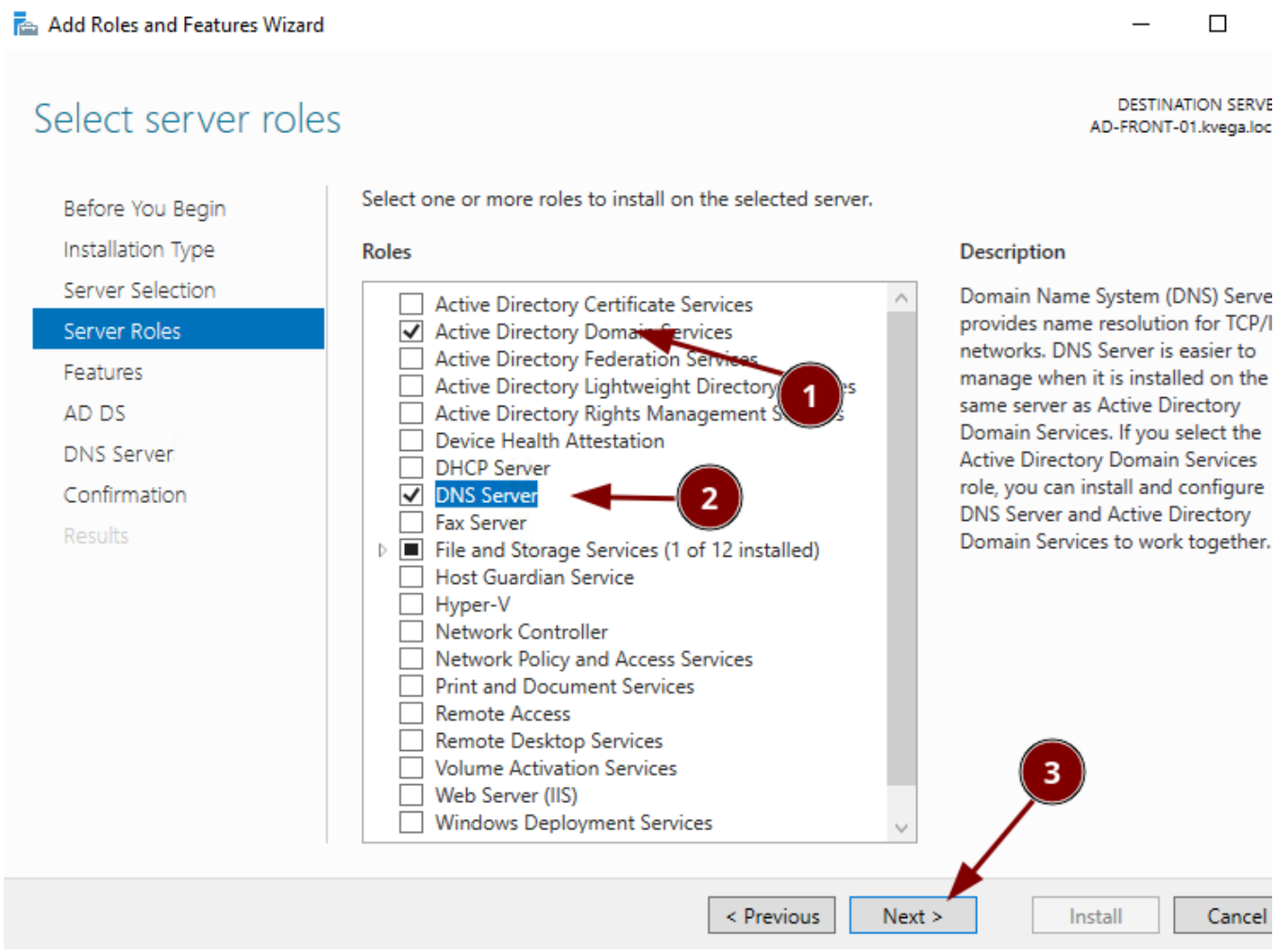
1. Ouvrir le Server Manager
2. Ajouter des rôles et des fonctionnalités

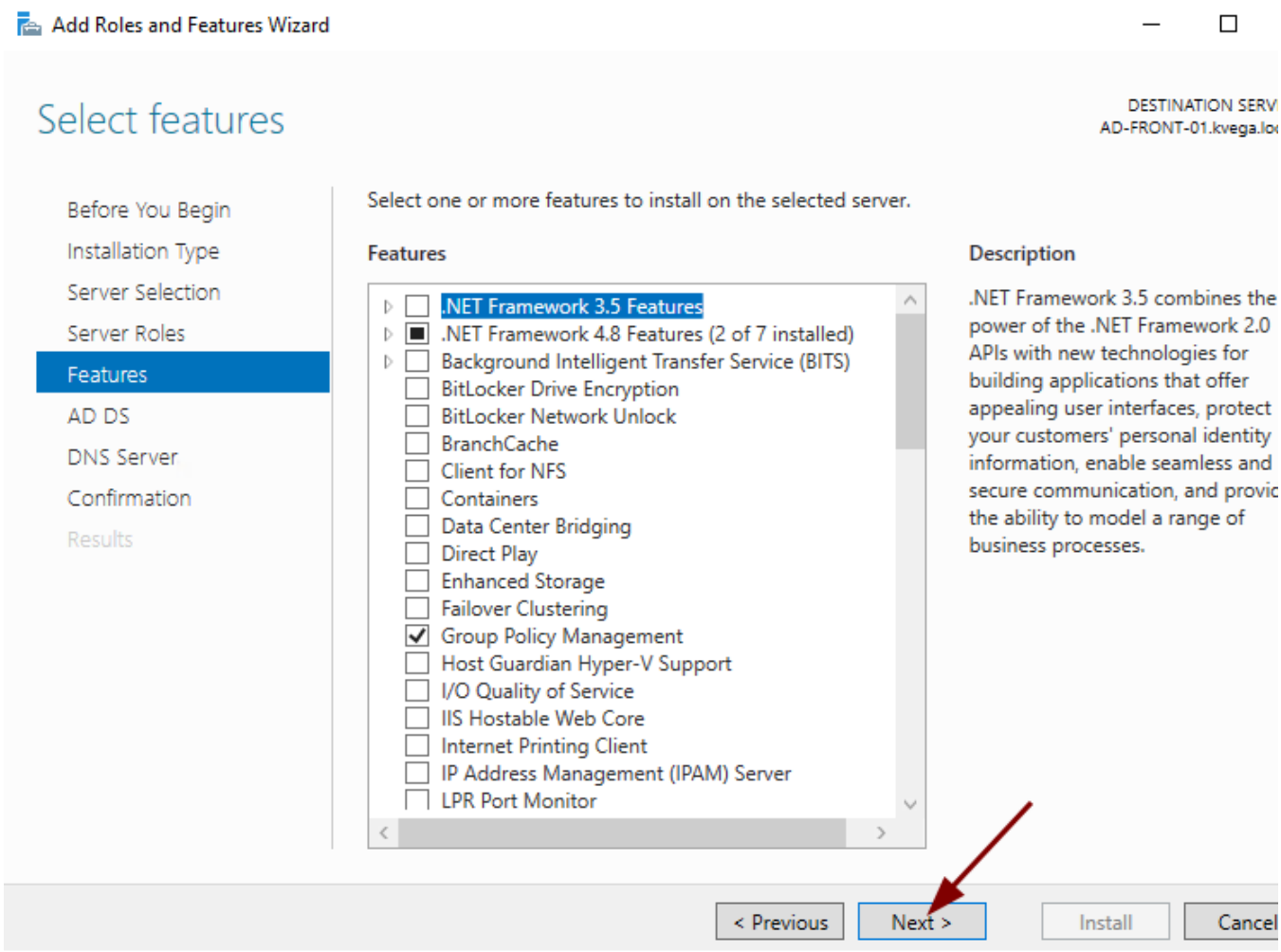



Add Roles and Features Wizard
Before you begin
DESTINATION SERV
AD-FRONT-01.kvega.lo
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
This wizard helps you install roles, role services, or features. You determine which roles, role services,
features to install based on the computing needs of your organization, such as sharing documents, c
hosting a website.
To remove roles, role services, or features:
Start the Remove Roles and Features Wizard
Before you continue, verify that the following tasks have been completed:
• The Administrator account has a strong password
• Network settings, such as static IP addresses, are configured
• The most current security updates from Windows Update are installed
If you must verify that any of the preceding prerequisites have been completed, close the wizard,
complete the steps, and then run the wizard again.
To continue, click Next.
1
Skip this page by default
2
< Previous
Next >
Install
Cance


Add Roles and Features Wizard
Select installation type
DESTINATION SERV
AD-FRONT-01.kvega.lo
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select the installation type. You can install roles and features on a running physical computer or virtu
machine, or on an offline virtual hard disk (VHD).
Role-based or feature-based installation
Configure a single server by adding roles, role services, and features.
Remote Desktop Services installation
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-ba
or session-based desktop deployment.
< Previous
Next >
Install
Cancel


Add Roles and Features Wizard
Select destination server
DESTINATION SERV
AD-FRONT-01.kvega.lo
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select a server or a virtual hard disk on which to install roles and features.
Select a server from the server pool
Select a virtual hard disk
Server Pool
Filter:
Name
IP Address
Operating System
AD-FRONT-01.kvega.local
192.168.1.168
Microsoft Windows Server 2022 Datacenter
1 Computer(s) found
This page shows servers that are running Windows Server 2012 or a newer release of Windows Serve
and that have been added by using the Add Servers command in Server Manager. Offline servers an
newly-added servers from which data collection is still incomplete are not shown.
< Previous
Next >
Install
Cance


Add Roles and Features Wizard
Select server roles
DESTINATION SERVE
AD-FRONT-01.kvega.loc
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
Active Directory Rights Management
Device Health Attestation
DHCP Server
DNS Server
Fax Server
File and Storage Services (1 of 12 installed)
Host Guardian Service
Hyper-V
Network Controller
Network Policy and Access Services
Print and Document Services
Remote Access
Remote Desktop Services
Volume Activation Services
Web Server (IIS)
Windows Deployment Services
Description
Domain Name System (DNS) Serve
provides name resolution for TCP/I
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.
1
2
3
< Previous
Next >
Install
Cancel


Add Roles and Features Wizard
Select features
DESTINATION SERV
AD-FRONT-01.kvega.lo
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
DNS Server
Confirmation
Results
Select one or more features to install on the selected server.
Features
.NET Framework 3.5 Features
.NET Framework 4.8 Features (2 of 7 installed)
Background Intelligent Transfer Service (BITS)
BitLocker Drive Encryption
BitLocker Network Unlock
BranchCache
Client for NFS
Containers
Data Center Bridging
Direct Play
Enhanced Storage
Failover Clustering
Group Policy Management
Host Guardian Hyper-V Support
I/O Quality of Service
IIS Hostable Web Core
Internet Printing Client
IP Address Management (IPAM) Server
LPR Port Monitor
Description
.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provic the ability to model a range of business processes.
< Previous
Next >
Install
Cancel

Add Roles and Features Wizard

Active Directory Domain Services

DESTINATION SERV
AD-FRONT-01.kvega.lo

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features
- AD DS
- DNS Server
- Confirmation
- Results

Active Directory Domain Services (AD DS) stores information about users, computers, and other devi
on the network. AD DS helps administrators securely manage this information and facilitates resourc
sharing and collaboration between users.

Things to note:

- To help ensure that users can still log on to the network in the case of a server outage, install a minimum of two domain controllers for a domain.
- AD DS requires a DNS server to be installed on the network. If you do not have a DNS server installed, you will be prompted to install the DNS Server role on this machine.

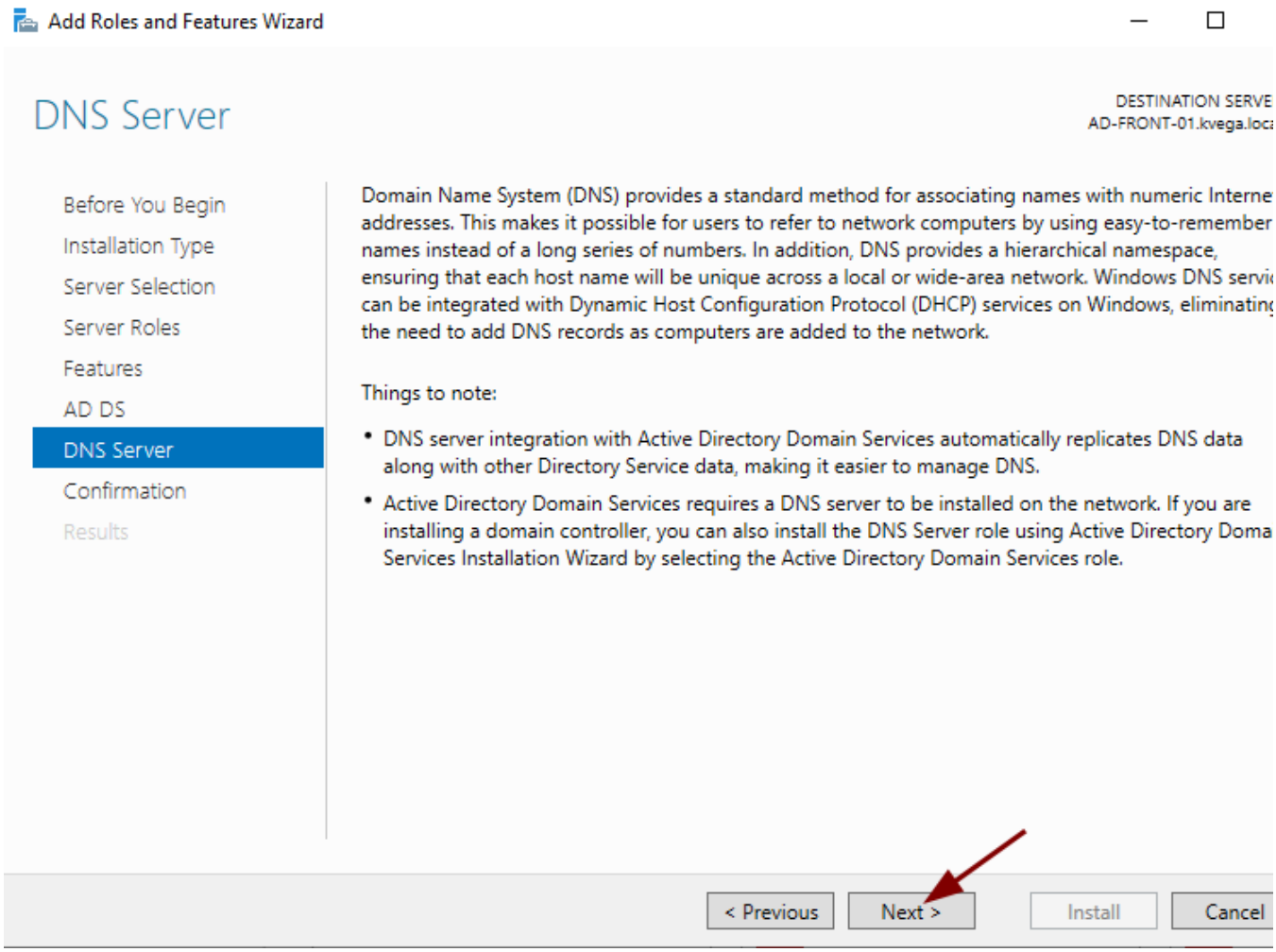


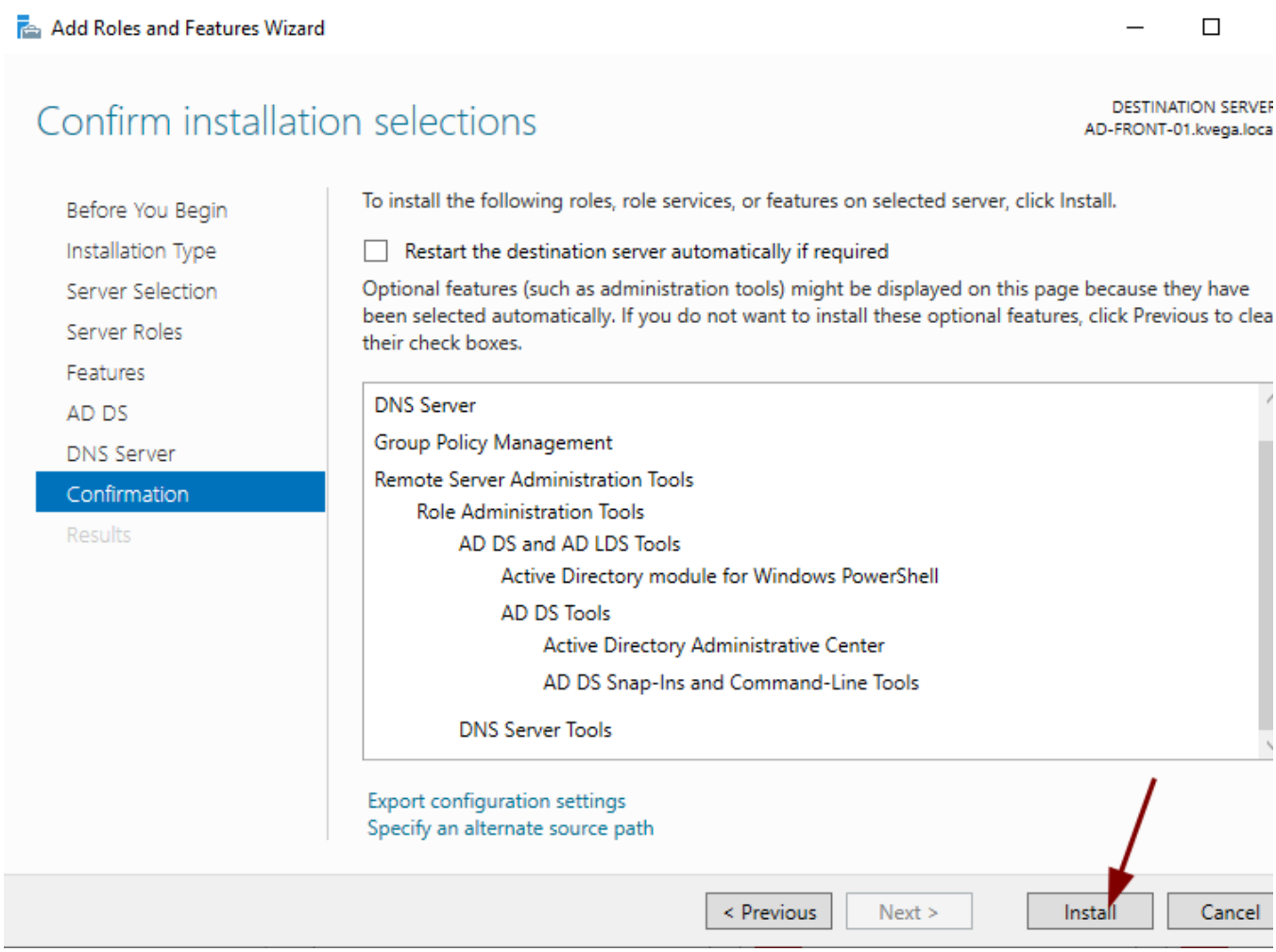
Azure Active Directory, a separate online service, can provide simplified identity and access management, security reporting, single sign-on to cloud and on-premises web apps.

Learn more about Azure Active Directory

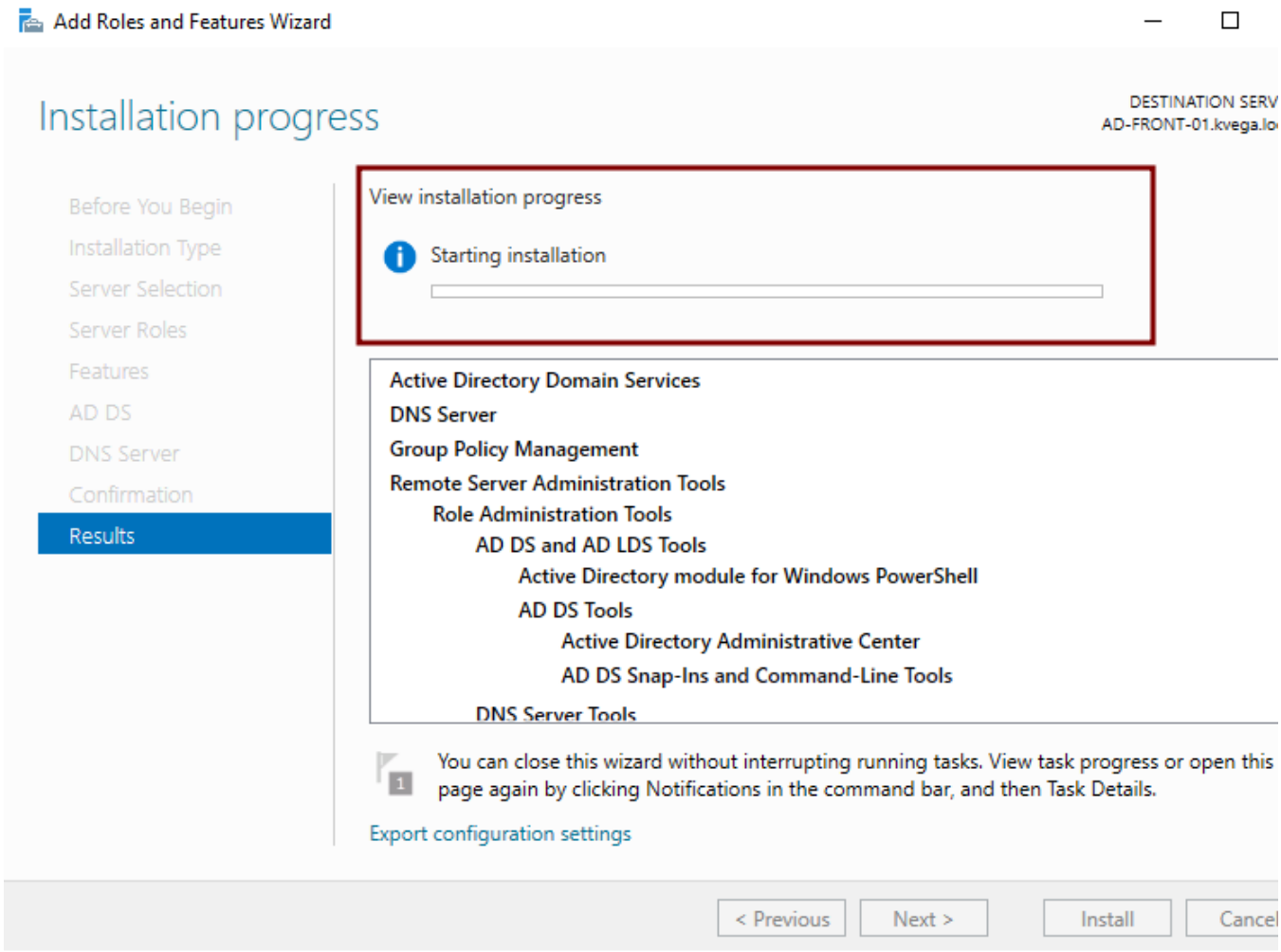
Configure Office 365 with Azure Active Directory Connect

< Previous | Next > | Install | Cancel

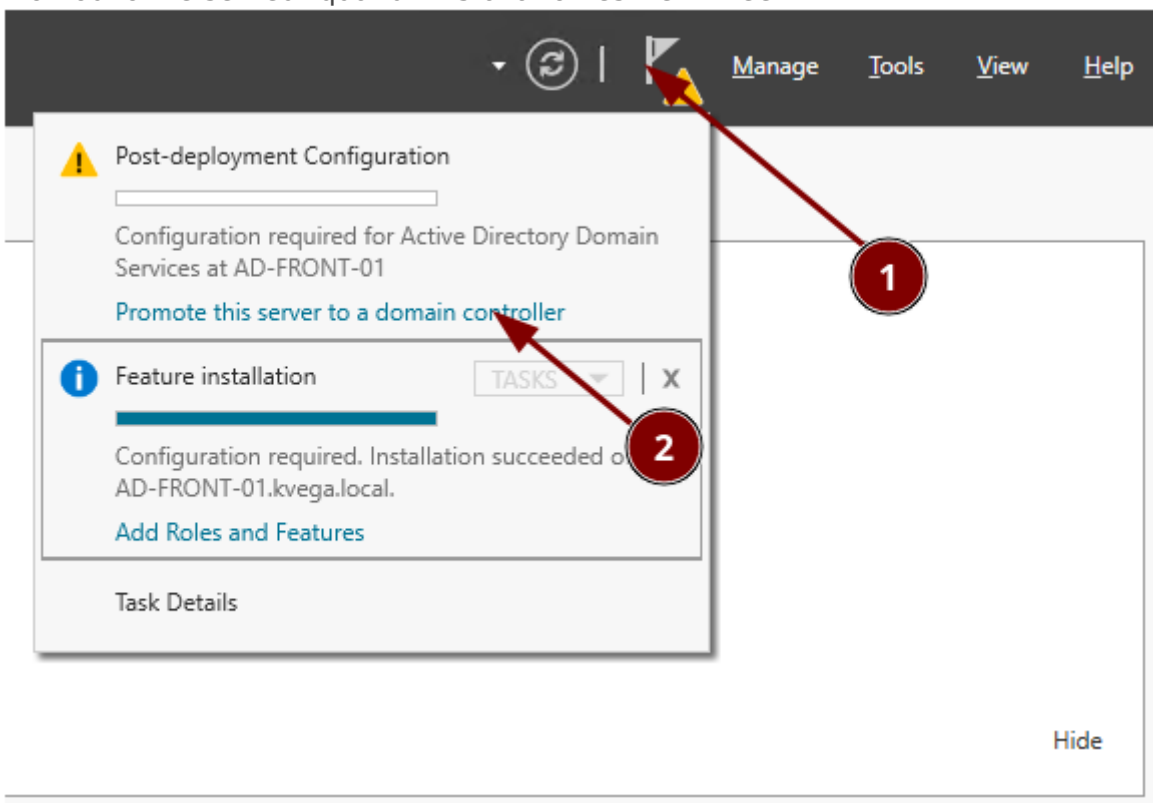

Add Roles and Features Wizard
DNS Server
DESTINATION SERVE
AD-FRONT-01.kvega.loc
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
DNS Server
Confirmation
Results
Domain Name System (DNS) provides a standard method for associating names with numeric Interne
addresses. This makes it possible for users to refer to network computers by using easy-to-remember
names instead of a long series of numbers. In addition, DNS provides a hierarchical namespace,
ensuring that each host name will be unique across a local or wide-area network. Windows DNS servi
can be integrated with Dynamic Host Configuration Protocol (DHCP) services on Windows, eliminatin
the need to add DNS records as computers are added to the network.
Things to note:
DNS server integration with Active Directory Domain Services automatically replicates DNS data along with other Directory Service data, making it easier to manage DNS.
Active Directory Domain Services requires a DNS server to be installed on the network. If you are installing a domain controller, you can also install the DNS Server role using Active Directory Doma Services Installation Wizard by selecting the Active Directory Domain Services role.
< Previous
Next >
Install
Cancel



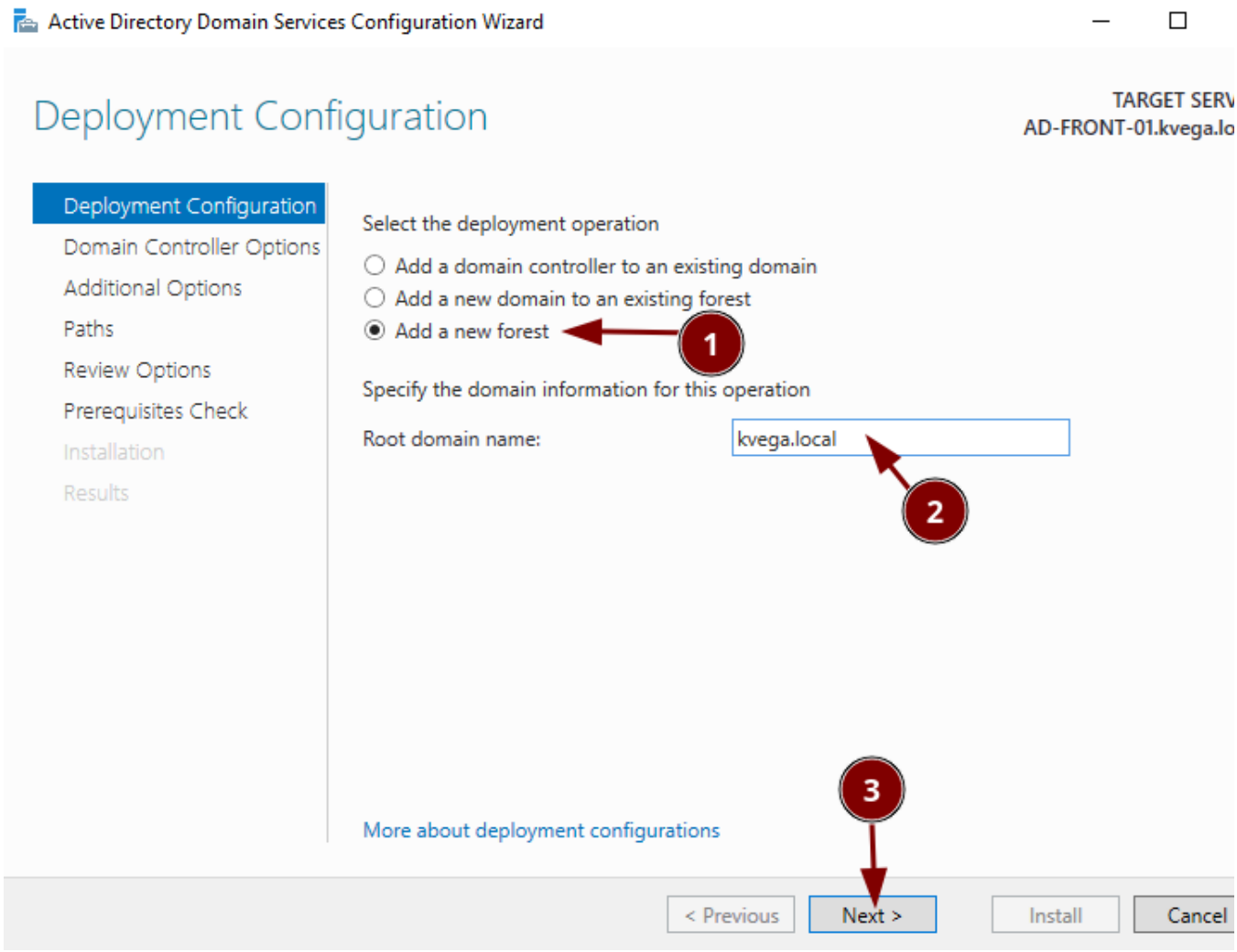
3. Attente de la fin d'installation



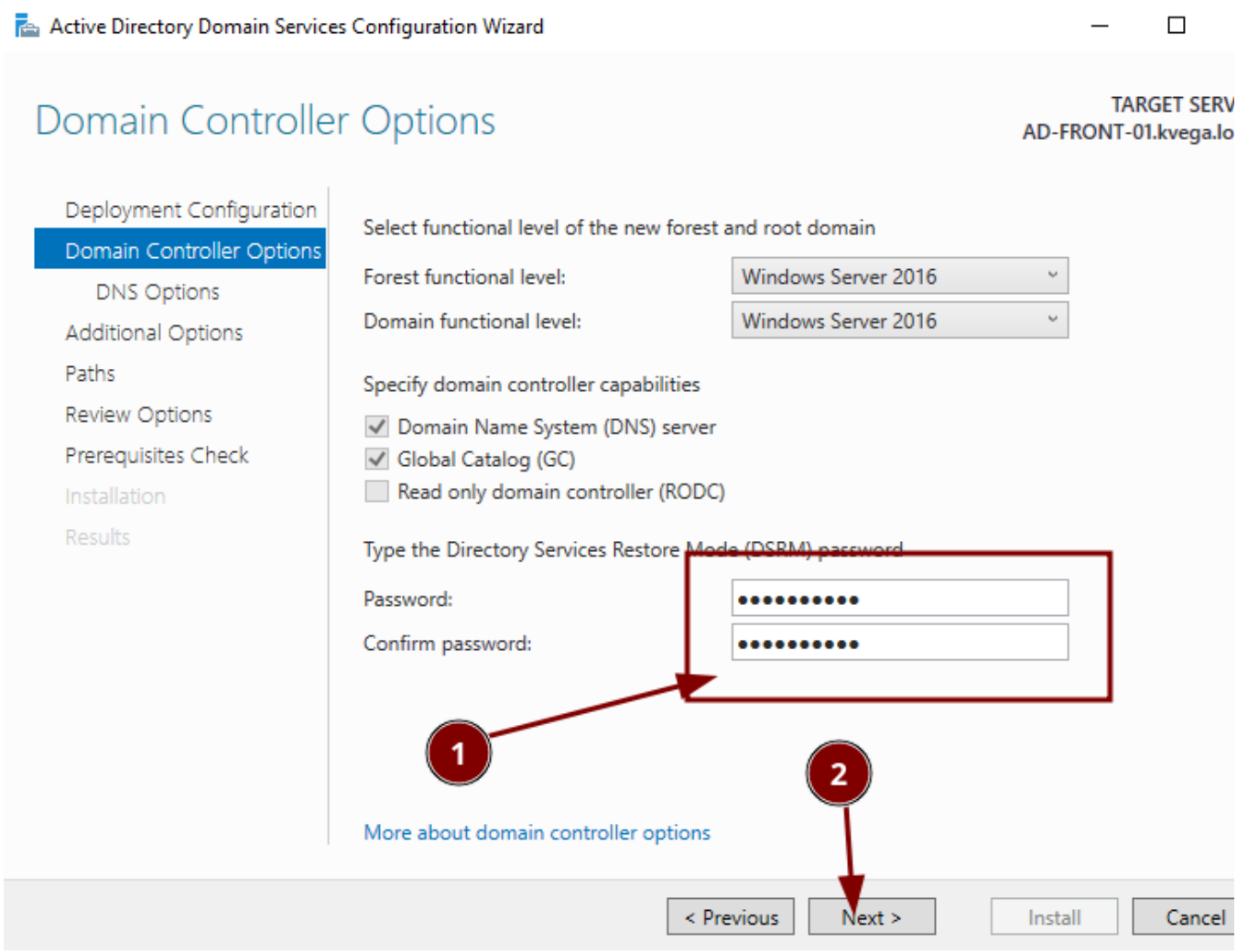
4. Promouvoir le serveur quand l'installation est terminée



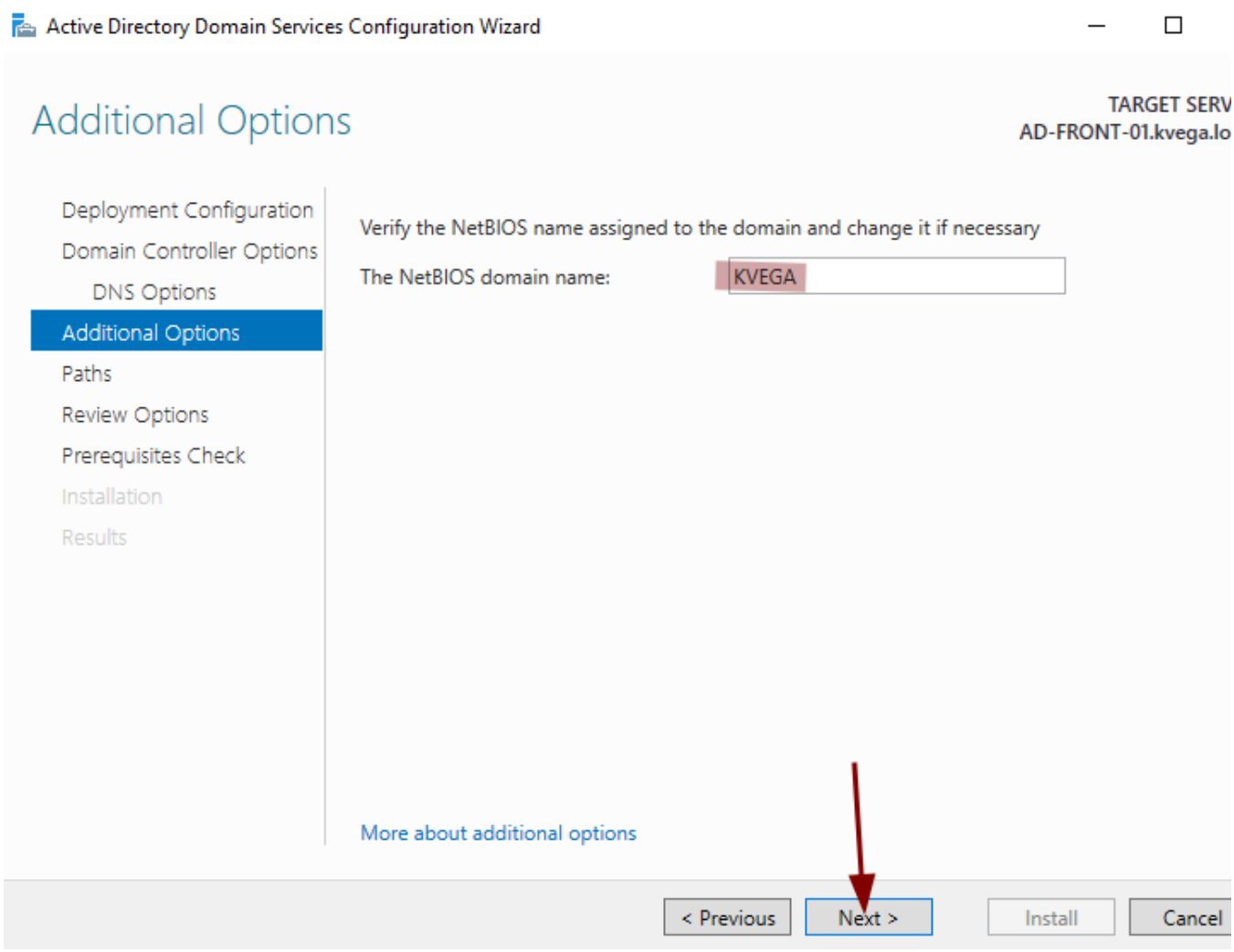
5. Créer la nouvelle forêt



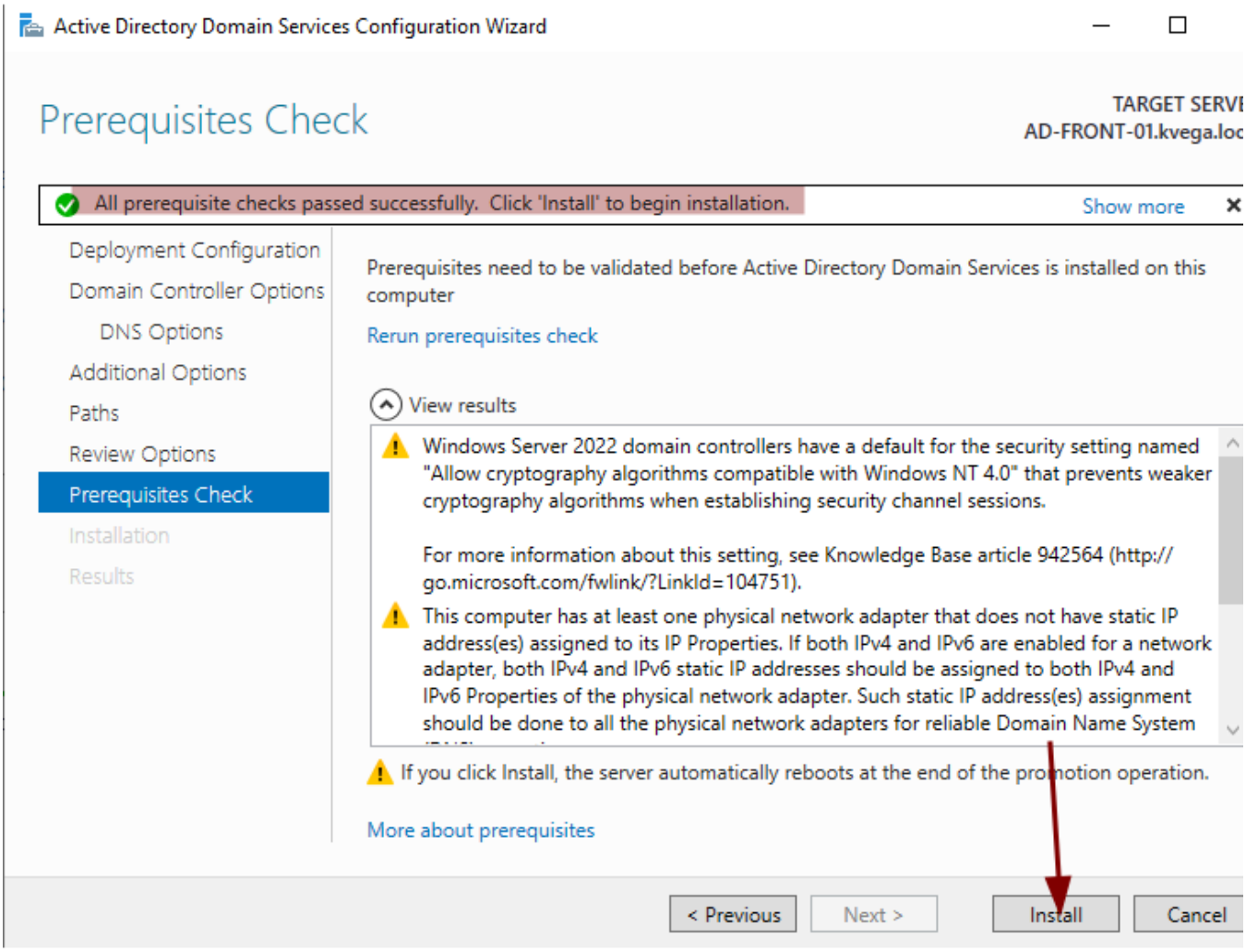
6. Créer le mot de passe de récupération



7. Ne pas créer de délégation DNS. Faire Next
8. Laisser le nom netbios par défault



9. Laisser les chemins par défaut
10. Réviser les modifications éffectuées
11. Laisser le check tourner et installer



12. Une fois installé si le serveur ne redémarre pas de lui même, le redémarrer à la main

---

Installation d’un active Directory Mode CORE

> Prérequis : Network OK, Sur le domaine et le bon nom d’ordinateur

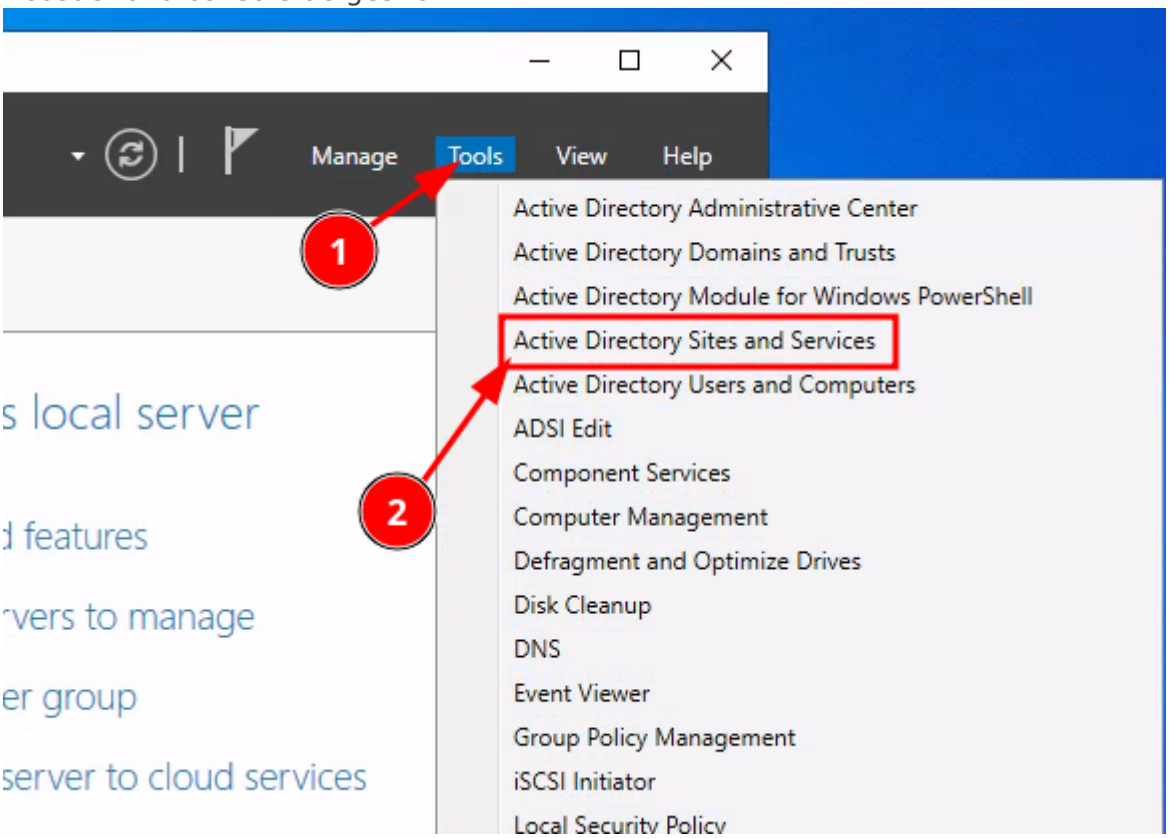
```
install-windowsfeature AD-Domain-Services
Install-ADDSDomainController -InstallDns -Credential (Get-Credential "CORP\Administrator") -
DomainName "corp.contoso.com"
```

UTILISATEUR ET GROUPES

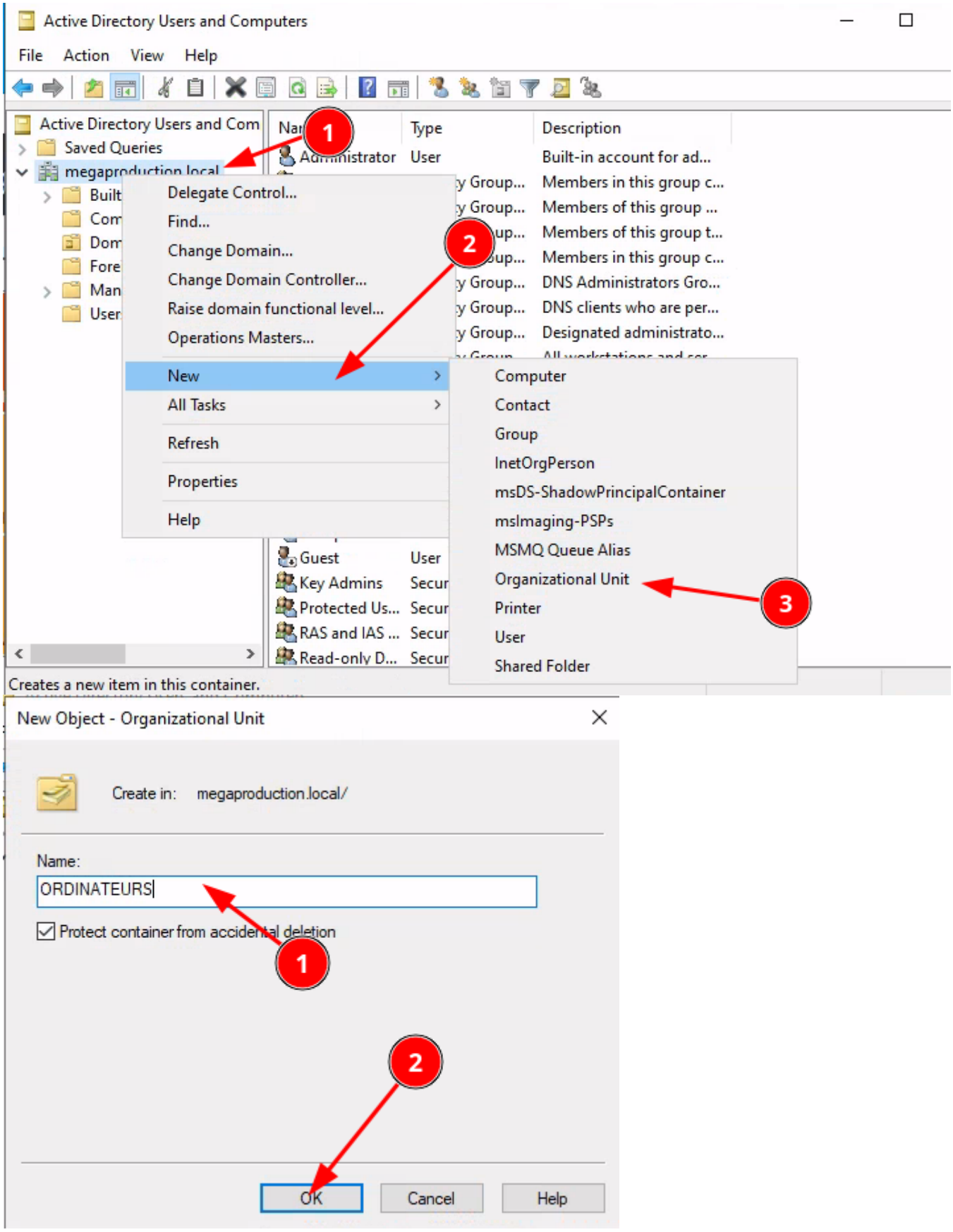
CREATION ET GESTION DES OU

Création des OU

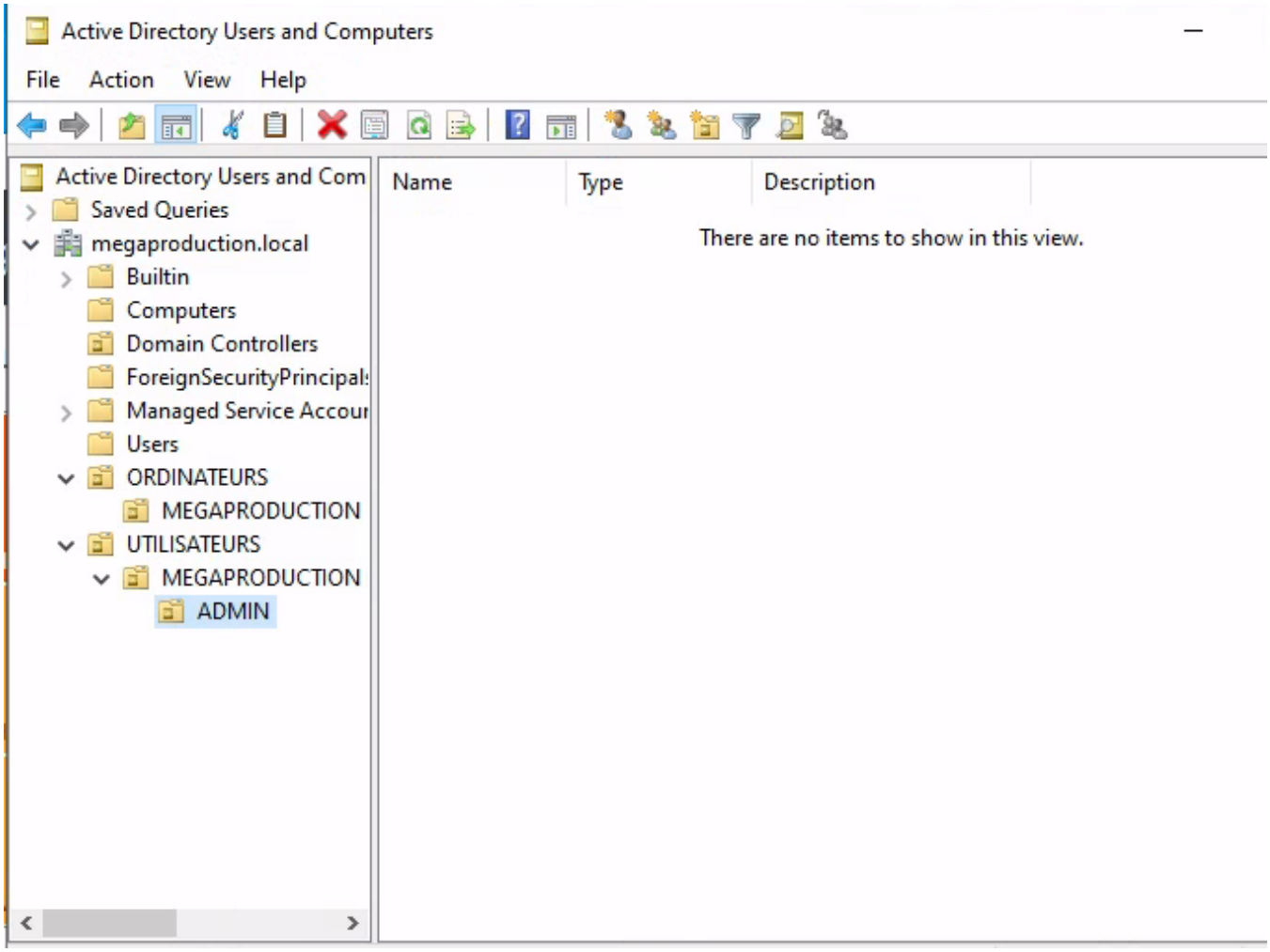
1. Accéder à la console de gestion active directory
    1. Ouvrir server manager
    2. Accéder à la console de gestion



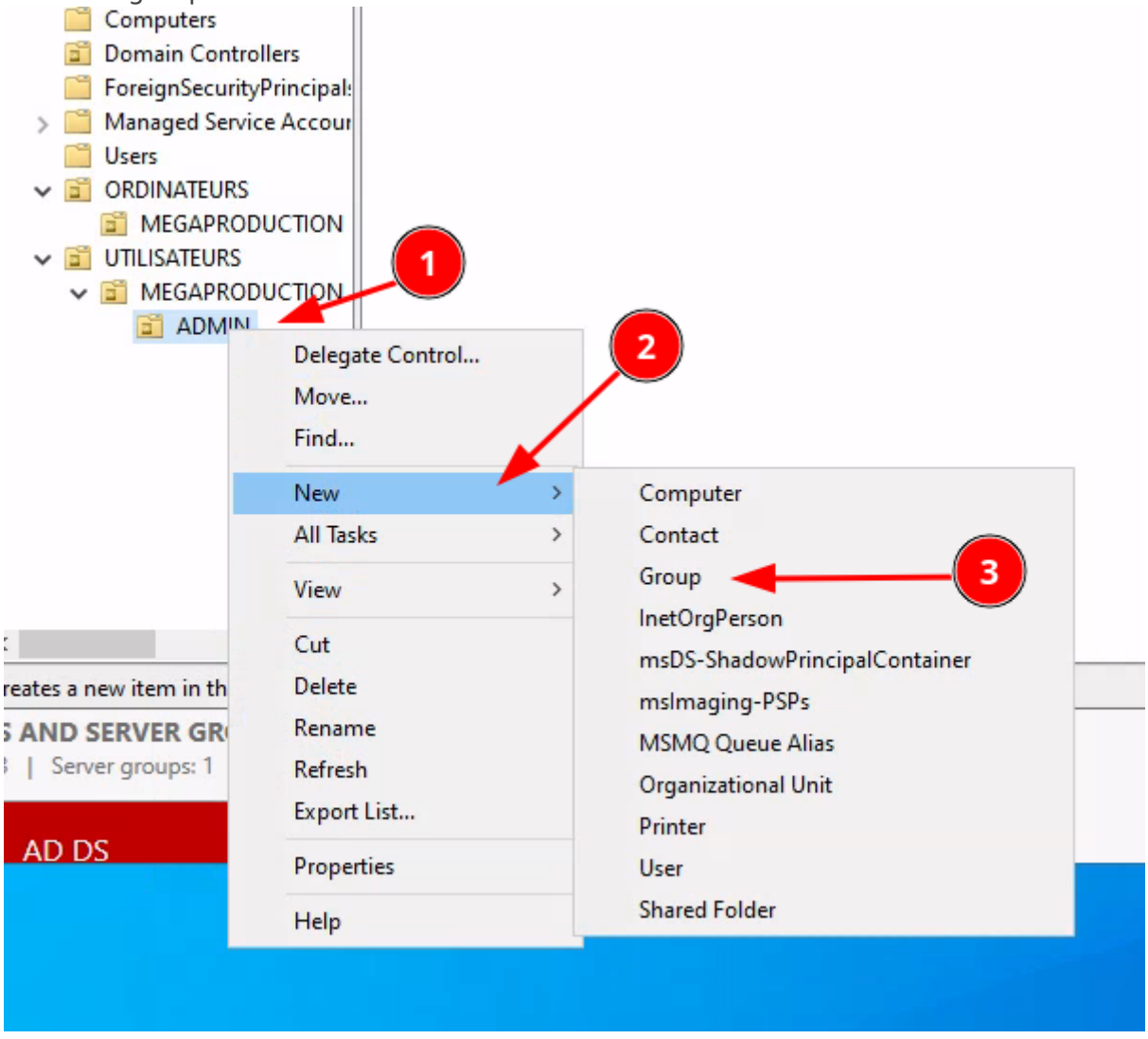
2. Créer une unité d'organisation



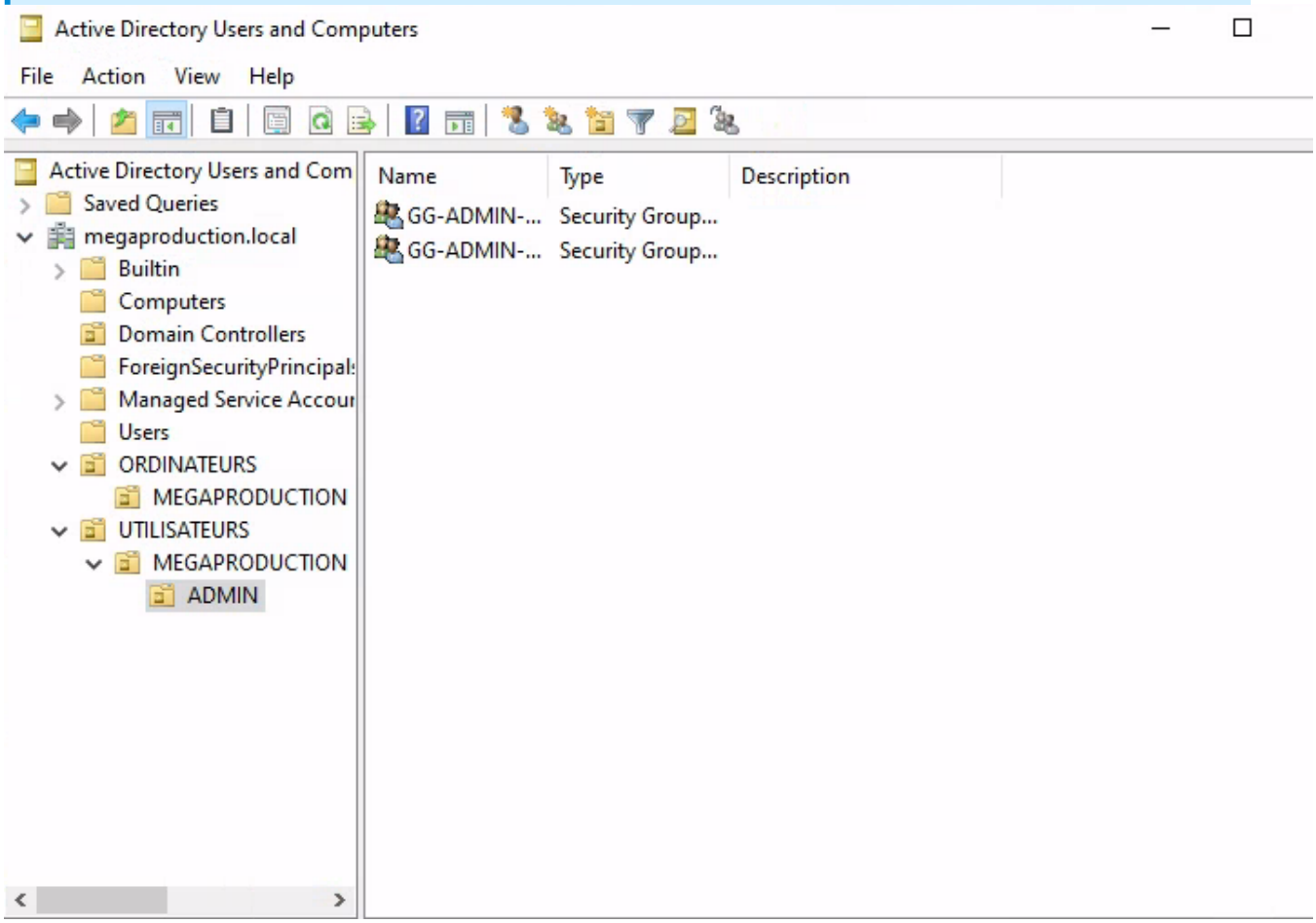
Exemple de ce qui devrait être en place après la création des OUs:



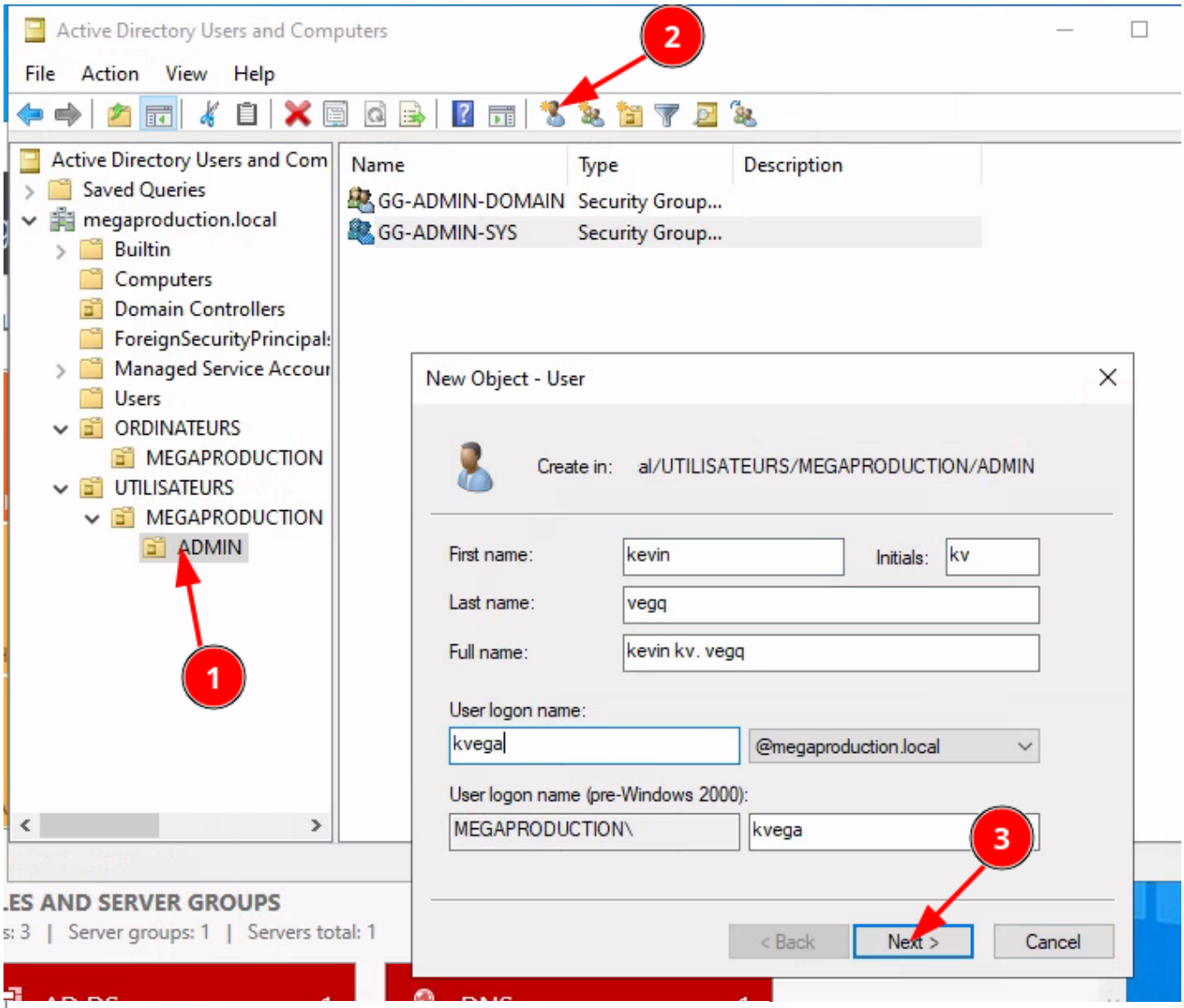
3. Créer un groupes dans la bonne OU:

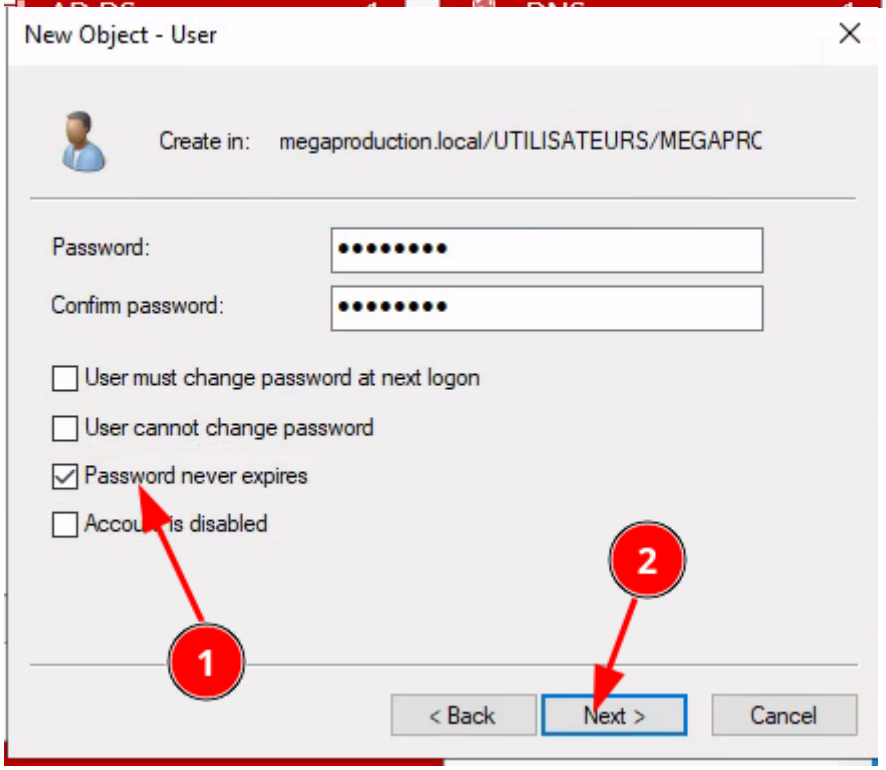


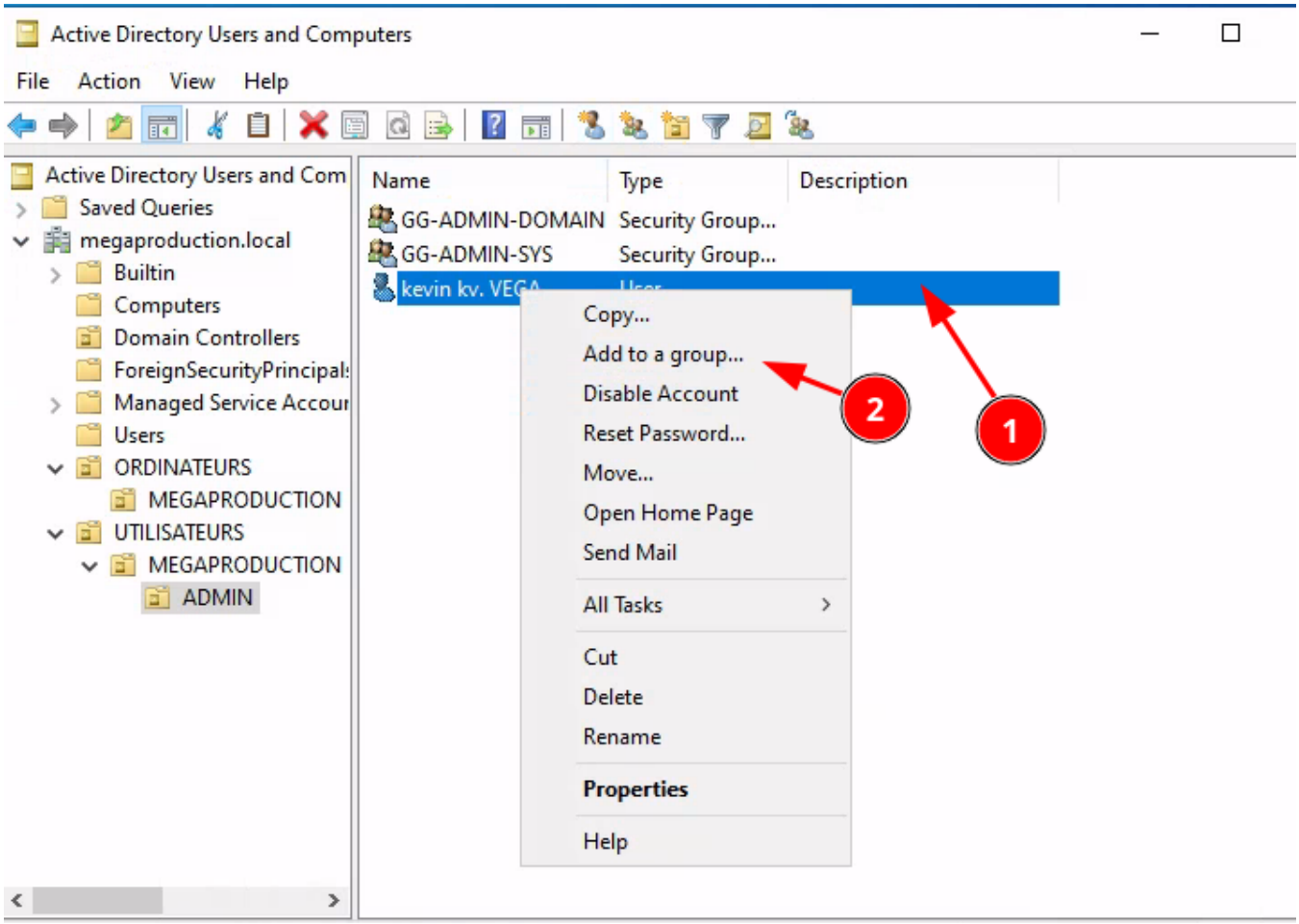
> On remarquera qu’il existe 2 familles de groupe, les groupes de sécurité (Affectation de droits) et les
> groupes de distribution (utilisé pour la messagerie).

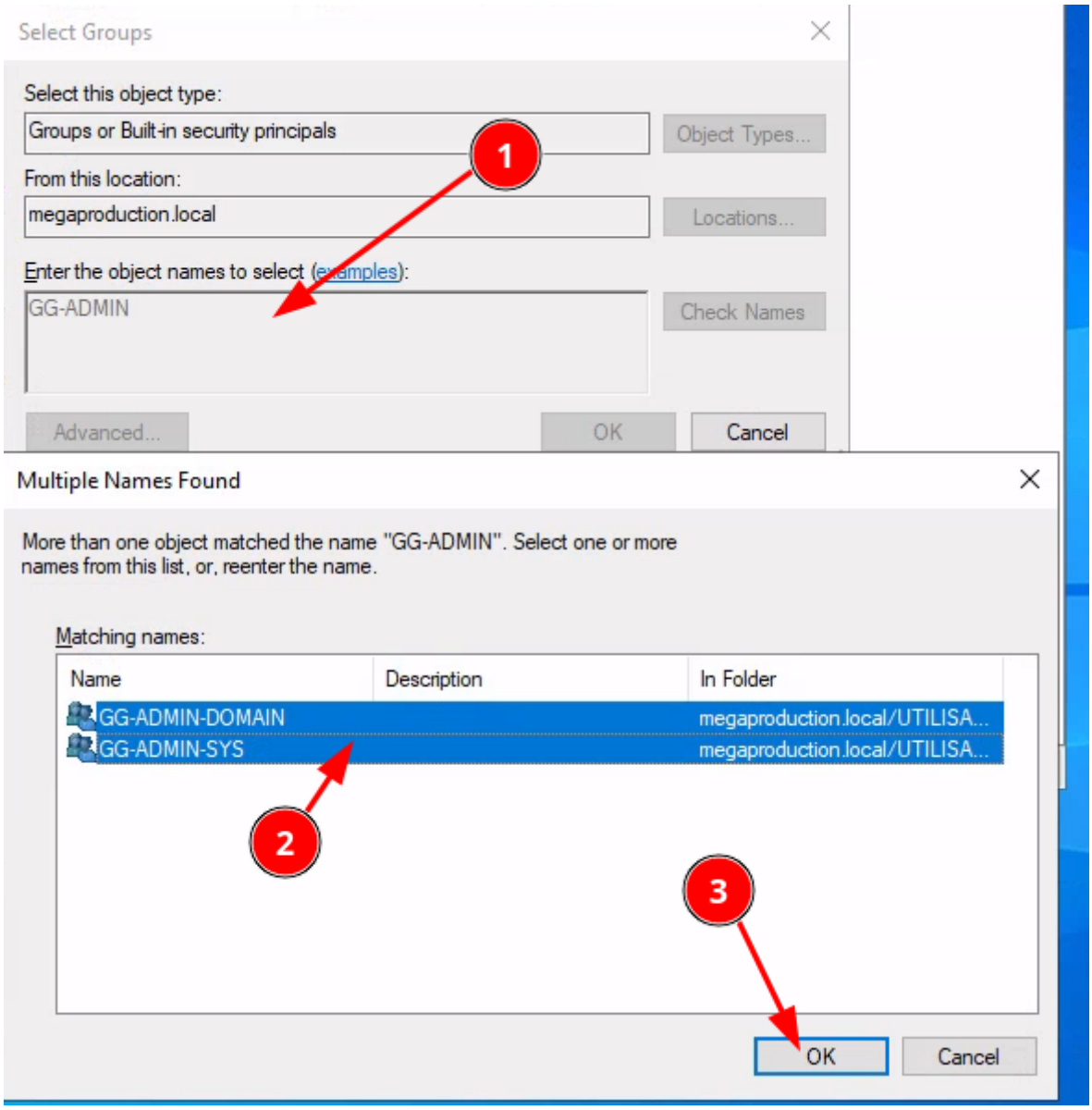


4. Créer un utilisateur et le mettre dans un groupe


Active Directory Users and Computers
File Action View Help
Active Directory Users and Com
Saved Queries
megaproduction.local
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipal:
Managed Service Accour
Users
ORDINATEURS
MEGAPRODUCTION
UTILISATEURS
MEGAPRODUCTION
ADMIN
Name
Type
Description
GG-ADMIN-DOMAIN
Security Group...
GG-ADMIN-SYS
Security Group...
2
1
New Object - User
Create in: al/UTILISATEURS/MEGAPRODUCTION/ADMIN
First name:
kevin
Initials:
kv
Last name:
vegq
Full name:
kevin kv. vegq
User logon name:
kvega
@megaproduction.local
User logon name (pre-Windows 2000):
MEGAPRODUCTION\
kvega
3
< Back
Next >
Cancel
ES AND SERVER GROUPS
s: 3 | Server groups: 1 | Servers total: 1


New Object - User
Create in: megaproduction.local/UTILISATEURS/MEGAPRC
Password:
Confirm password:
User must change password at next logon
User cannot change password
Password never expires
Accou is disabled
1
2
< Back
Next >
Cancel


Active Directory Users and Computers
File
Action
View
Help
Active Directory Users and Com
Saved Queries
megaproduction.local
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipal:
Managed Service Accour
Users
ORDINATEURS
MEGAPRODUCTION
UTILISATEURS
MEGAPRODUCTION
ADMIN
Name
Type
Description
GG-ADMIN-DOMAIN
Security Group...
GG-ADMIN-SYS
Security Group...
kevin kv. VEGA
Copy...
Add to a group...
Disable Account
Reset Password...
Move...
Open Home Page
Send Mail
All Tasks
Cut
Delete
Rename
Properties
Help
1
2



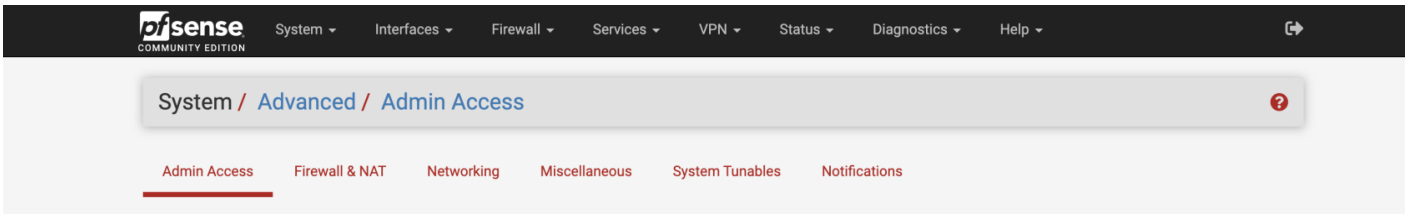
5. Faire en sorte que tous les nouveaux ordinateurs ajoutés au domaine aillent par défaut dans l'OU Ordinateurs\MEGAPRODUCTION
   1. Ouvrez un powershell et taper

```
PS C:\Users\Administrator> redircmp.exe
OU=megaproduction,OU=ORDINATEURS,DC=megaproduction,DC=local
Redirection was successful.
```

Ajouter PfSense à l'active directory

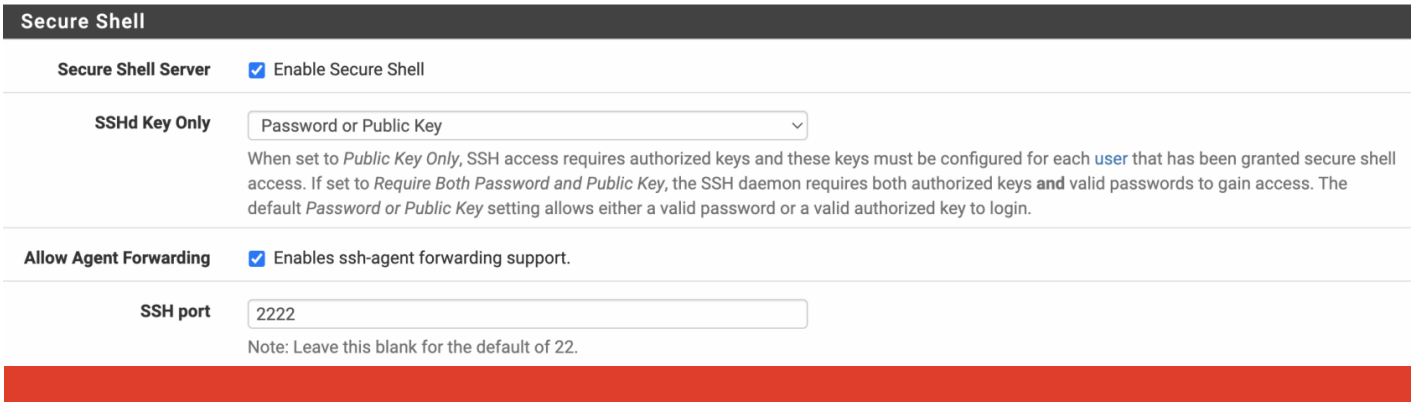
On va commencer par activer le secure shell pour administrer la VM en ssh.

Acceder à PfSense -> System -> Advanced -> Admin Access



Enable + Enable ssh-agent

On renseigne le ssh port en **2222**



Se connecter en ssh à l'infra **192.168.1.4** dans mon cas.

Puis se connecter au PfSense

```
ssh root@192.168.1.4 -p 2222
```

(user@ipPfsense -p PortConfiguré)

```
jules@MacBook-Pro-de-Navarro ~ % ssh jg@192.168.1.4
jg@192.168.1.4's password:
Linux adm-front-01 6.8.4-2-pve #1 SMP PREEMPT_DYNAMIC PMX 6.8.4-2 (2024-04-10T17:36Z)
x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Dec 10 10:17:56 2024 from 192.168.1.21
❯ ssh root@192.168.1.4 -p 2222
KVM Guest - Netgate Device ID: 2f8a84bd2402715342fc

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on fw-front-01 ***

 WAN (wan)       -> vtnet0     -> v4: 192.168.1.4/26
 LAN (lan)       -> vtnet1     -> v4: 172.16.1.1/27
 DMZ (opt1)      -> vtnet2     -> v4: 10.10.10.1/28

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Disable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option:
```

Option 8 (Shell)

On va éditer :

```
/usr/local/etc/pkg/repos/pfSense.conf
```

```
FreeBSD: { enabled: yes }


pfSense-core: {
    url: "pkg+https://pkg.pfsense.org/pfSense_v2_7_2_amd64-core",
    mirror_type: "srv",
    signature_type: "fingerprints",
    fingerprints: "/usr/local/share/pfSense/keys/pkg",
    enabled: yes
}
```

```
pfSense: {
    url: "pkg+https://pkg.pfsense.org/pfSense_v2_7_2_amd64-pfSense_v2_7_2",
    mirror_type: "srv",
    signature_type: "fingerprints",
    fingerprints: "/usr/local/share/pfSense/keys/pkg",
    enabled: yes
}
```

ET

```
/usr/local/etc/pkg/repos/FreeBSD.conf
```

```
            FreeBSD: {
                url: "pkg+https://pkg.freebsd.org/${ABI}/latest",
                enabled: true,
                signature_type: "fingerprints",
                fingerprints: "/usr/share/keys/pkg",
                mirror_type: "srv"
            }
```

On installe maintenant les packets

```
pkg install -y adcli sssd2 samba416
```

Une fois installés, on va éditer :

```
/etc/krb5.conf
```

```
[logging]
default = FILE:/var/log/krb5libs.log

[libdefaults]
default_realm = megaproduction.local
dns_lookup_realm = true
dns_lookup_kdc = true
ticket_lifetime = 24h
renew_lifetime = 7d
forwardable = true
rdns = false
```

default_realm = Nom de domaine

```
/usr/local/etc/smb4.conf
```

```
[global]
security = ads
realm = MEGAPRODUCTION.LOCAL
workgroup = MEGAPRODUCTION
log file = /var/log/samba/%m.log
log level = 3
kerberos method = secrets and keytab
client signing = yes
load printers = no
cups options = raw
printcap name = /dev/null
ntlm auth = disabled
idmap config MYDOMAIN: backend = sss
idmap config MYDOMAIN: range = 200000-2147483647
idmap config * : backend = tdb
idmap config * : range   = 100000-199999
inherit acls = no
server min protocol = SMB3
map to guest = bad user
unix extensions = no
```

(EN MAJUSCULE)

realm = NOM DE DOMAINE.LOCAL
workgroup = NOM DE DOMAINE

On redémarre les services

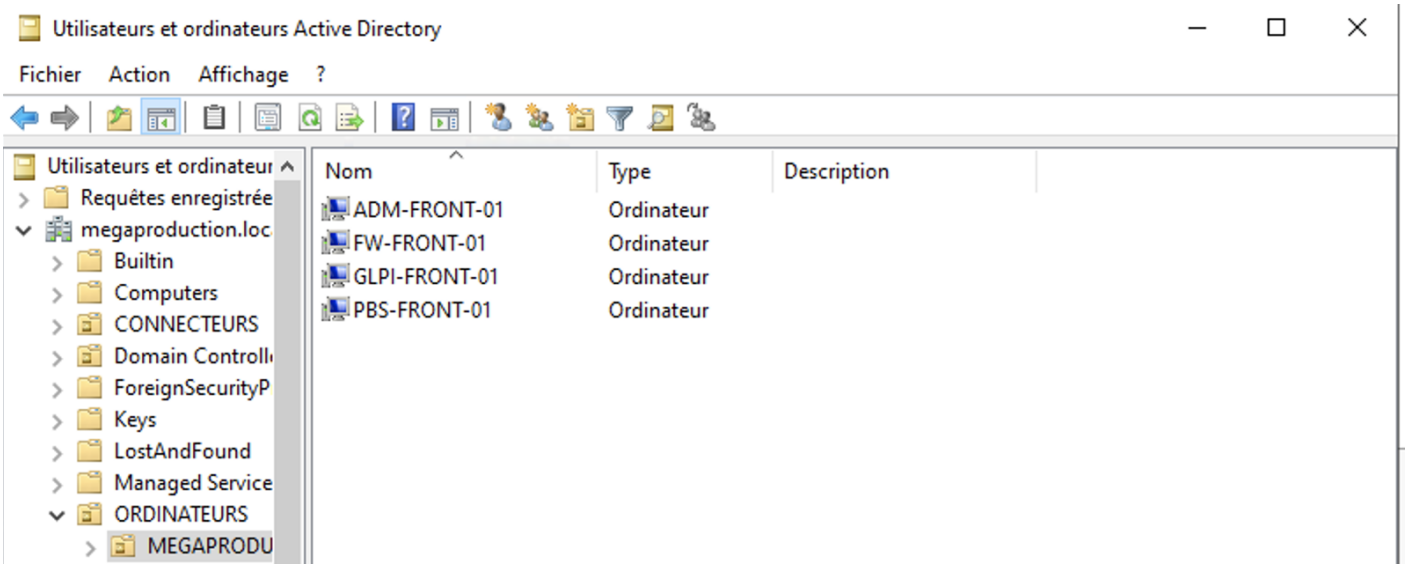
```
service kerberos restart && service samba_server restart
```

Maintenant, on va pouvoir découvrir la machine :

```
net ads join -U administrateur@megaproduction.local
```

```
[2.7.2-RELEASE][admin@fw-front-01.megaproduction.local]/root: net ads join -U administ
rateur@megaproduction.local
Password for [administrateur@megaproduction.local]:
Using short domain name -- MEGAPRODUCTION
Joined 'FW-FRONT-01' to dns domain 'megaproduction.local'
```

Voilà la machine est maintenant ajoutée à l'AD.


Utilisateurs et ordinateurs Active Directory
Fichier
Action
Affichage
?
Utilisateurs et ordinateur
Requêtes enregistrée
megaproduction.loc
Builtin
Computers
CONNECTEURS
Domain Controll
ForeignSecurityP
Keys
LostAndFound
Managed Service
ORDINATEURS
MEGAPRODU
Nom
Type
Description
ADM-FRONT-01
Ordinateur
FW-FRONT-01
Ordinateur
GLPI-FRONT-01
Ordinateur
PBS-FRONT-01
Ordinateur

Ajouter machine linux a l'AD

Ajout d'une machine linux a l'ad

prérequis:

- machine linux qui ping l'active directory

aller sur la machine linux et installé ces outils:

apt update && apt upgrade

apt install realmd sssd sssd-tools libnss-sss libpam-sss adcli samba-common krb5-user chrony

une fois l'installation faite faire:

realm discover "nom de domaine de l'ad"

```
root@sql-front-01:~# realm discover megaproduction.local
megaproduction.local
  type: kerberos
  realm-name: MEGAPRODUCTION.LOCAL
  domain-name: megaproduction.local
  configured: no
  server-software: active-directory
  client-software: sssd
  required-package: sssd-tools
  required-package: sssd
  required-package: libnss-sss
  required-package: libpam-sss
  required-package: adcli
  required-package: samba-common-bin
root@sql-front-01:~#
```

ensuite on join le domaine avec realm join -U "votrecompteAD" "nom de domaine de l'ad"

erreur normal:

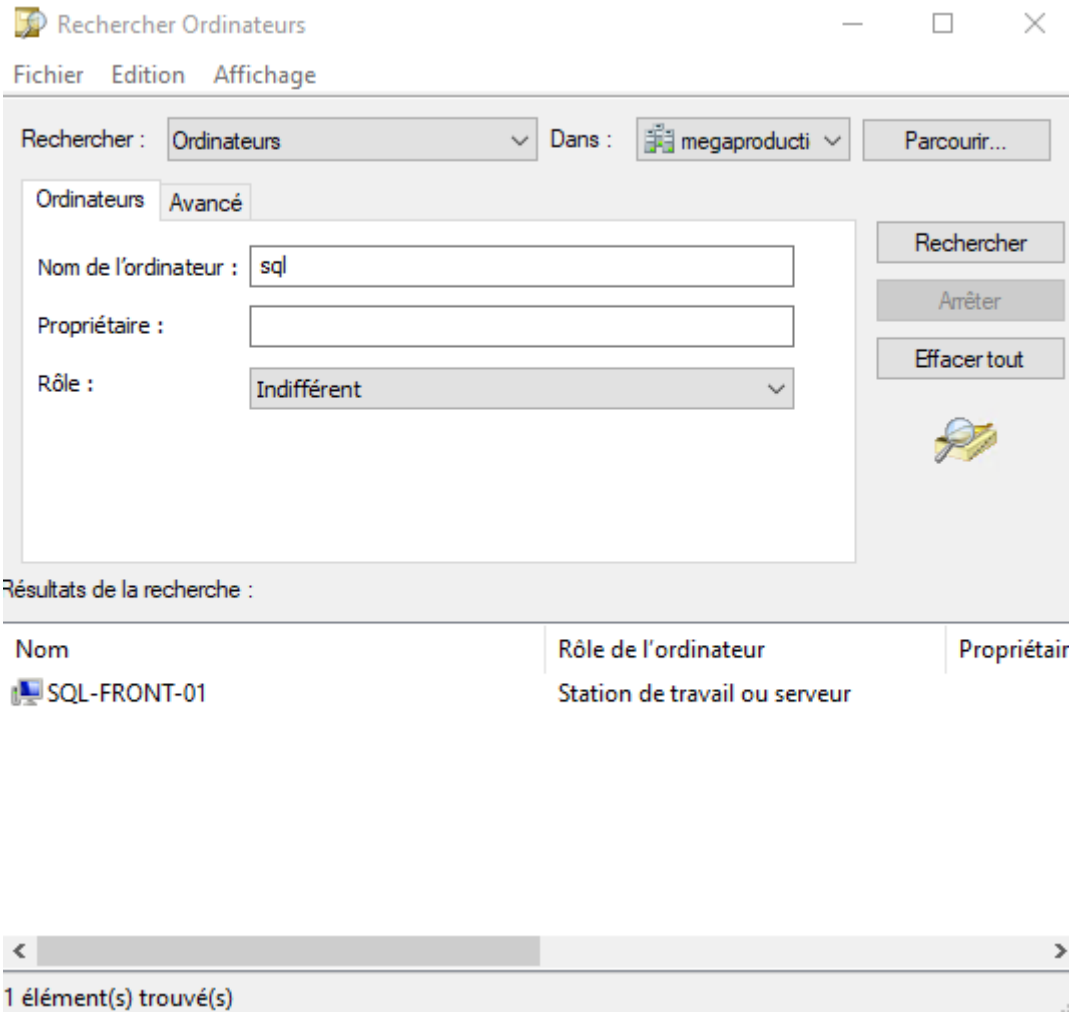
```
root@sql-front-01:~# sudo realm join -U Administrateur megaproduction.local
Password for Administrateur:
See: journalctl REALMD_OPERATION=r27965.3383
realm: Couldn't join realm: Necessary packages are not installed: sssd-tools sssd libnss-sss libpam-sss adc
li
root@sql-front-01:~#
```

il faut installer des outils supplémentaire:

apt update
apt install packagekit

ensuite on a juste a rejoindre le domaine avec nos info :

```
root@sql-front-01:~# sudo realm join -U Administrateur megaproduction.local
Password for Administrateur:
root@sql-front-01:~#
```



On a bien rejoint le domaine !