ANNEXE IV - PAGE DE GARDE DU DOSSIER PROFESSIONNEL

BREVET DE TECHNICIEN SUPERIEUR SERVICES INFORMATIQUES AUX ORGANISATIONS

Session 2026

DOSSIER PROFESSIONNEL

NOM : LANGEL

Prénom : MEWEN

Établissement de formation (sur un seul des deux exemplaires du dossier)

Visa du représentant de l'équipe pédagogique attestant la réalité des activités professionnelles décrites dans le dossier (sur un seul des deux exemplaires du dossier) :

Nom et qualité du signataire	Date	Signature

Attestation sur l'honneur pour les candidats individuels (sur un seul des deux exemplaires du dossier) :

Je soussigné(e), Mewen LANGEL, certifie que les activités décrites ainsi que les différentes informations reproduites dans ce dossier reflètent les activités professionnelles que j'ai personnellement réalisées au cours de ma formation.

Fait à Nantes, le 28/04/2026

Signature

BTS Services informatiques aux organisations **SESSION 2026**

ANNEXE VII-1-A : Fiche descriptive de réalisation professionnelle (recto)

Épreuve E6 - Administration des systèmes et des réseaux (option SISR)

DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE	**N° réalisation :** 1
Nom, prénom : LANGEL Mewen	**N° candidat :** 02302807062
Épreuve ponctuelle ☐ **Contrôle en cours de formation** ☐	**Date :** 28 / 04 / 2026

Organisation support de la réalisation professionnelle
REALIS – Infrastructure Système d'Information (projet BTS SIO SISR)

Intitulé de la réalisation professionnelle
Déploiement d'un Active Directory sur Windows Server 2022

Période de réalisation : **2025-2026** **Lieu :** Nantes, CFA SAINT FELIX LA SALLE
Modalité : ☐ **Seul(e)** ☐ **En équipe**

Compétences travaillées
- ☐ Concevoir une solution d'infrastructure réseau
- ☐ Installer, tester et déployer une solution d'infrastructure réseau
- ☐ Exploiter, dépanner et superviser une solution d'infrastructure réseau

Conditions de réalisation[1] (ressources fournies, résultats attendus)
Ressources fournies :
• Serveur Proxmox VE 9.1.1 (192.168.1.1) avec stockage local-lvm
• ISO Windows Server 2022 disponible sur Proxmox
Résultats attendus : AD Fonctionnel et opérationnel . Domaine reali.fr avec DC, DNS, DHCP, OUs, utilisateurs, GPOs, poste joint.

Description des ressources documentaires, matérielles et logicielles utilisées[2]
Déploiement d'un domaine AD reali.fr avec OUs, groupes de sécurité, utilisateurs et GPO fonctionnels
Matériel :
• PC sous Proxmox VE 9.1.1 (hyperviseur)
• VM 102 : Windows Server 2022 – 4 vCPU, 4 Go RAM, 80 Go disque (192.168.1.15)
• VM 103 : Windows 10 Client – joint au domaine reali.fr (192.168.1.50)
Logiciels :
• Proxmox VE 9.1.1, Windows Server 2022, Windows 10
• Console ADUC (Utilisateurs et ordinateurs Active Directory)
• Gestionnaire de stratégies de groupe (GPMC)
Documentation :
• Documentation procédure : Réalisation 1 - AD - Mewen LANGEL.docx

[1] En référence aux *conditions de réalisation et ressources nécessaires* du bloc « Administration des systèmes et des réseaux » prévues dans le référentiel de certification du BTS SIO.
[2] Les réalisations professionnelles sont élaborées dans un environnement technologique conforme à l'annexe II.E du référentiel du BTS SIO.

Modalités d'accès aux productions[3] et à leur documentation[4]
Documentation technique : dossier de réalisation AD (fichier .docx)
Accès à l'infrastructure : https://192.168.1.1:8006 (Proxmox VE) – Login : root mdp rootroot
VM 102 AD : 192.168.1.15 (Windows Server 2022) – Login : Administrateur mdp Azertyuiop44./
VM 103 CLIENT : 192.168.1.50 (WINDOWS 10) --- Login : (prendre un user) mdp : Azertyuiop44./
Domaine : reali.fr – Utilisateurs : francois.dupont, damien.robert, richard.premiz

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2026**

ANNEXE VII-1-A : Fiche descriptive de réalisation professionnelle (verso, éventuellement pages suivantes)

Épreuve E6 - Administration des systèmes et des réseaux (option SISR)

[3] Conformément au référentiel du BTS SIO « *Dans tous les cas, les candidats doivent se munir des outils et ressources techniques nécessaires au déroulement de l'épreuve. Ils sont seuls responsables de la disponibilité et de la mise en œuvre de ces outils et ressources. La circulaire nationale d'organisation précise les conditions matérielles de déroulement des interrogations et les pénalités à appliquer aux candidats qui ne se seraient pas munis des éléments nécessaires au déroulement de l'épreuve.* ». Les éléments nécessaires peuvent être un identifiant, un mot de passe, une adresse réticulaire (URL) d'un espace de stockage et de la présentation de l'organisation du stockage.

[4] Lien vers la documentation complète, précisant et décrivant, si cela n'a été fait au verso de la fiche, la réalisation, par exemples schéma complet de réseau mis en place et configurations des services.

Descriptif de la réalisation professionnelle, y compris les productions réalisées et schémas explicatifs

CONTEXTE

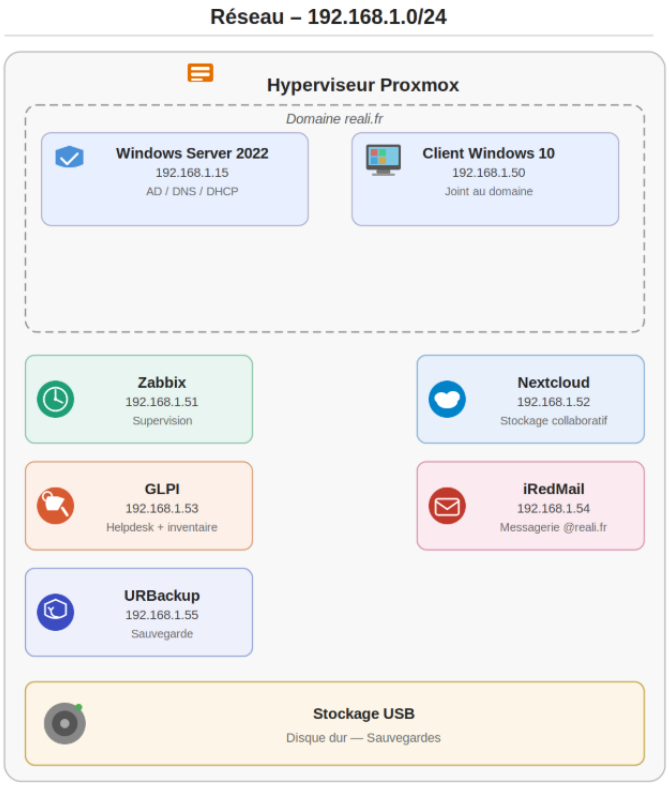
L'infrastructure REALIS est une simulation d'une PME fictive hébergée sur Proxmox VE. L'Active Directory centralise la gestion des utilisateurs et des politiques de sécurité.

CE QUI A ÉTÉ RÉALISÉ

1. Création de la VM Windows Server 2022 sur Proxmox (VM 102 – 192.168.1.15) : 4 vCPU, 4 Go RAM, 80 Go disque, bridge vmbr0
2. Installation de Windows Server 2022 avec Expérience de bureau
3. Installation du rôle AD DS via le Gestionnaire de serveur → Ajouter des rôles et fonctionnalités
4. Promotion du serveur en tant que contrôleur de domaine : nouvelle forêt reali.fr, rôles DNS et Catalogue global activés
5. Ajout DHCP : Plage 192.168.1.100 – 192.168.1.200 / Masque : 255.255.255.0
passerelle (192.168.1.1) et DNS (192.168.1.15).
6. Création de la structure organisationnelle :
   - OU RH → Groupe GRP_RH → Utilisateur francois.dupont
   - OU Direction → Groupe GRP_Direction → Utilisateur damien.robert
   - OU Informatique → Groupe GRP_Informatique → Utilisateur richard.premiz
7. Application de 2 GPO :
   - GPO 1 : Blocage de l'invite de commandes (CMD) sur l'OU RH
   - GPO 2 : Fond d'écran imposé sur tout le domaine reali.fr
8. Jonction du poste client Windows 10 (VM 103) au domaine reali.fr
9. Validation : connexion avec les utilisateurs sur le poste client, vérification de l'application des GPO

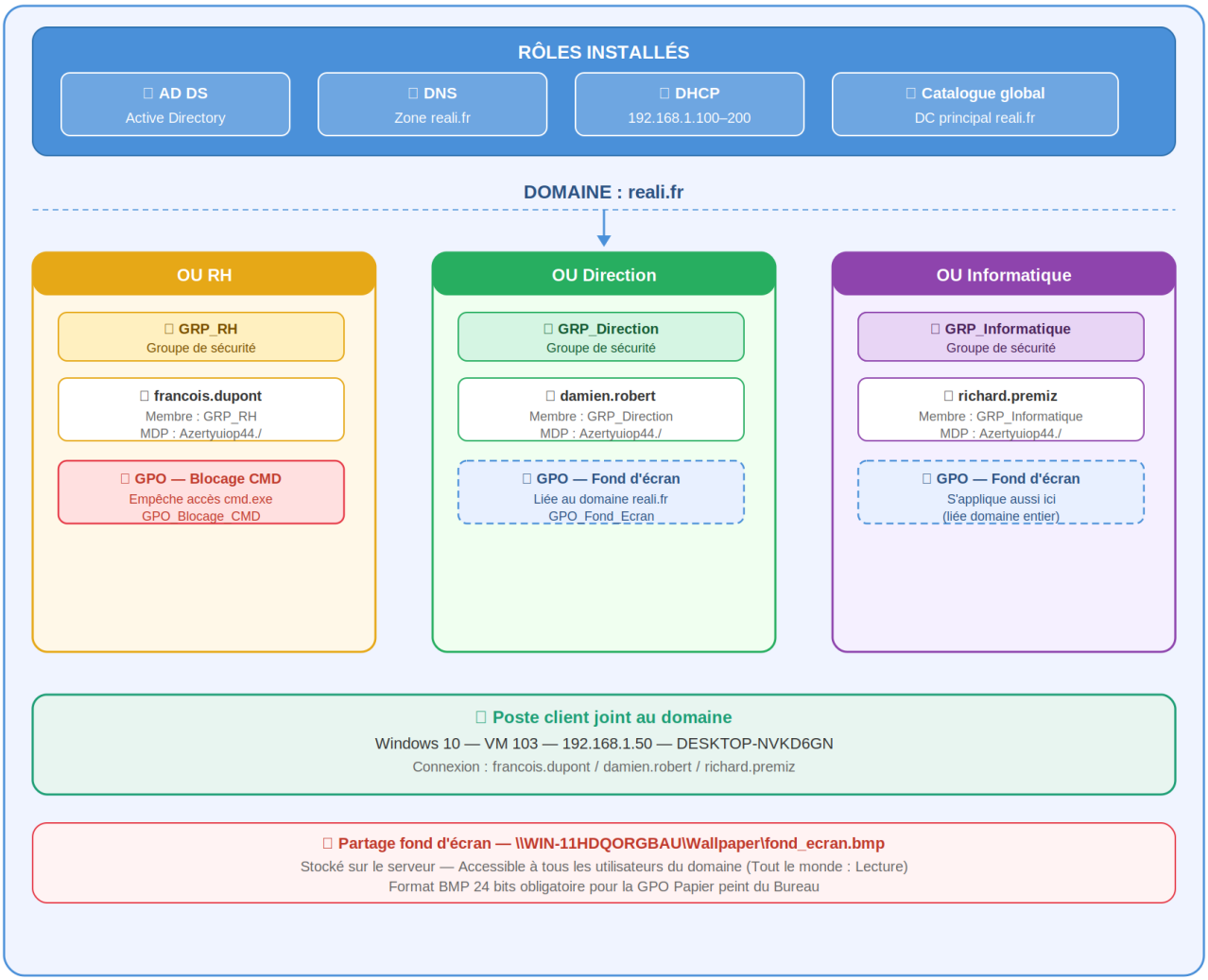
RÉSULTAT

Le domaine reali.fr est pleinement opérationnel avec 3 OUs, 3 groupes de sécurité, 3 utilisateurs et 2 GPO actives. Le poste client est joint au domaine et les politiques s'appliquent correctement.



Windows Server 2022 — Active Directory reali.fr

VM 102 — 192.168.1.15



Mewen LANGEL
BTS SIO SISR 2024-2026

CREATION D'UN ACTIVE DIRECTORY COMPLET

Déploiement d'un domaine Active Directory sur Windows Server 2022

BTS SIO – Option SISR
Infrastructure REALIS – domaine reali.fr

SOMMAIRE :

1. Contexte et objectifs ...p3
2. Création de la VM sur Proxmox (Virtual Machine) : ...p5
3. Installation Windows ...p10
4. Création du service DHCP ...p17
5. Création des Unités d'Organisation (OU) ...p20
6. Création des groupes de sécurité ...p22
7. Création des utilisateurs ...p24
8. Stratégies de groupe (GPO) ...p26
9. Jonction du poste client au domaine ...p28
10. Conclusion ...p28

1. Contexte et objectifs

1.1 Contexte de l'entreprise

REALIS (Réseau Administration et Logistique Informatisée des Systèmes) est une entreprise fictive dont l'infrastructure informatique est entièrement virtualisée sur un hyperviseur Proxmox VE (192.168.1.1). L'objectif est de mettre en place un système d'information complet et fonctionnel, répondant aux besoins d'une PME.

Dans ce contexte, la mise en place d'un Active Directory est une étape fondamentale : elle permet de centraliser la gestion des utilisateurs, des ordinateurs et des politiques de sécurité au sein d'un domaine unique : reali.fr.

1.2 Besoin identifié

Sans Active Directory, chaque poste utilisateur dispose de comptes locaux indépendants, ce qui pose plusieurs problèmes en entreprise :

- Pas de gestion centralisée des identités et des mots de passe
- Impossible d'appliquer des politiques de sécurité uniformes sur tous les postes
- Pas de contrôle des accès aux ressources réseau (partages, imprimantes)
- Administration fastidieuse poste par poste

L'Active Directory répond à ces besoins en offrant :

- Un annuaire centralisé pour tous les utilisateurs et ordinateurs
- Des Unités d'Organisation (OU) pour structurer les objets par service
- Des groupes de sécurité pour gérer les droits d'accès
- Des GPO (stratégies de groupe) pour uniformiser les configurations

1.3 Solution retenue

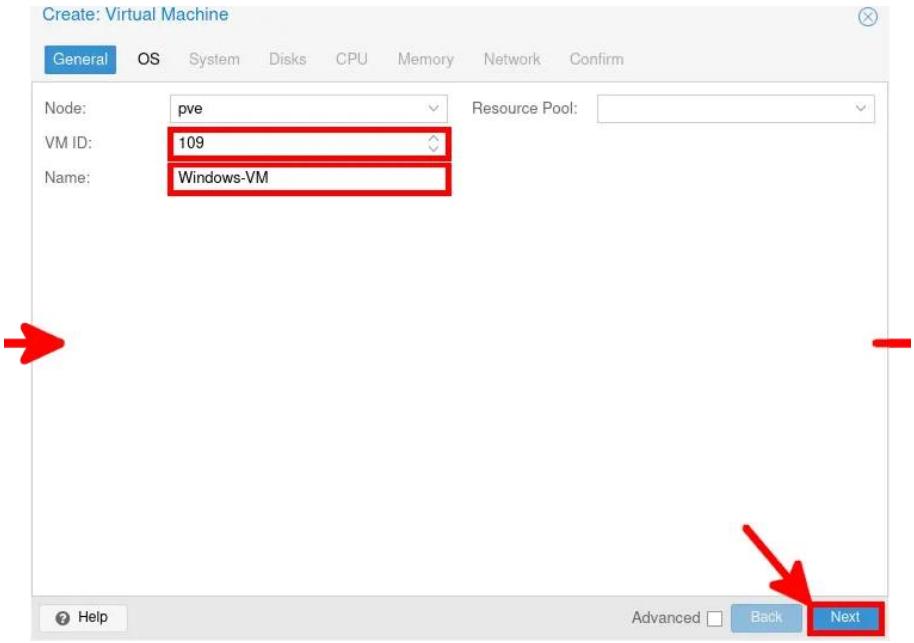
Déploiement d'un contrôleur de domaine Active Directory Domain Services (AD DS) sur une machine virtuelle Windows Server 2022, hébergée sur Proxmox VE. Le domaine créé est reali.fr, avec les caractéristiques suivantes :

- Contrôleur de domaine principal : VM 102 – 192.168.1.15
- Rôles installés : AD DS, DNS, DHCP, Catalogue global
- Structure organisationnelle : 3 OUs (RH, Direction, Informatique)
- GPO appliquées : blocage CMD sur OU RH, fond d'écran imposé sur le domaine

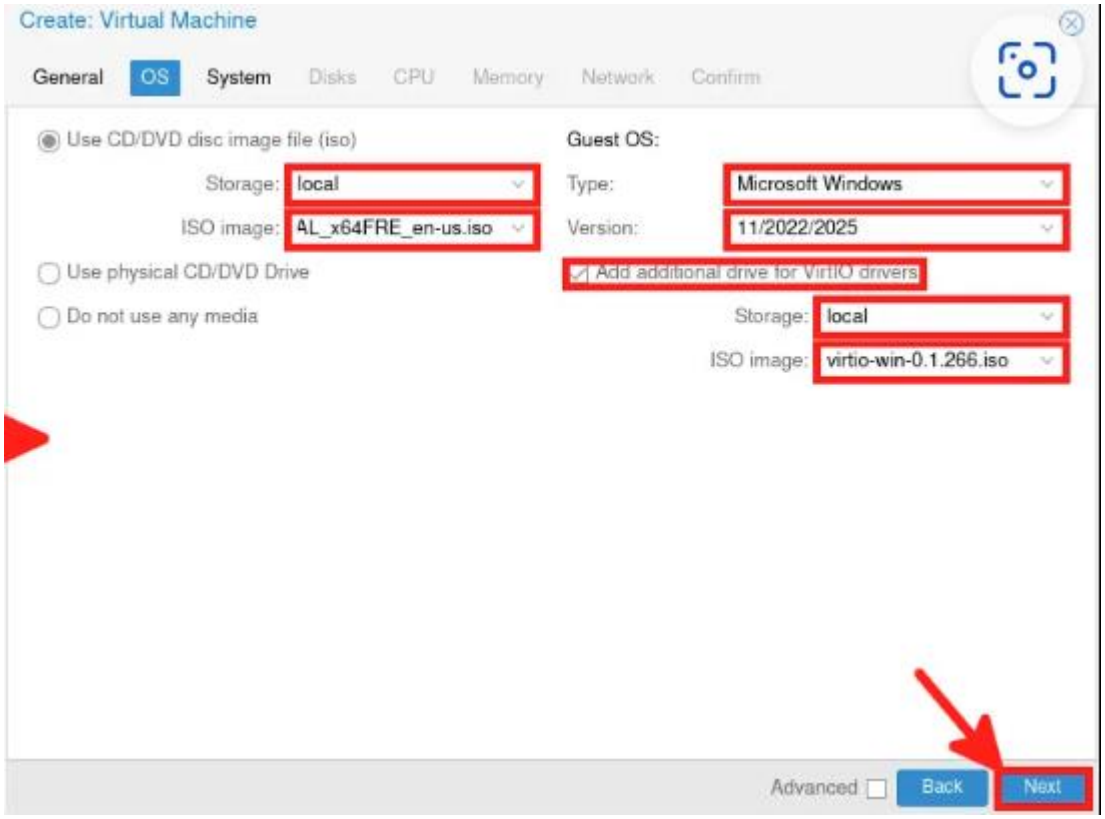
2. Création de la VM sur Proxmox (Virtual Machine) :

Etape 1 : On va créer la VM sur Proxmox
Une virtual machine (VM) est une représentation virtuelle ou une émulation d'un ordinateur physique qui utilise un logiciel plutôt que du matériel pour exécuter des programmes et déployer des applications.

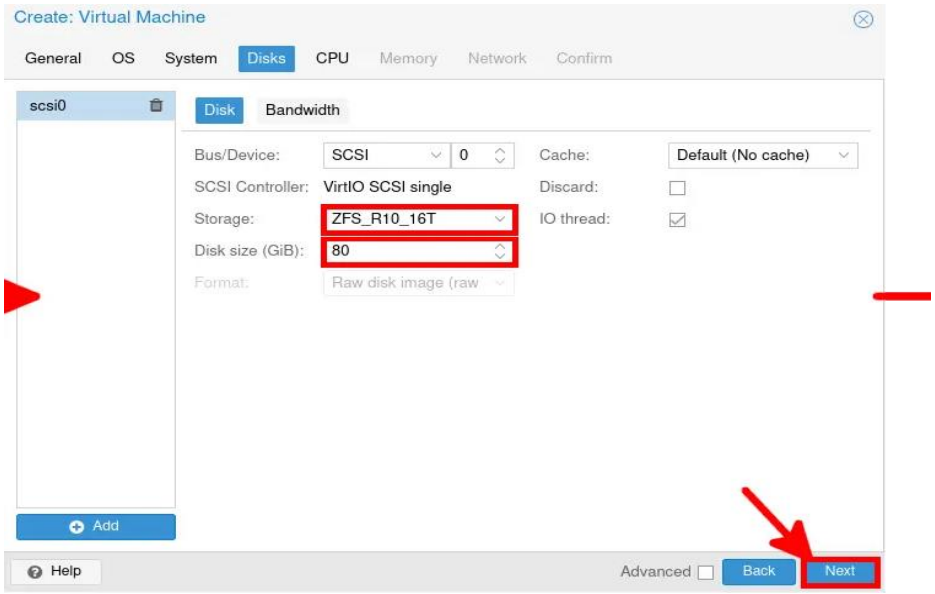
Une fois installé, on arrive sur l'interface suivante. C'est ici qu'on va créer et paramétrer la VM. Dans un premier temps on va nommer la VM.



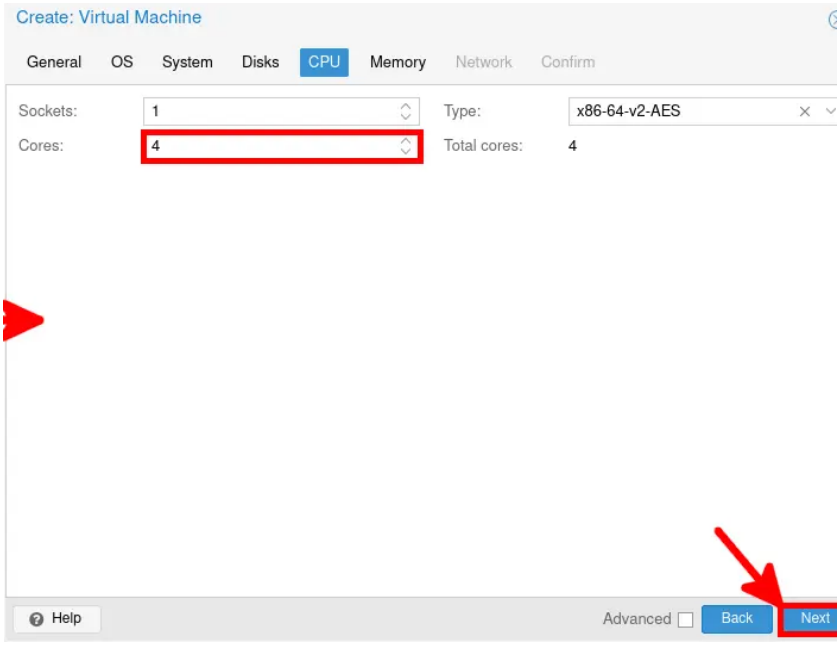
Ensuite, il faut sélectionner un ISO, donc celui de Windows server ici, le type est bien Windows puis il sera bien installé en local.



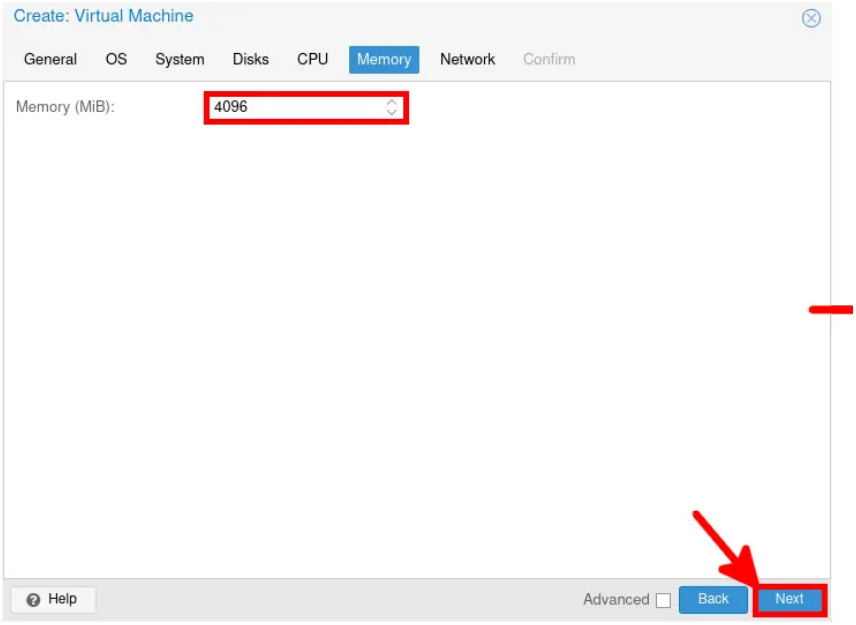
Sur cet écran, on configure le disque dur de la machine virtuelle, la taille du disque est fixée à 80 Go, ce qui correspond à l'espace alloué au système Windows. Le cache est laissé sur Default (No cache) et l'option IO thread est activée afin d'améliorer les performances d'accès au disque. Une fois la configuration terminée, on clique sur Next pour continuer la création de la machine virtuelle.



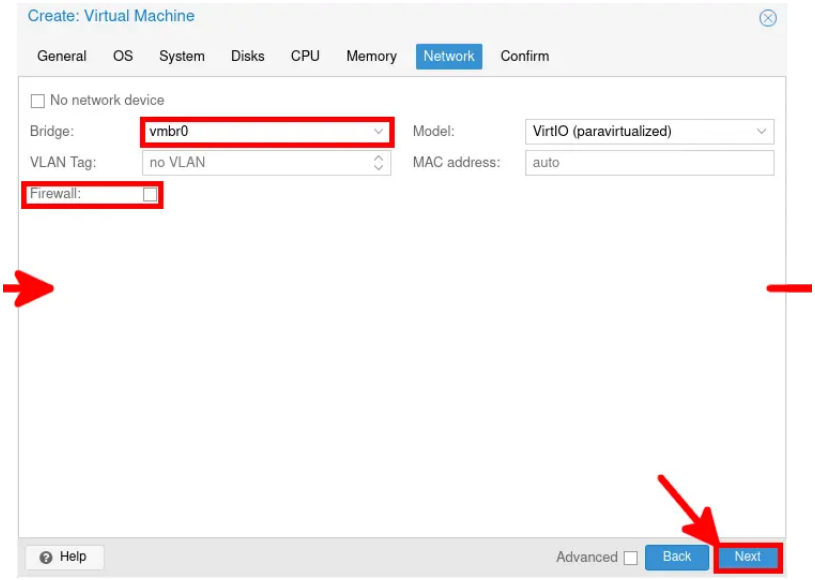
Ensuite, il faut configurer les ressources processeur de la machine virtuelle.
Le nombre de cœurs (cores) est réglé sur 4, ce qui permet d'allouer quatre cœurs CPU à la machine virtuelle.



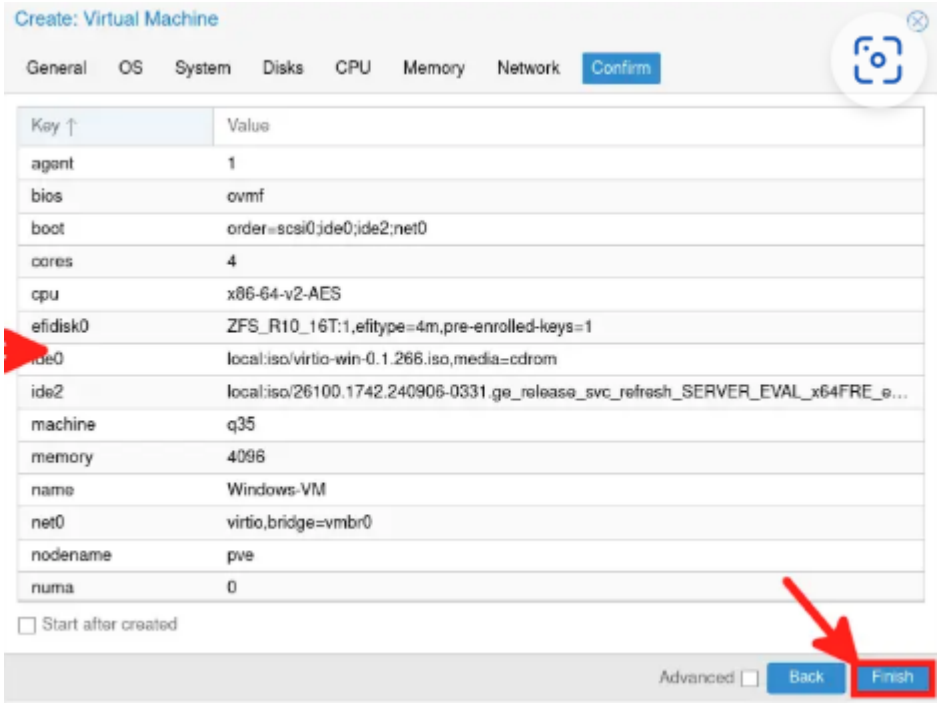
Sur cet écran, on configure la mémoire vive allouée à la machine virtuelle. La quantité de mémoire est définie à 4096 Mo (4 Go de RAM), ce qui permet au système Windows de fonctionner correctement. Cette mémoire sera réservée à la machine virtuelle lors de son démarrage. Une fois la mémoire configurée, on clique sur Next pour continuer la création de la machine virtuelle.



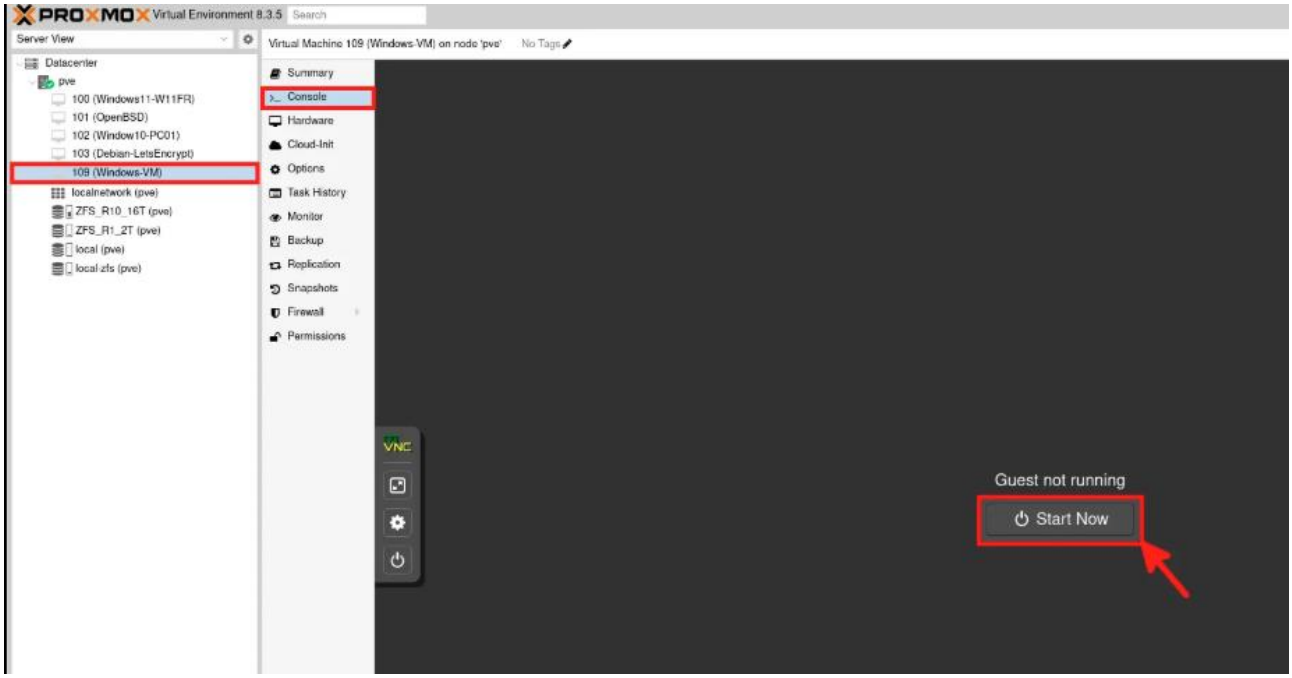
C’est bientôt fini, après il faut configurer le réseau de la VM, le Bridge est défini sur vmbr0, ce qui permet à la machine virtuelle d’être connectée directement au réseau physique de l’hôte Proxmox. Le champ Firewall est activé afin de permettre l’application des règles de pare-feu Proxmox à la machine virtuelle.



Pour finir, on peut apercevoir un résumé de la configuration de la VM, on y retrouve toutes nos configurations qu’on a effectuées.

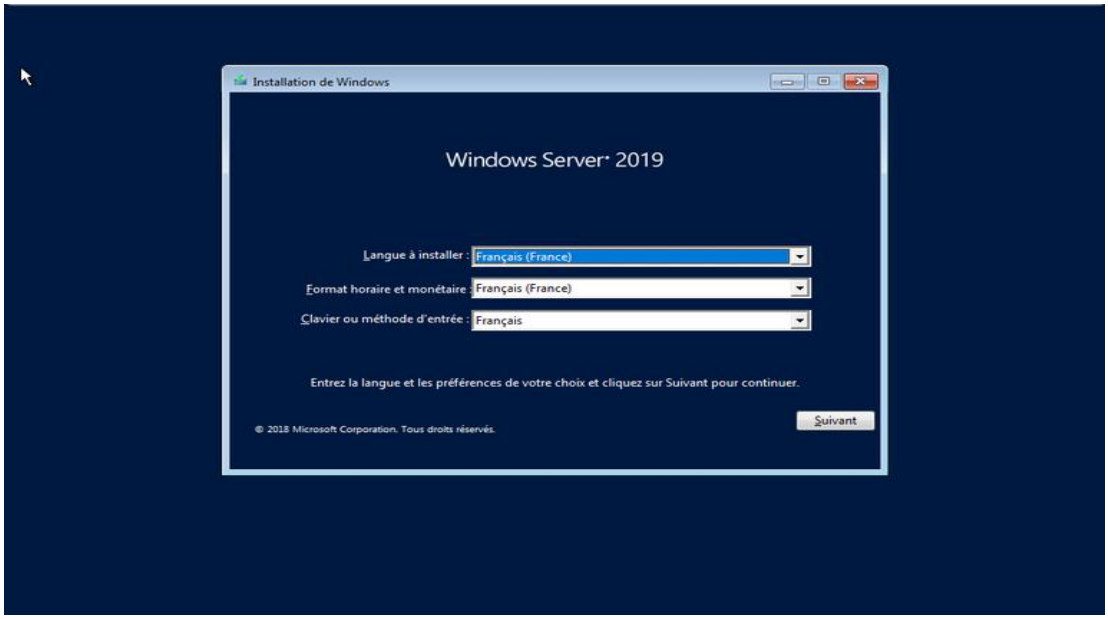


Une fois créée, démarrez la machine virtuelle depuis le menu Console :



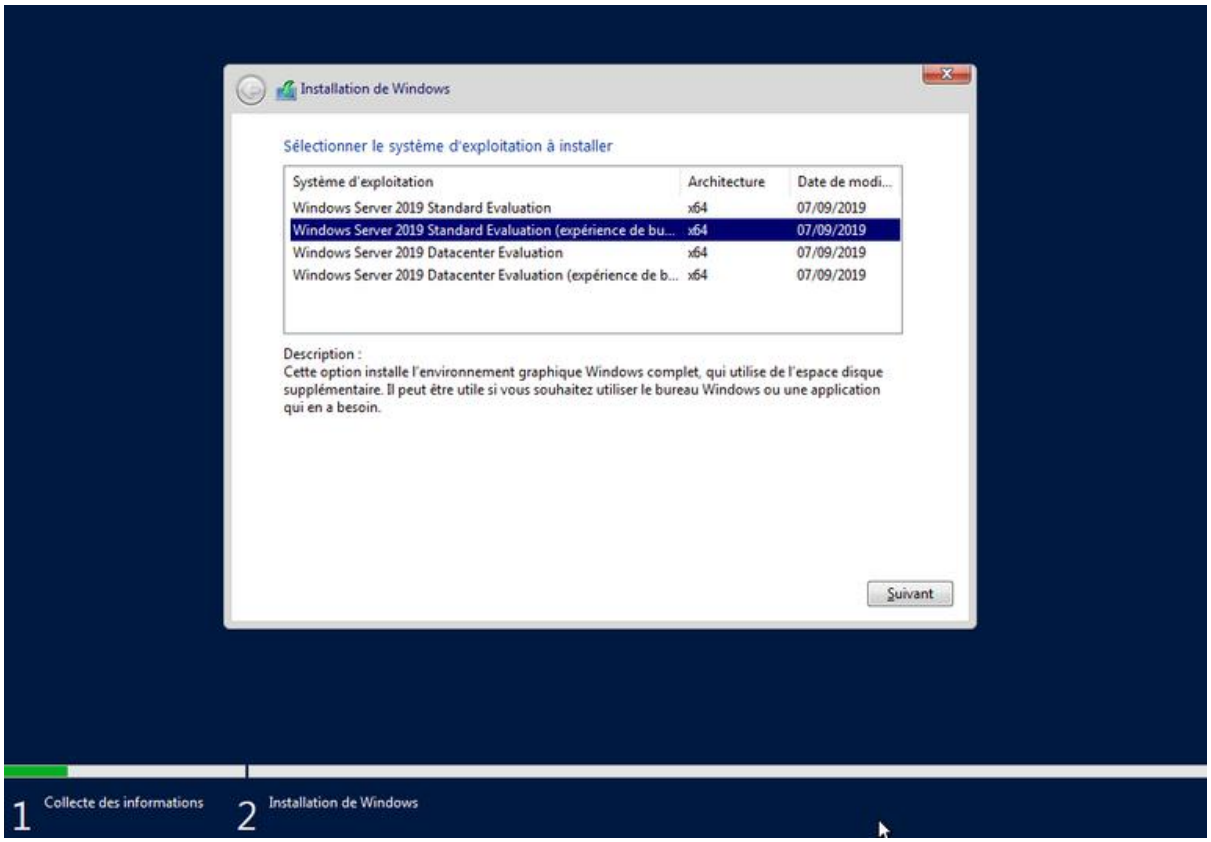
Ensuite, l'installation de Windows va commencer

3. Installation Windows



On sélectionne notre langue, français

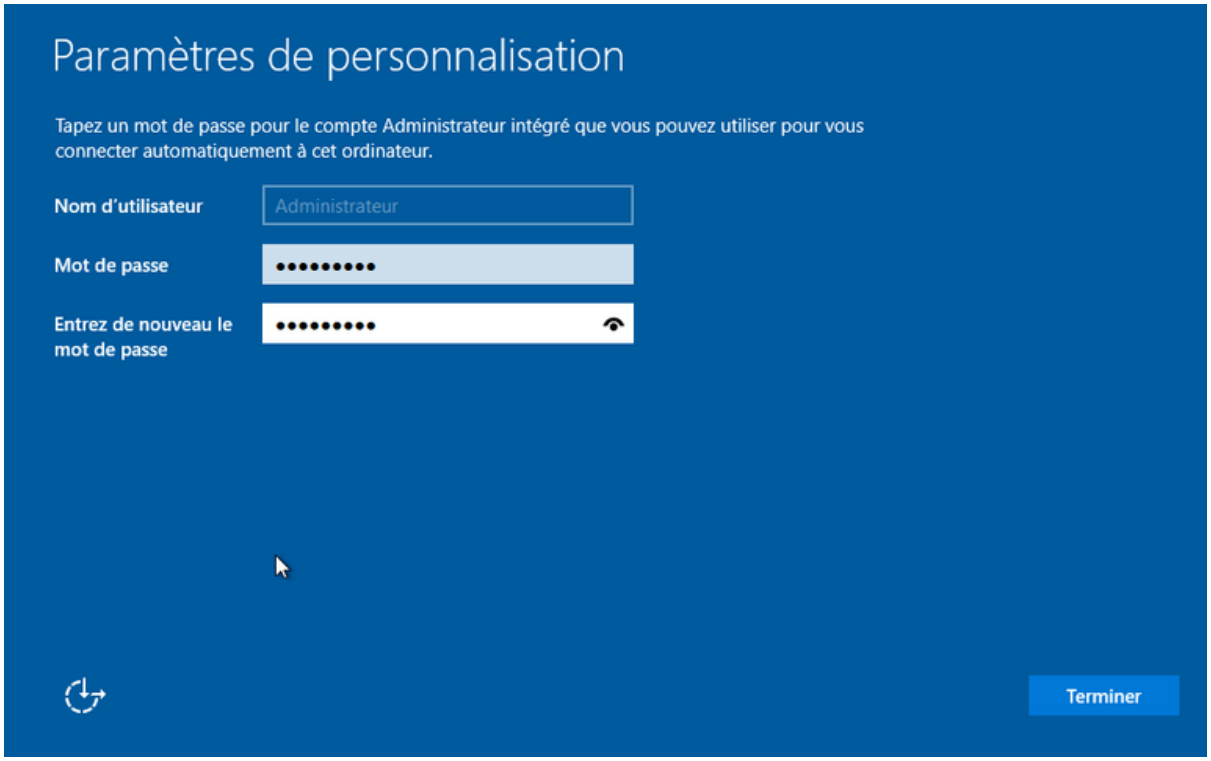
Ensuite on clique sur installer,



Maintenant on sélectionne la version de Windows Serveur qu'on veux, ici, on va choisir Windows Standard avec Expérience de bureau

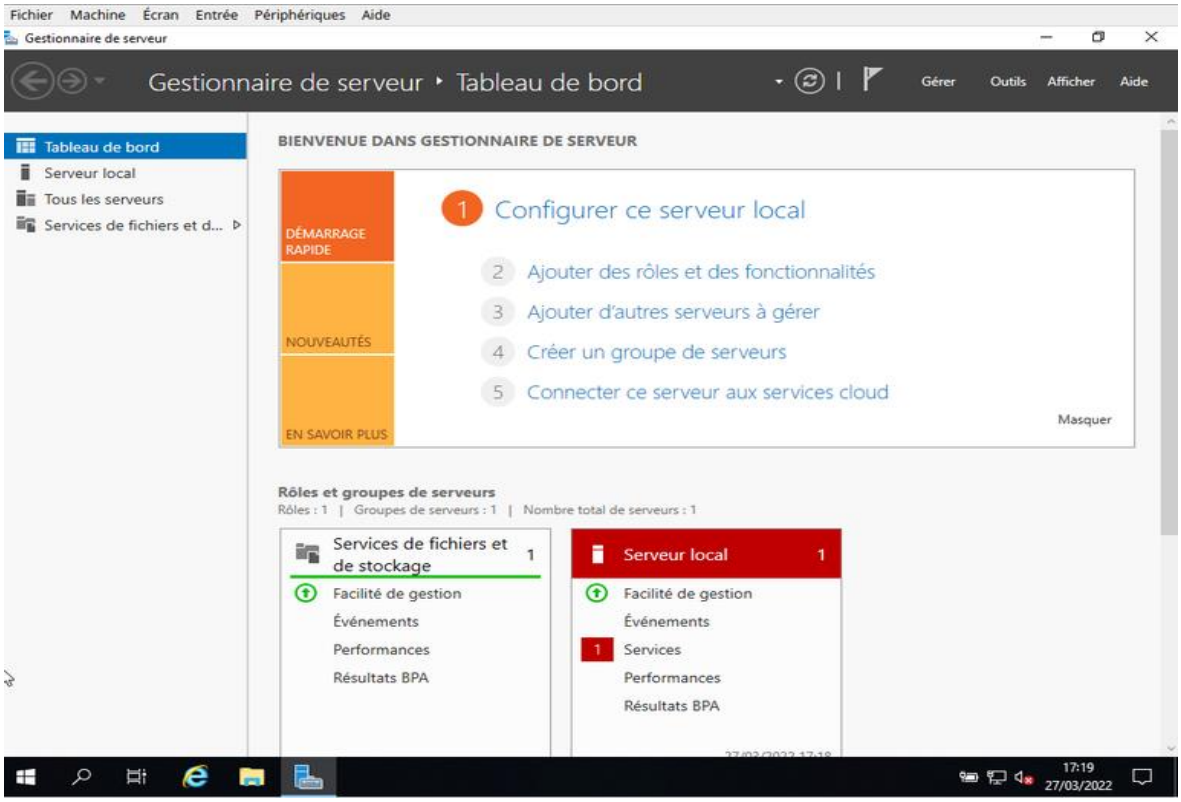
Ensuite, on continue, et on se laisse guider par windows.

Une fois l'installation finie, Windows Serveur va redémarrer et nous demande de choisir un mot de passe pour le compte administrateur :



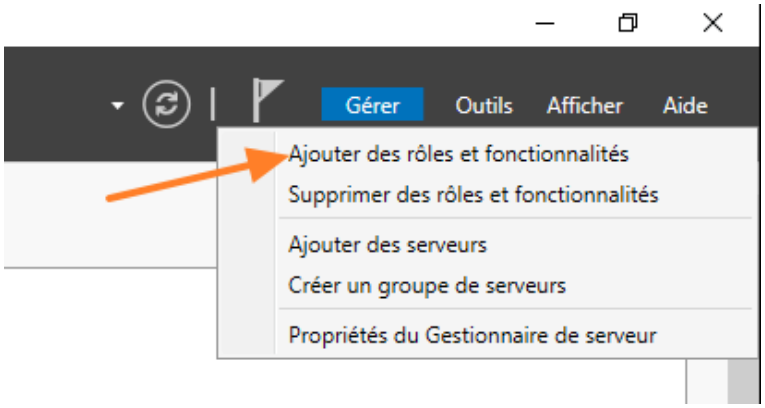
On renseigne donc un mot de passe puis on clique sur le bouton terminer

Ensuite l'installation du Serveur Windows est terminée, On va se connecter avec le compte administrateur et le mot de passe choisis précédemment.
- On arrive donc ici : ceci est le tableau de bord du gestionnaire de serveur.



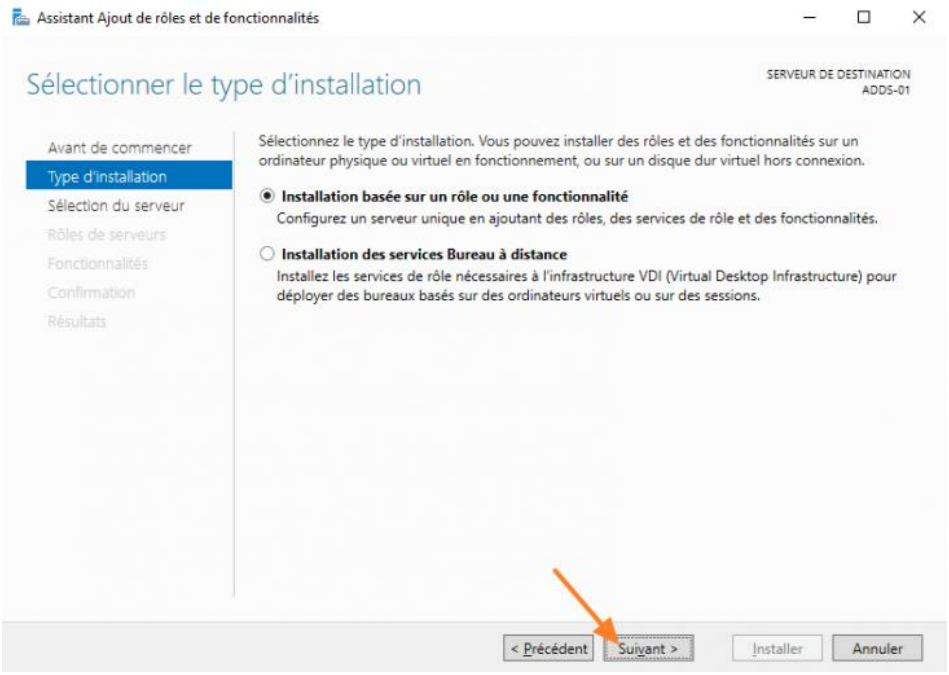
Installer Active Directory :

La première étape, avant de créer le domaine Active Directory, consiste à installer le rôle "ADDS" : Active Directory Domain Services. Il s'agit du rôle permettant de créer un domaine Active Directory. On ouvre le Gestionnaire de serveur, puis on clique sur "Gérer" puis "Ajouter des rôles et fonctionnalités".



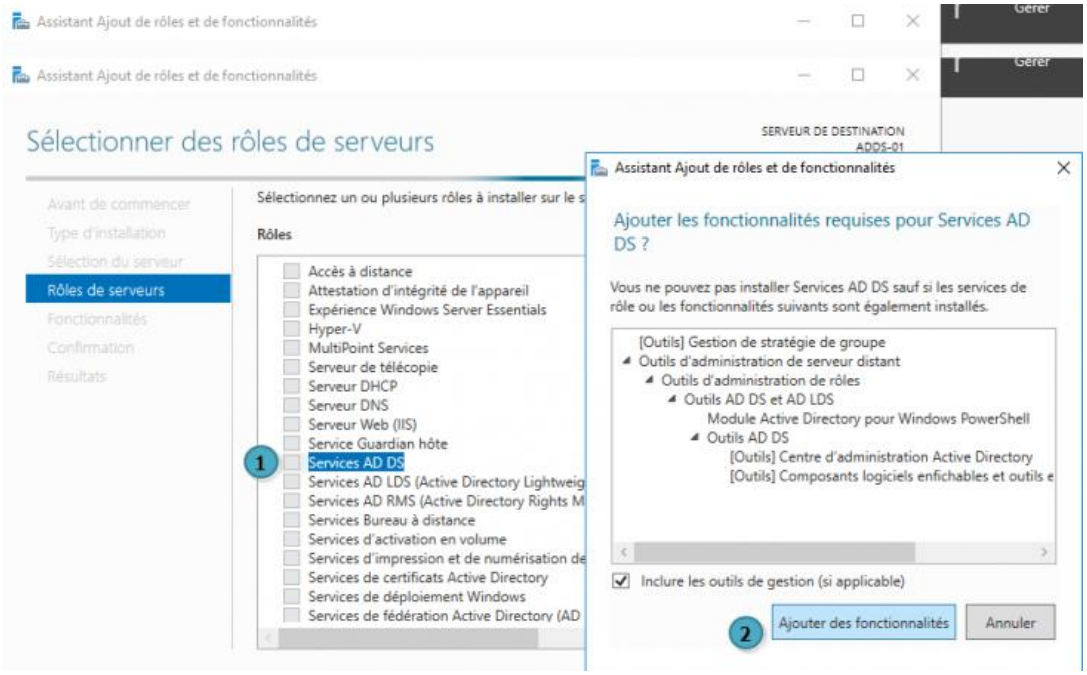
Active Directory (AD) est une base de données et un ensemble de services qui permettent de mettre en lien les utilisateurs avec les ressources réseau dont ils ont besoin pour mener à bien leurs missions.

Ensuite il faut passer l’étape "Avant de commencer" et poursuive ensuite en laissant le type d'installation sur le choix "Installation basée sur un rôle ou une fonctionnalité".



Pour la 3eme étape (sélection du serveur) on laisse le choix par défaut et cliquez sur suivant

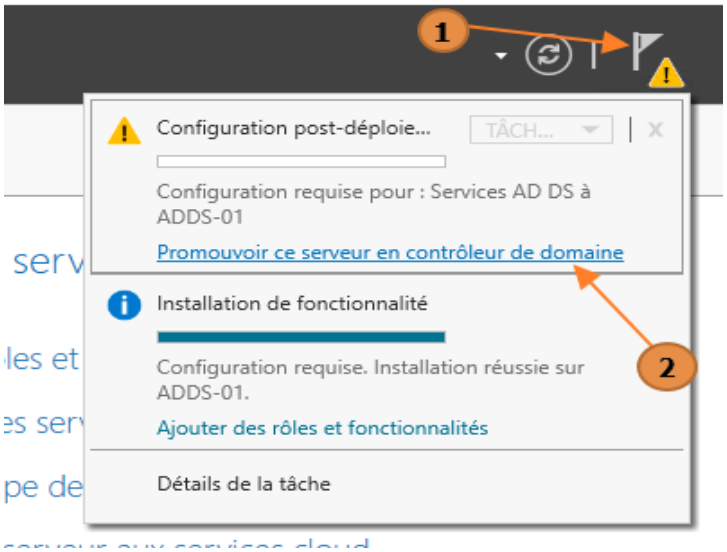
L'étape cruciale de l'installation du rôle est ici, puisqu'il va falloir cocher "Services AD DS" dans la liste. Une seconde fenêtre va apparaître pour nous proposer d'installer les outils de gestion : validez. Qui dit outils de gestion, dit console d'administration comme "Utilisateurs et ordinateurs Active Directory" mais aussi le module PowerShell pour Active Directory.



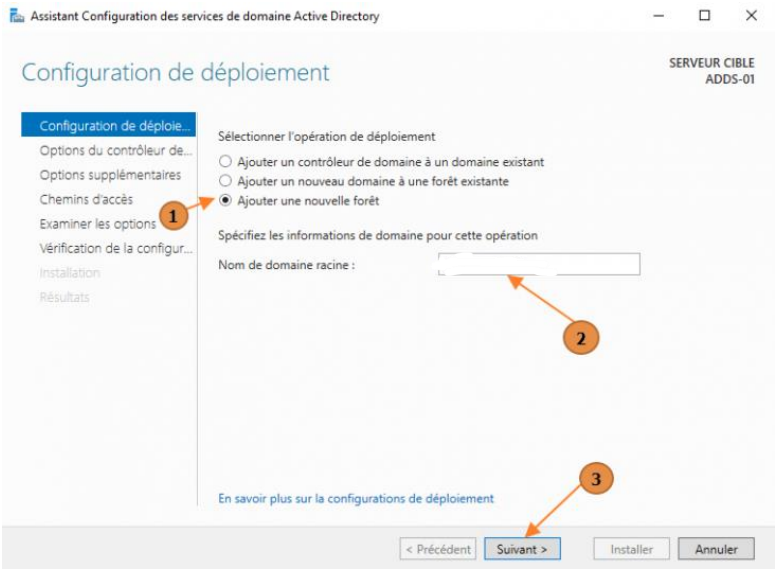
Une fois à la 5eme étape “fonctionnalités”, nous n'installons pas de fonctionnalités en plus, donc il faut poursuivre sans rien sélectionner.

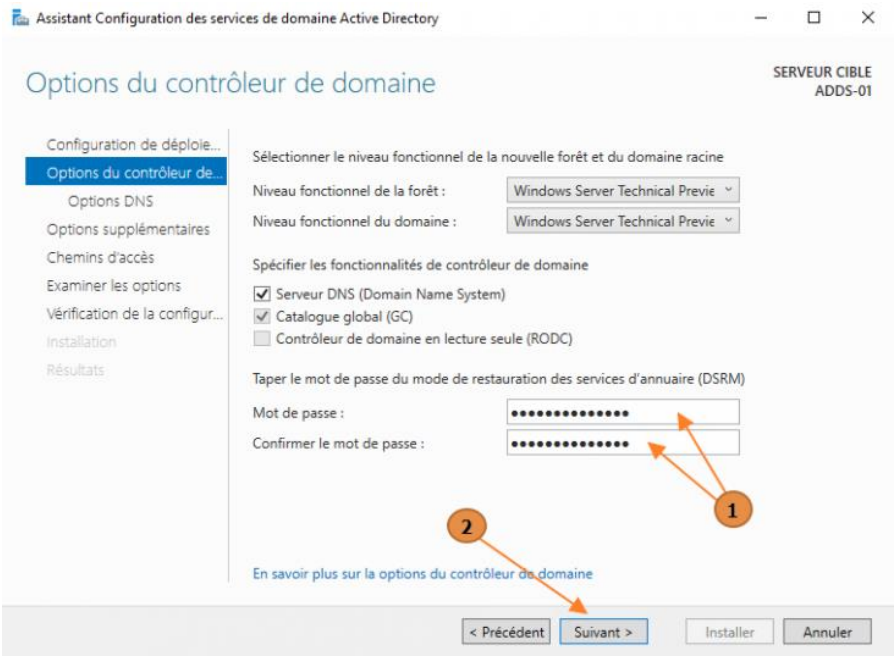
Ensuite pour le reste, nous cliquons sur suivant, puis Installer, on le laisse s’installer et puis on clique sur Fermer.

Ensuite il faut promouvoir le serveur en tant que contrôleur de domaine. Comme ceci :



Comme il s'agit d'un nouveau domaine dans une nouvelle forêt, il faut choisir "Ajouter une nouvelle forêt" et indiquez le nom de domaine.





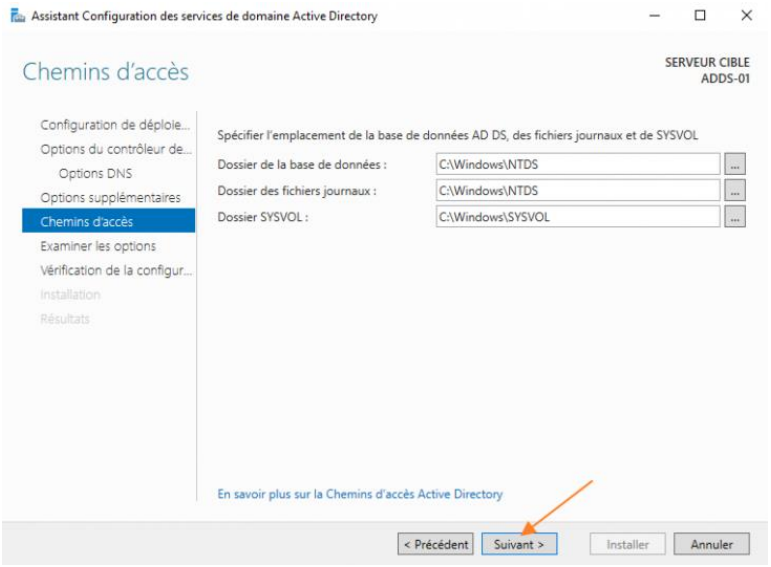
Définissons-le aussi comme serveur DNS et Catalogue global.

Enfin, il faut indiquez un mot de passe pour les services de restauration de l'annuaire (ce mot de passe ne correspond pas au mot de passe Administrateur du futur domaine !)

Puis un message apparait dans “Options DNS”, on clique sur ok puis suivant,
(Le système DNS d'Internet fonctionne comme un annuaire téléphonique en gérant le mappage entre les noms et les numéros)

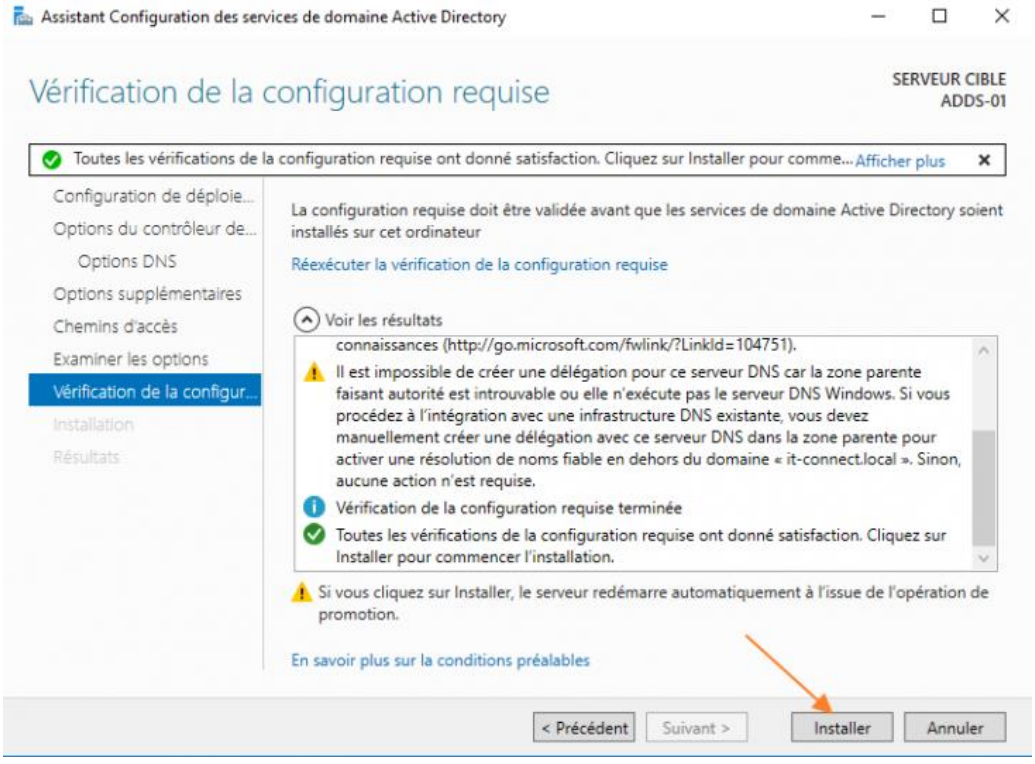
Ensuite, On Indique un nom NETBIOS pour le domaine, à savoir un nom court et qui ne s'appuie pas sur DNS pour être résolu.

Puis on laisse par défaut et on poursuit.



Ensuite dans “examinez les options” il faut verifier les options et cliquer sur suivant

On finit en cliquant sur installer pour démarrer la création du domaine



On patiente pendant l'installation. Quand ce sera terminé, le serveur va obligatoirement redémarrer, de façon automatique.

Dès que l'installation est terminée et que le serveur a redémarré, nous pouvons commencer à utiliser le domaine Active Directory, avec les consoles "Utilisateurs et ordinateurs Active Directory" et "Centre d'administration Active Directory" qui servent à gérer les objets dans l'annuaire (utilisateurs, ordinateurs, serveurs, etc.).

4. Création du service DHCP

4.1 Qu’est-ce que le DHCP ?

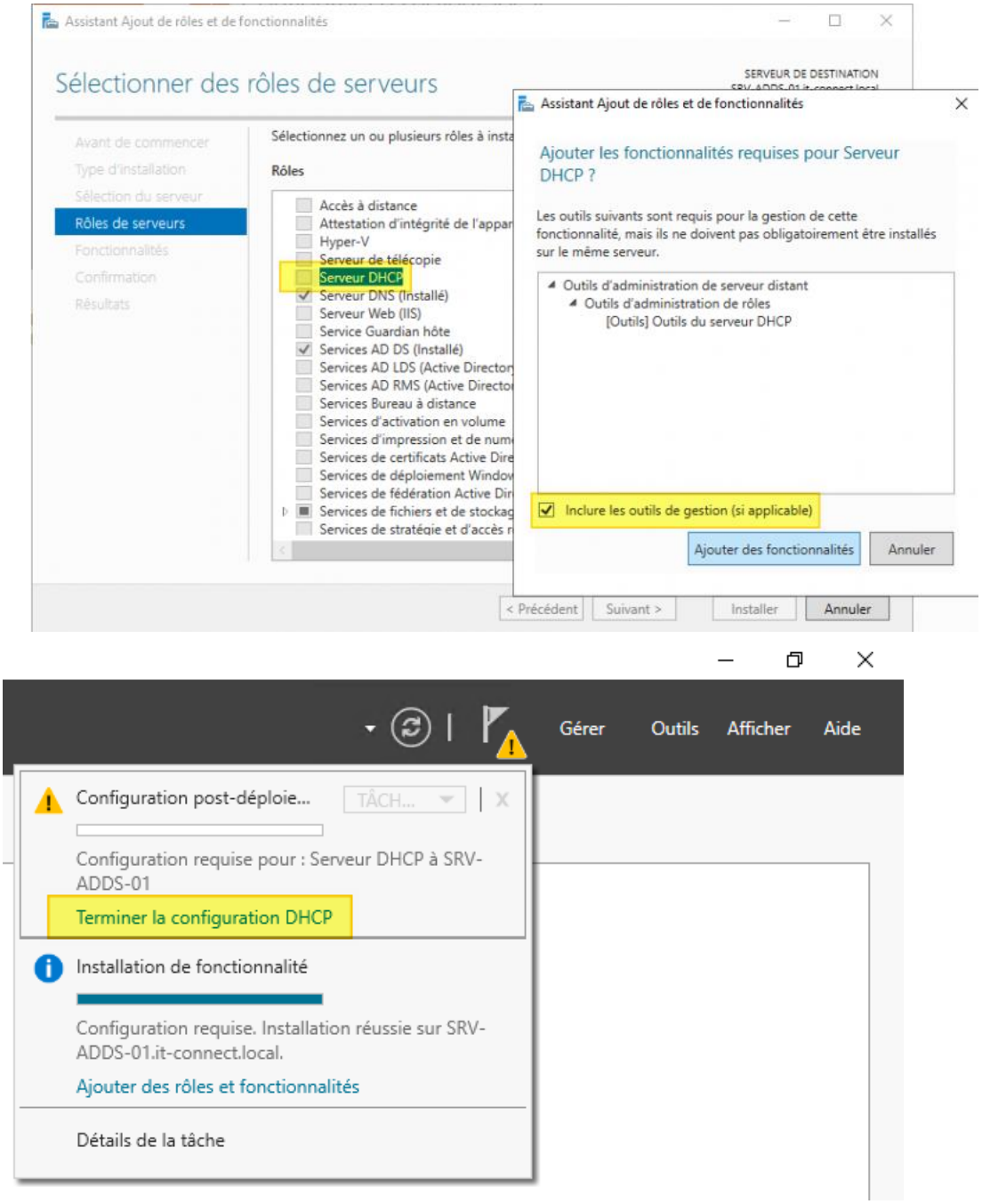
Le DHCP (Dynamic Host Configuration Protocol) est un protocole réseau qui attribue automatiquement une adresse IP à chaque machine connectée au réseau, sans configuration manuelle. Il distribue également la passerelle par défaut, le serveur DNS et le nom de domaine.

Dans l’infrastructure REALIS, le service DHCP est installé sur le même serveur que l’Active Directory (VM 102 – 192.168.1.15), ce qui permet son autorisation automatique dans le domaine reali.fr.

4.2 Installation du rôle DHCP

Procédure :

- Ouvrir le Gestionnaire de serveur
- Cliquer sur Gérer → Ajouter des rôles et fonctionnalités
- Sélectionner Installation basée sur un rôle ou une fonctionnalité → Suivant
- Sélectionner le serveur WIN-11HDQORGBAU → Suivant
- Cocher Serveur DHCP → Ajouter des fonctionnalités → Suivant → Installer
- Une fois installé, cliquer sur Terminer la configuration DHCP dans la notification du Gestionnaire de serveur → Valider (autorisation automatique dans l’AD)

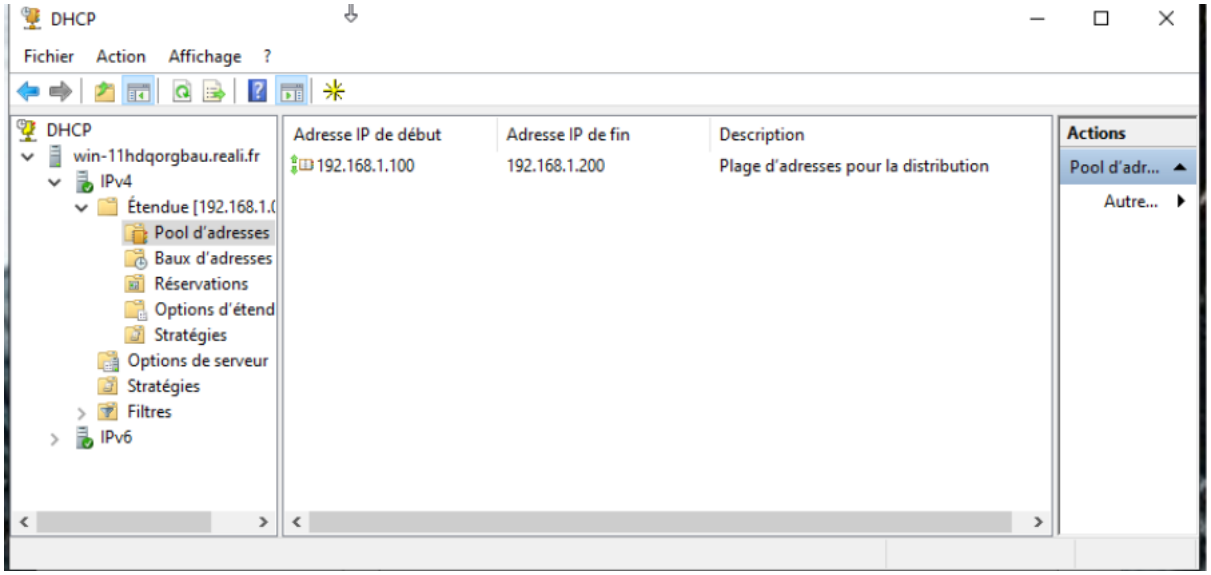


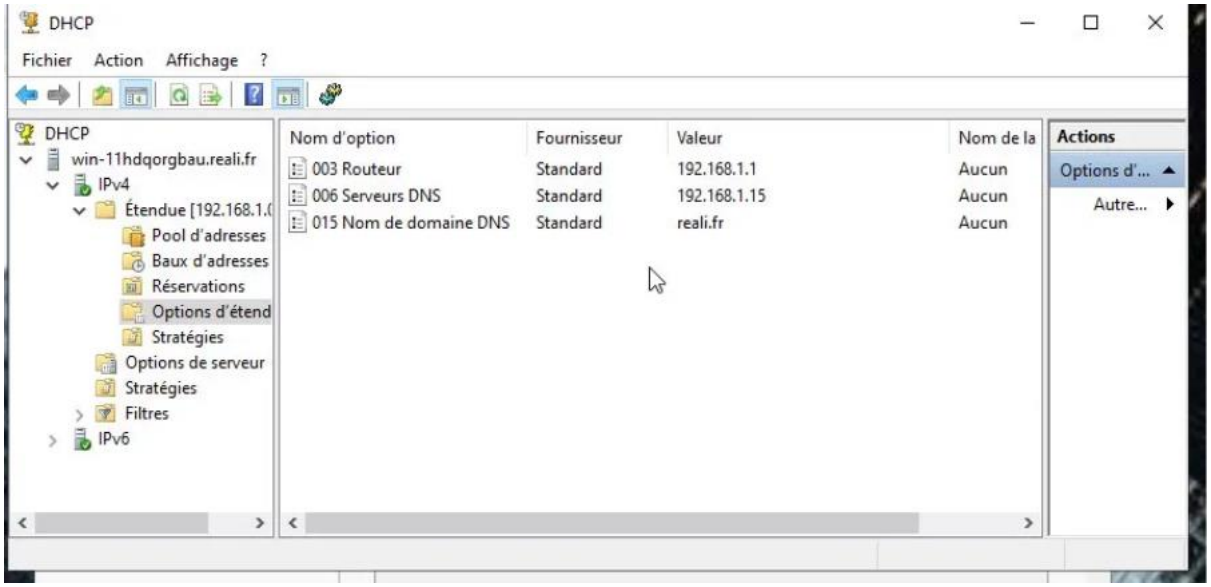
4.3 Configuration de l'étendue DHCP

Une étendue définit la plage d'adresses IP distribuées automatiquement aux clients. Voici la configuration appliquée :

- Ouvrir le Gestionnaire DHCP : Outils → DHCP dans le Gestionnaire de serveur
- Développer WIN-11HDQORGBAU → IPv4 → Clic droit → Nouvelle étendue
- Nom de l'étendue : REALIS_LAN
- Plage d'adresses : 192.168.1.100 – 192.168.1.200 / Masque : 255.255.255.0

- Exclusions : aucune (les adresses .1 à .99 sont statiques, hors étendue)
- Durée du bail : valeur par défaut (8 jours)
- Configurer les options DHCP : Oui
- Passerelle (routeur) : 192.168.1.1
- Serveur DNS : 192.168.1.15 / Nom de domaine : reali.fr
- Activer l'étendue maintenant : Oui → Terminer





4.4 Vérification depuis le poste client

Une fois le DHCP activé, on vérifie que le poste client Windows 10 (VM 103 – 192.168.1.50) obtient bien une adresse IP automatiquement.

Procédure sur le poste client :

- Vérifier que la carte réseau est en "Obtenir une adresse IP automatiquement"
- Ouvrir une invite de commandes et exécuter :

ipconfig /release

ipconfig /renew

- Vérifier que l'IP obtenue est dans la plage 192.168.1.100 – 192.168.1.200
- Vérifier la passerelle : 192.168.1.1 et le DNS : 192.168.1.15

5. Création des Unités d'Organisation (OU)

5.1 Qu'est-ce qu'une OU ?

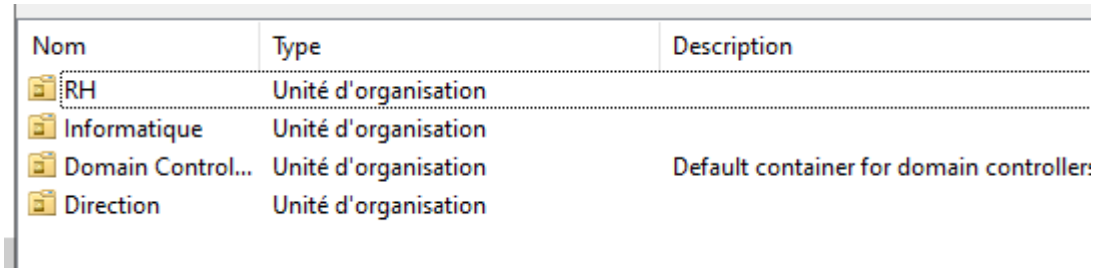
Une Unité d'Organisation (OU) est un conteneur dans l'Active Directory qui permet de regrouper des objets (utilisateurs, ordinateurs, groupes) de manière logique, généralement par service ou par département. Les OUs permettent de :

- Organiser les objets AD de façon hiérarchique
- Déléguer l'administration à des sous-administrateurs
- Appliquer des GPO (stratégies de groupe) ciblées sur un groupe d'utilisateurs spécifique

5.2 Structure des OUs créées

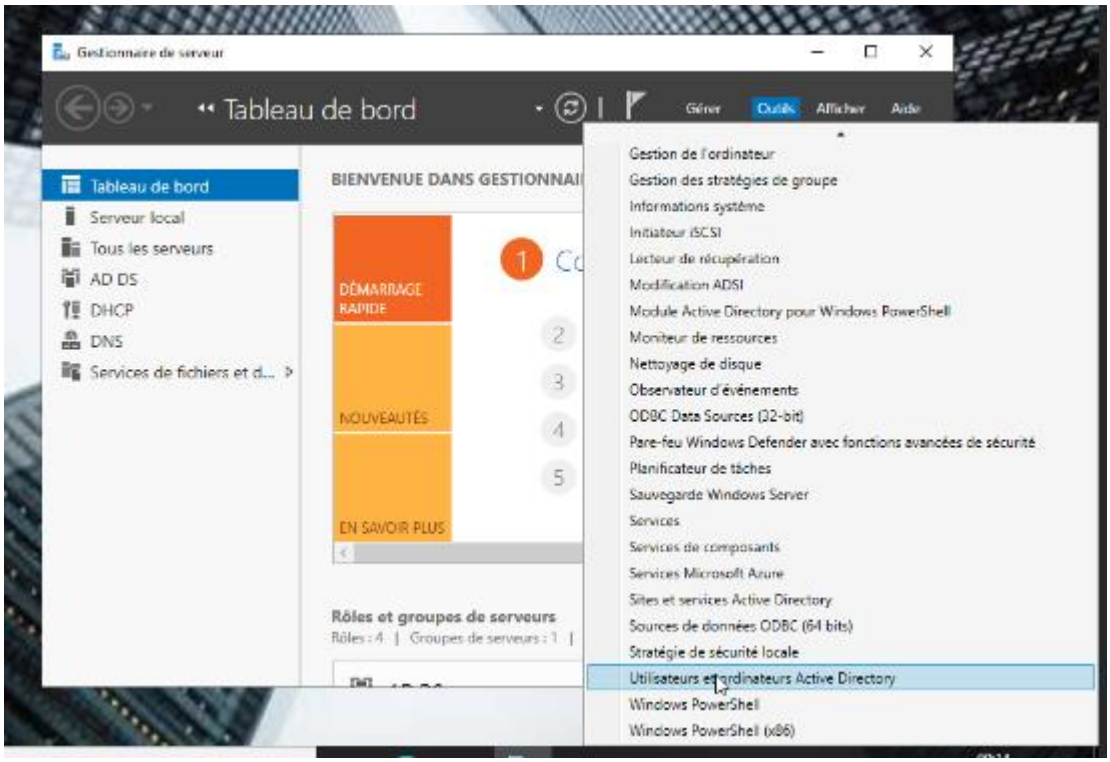
Pour l'infrastructure REALIS, trois Unités d'Organisation ont été créées, correspondant aux services de l'entreprise :

- OU RH – contient les utilisateurs du service Ressources Humaines
- OU Direction – contient les utilisateurs de la Direction
- OU Informatique – contient les utilisateurs du service Informatique



5.3 Procédure de création

On ouvre la console « Utilisateurs et ordinateurs Active Directory » depuis le Gestionnaire de serveur → Outils → Utilisateurs et ordinateurs Active Directory.

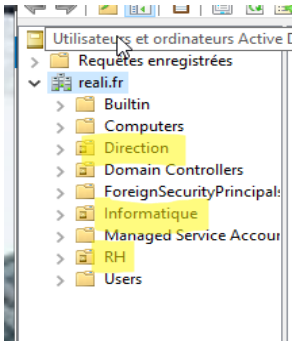


Pour créer une OU, on fait un clic droit sur le domaine reali.fr → Nouveau → Unité d'organisation.

On renseigne le nom de l'OU (ex : **RH**) puis on valide. On répète l'opération pour **Direction** et **Informatique**.

On obtient alors la structure suivante dans l'annuaire :

- reali.fr
- └── OU RH
- └── OU Direction
- └── OU Informatique



6. Création des groupes de sécurité

6.1 Pourquoi des groupes ?

Les groupes de sécurité permettent de gérer les droits d'accès aux ressources (dossiers partagés, imprimantes, applications) de façon collective. Au lieu d'assigner des permissions utilisateur par utilisateur, on assigne les permissions au groupe, et tous les membres héritent automatiquement de ces droits.

6.2 Groupes créés

Trois groupes de sécurité ont été créés, un par service :

- GRP_RH – groupe de sécurité pour les utilisateurs de l'OU RH
- GRP_Direction – groupe de sécurité pour les utilisateurs de l'OU Direction
- GRP_Informatique – groupe de sécurité pour les utilisateurs de l'OU Informatique

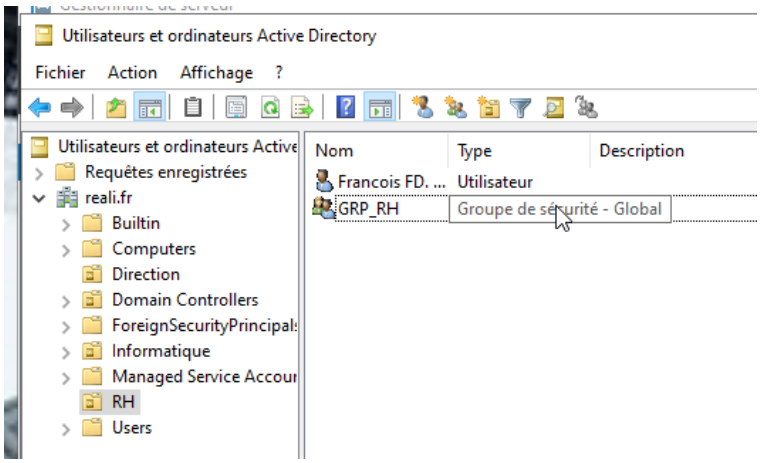
6.3 Procédure de création

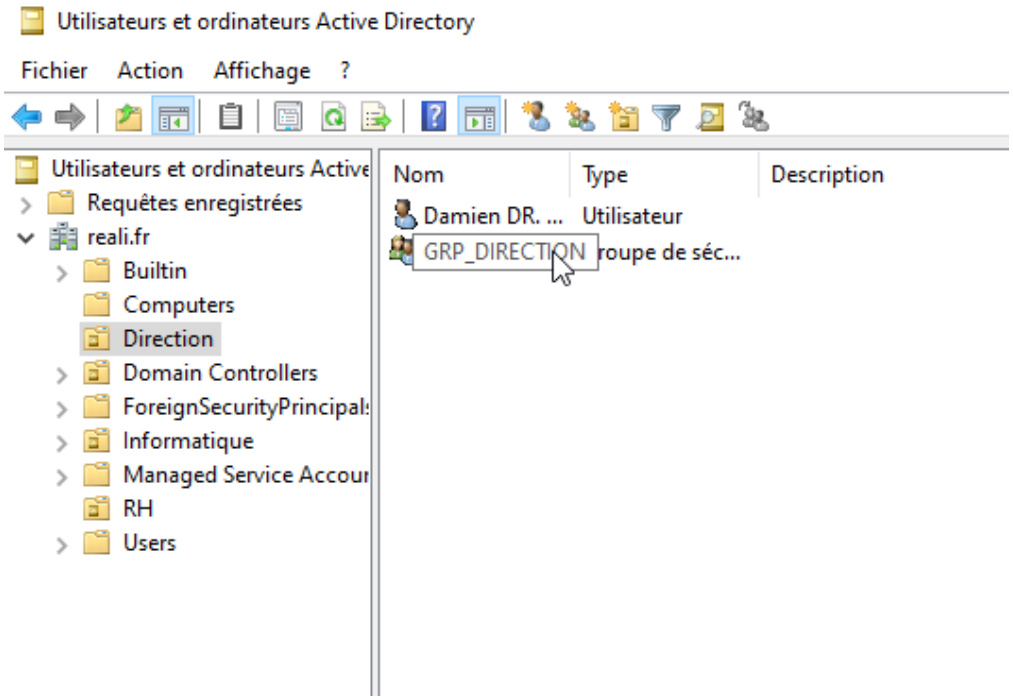
Dans la console « Utilisateurs et ordinateurs Active Directory », on fait un clic droit sur l'OU concernée (ex : OU RH) → Nouveau → Groupe.

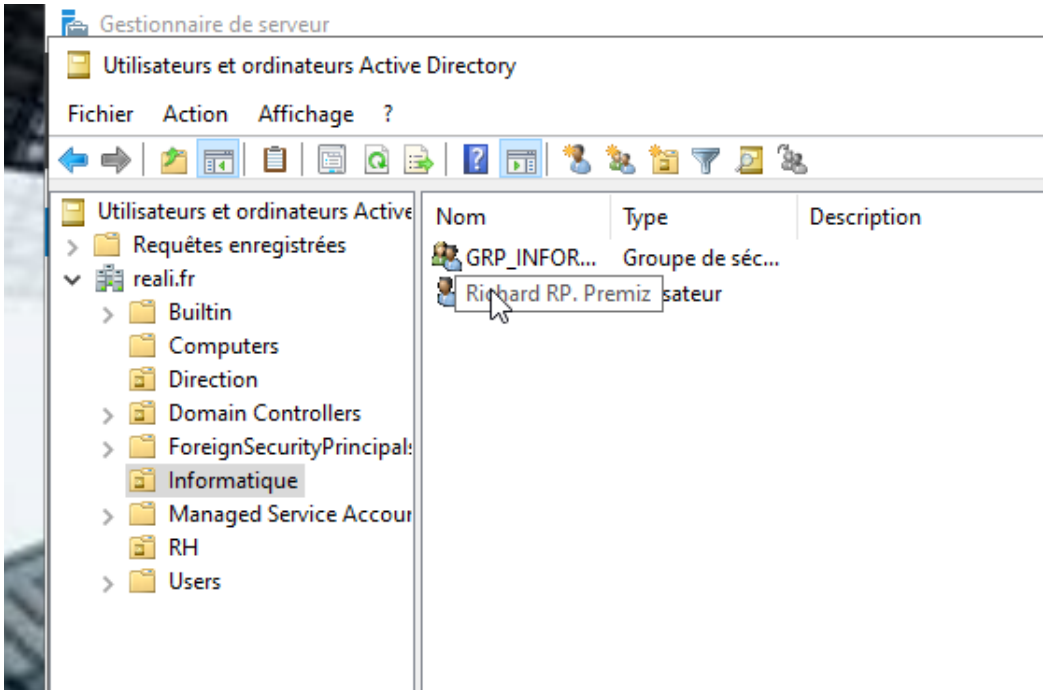
On renseigne :

- Nom du groupe : GRP_RH
- Étendue du groupe : Domaine local
- Type de groupe : Sécurité

On valide et on répète pour GRP_Direction et GRP_Informatique dans leurs OUs respectives.




Utilisateurs et ordinateurs Active Directory
Fichier Action Affichage ?
Utilisateurs et ordinateurs Active
Requêtes enregistrées
reali.fr
Builtin
Computers
Direction
Domain Controllers
ForeignSecurityPrincipal
Informatique
Managed Service Accour
RH
Users
Nom
Type
Description
Damien DR. ...
Utilisateur
GRP_DIRECTION
roupe de séc...

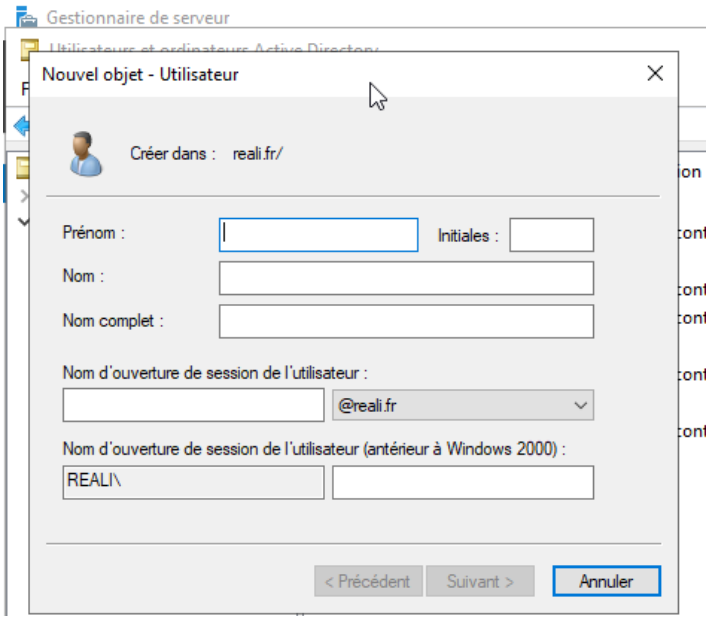

Gestionnaire de serveur
Utilisateurs et ordinateurs Active Directory
Fichier Action Affichage ?
Utilisateurs et ordinateurs Active
Requêtes enregistrées
reali.fr
Builtin
Computers
Direction
Domain Controllers
ForeignSecurityPrincipal
Informatique
Managed Service Accour
RH
Users
Nom
Type
Description
GRP_INFOR...
Groupe de séc...
Richard RP. Premiz
sateur

7. Création des utilisateurs

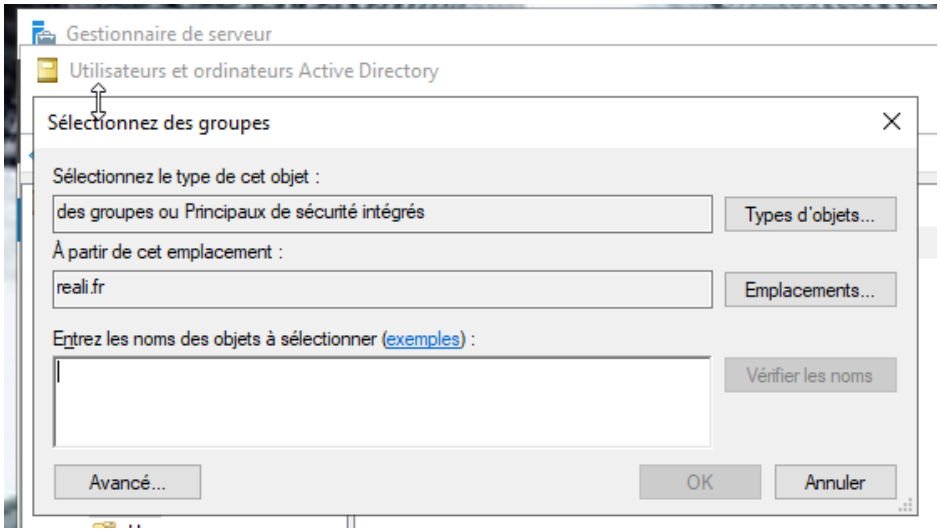
7.1 Procédure

Dans la console « Utilisateurs et ordinateurs Active Directory », on fait un clic droit sur l'OU souhaitée → Nouveau → Utilisateur. On renseigne :

- Prénom / Nom
- Nom d'ouverture de session (ex : francois.dupont)
- Mot de passe : (le mot de passe ne doit pas expirer pour cet environnement de lab)



Après création de l'utilisateur, on l'ajoute à son groupe de sécurité : clic droit sur l'utilisateur → Ajouter à un groupe → on saisit le nom du groupe (ex : GRP_RH).



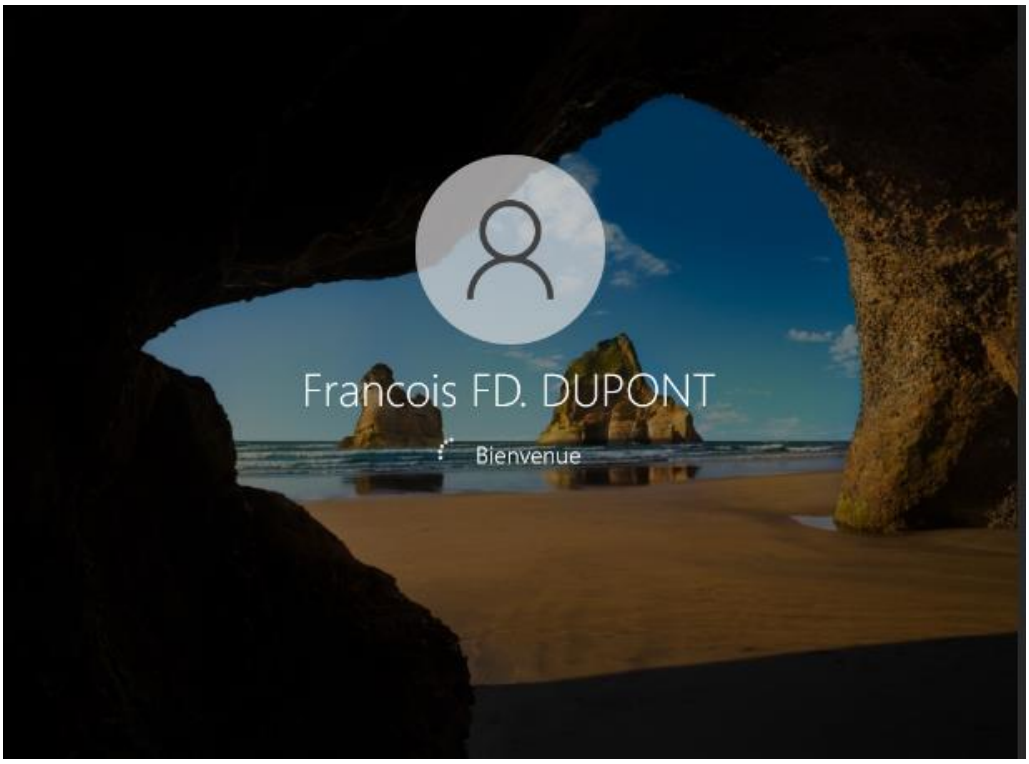
7.2 Utilisateurs créés

Les utilisateurs suivants ont été créés dans leur OU respective :

- francois.dupont → OU RH → membre de GRP_RH
- damien.robert → OU Direction → membre de GRP_Direction
- richard.premiz → OU Informatique → membre de GRP_Informatique

Une fois les utilisateurs créés, on peut tester pour voir sur une VM cliente, de se connecter, pour bien verifier que l'utilisateur a bien été crée.

Dans notre cas, oui



8. Stratégies de groupe (GPO)

8.1 Qu'est-ce qu'une GPO ?

Une GPO (Group Policy Object) est un ensemble de règles et de configurations appliquées automatiquement aux utilisateurs et/ou ordinateurs d'une OU. Elles permettent de standardiser l'environnement de travail et d'appliquer des politiques de sécurité sans intervenir poste par poste.

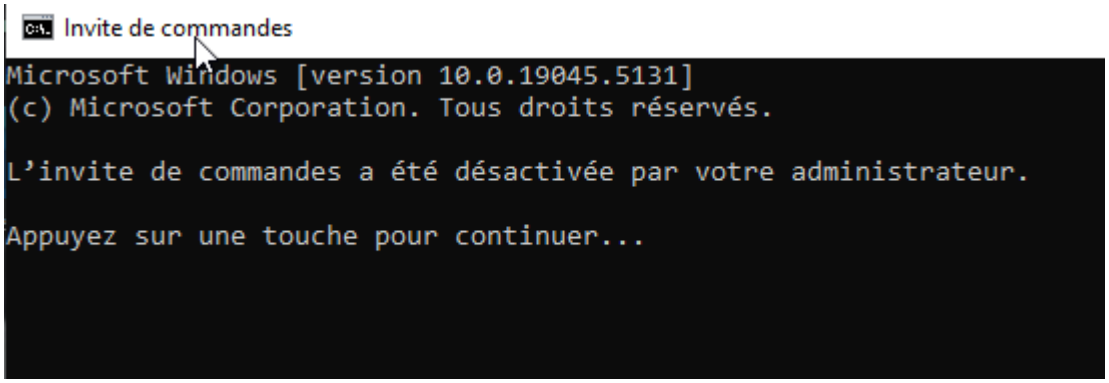
8.2 GPO 1 – Blocage de l'invite de commandes (CMD) sur OU RH

Cette GPO empêche les utilisateurs de l'OU RH d'accéder à l'invite de commandes Windows (cmd.exe), afin de limiter les risques de manipulation du système.

Procédure :

- Ouvrir la console « Gestion des stratégies de groupe » (gpmc.msc)
- Clic droit sur l'OU RH → Créer un objet GPO dans ce domaine et le lier ici
- Nommer la GPO : GPO_Blocage_CMD
- Clic droit sur la GPO → Modifier
- Configuration utilisateur → Modèles d'administration → Système
- Double-cliquer sur « Empêcher l'accès à l'invite de commandes » → Activé
- Appliquer et fermer

On peut donc maintenant constater que les utilisateurs de l'OU RH n'ont plus accès a l'invite de commande



8.3 GPO 2 – Fond d'écran imposé sur le domaine

Cette GPO impose un fond d'écran identique à tous les utilisateurs du domaine reali.fr, pour une image cohérente et professionnelle.

L'image du fond d'écran est stockée sur le serveur :

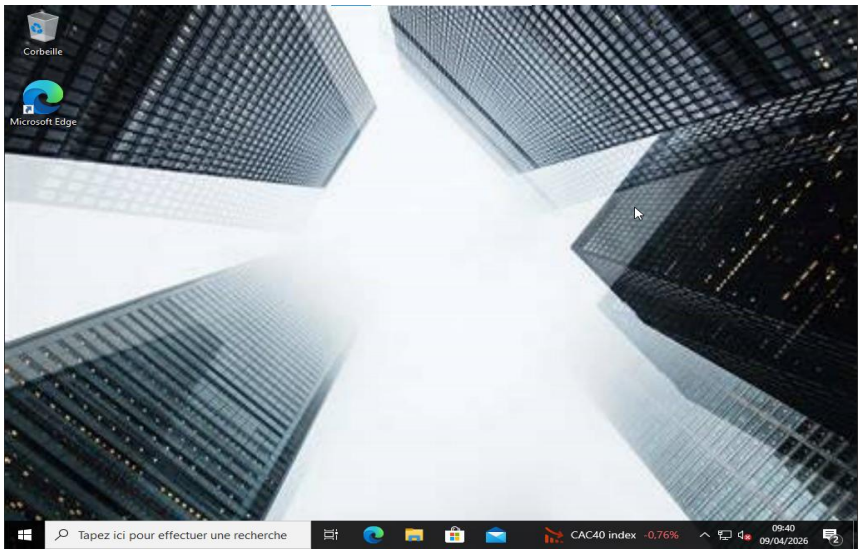
\\WIN-11HDQORGBAU\Wallpaper\fond_ecran.bmp

Procédure :

- Créer un objet GPO lié au domaine reali.fr : GPO_Fond_Ecran
- Configuration utilisateur → Modèles d'administration → Bureau → Bureau
- Double-cliquer sur « Papier peint du Bureau » → Activé
- Renseigner le chemin de l'image
- Style : Étiré → Appliquer et fermer

Pour etre sûr que sa fonctionne, on fais un gpupdate /force

Ceci permet de forcer les GPO.



Voila, les utilisateurs ont donc maintenant un fond d'écran imposé, pour une image plus professionnel.

9. Jonction du poste client au domaine

Pour que les utilisateurs AD puissent se connecter depuis le poste Windows 10 (VM 103 – 192.168.1.50), il faut joindre ce poste au domaine reali.fr.

Procédure sur le poste Windows 10 :

- Configurer l'adresse DNS du poste avec l'IP du contrôleur de domaine : 192.168.1.15
- Clic droit sur « Ce PC » → Propriétés → Paramètres système avancés → Nom de l'ordinateur → Modifier
- Sélectionner « Domaine » et saisir : reali.fr
- Renseigner les identifiants Administrateur du domaine
- Redémarrer le poste

Après redémarrage, le poste apparaît dans la console AD dans le conteneur « Computers » et les utilisateurs du domaine peuvent se connecter.

10. Conclusion

L'Active Directory du domaine reali.fr est désormais pleinement opérationnel. L'infrastructure mise en place comprend :

- Un contrôleur de domaine Windows Server 2022 (VM 102 – 192.168.1.15)
- 3 Unités d'Organisation : RH, Direction, Informatique
- 3 groupes de sécurité : GRP_RH, GRP_Direction, GRP_Informatique
- 3 utilisateurs : francois.dupont, damien.robert, richard.premiz
- 2 GPO actives : blocage CMD (OU RH) et fond d'écran (domaine)
- 1 poste client Windows 10 joint au domaine (VM 103 – 192.168.1.50)

Cette base constitue le socle d'authentification centralisée de l'infrastructure REALIS. Elle est interconnectée avec les autres services du SI (GLPI, Nextcloud, iRedMail) qui utilisent l'annuaire AD pour l'authentification et la gestion des droits des utilisateurs.

BTS Services informatiques aux organisations **SESSION 2026**

ANNEXE VII-1-A : Fiche descriptive de réalisation professionnelle (recto)

Épreuve E6 - Administration des systèmes et des réseaux (option SISR)

DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE

N° réalisation : 2

Nom, prénom : LANGEL Mewen

N° candidat : 02302807062

Épreuve ponctuelle x☐ **Contrôle en cours de formation** ☐ **Date :** 29 / 04 / 2026

Organisation support de la réalisation professionnelle
REALIS – Infrastructure Système d'Information (projet BTS SIO SISR)

Intitulé de la réalisation professionnelle
MISE EN PLACE D'UNE SOLUTION DE SUPERVISION AVEC ZABBIX

Période de réalisation : 2025-2026 **Lieu :** CFA Saint Felix La-Salle Nantes.....
Modalité : ☐ **Seul(e)** ☐ **En équipe**

Compétences travaillées
Concevoir une solution d'infrastructure réseau
Installer, tester et déployer une solution d'infrastructure réseau
Exploiter, dépanner et superviser une solution d'infrastructure réseau

Conditions de réalisation[1] (ressources fournies, résultats attendus)
Ressources fournies :
• Serveur Proxmox VE 9.1.1 (192.168.1.1) avec stockage local-lvm
• LXC 100 Debian 12 (192.168.1.51) créé sur Proxmox
Résultats attendus : serveur Zabbix 7.0 LTS opérationnel, 6 hôtes supervisés (statut ZBX vert), interface web accessible sur http://192.168.1.51/zabbix.

Description des ressources documentaires, matérielles et logicielles utilisées[2]
Déploiement de Zabbix 7.0 LTS sur LXC Debian 12, supervision de 6 hôtes Windows et Linux
Matériel :
• PC sous Proxmox VE 9.1.1 (hyperviseur)
• LXC 100 : Zabbix Server – Debian 12, 1 vCPU, 512 Mo RAM, 8 Go disque (192.168.1.51)
• VM 102 : Windows Server 2022 (192.168.1.15), VM 103 : Windows 10 (192.168.1.50)
• LXC 101 Nextcloud (192.168.1.52), LXC 104 GLPI (192.168.1.53), LXC 105 iRedMail (192.168.1.54)
Logiciels :
• Proxmox VE 9.1.1, Debian 12, Zabbix Server 7.0 LTS, Apache2, MariaDB
• Zabbix Agent 7.0 LTS (MSI Windows + paquet Linux)
Documentation :
• Documentation procédure : Realisation_2_Zabbix_Mewen_LANGEL.docx

Modalités d'accès aux productions[3] et à leur documentation[4]
Documentation technique : dossier de réalisation Zabbix (fichier .docx)
Accès à l'infrastructure : https://192.168.1.1:8006 (Proxmox VE) – Login : root mdp rootroot
Interface Zabbix : http://192.168.1.51/zabbix – Login : Admin mdp Azertyuiop44./
VM 102 Windows Server 2022 : 192.168.1.15 – Login : Administrateur mdp Azertyuiop44./
VM 103 Windows 10 : 192.168.1.50 – Login : (prendre un user) mdp : Azertyuiop44./

---

[1] En référence aux *conditions de réalisation et ressources nécessaires* du bloc « Administration des systèmes et des réseaux » prévues dans le référentiel de certification du BTS SIO.

[2] Les réalisations professionnelles sont élaborées dans un environnement technologique conforme à l'annexe II.E du référentiel du BTS SIO.

[3] Conformément au référentiel du BTS SIO « *Dans tous les cas, les candidats doivent se munir des outils et ressources techniques nécessaires au déroulement de l'épreuve. Ils sont seuls responsables de la disponibilité et de la mise en œuvre de ces outils et ressources. La circulaire nationale d'organisation précise les conditions matérielles de déroulement des interrogations et les pénalités à appliquer aux candidats qui ne se seraient pas munis des éléments nécessaires au déroulement de l'épreuve.* ». Les éléments nécessaires peuvent être un identifiant, un mot de passe, une adresse réticulaire (URL) d'un espace de stockage et de la présentation de l'organisation du stockage.

[4] Lien vers la documentation complète, précisant et décrivant, si cela n'a été fait au verso de la fiche, la réalisation, par exemples schéma complet de réseau mis en place et configurations des services.

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2026**

ANNEXE VII-1-A : Fiche descriptive de réalisation professionnelle (verso, éventuellement pages suivantes)

Épreuve E6 - Administration des systèmes et des réseaux (option SISR)

Descriptif de la réalisation professionnelle, y compris les productions réalisées et schémas explicatifs

CONTEXTE

Dans le cadre du projet REALIS (infrastructure virtualisée sur Proxmox VE), j'ai mis en place une solution de supervision centralisée avec Zabbix 7.0 LTS, déployée sur un conteneur LXC Debian 12 (LXC 100 – 192.168.1.51). L'objectif est de surveiller en temps réel l'ensemble des machines de l'infrastructure REALIS.

CE QUI A ÉTÉ RÉALISÉ

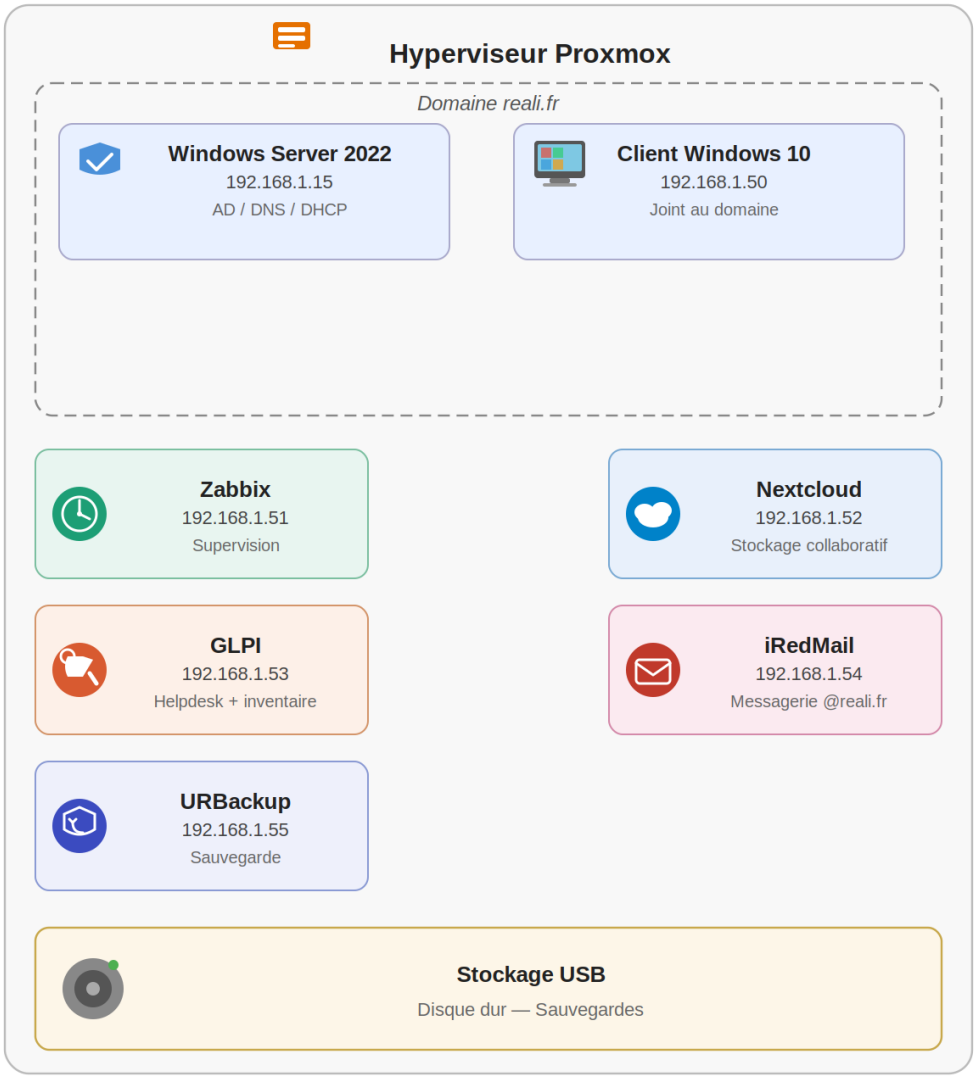
1. Création du LXC 100 sur Proxmox : Debian 12, 1 vCPU, 512 Mo RAM, 8 Go disque, bridge vmbr0, IP 192.168.1.51/24, passerelle 192.168.1.1, DNS 192.168.1.15
2. Installation de Zabbix 7.0 LTS : ajout du dépôt officiel Zabbix, installation des paquets (zabbix-server-mysql, zabbix-frontend-php, zabbix-apache-conf, zabbix-sql-scripts, zabbix-agent), installation MariaDB, création base zabbix + utilisateur zabbix, import schéma SQL, configuration DBPassword=zabbix dans zabbix_server.conf, démarrage des services
3. Configuration interface web : correction locale (dpkg-reconfigure locales → en_US.UTF-8), assistant installation (DB localhost/zabbix/zabbix, serveur zabbix-realis, timezone Europe/Paris), connexion Admin/zabbix puis changement mdp Azertyuiop44./
4. Installation agents Zabbix : Windows (VM 102 + VM 103) via MSI 7.0 LTS (Server=192.168.1.51, port 10050, règle pare-feu TCP 10050) ; Linux (GLPI, Nextcloud, iRedMail) via dépôt + zabbix_agentd.conf (Server/ServerActive=192.168.1.51) ; cas iRedMail : ajout règle nftables (tcp dport 10050 accept)
5. Ajout des 6 hôtes dans Zabbix (Data collection → Hosts → Create host) :

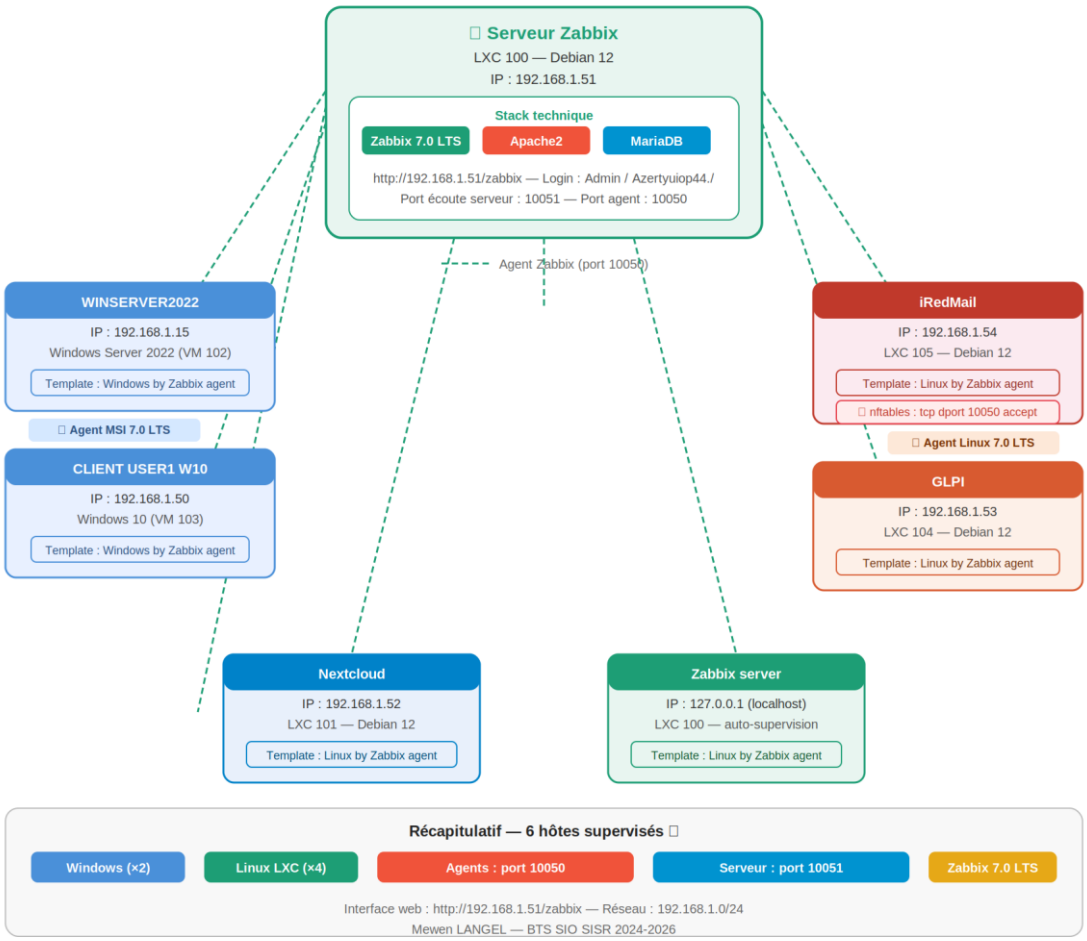
• WINSERVER2022 (192.168.1.15) – Windows by Zabbix agent
• CLIENT USER1 W10 (192.168.1.50) – Windows by Zabbix agent
• iRedMail (192.168.1.54), GLPI (192.168.1.53), Nextcloud (192.168.1.52), Zabbix server (127.0.0.1) – Linux by Zabbix agent

RÉSULTAT

La solution de supervision Zabbix 7.0 LTS est pleinement opérationnelle. Les 6 hôtes sont supervisés en temps réel (statut ZBX vert), les agents communiquent correctement sur le port 10050, et l'interface web est accessible sur http://192.168.1.51/zabbix.

Réseau – 192.168.1.0/24




Infrastructure Zabbix — Supervision REALIS
LXC 100 — 192.168.1.51 — Zabbix 7.0 LTS
Serveur Zabbix
LXC 100 — Debian 12
IP : 192.168.1.51
Stack technique
Zabbix 7.0 LTS
Apache2
MariaDB
http://192.168.1.51/zabbix — Login : Admin / Azertyuiop44./
Port écoute serveur : 10051 — Port agent : 10050
Agent Zabbix (port 10050)
WINSERVER2022
IP : 192.168.1.15
Windows Server 2022 (VM 102)
Template : Windows by Zabbix agent
Agent MSI 7.0 LTS
CLIENT USER1 W10
IP : 192.168.1.50
Windows 10 (VM 103)
Template : Windows by Zabbix agent
iRedMail
IP : 192.168.1.54
LXC 105 — Debian 12
Template : Linux by Zabbix agent
nftables : tcp dport 10050 accept
Agent Linux 7.0 LTS
GLPI
IP : 192.168.1.53
LXC 104 — Debian 12
Template : Linux by Zabbix agent
Nextcloud
IP : 192.168.1.52
LXC 101 — Debian 12
Template : Linux by Zabbix agent
Zabbix server
IP : 127.0.0.1 (localhost)
LXC 100 — auto-supervision
Template : Linux by Zabbix agent
Récapitulatif — 6 hôtes supervisés
Windows (×2)
Linux LXC (×4)
Agents : port 10050
Serveur : port 10051
Zabbix 7.0 LTS
Interface web : http://192.168.1.51/zabbix — Réseau : 192.168.1.0/24
Mewen LANGEL — BTS SIO SISR 2024-2026

Mewen LANGEL
BTS SIO SISR 2024-2026

MISE EN PLACE D'UNE SOLUTION DE SUPERVISION AVEC ZABBIX

Déploiement de Zabbix 7.0 LTS sur infrastructure REALIS

BTS SIO – Option SISR
Infrastructure REALIS – domaine reali.fr

SOMMAIRE :

1. Contexte et objectifs ...p3
2. Création du conteneur LXC sur Proxmox ...p5
3. Configuration réseau et mise à jour ...p6
4. Installation de Zabbix 7.0 LTS ...p6
5. Configuration de l'interface web ...p9
6. Installation des agents Zabbix ...p10
7. Ajout des hôtes dans Zabbix ...p14
8. Vérification de la supervision ...p15
9. Conclusion ...p16

1. Contexte et objectifs

1.1 Contexte de l'entreprise

REALIS (Réseau Administration et Logistique Informatisée des Systèmes) est une entreprise fictive dont l'infrastructure informatique est entièrement virtualisée sur un hyperviseur Proxmox VE (192.168.1.1). L'objectif est de mettre en place un système d'information complet et fonctionnel, répondant aux besoins d'une PME.

Dans ce contexte, la mise en place d'une solution de supervision est essentielle : elle permet de surveiller en temps réel l'état de toutes les machines de l'infrastructure, de détecter les pannes et d'anticiper les problèmes de performance.

1.2 Besoin identifié

Sans outil de supervision, l'administrateur ne dispose d'aucune visibilité sur l'état de l'infrastructure, ce qui pose plusieurs problèmes :

- Aucune alerte en cas de panne d'un service ou d'un serveur
- Impossible de détecter une surcharge CPU ou mémoire avant qu'elle impacte les utilisateurs
- Pas de traçabilité sur l'historique des performances
- Administration réactive (on découvre le problème quand l'utilisateur signale une panne)

Zabbix répond à ces besoins en offrant :

- Une interface centralisée pour superviser tous les équipements
- Des agents légers installés sur chaque machine (Windows et Linux)
- Des graphes de performance (CPU, mémoire, réseau, disque)
- Un système d'alertes configurable

1.3 Solution retenue

Déploiement de Zabbix 7.0 LTS sur un conteneur LXC Debian 12, hébergé sur Proxmox VE. Les caractéristiques du déploiement sont :

- Conteneur LXC 100 – IP : 192.168.1.51 – Debian 12
- Zabbix Server 7.0 LTS + Apache2 + MariaDB
- Interface web accessible sur http://192.168.1.51/zabbix
- 6 hôtes supervisés : WinServer2022, Win10, iRedMail, GLPI, Nextcloud, Zabbix lui-même

1.4 Tableau des compétences mobilisées

Code	Compétence
C1.1	Recueillir les besoins et les contraintes techniques
C2.1	Installer et configurer les équipements et services réseau
C3.1	Administrer les services réseau (supervision, agents)
C3.2	Diagnostiquer et corriger les dysfonctionnements
C4.1	Rédiger une documentation technique claire et structurée

2. Création du conteneur LXC sur Proxmox

2.1 Prérequis

Avant de créer le conteneur, il faut télécharger le template Debian 12 dans Proxmox. Dans l'interface Proxmox → local (proxmox) → CT Templates → Télécharger, sélectionner debian-12-standard.

2.2 Paramètres du conteneur

Sur l'interface Proxmox (https://192.168.1.1:8006), je clique sur Créer CT et remplis les champs suivants :

Paramètre	Valeur
CT ID	**100**
Hostname	**zabbix**
Template	Debian 12
Mot de passe root	**Azertyuiop44./**
CPU	1 cœur
RAM	512 Mio
Disque	8 Gio sur local-lvm
IP	**192.168.1.51/24**
Passerelle	**192.168.1.1**
DNS server	**192.168.1.15 (Windows Server)**
Non privilégié	Oui

Une fois le conteneur créé, le démarrer depuis l'interface Proxmox et ouvrir la console.

3. Configuration réseau et mise à jour

3.1 Vérification de la connectivité

Une fois connecté en root dans la console du LXC, vérifier que le réseau fonctionne :

```
ping -c 4 192.168.1.1
ping -c 4 8.8.8.8
```

3.2 Mise à jour du système

Avant toute installation, mettre à jour les paquets :

```
apt update && apt upgrade -y
```

Cette commande met à jour la liste des paquets disponibles puis installe les mises à jour. Cela peut prendre 1 à 2 minutes.

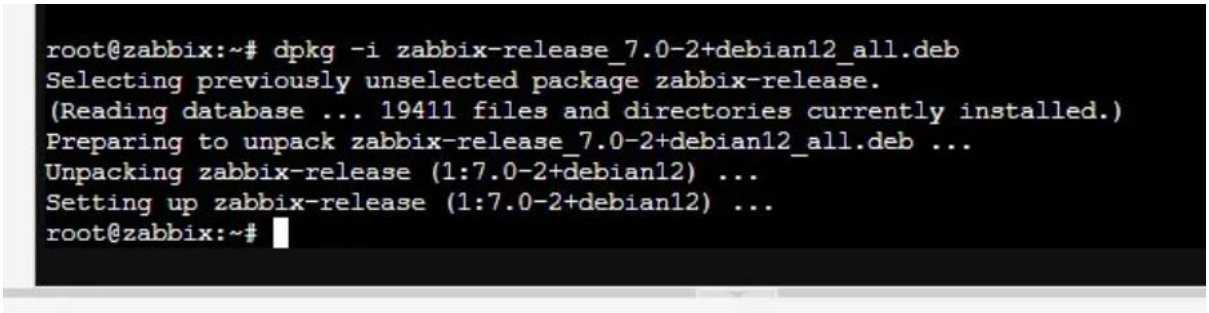
4. Installation de Zabbix 7.0 LTS

4.1 Ajout du dépôt officiel Zabbix

Zabbix n'est pas disponible dans les dépôts Debian par défaut. Il faut ajouter le dépôt officiel Zabbix 7.0 LTS :

```
wget https://repo.zabbix.com/zabbix/7.0/debian/pool/main/z/zabbix-release/zabbix-release_latest_7.0+debian12_all.deb
```

Puis `dpkg -i zabbix-release_latest_7.0+debian12_all.deb`



Puis `apt update` pour mettre à jour.

4.2 Installation des paquets Zabbix

Installer le serveur Zabbix, l'interface web, l'agent et le frontend Apache :

```
apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-sql-scripts zabbix-agent -y
```

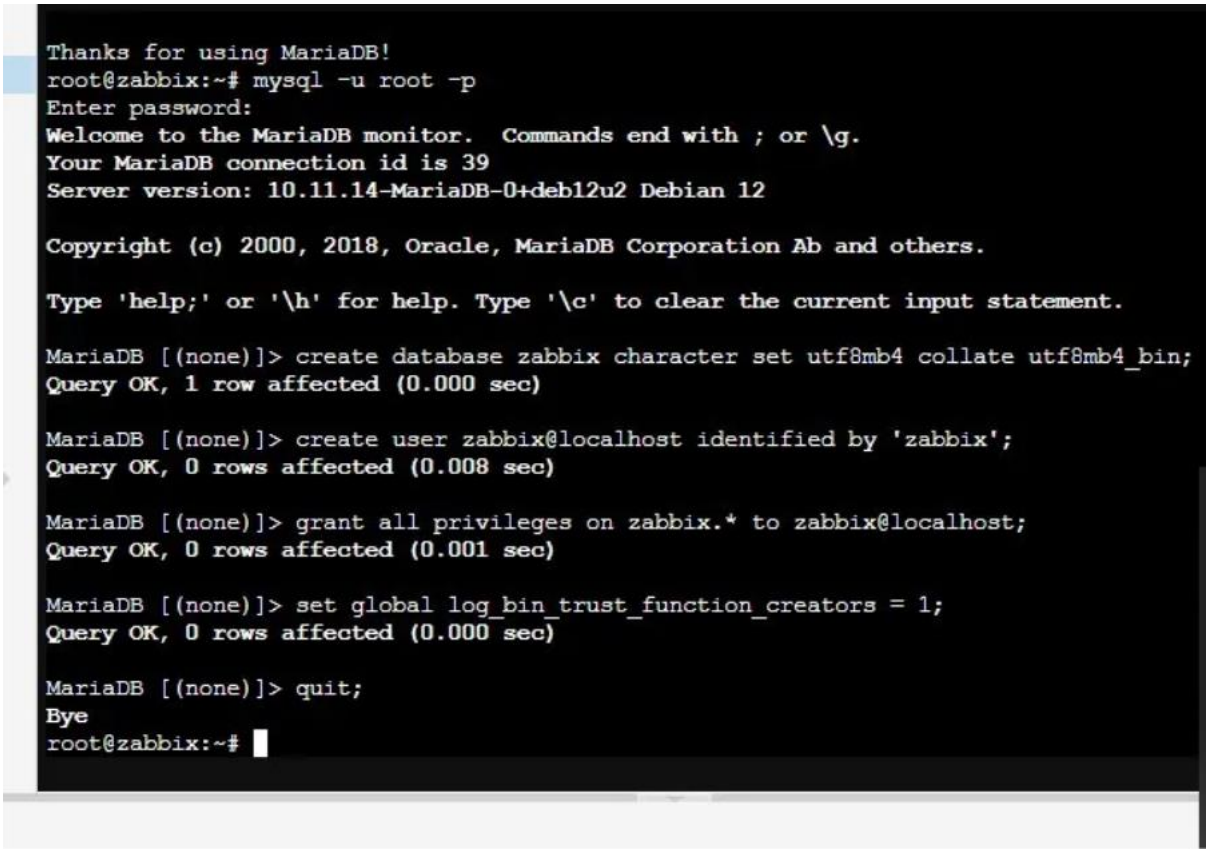
4.3 Installation et configuration de MariaDB

Zabbix utilise une base de données MariaDB pour stocker les données de supervision. Installer MariaDB :

```
apt install mariadb-server -y
mysql_secure_installation
```

Créer la base de données et l'utilisateur Zabbix :

```
mysql -uroot -p
CREATE DATABASE zabbix CHARACTER SET utf8mb4 COLLATE utf8mb4_bin;
CREATE USER zabbix@localhost IDENTIFIED BY 'zabbix';
GRANT ALL PRIVILEGES ON zabbix.* TO zabbix@localhost;
SET GLOBAL log_bin_trust_function_creators = 1;
FLUSH PRIVILEGES; EXIT;
```



4.4 Import du schéma SQL

Importer le schéma de base de données Zabbix :

```
zcat /usr/share/zabbix-sql-scripts/mysql/server.sql.gz | mysql --default-character-set=utf8mb4 -uzabbix -p zabbix
```

Cette commande peut prendre 1 à 2 minutes. Elle importe toutes les tables nécessaires au fonctionnement de Zabbix.

Puis désactiver l'option log_bin :

```
mysql -uroot -p
SET GLOBAL log_bin_trust_function_creators = 0;
EXIT;
```

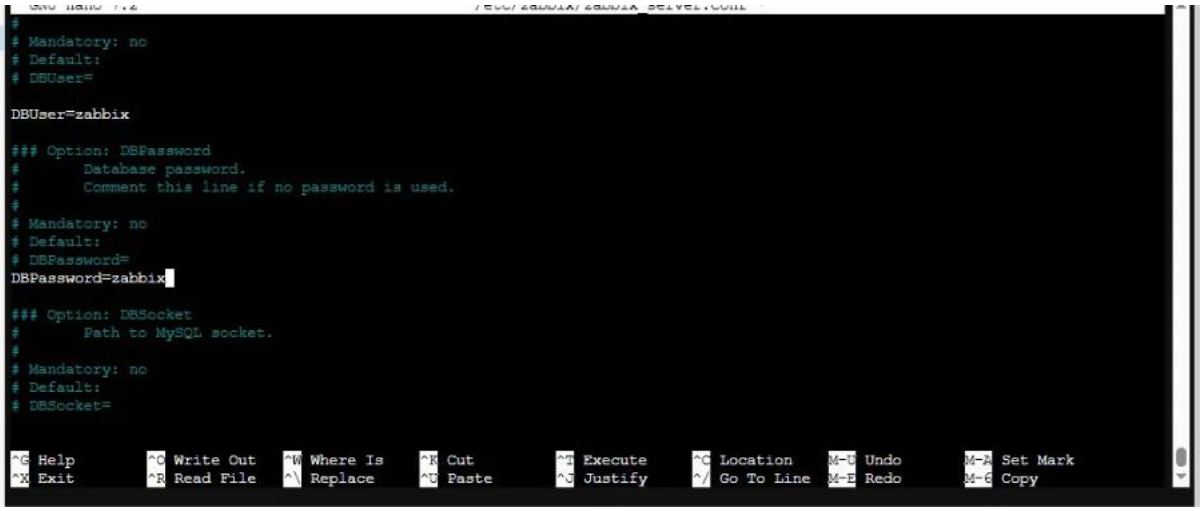
4.5 Configuration du fichier zabbix_server.conf

Renseigner le mot de passe de la base de données dans le fichier de configuration :

```
nano /etc/zabbix/zabbix_server.conf
```

Trouver la ligne DBPassword et renseigner :

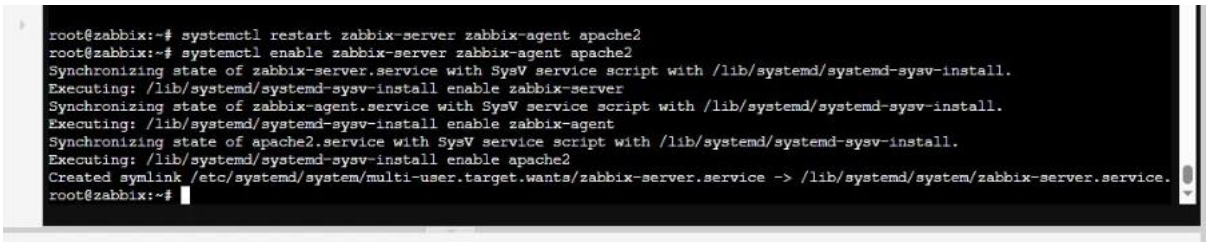
```
DBPassword=zabbix
```



4.6 Démarrage des services

Démarrer et activer les services Zabbix au démarrage :

```
systemctl restart zabbix-server zabbix-agent apache2
systemctl enable zabbix-server zabbix-agent apache2
```



5. Configuration de l'interface web

5.1 Correction de la locale

Avant d'accéder à l'interface web, il faut corriger la locale du système pour éviter un avertissement dans l'assistant d'installation :

```
dpkg-reconfigure locales
```

Dans le menu : sélectionner en_US.UTF-8, valider, choisir en_US.UTF-8 comme locale par défaut.

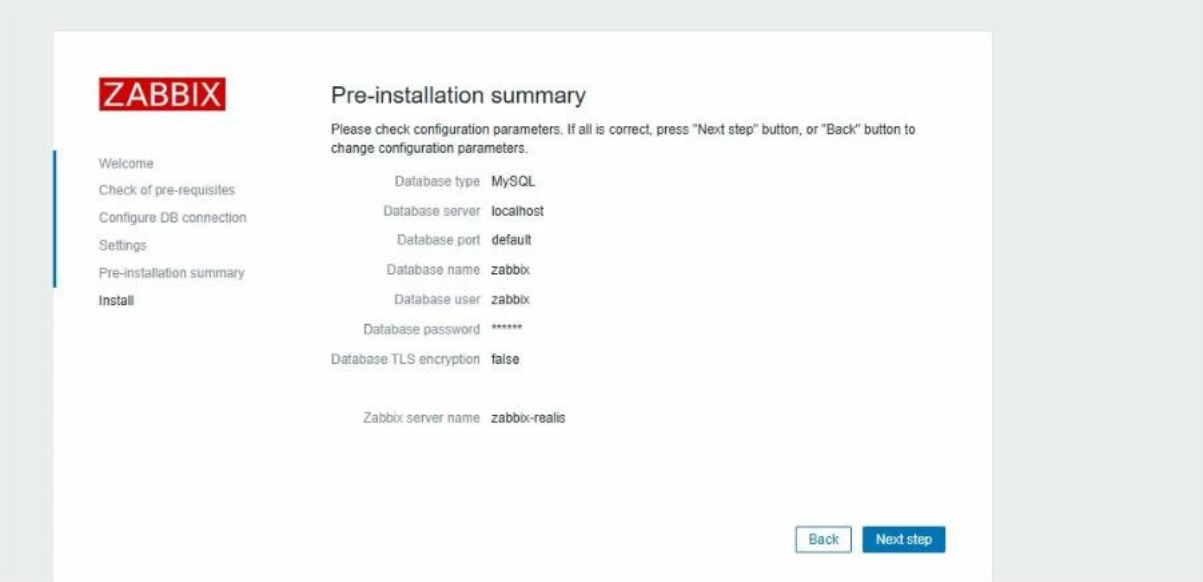
```
systemctl restart apache2
```

5.2 Assistant d'installation web

Ouvrir un navigateur et aller sur : http://192.168.1.51/zabbix

L'assistant d'installation se lance. Suivre les étapes :

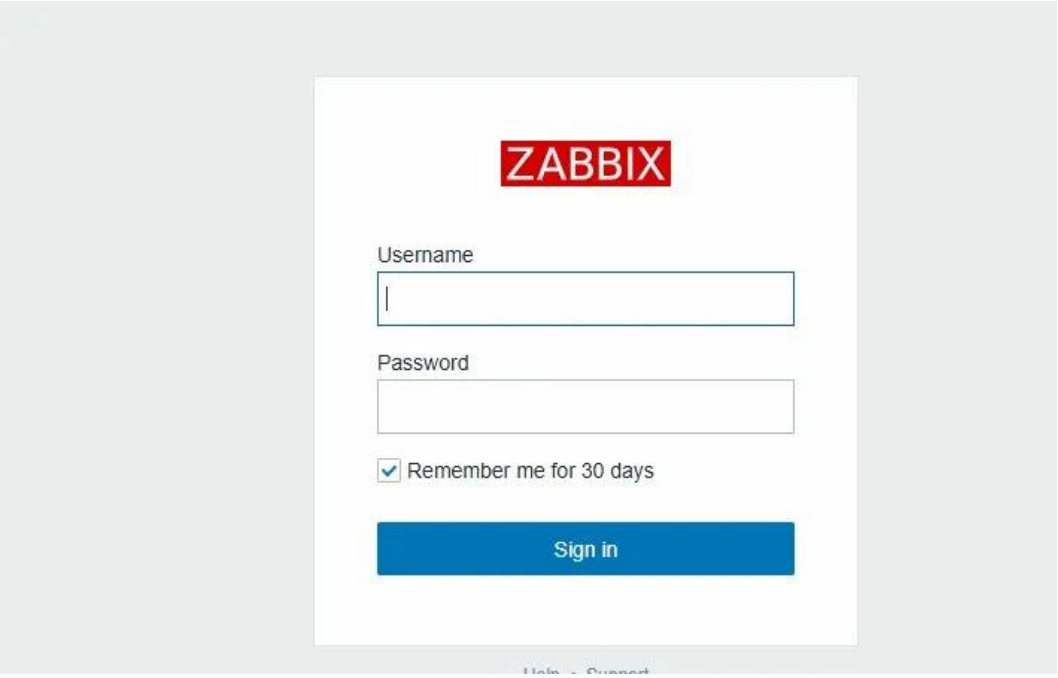
- Étape 1 – Check of pre-requisites : tout doit être vert → Next step
- Étape 2 – Configure DB connection : Database host : localhost / Database name : zabbix / User : zabbix / Password : zabbix → Next step
- Étape 3 – Settings : Zabbix server name : zabbix-realis / Default time zone : Europe/Paris → Next step
- Étape 4 – Pre-installation summary : vérifier et Next step
- Étape 5 – Install : Zabbix est installé → Finish



5.3 Première connexion

Se connecter avec les identifiants par défaut : Login : Admin / Mot de passe : zabbix

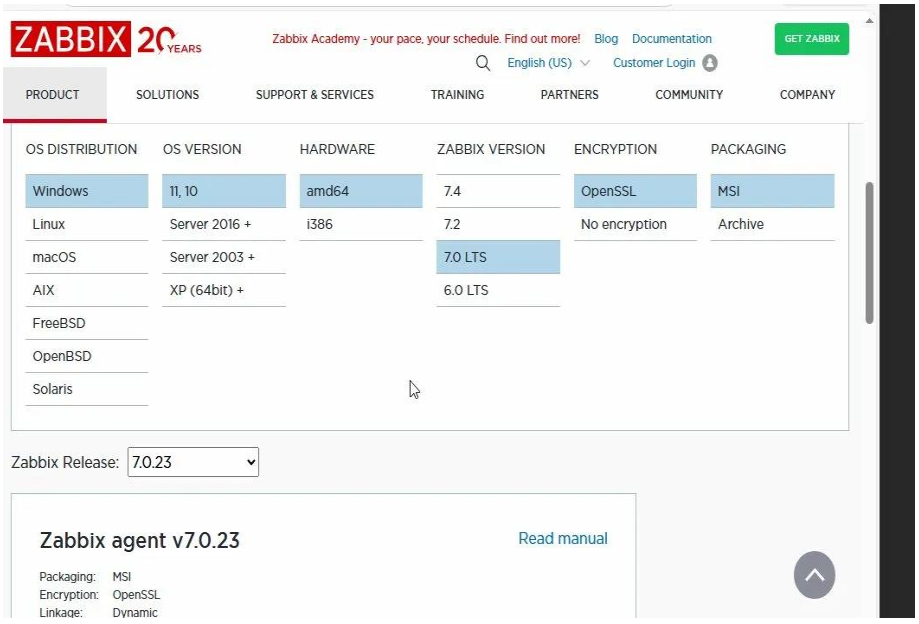
Puis changer le mot de passe dans Administration → Users → Admin → Change password : Azertyuiop44./

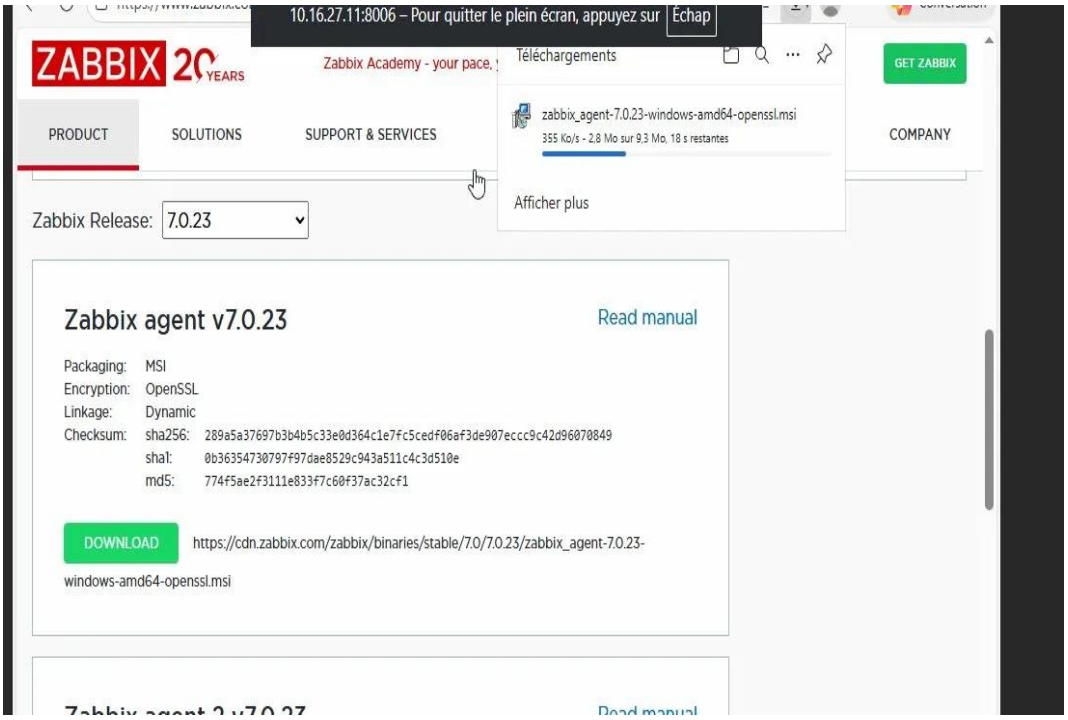


6. Installation des agents Zabbix

6.1 Agents sur les VMs Windows

Pour superviser les machines Windows (VM 102 – 192.168.1.15 et VM 103 – 192.168.1.50), installer l'agent Zabbix 7.0 LTS (MSI amd64) téléchargé depuis le site officiel zabbix.com.

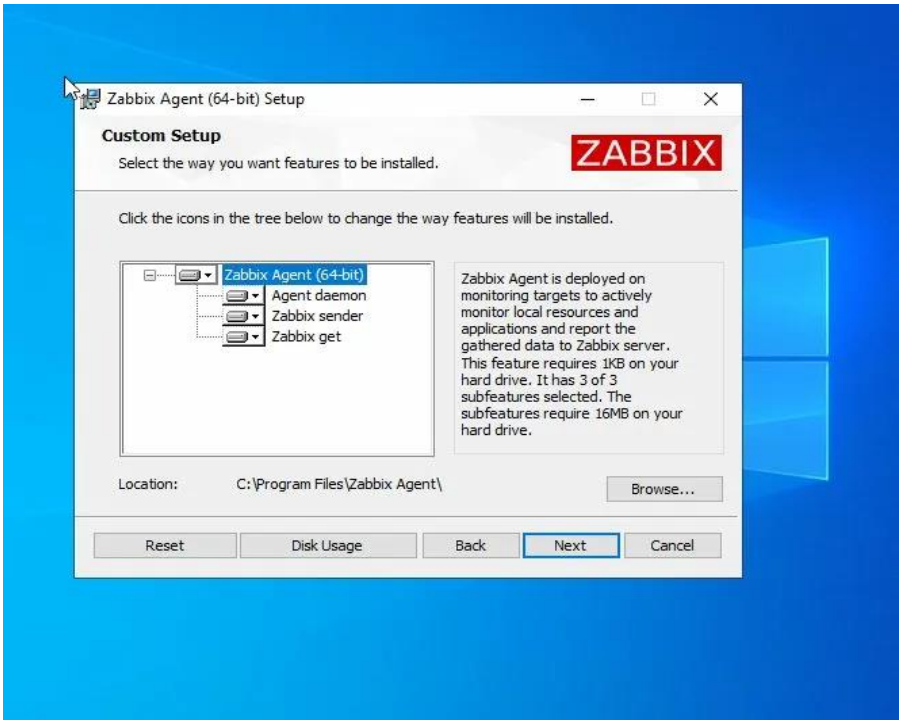


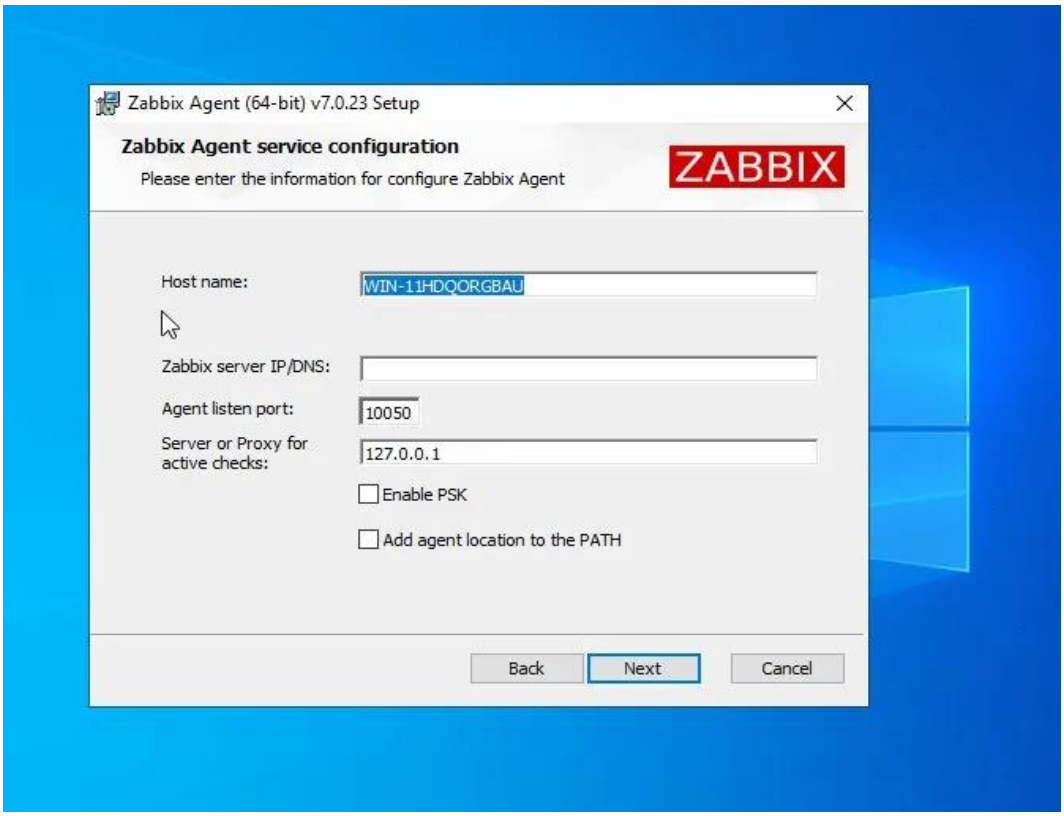


Ensuite,

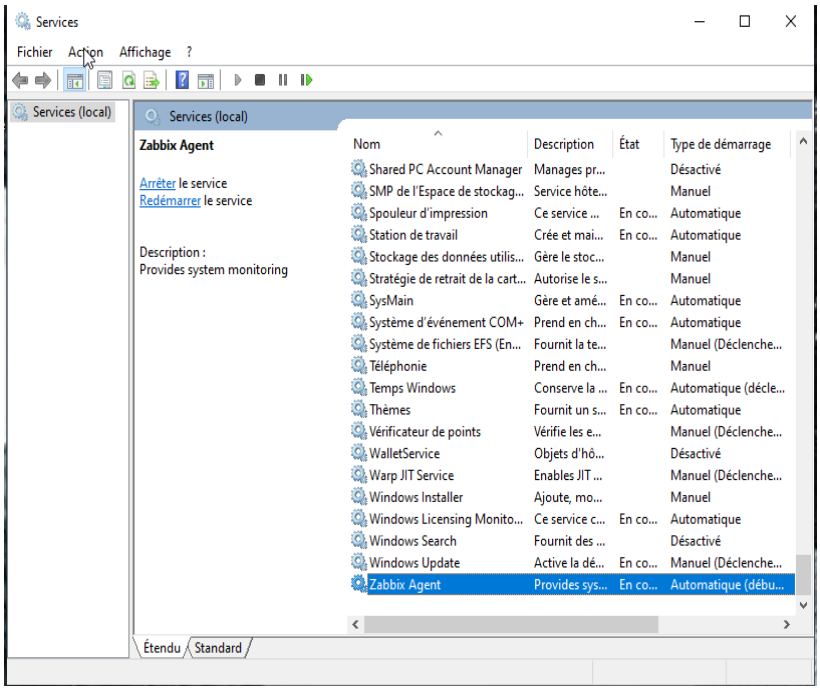
Lors de l'installation du MSI, renseigner :

- Zabbix server IP/DNS : 192.168.1.51
- Agent hostname : WINSERVER2022 (ou CLIENT USER1 W10 pour le poste client)
- Server port : 10050





Vérifier que le service Zabbix Agent est bien démarré dans les services Windows (services.msc).



6.2 Agents sur les conteneurs LXC Linux

Pour les LXCs Linux (GLPI, Nextcloud, iRedMail), installer l'agent Zabbix depuis le dépôt officiel :

```
wget https://repo.zabbix.com/zabbix/7.0/debian/pool/main/z/zabbix-release/zabbix-release_latest_7.0+debian12_all.deb
dpkg -i zabbix-release_latest_7.0+debian12_all.deb
apt update && apt install zabbix-agent -y
```

Configurer le fichier /etc/zabbix/zabbix_agentd.conf :

```
nano /etc/zabbix/zabbix_agentd.conf
```

Modifier les lignes :

```
Server=192.168.1.51
ServerActive=192.168.1.51
Hostname=glpi   (adapter selon la machine)

systemctl restart zabbix-agent
systemctl enable zabbix-agent
```

6.3 Cas particulier – iRedMail (nftables)

Sur le LXC iRedMail (192.168.1.54), le pare-feu nftables bloque par défaut le port 10050 utilisé par l'agent Zabbix. Il faut ajouter une règle :

```
nano /etc/nftables.conf
```

Ajouter dans la section tcp dport :

```
tcp dport 10050 accept
systemctl restart nftables
```

7. Ajout des hôtes dans Zabbix

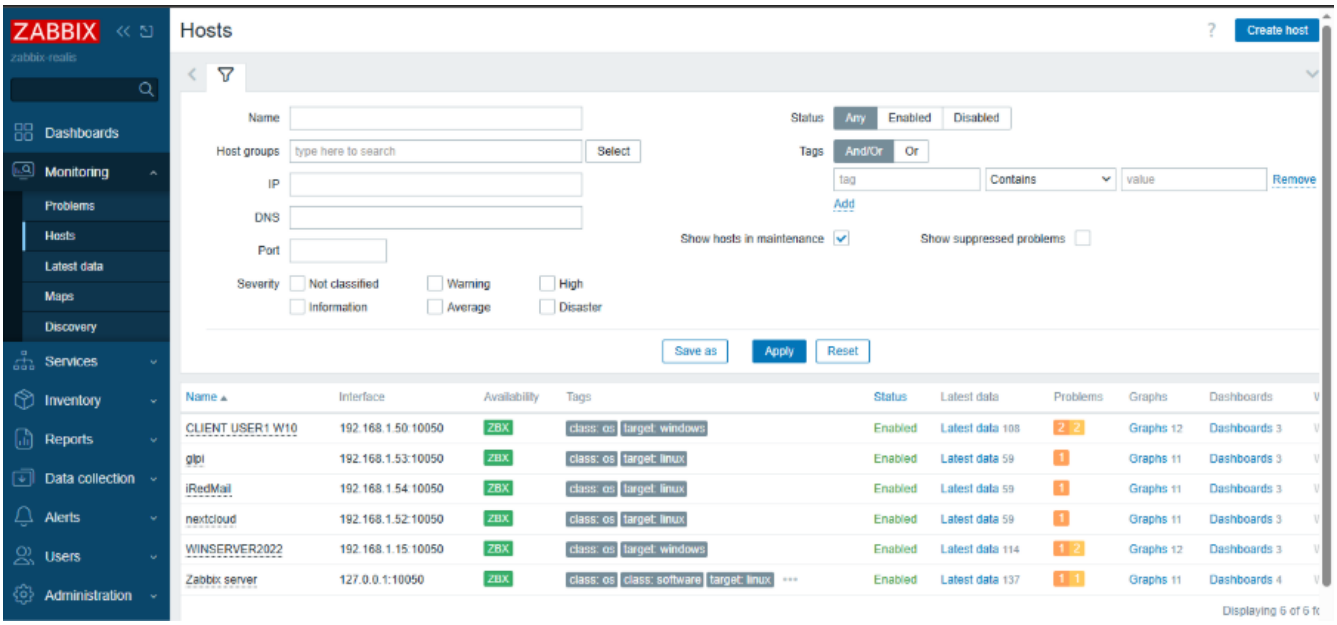
7.1 Procédure d'ajout d'un hôte

Dans l'interface Zabbix → Data collection → Hosts → Create host :

- Host name : nom de la machine (ex : WINSERVER2022)
- Templates : sélectionner le template correspondant (Windows by Zabbix agent ou Linux by Zabbix agent)
- Agent interface : IP de la machine, port 10050
- Valider avec Add

7.2 Hôtes supervisés

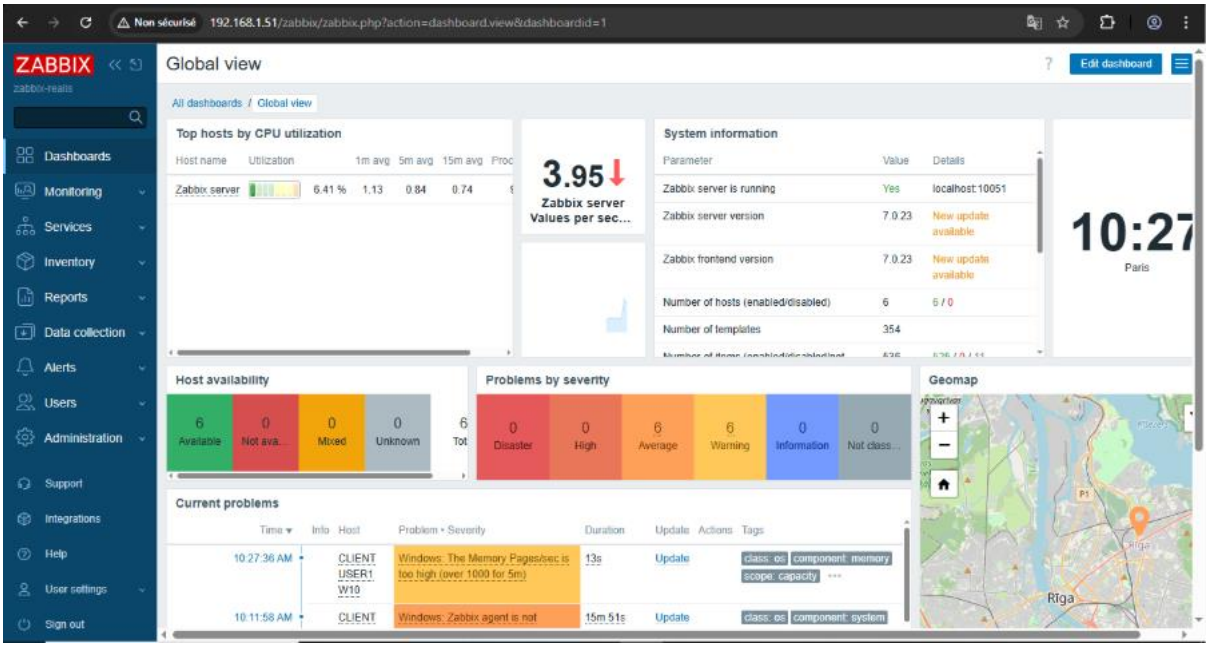
Hôte	IP	Template
WINSERVER2022	192.168.1.15	Windows by Zabbix agent
CLIENT USER1 W10	192.168.1.50	Windows by Zabbix agent
iRedMail	192.168.1.54	Linux by Zabbix agent
glpi	192.168.1.53	Linux by Zabbix agent
nextcloud	192.168.1.52	Linux by Zabbix agent
Zabbix server	127.0.0.1	Linux by Zabbix agent



8. Vérification de la supervision

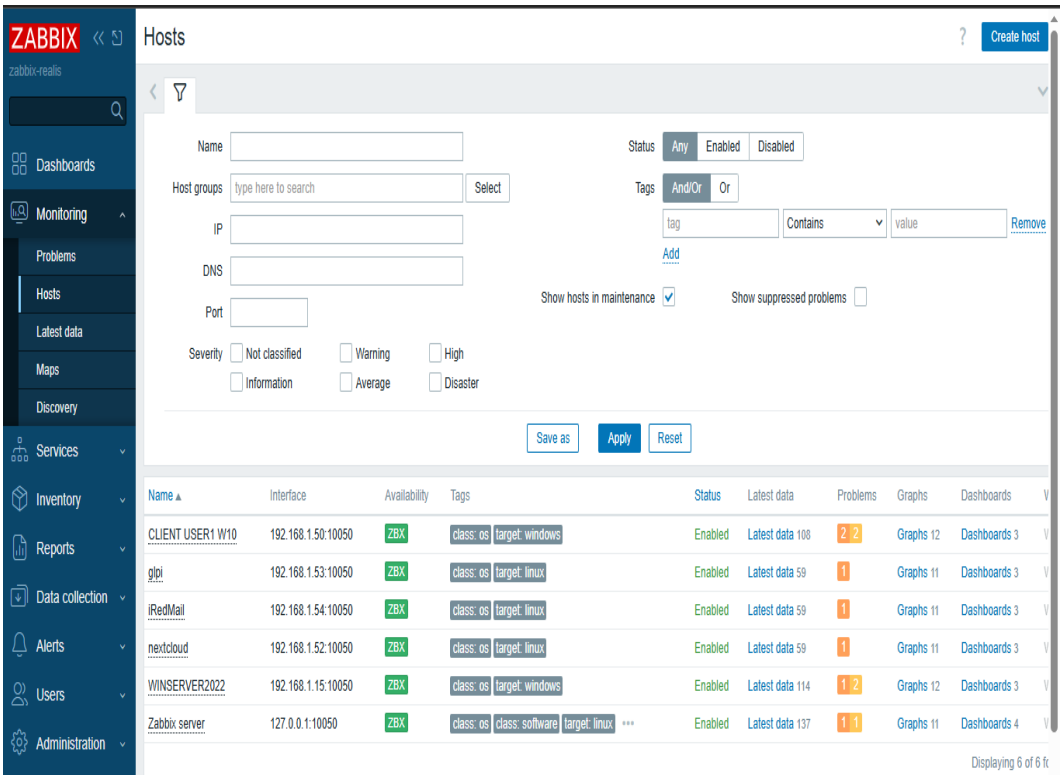
8.1 Tableau de bord Zabbix

Une fois tous les hôtes ajoutés et les agents configurés, le tableau de bord Zabbix affiche l'état de tous les équipements en temps réel.



8.2 Liste des hôtes actifs

Dans Monitoring → Hosts, les 6 hôtes apparaissent avec le statut ZBX vert, indiquant que les agents communiquent correctement avec le serveur Zabbix.



8.3 Données de supervision

Pour chaque hôte, il est possible de consulter les données collectées (CPU, mémoire, disque, réseau) via Latest data et d'afficher des graphes historiques.

9. Conclusion

La solution de supervision Zabbix 7.0 LTS est désormais pleinement opérationnelle sur l'infrastructure REALIS. L'ensemble des machines est supervisé en temps réel.

L'infrastructure mise en place comprend :

- Un serveur Zabbix 7.0 LTS sur LXC 100 (192.168.1.51) – Debian 12 + Apache2 + MariaDB
- 6 hôtes supervisés : WINSERVER2022, CLIENT USER1 W10, iRedMail, GLPI, Nextcloud, Zabbix server
- Agents Windows (MSI) installés sur les deux VMs Windows
- Agents Linux installés sur les 3 LXCs (GLPI, Nextcloud, iRedMail) + règle nftables sur iRedMail
- Interface web accessible sur http://192.168.1.51/zabbix

Cette solution de supervision constitue un élément clé de l'infrastructure REALIS. Elle permet à l'administrateur de détecter rapidement tout dysfonctionnement et d'assurer la disponibilité des services pour les utilisateurs du domaine reali.fr.