DHCP

Active Directory

- Créer la VM sur proxmox

1-Renommer le nom du serveur

l'adresse ip , connecter le serveur au réseau

Dans gestion des serveur :: 10.3.0.203

Définir le serveur AD

Configuration du contrôleur de domaine

Activation des certificats AD

Création des unité d'organisation

Menu démarrer taper gestionnaire de stratégie de group

- Utilisateur puis organisation pour créer les utilisateur dans l'unité d'organisation
- Puis créer le gpo dans utilisateur
- Clik droit et modifier
- Ici restriction gestionniare de tache

→ **Modèles d’administration**

→ **Système**

→ 👉 **Options Ctrl+Alt+Suppr**

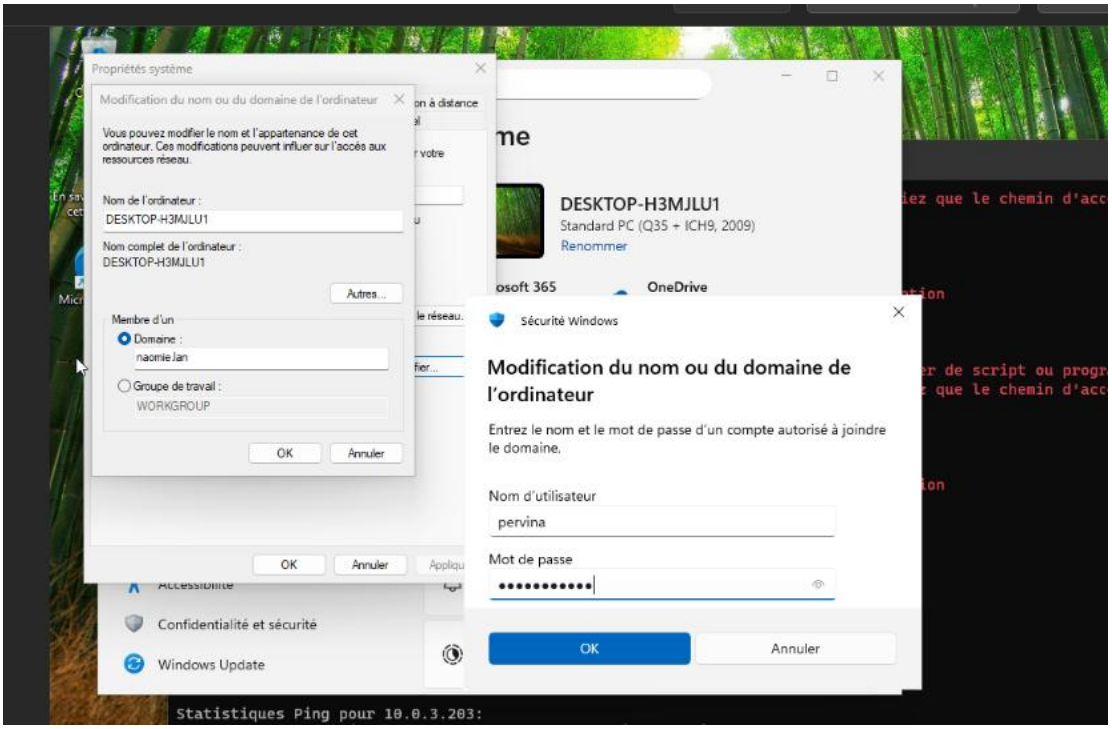
Supprimer le gestionnaire de taches

Cliqué sur activé puis terminer

Appliquer un gpo par

Domaine + controleur de domaine

Intégrer le poste client dans le domaine (administrateur/naomie.lan



VM client

Client configuration réseau : maj+f10

start ms-cxh:localonly

Pui entrer les information

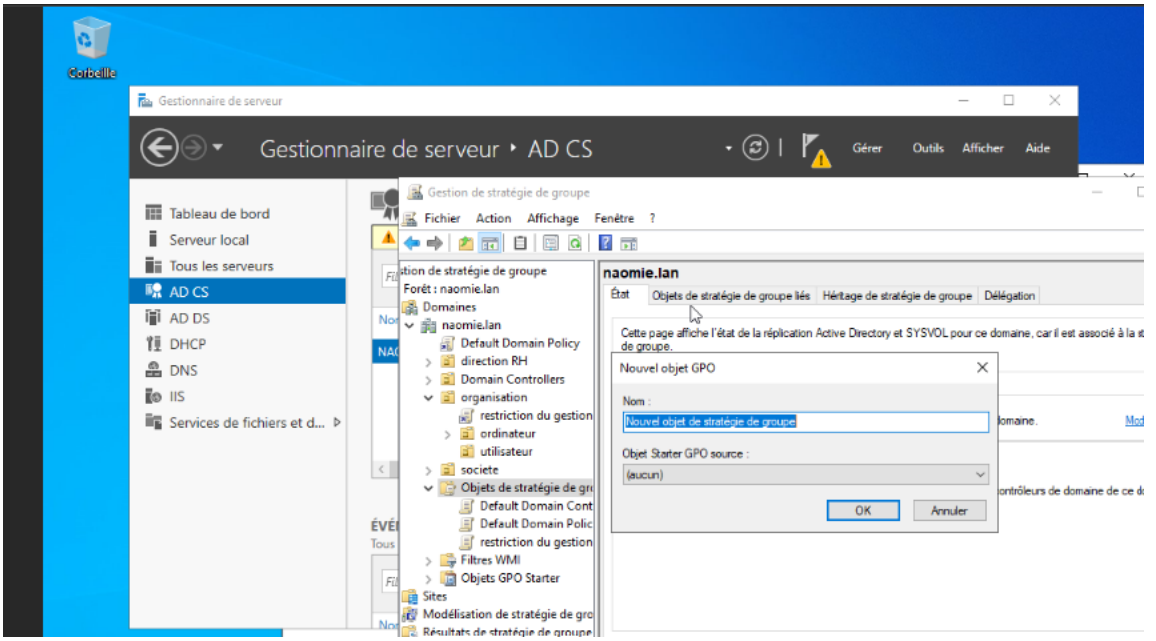
10.3.0.208 pervina

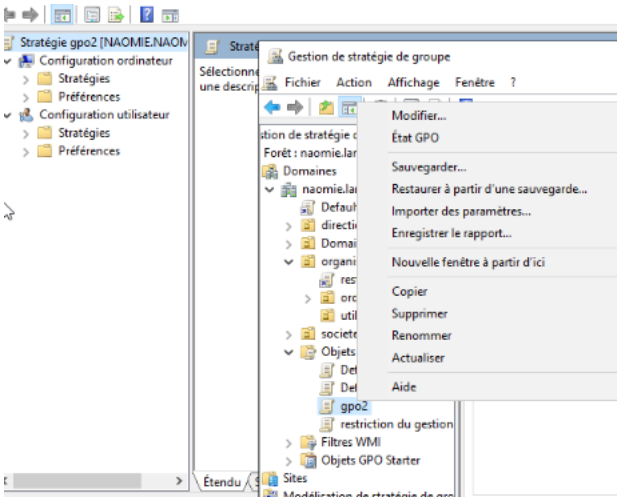
Gpo : j'ai créer une gpo qui délivre automatiquement le certificats

Je voudrai créer Un modèle de certificat à Créer de façon automatique par gpo

Ajouter une GPO

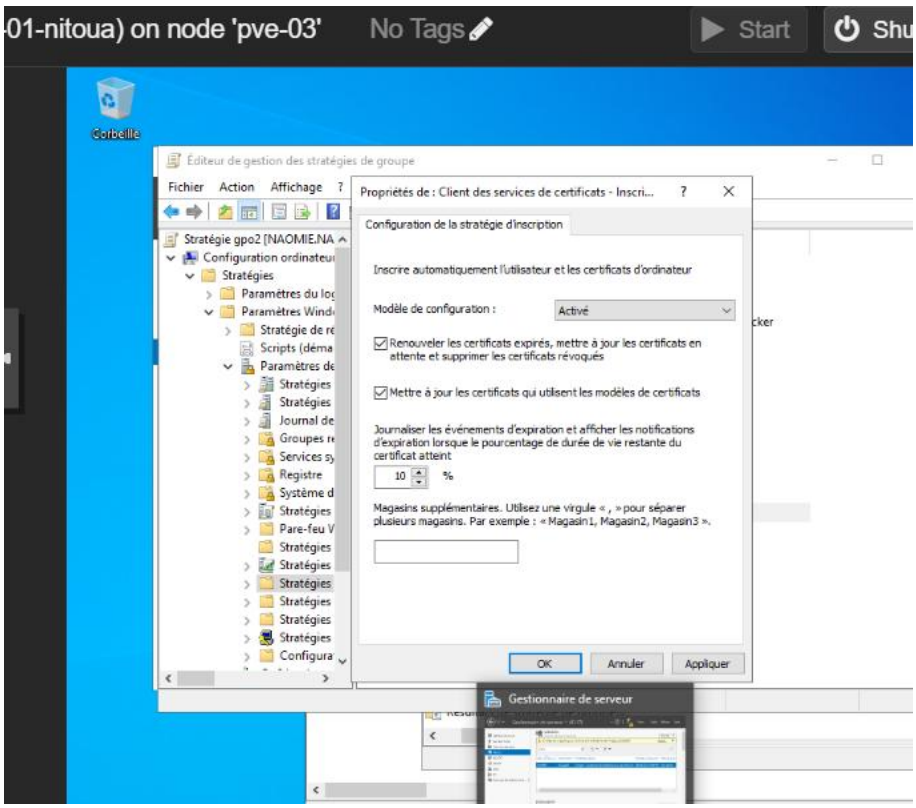
Taper gpo dans le menu démarrer

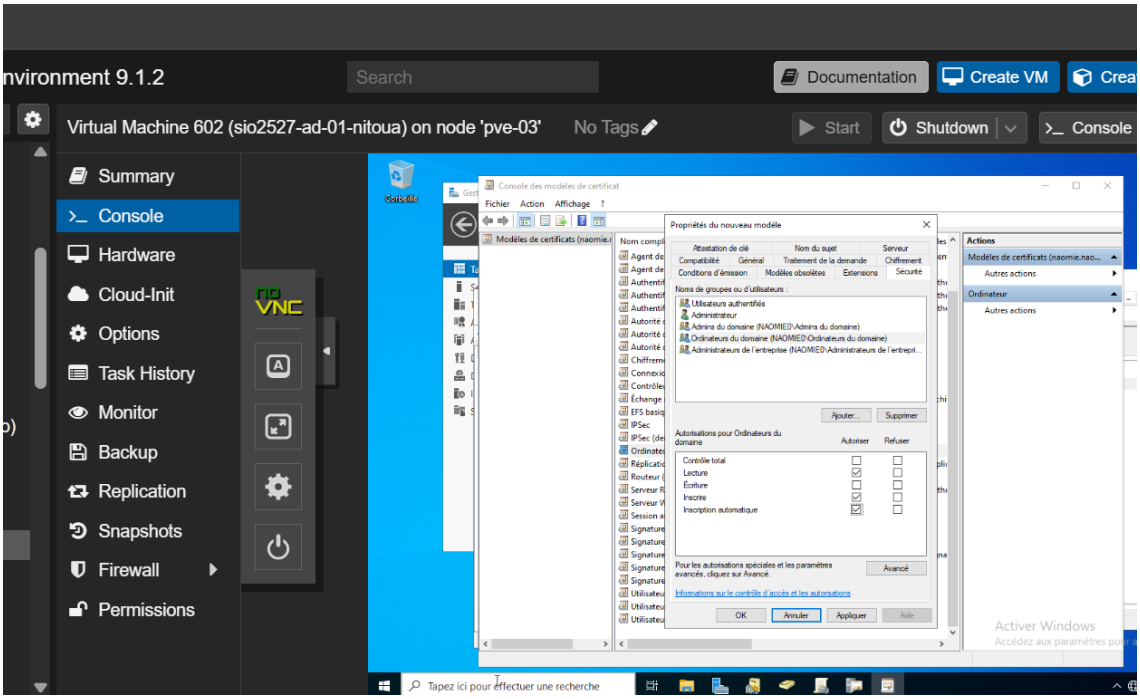




Gpo : j'ai créer une gpo qui délivre automatiquement le certificats

Je voudrai créer Un modèle de certificat à Créer de façon automatique gpo




Search
Documentation
Create VM
Virtual Machine 602 (sio2527-ad-01-nitoua) on node 'pve-03'
No Tags
Start
Shutdown
Console
Summary
Console
Hardware
Cloud-Init
Options
Task History
Monitor
Backup
Replication
Snapshots
Firewall
Permissions
noVNC
Propriétés du nouveau modèle
Tapez ici pour effectuer une recherche

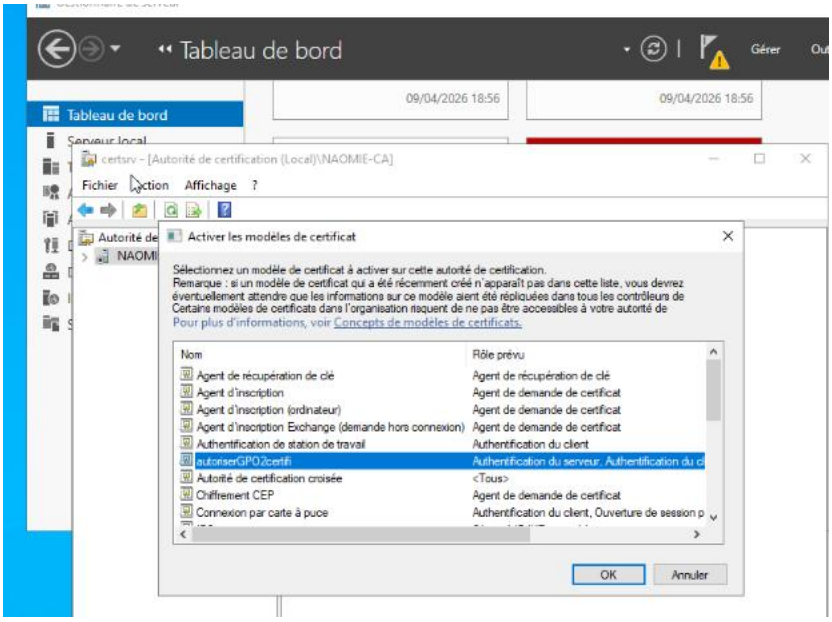
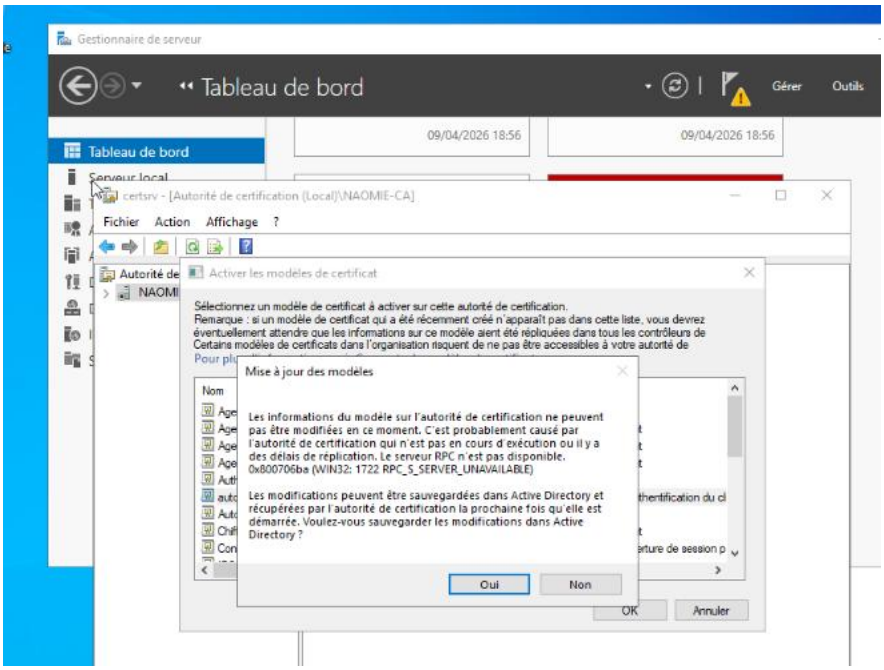


Tableau de bord
Gérer
09/04/2026 18:56
09/04/2026 18:56
certsrv - [Autorité de certification (Local)\NAOMIE-CA]
Fichier
Action
Affichage
Activer les modèles de certificat
Sélectionnez un modèle de certificat à activer sur cette autorité de certification.
Remarque : si un modèle de certificat qui a été récemment créé n'apparaît pas dans cette liste, vous devrez éventuellement attendre que les informations sur ce modèle aient été répliquées dans tous les contrôleurs de
Pour plus d'informations, voir Concepts de modèles de certificats.
Nom
Rôle prévu
Agent de récupération de clé
Agent d'inscription
Agent d'inscription (ordinateur)
Agent d'inscription Exchange (demande hors connexion)
Authentification de station de travail
autoriserGPO2certifi
Autorité de certification croisée
Chiffrement CEP
Connexion par carte à puce
OK
Annuler



Objectif de la manipulation

Automatiser la distribution de certificats numériques aux ordinateurs du domaine sans aucune intervention manuelle sur les postes clients.

Les 4 étapes clés du déploiement

1. Création du Modèle de Certificat

Comme on ne part jamais de zéro, nous sommes allés dans la console certtmpl.msc pour **dupliquer** le modèle existant "Ordinateur".

- *Pourquoi ?* Pour créer un modèle personnalisé capable d'être distribué automatiquement.

2. Configuration des Droits (Sécurité)

C'est l'étape cruciale. Dans l'onglet **Sécurité** du modèle, nous avons configuré le groupe **Ordinateurs du domaine** avec les droits :

- **Lecture** : Pour voir le modèle.
- **Inscrire** : Pour avoir le droit de demander le certificat.
- **Inscription automatique** (Auto-enroll) : Pour que la demande se fasse toute seule en arrière-plan.

3. Publication du Modèle

Dans la console **Autorité de certification** (certsrv.msc), nous avons ajouté le nouveau modèle dans le dossier **Modèles de certificats à délivrer**.

- *Résultat :* Le serveur de certificats (CA) est maintenant prêt à fabriquer et à envoyer ces certificats.

4. Distribution par GPO

Tu avais déjà créé la GPO (dans gpmc.msc). Cette stratégie dit aux ordinateurs : *"Allez vérifier régulièrement sur l'Active Directory s'il y a des certificats qui vous sont destinés et téléchargez-les."*

Résumé technique (La minute SISR 🤓)

- **Technologie :** AD CS (Active Directory Certificate Services).
- **Protocole :** Auto-enrollment via RPC.
- **Bénéfice :** Sécurisation du parc informatique (authentification des machines, chiffrement, Wi-Fi sécurisé) de manière centralisée et invisible pour l'utilisateur.

Note pour Naomie : Si un examinateur te demande comment tu vérifies que ça a marché, tu lui réponds : *"Je lance un gpupdate /force sur un PC client et je vérifie la présence du certificat dans la console certlm.msc (magasin de certificats local)."*

po map réseaux

Serveur de fichier sur widows

Jouer avec le DNS