Mode Opératoire

OCS Déploiement – Plugin - Package - CVE Search

MENAGE-BIMENET Cylian / COELHO Tom
15/11/2024

OCS Déploiement – Plugin - Package - CVE Search

Auteur	MENAGE BIMBENET Cylian / COELHO Tom
Date de création	15/11/2024
Rédiger par	MENAGE BIMBENET Cylian / COELHO Tom
Réalisé par	MENAGE BIMBENET Cylian / COELHO Tom
Valider par	MENAGE BIMBENET Cylian / COELHO Tom

Objectif de la procédure : Installation et configuration du déploiement de clients OCS (& plugins). Découverte réseau via OCS. Déploiement de paquets via OCS. Installation et configuration de CVE-Search.

Matériels utilisés : Une Debian12 (pour le serveur OCS), une debian 12 (pour le serveur CVE-Search) et un Windows 11.

OCS Déploiement – Plugin - Package - CVE Search

Sommaire

Table des matières

OCS Déploiement – Plugin - Package - CVE Search

I. Différentes solution de déploiement

1er Solution AD.

OCS INVENTORY sur des machines clientes, qui font partie d'un domaine, en utilisant l'outil de déploiement OCS PACKAGER et en utilisant une stratégie de groupe (GPO).

Prérequis :

- Un serveur Windows 2022 :
  - Fonctionnel, avec le rôle Active Directory Domain Services (AD/DS) installé.
  - Géré dans un domaine Active Directory.
- Un utilisateur du domaine :
  - Avec des permissions d'administration pour créer et appliquer des stratégies de groupe (GPO).
- Un serveur LAMP (Linux, Apache, MySQL, PHP) :
  - Basé sur Debian 12, configuré pour héberger OCS Inventory.
- OCS Inventory fonctionnel :
  - Installé et configuré sur le serveur Debian, avec une base de données accessible et un certificat SSL configuré (http 80 pour le moment).
- OCS PACKAGER :
  - Outil installé sur le poste administrateur pour créer un package agent configuré avec les paramètres du serveur.

Pourquoi c'est une bonne pratique :

- Centralisé et automatisé : Convient pour les environnements Active Directory.
- Facile à maintenir : Les modifications ou mises à jour sont gérées via la GPO.
- Respecte les standards de sécurité et d'organisation IT.

2e Solution OCS-Deploy.

Déploiement à distance depuis le serveur OCS Inventory.

Prérequis :

- Serveur OCS Inventory fonctionnel :
  - Hébergé sur une distribution Linux, configuré pour gérer les agents clients.
- Connectivité réseau :
  - Les postes cibles doivent être accessibles depuis le serveur via des ports ouverts (ex. 135 pour RPC, 445 pour SMB).
- Compte administrateur réseau :
  - Utilisé pour exécuter les installations distantes (peut être un compte de service).
- Postes Windows préconfigurés :
  - Les services nécessaires doivent être activés :
    - Partage de fichiers et imprimantes (SMB).
    - WMI (Windows Management Instrumentation) pour la communication distante.

Pourquoi c'est une bonne pratique :

- Fonction intégrée à OCS Inventory.
- Pas besoin d’outils externes ou de dépendances complexes.

3e Solution SCCM.

Déploiement avec SCCM (Microsoft Endpoint Configuration Manager)

Prérequis :

- Infrastructure SCCM fonctionnelle :
  - Configurée pour gérer les postes clients Windows.
- Accès au serveur OCS Inventory :
  - Les postes cibles doivent pouvoir communiquer avec le serveur via HTTP/HTTPS.
- Fichier d'installation configuré :
  - Préparer un package SCCM avec l'installateur de l'agent et ses paramètres (exemple : /S /SERVER=http://adresse_du_serveur_OCS).
- Postes clients Windows gérés par SCCM :
  - Tous les postes cibles doivent être inscrits dans SCCM et accessibles via le réseau.

Pourquoi c'est une bonne pratique :

- Permet un contrôle fin sur les machines cibles (groupes, conditions spécifiques).
- Suivi détaillé : Statut de l'installation, erreurs, rapports.
- Très adapté pour des environnements à grande échelle.

4e Comparaison des solutions.

Comparaison des solutions

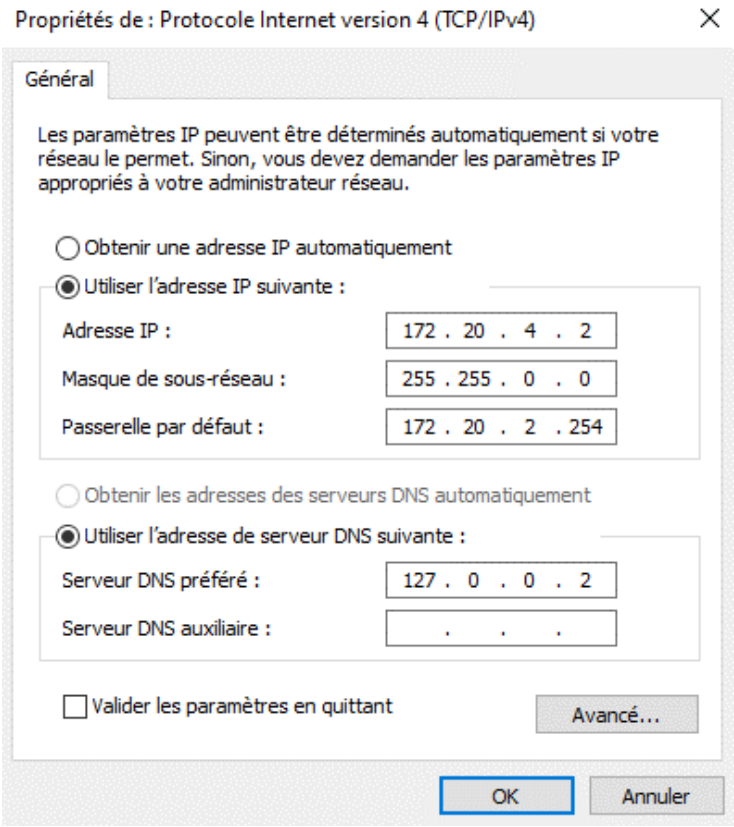
Solution	Efficacité	Complexité de mise en œuvre	Taille de l'environnement cible	Maintenabilité
GPO avec OCS PACKAGER	Très élevée	Moyenne	Moyenne à grande	Facile
Déploiement depuis le serveur	Moyenne à élevée	Faible	Petite à moyenne	Moyenne
SCCM	Très élevée	Élevée	Grande	Très facile

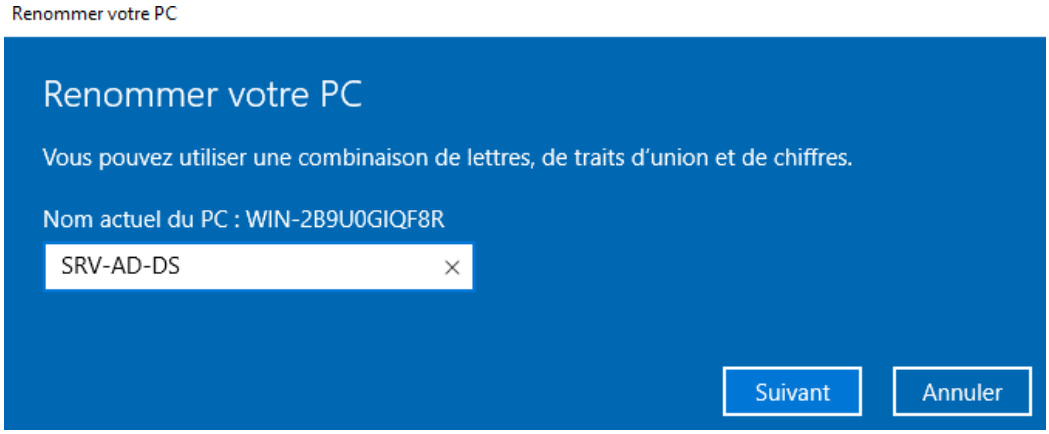
II. Choix d'Active Directory

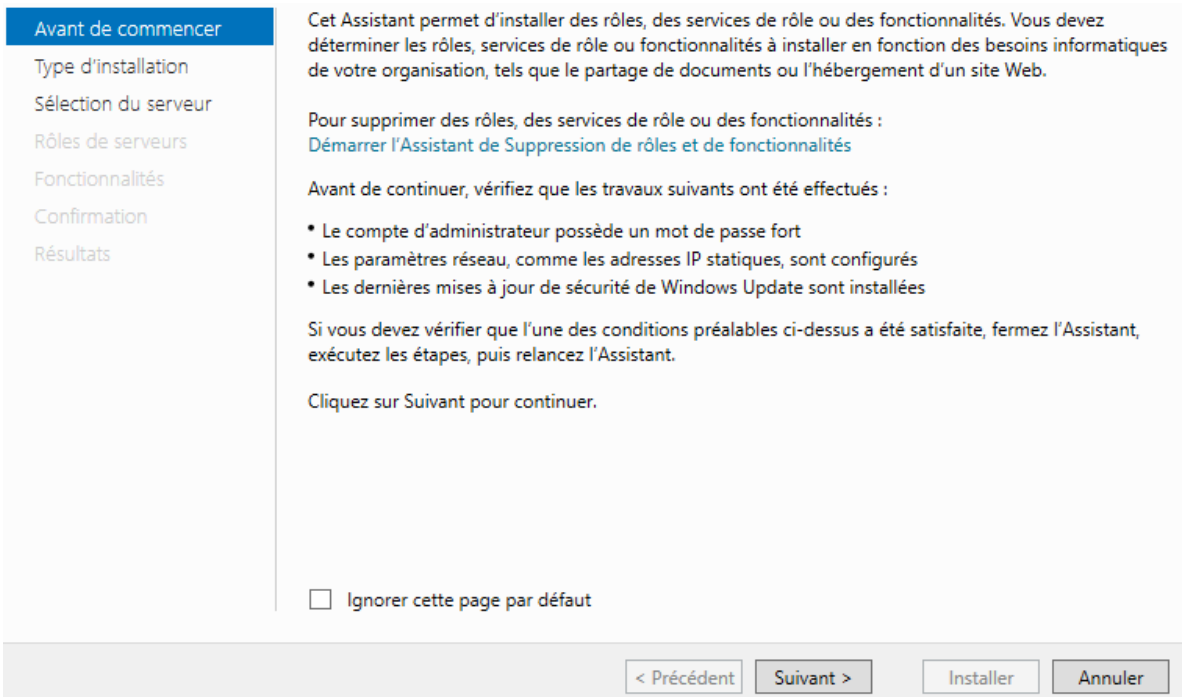
Etape 1. Configuration de l'AD

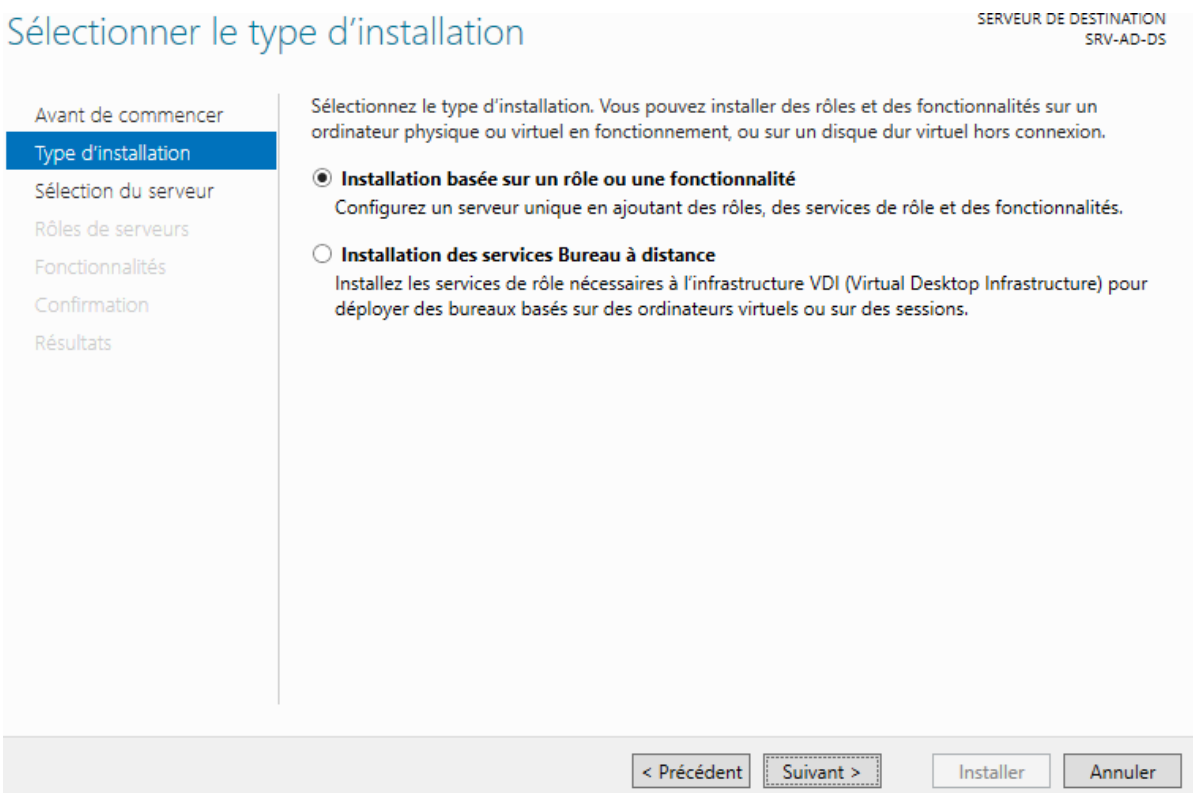
Pour effectuer le déploiement des agents sur les différents postes, nous avons décidé d'utiliser un Active Directory (AD) associé à des stratégies de groupe. Pour ce faire, il est nécessaire d'installer les services Active Directory (AD) et DNS, puis de les configurer correctement :

Quand vous crée un serveur AD, vous devez vous assurer de changer l'adresse IP Fixe du pc pour mettre son propre serveur DNS. Et changer le nom du pc :

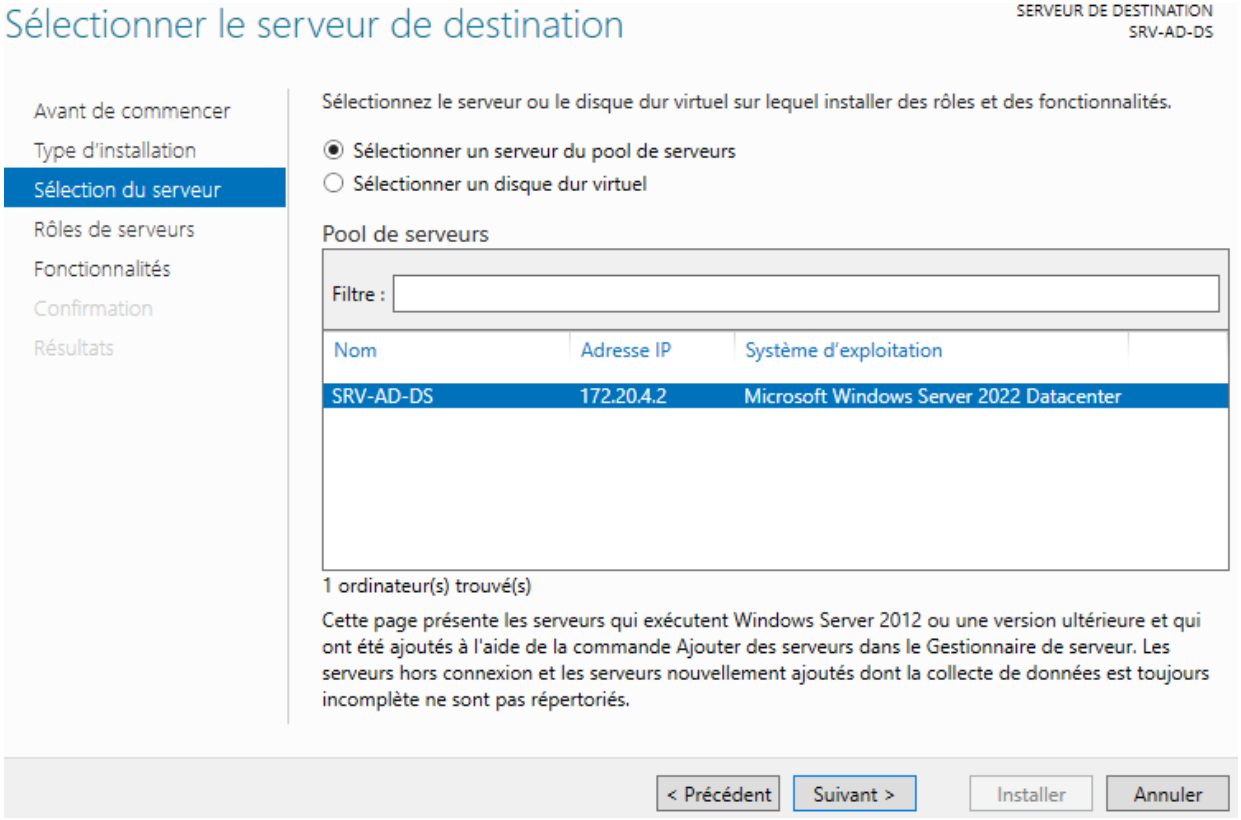




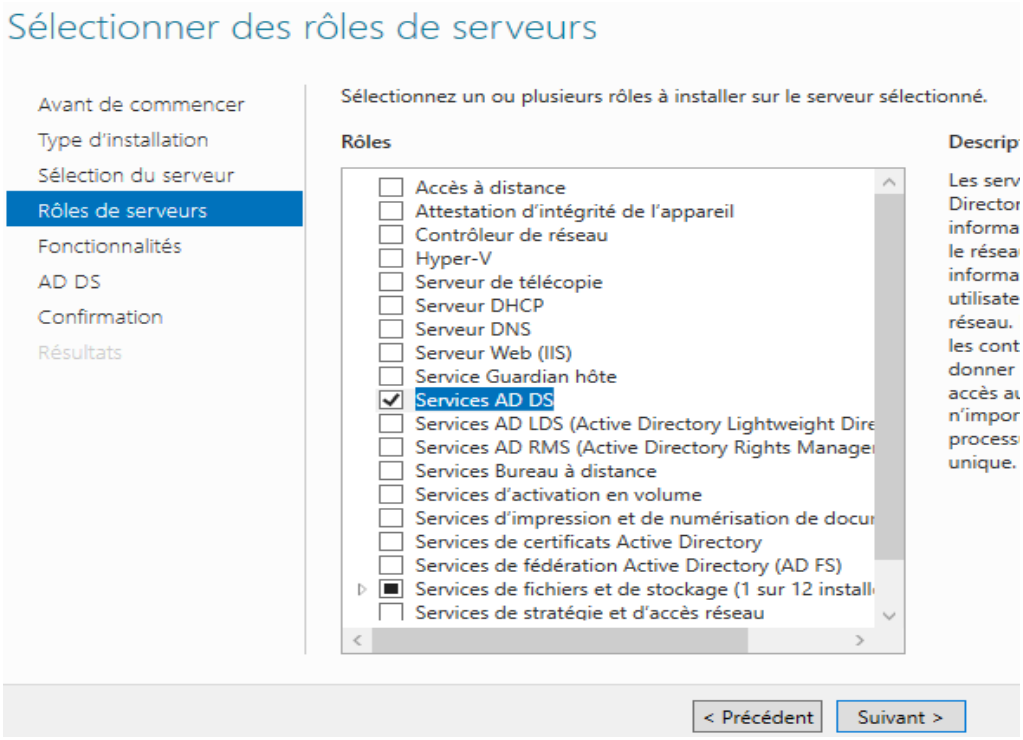

Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Confirmation
Résultats
Cet Assistant permet d'installer des rôles, des services de rôle ou des fonctionnalités. Vous devez déterminer les rôles, services de rôle ou fonctionnalités à installer en fonction des besoins informatiques de votre organisation, tels que le partage de documents ou l'hébergement d'un site Web.
Pour supprimer des rôles, des services de rôle ou des fonctionnalités :
Démarrer l'Assistant de Suppression de rôles et de fonctionnalités
Avant de continuer, vérifiez que les travaux suivants ont été effectués :
• Le compte d'administrateur possède un mot de passe fort
• Les paramètres réseau, comme les adresses IP statiques, sont configurés
• Les dernières mises à jour de sécurité de Windows Update sont installées
Si vous devez vérifier que l'une des conditions préalables ci-dessus a été satisfaite, fermez l'Assistant, exécutez les étapes, puis relancez l'Assistant.
Cliquez sur Suivant pour continuer.
Ignorer cette page par défaut
< Précédent
Suivant >
Installer
Annuler


Sélectionner le type d'installation
SERVEUR DE DESTINATION
SRV-AD-DS
Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Confirmation
Résultats
Sélectionnez le type d'installation. Vous pouvez installer des rôles et des fonctionnalités sur un ordinateur physique ou virtuel en fonctionnement, ou sur un disque dur virtuel hors connexion.
Installation basée sur un rôle ou une fonctionnalité
Configurez un serveur unique en ajoutant des rôles, des services de rôle et des fonctionnalités.
Installation des services Bureau à distance
Installez les services de rôle nécessaires à l'infrastructure VDI (Virtual Desktop Infrastructure) pour déployer des bureaux basés sur des ordinateurs virtuels ou sur des sessions.
< Précédent
Suivant >
Installer
Annuler

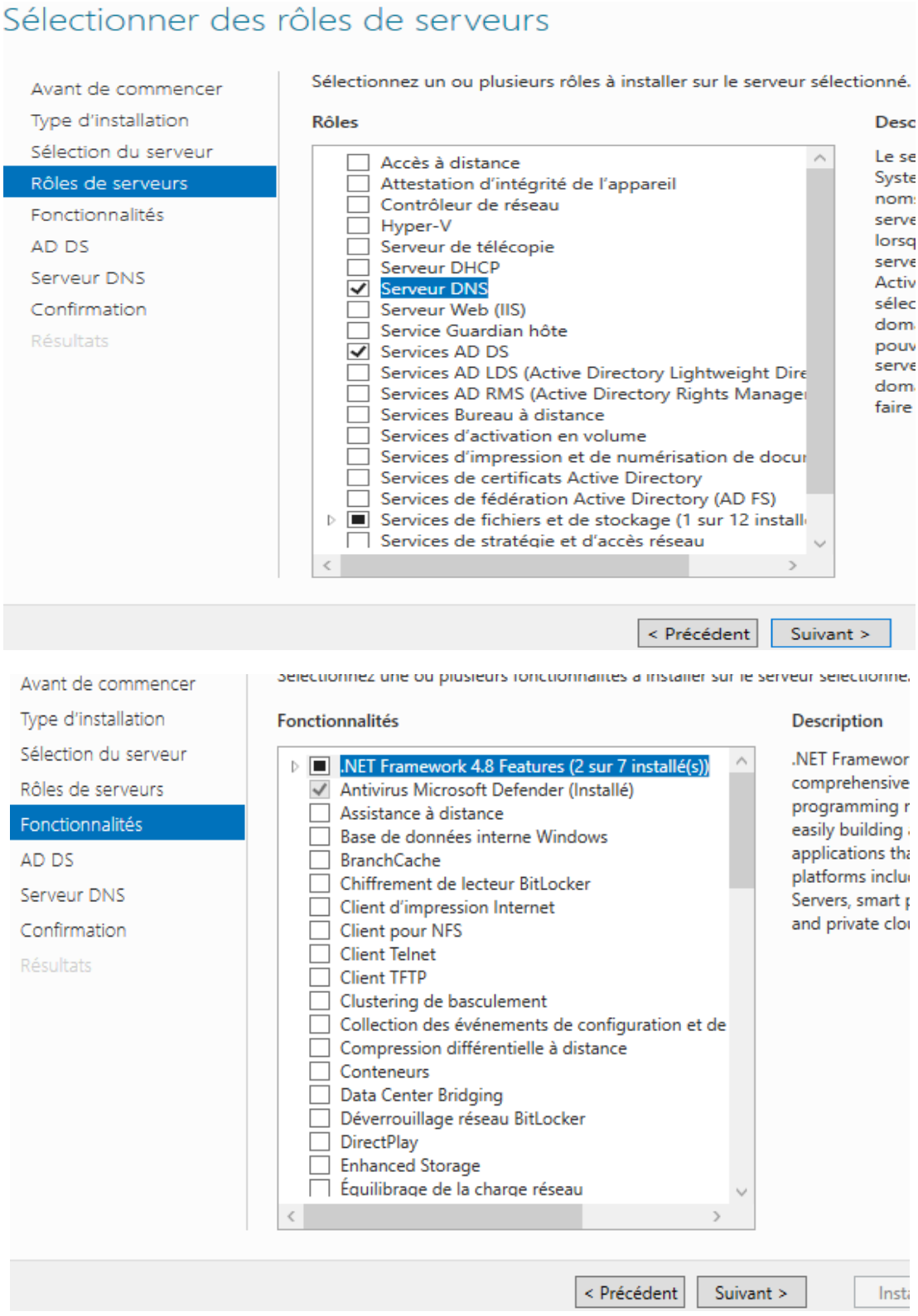
Ensuite, sélectionnez dans le pool, le serveur de destination c'est-à-dire le serveur sur lequel vous souhaitez installer le rôle AD :

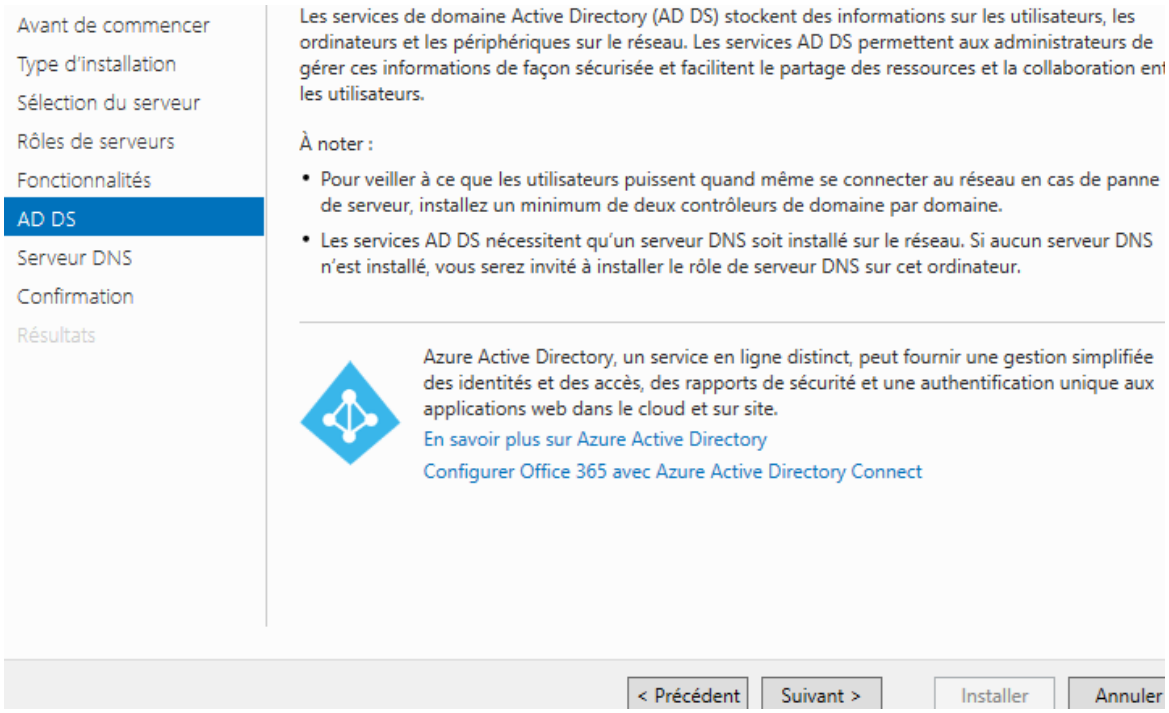


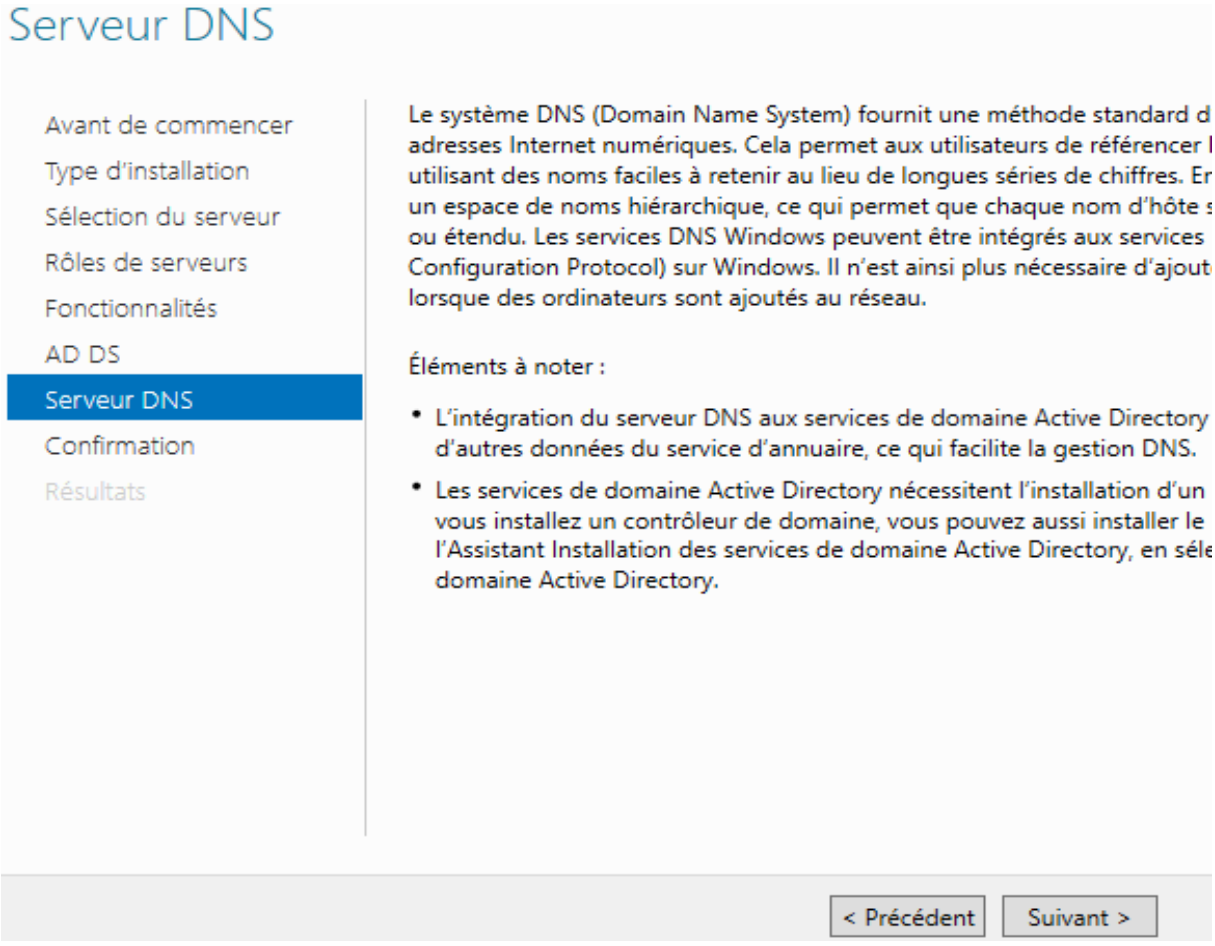
On va maintenant installer le rôle Active Directory sur notre serveur. Dans la liste des rôles, cochez la case correspondant aux « Services AD DS » :



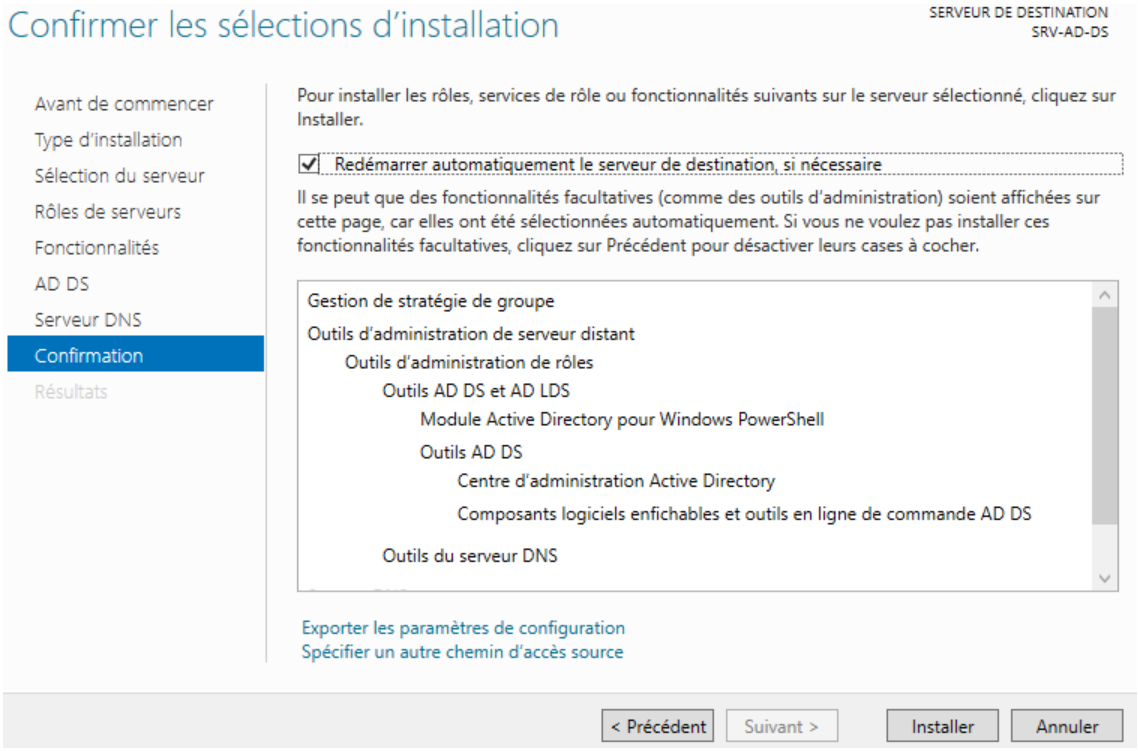
Pour fonctionner, le serveur AD aura également besoin du service DNS qui est le service de résolution des noms de domaine. Dans la liste des rôles, cochez la case correspondant à « Serveur DNS » :




Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
AD DS
Serveur DNS
Confirmation
Résultats
Les services de domaine Active Directory (AD DS) stockent des informations sur les utilisateurs, les ordinateurs et les périphériques sur le réseau. Les services AD DS permettent aux administrateurs de gérer ces informations de façon sécurisée et facilitent le partage des ressources et la collaboration ent les utilisateurs.
À noter :
• Pour veiller à ce que les utilisateurs puissent quand même se connecter au réseau en cas de panne de serveur, installez un minimum de deux contrôleurs de domaine par domaine.
• Les services AD DS nécessitent qu'un serveur DNS soit installé sur le réseau. Si aucun serveur DNS n'est installé, vous serez invité à installer le rôle de serveur DNS sur cet ordinateur.
Azure Active Directory, un service en ligne distinct, peut fournir une gestion simplifiée des identités et des accès, des rapports de sécurité et une authentification unique aux applications web dans le cloud et sur site.
En savoir plus sur Azure Active Directory
Configurer Office 365 avec Azure Active Directory Connect
< Précédent
Suivant >
Installer
Annuler

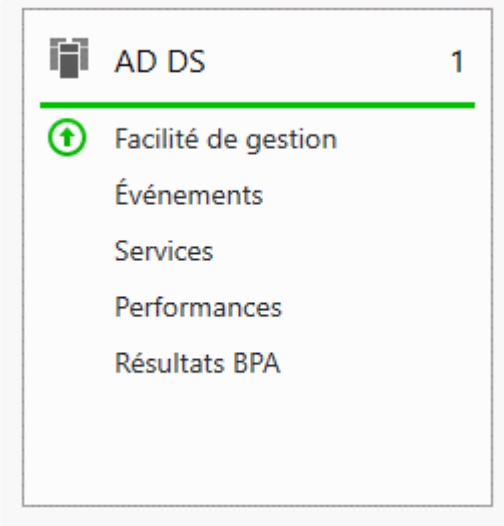

Serveur DNS
Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
AD DS
Serveur DNS
Confirmation
Résultats
Le système DNS (Domain Name System) fournit une méthode standard d
adresses Internet numériques. Cela permet aux utilisateurs de référencer l
utilisant des noms faciles à retenir au lieu de longues séries de chiffres. Er
un espace de noms hiérarchique, ce qui permet que chaque nom d'hôte s
ou étendu. Les services DNS Windows peuvent être intégrés aux services
Configuration Protocol) sur Windows. Il n'est ainsi plus nécessaire d'ajout
lorsque des ordinateurs sont ajoutés au réseau.
Éléments à noter :
• L'intégration du serveur DNS aux services de domaine Active Directory
d'autres données du service d'annuaire, ce qui facilite la gestion DNS.
• Les services de domaine Active Directory nécessitent l'installation d'un
vous installez un contrôleur de domaine, vous pouvez aussi installer le
l'Assistant Installation des services de domaine Active Directory, en séle
domaine Active Directory.
< Précédent
Suivant >

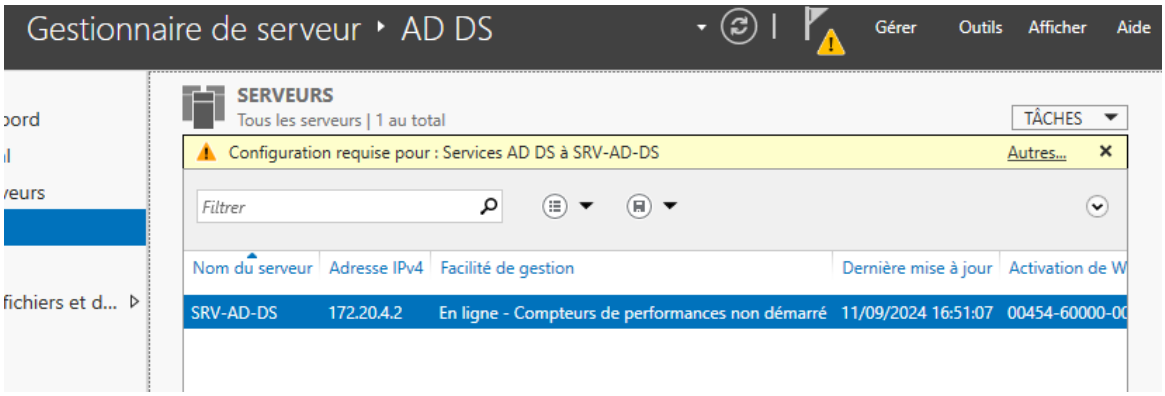
A la fenêtre de confirmation, vérifiez les fonctionnalités qui seront également installées, cochez la case « Redémarrer automatiquement le serveur de destination si nécessaire » et cliquez sur Installer :

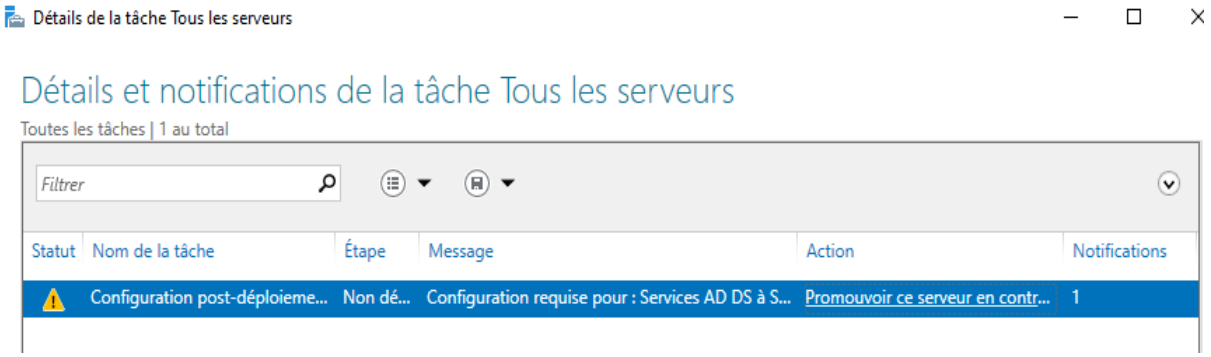


Enfin si l'ordinateur na par redémarrer, redémarrer le !

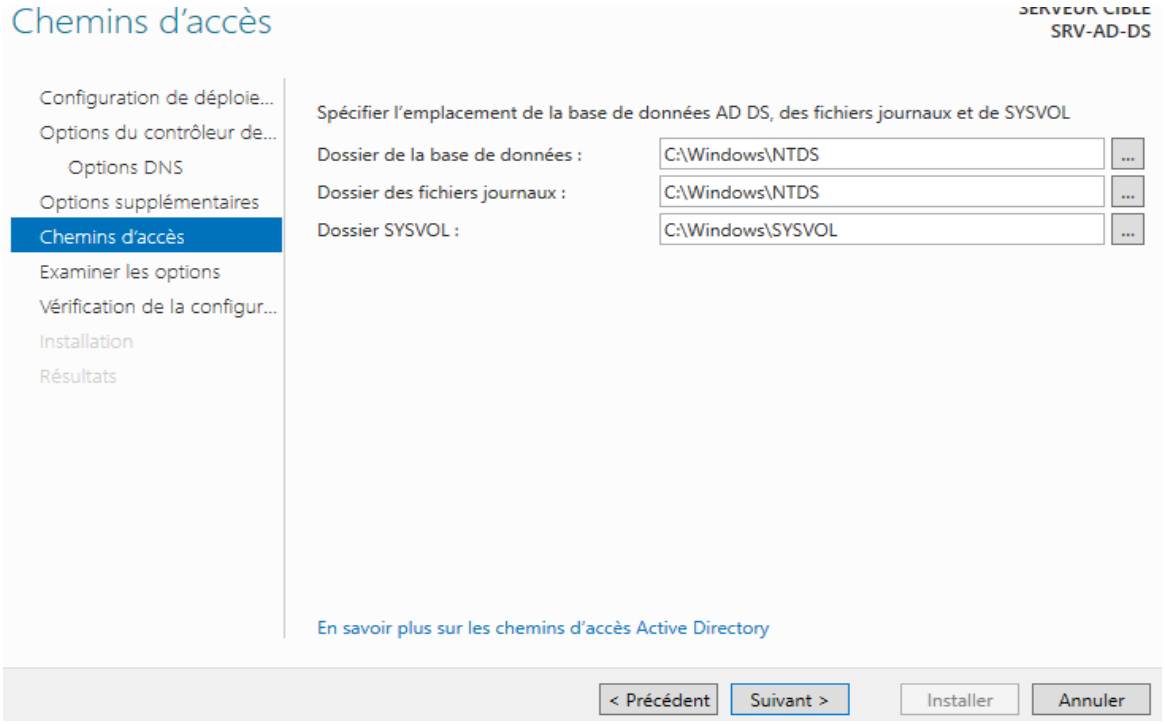
Nous allons créer un nouveau domaine dans une nouvelle forêt. Ce domaine sera le domaine « racine » de l'entreprise :

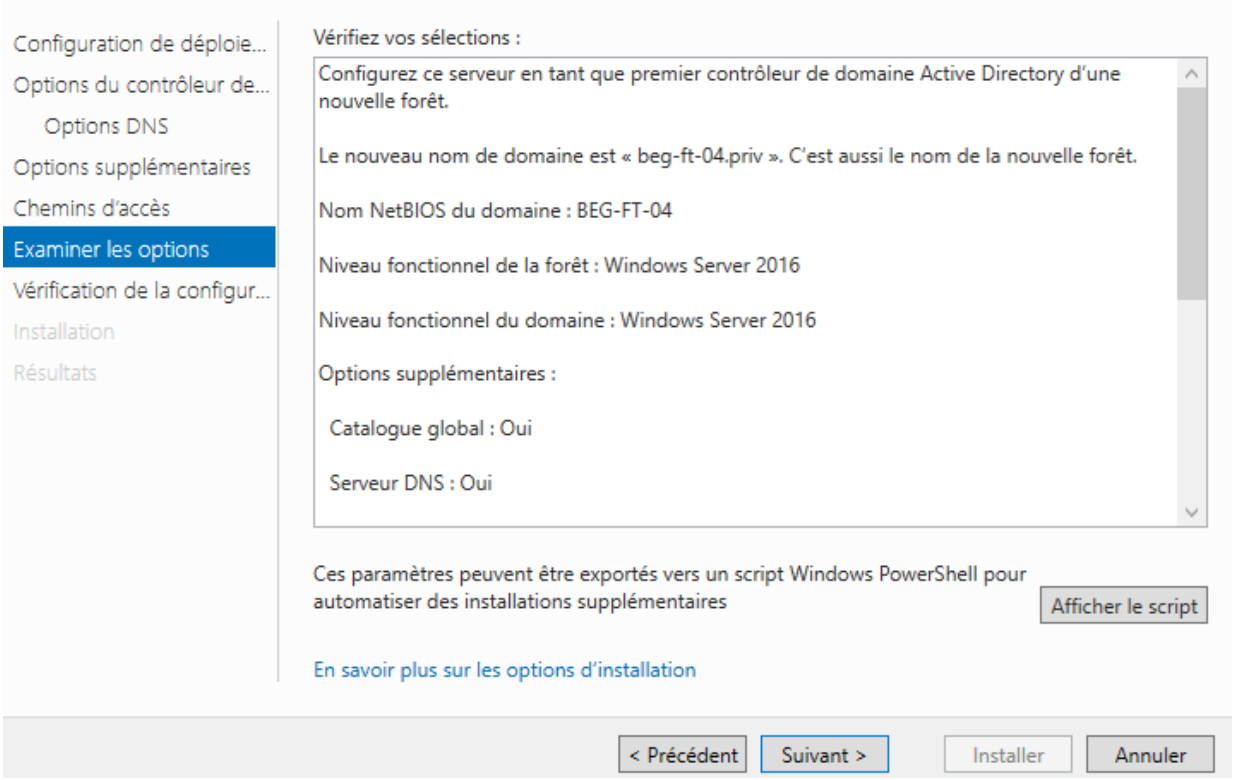


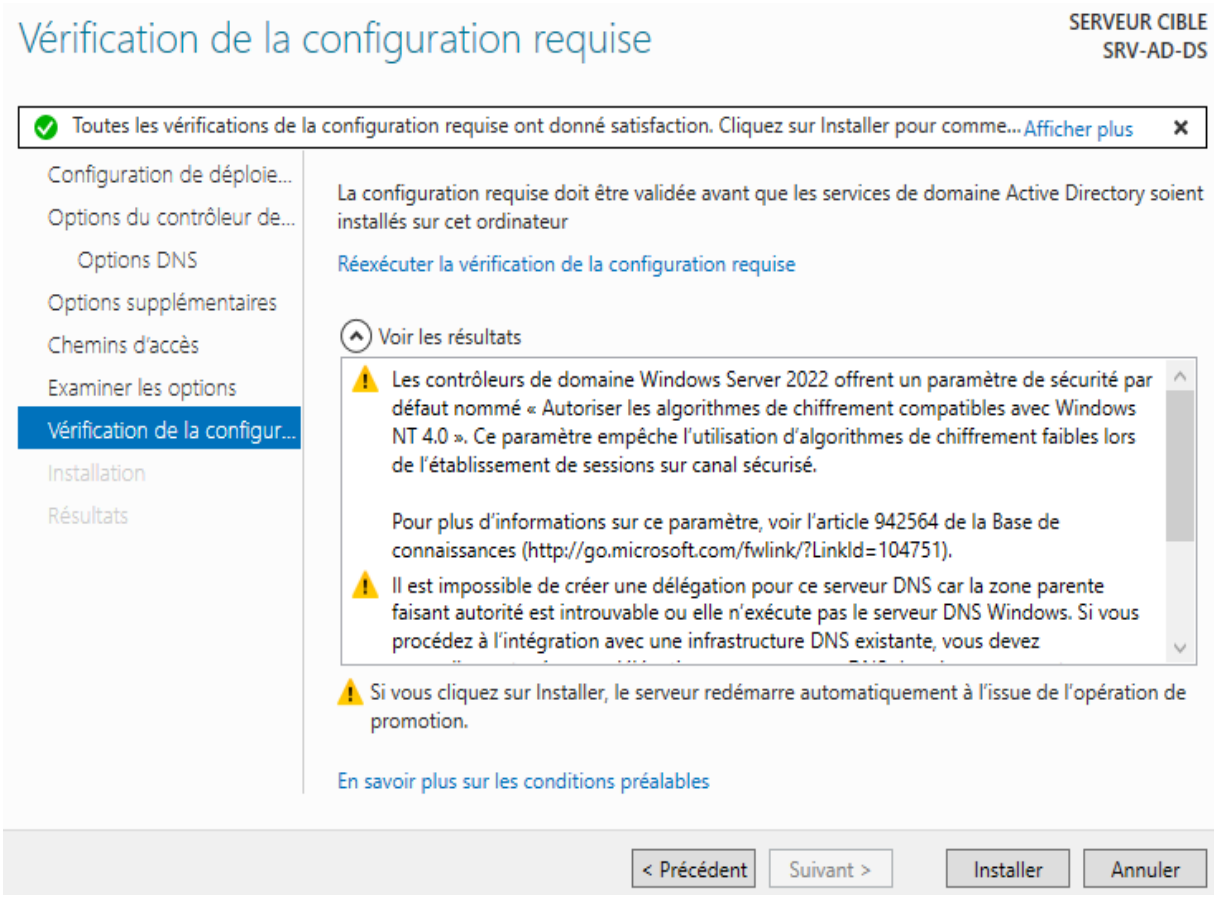




Laissez les chemins d'accès par défaut. Les répertoires définis ici représentent l'emplacement de stockage de la base de données de l'Active Directory, les fichiers de logs et le dossier SYSVOL :

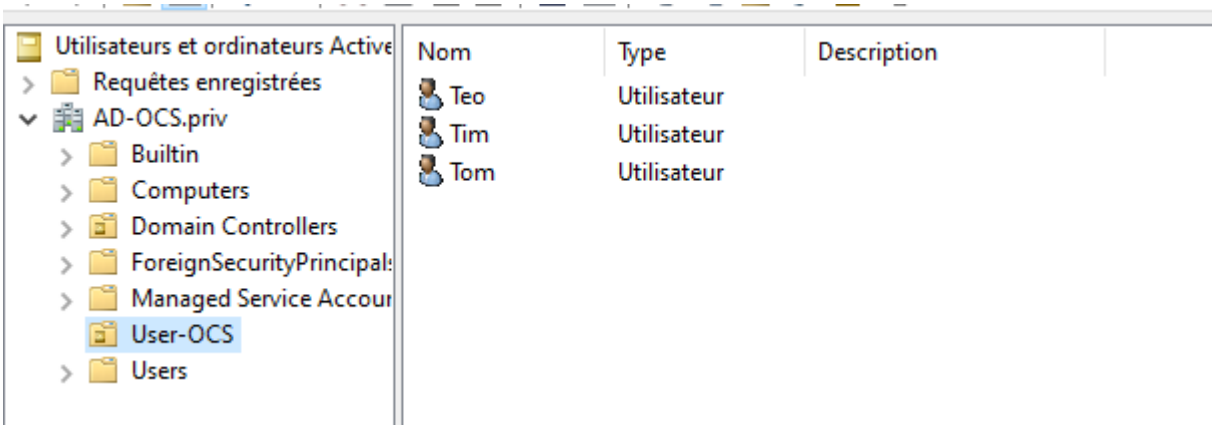




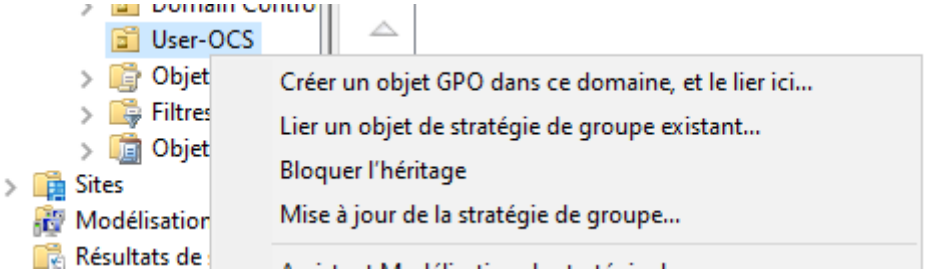

Vérification de la configuration requise
SERVEUR CIBLE
SRV-AD-DS
Toutes les vérifications de la configuration requise ont donné satisfaction. Cliquez sur Installer pour comme... Afficher plus
Configuration de déploie...
Options du contrôleur de...
Options DNS
Options supplémentaires
Chemins d'accès
Examiner les options
Vérification de la configur...
Installation
Résultats
La configuration requise doit être validée avant que les services de domaine Active Directory soient installés sur cet ordinateur
Réexécuter la vérification de la configuration requise
Voir les résultats
Les contrôleurs de domaine Windows Server 2022 offrent un paramètre de sécurité par défaut nommé « Autoriser les algorithmes de chiffrement compatibles avec Windows NT 4.0 ». Ce paramètre empêche l'utilisation d'algorithmes de chiffrement faibles lors de l'établissement de sessions sur canal sécurisé.
Pour plus d'informations sur ce paramètre, voir l'article 942564 de la Base de connaissances (http://go.microsoft.com/fwlink/?LinkId=104751).
Il est impossible de créer une délégation pour ce serveur DNS car la zone parente faisant autorité est introuvable ou elle n'exécute pas le serveur DNS Windows. Si vous procédez à l'intégration avec une infrastructure DNS existante, vous devez
Si vous cliquez sur Installer, le serveur redémarre automatiquement à l'issue de l'opération de promotion.
En savoir plus sur les conditions préalables
< Précédent
Suivant >
Installer
Annuler

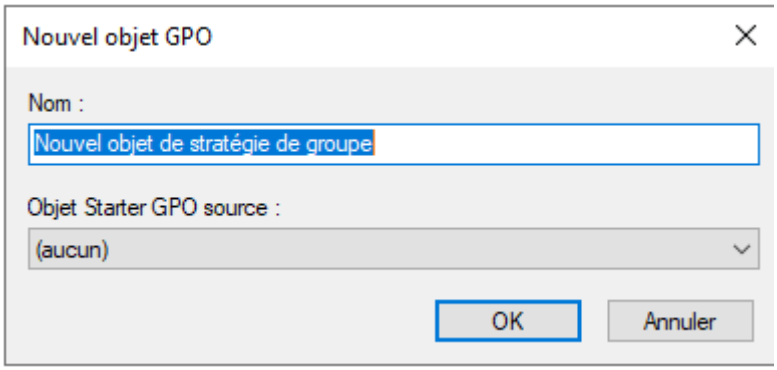
Etape 2. Mise en place des stratégies de groupe

Une fois votre serveur AD est monter vous pouvez crée un groupe pour les utilisateurs de l'AD avec OCS :

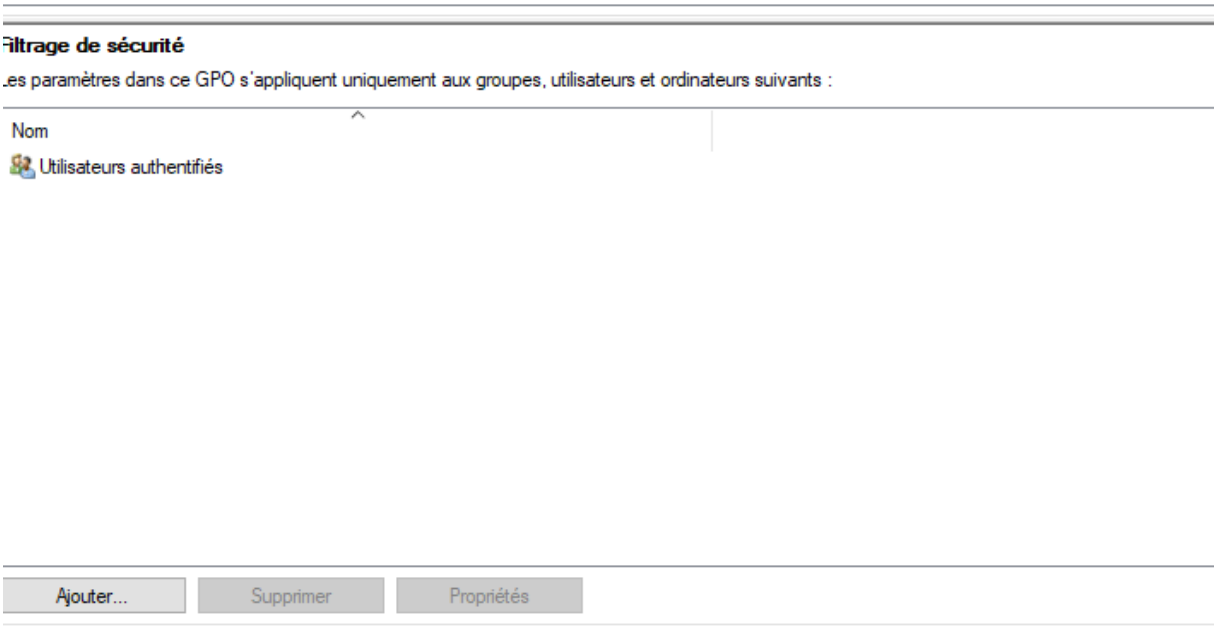


Une fois votre utilisateur créé, vous pouvez accéder à la stratégie de groupe :





Vérifier que les utilisateurs authentifiés sont présents :



Etape 3. Mise en place de Packager (& plugins)

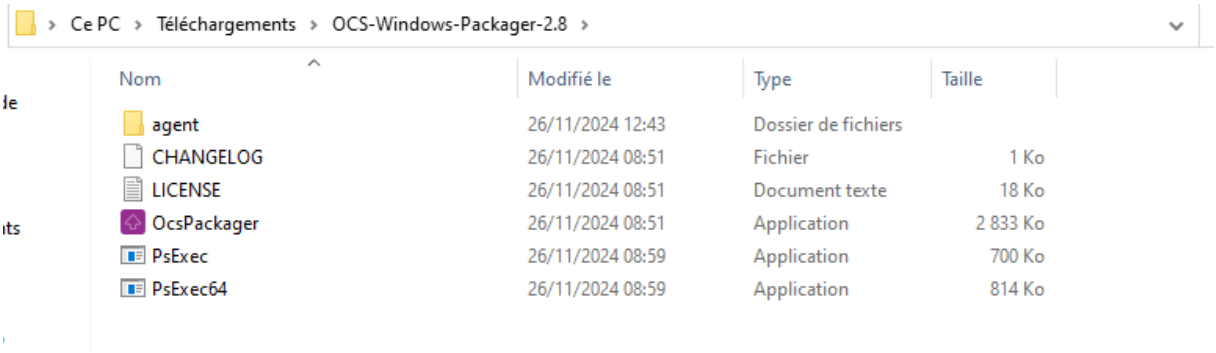
La première étape consiste à se rendre sur le site officiel et de télécharger le « package » complet de déploiement, nommé « OCSNG-Windows-Agent-2.4 » ainsi que « OCSNG-Windows-Packager-2.3 ». Aller sur :

https://ocsinventory-ng.org/?page_id=1235&lang=fr

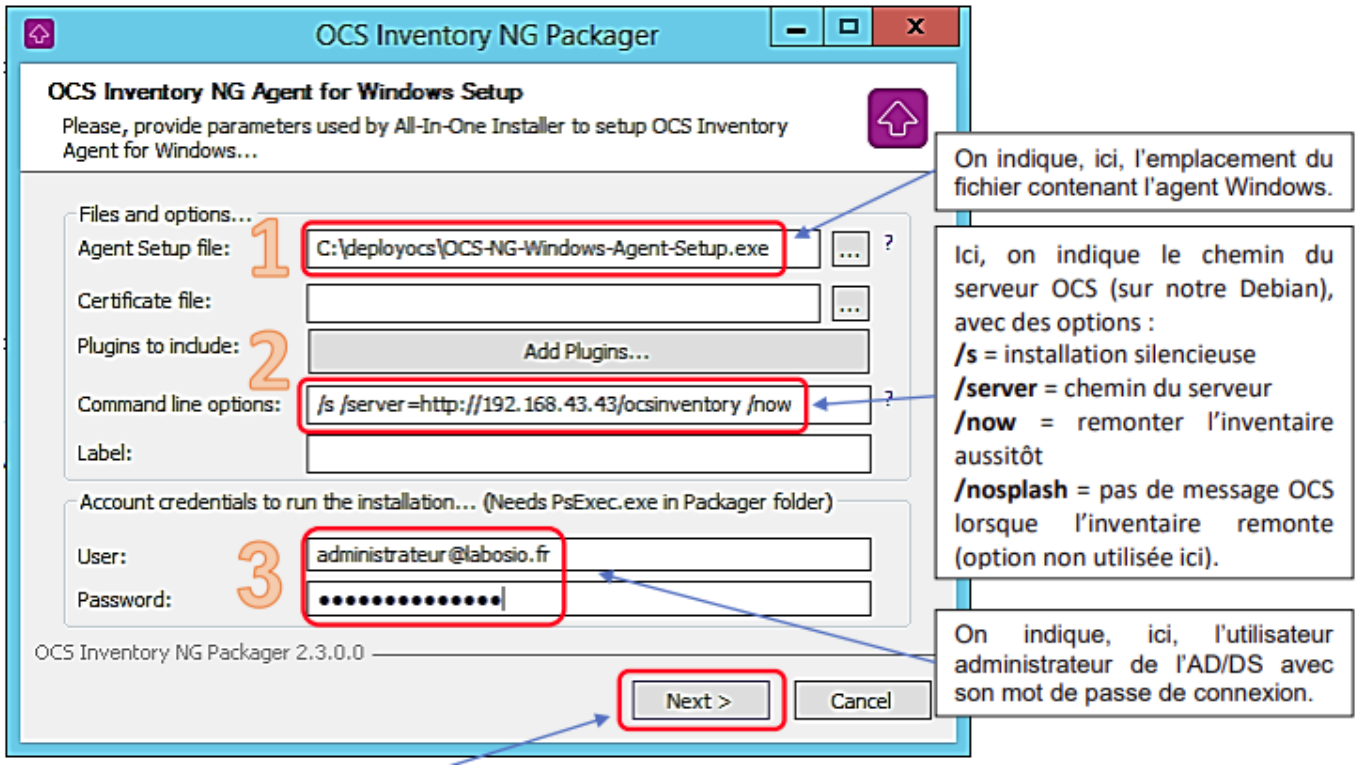
Une fois cela fait téléchargez l'outils « PsExec » :

https://download.sysinternals.com/files/PSTools.zip

Décompressez les deux packagent OCS et copiez également le fichier utilitaire dans votre dossier « ocsdeploy » afin qu'il recense les fichiers suivants :



Double-cliquez le fichier exécutable « OcsPackager » ; une fenêtre de configuration s'ouvre :



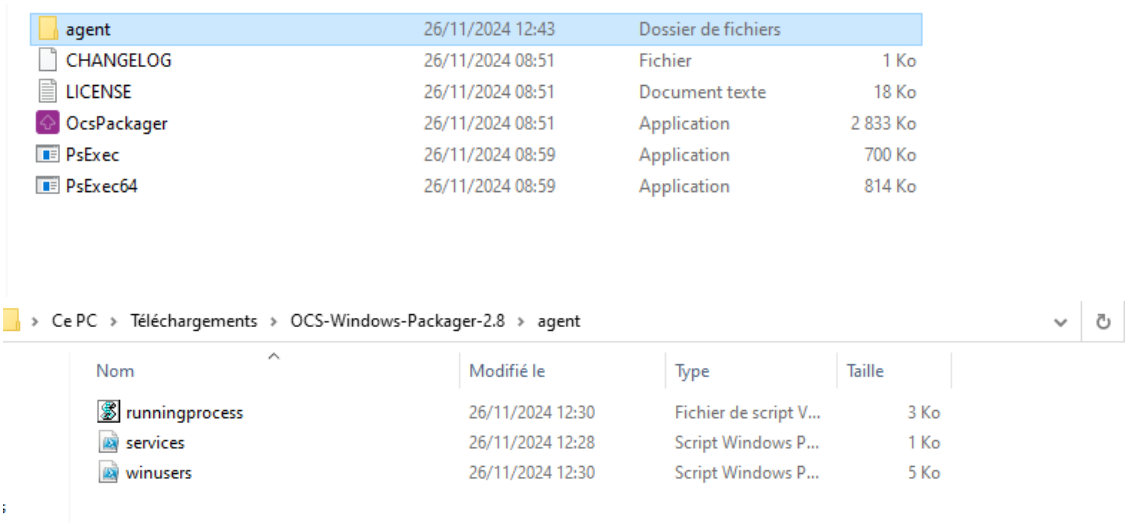
Etape 3.1 Plugins.

Nous allons faire une petite parenthèse dans la documentation pour expliquer comment installer les plugins sur OCS. Pour installer ces **plugins**, il est nécessaire de les packager avec **OCSPackager**.

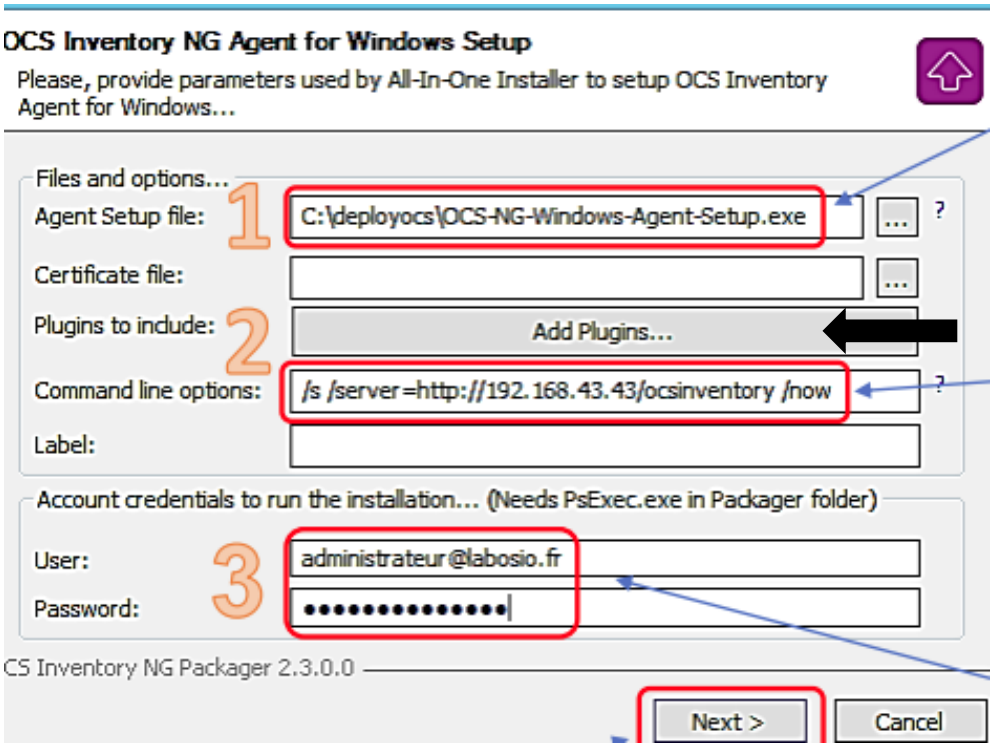
Rendez-vous sur le site officiel d'OCS et téléchargez les plugins que vous souhaitez installer :

https://plugins.ocsinventory-ng.org/

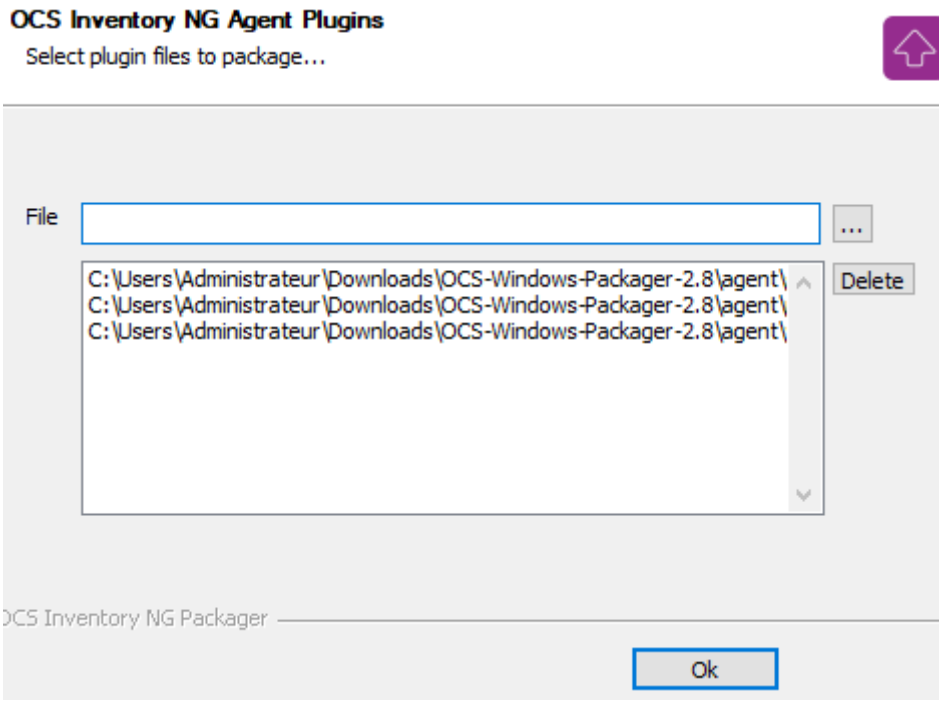
Une fois vos plugins téléchargés, copiez les dossiers contenant les fichiers avec l'extension « .ps1 » dans le répertoire **Agent** du packager :



Cliquez sur le bouton **Add Plugins** :



Ajouter les chemins des agents à ajouter :

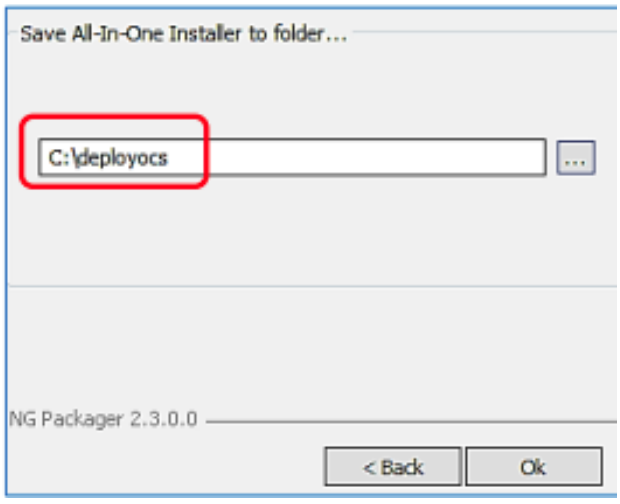


Fin de la parenthèse. Pour ajouter des plugins, vous pouvez continuer à utiliser le packager.

Fin Etape 3.1 Plugins.

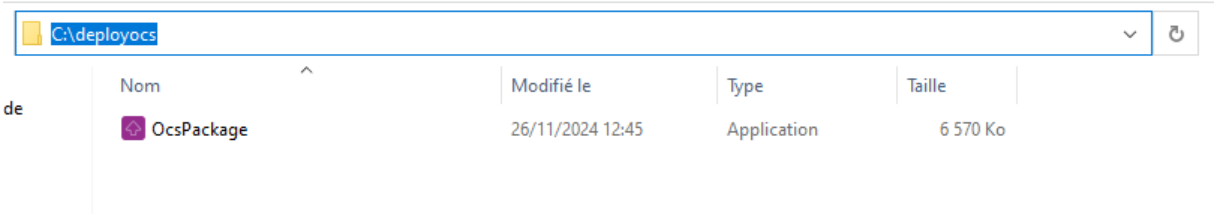
Cliquez le bouton « Next » pour lancer la création du package de déploiement OCS.

Indiquez que le fichier « OCSPACKAGE » doit être généré dans notre dossier « ocsdeploy » et cliquez le bouton « OK » :



OCS Déploiement – Plugin - Package - CVE Search

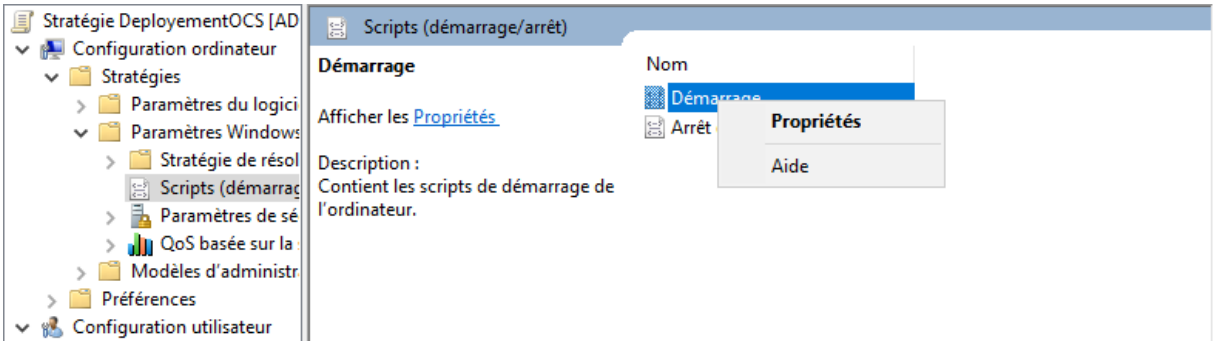
Maintenant, le dossier « ocsdeploy » comporte un nouveau fichier nommé « OcsPackage ». Il s'agit du package automatiser de déploiement que nous utiliserons dans notre stratégie de groupe :



Connecter vous est vérifier que cela apparait :

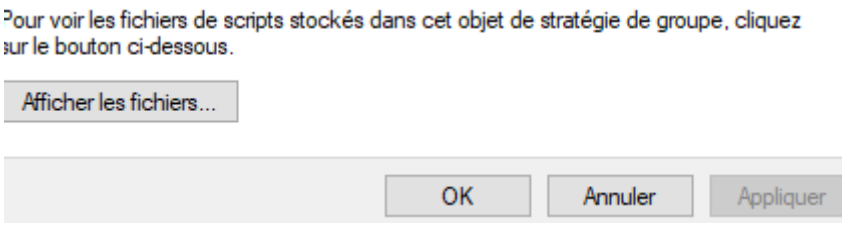
Maintenant vous pouvez retourner dans vos stratégies de groupe et les configurer.

Déployez l'arborescence « Configuration ordinateur » et déployez « Paramètres Windows » :

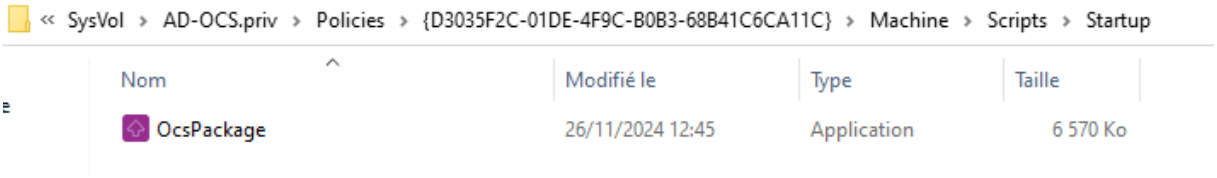


Dans la fenêtre qui s'ouvre, nous allons repérer le dossier dans lequel nous devrons placer nos fichiers issus du dossier « deployocs » afin que le déploiement s'effectue.

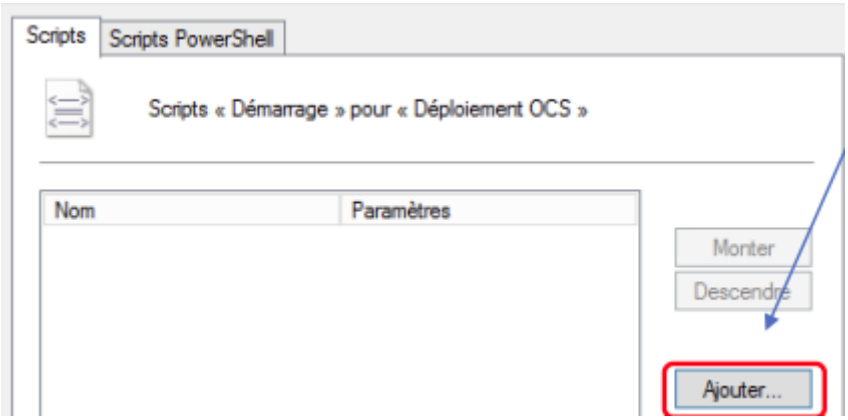
Cliquez sur « Affichez les fichiers… » :



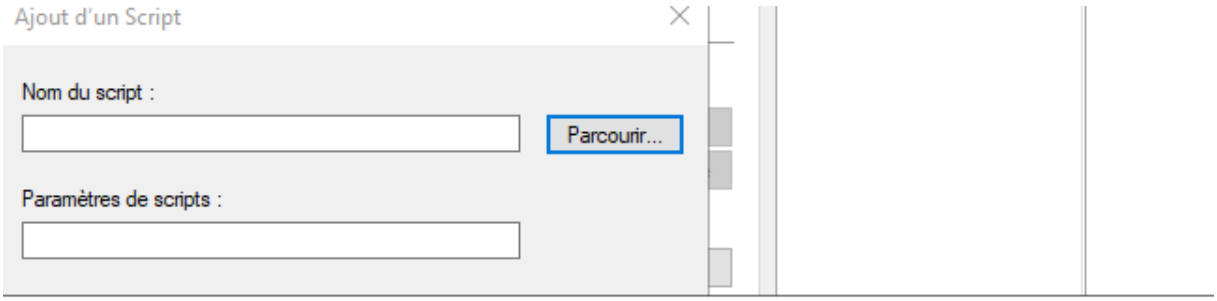
Nous obtenons le chemin exact du dossier dans lequel nous devons copier-coller tous les fichiers de notre dossier « ocsdeploy » ; attention, ne vous trompez pas de dossier sinon la stratégie ne fonctionnera pas !

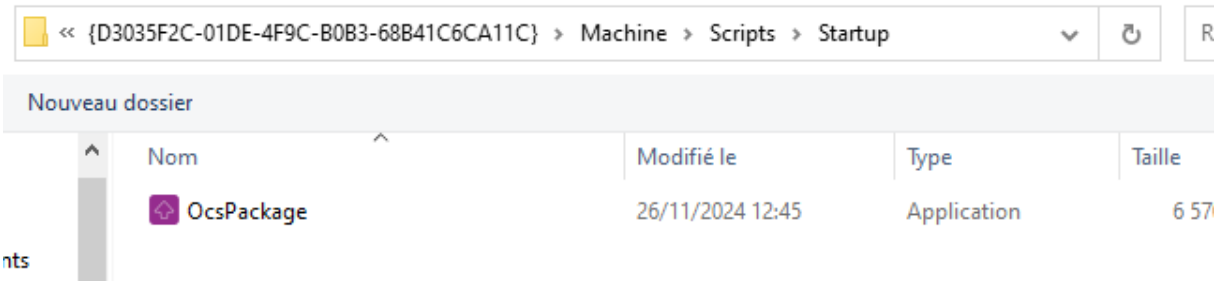


Puis ajouter le sur le bouton « Ajouter » :

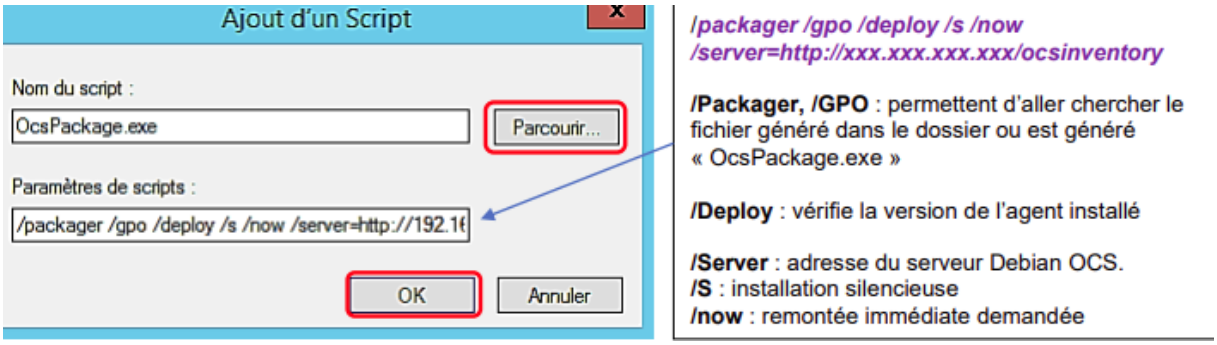


Cliquez le bouton « Parcourir… » et sélectionnez le fichier « OcsPackage.exe » et saisissez les paramètres de scripts ; validez en cliquant le bouton « OK » :

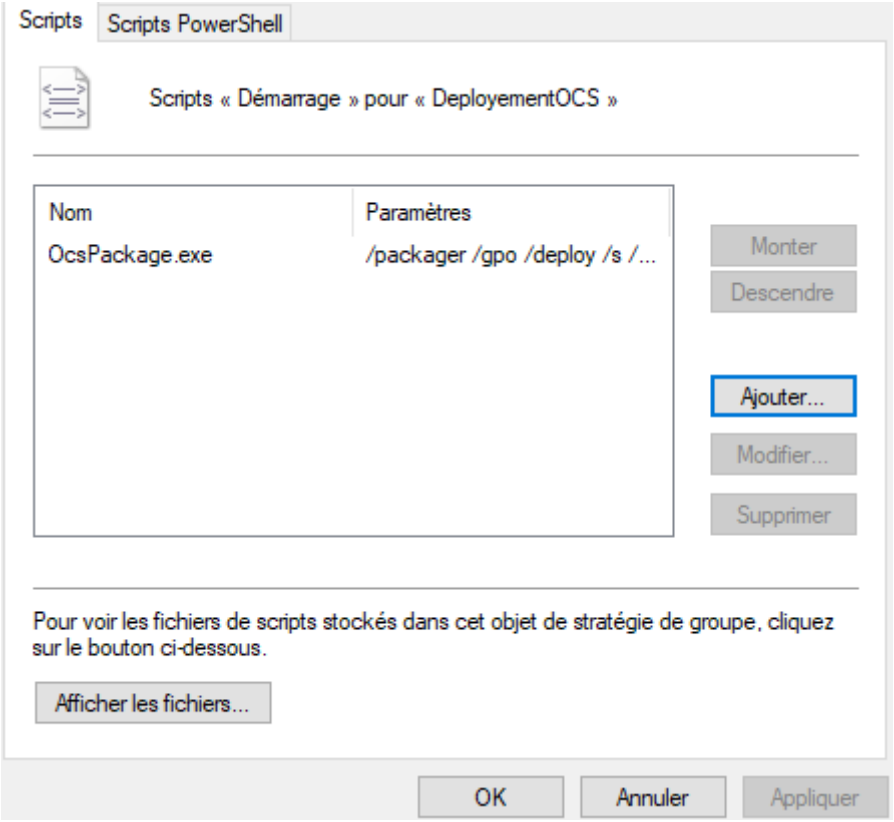




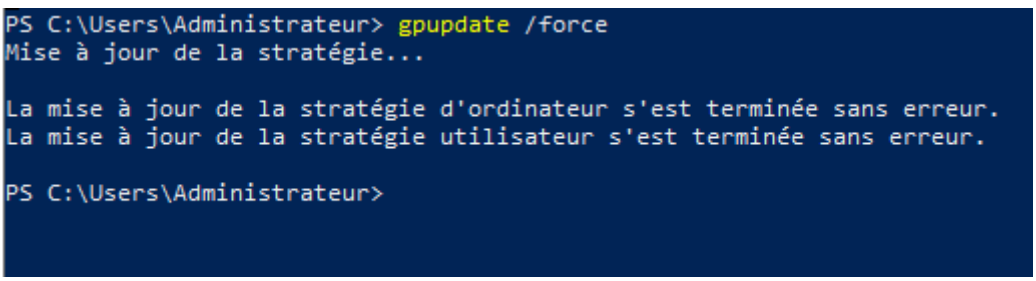
OCS Déploiement – Plugin - Package - CVE Search



La fenêtre de configuration doit s'afficher ainsi ; cliquez « Appliquer » et « Ok » :

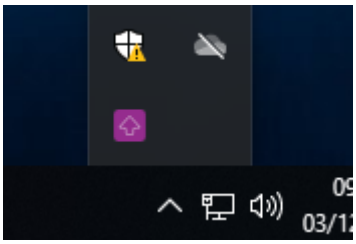


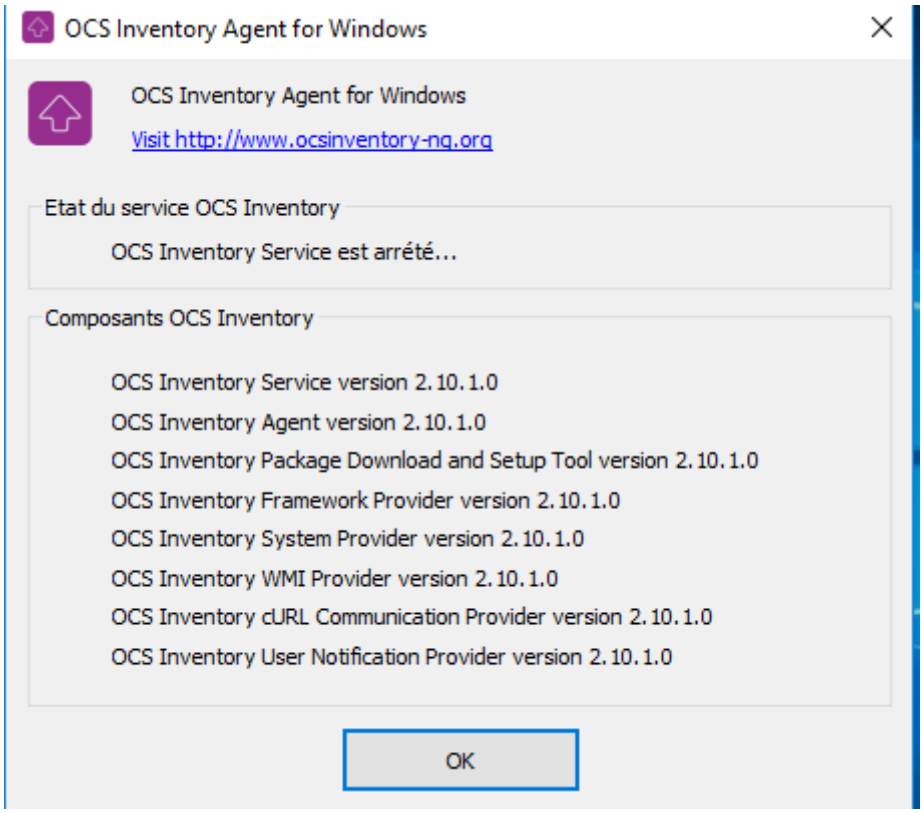
Ouvrez une console et saisissez « gpupdate /force » pour mettre à jour vos stratégies de groupe :



OCS Déploiement – Plugin - Package - CVE Search

Vous pouvez maintenant tester en lançant un poste et vérifier si le déploiement d'OCS fonctionne correctement :





Vous pouvez également vous rendre dans le centre d'administration de votre OCS et vérifier que le PC y est bien remonté :

	Account info : TAG	Dernier inventaire	Machine
☐	NA	2024-11-26 11:41:08	AD-OCS
☐	NA	2024-12-03 09:47:55	CLIENT-OCS
☐	NA	2024-11-26 09:23:01	DESKTOP-7E2MI59

III. Configuration plugins sur OCS-Server

Etape 1. Prérequis pour installer des plugins

Pour utiliser le moteur d'extension, Python3 est nécessaire.

Tout d'abord, vous avez besoin d'un paquetage de Python : scp.

```
apt install python3-scp
```

Installer unzip pour pouvoir extraire le fichier de plugin.

```
apt install unzip
```

Ensuite, placez le fichier zip téléchargé dans le dossier extensions de votre serveur d'administration et décompressez-le. Le dossier extensions du serveur d'administration est par défaut « /usr/share/ocsinventory-reports/ocsreports/extensions ».

```
cd /usr/share/ocsinventory-reports/ocsreports/extensions
```

Vous pouvez supprimer le fichier zip après l'avoir décompressé.

Trouver les plugins que vous voulez sur « https://plugins.ocsinventory-ng.org/ ».

Exemple avec le plugin des services Windows :

```
wget -c https://github.com/PluginsOCSInventory-NG/services/releases/download/2.0/services.zip
```

Extraire le contenu :

```
unzip services.zip
```

Etape 2. Installer le plugin sur le serveur

Note : Il existe aussi la méthode d'installation via le fichier « install_plugin.py » (non utiliser dans notre cas).

Pour installer des plugins sans le script install_plugin.py, connectez-vous à votre serveur de communication (APACHE) et allez dans le répertoire de configuration (par défaut « /etc/ocsinventory-server/ »).

Là, créez un nouveau répertoire dans « perl/Apache/Ocsinventory/Plugins/ » avec le nom du plugin :

mkdir /etc/ocsinventory-server/perl/Apache/Ocsinventory/Plugins/Services

Note : N'oubliez pas de mettre la première lettre en majuscule. Services ici fait références au plugin Services de Windows extrait plus tôt.

Ensuite, placer le fichier Map.pm a l'intérieur.

cp services/APACHE/Map.pm /etc/ocsinventory-server/perl/Apache/Ocsinventory/Plugins/Services

Enfin, placez le fichier de configuration du plugin dans le dossier « plugins/ ».

cp services/APACHE/services.conf /etc/ocsinventory-server/plugins/

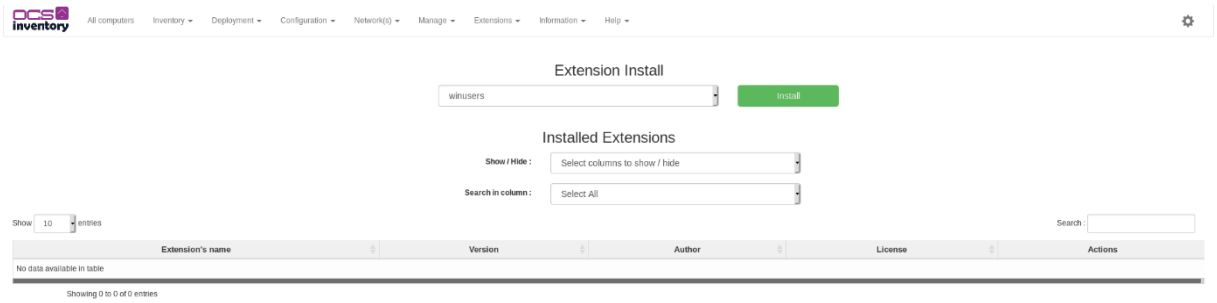
Redémarrez les services apache2.

systemctl restart apache2.service

Etape 3. Activer le plugin

Connectez-vous à votre console d'administration et allez dans l'onglet « Extensions ».

Sélectionnez le plugin et cliquez sur « Installer ».

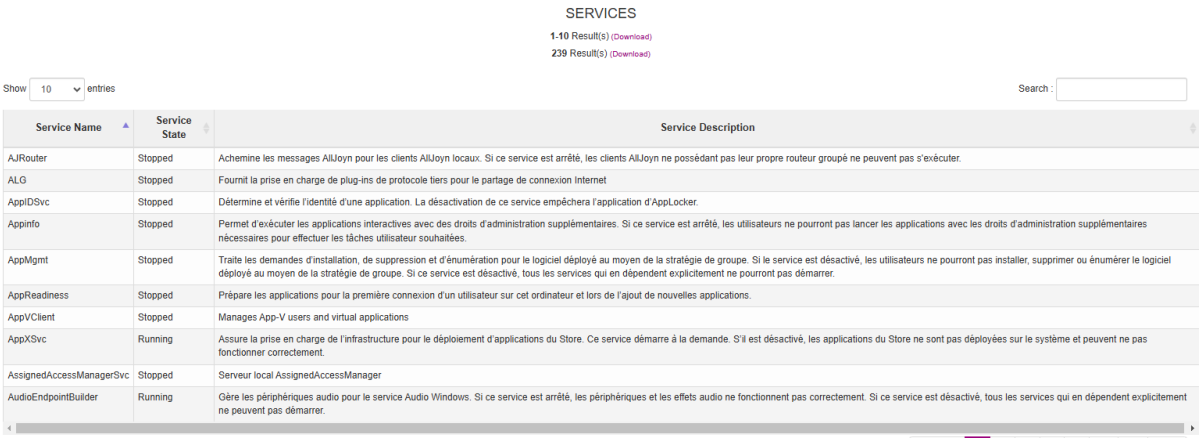


Note : Cela est l'installation et l'activation du plugin pour le serveur OCS, si ce n'est pas déjà fait, se référer à la partie Active Directory pour les plugins côté client.

Etape 4. Exemple de rendu

Les résultats sont fournis dans les détails des machines clientes remonté par OCS.

Plugin Services de Windows :



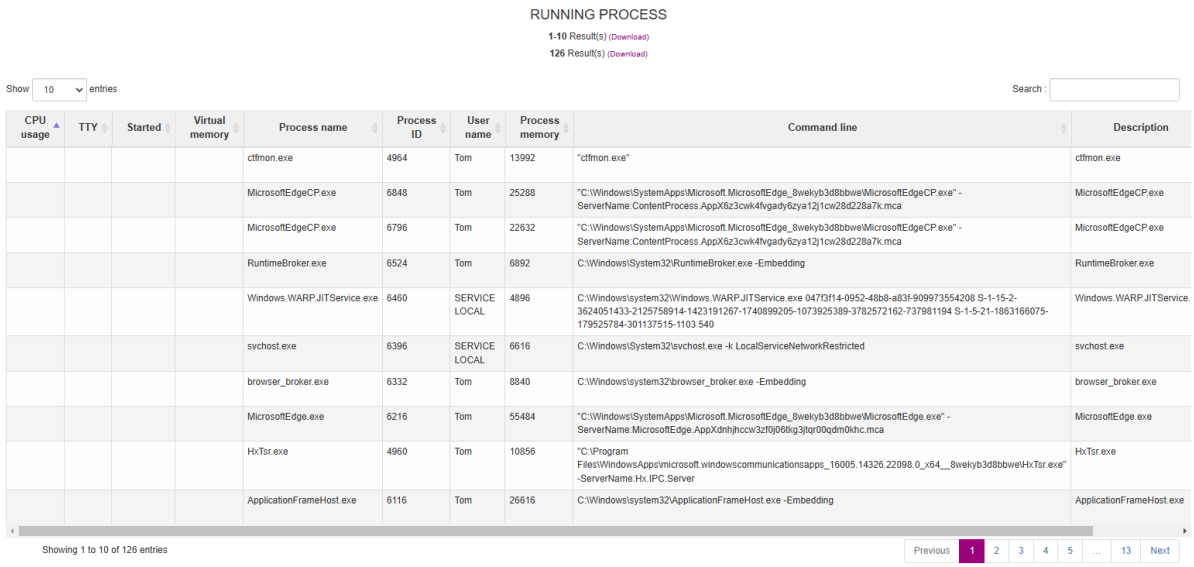
SERVICES

1-10 Result(s) (Download)
239 Result(s) (Download)

Show 10 entries Search :

Service Name	Service State	Service Description
AJRouter	Stopped	Achemine les messages AllJoyn pour les clients AllJoyn locaux. Si ce service est arrêté, les clients AllJoyn ne possédant pas leur propre routeur groupé ne peuvent pas s'exécuter.
ALG	Stopped	Fournit la prise en charge de plug-ins de protocole tiers pour le partage de connexion Internet
AppIDSvc	Stopped	Détermine et vérifie l'identité d'une application. La désactivation de ce service empêchera l'application d'AppLocker.
Appinfo	Stopped	Permet d'exécuter les applications interactives avec des droits d'administration supplémentaires. Si ce service est arrêté, les utilisateurs ne pourront pas lancer les applications avec les droits d'administration supplémentaires nécessaires pour effectuer les tâches utilisateur souhaitées.
AppMgmt	Stopped	Traite les demandes d'installation, de suppression et d'énumération pour le logiciel déployé au moyen de la stratégie de groupe. Si le service est désactivé, les utilisateurs ne pourront pas installer, supprimer ou énumérer le logiciel déployé au moyen de la stratégie de groupe. Si ce service est désactivé, tous les services qui en dépendent explicitement ne pourront pas démarrer.
AppReadiness	Stopped	Prépare les applications pour la première connexion d'un utilisateur sur cet ordinateur et lors de l'ajout de nouvelles applications.
AppVClient	Stopped	Manages App-V users and virtual applications
AppXSvc	Running	Assure la prise en charge de l'infrastructure pour le déploiement d'applications du Store. Ce service démarre à la demande. S'il est désactivé, les applications du Store ne sont pas déployées sur le système et peuvent ne pas fonctionner correctement.
AssignedAccessManagerSvc	Stopped	Serveur local AssignedAccessManager
AudioEndpointBuilder	Running	Gère les périphériques audio pour le service Audio Windows. Si ce service est arrêté, les périphériques et les effets audio ne fonctionnent pas correctement. Si ce service est désactivé, tous les services qui en dépendent explicitement ne peuvent pas démarrer.

Plugin Processus de Windows :



RUNNING PROCESS

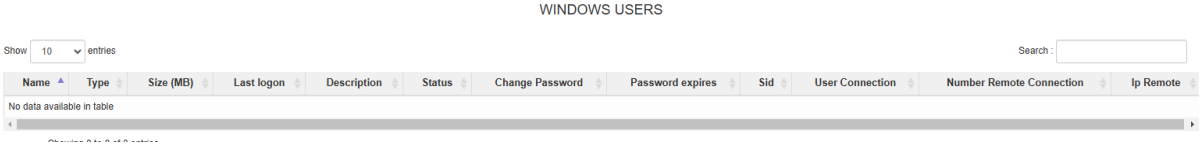
1-10 Result(s) (Download)
126 Result(s) (Download)

Show 10 entries Search :

CPU usage	TTY	Started	Virtual memory	Process name	Process ID	User name	Process memory	Command line	Description
				ctfmon.exe	4964	Tom	13992	"ctfmon.exe"	ctfmon.exe
				MicrosoftEdgeCP.exe	6848	Tom	25288	"C:\Windows\SystemApps\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\MicrosoftEdgeCP.exe" -ServerName:ContentProcess.AppX6z3cwk4fvgady6zya1zj1cw28d228a7k.mca	MicrosoftEdgeCP.exe
				MicrosoftEdgeCP.exe	6796	Tom	22632	"C:\Windows\SystemApps\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\MicrosoftEdgeCP.exe" -ServerName:ContentProcess.AppX6z3cwk4fvgady6zya1zj1cw28d228a7k.mca	MicrosoftEdgeCP.exe
				RuntimeBroker.exe	6524	Tom	6892	C:\Windows\System32\RuntimeBroker.exe -Embedding	RuntimeBroker.exe
				Windows.WARP.JITService.exe	6460	SERVICE LOCAL	4896	C:\Windows\system32\Windows.WARP.JITService.exe 047f3f14-0952-48b8-a83f-909973554208 S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389-3782572162-737981194 S-1-5-21-1863166075-179525784-301137515-1103 540	Windows.WARP.JITService.
				svchost.exe	6396	SERVICE LOCAL	6616	C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted	svchost.exe
				browser_broker.exe	6332	Tom	8840	C:\Windows\system32\browser_broker.exe -Embedding	browser_broker.exe
				MicrosoftEdge.exe	6216	Tom	55484	"C:\Windows\SystemApps\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\MicrosoftEdge.exe" -ServerName:MicrosoftEdge.AppXdnhjhccw3zf0j06tkg3jtqr00qdm0khc.mca	MicrosoftEdge.exe
				HxTsr.exe	4960	Tom	10856	"C:\Program Files\WindowsApps\microsoft.windowscommunicationsapps_16005.14326.22098.0_x64__8wekyb3d8bbwe\HxTsr.exe" -ServerName:Hx.IPC.Server	HxTsr.exe
				ApplicationFrameHost.exe	6116	Tom	26616	C:\Windows\system32\ApplicationFrameHost.exe -Embedding	ApplicationFrameHost.exe

Showing 1 to 10 of 126 entries Previous 1 2 3 4 5 … 13 Next

Plugin Utilisateurs de Windows :



WINDOWS USERS

Show 10 entries Search :

Name	Type	Size (MB)	Last logon	Description	Status	Change Password	Password expires	Sid	User Connection	Number Remote Connection	Ip Remote
No data available in table											

IV. Découverte réseau OCS

Etape 1. Configuration de la découverte réseau.

Accédez à la console d'administration d'OCS Inventory.

Allez dans le menu « Configuration », puis « Configuration générale ».

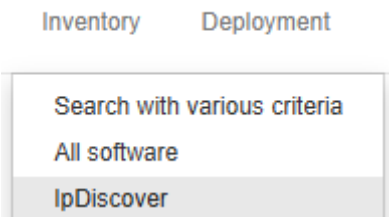
Activez la fonctionnalité « IP Discovery » et configurez les paramètres selon vos besoins.

Titre	Description
IPDISCOVER	Nombre maximum d'ordinateurs par passerelle récupérant une adresse IP sur le réseau.
IPDISCOVER_BETTER_THRESHOLD	Spécifie la différence minimale pour remplacer un agent ipdiscover.
IPDISCOVER_LATENCY	Latence ipdiscover (doit être supérieure ou égale à 10 millisecondes).
IPDISCOVER_MAX_ALIVE	Nombre maximum de jours avant qu'un ordinateur ipdiscover soit remplacé.
IPDISCOVER_NO_POSTPONE	Désactive le temps avant une première détection (non recommandé).
IPDISCOVER_USE_GROUPS	Active les groupes pour ipdiscover (par exemple, pour limiter les agents ipdiscover à certains groupes).
IPDISCOVER_LINK_TAG_NETWORK	Lien entre le réseau ipdiscover et l'étiquette des ordinateurs (nécessite une reconnexion après modification).
IPDISCOVER_UPDATE_DATE	Met à jour la date lorsque les périphériques sont mis à jour.
IPDISCOVER_PURGE_OLD	Permet de purger les anciennes données ipdiscover.
IPDISCOVER_PURGE_VALIDITY_TIME	Durée de validité (en jours) des données ipdiscover (doit être supérieure ou égale à 1).

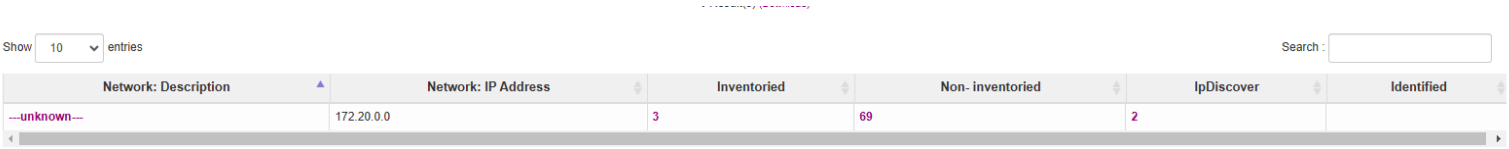
Etape 2. Visualisation de la découverte réseau

Accédez à la console d'administration d'OCS Inventory.

Allez dans le menu « Inventory », puis « IP Discover ».



Vous pouvez maintenant visualisée :



Network: Description : Une colonne affichant la description du réseau.

Network: IP Address : Montre l'adresse IP du réseau, dans ce cas "172.20.0.0".

Inventoried : Indique le nombre d'équipements inventoriés, ici "3".

Non-inventoried : Montre les équipements non inventoriés, ici "69".

IpDiscover : Montre les adresses IP découvertes, ici "2".

Identified : Cette colonne est vide, indiquant peut-être aucun élément identifié ou non applicable.

V. Déploiement de package via OCS

Etape 1. Configuration côté serveur

Configurer correctement le déploiement sur le serveur n'est pas vraiment compliqué, vous devrez garder deux choses à l'esprit : Par défaut, le déploiement n'est pas activé, SSL / HTTPS est obligatoire, OCS n'envoie pas le paquet de déploiement si le serveur n'est pas configuré avec HTTPS.

Pour comprendre : Le serveur de déploiement qui stocke les fichiers d'information doit activer le protocole SSL, car le téléchargement du fichier d'information sur le déploiement est très critique. Ce fichier d'information contient la description du paquet et la commande à lancer. Ainsi, si quelqu'un peut usurper votre serveur de déploiement, il peut lancer n'importe quelle commande sur vos ordinateurs. C'est pourquoi le serveur de déploiement doit utiliser le protocole SSL pour permettre aux agents d'authentifier le serveur et de s'assurer qu'il s'agit bien du véritable serveur de déploiement.

L'agent doit disposer d'un certificat pour valider l'authentification du serveur de déploiement. Ce certificat doit être stocké dans un fichier nommé cacert.pem dans le dossier de l'agent OCS Inventory NG sous Windows, et dans le répertoire /etc/ocsinventory-client sous Linux.

Si vous disposez d'une infrastructure à clé publique, vous devez créer un certificat de serveur valide pour votre serveur de déploiement et copier votre fichier de certificat d'autorité dans le fichier cacert.pem.

Si vous ne disposez pas d'une infrastructure à clé publique, vous pouvez utiliser un certificat auto-signé pour votre serveur de déploiement et copier le certificat du serveur dans le fichier cacert.pem.

Pour utiliser un certificat auto-signé : https://wiki.ocsinventory-ng.org/05.Deployment/Deploying-packages-or-executing-commands-on-client-hosts/#using-ssl-certificates-in-package-deployment

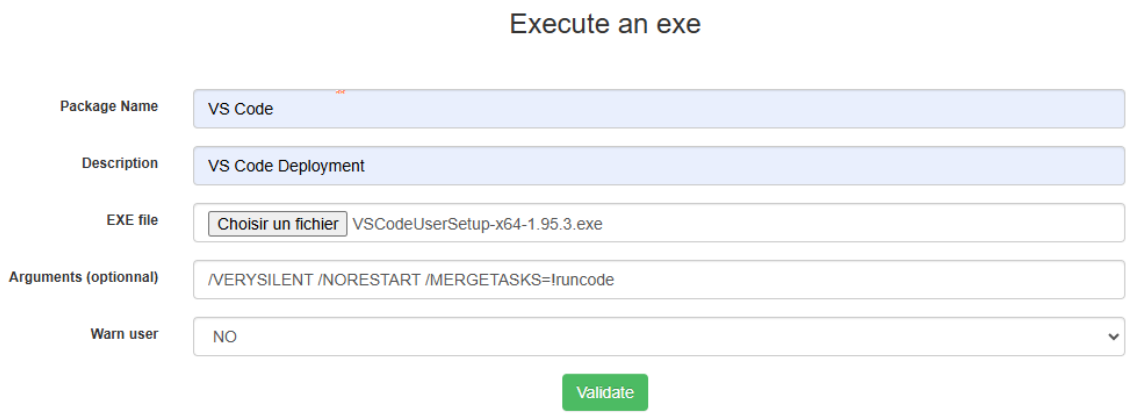
Bien, dans notre cas je n'ai pas pris le temps de configurer le serveur OCS avec SSL / HTTPS, mais nous allons tout de même passer à la configuration.

Pour activer la fonction de déploiement de l'inventaire d'OCS, accédez à la console d'administration d'OCS Inventory et naviguez vers le menu Configuration -> Configuration générale.

Sur la gauche de la page, cliquez sur l'onglet Déploiement et réglez les paramètres de téléchargement sur ON. *N'oubliez pas de cliquer sur le bouton de mise à jour en bas de la page, sinon vos paramètres ne seront pas sauvegardés.*

Etape 2. Déployer un logiciel exe.

Pour déployer un logiciel/package en .exe, aller sur « Deployment > Build > Windows > Install / Uninstall » et cliquer sur « Execute an exe ».



Argument d'installation pour Visual Studio Code : /VERYSILENT /NORESTART /MERGETASKS=!runcode

Paramètres configurables par l'utilisateur :

Titre	Description
Package Name	Nom affiché du package.
Description	Description du package.
EXE file	Fichier exécutable.
Arguments	Arguments en ligne de commande (optionnel).
Warn user	Avertir l'utilisateur avant le déploiement (Non par défaut).
Text	Message d'avertissement (Non visible si "Warn user" est défini sur Non).
Countdown	Compte à rebours pour le message d'avertissement (Non visible si "Warn user" est défini sur Non).

Paramètres par défaut (non configurables par l'utilisateur) :

Titre	Description
Priority	Priorité : 5.
Action	Action : Lancement.
Protocol	Protocole : HTTP.
Command	Commande : `executable.exe {custom arguments}`.
Notify can abort	Notification : Annulation non permise (Non).
Notify can delay	Notification : Délai non permis (Non).
Need done action	Action requise : Non.

OCS Déploiement – Plugin - Package - CVE Search

Souvent les logiciels à déployer sont volumineux, il se peut que vous rencontreriez ce message d'erreur « CSRF ATTACK ».

Ce problème vient du fait que les valeurs d'envoie via le formulaire et php sont limité en taille.

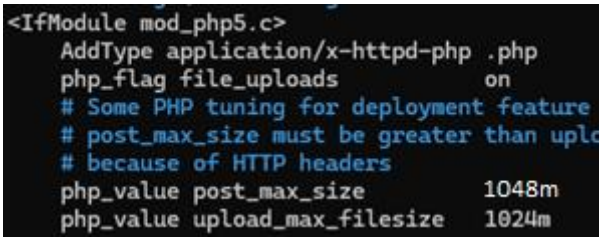
Editer le fichier de configuration apache d'ocs-inventory :

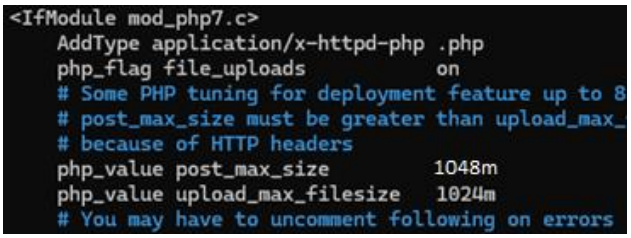
nano /etc/apache2/conf-enabled/ocsinventory-reports.conf

Augmenter la valeur du champ upload & post :

post_max_size à 1048M

upload_max_filesize 1024M

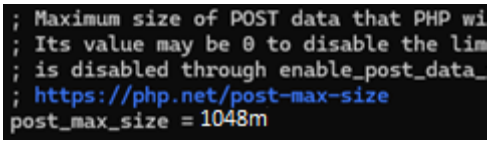




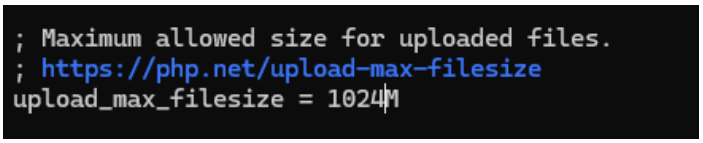
Note : « post_max_size » doit toujours être équivalent ou supérieur à « upload_max_filesize ».

Faire de même pour le fichier de configuration « php.ini » :

nano /etc/php/8.3/apache2/php.ini



Note : Ligne 713



Note : Ligne 865

Redémarrer les services apache2 :

systemctl restart apache2

Pour finir ajouter le logiciel/package sur un client Windows :

Select the client > Deployment > Add package > No > Select the package VS Code.

Si comme moi vous êtes en HTTP, il ce peut que le déploiement soit bloqué en « Awaiting deployment », comme dit précédemment il faut que le serveur OCS soit configuré en HTTPS.

Package Name	Timestamp	Server	Active status	Deployment date
VS Code	1733216243	172.20.133.11/download	WAITING NOTIFICATION	Awaiting deployment

VI. Installation du serveur CVE-Search

I. Installation de CVE-Search

Etape 1. Installation des dépendances principales

Installer le paquet git :

```
apt install git -y
```

Cloner le projet CVE-Search :

```
git clone https://github.com/cve-search/cve-search.git
```

Installer les paquets nécessaires pour le fonctionnement du projet CVE-Search :

```
xargs apt-get install -y < cve-search/requirements.system
```

Installer le paquet python3 environnement :

```
apt install python3-venv -y
```

Etape 2. Création d'un environnement virtuel Python

Création d'un environnement virtuel Python sous « /pythonENV/ » :

```
python3 -m venv /pythonENV/
```

Installer CVE-Search et ses dépendances Python :

```
/pythonENV/bin/pip3 install -r cve-search/requirements.txt
```

Etape 3. Installation de MongoDB

Installer gnupg et curl :

```
apt install gnupg curl
```

Ces paquets sont requis pour importer la clé publique du dépôt MongoDB et configurer les sources APT.

Telecharger la clé publique (dépôt MongoDB), la convertir au format gpg et la placer dans « /usr/share/keyrings » :

```
curl -fsSL https://www.mongodb.org/static/pgp/server-8.0.asc | gpg -o /usr/share/keyrings/mongodb-server-8.0.gpg --dearmor
```

Ajouter le dépôt MongoDB à APT :

```
echo "deb [ arch=amd64,arm64 signed-by=/usr/share/keyrings/mongodb-server-8.0.gpg ] https://repo.mongodb.org/apt/debian bookworm/mongodb-org/8.0 main" | tee /etc/apt/sources.list.d/mongodb-org-8.0.list > /dev/null
```

Cela créez un fichier de liste dans « /etc/apt/sources.list.d/ » pour spécifier l'URL du dépôt MongoDB. Le fichier inclut l'architecture (amd64, arm64) et la clé publique utilisée (signed-by=/usr/share/keyrings/mongodb-server-8.0.gpg) :

Mettre à jour la base des paquets disponibles :

```
apt update
```

Installer MongoDB :

```
apt install -y mongodb-org
```

Recharger le démon systemd :

```
systemctl daemon-reload
```

Démarrer le service MongoDB :

```
systemctl start mongod
```

Vérifiez que MongoDB est en cours d'exécution :

```
systemctl status mongod
```

Configurez MongoDB pour démarrer automatiquement au démarrage du système :

```
systemctl enable mongod
```

I.2 Installation de CVE-Search en production (NOT USE)

Etape1 Installation en production

DISCLAIMER : Dans mon cas je n'ai pas utilisé ce type d'installation (avec utilisateur dédiée etc.). Le contenu de cette section est directement tiré de la documentation officiel d'OCS. Le contenu reste à titre d'information, si vous voulez le reproduire, adapter le contenu a votre situation.

→After the common steps from Standard Installation:

Create a dedicated, unprivileged, user to run the cve-search service

```
adduser cve --home /opt/cve
```

Create and activate a python virtual environment called cve-env

```
su - cve
```

```
virtualenv cve-env
```

```
source ./cve-env/bin/activate
```

Installation of cve-search in the home directory of the user cve

```
cd
```

```
git clone https://github.com/cve-search/cve-search.git
```

```
cd cve-search
```

```
pip3 install -r requirements.txt
```

```
exit
```

II. Configuration de CVE-Search

Etape 1. Fichier de configuration

Par défaut, CVE-Search prend en compte certains aspects de la configuration de l'application. Ces valeurs par défaut sont indiquées dans le fichier <<install_dir>>/etc/configuration.ini.sample :

Si votre installation nécessite d'autres paramètres et configurations, copiez le fichier etc/configuration.ini.sample dans <<install_dir>>/etc/configuration.ini et adaptez-le en conséquence.

Copier le fichier de configuration « configuration.ini » et modifier son contenu avec celui-ci :

cp ./cve-search/etc/configuration.ini.sample ./cve-search/etc/configuration.ini

Etape 2. Peuplement de la base de données

Activer l'environnement virtuel « /pythonENV/ » :

source /pythonENV/bin/activate

Permet de bénéficier des dépendances nécessaires pour l'activations du fichier « db_updater.py ».

Pour l'exécution initiale, vous devez alimenter la base de données CVE (de manière forcée, donc drop et réinjecte) :

./cve-search/sbin/db_updater.py -f -c

*Cela récupérera toutes les données CVE (Common Vulnerabilities and Exposures) et CPE (Common Platform Enumeration) existantes à partir de l'API NIST de la NVD et, par défaut, les **sources supplémentaires** également. L'importation initiale peut prendre un certain temps en fonction de votre configuration, par exemple plus de 45 minutes.*

Cette opération peut également être exécutée en tant que service SystemD. Les exemples d'unités se trouvent sous _etc/systemd/system/ : cvesearch.db_init.service & cvesearch.db_init.target. « systemctl start --no-block cvesearch.db_init.target ». Mais dans mon cas, je ne les utilise pas.

*Les **sources supplémentaires** disponibles sont : **CWE**, **CAPEC**, **VIA4** & **EPSS**. Si vous n'avez pas besoin de certaines d'entre elles, elles peuvent être désactivées dans le fichier sources.ini. Les sources désactivées peuvent être mises à jour en une seule fois avec -s (-sources) qui prend une liste des sources disponibles, par exemple :*

« ./sbin/db_updater.py -s cwe capec via4 epss »

Les VIA4 sont des références croisées du NIST, de Red Hat et d'autres vendeurs grâce à VIA4CVE. De plus, si vous voulez importer votre propre JSON de VIA4CVE, vous devez remplacer dans sources.ini l'attribut VIA4 par « file:///PATH/TO/VIA4CVE/VIA4CVE-feed.json ».

Ensuite sortir de l'environnement python avec :

deactivate

Etape 3. Lancement du serveur web

Démarrer le serveur web :

/pythonENV/bin/python3 ./cve-search/web/index.py

Information complementaire pour un environnement en production (Not USE):

Potentiel web gui en version de production "./cve-search/web/wsgi.py".

Standard Installation

Once you set up the configurations.ini file how you want it to be, you can start the webserver by simply running *python3 web/index.py*. To stop the server, you can simply press the **CTRL+C** combination.

Alternatively, on Linux, you can start the server by running *nohup python3 web/index.py &*. This will make the server run in the background. However, this makes it so you cannot use the **CTRL+C** combination. Instead, you will have to find the processes related to the web-server, by using *ps aux | grep web/index.py*. Then kill them using the *kill -15* command on all the processes related to the server.

The web server could be also run as a SystemD service. Example unit is in *_etc/systemd/system/*: cvesearch.web.service.

```
sudo systemctl start --no-block cvesearch.web.service
```

Production Installation

Configure cve-search as a UWSGI app listening on a unix socket, and enable the app to start at boot.

```
sudo cat /opt/cve/cve-search/etc/wsgi.ini.sample \
    > /etc/uwsgi/apps-available/cve-search.ini

sudo ln -s /etc/uwsgi/apps-available/cve-search.ini \
    /etc/uwsgi/apps-enabled/

sudo systemctl restart uwsgi
```

Disable NGINX's default config, and configure proxying connections to the uwsgi socket

```
sudo rm /etc/nginx/sites-enabled/default

sudo cat /opt/cve/cve-search/etc/nginx.conf.sample \
    > /etc/nginx/sites-available/cve-search.conf

sudo ln -s /etc/nginx/sites-available/cve-search.conf \
    /etc/nginx/sites-enabled/

sudo systemctl restart nginx
```

Visit *http://127.0.0.1/MOUNT/*

App mounting (base_url)

When running cve-search under a 'production installation', a *base_url* can be configured through the *MountPath* setting in the configuration. By default, the production installation is mounted at */MOUNT*.

NOTE:

- When running cve-search using UWSGI and NGINX, cve-search's *SSL*, *host*, and *port* configuration settings are ignored. TLS/SSL should instead be configured via NGINX.

Setting up TLS

To set up TLS on your server, you need a certificate and a key. On Linux, you can create these by running the following command:

```
openssl req -x509 -nodes -days 365 -newkey rsa:2048 \
    -keyout /ssl/cve-search.key -out /ssl/cve-search.crt
```

The parameter *-days* lets you choose the duration the certificate must be valid. In this example, this is 365 days.

Etape 4. Mise à jour BDD avec SystemD & Timer.
Informations complémentaire et automatisation avec SystemD & Timer.

Depuis la version 5.0.2 de CVE-Search (utilisant CveXplore v0.3.28), les mises à jour utilisent plus efficacement toutes les sources en ne téléchargeant que les données modifiées. Pour les CPEs et CVEs, cela signifie que seules les entrées ajoutées ou modifiées depuis la dernière mise à jour sont récupérées. Pour les autres sources, CVE-Search vérifie si le fichier a changé avant de le télécharger. Il est donc désormais sûr de lancer les mises à jour régulièrement, par exemple toutes les heures, en utilisant un outil comme **crontab**. Les journaux des mises à jour sont enregistrés par défaut dans « cve-search/log/update_populate.log ».

Il est également possible d'automatiser ces mises à jour via un service et un timer SystemD. Des exemples d'unités SystemD sont disponibles dans « cve-search/_etc/systemd/system/ » :

- cvesearch.db_updater.service
- cvesearch.db_updater.timer

Modifier le contenu du service :

nano cve-search/_etc/systemd/system/cvesearch.db_updater.service

Contenu :

```
[Unit]
Description=circl dot lu CVE-Search db_updater service
Requires=mongod.service redis-server.service
After=network.target cvesearch.db_init.service cvesearch.db_repopulate.service mongod.service redis-server.service
Documentation=https://cve-search.github.io/cve-search/database/database.html

[Service]
WorkingDirectory=/root/cve-search
ExecStart=/pythonENV/bin/python3 ./sbin/db_updater.py
User=root
Type=oneshot
SyslogIdentifier=cvesearch.db_updater
```

Pour activer et démarrer le service ainsi que le timer:

systemctl enable cve-search/_etc/systemd/system/cvesearch.db_updater.service

systemctl enable cve-search/_etc/systemd/system/cvesearch.db_updater.timer

systemctl start cvesearch.db_updater.timer

Si vous voulez tester le bon fonctionnement du service :

systemctl start cvesearch.db_updater.service

Si certains CVEs ou CPEs récents (datant des 1 à 120 derniers jours) sont manquants malgré des mises à jour régulières, vous pouvez éviter de reconstituer toute la base en utilisant l'option -d 1..120. Cela peut être utile en cas de problèmes de connectivité ou d'interruption des mises à jour avec l'API NVD.

Par exemple, pour forcer la récupération des données des 7 derniers jours :

source /pythonENV/bin/activate (active l'environnement python)

./cve-search/sbin/db_updater.py -d 7

deactivate (désactive l'environnement python)

La liste complète des options est disponible avec -h ou --help.

```
options:
  -h, --help            show this help message and exit
  -s [SOURCE ...], --sources [SOURCE ...]
                        Sources to be updated if available in CveXplore. Defaults to all sources available & configured.
  -i, --index           Indexing new CVE entries in the fulltext indexer
  -l, --loop            Running at regular interval; waits 1 hour (disabled with -d, --days)
  -f, --force           Drop collections and force initial import (only on first iteration with -l, --loop)
  -d 1..120, --days 1..120
                        Set update interval (1-120 days) manually for NVD API (CPE, CVE)
  -c, --cache           Enable CPE redis cache (unless -m, --minimal is set)
  -m, --minimal         Minimal import without redis-cache-cpe source (disables CPE redis cache)
  -v                    Dummy option for backwards compatibility
```

III. Configuration côté serveur OCS

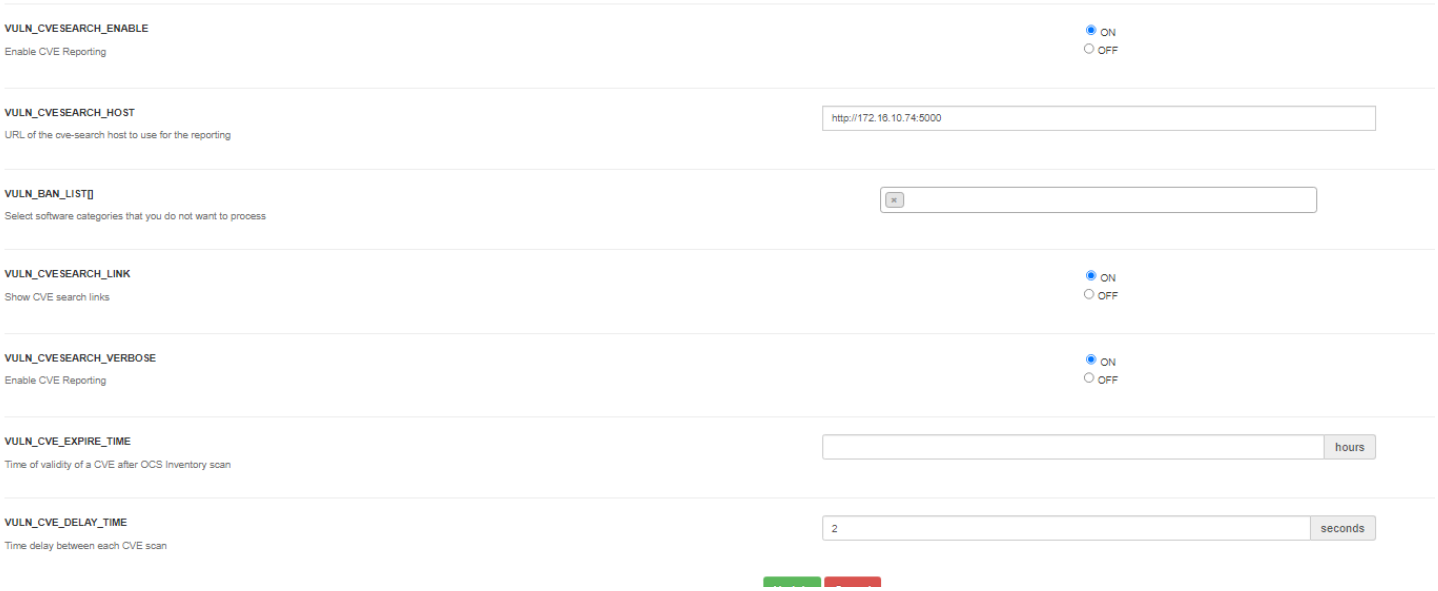
Etape 1. Prérequis

Pour accéder à la configuration de gestion de CVE-search, vous devez activer la configuration avancée :

- Naviguer vers Configuration > General configuration > Server
- Mettre ADVANCE_CONFIGURATION a ON
- Cliquer sur Update

Etape 2. Paramètres de gestion CVE-Search

En tant qu'administrateur, allez dans le menu Configuration > Configuration générale, et cliquez sur l'entrée « Gestion de la recherche CVE » dans le volet de navigation gauche.



Settings:

- ***VULN_CVESEARCH_ENABLE :*** *Define wether the integration is enabled or not (default : Disabled);*
- ***VULN_CVESEARCH_HOST :*** *Define the URL of the cve-search server to be queried.*
- ***VULN_BAN_LIST :*** *Select software categories that you do not want to process. When a sofwtare category has been added to VULN_BAN_LIST, All CVE for software in this category will not be processed by OCS Inventory.*
- ***VULN_CVESEARCH_LINK :*** *Enable display of redirect link to CVE details page.*
- ***VULN_CVESEARCH_VERBOSE :*** *Enable verbose mode in CVE Crontab, can help in a debugging process.*
- ***VULN_CVE_EXPIRE_TIME :*** *Time of validity of a CVE after OCS Inventory scan. After this time, the CVE entry will become invalid and will be re-processed by OCS.*
- ***VULN_CVE_DELAY_TIME :*** *Time delay between each CVE api call.*

Etape 3. Configuration des tâches planifiées (CronTab)
Dans votre serveur, configurez un CronTab pour appeler le fichier cron_cve.php et le fichier cron_all_software.php situer dans « /usr/share/ocsinventory-reports/ocsreports/crontab/ » :

php /usr/share/ocsinventory-reports/ocsreports/crontab/cron_all_software.php

php /usr/share/ocsinventory-reports/ocsreports/crontab/cron_cve.php

« cron_all_software.php » permet de récupérer les données des logiciels client d'OCS.
« cron_cve.php » appelle le serveur « cve-search » et récupère tous les CVE par éditeur, nom et version du logiciel.

Ils peuvent être lancer indépendamment de la tache cron pour une mise à jour manuel, cependant, il est recommandé de lancer cron_all_software.php avant cron_cve.php afin d'avoir les données logicielles à jour lors de la récupération sur le serveur CVE-Search.

Ouvrir l'éditeur crontab :

crontab -e

```
Select an editor.  To change later, run 'select-editor'.
  1. /bin/nano        <---- easiest
  2. /usr/bin/vim.tiny

Choose 1-2 [1]: 1
```

Coller le contenu du fichier crontab suivant :

```
# Update software data daily at 1:00 AM
0 1 * * * cd /usr/share/ocsinventory-reports/ocsreports/crontab/ && php cron_all_software.php

# Retrieve CVE information daily at 2:00 AM
0 2 * * * cd /usr/share/ocsinventory-reports/ocsreports/crontab/ && php cron_cve.php
```

Vous pouvez ajouter un fichier journal pour chaque opération, voir le fichier crontab fourni pour cela.

Lister les tâches cron pour s'assurer qu'elles ont bien été ajoutées :

crontab -l