Installation de Trend OfficeScan XG (version 12)

Lionel FIS déc. 2017

Ce document récapitule les modalités d'installation de Trend OPfficeScan XG, ainsi que le paramétrage conseillé. Il a été rédigé à partir des documents suivants :

- TRENDOfficeScan11ReseauPedagogiqueV1-0.pdf (DACE, mise à jour : 3 septembre 2015)
- OFFICESCAN_RANSOMWARE_TCh.pdf disponible sur le site MAGRET : http://pedagogie.ac-toulouse.fr/matice/magret/gestion.htm

Documentation Trend Micro :

- XG OfficeScan Manuel de l'administrateur : http://docs.trendmicro.com/all/ent/officescan/v12.0/fr-fr/osce_12.0_ag.pdf
- Aide en ligne de l'agent OfficsScan XG : http://docs.trendmicro.com/all/ent/officescan/v12.0/fr-fr/osce_12.0_agent_olh/About.html#GUID-401DC417-7463-4B1E-A888-D1FD74FD3B82

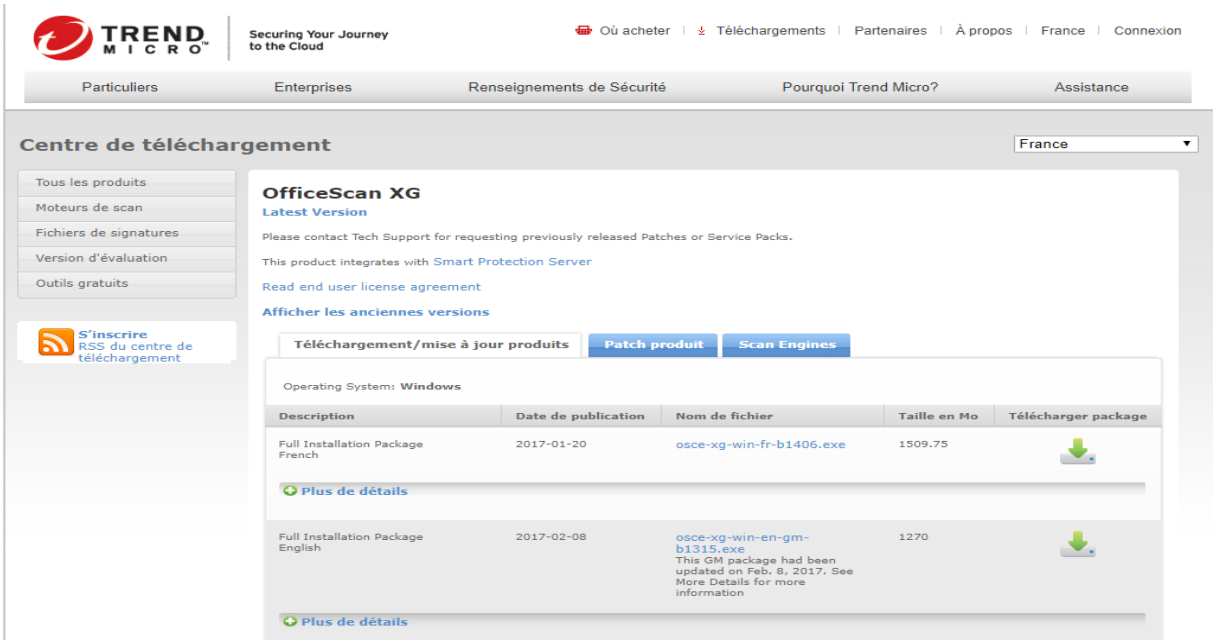
Champs d'application :

- Réseau pédagogique
- L'installation de la console Trend sur un serveur membre du domaine (serveur02) est vivement recommandée
- Système Windows serveur 2008 R2 ou supérieur
- IIS installé
- Installation initiale ou « par-dessus » une autre version d'OfficeScan (10.6 SP3 minimum)

Sommaire :

1- Téléchargements pour OfficeScan :

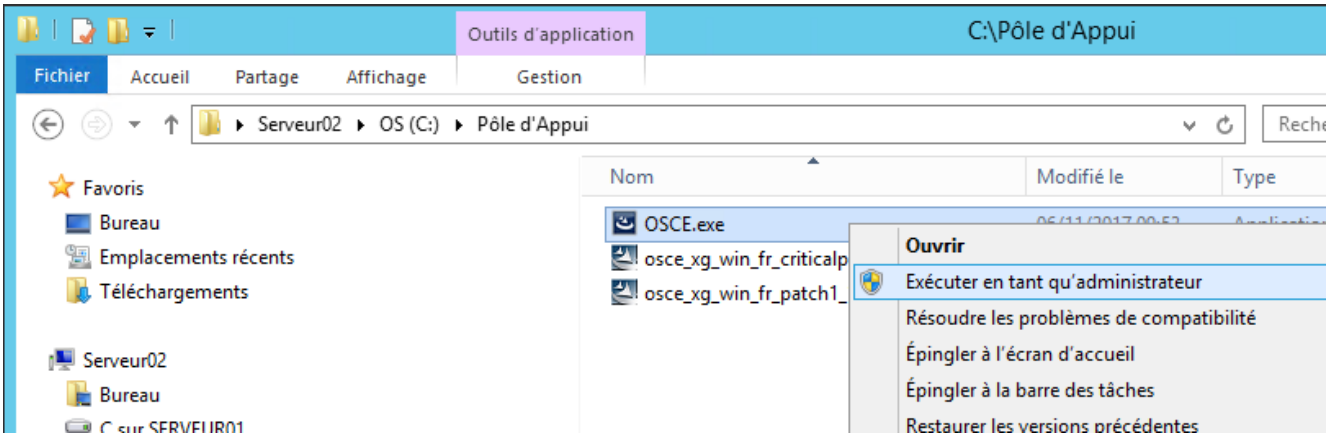
La version XG (version 12) et les Patchs sont disponibles sur le site Trend Micro ci-dessous :
http://downloadcenter.trendmicro.com/index.php?regs=fr&clk=latest&clkval=4973&lang_loc=2

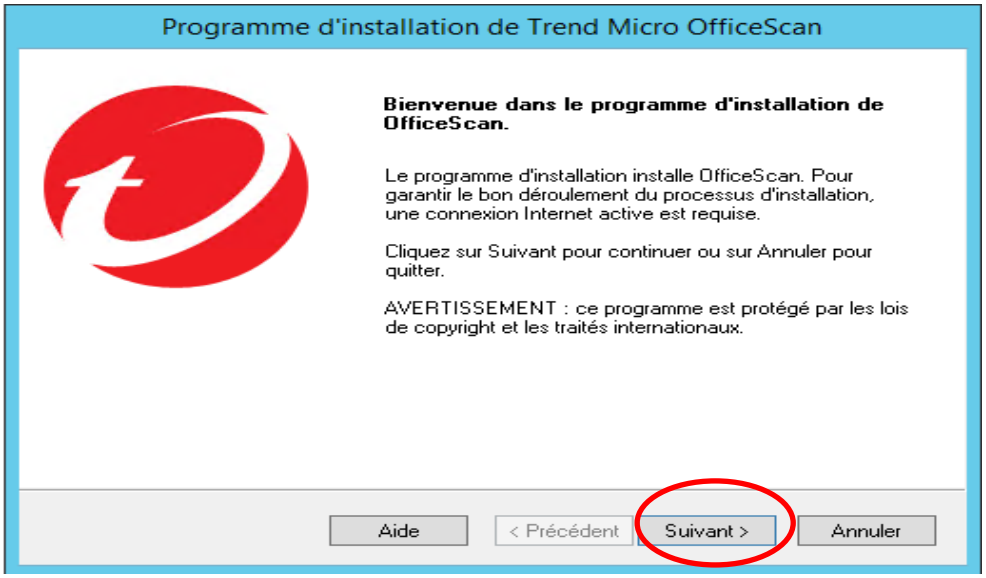


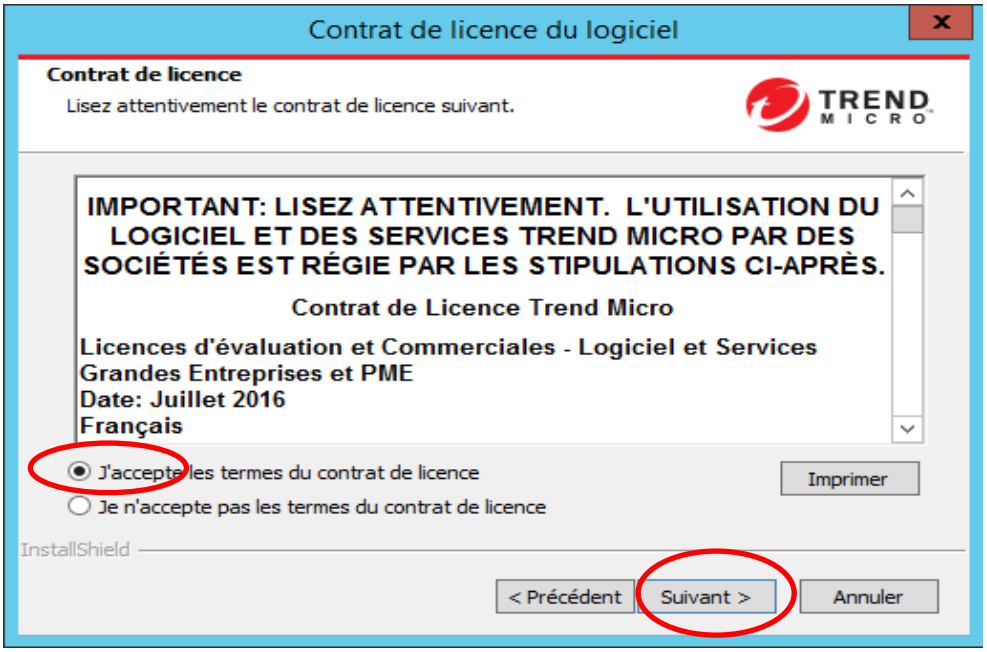
- Télécharger les versions françaises :
  - Full Installation Package (osce-xg-win-fr-b1406.exe)
  - Product Patch (osce_xg_win_fr_patch1_1576.exe)
  - Critical Patch (osce-xg-win-fr-criticalpatch-1775.exe)
- Débloquer les archives.

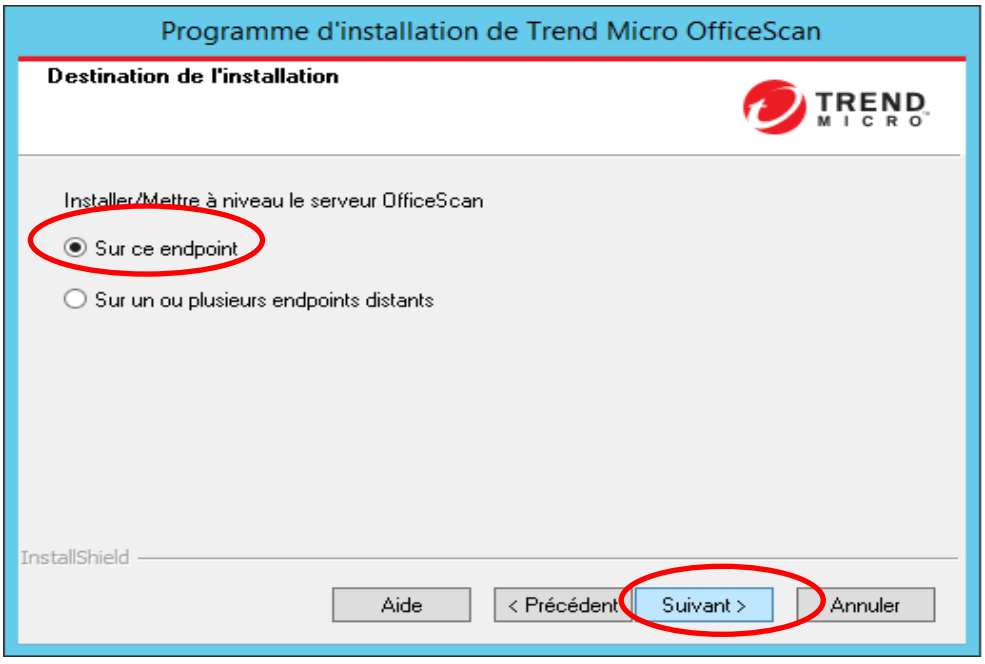
2- Installation de Trend OfficeScan XG sur un serveur membre (Serveur02) :

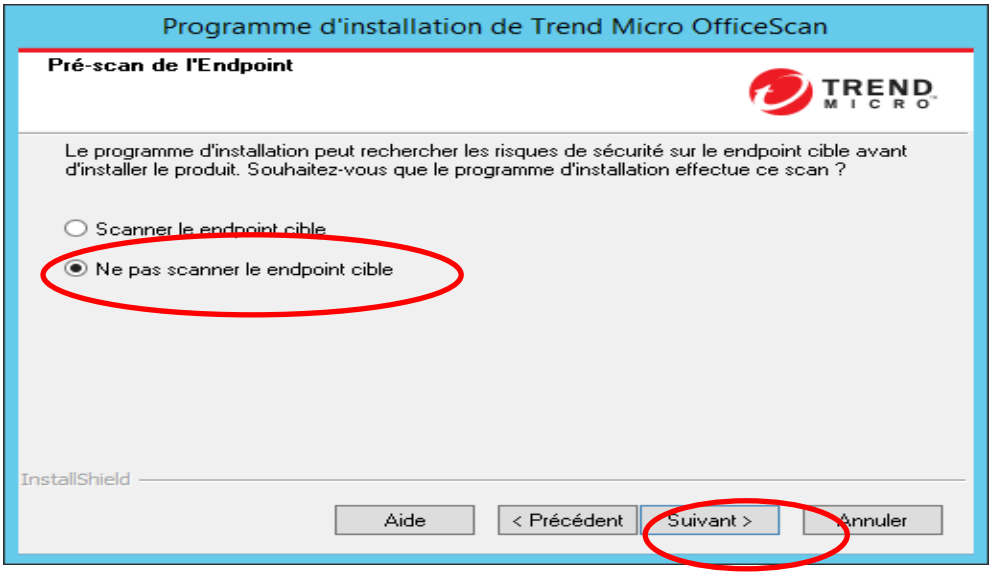
Exécuter OSCE.exe en tant qu'administrateur :

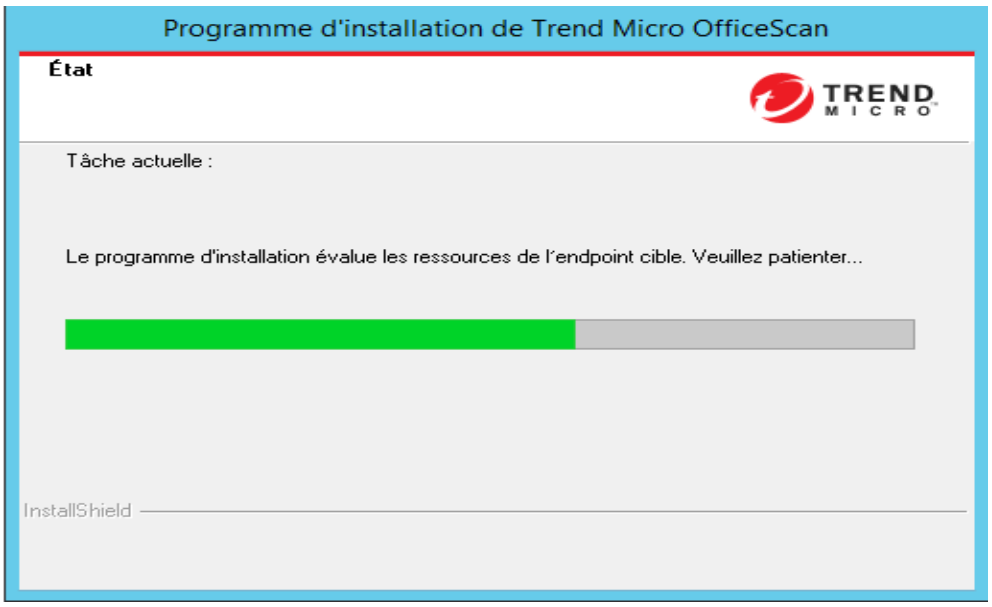



Programme d'installation de Trend Micro OfficeScan
Bienvenue dans le programme d'installation de OfficeScan.
Le programme d'installation installe OfficeScan. Pour garantir le bon déroulement du processus d'installation, une connexion Internet active est requise.
Cliquez sur Suivant pour continuer ou sur Annuler pour quitter.
AVERTISSEMENT : ce programme est protégé par les lois de copyright et les traités internationaux.
Aide
< Précédent
Suivant >
Annuler

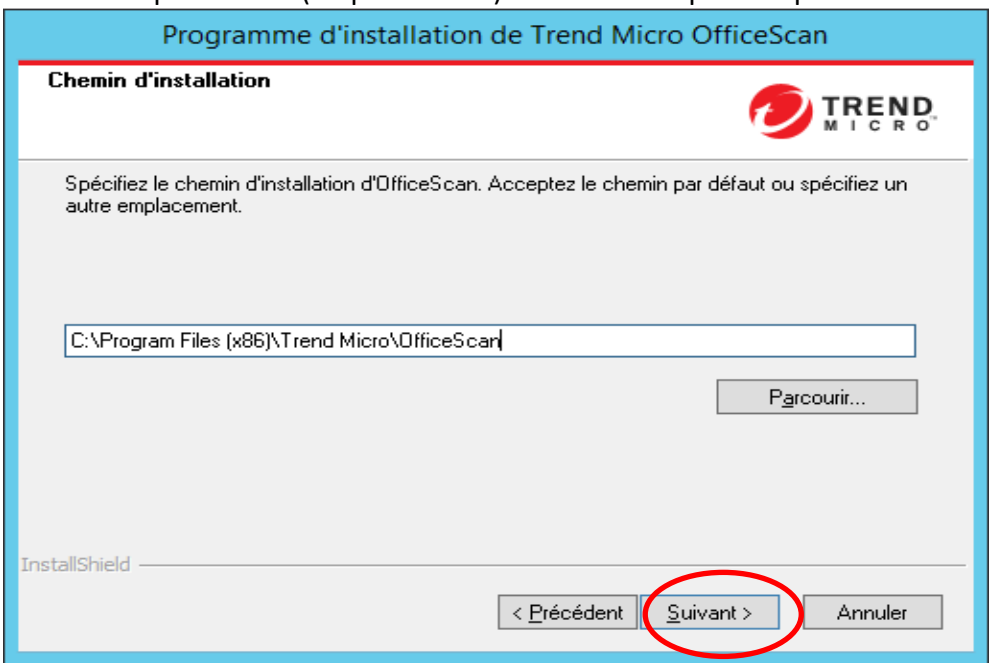

Contrat de licence du logiciel
Contrat de licence
Lisez attentivement le contrat de licence suivant.
TREND MICRO
IMPORTANT: LISEZ ATTENTIVEMENT. L'UTILISATION DU LOGICIEL ET DES SERVICES TREND MICRO PAR DES SOCIÉTÉS EST RÉGIE PAR LES STIPULATIONS CI-APRÈS.
Contrat de Licence Trend Micro
Licences d'évaluation et Commerciales - Logiciel et Services
Grandes Entreprises et PME
Date: Juillet 2016
Français
J'accepte les termes du contrat de licence
Je n'accepte pas les termes du contrat de licence
Imprimer
InstallShield
< Précédent
Suivant >
Annuler


Programme d'installation de Trend Micro OfficeScan
Destination de l'installation
TREND MICRO
Installer/Mettre à niveau le serveur OfficeScan
Sur ce endpoint
Sur un ou plusieurs endpoints distants
InstallShield
Aide
< Précédent
Suivant >
Annuler

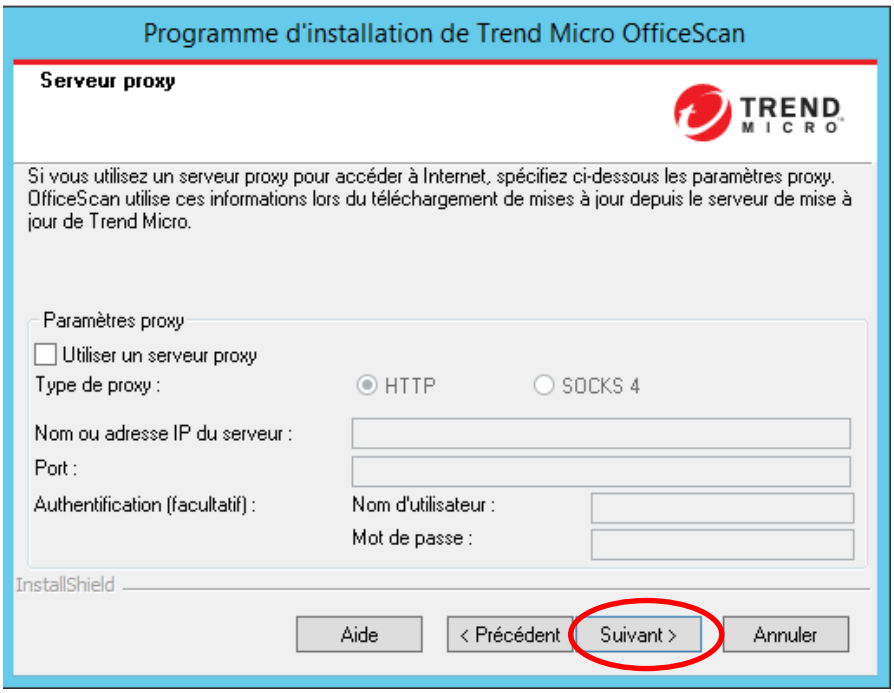




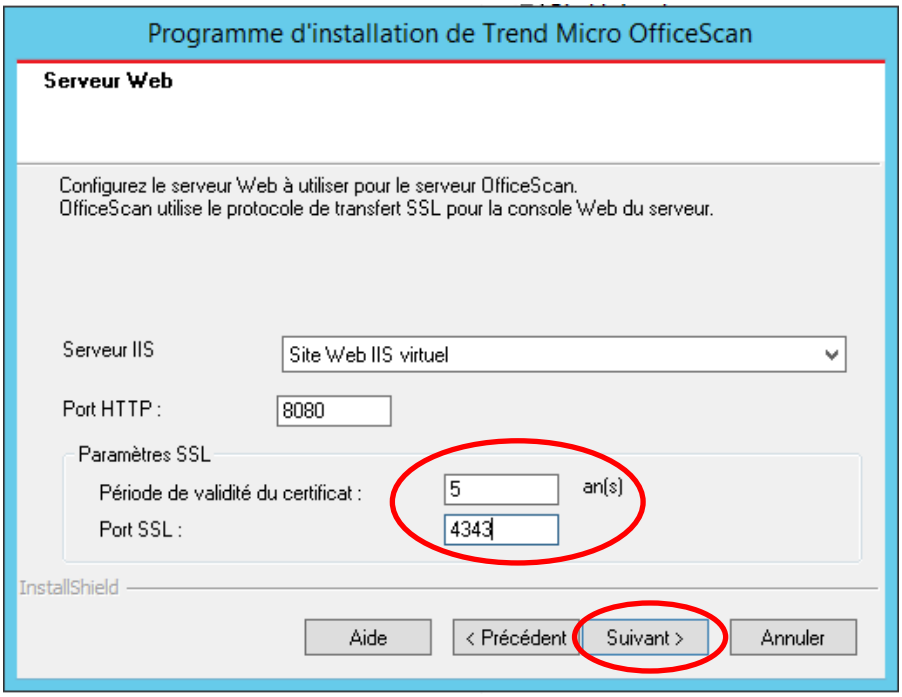
Suivant l'espace disque disponible on pourra mettre le répertoire « Trend Micro » sur la partition C ou sur la partition D (de préférence). Prévoir un espace disponible de l'ordre de 30 Go :



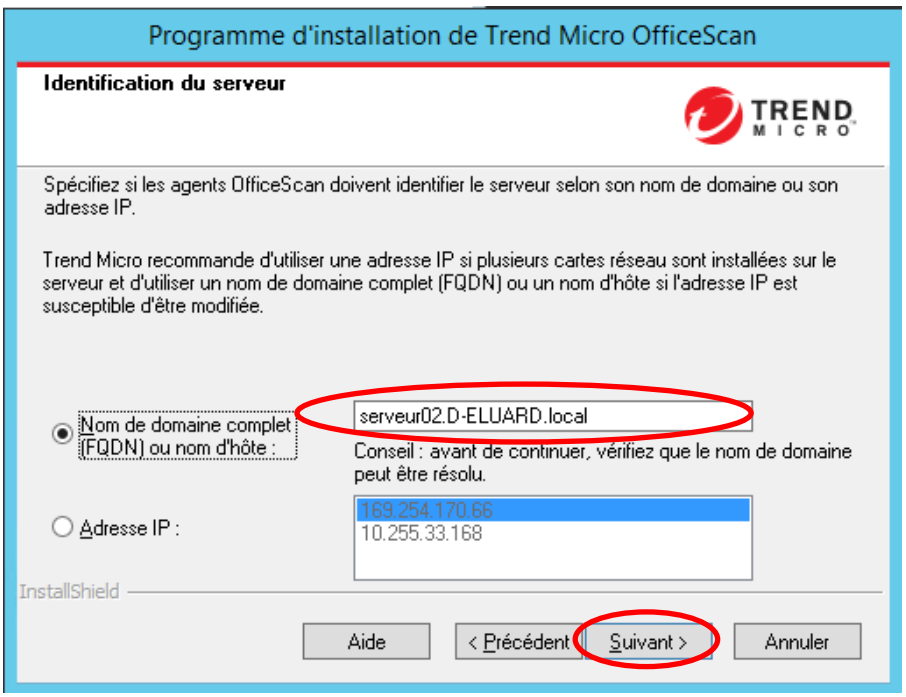
Pas de serveur proxy, car on est sur un serveur pouvant accéder directement à Internet au travers du PFS.
L'adresse IP du serveur doit être dans la plage 10.255.X.Y+1 à 10.255.X.Y+11 (voir documentation Magret « MagretV16_Installation_serveur_V2012R2) :



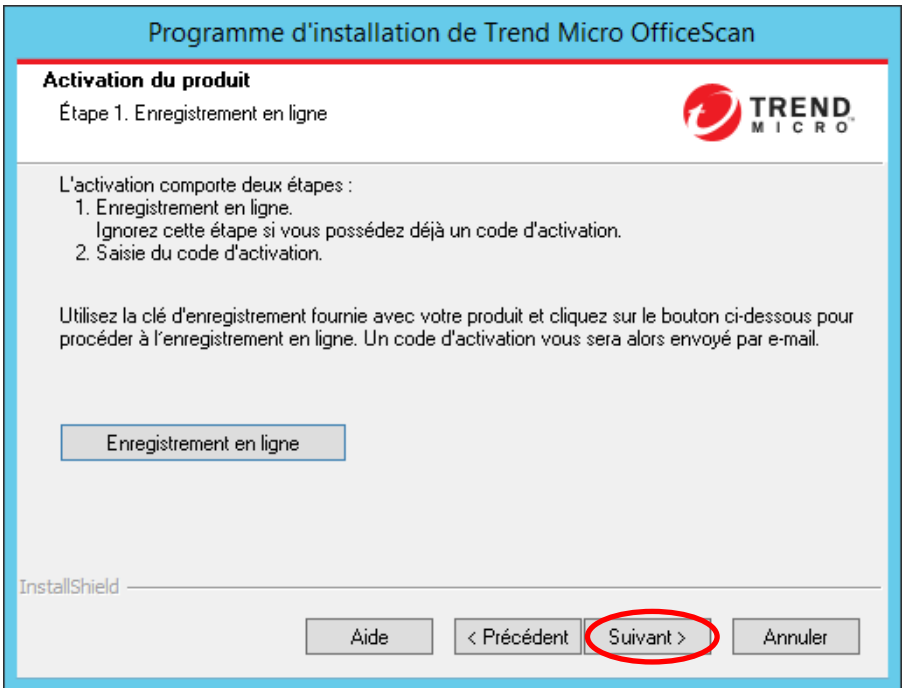
Choisir une période de validité du certificat de 5 ans et garder le port SSL 4343 :



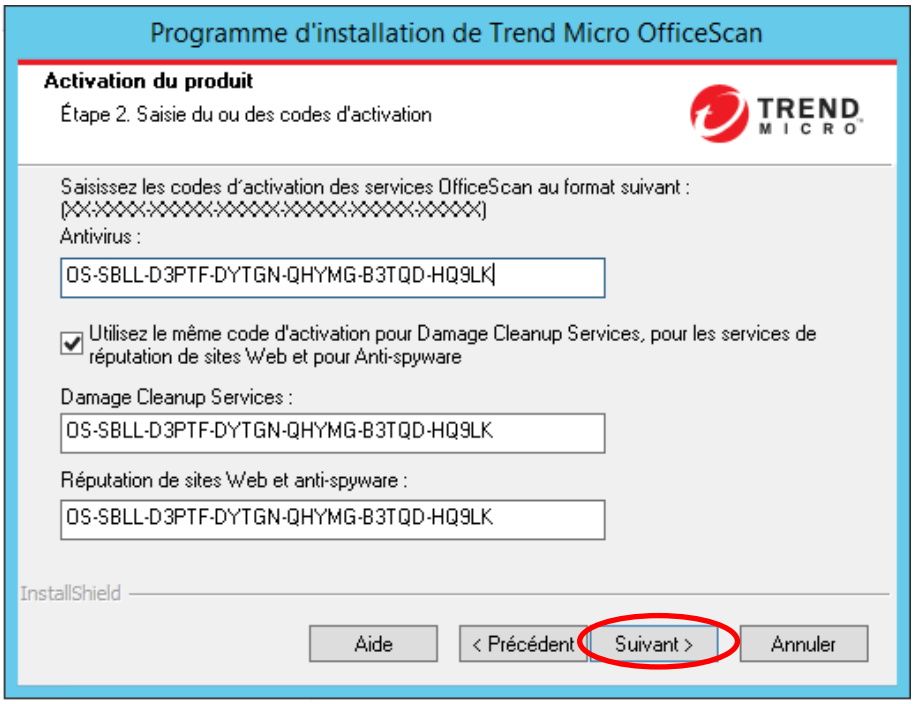
Indiquer le nom de domaine complet (FQDN) :



Ignorer l'enregistrement en ligne et faire suivant :

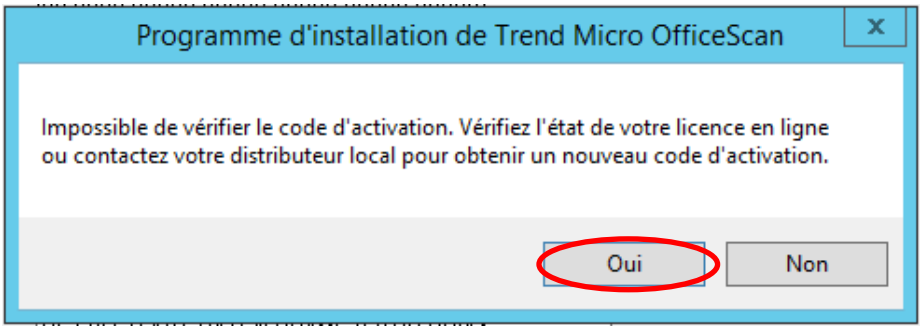


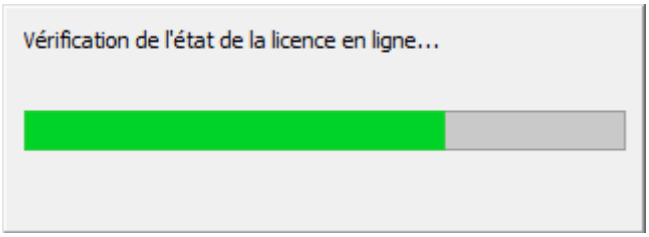
Copier les 37 caractères de la clé d'activation qui se trouve dans le fichier « cle d'activation.pdf » et les coller dans la fenêtre ci-dessous.
Cocher la case « Utiliser le même code d'activation pour Damage… »

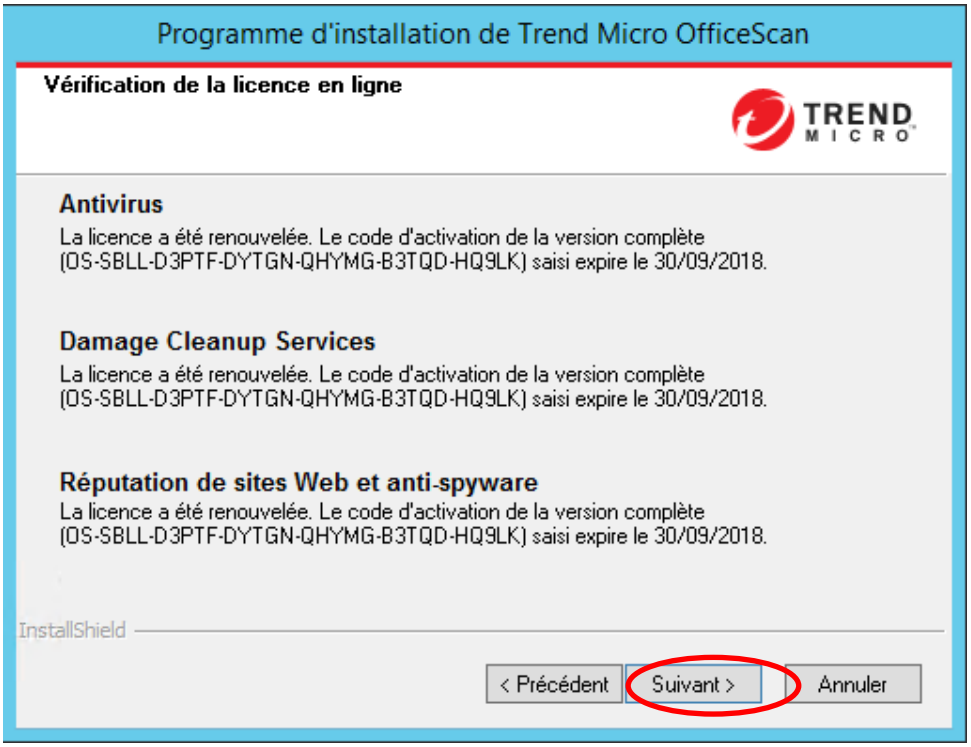


Le fichier de licence obtenu lors de la négociation initiale du contrat était valable pour une période de cinq ans (30/09/2010 au 30/09/2015).
Ce contrat a ensuite été reconduit pour trois ans, jusqu'au 30/09/2018. Bien qu'il soit obsolète le fichier de licence dont on dispose ici, permet l'activation en ligne de la licence :

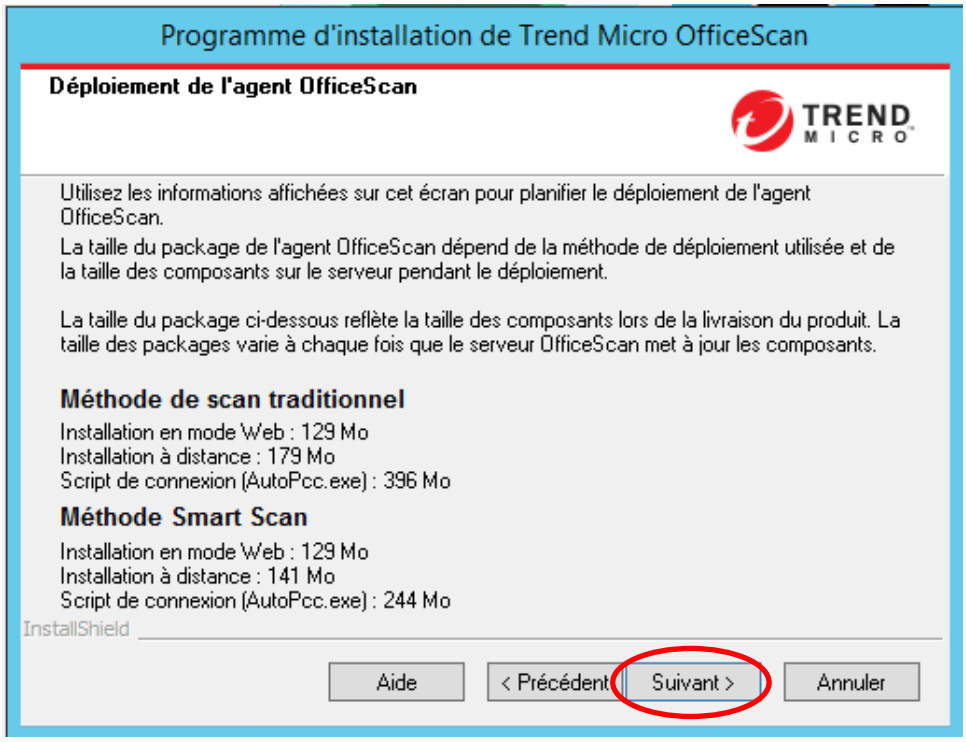
Répondre Oui, pour vérifier l'état de la licence en ligne :





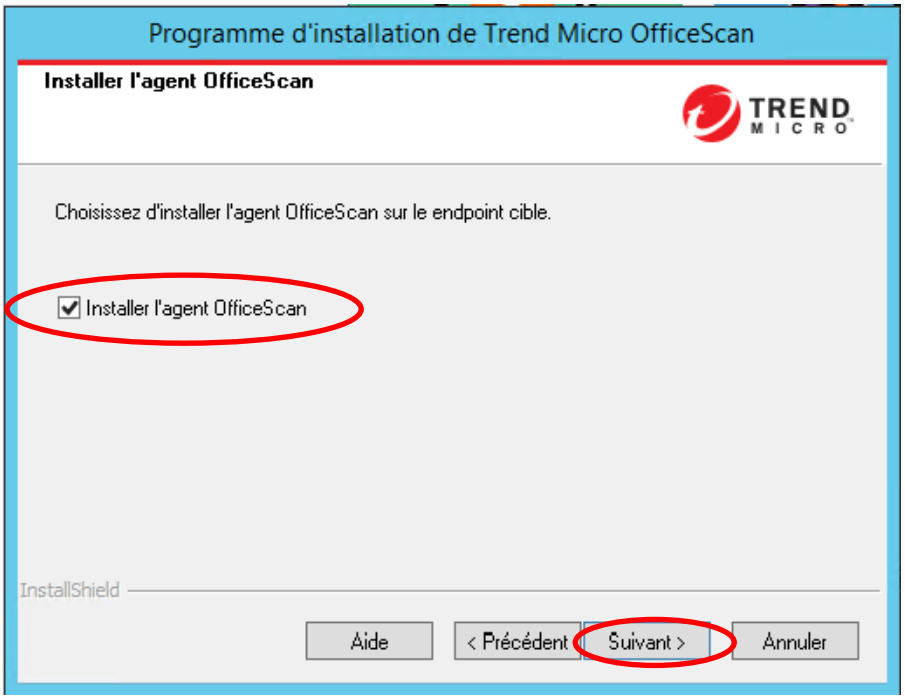


Le choix de la méthode de scan s'effectuera plus tard (voir paragraphe 7-4-3) :

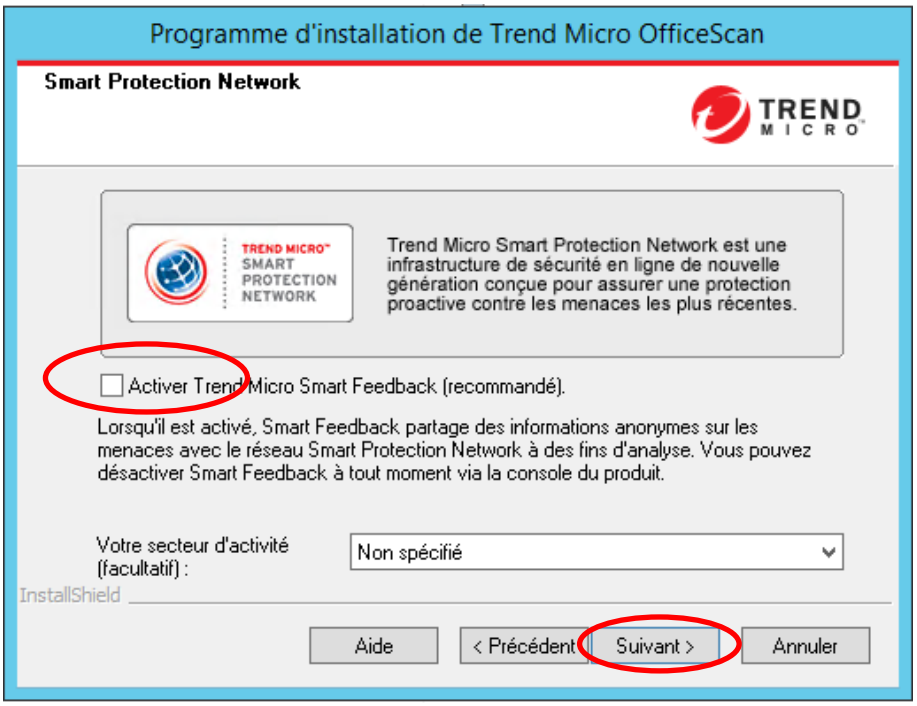


Installer le serveur Smart Protection Server intégré en l'absence de serveur Smart Protection autonome :

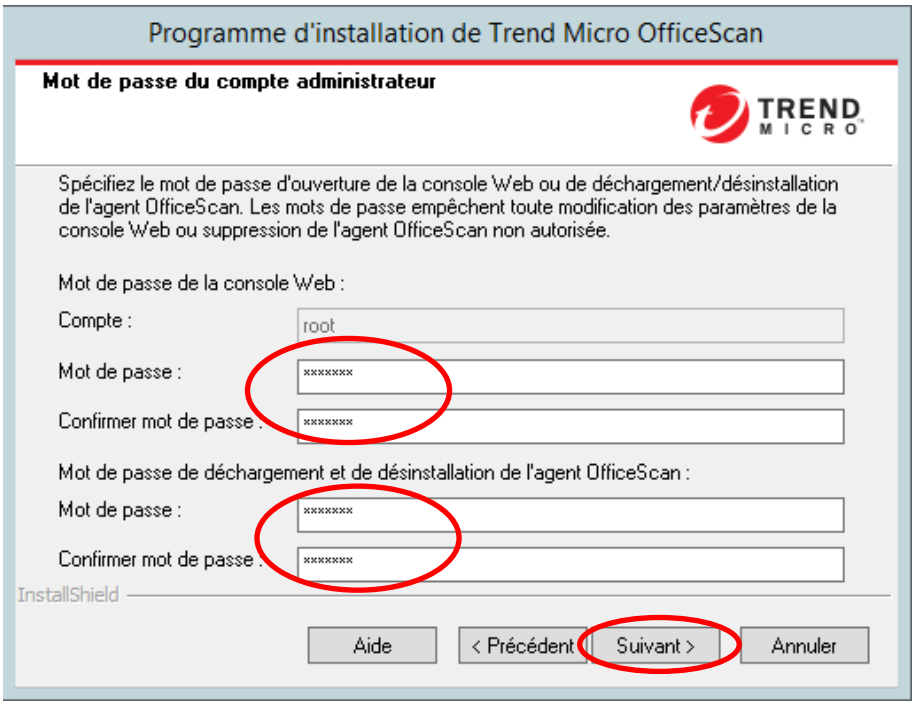
Installer l'agent OfficeScan sur le serveur :



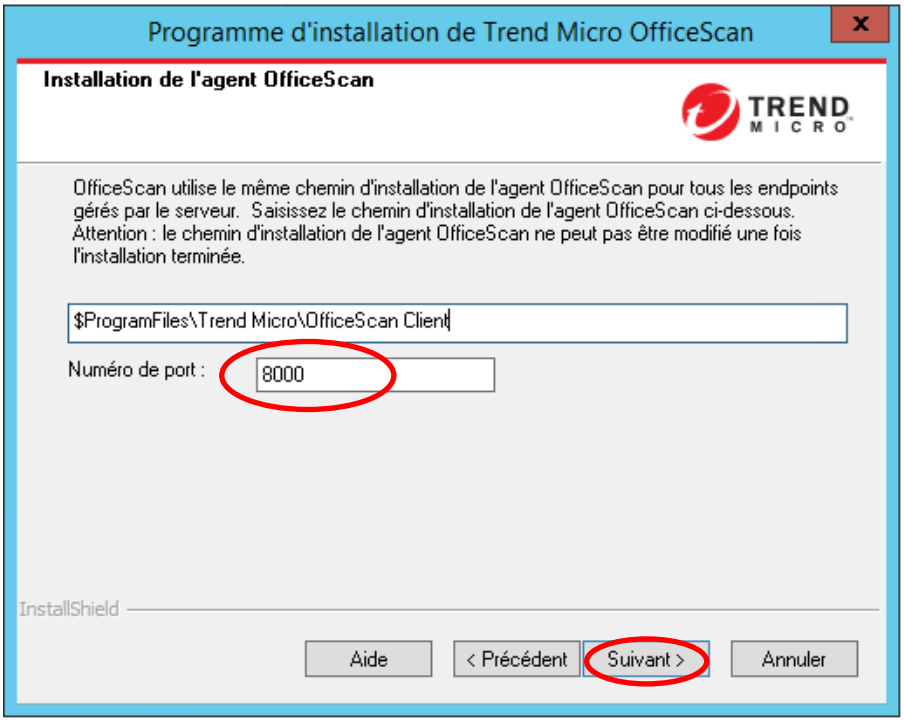
Pas de partage des informations :



Choisir un mot de passe pour l'accès à la console, et un autre mot de passe différent pour le déchargement et la désinstallation de l'agent.
Une complexité minimale est requise (Exemple : première lettre en majuscule) :

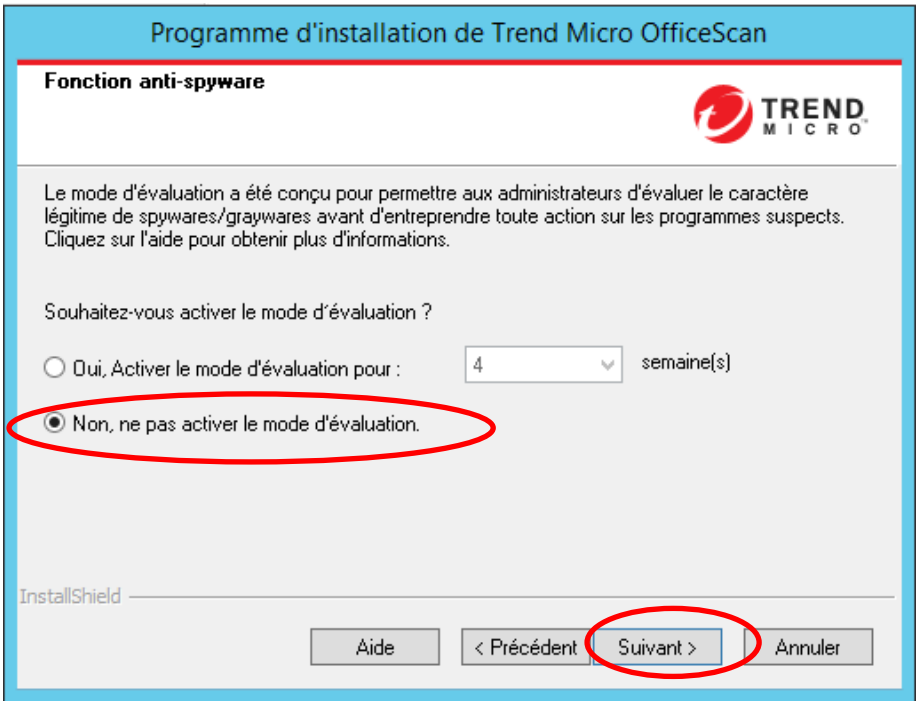


Installation de l'agent : conserver le chemin d'installation par défaut et fixer la valeur du port à 8000 :



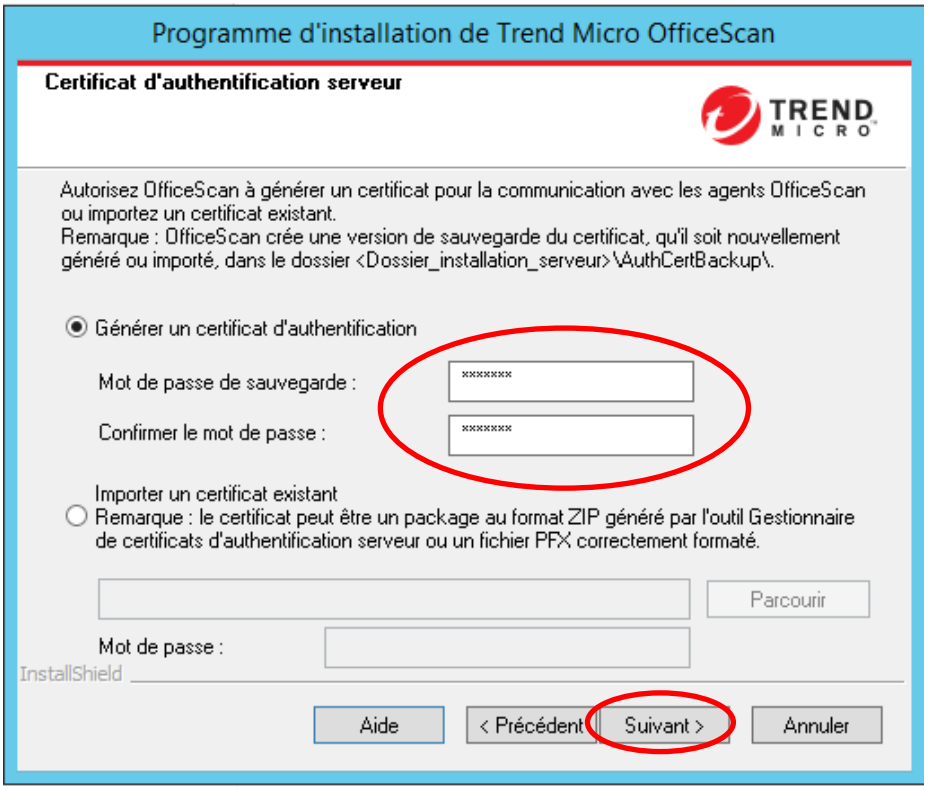
Ne pas activer le pare-feu OfficeScan :

Ne pas activer le mode d'évaluation, du caractère légitime des programmes suspects :

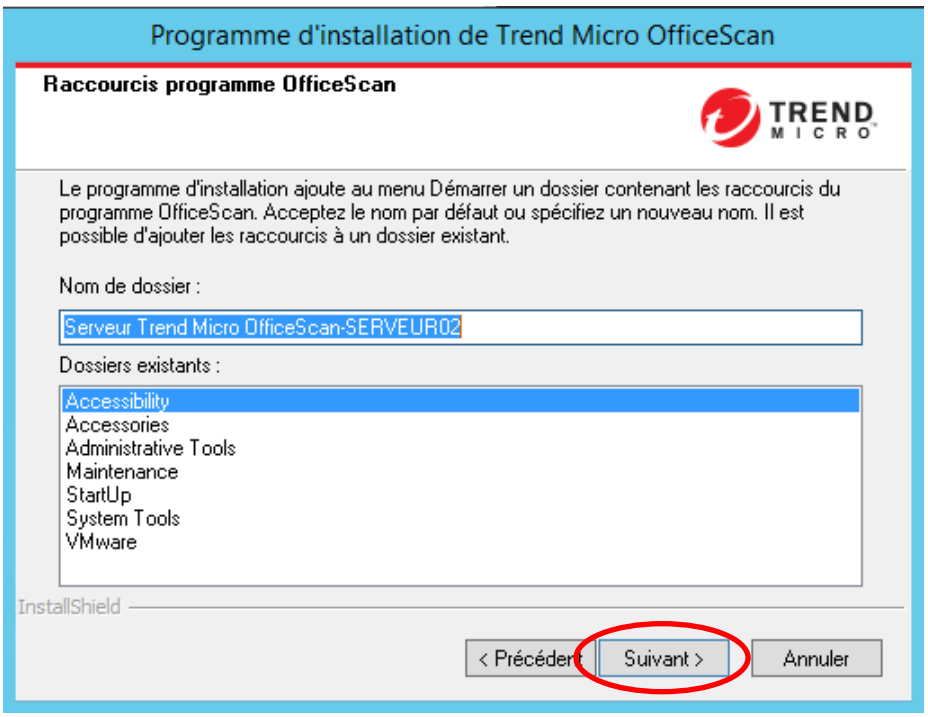


Activer la stratégie de réputation de sites Web :

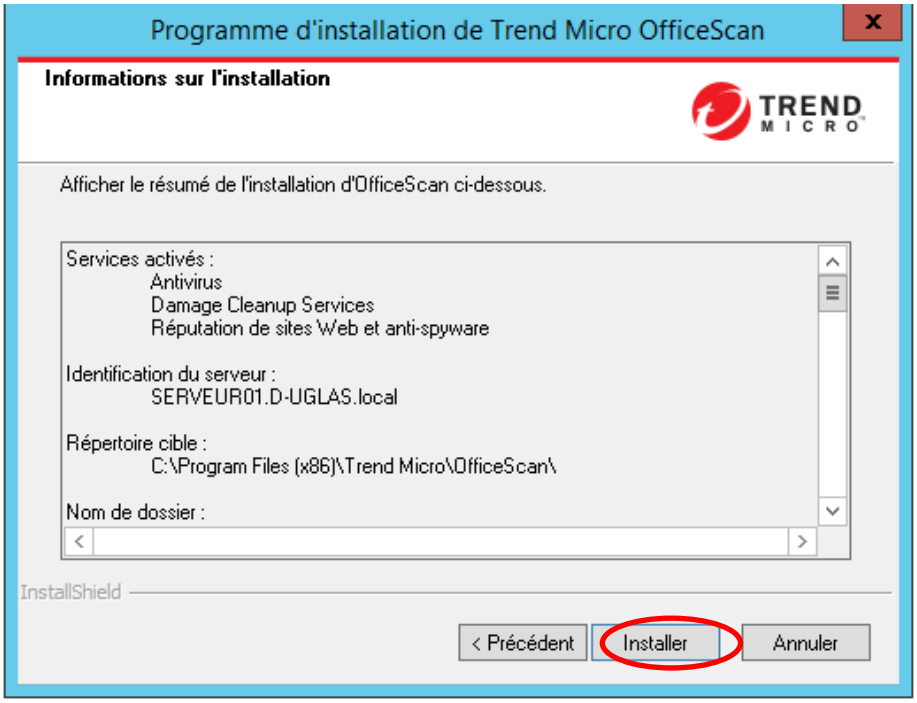
Générer un certificat de sécurité et indiquer un mot de passe pour ce certificat (donner le même mot de passe que pour l'accès à la console Web) :



Raccourcis du menu Démarrer :

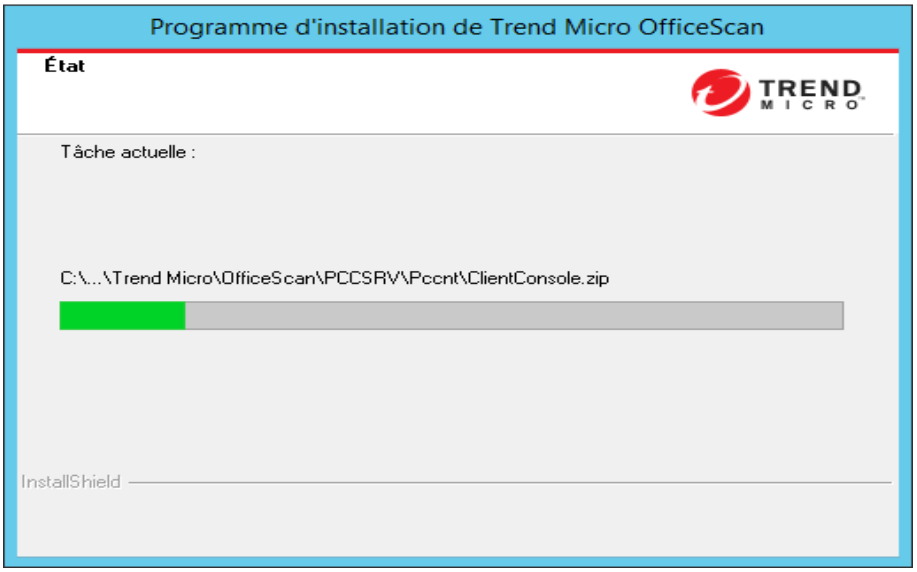


Récapitulatif avant le début de l'installation. Cliquer sur « Installer » :

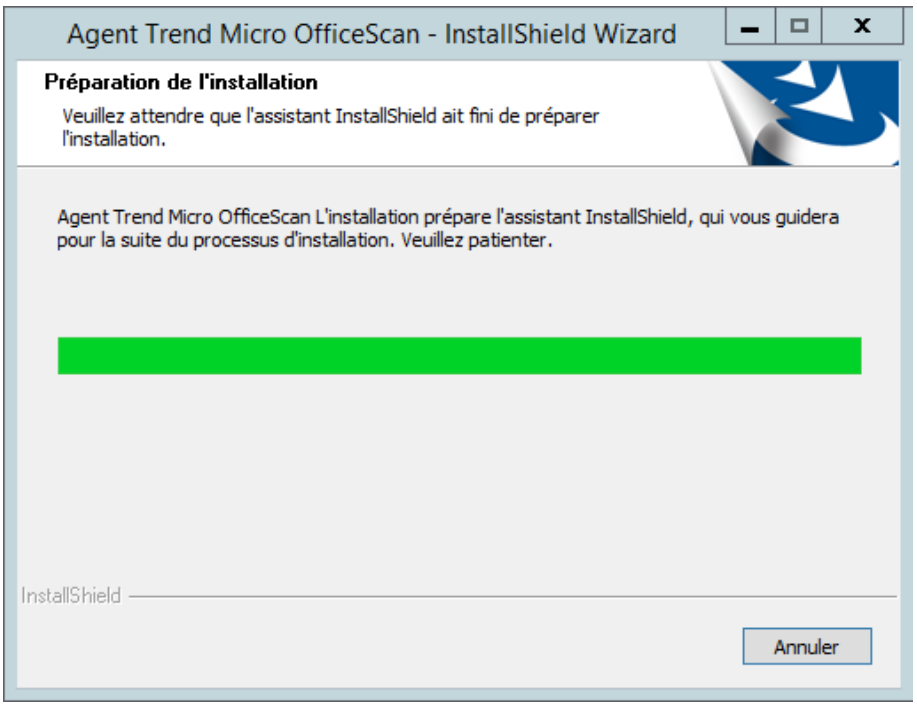


<u>Remarque :</u> IIS s'installera automatiquement dans le cas de Windows 2012R2, il pourra être nécessaire de l'installer préalablement sur des systèmes plus anciens.

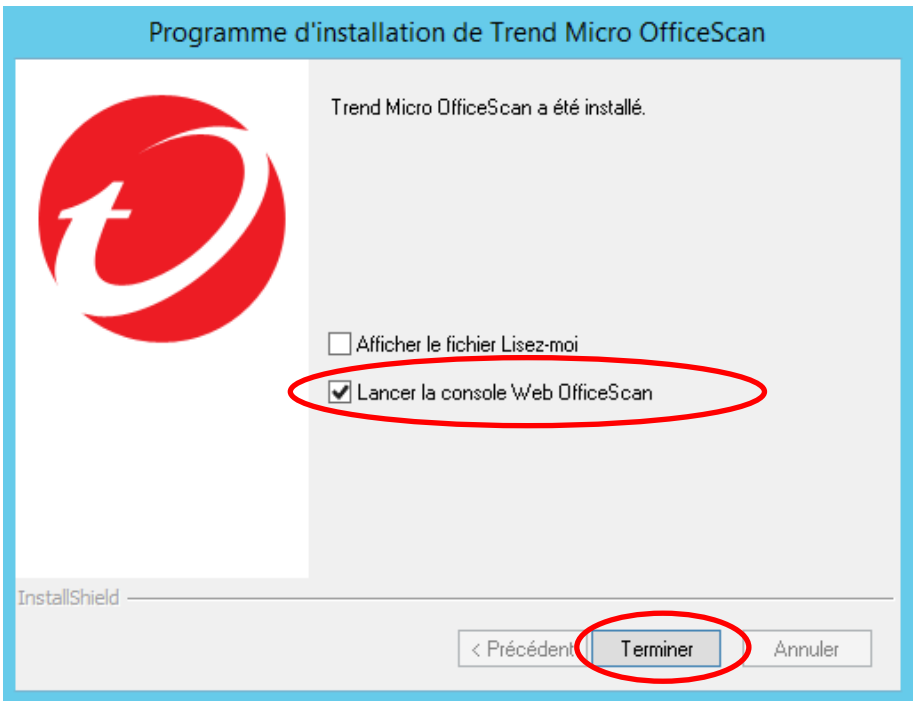
Début de l'installation : durée 10 à 15 mn environ suivant la configuration matérielle du serveur :



Installation de l’agent sur le serveur :

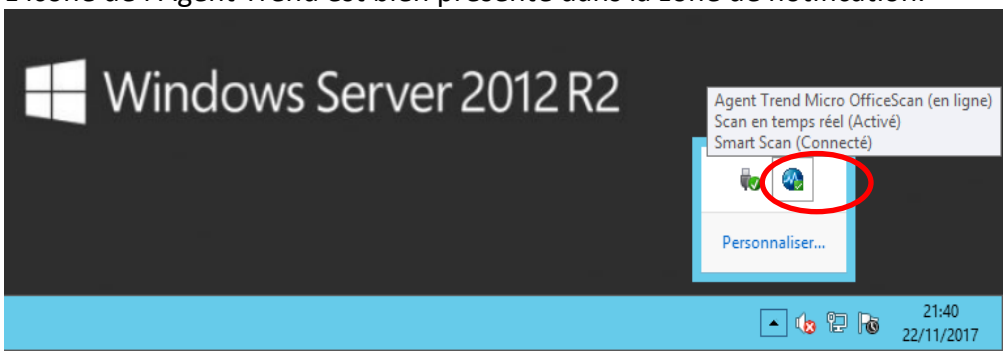


Installation terminée. Sélectionner « lancer la console Web OfficeScan » :

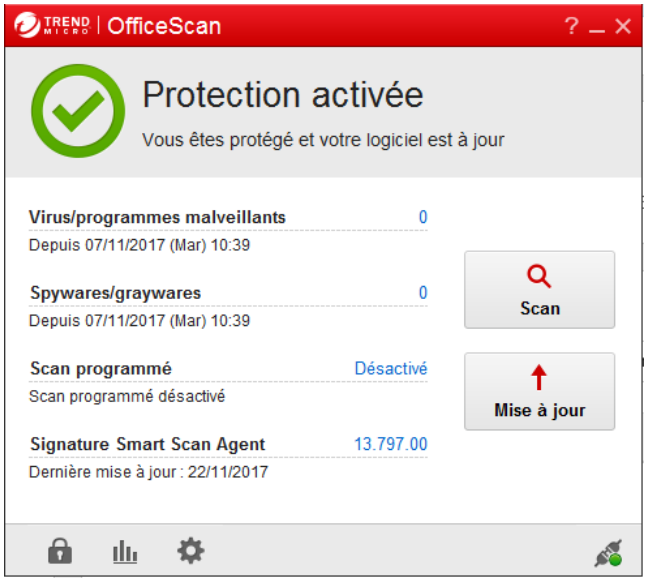


4- Vérification de la présence de l'Agent Trend sur le serveur :

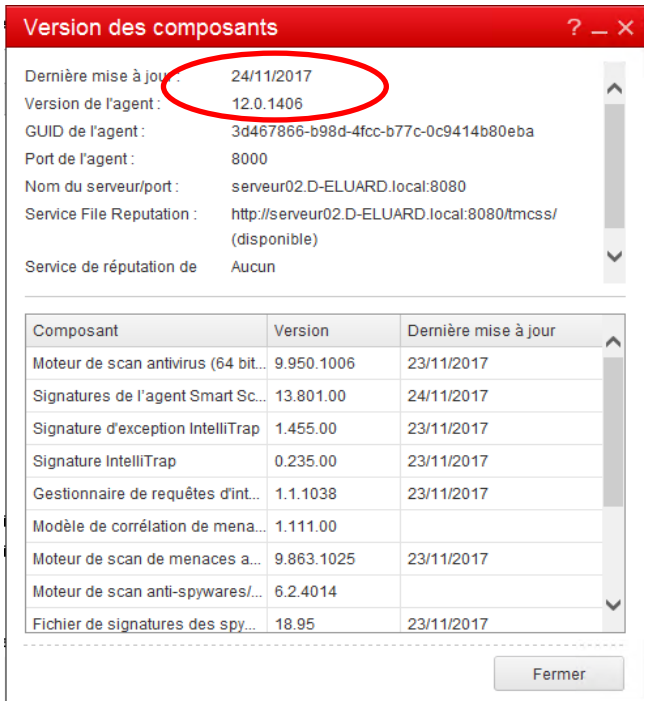
L'icône de l'Agent Trend est bien présente dans la zone de notification.



Dans le menu contextuel accessible avec un clic droit, on peut ouvrir la console de l'agent :



On peut aussi visualiser la version de l'agent, celle des différents moteurs de scan, la référence du fichier de signatures, les dates des dernières mises à jour, etc…



5- Installation des Patchs :

D'une manière générale, il est important de procéder à l'installation du dernier patch de la version française en vigueur.
Si un autre patch plus ancien est requis, l'installation s'arrête. Un message indique alors la marche à suivre.

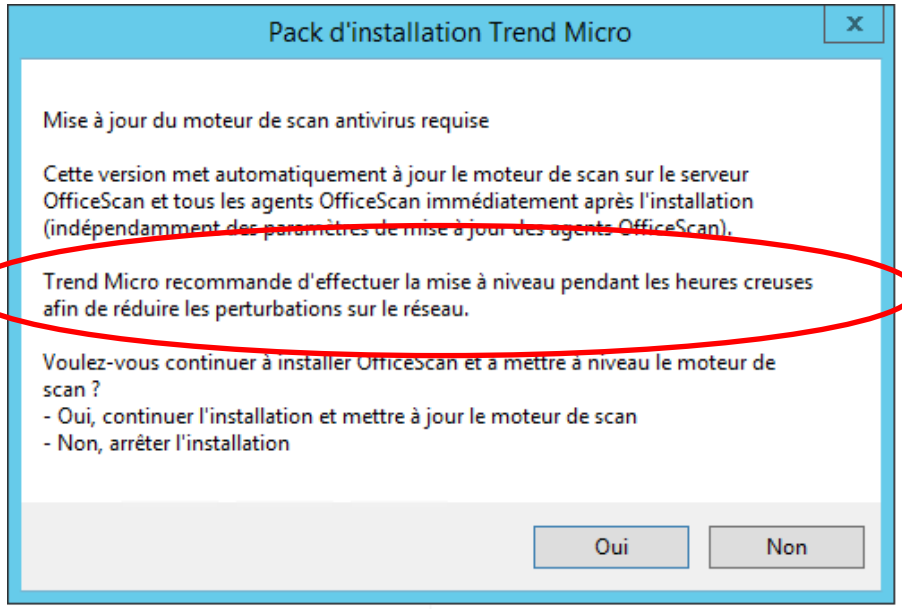
Ces patchs sont disponibles sur le même site de téléchargement que la version complète : http://downloadcenter.trendmicro.com/index.php?regs=fr&clk=latest&clkval=4973&lang_loc=2

A ce jour, il faut installer dans cet ordre :

- Product Patch (osce-xg-win-fr-patch1-1576.exe)
- Critical Patch (osce-xg-win-fr-criticalpatch-1775.exe)

Ne pas oublier de débloquer les archives.

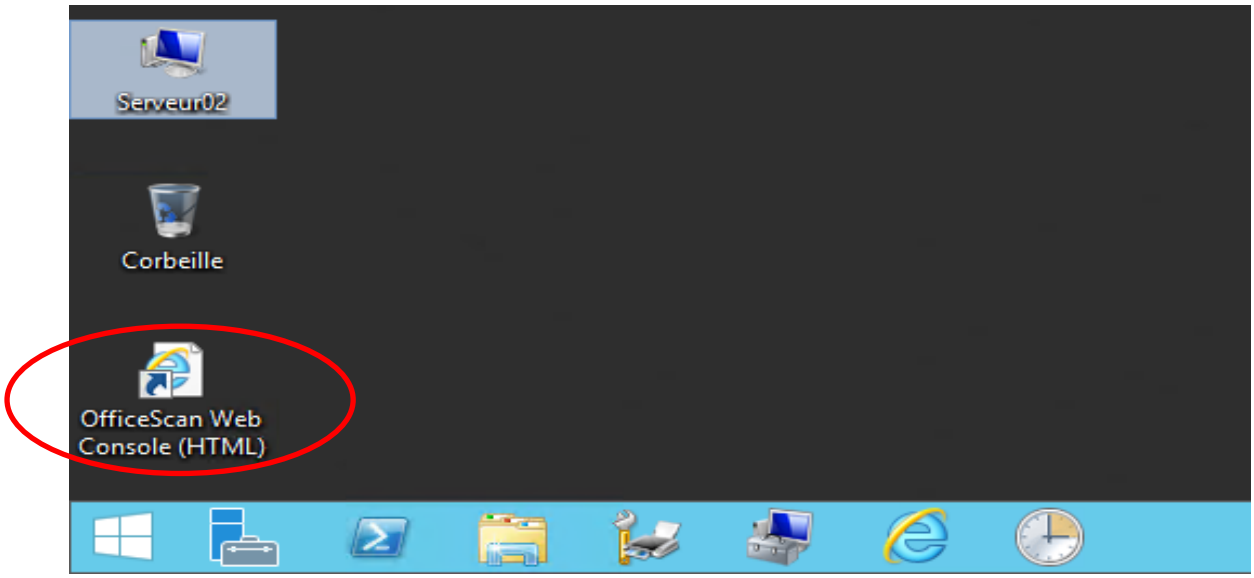
L'installation ne présente pas de difficulté particulière. Il suffit généralement, de valider les options proposées par défaut.
Attention toutefois aux avertissements, comme celui obtenu lors de l'installation du patch 1775 :



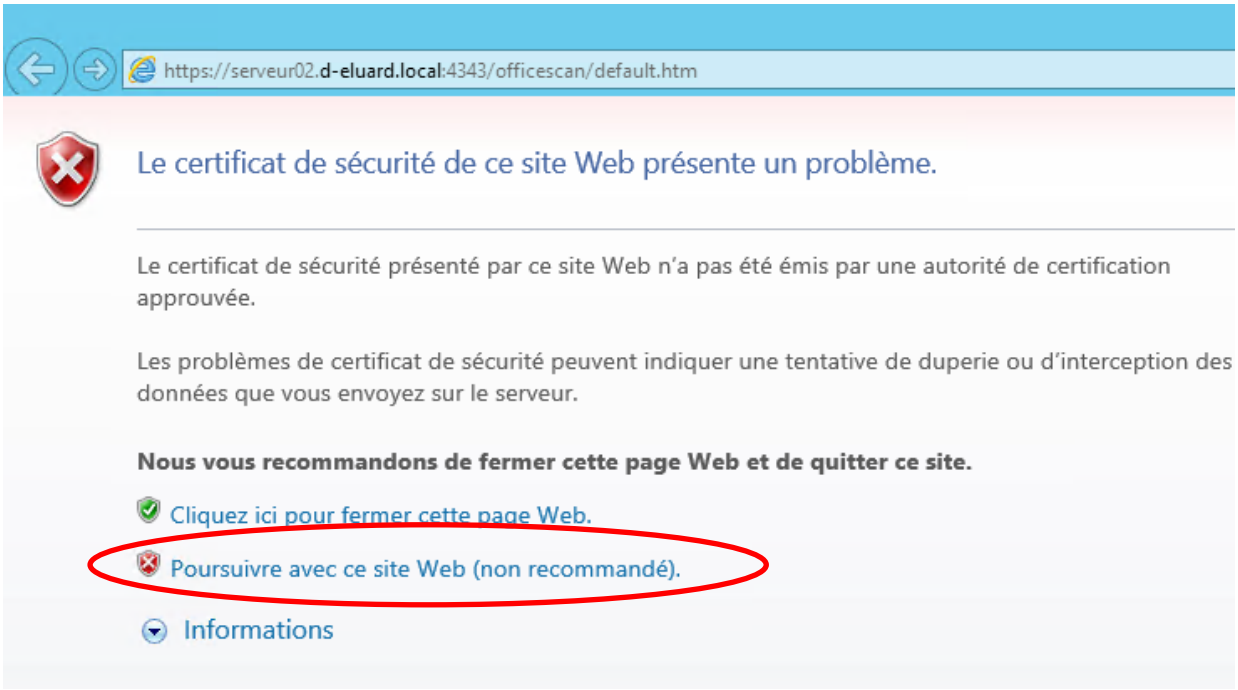
Des perturbations sur le réseau, sont à craindre. En cas de doute ne pas hésiter à reporter l'installation à une date à laquelle le réseau sera moins sollicité.

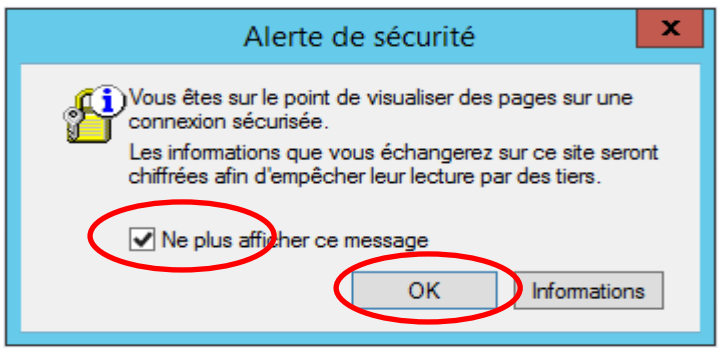
6- Ouverture de la console Web OfficeScan :

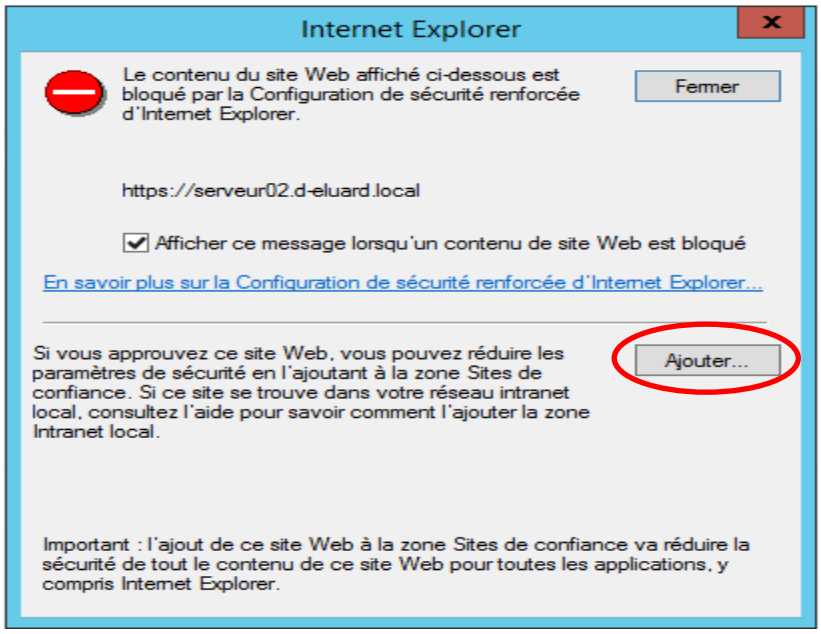
Une nouvelle icône est présente sur le bureau :



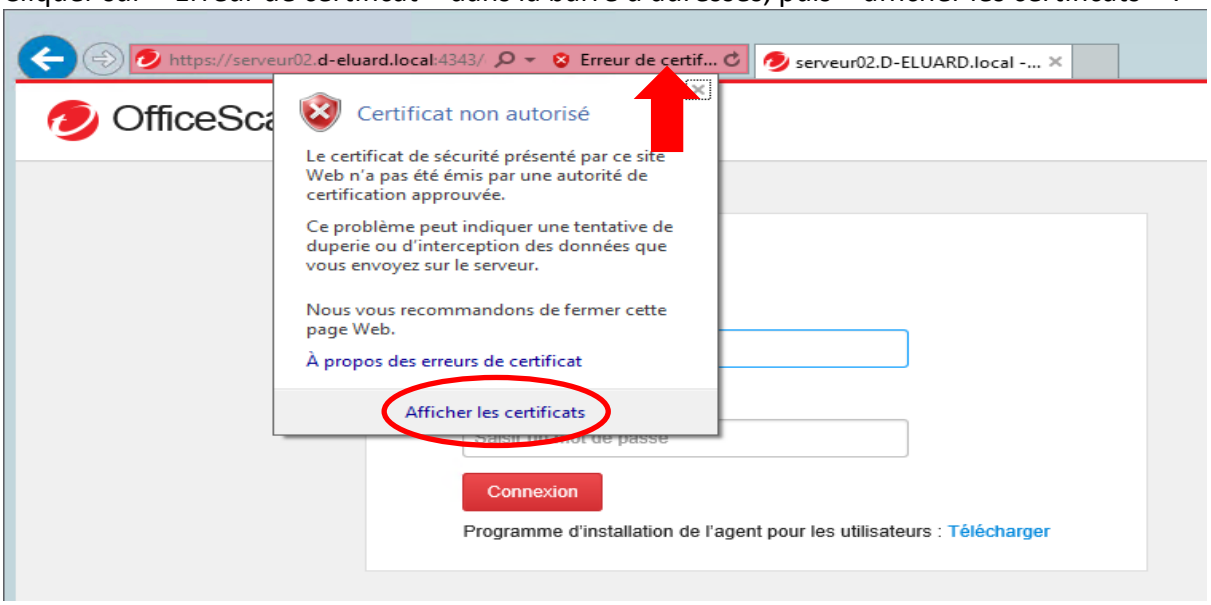
Au démarrage de la console : https://serveurxx.d-xxxxx.local:4343/officescan/
On obtient un avertissement de sécurité, faire « Poursuivre avec ce site Web » :



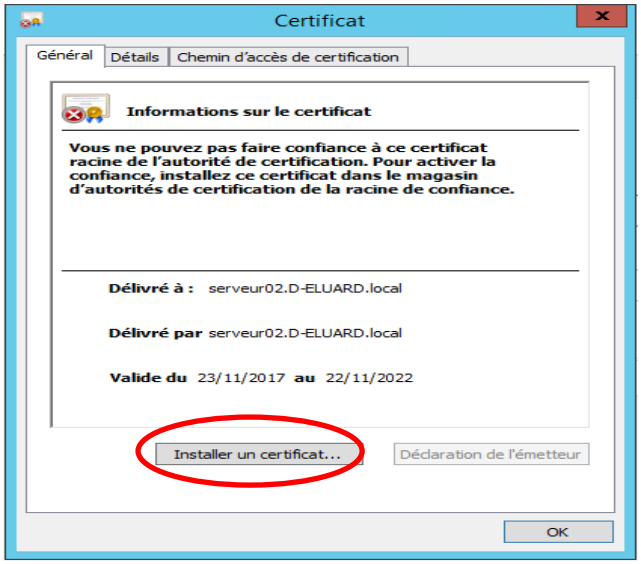


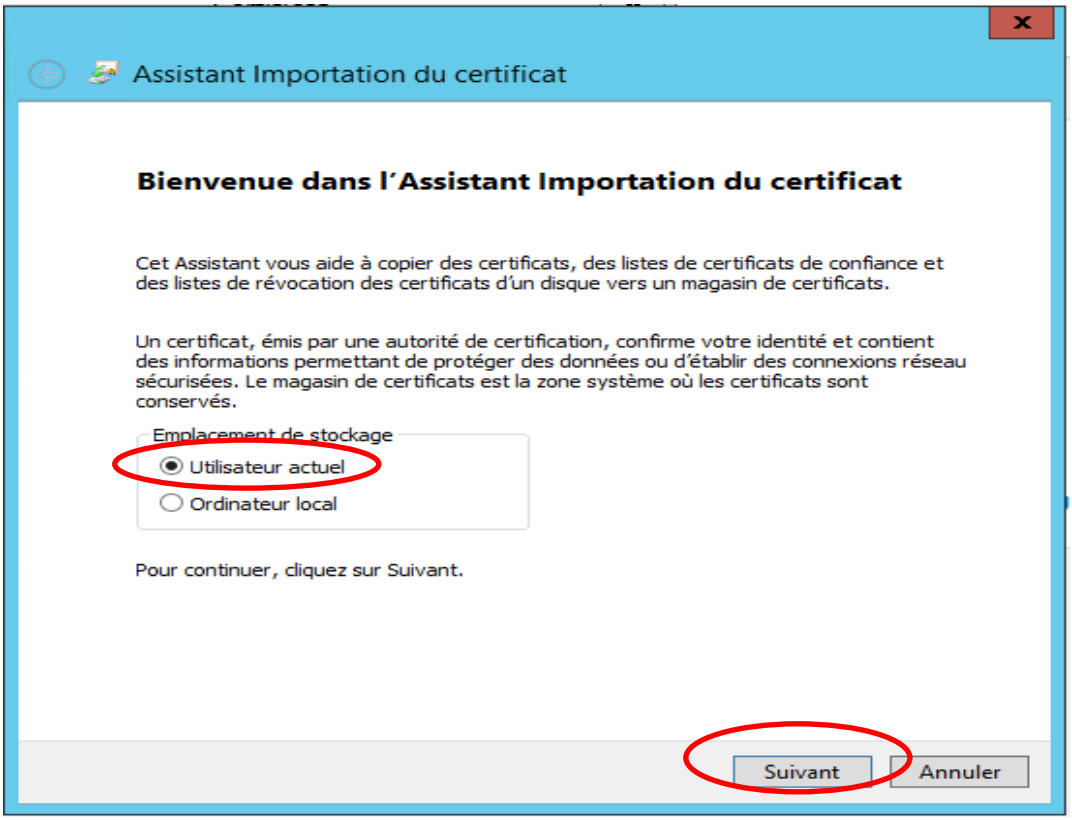


Cliquer sur « Erreur de certificat » dans la barre d'adresses, puis « afficher les certificats » :

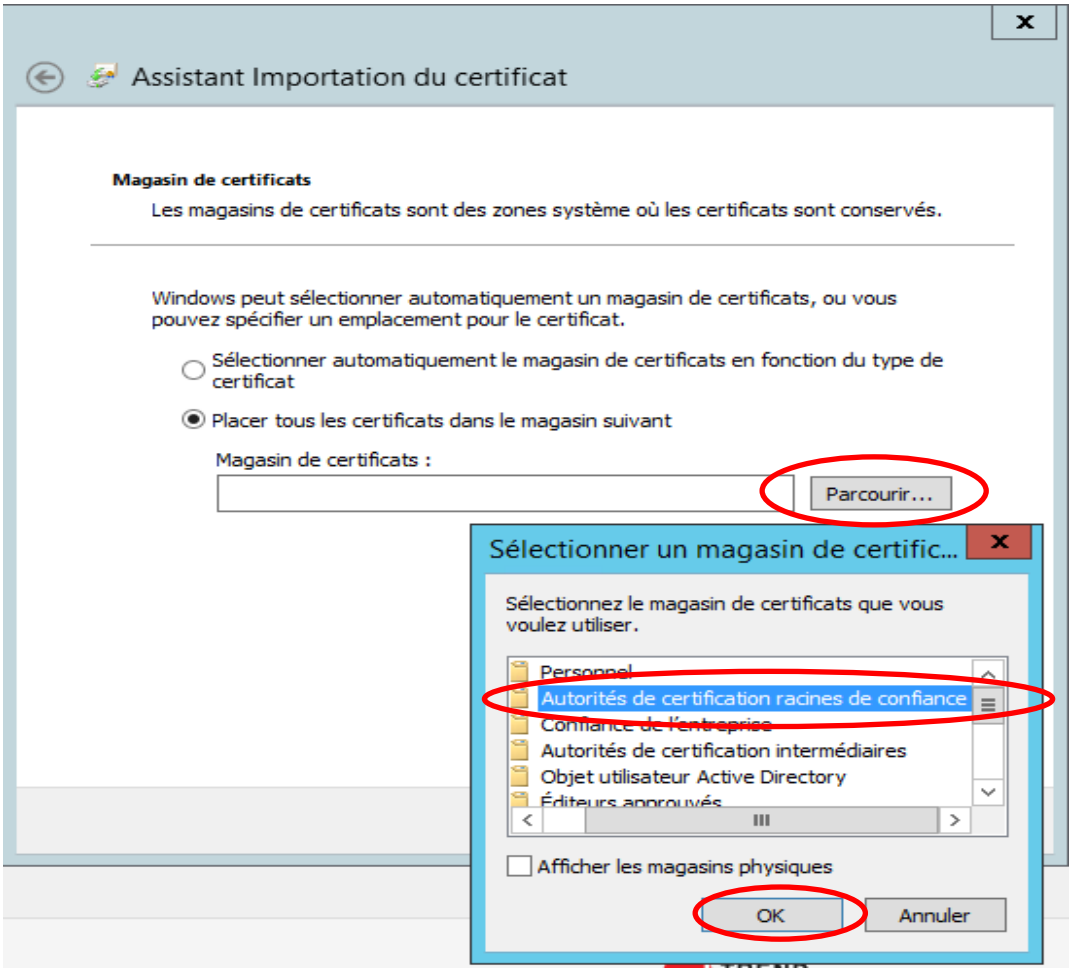


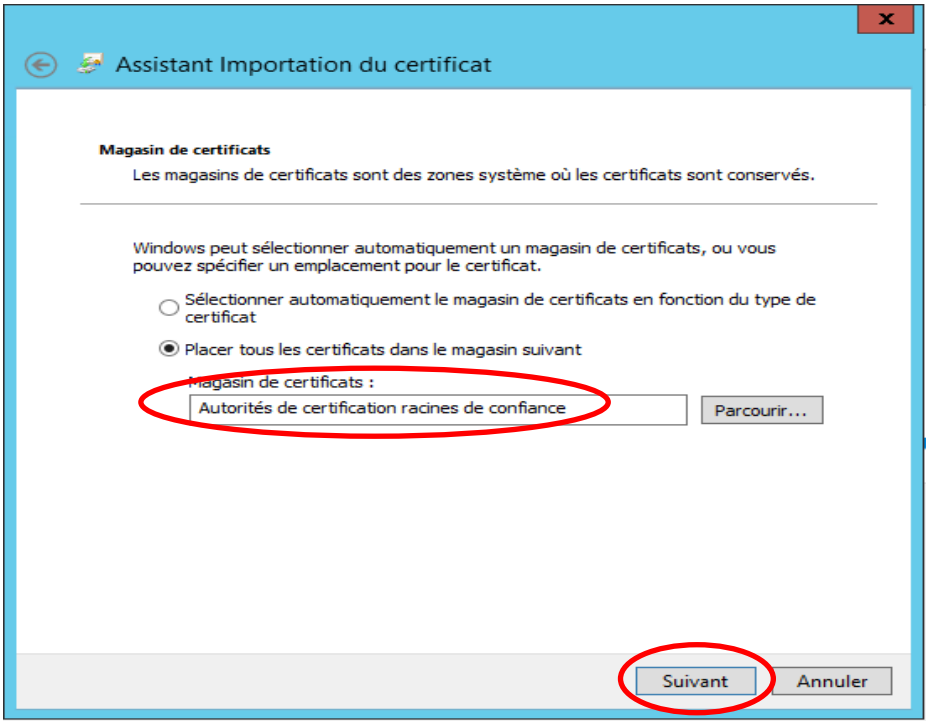
Faire : « Installer le certificat » :

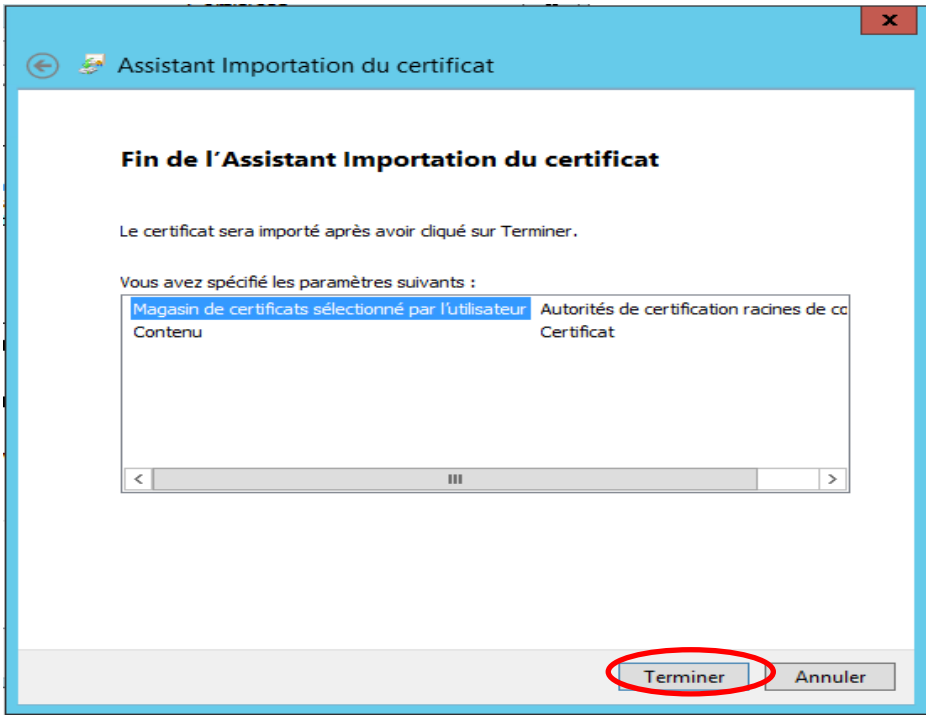


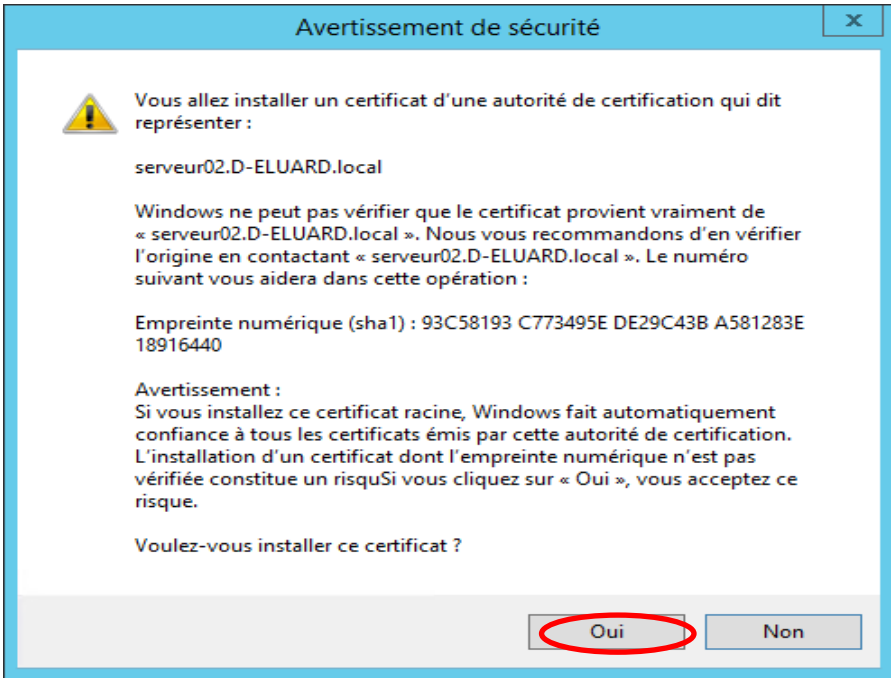


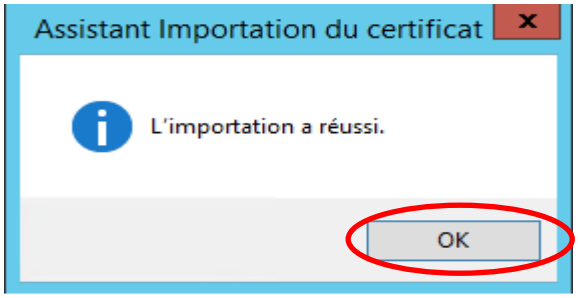
Choisir « Autorités de certification racine de confiance » :



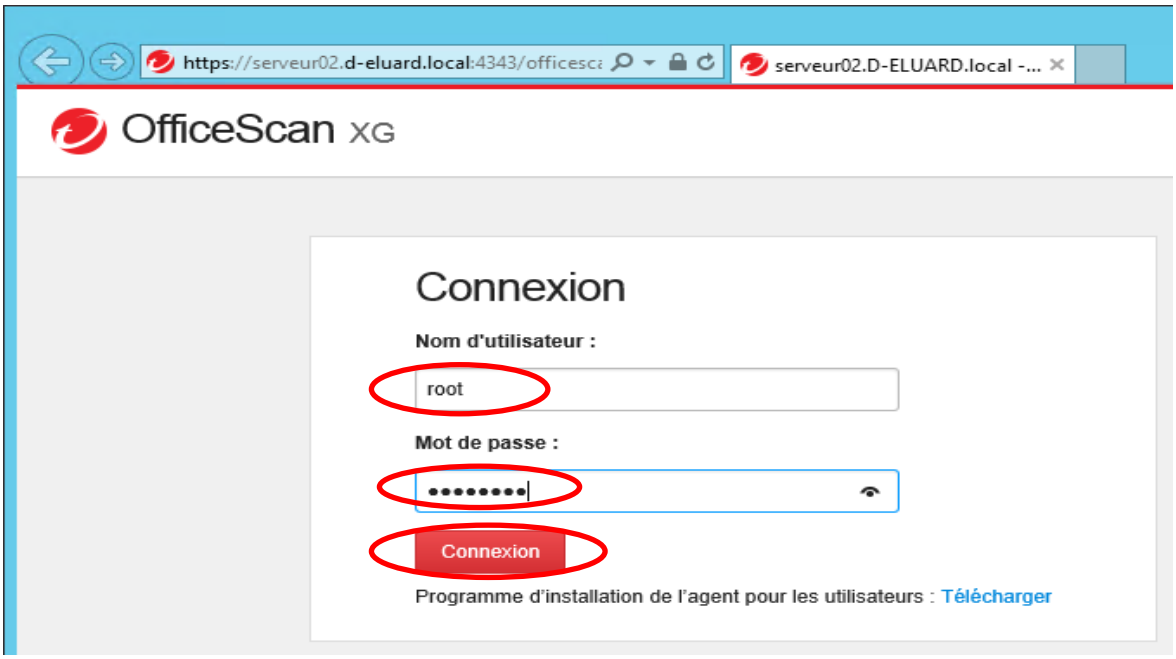

Assistant Importation du certificat
Magasin de certificats
Les magasins de certificats sont des zones système où les certificats sont conservés.
Windows peut sélectionner automatiquement un magasin de certificats, ou vous pouvez spécifier un emplacement pour le certificat.
Sélectionner automatiquement le magasin de certificats en fonction du type de certificat
Placer tous les certificats dans le magasin suivant
Magasin de certificats :
Autorités de certification racines de confiance
Parcourir...
Suivant
Annuler


Assistant Importation du certificat
Fin de l'Assistant Importation du certificat
Le certificat sera importé après avoir cliqué sur Terminer.
Vous avez spécifié les paramètres suivants :
Magasin de certificats sélectionné par l'utilisateur
Autorités de certification racines de cc
Contenu
Certificat
Terminer
Annuler

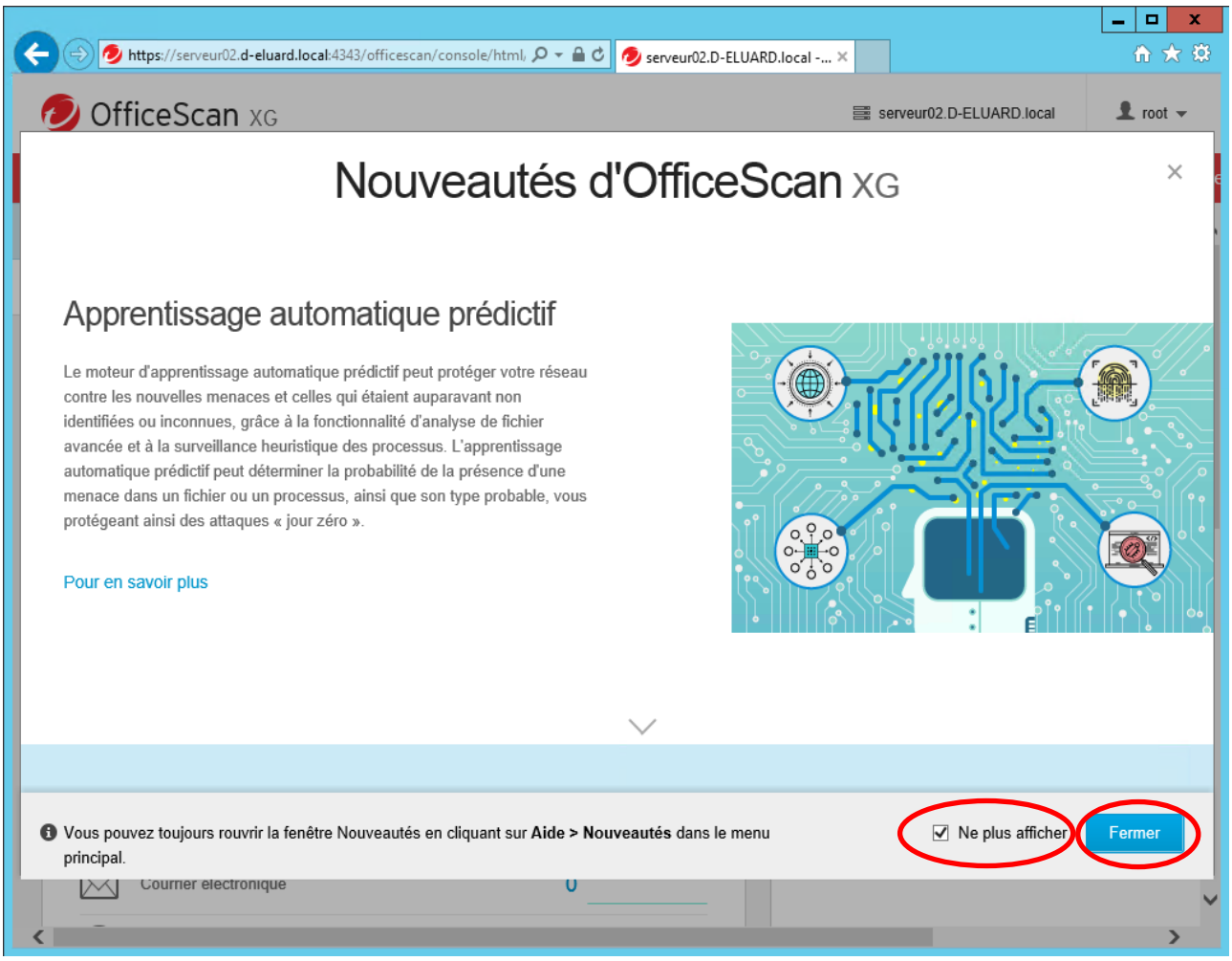




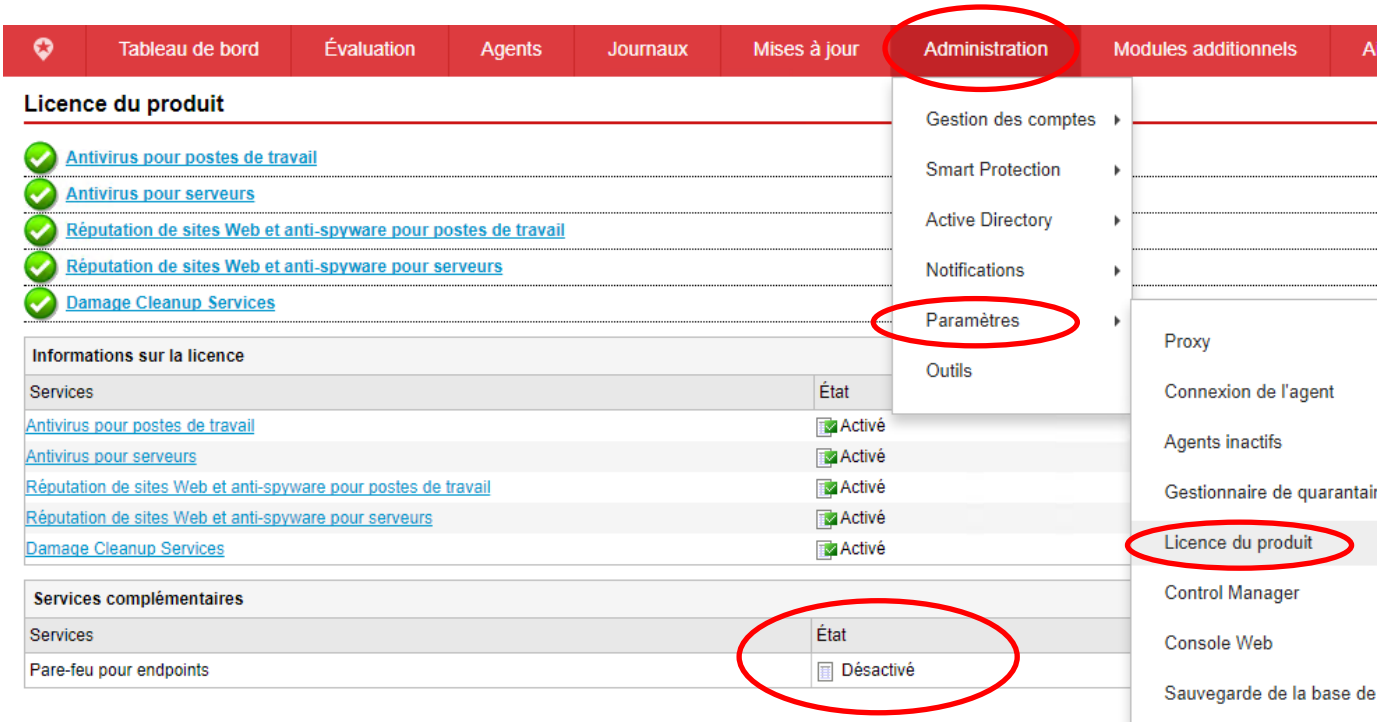
Au lancement suivant de la console le message d'erreur concernant le certificat a disparu. S'identifier avec le compte root :



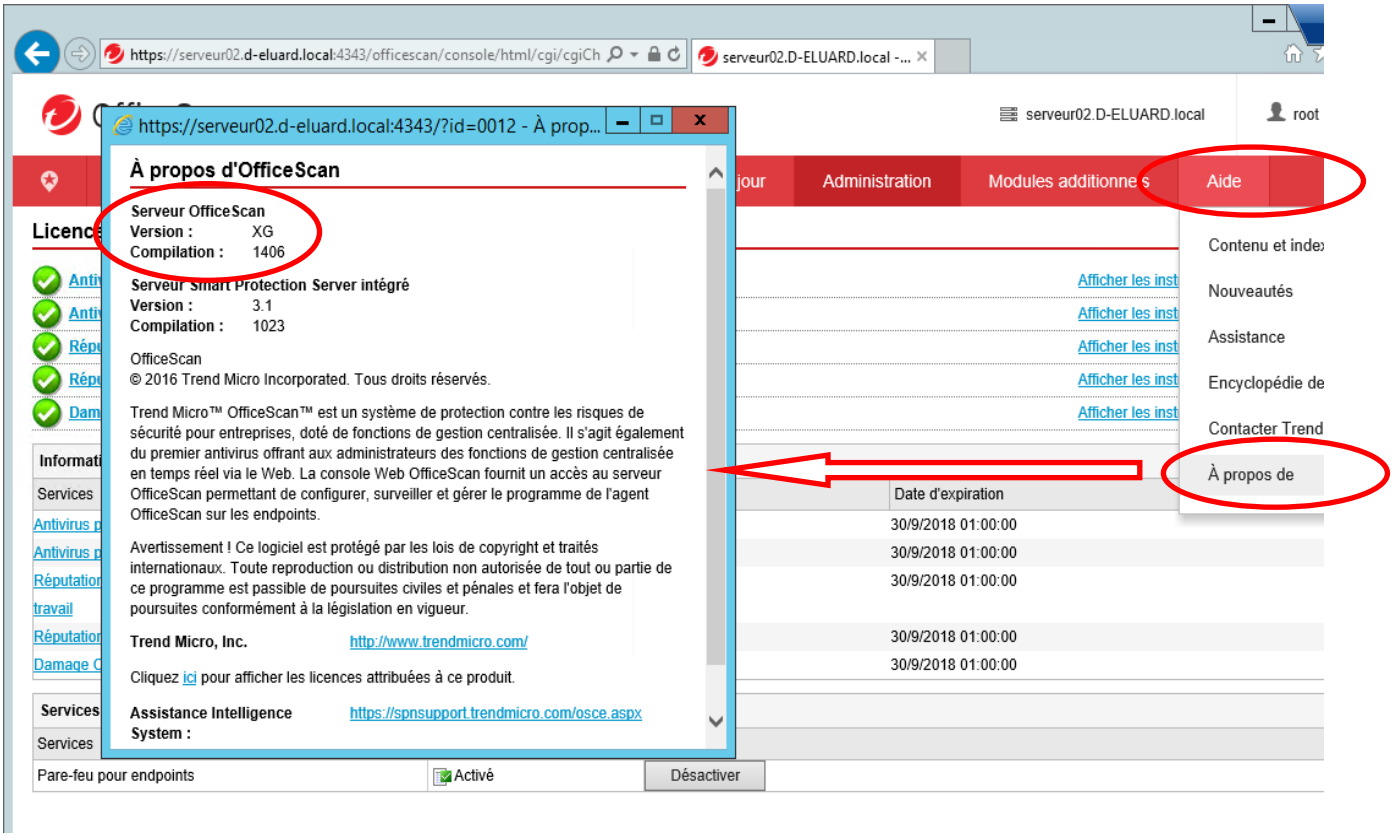
Une fenêtre présente les nouveautés d'OfficeScan XG. Cocher « Ne plus afficher » puis « Fermer » :



Dans le menu « Administration », « Paramètres », « Licence du produit » : tous les produits doivent être activés sauf le Parefeu :



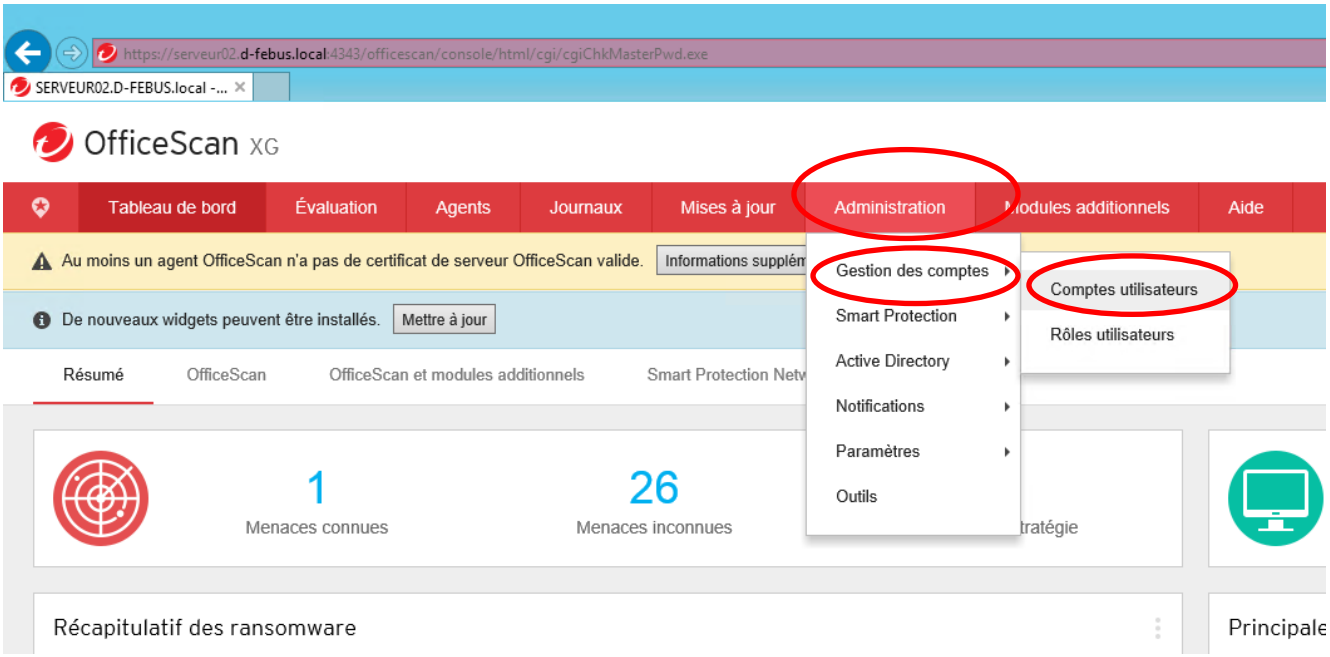
Dans le menu « Aide », « A propos de », on peut vérifier l'installation de la version XG :



7- Paramétrage de Trend OfficeScan :

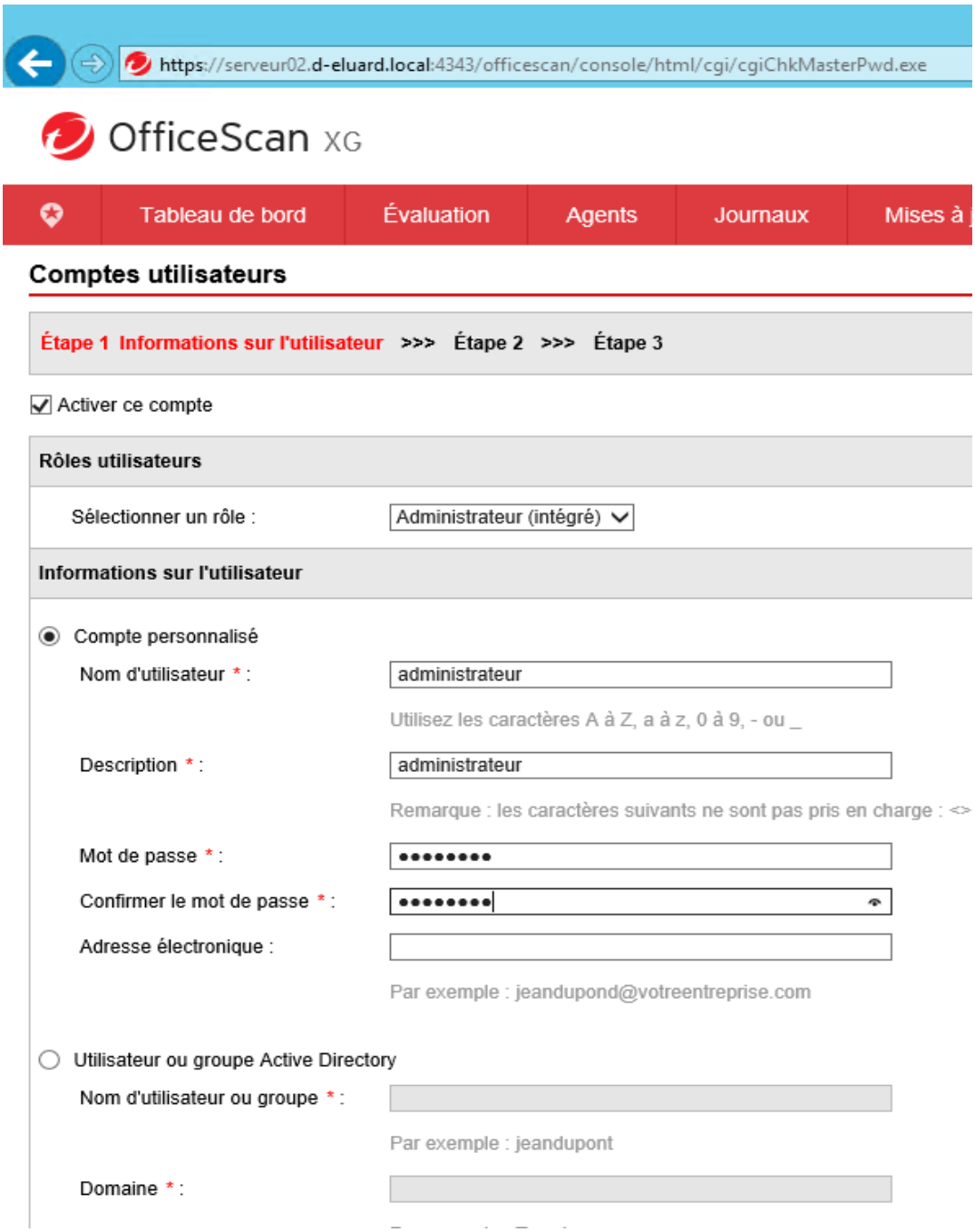
7-1 Menu Administration :

Administration… Gestion des Comptes… Comptes utilisateurs…



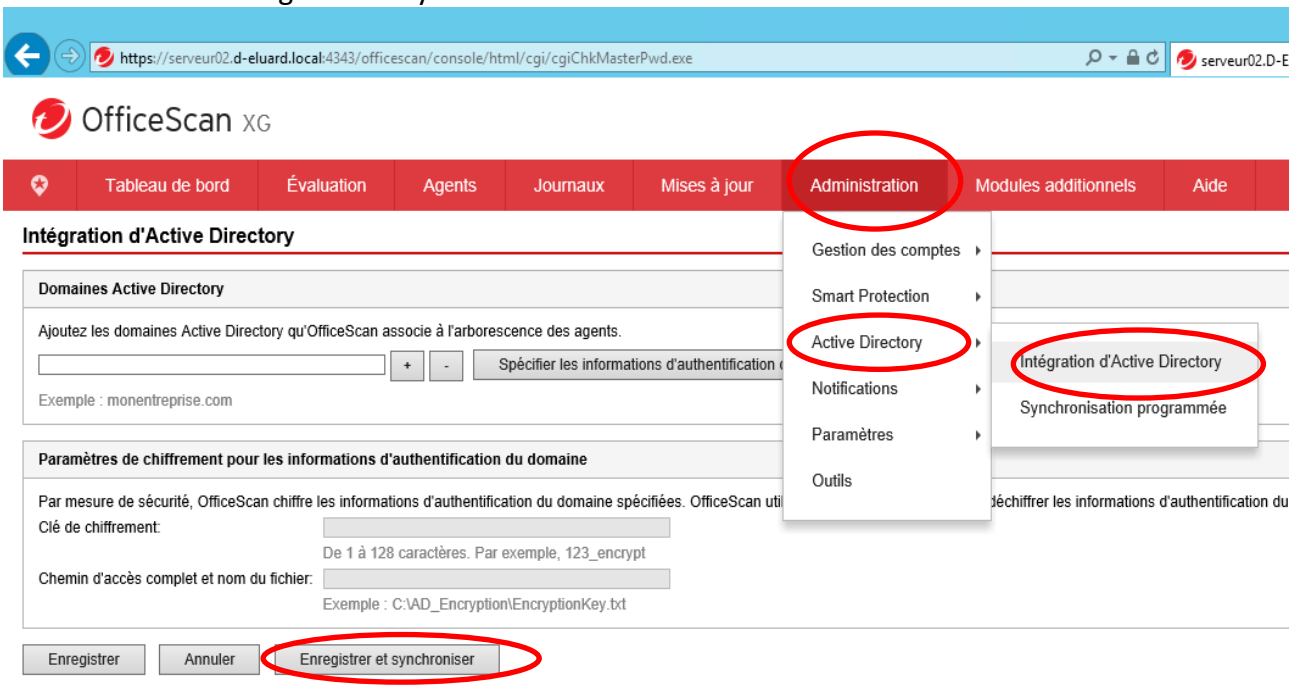
On pourra ici, changer le mot de passe du compte root, si cela s'avère nécessaire :

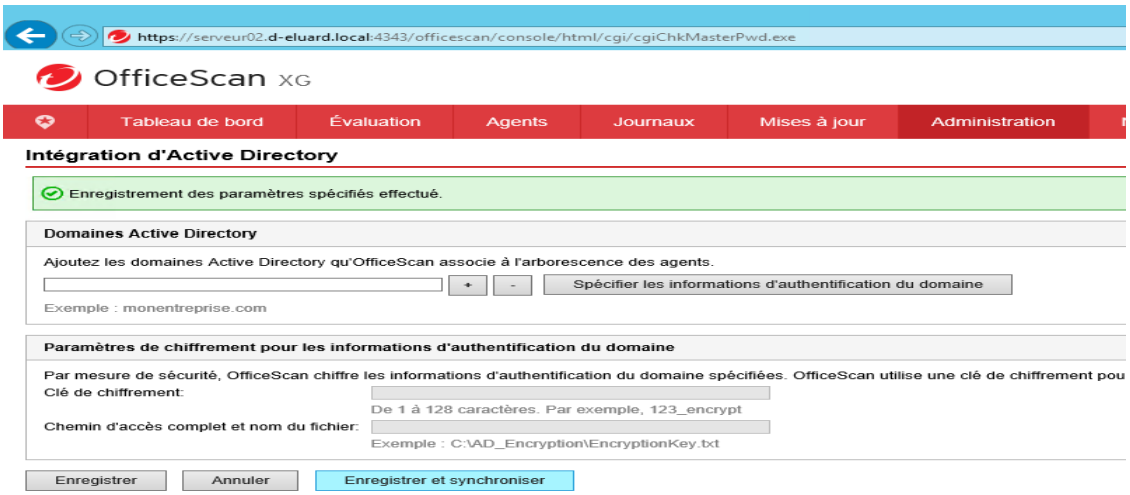
Ajouter un compte Administrateur (utile en cas de perte du mot de passe du compte root) :



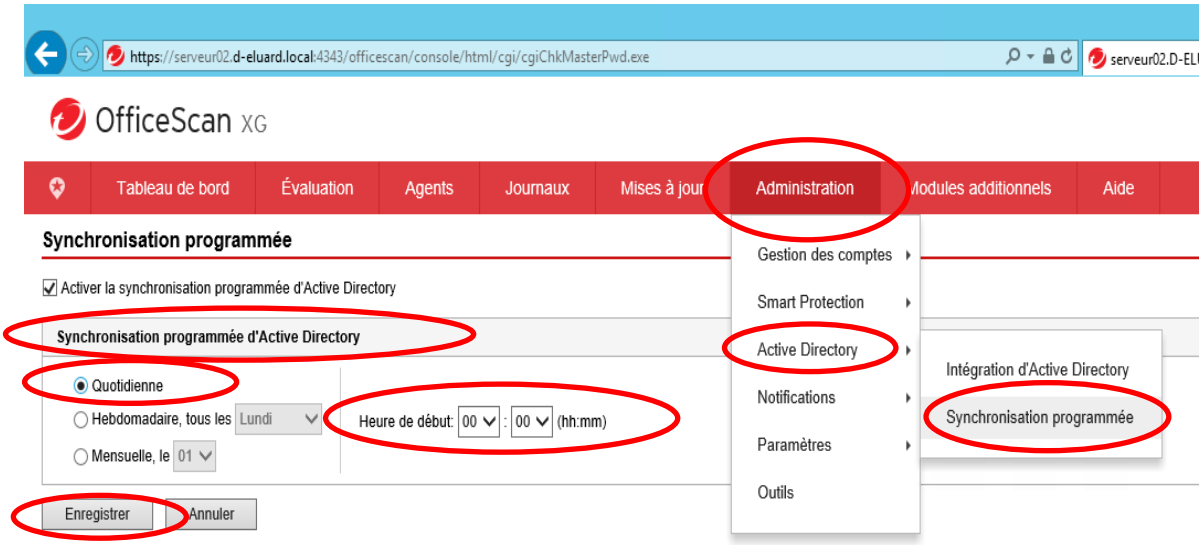
Administration… Active Directory… Intégration Active Directory…

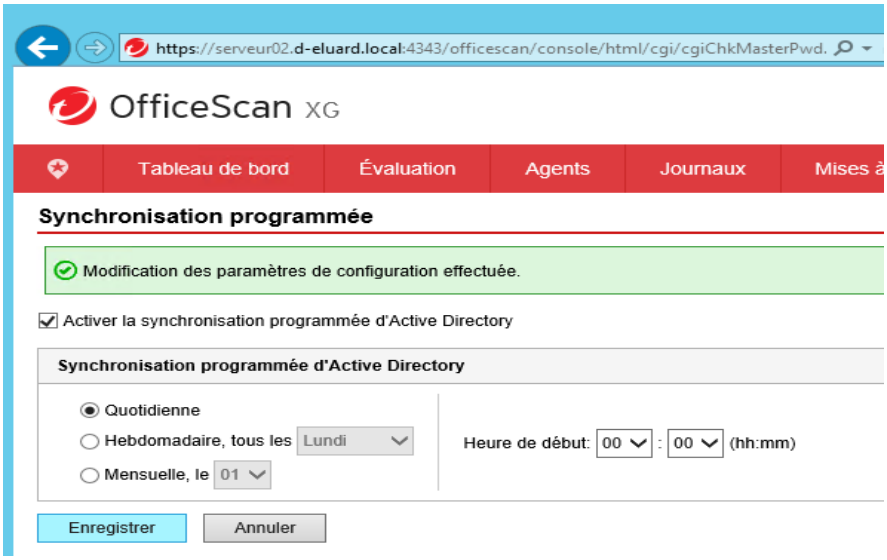
Faire « Enregistrer et synchroniser » :





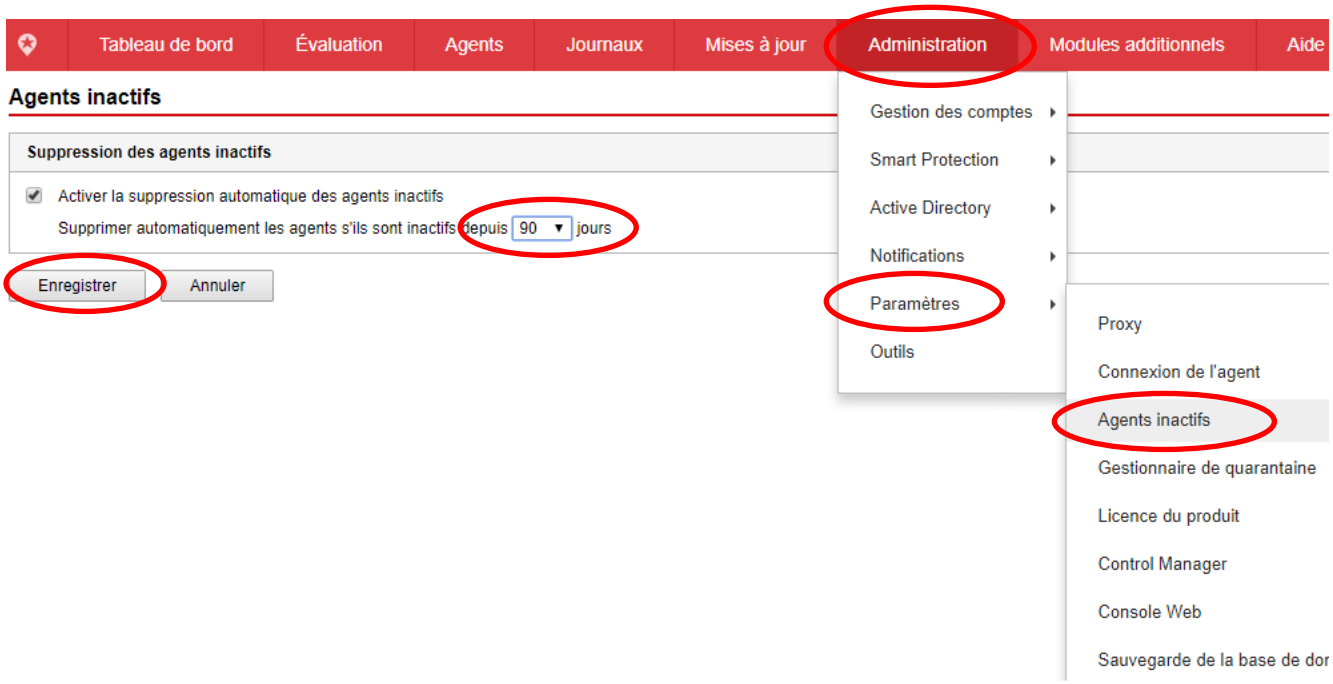
Administration… Active Directory… Synchronisation programmée…

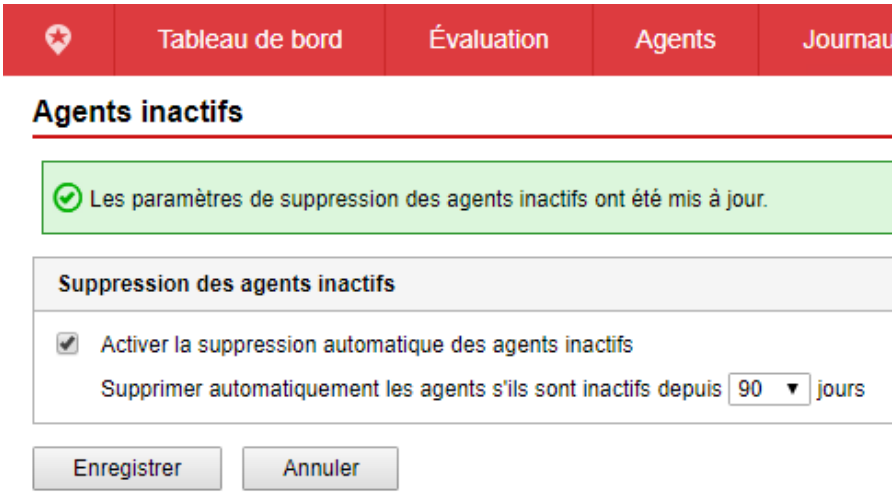




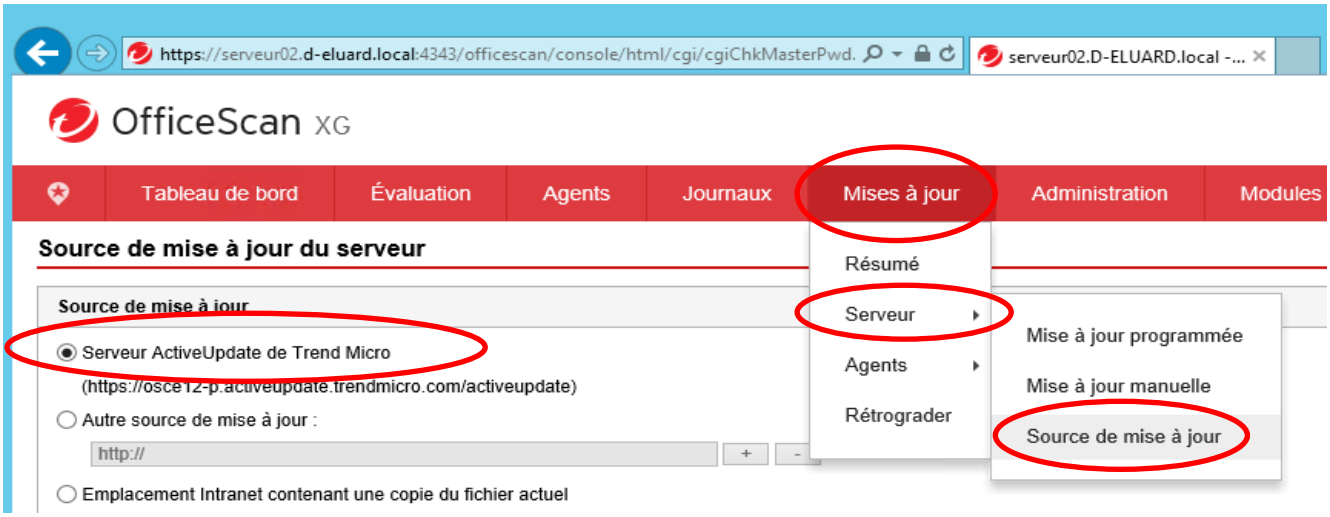
Administration… Paramètres… Agents inactifs…

Activer la Suppression automatique des agents, inactifs depuis plus de **90** jours :

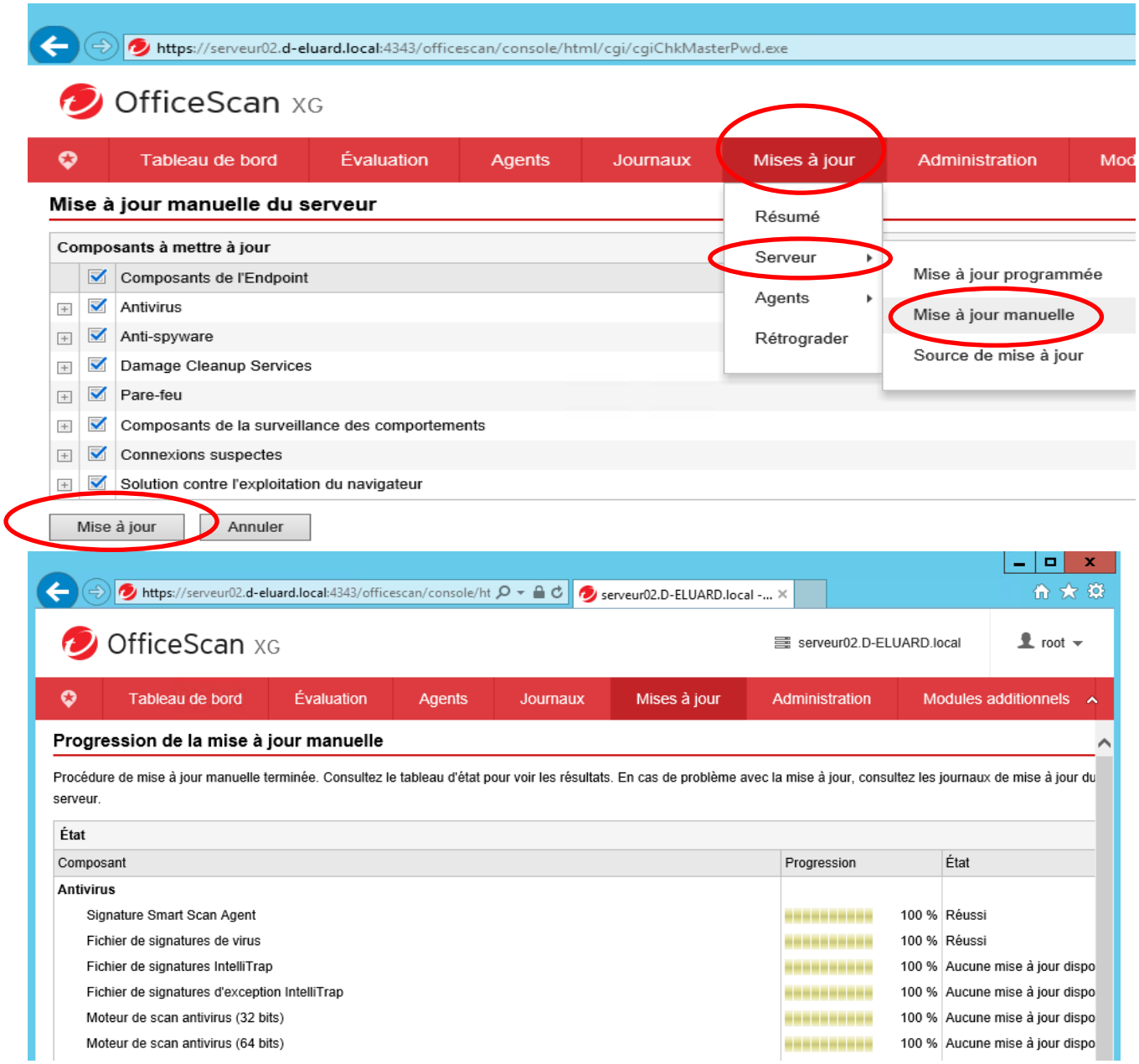




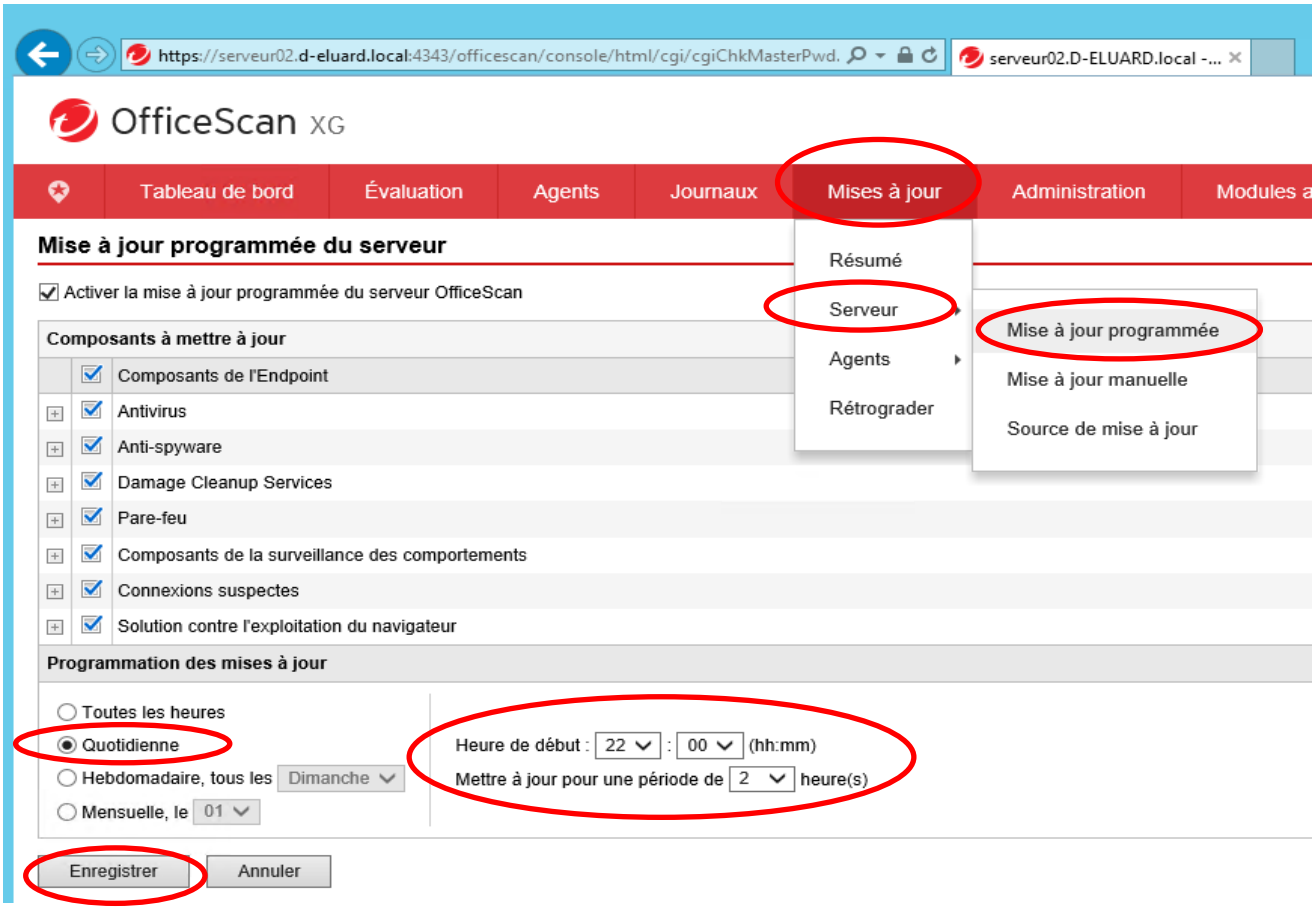
7-2 **Menu « Mises à jour » :** **Mises à jour… Serveur… Source de mise à jour…**

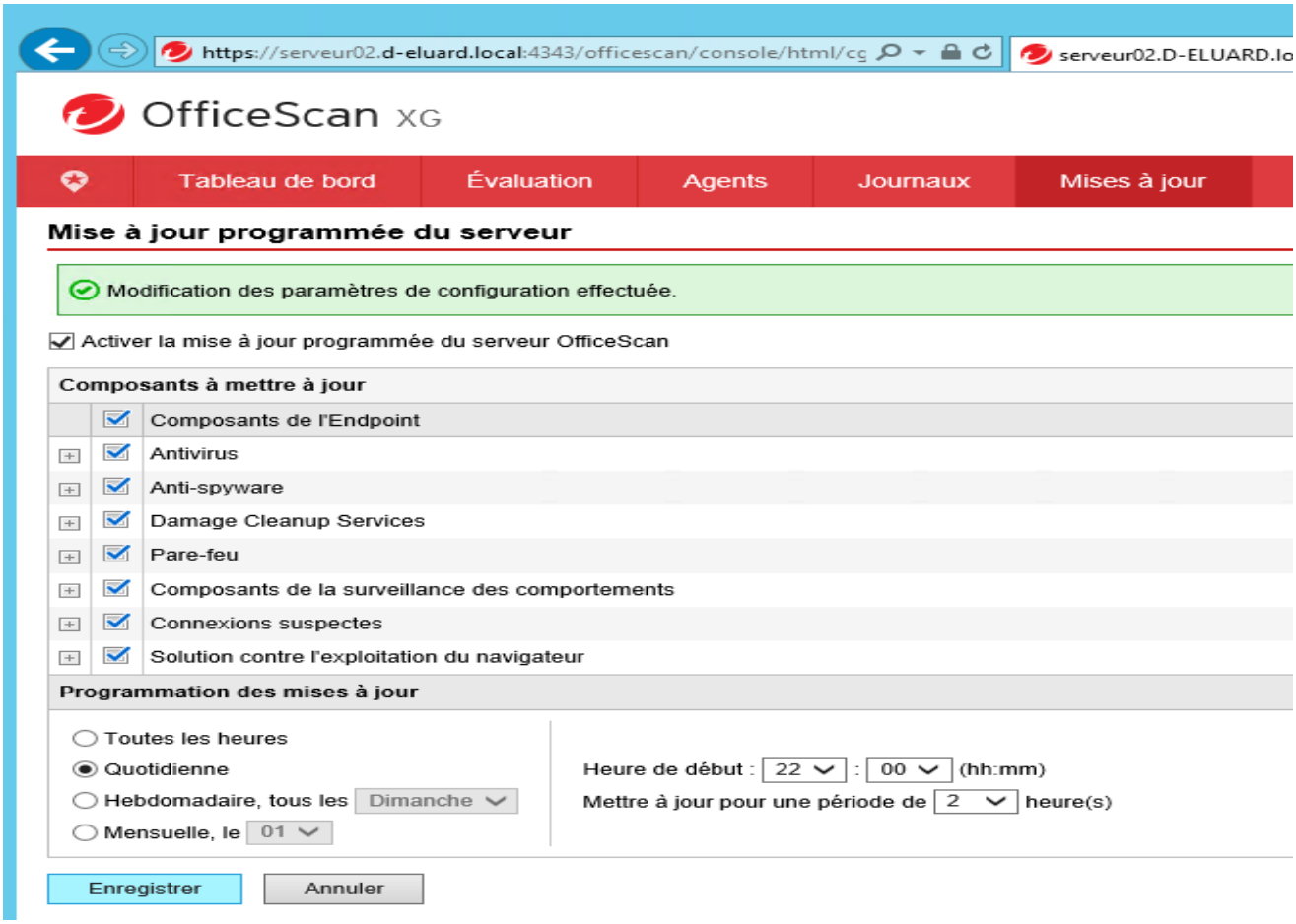


Mises à jour… Serveur… Mise à jour manuelle… cliquer sur « Mise à jour » :

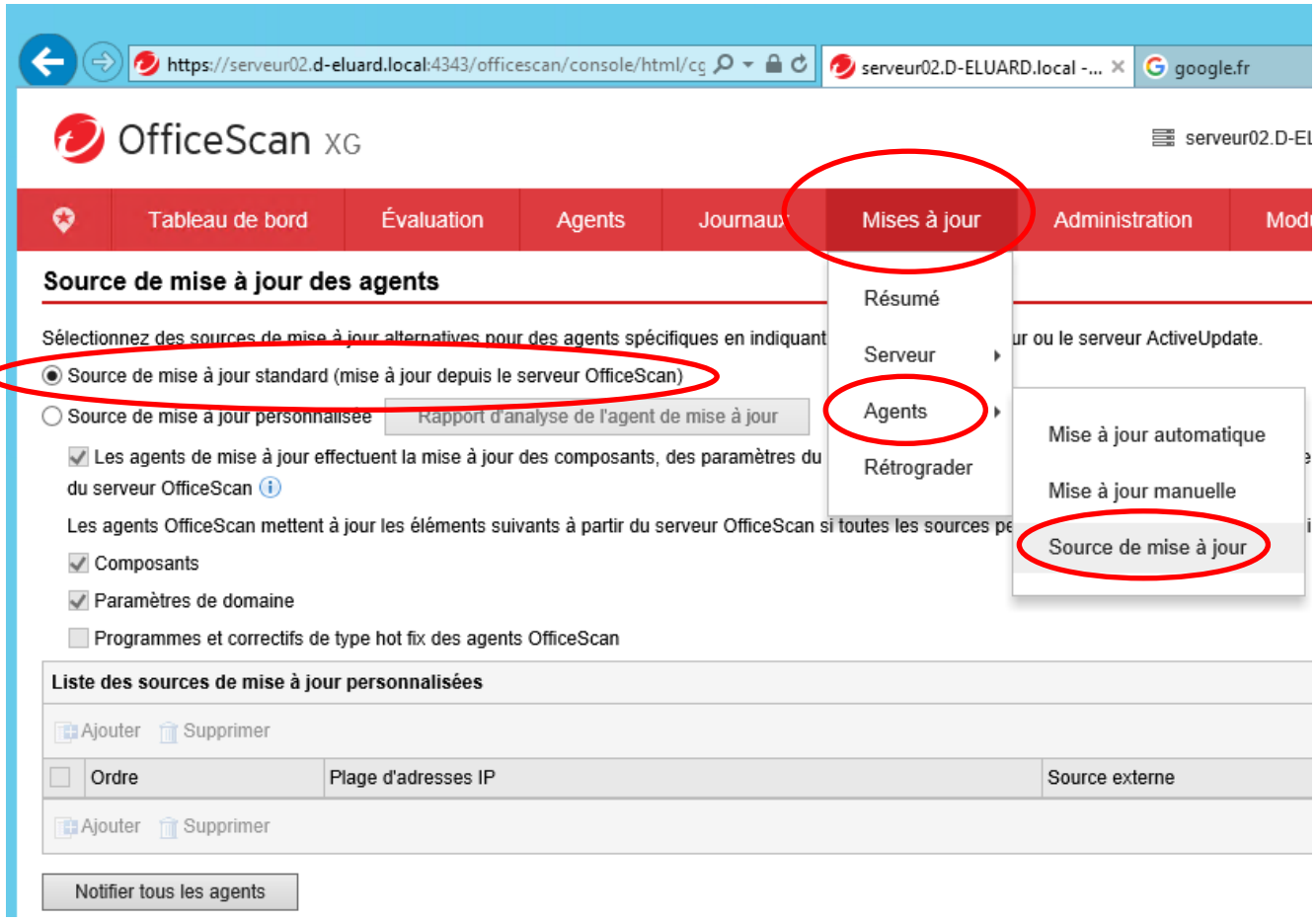


Mises à jour… Serveur… Mise à jour programmée…

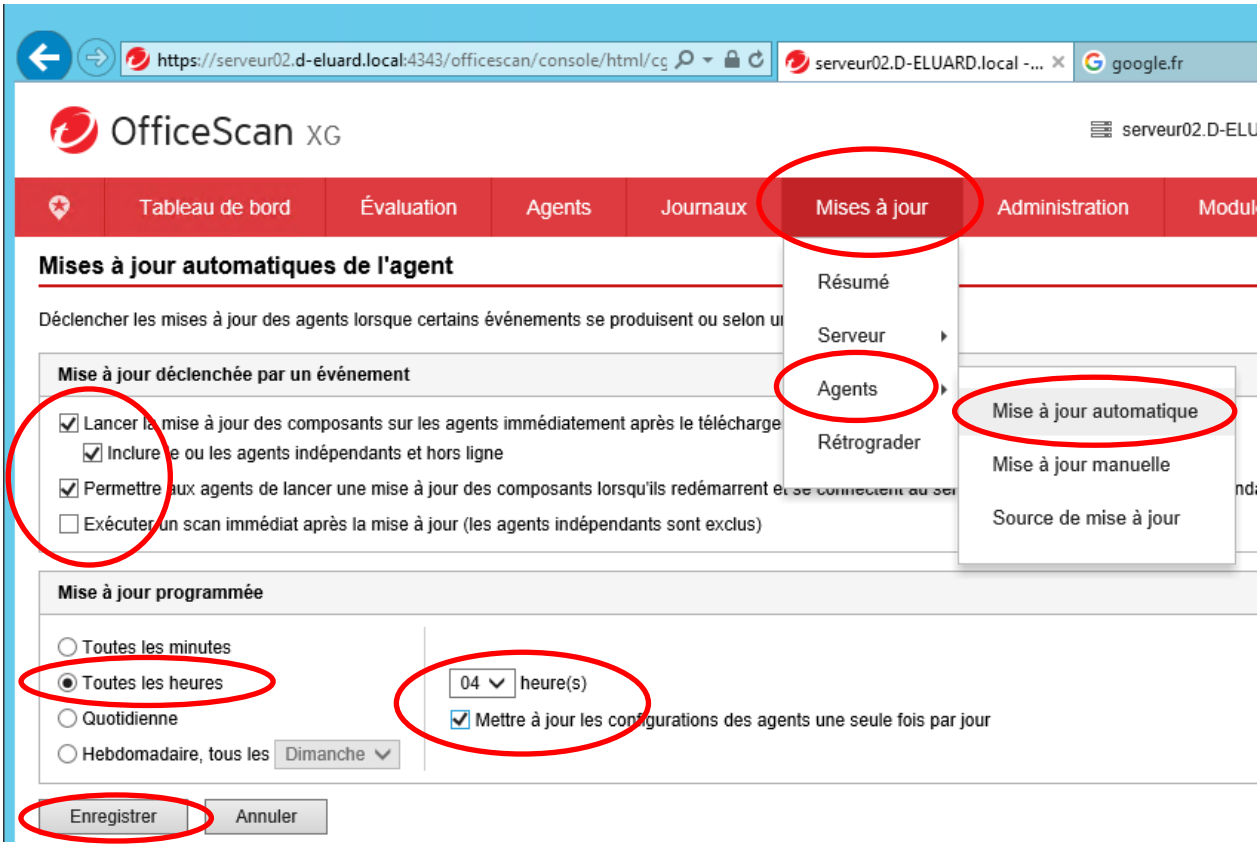




Mises à jour… Agents… Source de mise à jour… simple vérification :



Mises à jour… Agents… Mise à jour automatique…



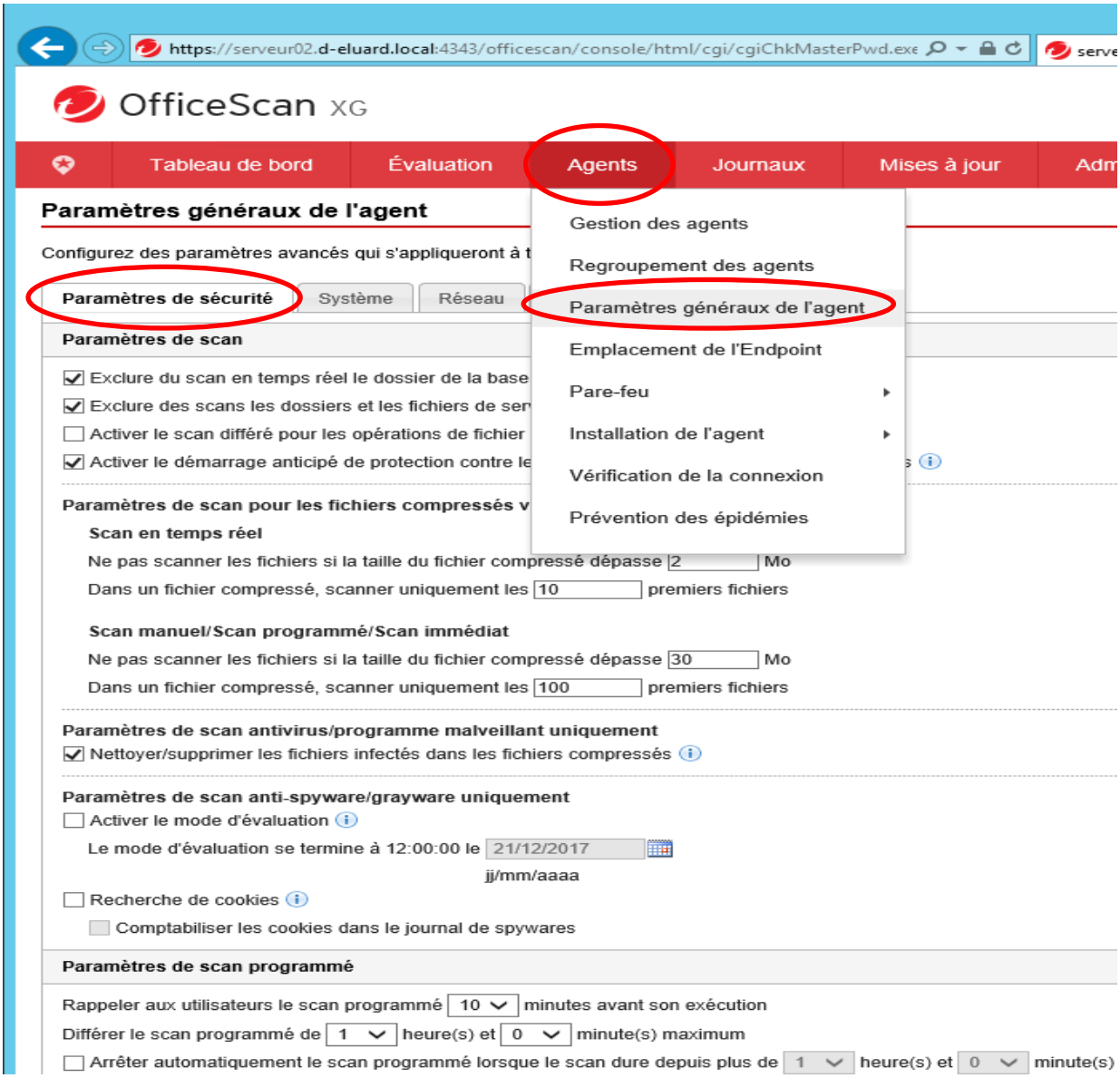
7-3 Menu « Agents » :

Agents… Regroupement des agents…

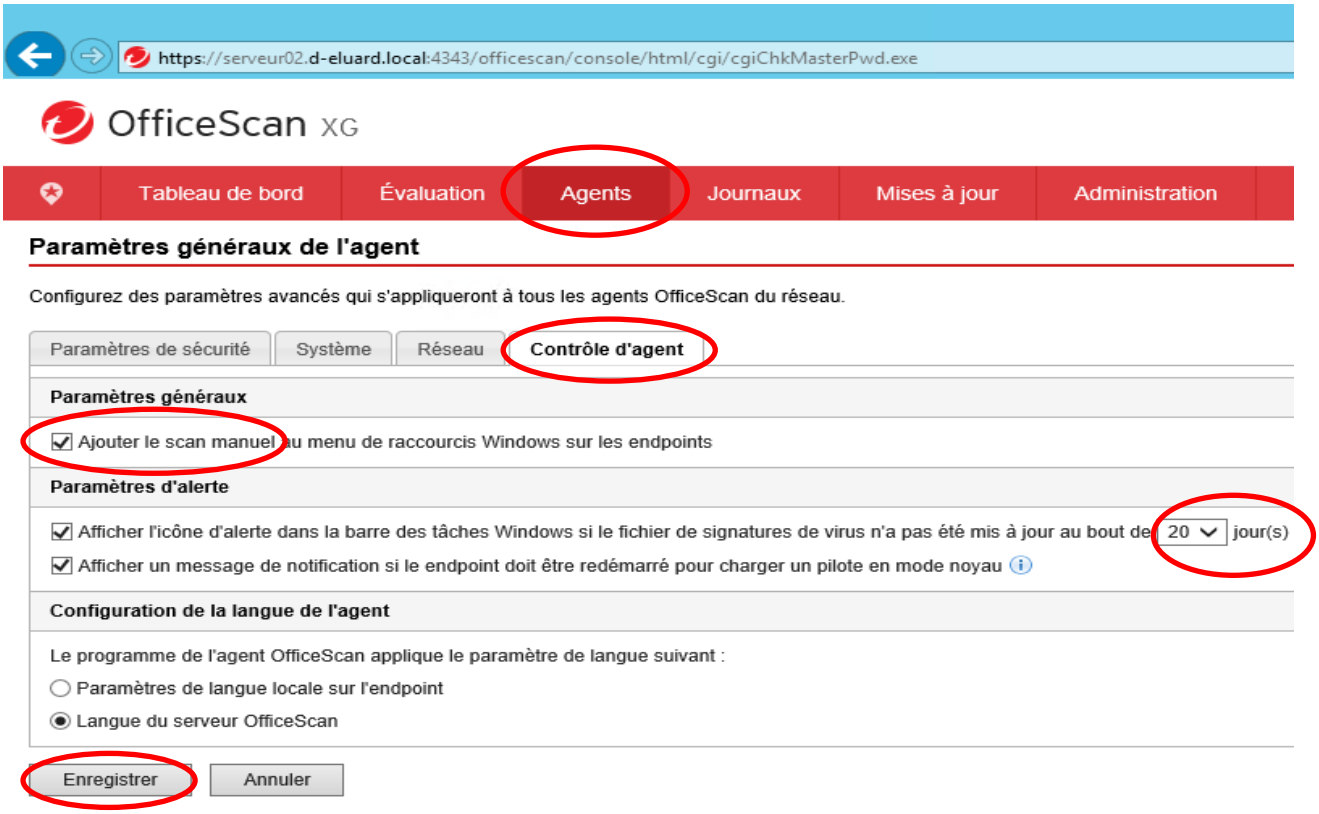
Regrouper les agents suivant leur appartenance au domaine :

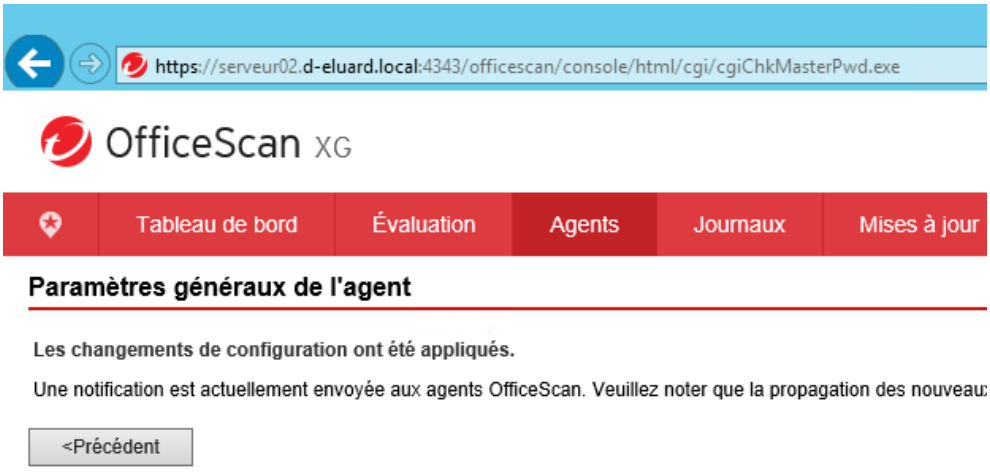
Agents… Paramètres généraux de l'agent… Paramètres de sécurité…

Pas de modifiactions dans cet onglet :



Agents… Paramètres généraux de l'agent… Contrôle d'agent…
Ajouter le scan manuel pour les utilisateurs , et fixer le délais d'alerte à 20 jours.



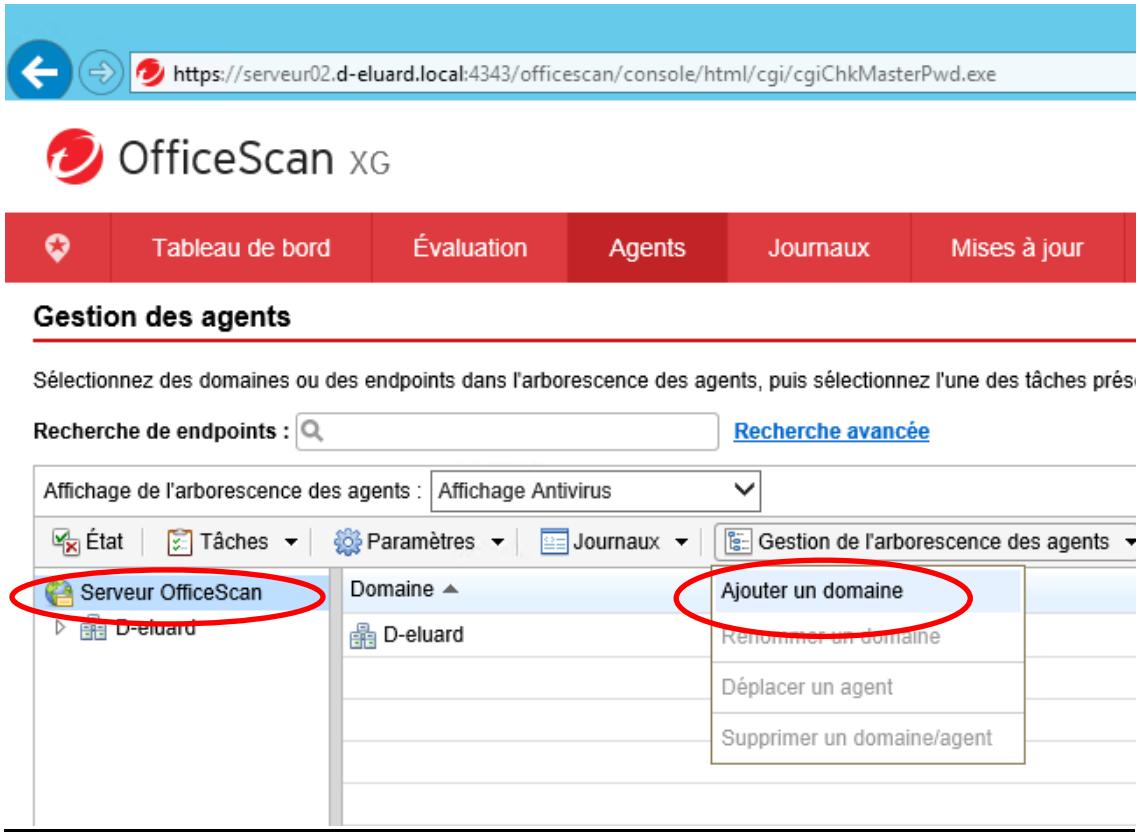


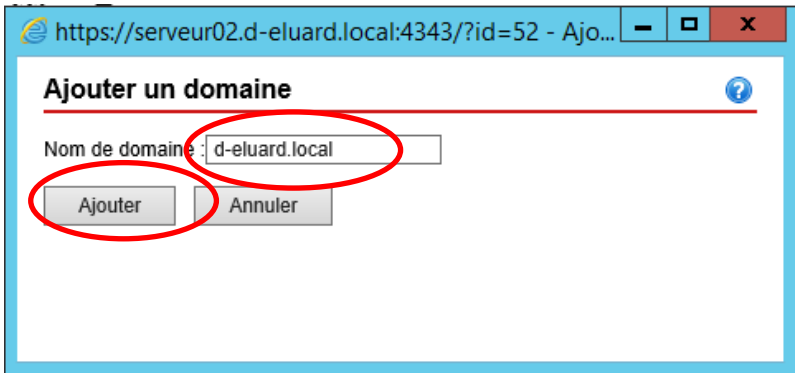
7-4 Gestion des agents :

7-4.1 Gestion de l'arborescence des agents :

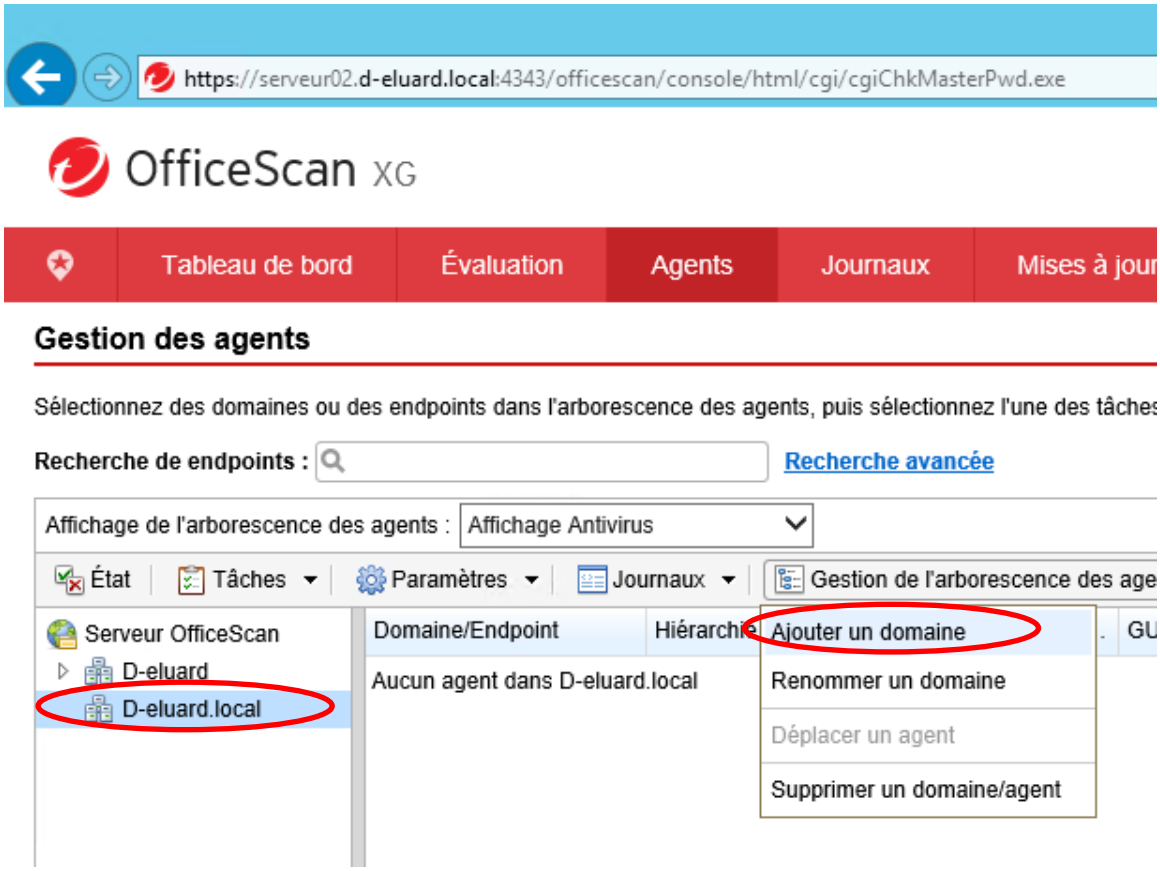
Nous allons regrouper les agents des stations et des serveurs dans un même domaine.
Les serveurs pourront être regroupés dans un sous-ensemble « Serveurs ».

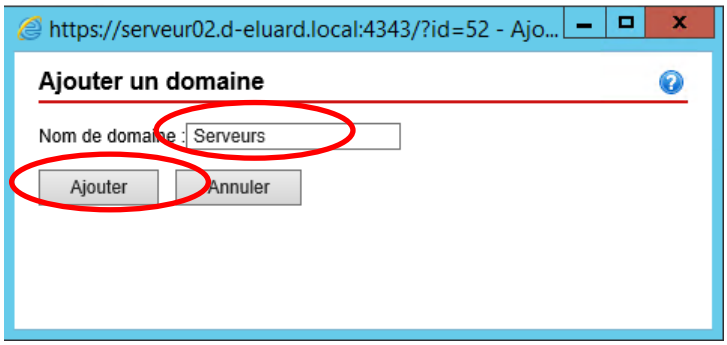
S'il n'existe pas déjà, créer le domaine : D-domaine.local :
Agents… Gestion des agents… Gestion de l'arborescence des agents…
Se placer au niveau « **Serveur OfficeScan** » et faire « Ajouter un domaine » :



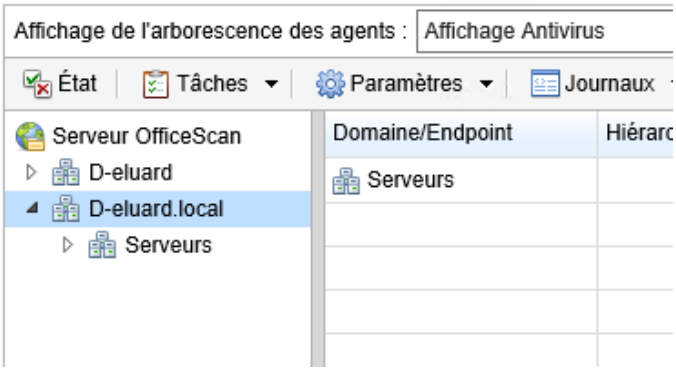


Se placer au niveau « **D-domaine.local** » et Faire « Ajouter un domaine » :

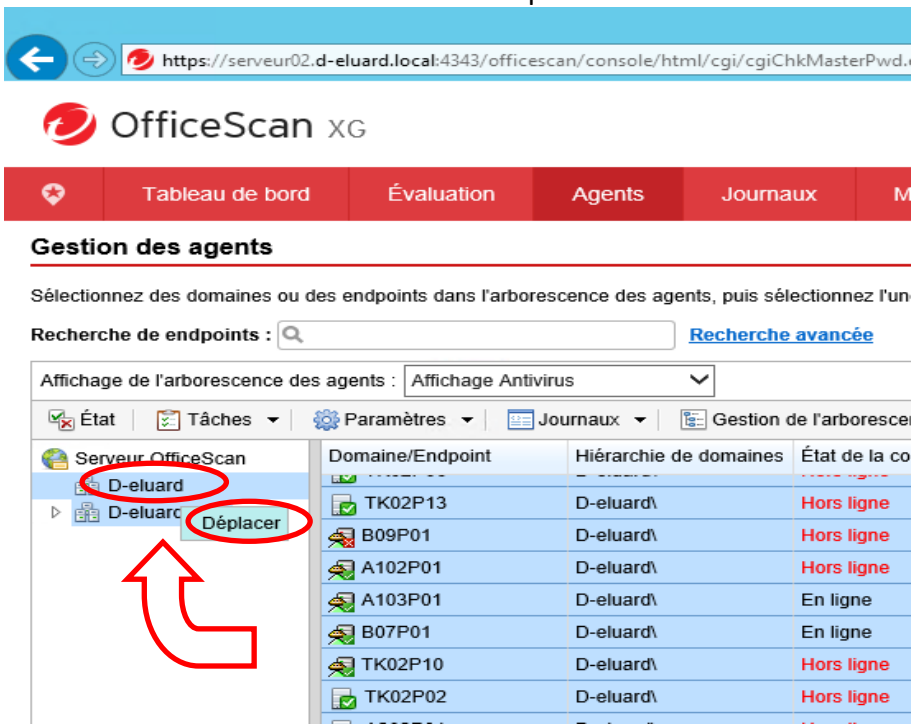




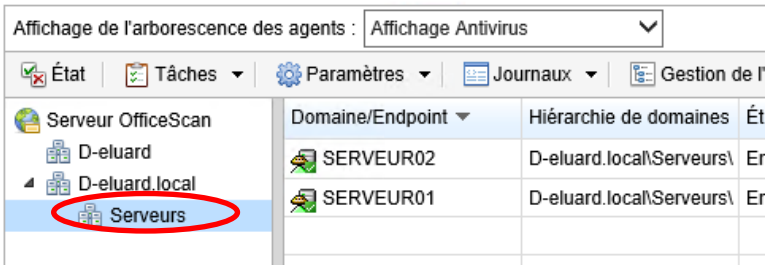
On obtient :



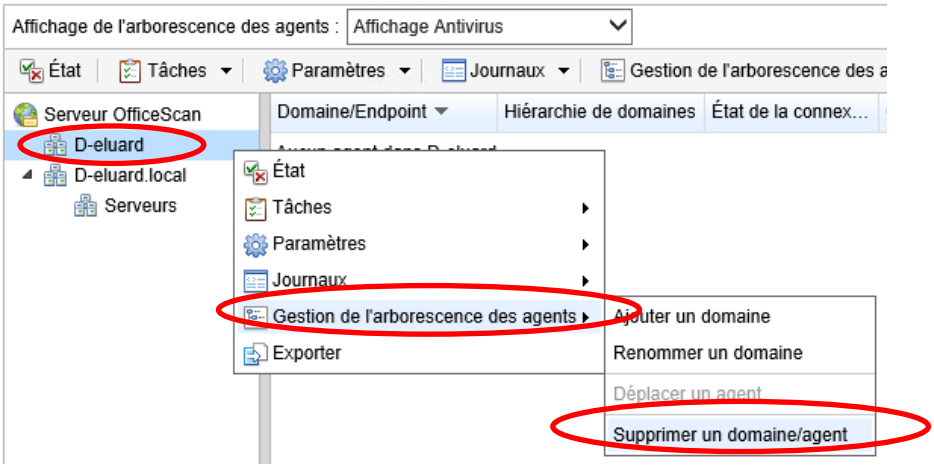
Se placer au niveau « D-domaine ».
Sélectionner toutes les stations et les déplacer dans le domaine nouvellement créé :



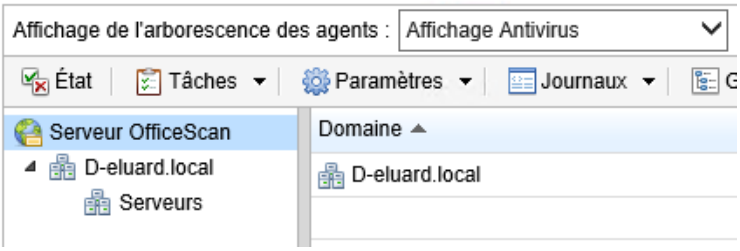
Procéder de même, afin de regrouper les serveurs dans le sous-domaine « Serveurs » :



Supprimer le domaine « D-domaine » qui est vide :

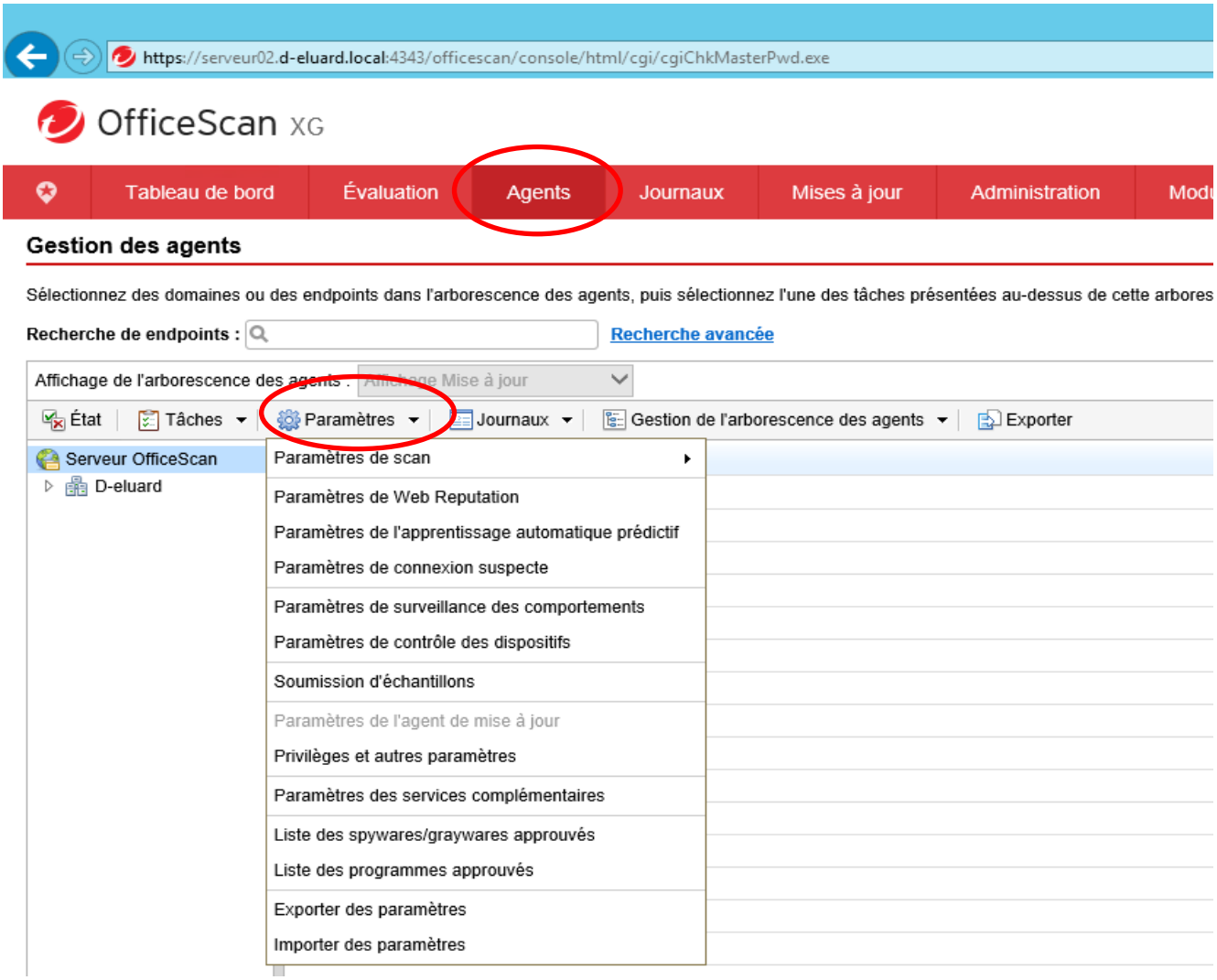


On obtient :



7-4.2 Menu Paramètres – Paramétrage par import d'un fichier .dat

Agents… Gestion des agents… Paramètres…



Remarques importantes :

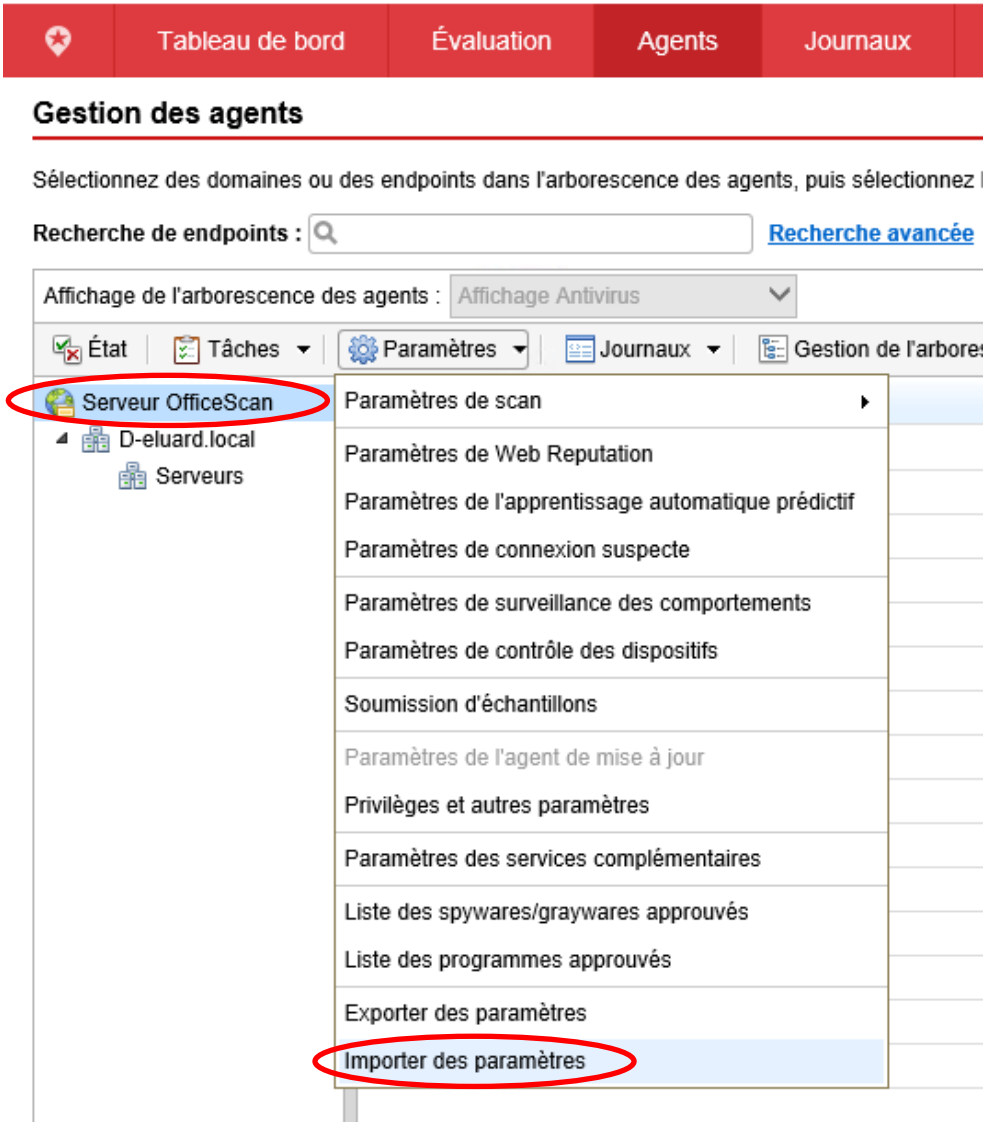
- De nombreux paramètres (voir ci-dessus), concernant le serveur OfficeScan et son arborescence, doivent encore être configurés.
- Cette démarche pourra être simplifiée en effectuant l'import d'un fichier, comprenant l'ensemble de ce paramétrage (fichier .dat).
- Toutefois l'application de ce fichier, peut entrainer des perturbations importantes sur le réseau.
  On évitera en particulier, le changement de la méthode de scan (passage de la méthode « Smart scan » à la méthode « Scan traditionnel » ou inversement), dans les périodes ou le réseau est déjà fortement sollicité.

- L'import du fichier peut être réalisé à différents niveaux dans l'arborescence :
  - L'import au niveau « **Serveur OfficeScan** » concernera tous les domaines et sous-domaines.
  - L'import au niveau d'un domaine, ne s'appliquera qu'aux stations et serveurs du domaine.
- Les mots de passe permettant le déchargement ou la désinstallation de l'agent, ne sont pas modifiés lors de l'import du fichier dat.

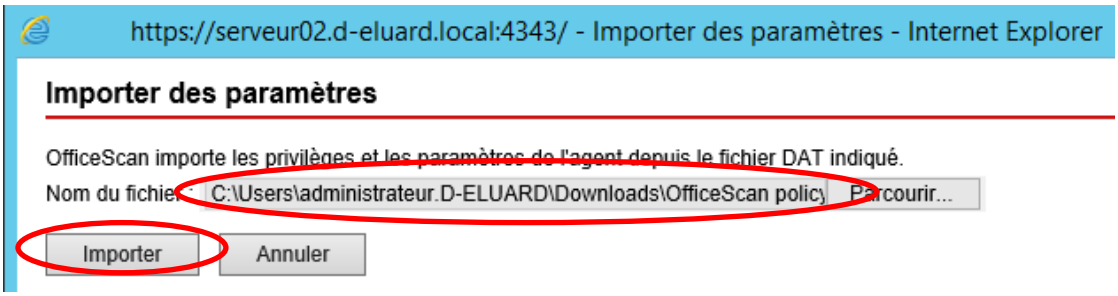
Import d'un fichier .dat : Le fichier **OfficeScan policy_L2.dat** n'est valable que si la console est installée sur Serveur02. Dans le cas contraire voir remarque page 40.

Se placer au niveau « Serveur OfficeScan » puis faire :

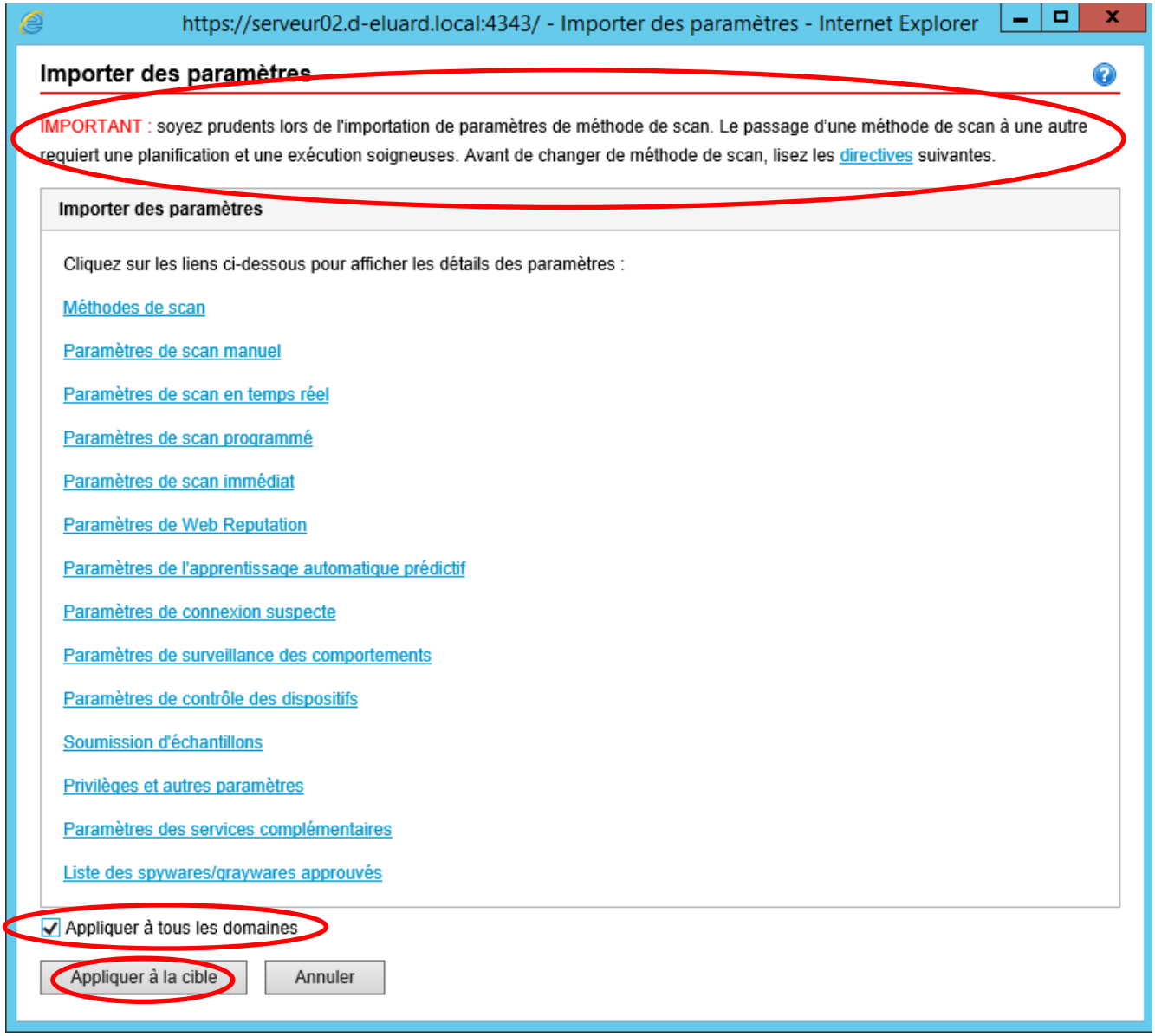
Agents… Gestion des agents… Paramètres… Importer des paramètres…



Indiquer le chemin du fichier .dat et faire Importer :



Le changement de méthode de scan peut entrainer quelques perturbations sur le réseau :


https://serveur02.d-eluard.local:4343/ - Importer des paramètres - Internet Explorer
Importer des paramètres
IMPORTANT : soyez prudents lors de l'importation de paramètres de méthode de scan. Le passage d'une méthode de scan à une autre requiert une planification et une exécution soigneuses. Avant de changer de méthode de scan, lisez les directives suivantes.
Importer des paramètres
Cliquez sur les liens ci-dessous pour afficher les détails des paramètres :
Méthodes de scan
Paramètres de scan manuel
Paramètres de scan en temps réel
Paramètres de scan programmé
Paramètres de scan immédiat
Paramètres de Web Reputation
Paramètres de l'apprentissage automatique prédictif
Paramètres de connexion suspecte
Paramètres de surveillance des comportements
Paramètres de contrôle des dispositifs
Soumission d'échantillons
Privilèges et autres paramètres
Paramètres des services complémentaires
Liste des spywares/graywares approuvés
Appliquer à tous les domaines
Appliquer à la cible
Annuler

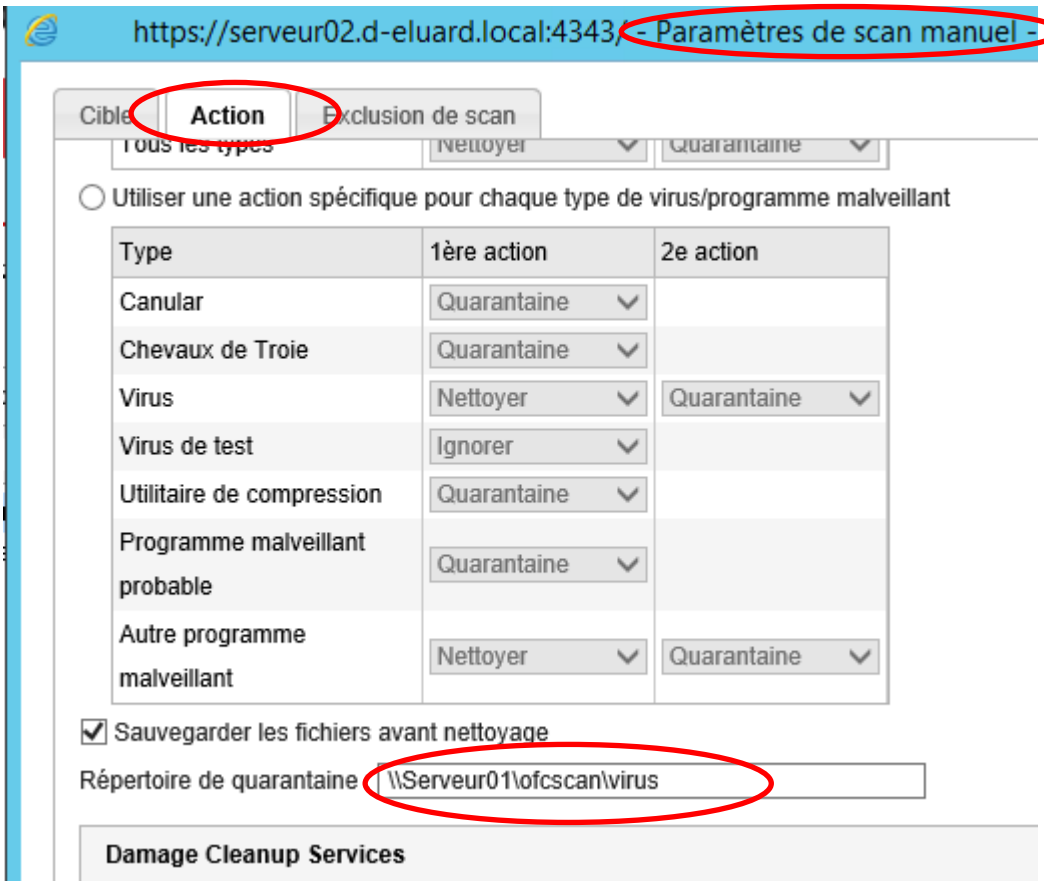

https://serveur02.d-eluard.local
Importer paramètres
Le fichier de paramètres a été importé.
Fermer

Remarque :

Si la console Trend est installée sur un Serveur01 et non sur un Serveur02, modifier les chemins de mise en quarantaine, après importation du fichier .dat.

Agents… Gestion des agents… Paramètres de scan… Paramètres de scan manuel…

Onglet **Action…**



Procéder de même pour les menus :

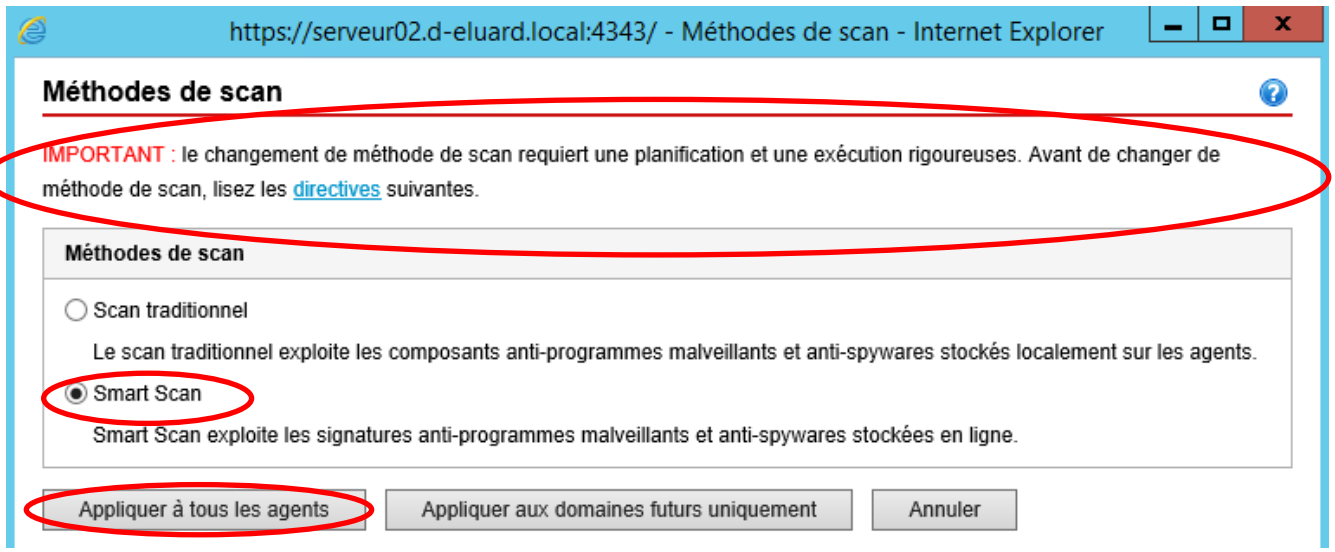
- **Paramètres de scan… Paramètres de scan en temps réel…**
- **Paramètres de scan… Paramètres de scan programmé…**
- **Paramètres de scan… Paramètres de scan immédiat…**

7-4.3 Menu Paramètres - Paramétrage manuel :

Remarque : On est ici dans le cas où aucun fichier .dat n'a été importé, ou bien on souhaite vérifier le résultat de l'import.

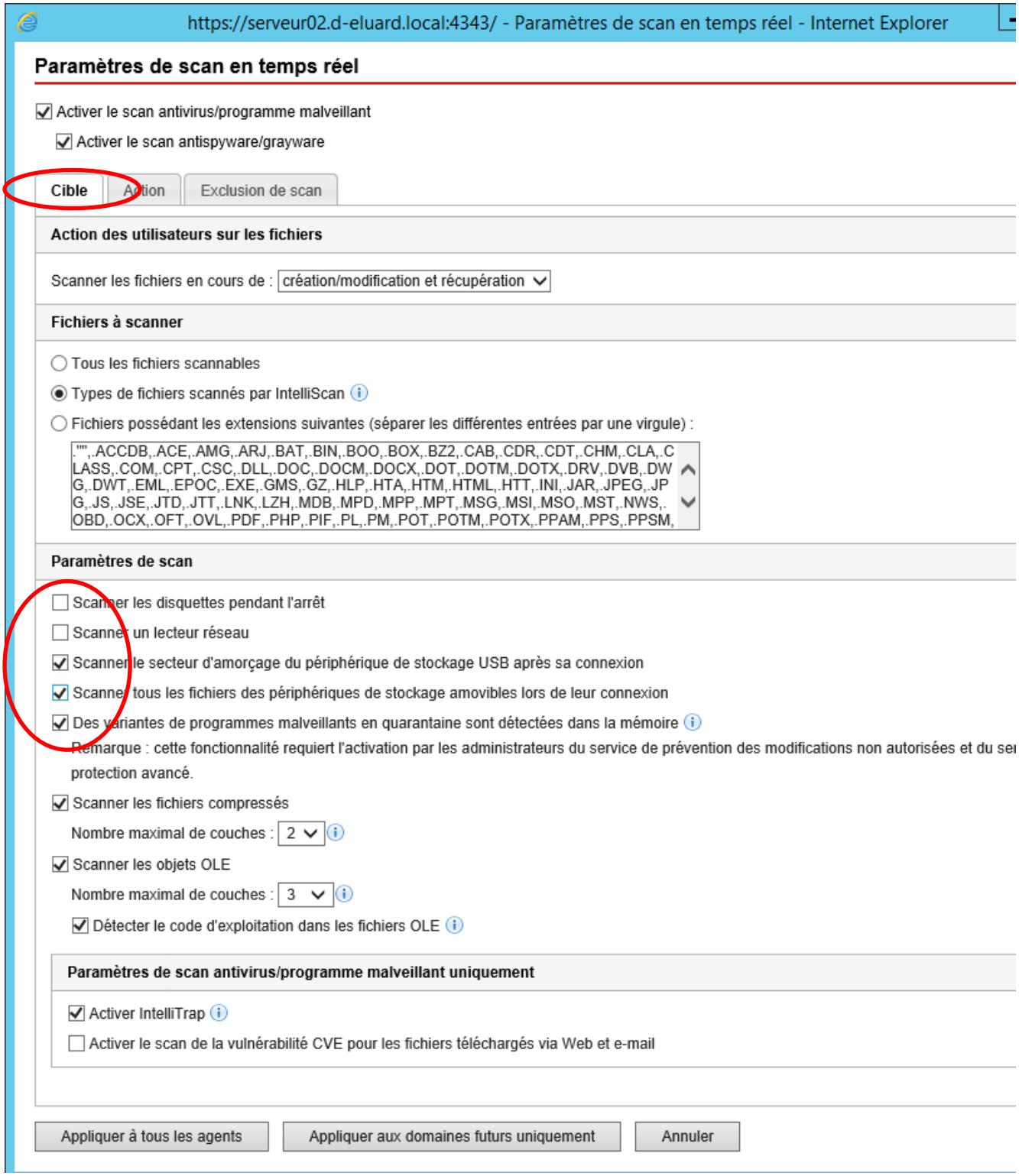
Paramètres… Paramètres de scan… Méthodes de scan…

Le changement de méthode de scan peut entrainer quelques perturbations sur le réseau :



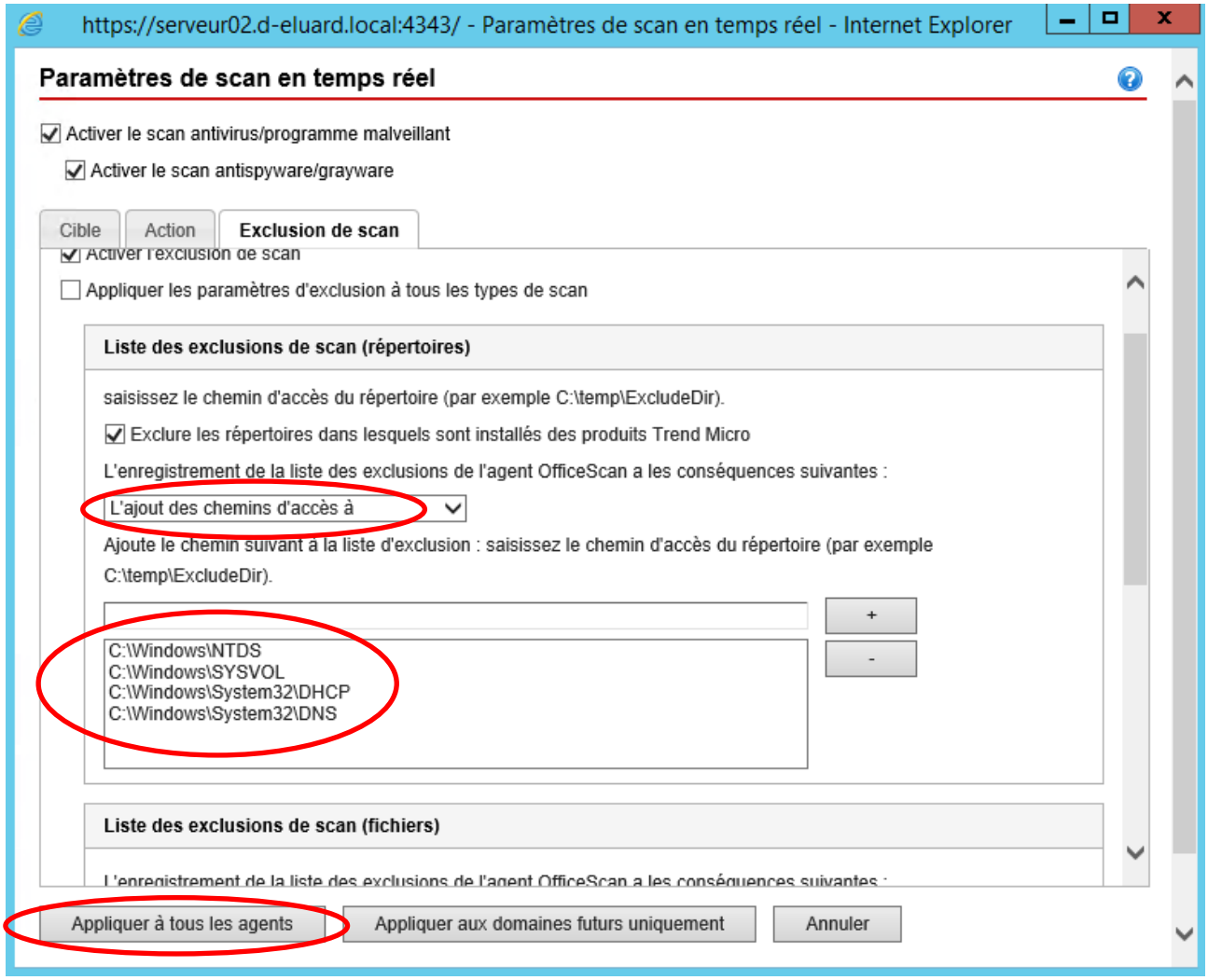
Paramètres… Paramètres de scan… Paramètres de scan en temps réel… Cible…

Décocher impérativement : « Scanner un lecteur réseau » :

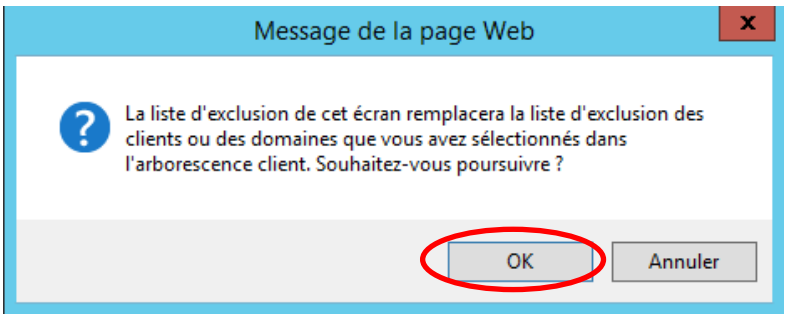


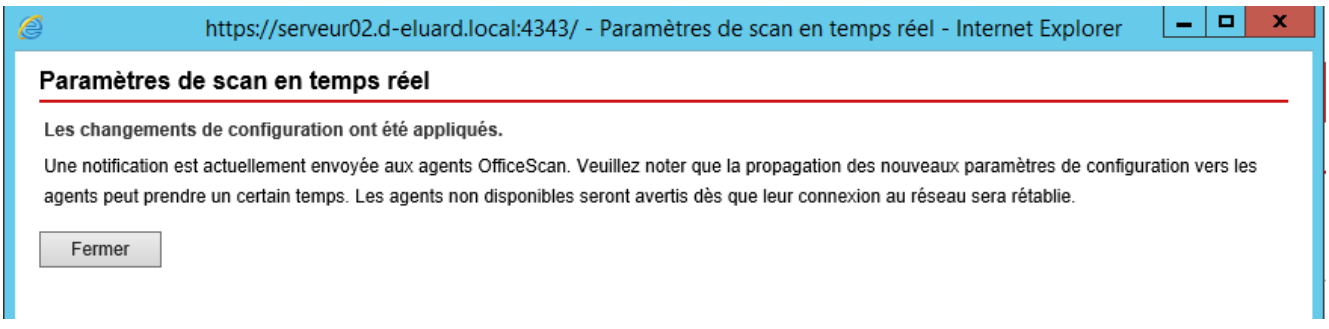
Paramètres… Paramètres de scan… Paramètres de scan en temps réel… Exclusion de scan…

Exclure du scan les dossiers systèmes sensibles :



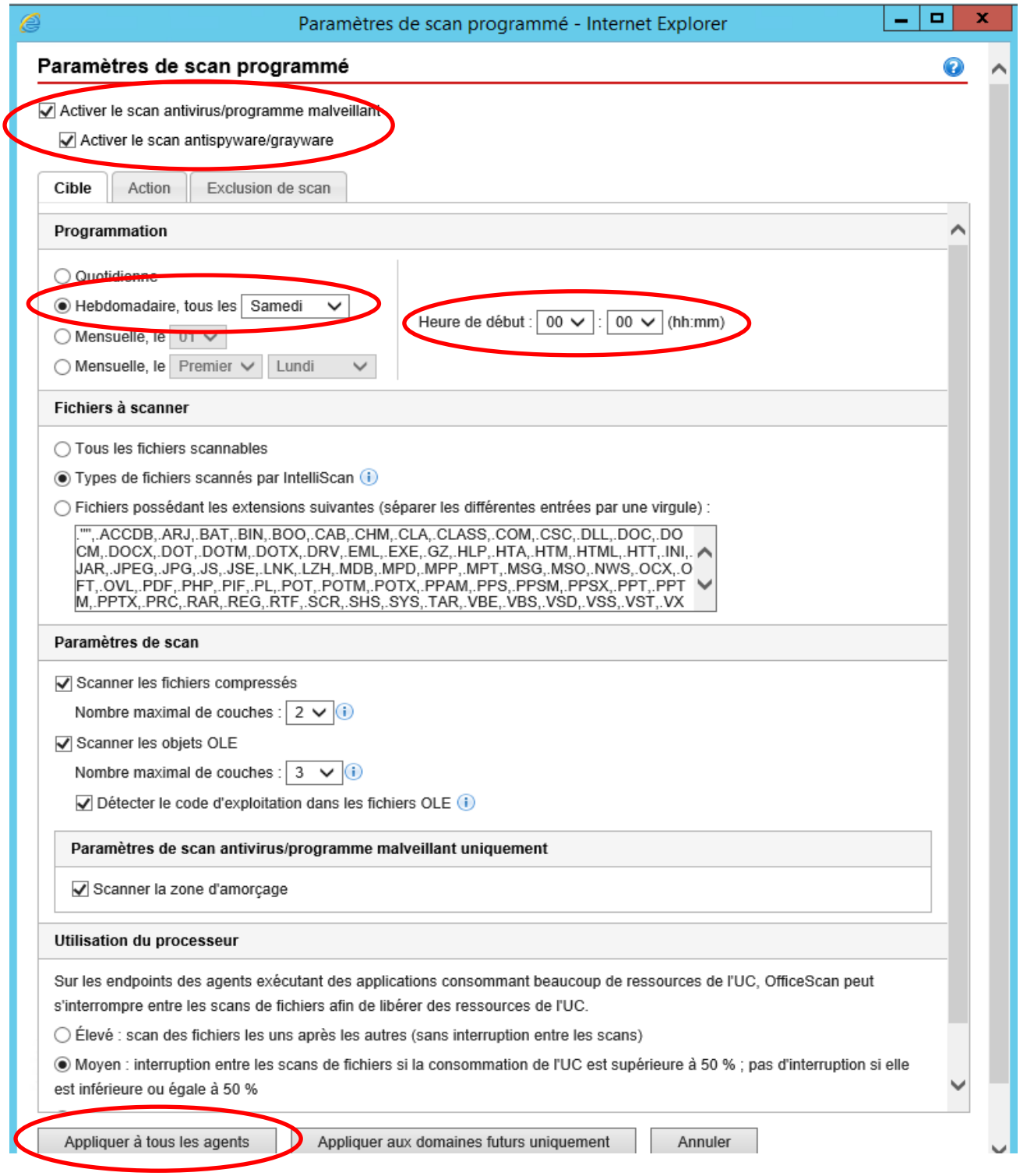
Faire « Appliquer à tous les agents » :

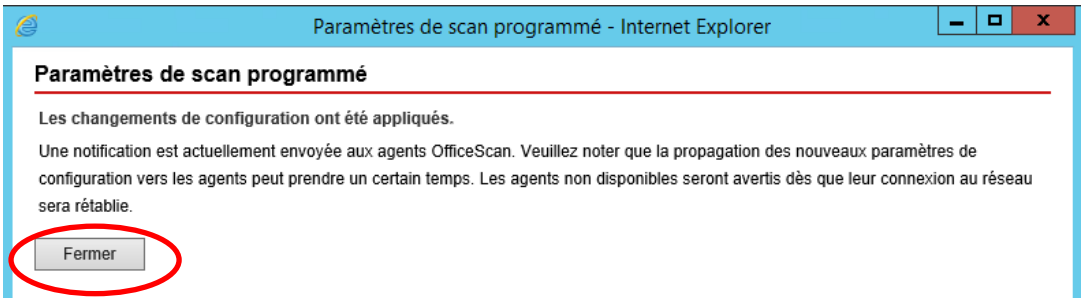




Paramètres… Paramètres de scan… Paramètres de scan programmé… Exclusion de scan…

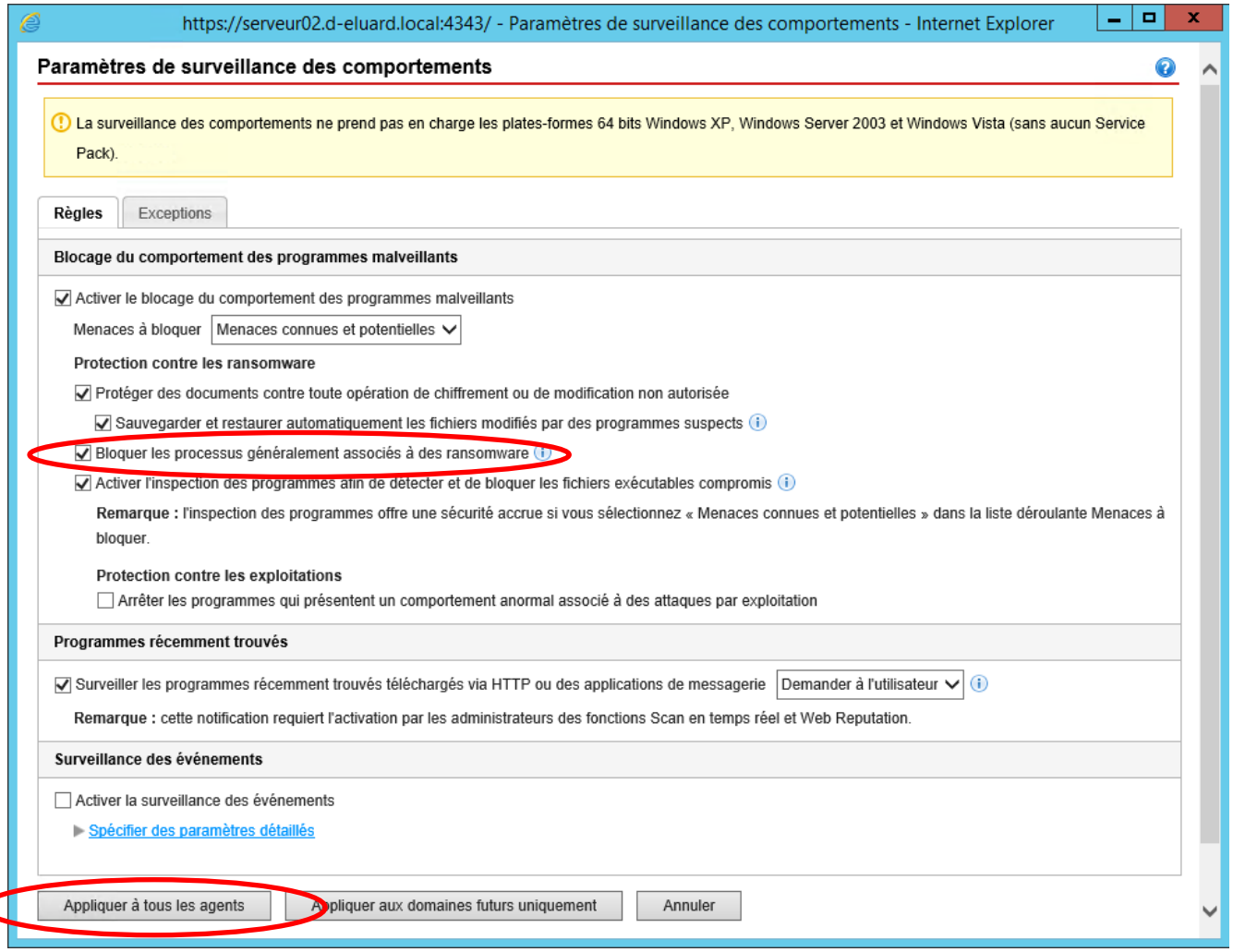
Faire un scan hebdomadaire, sans aucune exclusion :

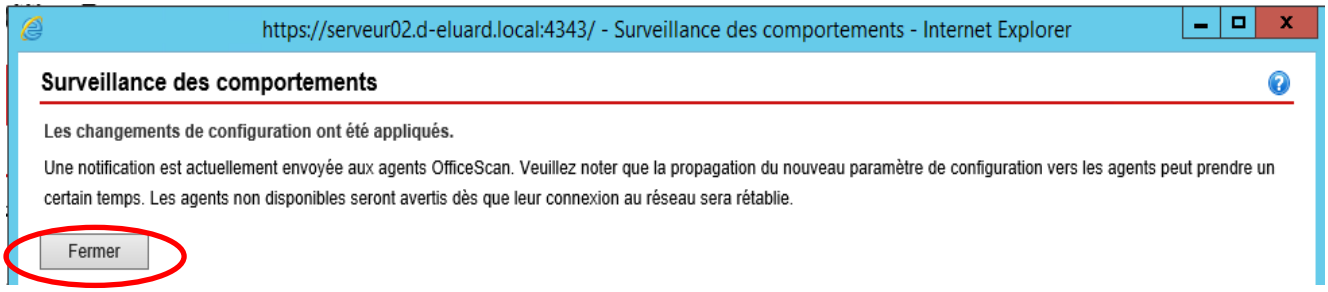




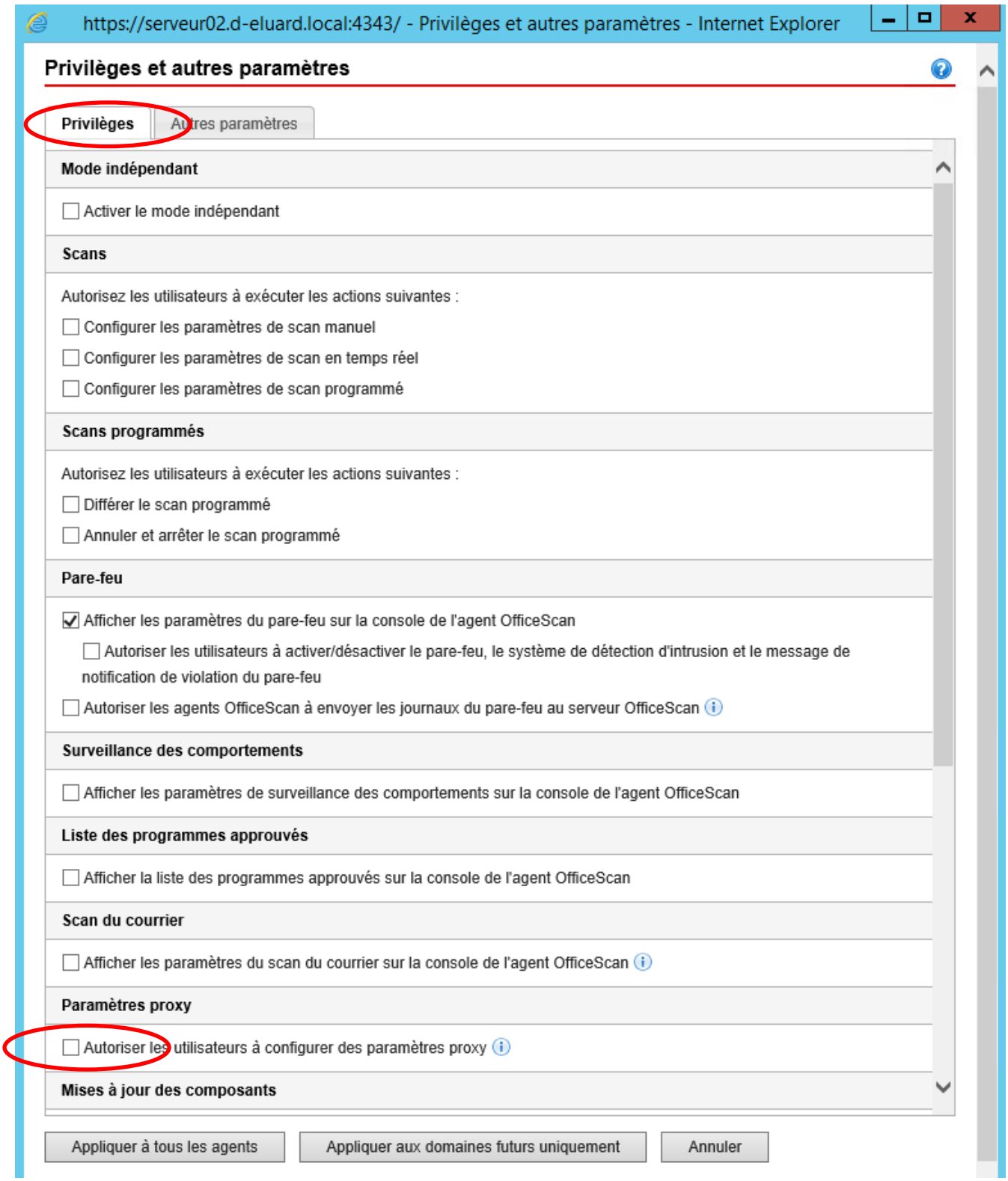
Paramètres… Paramètres de surveillance des comportements…

Activer le blocage des processus de type Ransomware, et « Appliquer à tous les agents » :

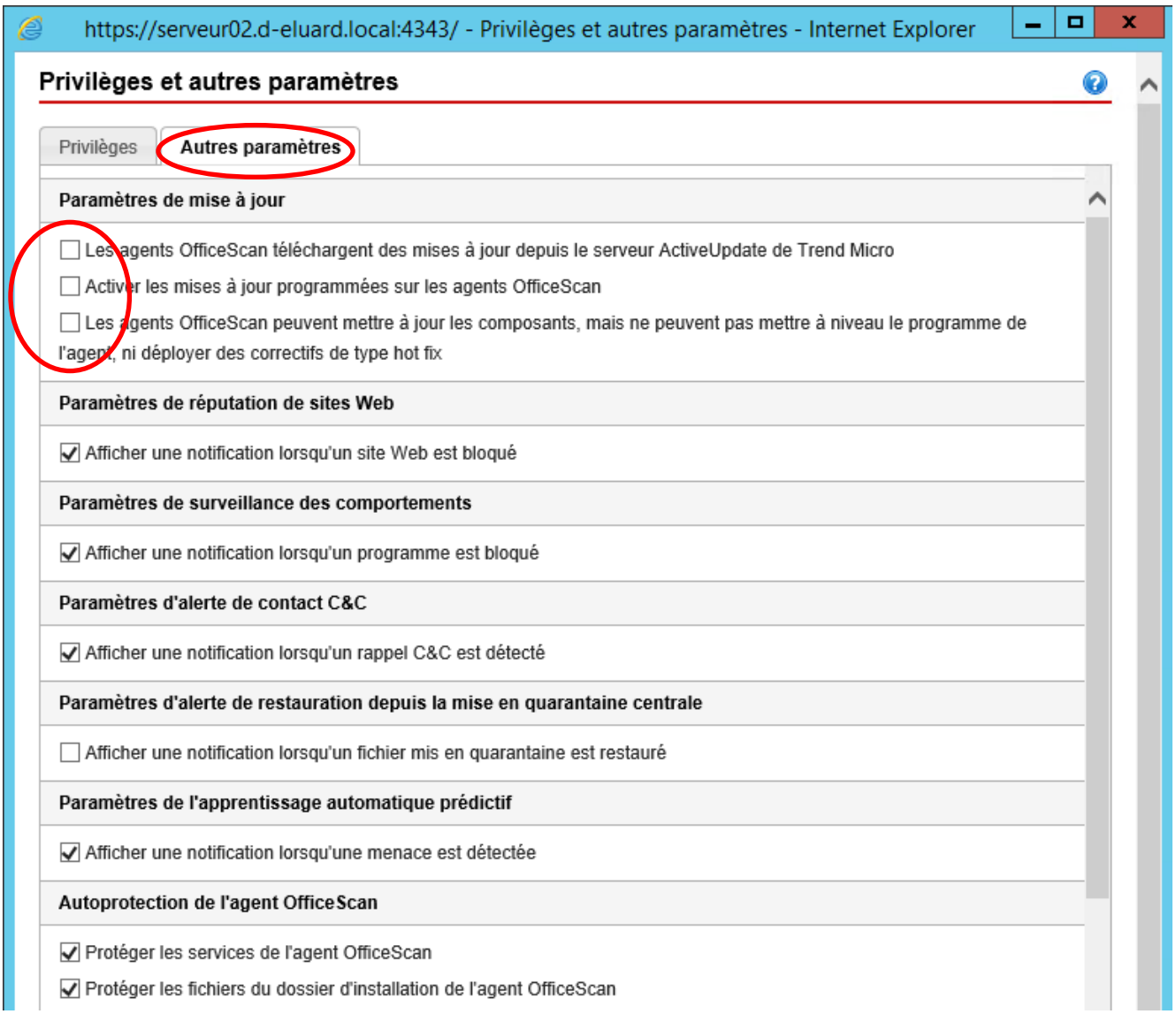




Paramètres… Privilèges et autres paramètres… Privilèges…



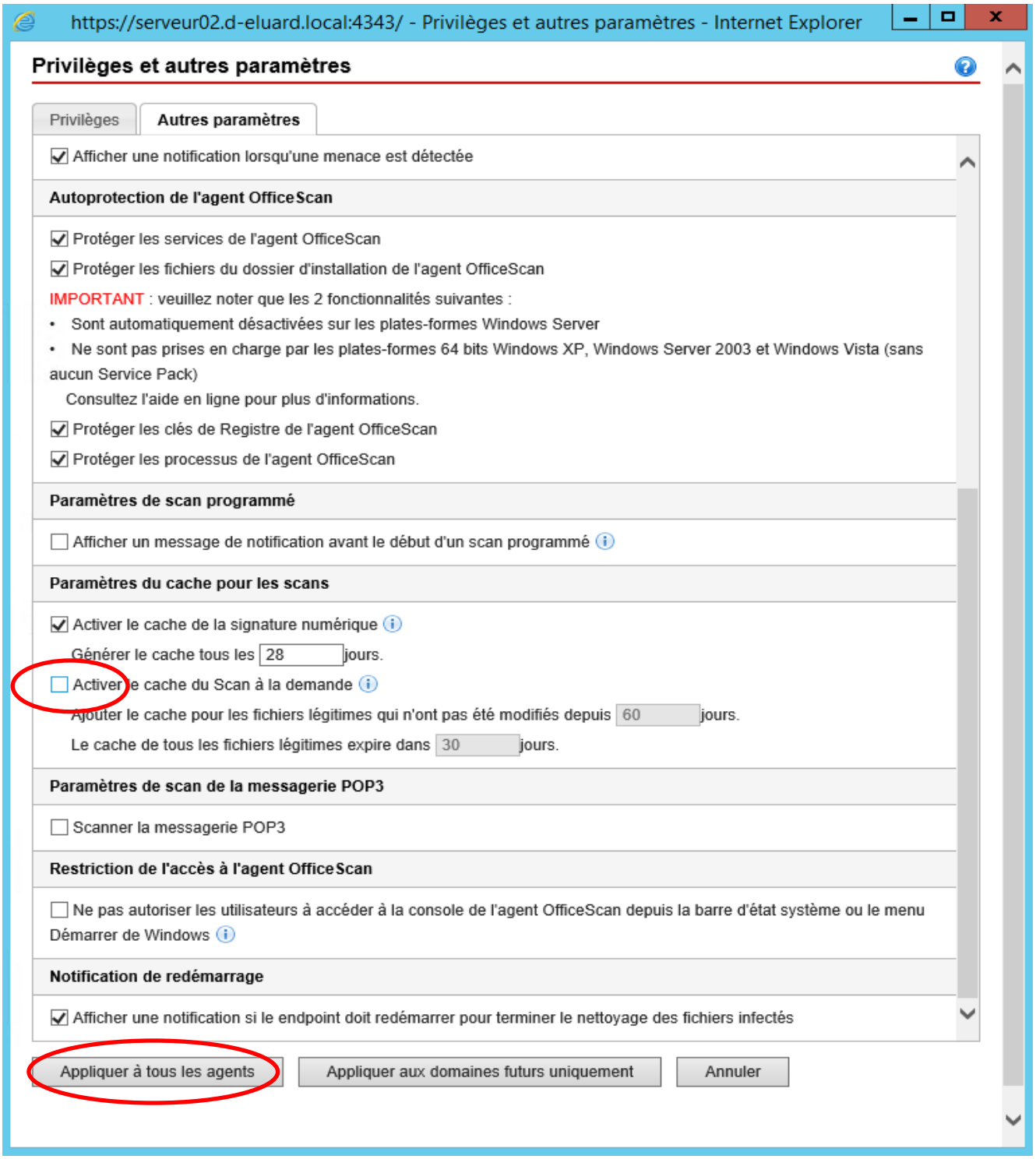
Paramètres… Privilèges et autres paramètres… Autres Paramètres…

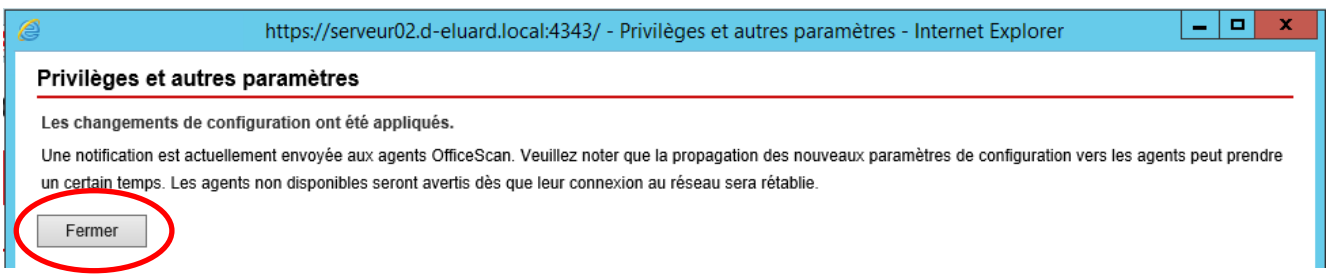


Toujours dans :

Paramètres… Privilèges et autres paramètres… Autres Paramètres…

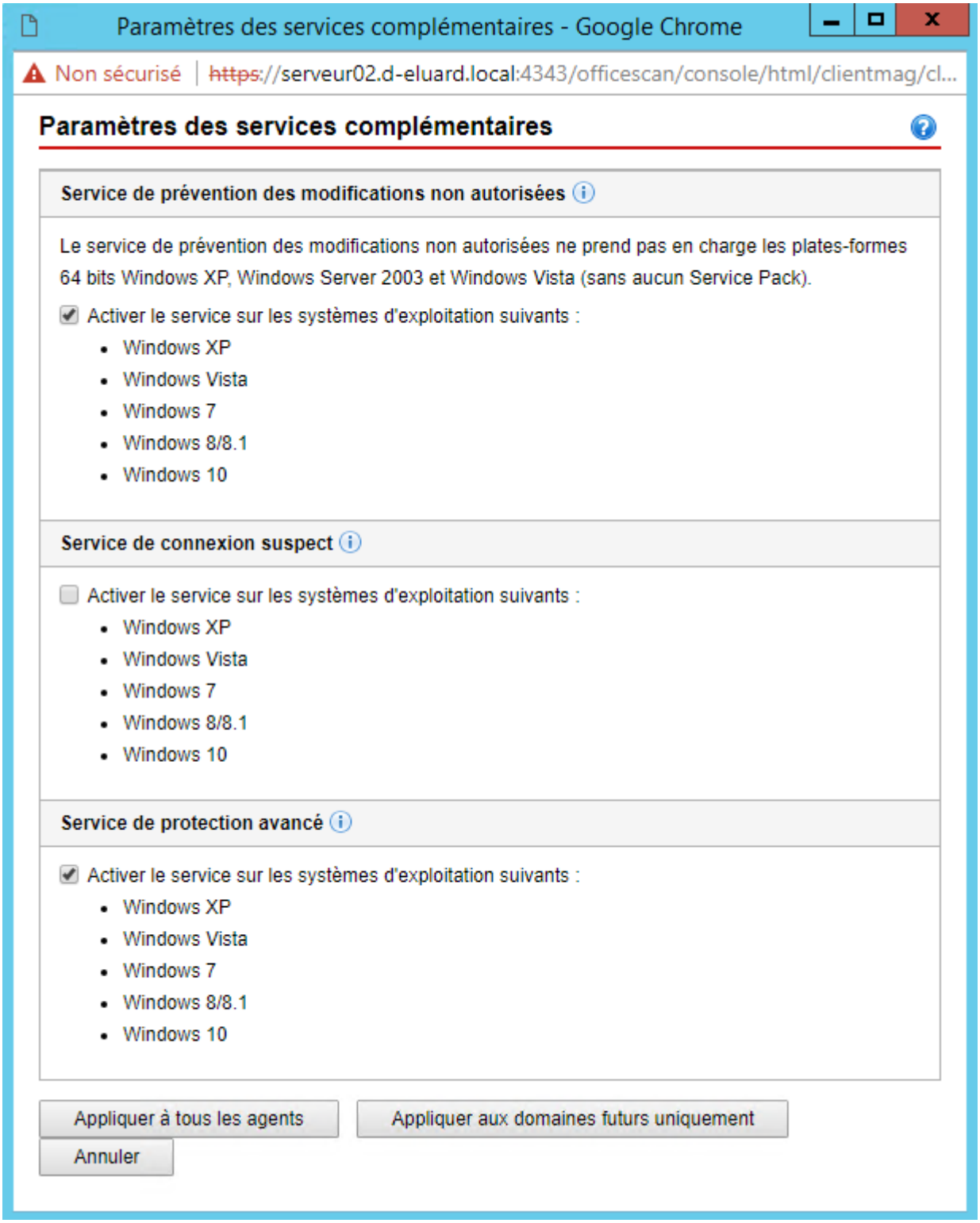
Désactiver le cache de Scan à la demande, puis « appliquer à tous les agents » :





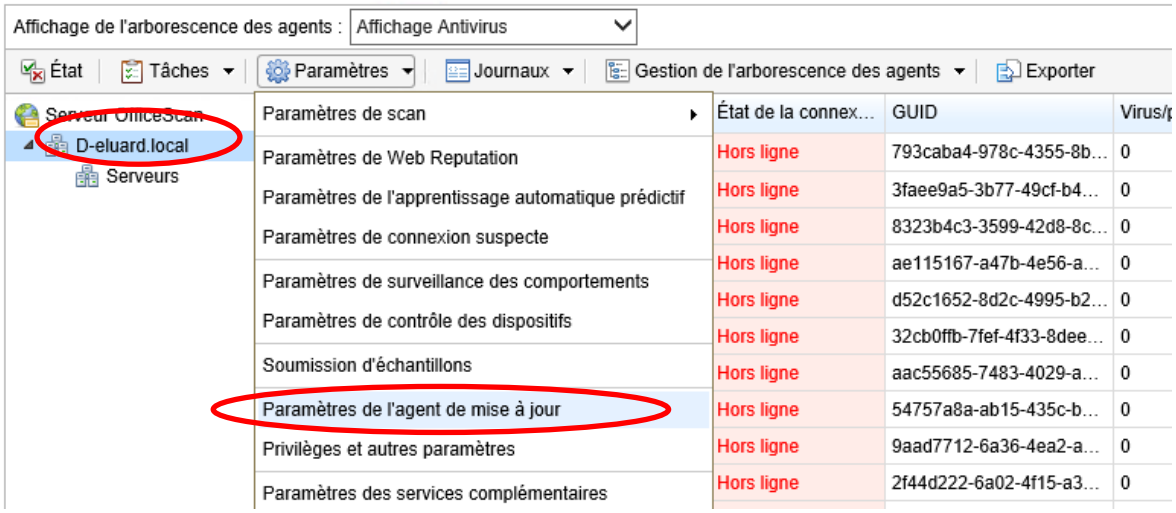
Paramètres… Paramètres des services complémentaires…

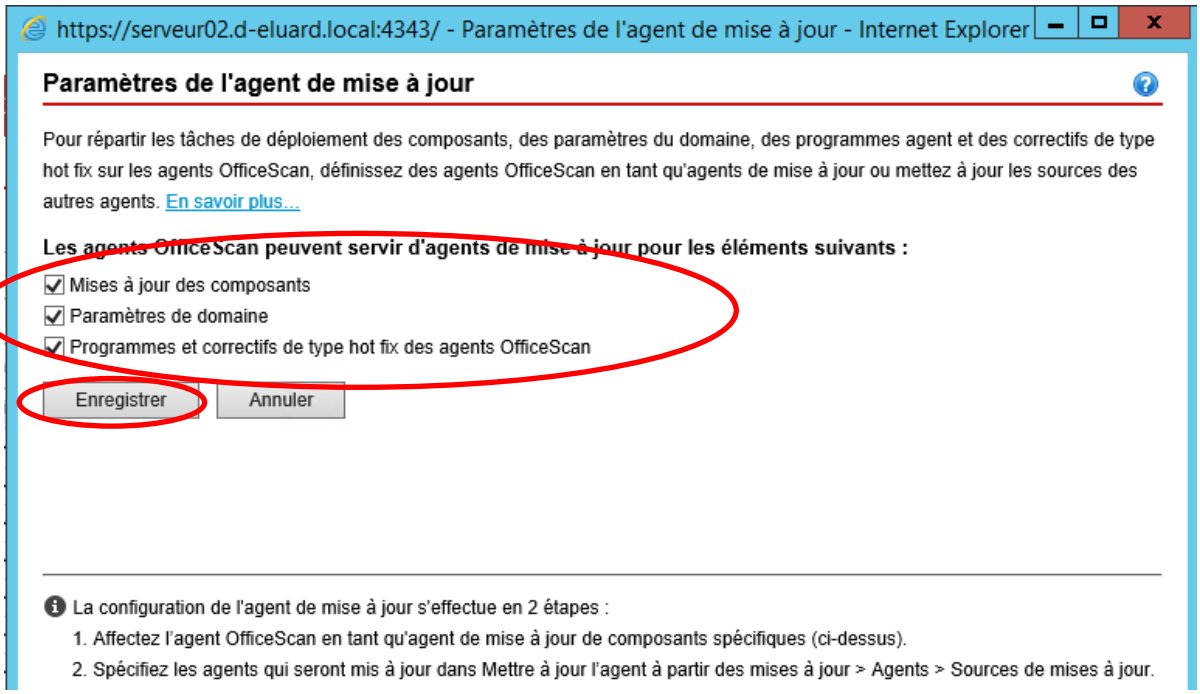
Pas de modifications sur cette page :

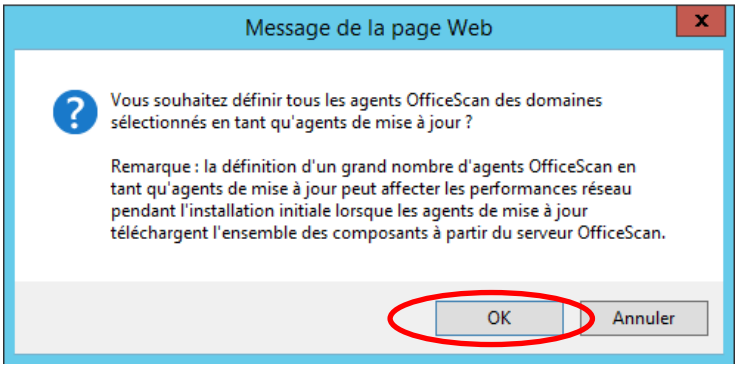


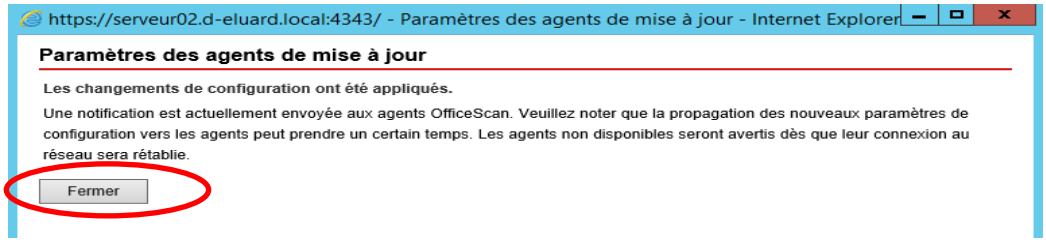
Se placer sur le domaine D-Domaine.local puis faire :

Paramètres… Paramètres de l'agent de mise à jour…









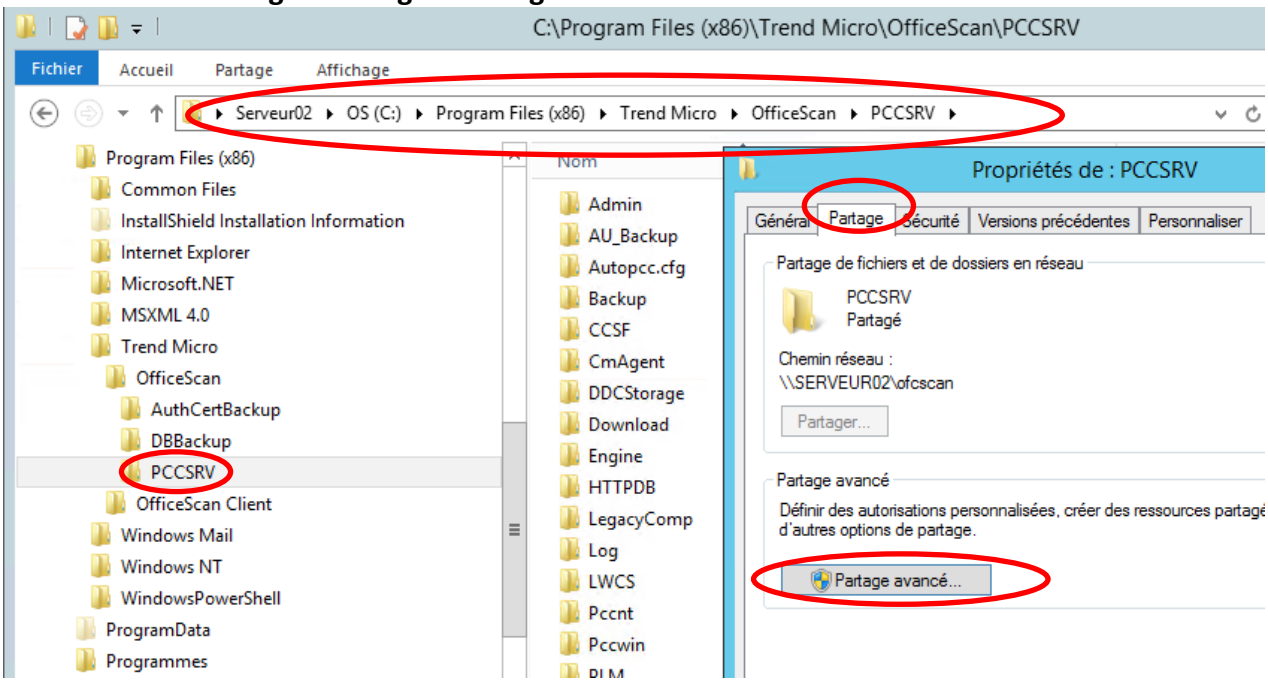
8- Installation et déploiement de l'agent Trend

8-1 Modification des fichiers et des droits, dans le répertoire d'installation de Trend OfficeScan :

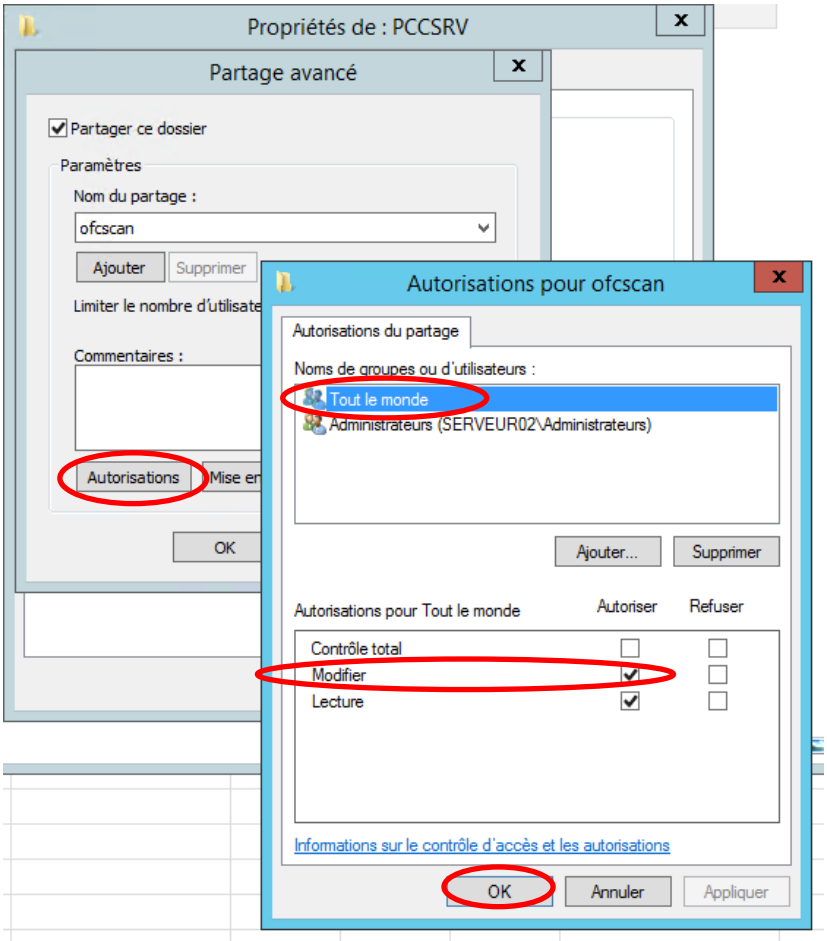
Ouvrir les propriétés du répertoire :

C:\Program Files (x86)\Trend Micro\OfficeScan\PCCSRV :

Onglet Partage… Partage avancé…

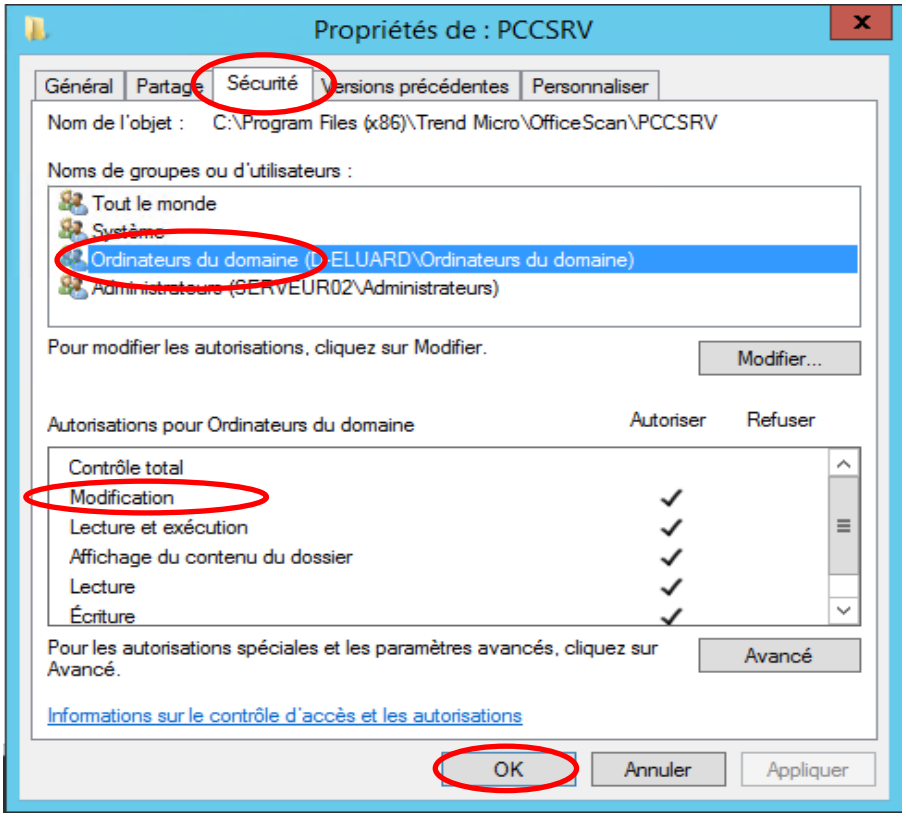


Dans les « **autorisations du partage** », donner les droits de « **modification** » à « **Tout le monde** » :



Onglet Sécurité…

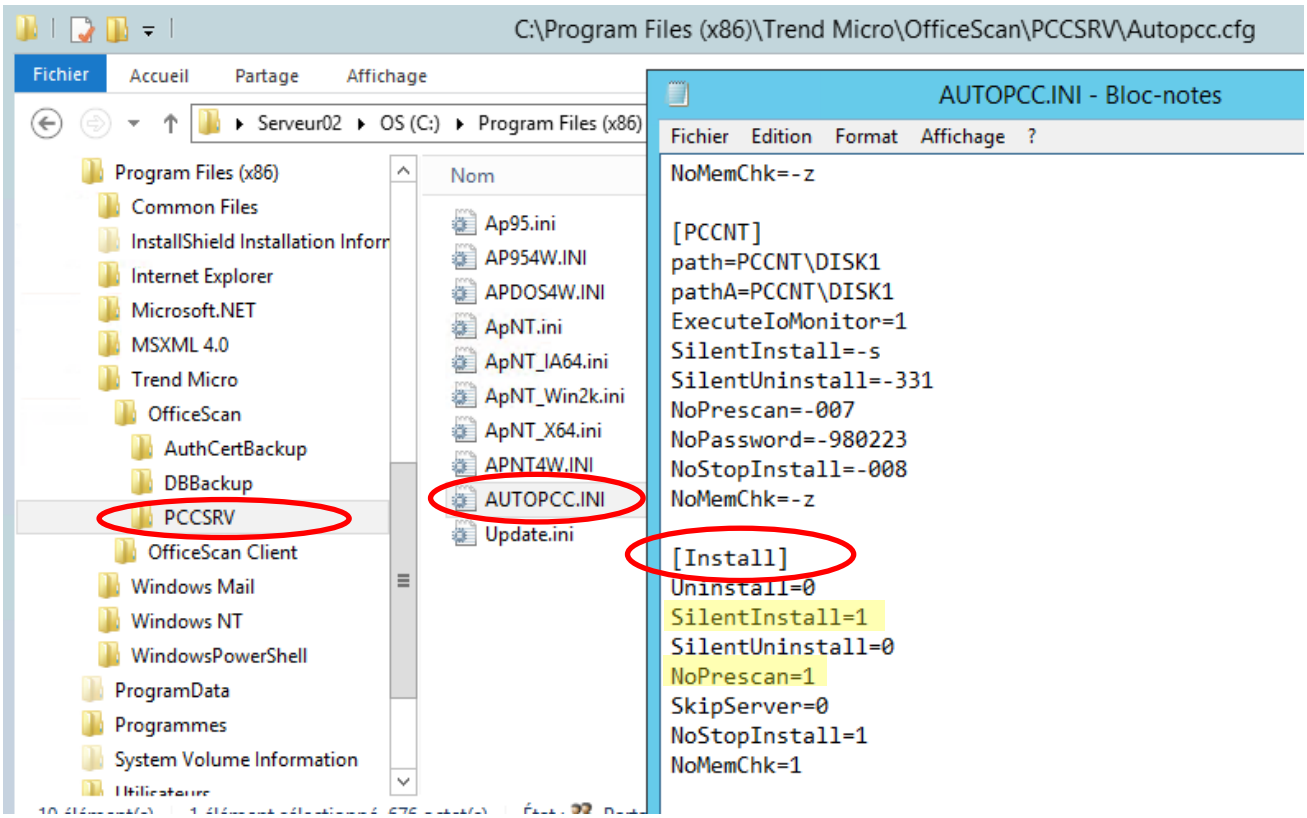
Ajouter le groupe « **Ordinateurs du domaine** » avec les autorisations « **Modification** » :



Dans le répertoire : **C:\Program Files (x86)\Trend Micro\OfficeScan\PCCSRV\Autopcc.cfg**

Editer le fichier **AUTOPCC.ini** et afin d'avoir une installation silencieuse de l'agent sans « préscan », apporter les modifications suivantes dans la section « Install » :

SilentInstall=1 **NoPrescan=1**

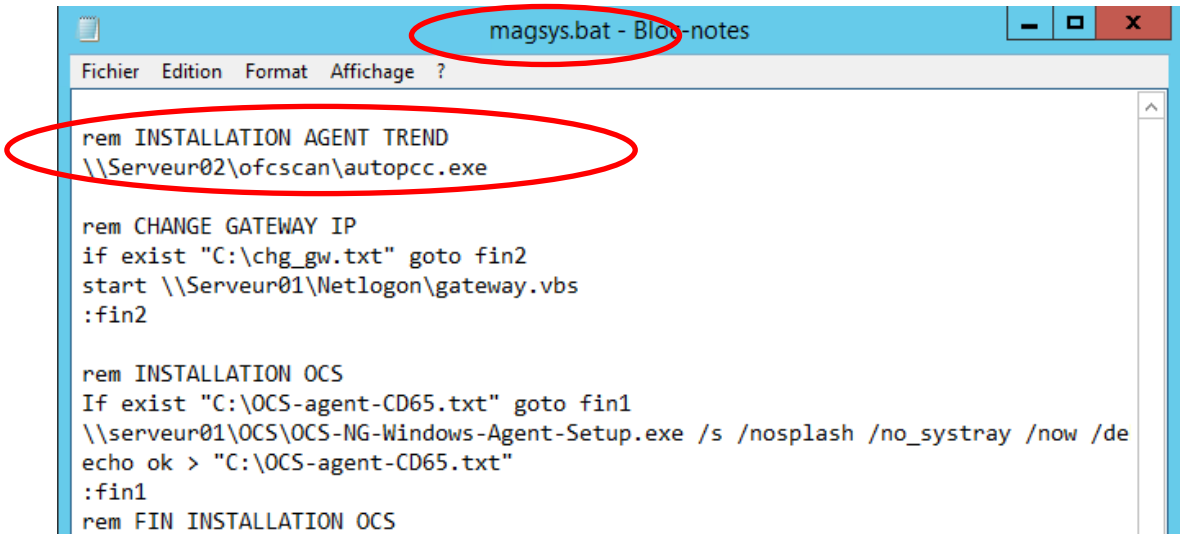


8-2 Installation de l'agent Trend :

La commande : **\\Serveur02\ofcscan\autopcc.exe** lancera l'installation de l'agent sur les stations ou les serveurs membres du domaine.

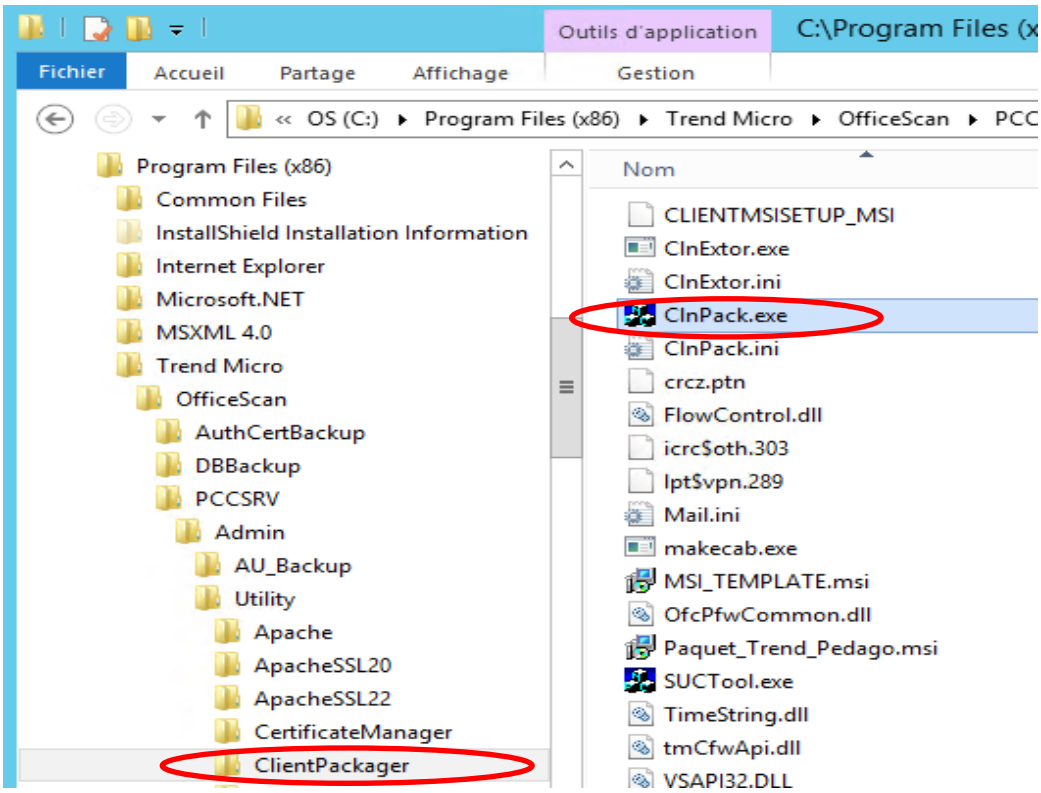
8-3 Installation automatique de l'agent Trend :

Ajouter la ligne **\\Serveur02\ofcscan\autopcc.exe** au fichier **Magsys.bat** dans **Netlogon** :

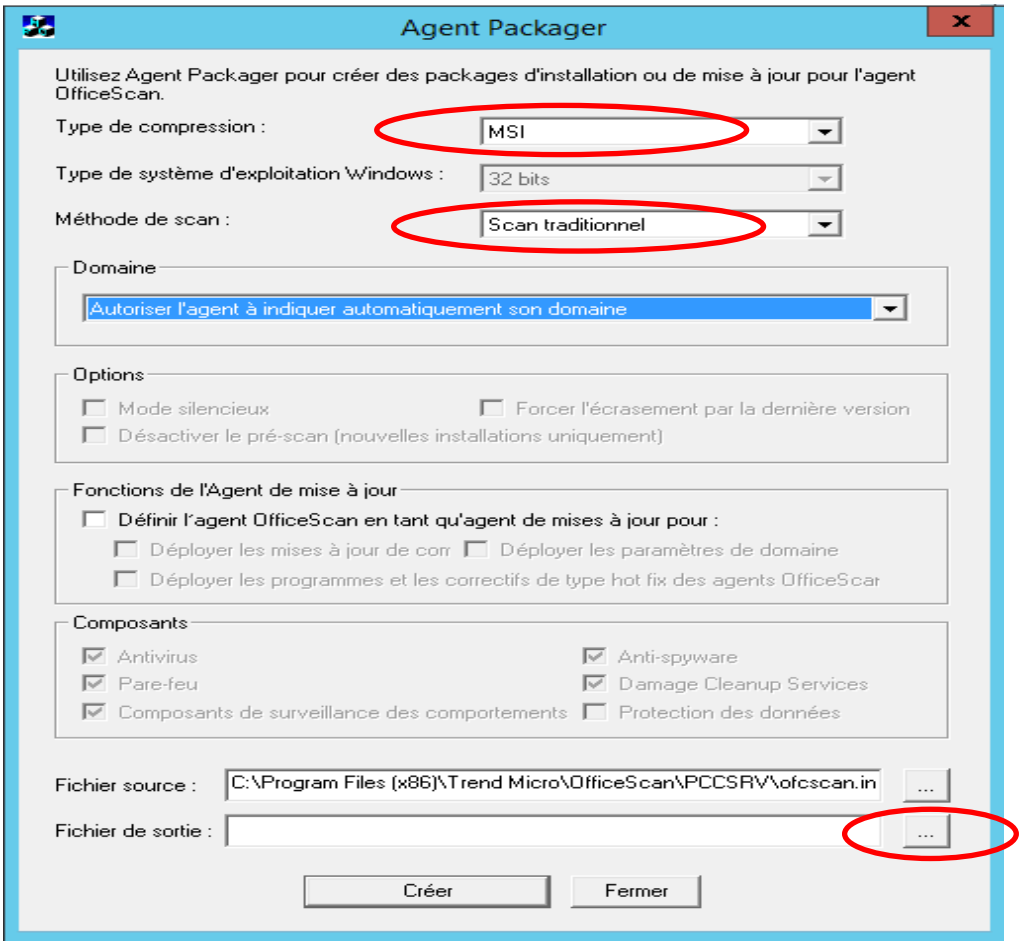


9- Création d'un paquet pour les serveurs DMZ, ZMI et pour les postes isolés du réseau :

Dans le répertoire : **C:\Program Files (x86)\Trend Micro\OfficeScan\PCCSRV\Utility\ClientPackager**



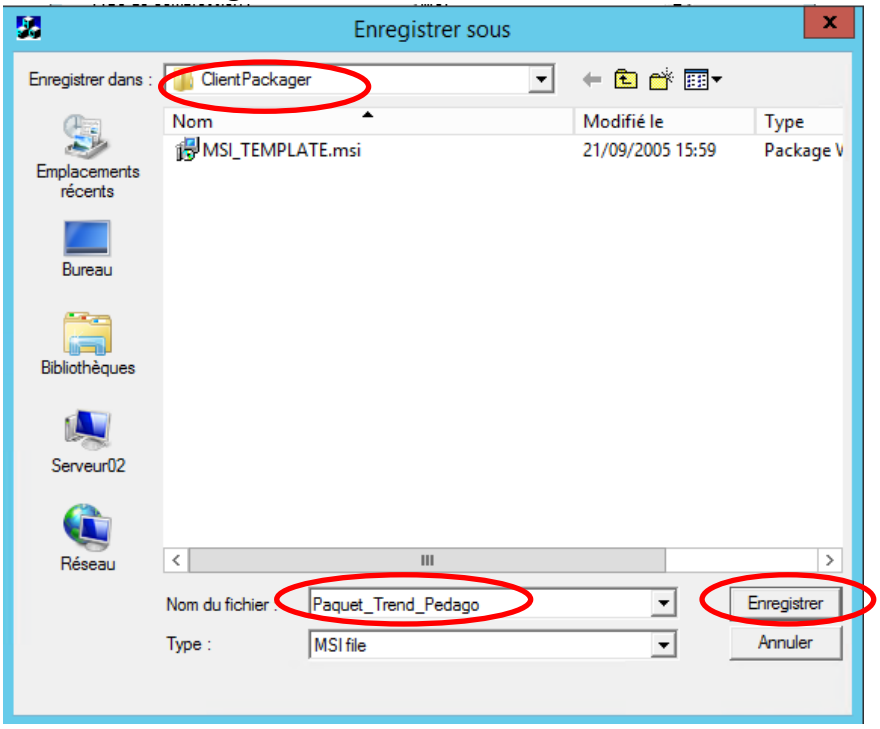
Exécuter **ClnPack.exe** fixer les paramètres du fichier de sortie (**MSI, Scan traditionnel**)



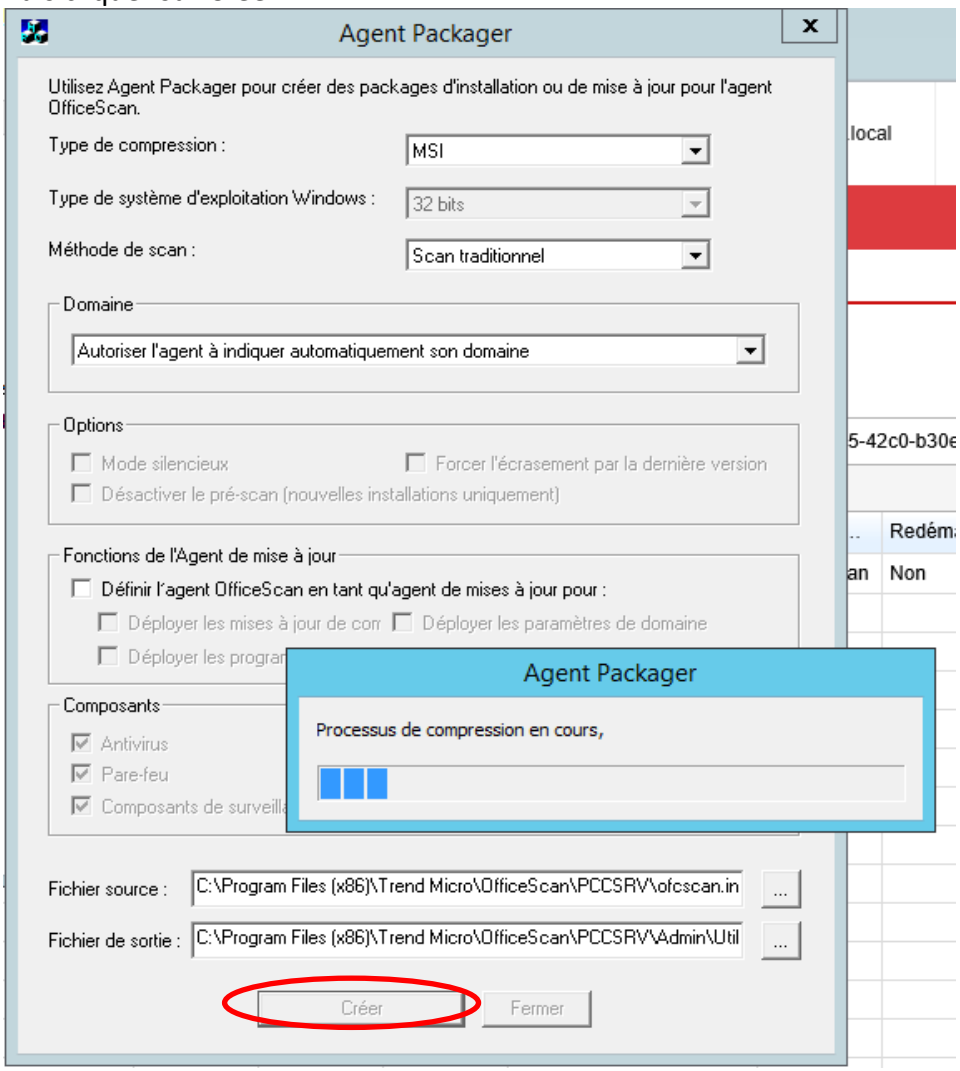
Indiquer le chemin et le nom du fichier de sortie :

C:\Program Files (x86)\Trend Micro\OfficeScan\PCCSRV\Utility\ClientPackager\Paquet_trend_Pedago

Puis faire **Enregistrer** :



Puis cliquer sur Créer :



10- Migration des agents vers le nouveau Serveur :

Si la console Trend OfficeScan a été transférée d'un Serveur01 vers un Serveur02, il est nécessaire de connecter les agents Trend des stations à la nouvelle console.
On utilisera pour cela la commande IpXfer.
Dans Netlogon créer le fichier « **TrendMover.bat** » suivant :

```
Rem     Migration des Agents Trend vers Serveur02 permettant le passage à la version Trend XG (12)
Rem Il est indispensable de connaître l'ancien mot de passe (ici "Aneto"), qui permettait, sur les stations, de
Rem             décharger l'agent Trend version 11
Rem             10.255.33.168  est l'adresse IP du Serveur02

if exist c:\cltmv.txt goto fin

Rem Stations 64 bits :
\\serveur02\ofcscan\Admin\utility\ipxfer\IpXfer_x64.exe -s 10.255.33.168 -p 8080 -c 8000 -e
\\serveur02\ofcscan\PCCNT\Common\OfcNTCer.dat -pwd Aneto

Rem Stations 32 bits :
\\serveur02\ofcscan\Admin\utility\ipxfer\IpXfer.exe -s 10.255.33.168 -p 8080 -c 8000 -e
\\serveur02\ofcscan\PCCNT\Common\OfcNTCer.dat -pwd Aneto

Rem Vérifier que "Ordinateurs du domaine" ont les droits de "Modification" sur le dossier "Packages"
echo %COMPUTERNAME% %DATE% %TIME% OK >> \\Serveur01\Packages\MigrationTrend.log
echo %COMPUTERNAME% OK >C:\cltmv.txt

:fin
```

Remarques :

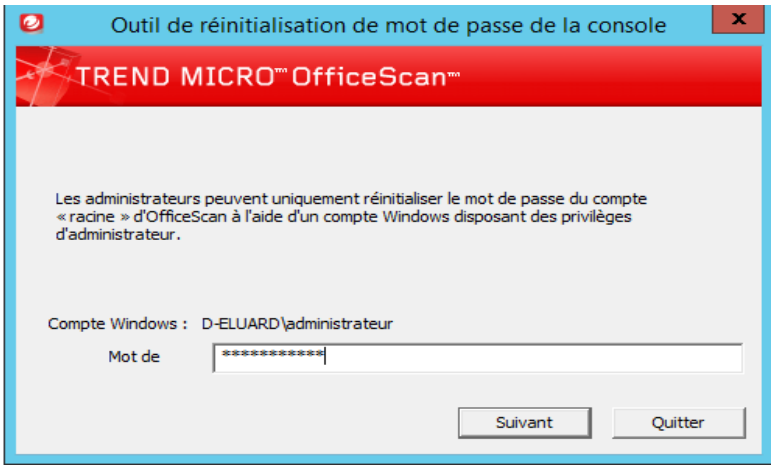
- Mettre un espace, et pas de retour à la ligne après « -e ».

- A partir d'une station, lancer manuellement le script afin de vérifier, que le mot de passe est valide et que son exécution est correcte .

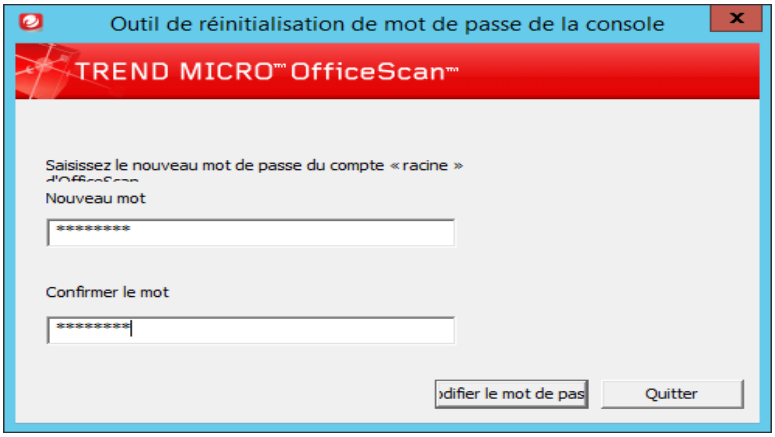
- Automatiser l'exécution du script en ajoutant la ligne :
  \\Serveur01\Netlogon\TrendMover.bat
  Aux « **Scripts** » « **Arrêt du système** » de la **Stratégie Ordinateurs**

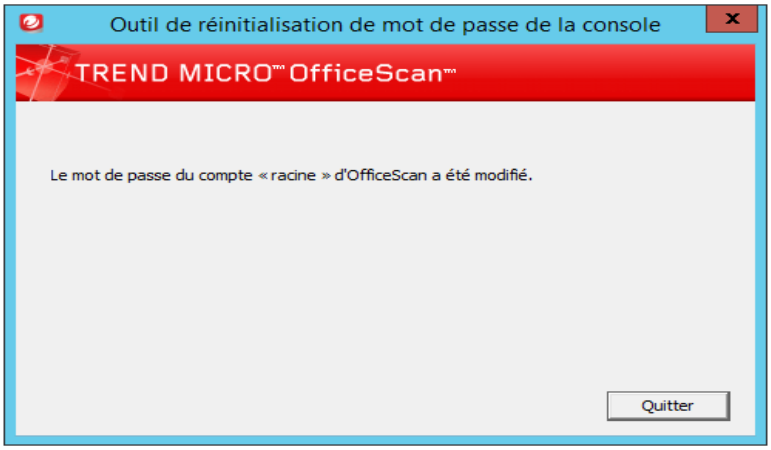
11- Réinitialisation du mot de passe de la console Trend OfficeScan :

En cas de perte, le mot de passe du compte **root** de la console Web OfficeScan peut être réinitialisé.
Dans l'explorateur Windows, accéder au dossier :
C:\Program Files (x86)\Trend Micro\OfficeScan\PCCSRV\Admin\Utility\OSCEResetPW
Lancer l'exécutable : **OSCEResetPW.exe**
Le mot de passe de l'administrateur du domaine est nécessaire **:**



Indiquer le nouveau mot de passe du compte « root » :





Remarque : Les mots de passe nécessaires pour le déchargement ou la désinstallation de l'agent sur les stations, peuvent être modifiés dans :

Paramètres… Privilèges et autres paramètres… Privilèges…