Guide d’identification de l’utilisateur – WebTitan Web Filter Cloud

Ce guide explique comment installer et configurer les composants d'WebTitan Web Filter Cloud Active Directory nécessaires pour rendre compte de l’activité des utilisateurs, des groupes et des réseaux internes.

## PRESENTATION

L’intégration de l’identification des utilisateurs Active Directory est fondée sur deux composants devant être installés sur votre réseau :

1. **Le proxy DNS WebTitan Web Filter, qui est chargé de :**

- télécharger de manière sécurisée les informations sur les utilisateurs et les groupes d’ordinateurs sur le service WebTitan Web Filter Cloud ;
- rediriger toutes les requêtes de DNS locales vers vos serveurs DNS internes existants ;
- rediriger toutes les requêtes DNS externes avec des métadonnées vers WebTitan Web Filter Cloud.

2. **WebTitan Web Filter Active Directory Agent (WADA), qui est chargé de :**

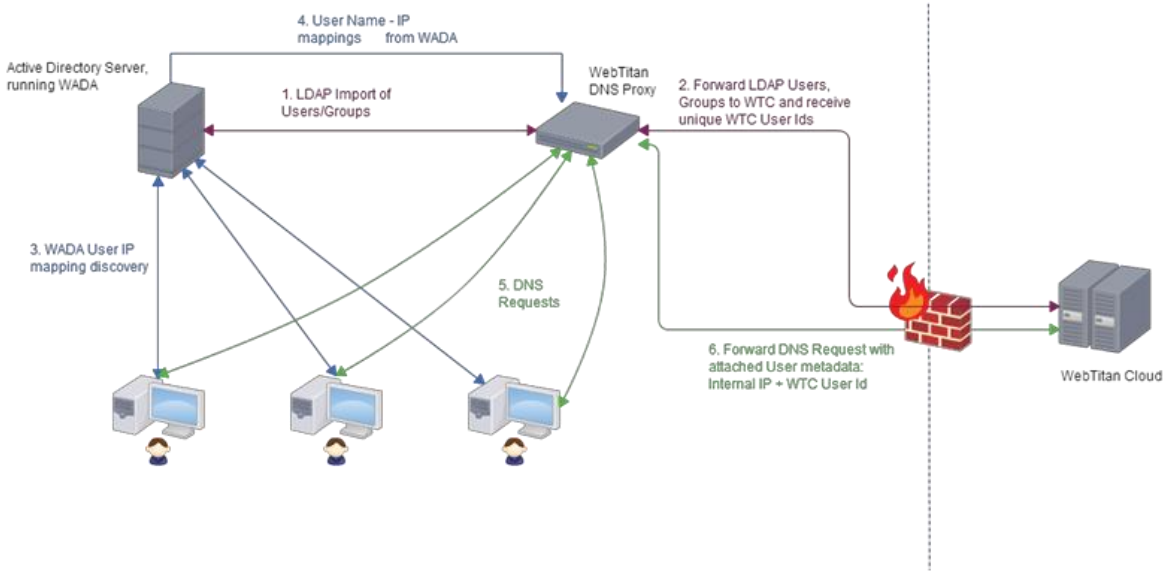
- dresser la liste des sessions de connexion actives, en mappant une adresse IP à un nom d'utilisateur ;
- transférer de manière sécurisée ces informations au proxy DNS WebTitan Web Filter ;
- Les informations sont obtenues à partir de 3 sources différentes (LDAP, journal des événements et sessions réseau).

a) Le mécanisme LDAP collecte une liste d’ordinateurs dans le domaine et, en fonction du paramètre lastLogon (Dernière connexion), contacte chaque ordinateur en utilisant le protocole WMI afin de vérifier les sessions de connexion actives et, finalement, obtient le nom d’utilisateur. Tous les ordinateurs ne sont pas contrôlés ; seuls ceux dont le champ Dernière connexion se trouve dans la plage définie dans la configuration (1 an par défaut).

b) Le mécanisme Journal des événements est « à l’écoute » de certains événements qui contiennent des informations sur le nom d’utilisateur et l’IP.

c) En outre, les sessions réseau sont énumérées (toutes les 10 secondes par défaut) afin de découvrir les sessions actives. Cette méthode est importante, notamment lorsqu’il y a des utilisateurs sur le réseau qui n’éteignent pas leur ordinateur pendant longtemps et que, pour une raison quelconque, leur ordinateur n’est pas accessible avec WMI.

## FLUX DE TRAVAIL




1. Installez le proxy DNS WebTitan Web Filter sur un hyperviseur ou sur un système « nu ». Le proxy DNS WebTitan Web Filter importe tous les utilisateurs et groupes (actuellement, nous importons uniquement les utilisateurs) depuis Active Directory.

2. Ils sont ensuite transmis de manière sécurisée à WebTitan Web Filter Cloud. En retour, le proxy DNS reçoit un ID d'utilisateur unique pour chaque utilisateur.

3. Installez WebTitan Web Filter Active Directory Agent (WADA) sur le serveur Active Directory (ou sur un autre serveur dans le domaine). WADA utilisera plusieurs techniques afin de découvrir qui est connecté et où il/elle est connecté(e).

4. Les mappages utilisateur-IP découverts sont transmis en continu au proxy DNS WebTitan Web Filter.

5. Tous les ordinateurs internes doivent faire passer leur trafic DNS par le proxy DNS WebTitan Web Filter. Lors de la réception d'une requête DNS, le proxy DNS WebTitan Web Filter contrôle si un utilisateur est associé à l'adresse IP source de la requête. L'ID WTC de cet utilisateur (s'il a été trouvé) est ajouté à la requête sous forme de métadonnées avec l'adresse IP source interne.

6. La requête contenant les métadonnées est ensuite transférée au serveur WebTitan Web Filter Cloud où chaque requête est journalisée avec l'identification de l'utilisateur.

## PROXY DNS D'WEBTITAN WEB FILTER

Une fois configuré, le proxy DNS WebTitan Web Filter collecte les données d'utilisateur et de groupes de votre service de répertorie et les envoie à intervalles réguliers et de manière sécurisée à WebTitan Web Filter Cloud. Un ID d'utilisateur unique est reçu pour chaque utilisateur. Il est utilisé pour former les métadonnées qui sont ajoutées à toutes les requêtes DNS passant par le proxy DNS WebTitan Web Filter.

Si une requête concerne un domaine local, celle-ci est transférée au serveur DNS interne approprié.

**Configuration requise**

Avant de pouvoir installer les composants d' WebTitan Web Filter Cloud AD, la configuration suivante est requise :

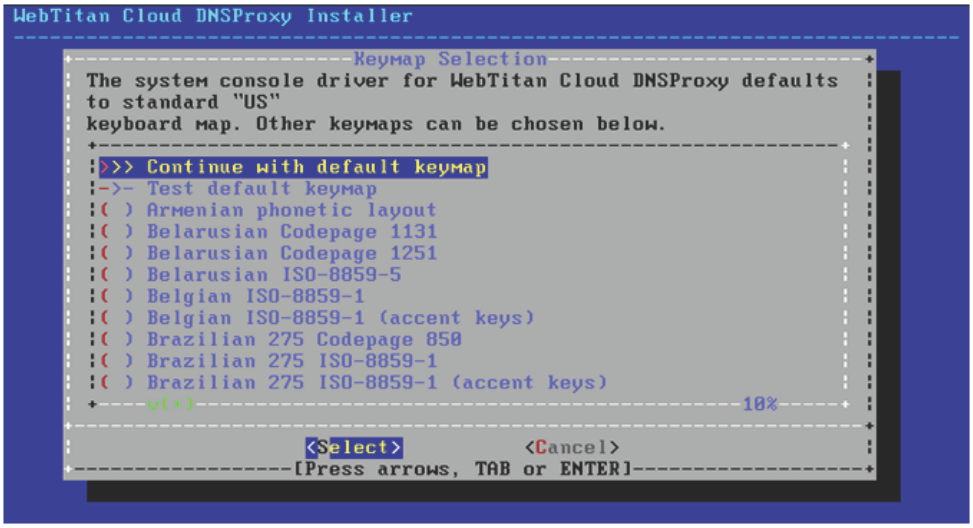
- VMware ESXi 4.1 ou ultérieur (peut également être installé sur un système nu) ;
- La configuration minimale requise pour l'appliance de proxy DNS est 1 CPU core', 512 Mo de RAM, 6 Go d'espace disque.

**Installez l'appliance de proxy DNS**

Les étapes suivantes décrivent le processus d'installation du proxy DNS WebTitan Web Filter à partir d'une image CD (ISO).

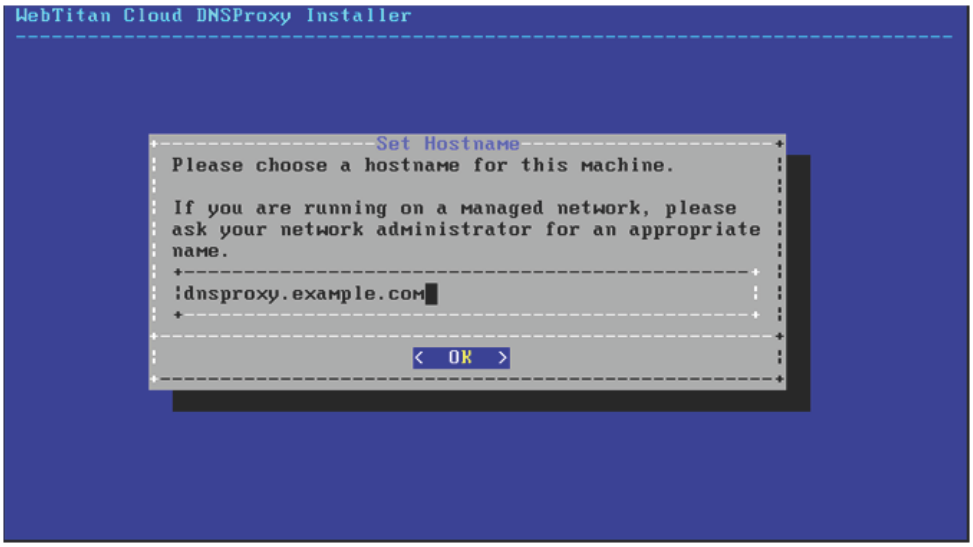
1. Après avoir déployé l'image ISO ou OVA, vous êtes invité(e) à configurer l'appliance.


2. Disposition du clavier



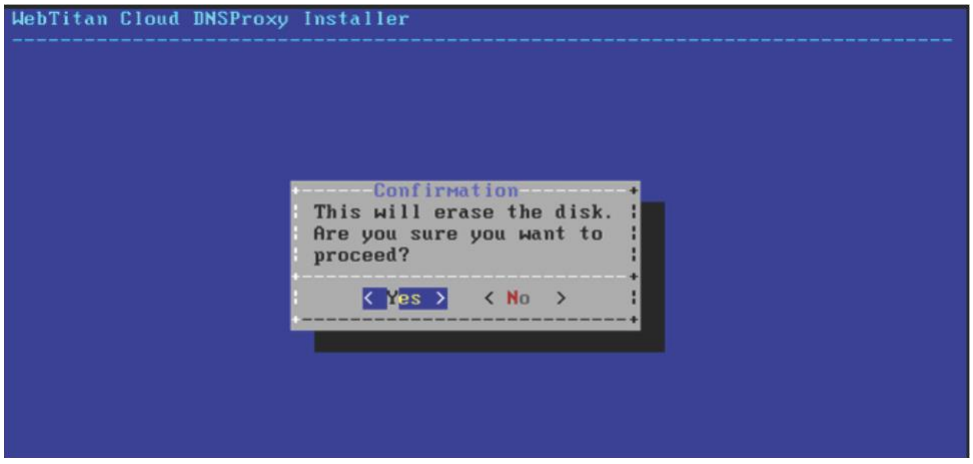

L'écran de la configuration du clavier est affiché. Il vous permet de choisir la disposition du clavier qui représente le plus fidèlement le mappage du clavier associé au système. En cas de doute, utilisez la configuration par défaut ou choisissez français de France ISO-8859-15.

3. Attribution du nom d’hôte



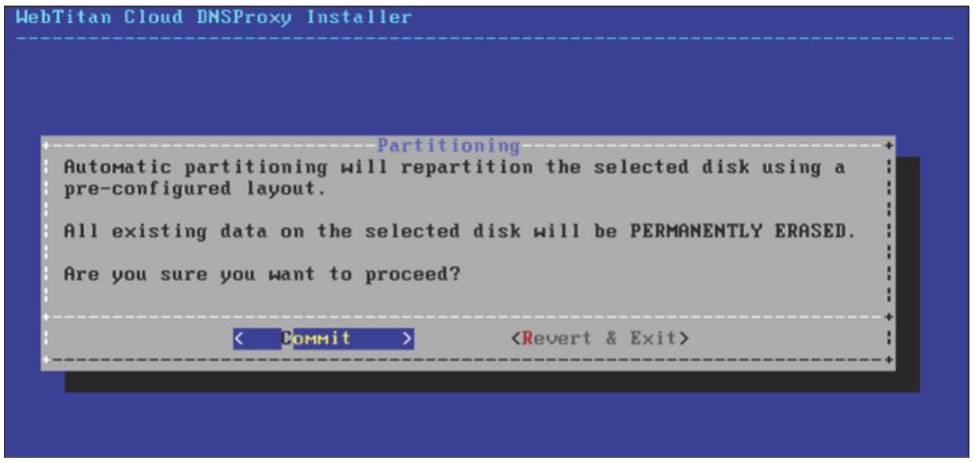

Le programme d’installation vous invite à donner un nom d’hôte à l’appliance qui vient d’être installée. Le nom d’hôte doit être pleinement nommé.

4. Validation




Sélectionnez <Oui> pour continuer.

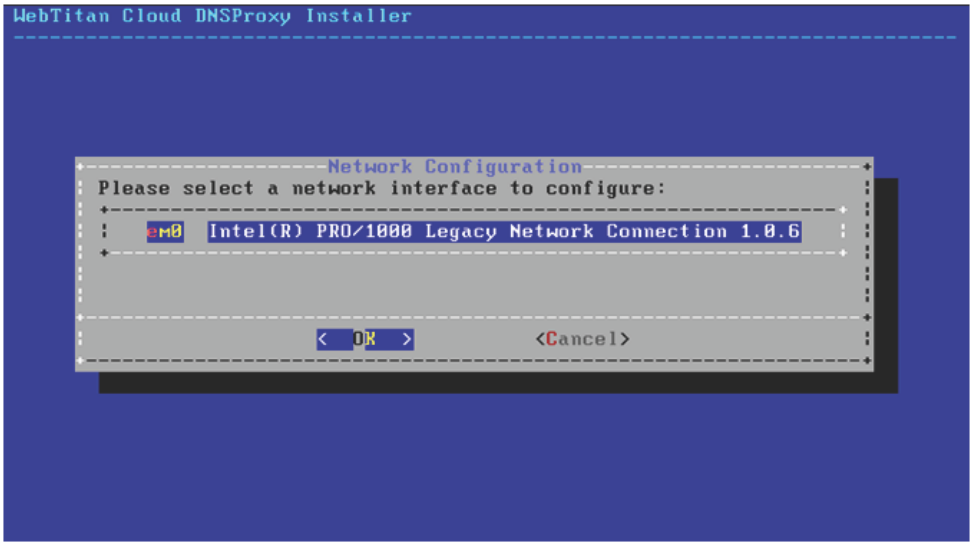
5. Partitionnement



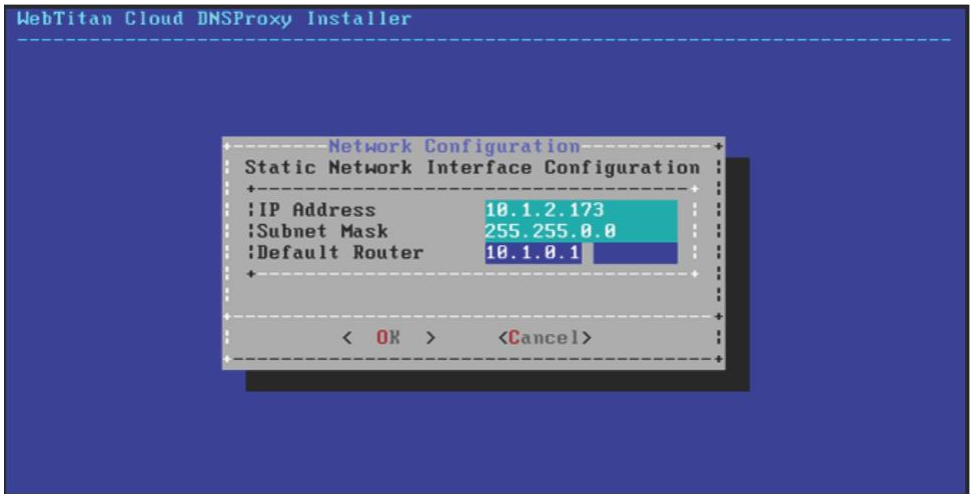
Le proxy DNS WebTitan Web Filter partitionne automatiquement le disque. Choisissez <Valider> pour continuer et partitionner le disque. Il s'agit de votre dernière chance d'interrompre l'installation afin de ne pas modifier le disque dur.

Après avoir vérifié l'intégrité de la distribution des fichiers pour s'assurer qu'il n'y a pas eu d'erreur de lecture sur le support d'installation, le programme d'installation extrait les fichiers distribués sur le disque.

6. Configuration de l'interface réseau



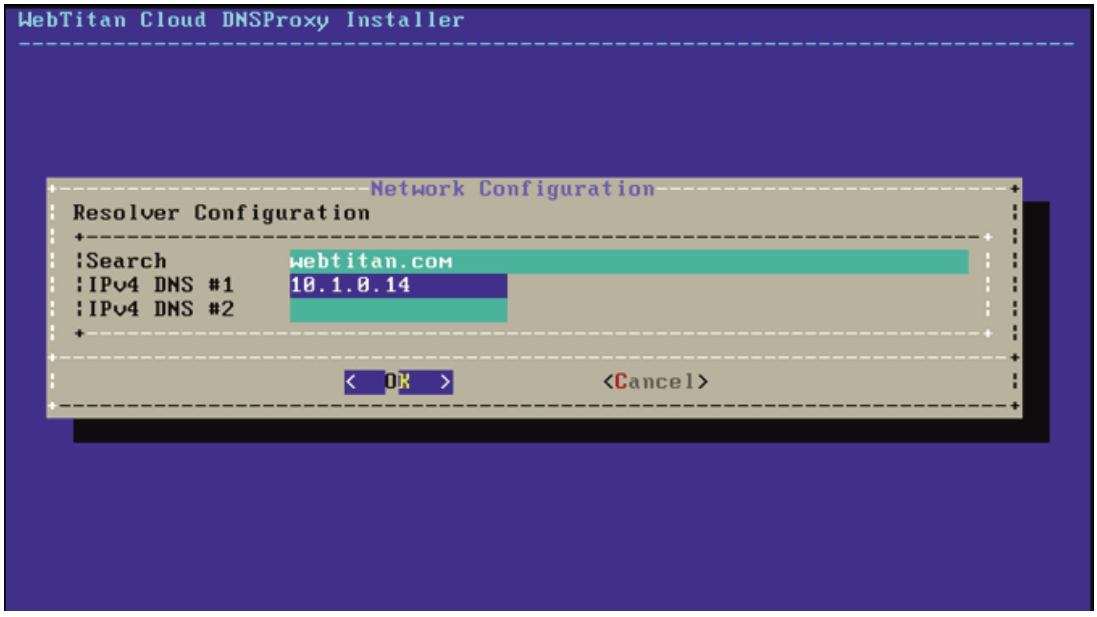

Une liste de toutes les interfaces réseau qui se trouvent sur l'ordinateur est présentée ci-après. Sélectionnez-en une à configurer.




L'application doit être configurée avec une adresse IP statique et ne permet pas de configurer l'interface à l'aide du protocole DHCP. La configuration statique de l'interface réseau nécessite certaines informations IPv4 :

- Adresse IP : adresse IPv4 à assigner manuellement à cet ordinateur. Cette adresse doit être unique et ne doit pas être déjà utilisée autre part sur le réseau local.
- Masque de sous-réseau : masque de sous-réseau utilisé pour le réseau local. En général, il s'agit de 255.255.255.0.
- Routeur par défaut : adresse IP du routeur/de la passerelle par défaut sur ce réseau.

7. Configuration DNS

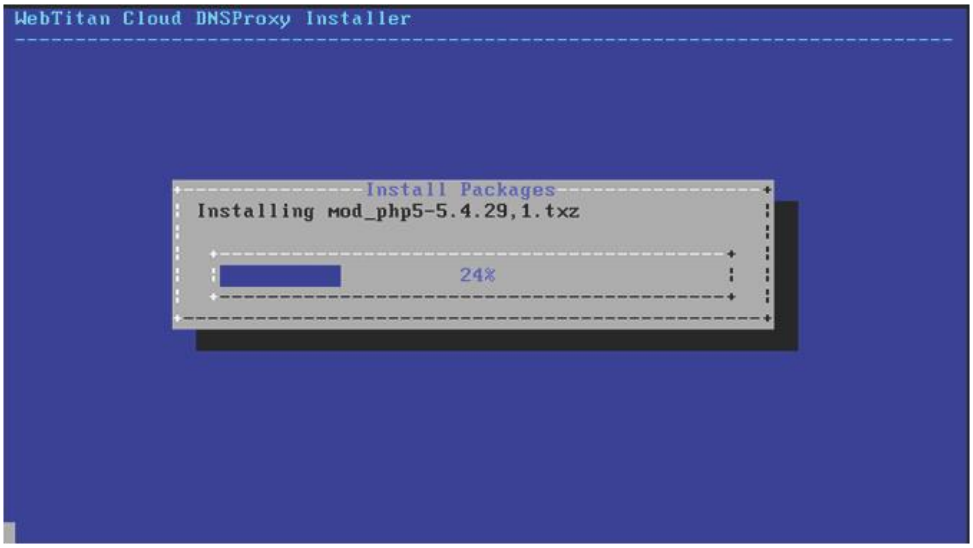



Le programme de résolution DNS (Domain Name System) convertit les noms d'hôte vers et depuis les adresses réseau. Saisissez le nom de domaine du réseau local dans le champ de recherche. Adresses DNS nº 1 et DNS nº 2 des serveurs DNS locaux. Au moins un serveur DNS est nécessaire.

8. Réglage du fuseau horaire


Le réglage du fuseau horaire de votre application lui permettra de répercuter automatiquement tout changement d'heure régional et d'effectuer correctement d'autres fonctions liées au fuseau horaire. Sélectionnez <Oui> ou <Non> en fonction de la configuration de l'horloge de la machine. Si vous ne savez pas si le système utilise le temps universel coordonné ou l'heure locale, sélectionnez <Non> afin de choisir la région locale et le pays.

9. Installation des paquets




Le programme d'installation poursuit ensuite par l'installation des paquets ainsi que par d'autres tâches d'installation.


Une fois que tout a été installé et configuré, le programme d'installation vous invite à redémarrer dans la nouvelle appliance. Sélectionnez <Redémarrer> pour redémarrer l'ordinateur et lancer la nouvelle application du proxy DNS WebTitan Web Filter. N'oubliez pas de retirer le support d'installation, car sinon l'ordinateur pourrait redémarrer à partir de celui-ci.

10. Fin de l'installation

Une fois que l'application a redémarré, utilisez l'URL affichée pour connecter votre navigateur à l'interface utilisateur Web du proxy DNS WebTitan Web Filter. L'interface utilisateur vous permettra de terminer la configuration de l'application du proxy DNS WebTitan Web Filter.

Connectez-vous avec les identifiants suivants :
**Administrateur : admin**
**Mot de passe : hiadmin**

Remarque : Si votre navigateur Internet ne se connecte pas à l'application, il est probable que ce soit dû à une mauvaise configuration des paramètres réseau. Vous pouvez corriger la configuration en vous connectant à la console.

## CONFIGURATION DU PROXY DNS

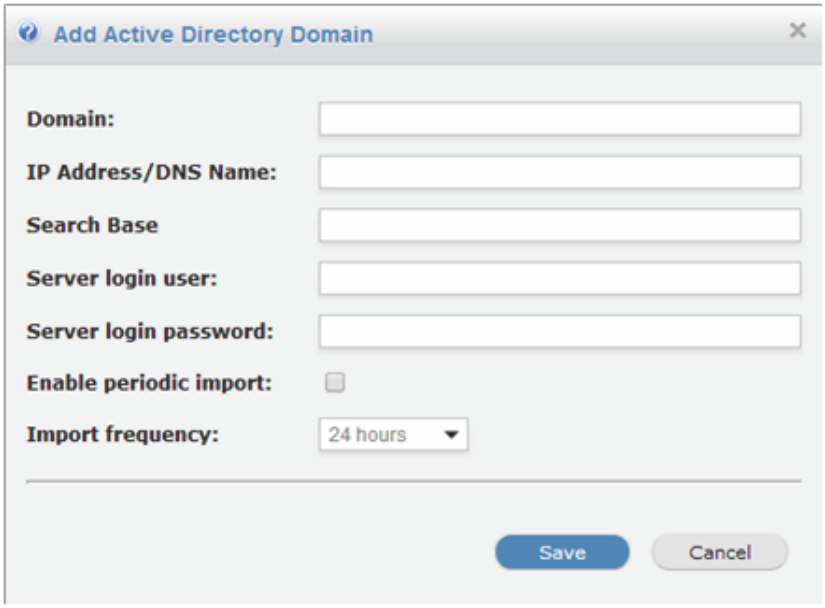
Une fois connecté à l'interface utilisateur, accédez à l'onglet Configuration afin de terminer la configuration de l'appliance du Proxy DNS.

Sous Réseau -> onglet Paramètres DNS, vous devez configurer l'appliance afin qu'elle achemine les requêtes DNS locales vers vos serveurs DNS existants. Le tableau des paramètres DNS contient la liste des requêtes qui doivent être redirigées vers les serveurs DNS locaux afin d'être résolues. Il est également possible de préciser des requêtes devant systématiquement être éliminées. Le tableau doit contenir la liste de toutes les zones internes (par ex., mondomaine.com) et de toutes les zones inversées. Par exemple, si votre réseau est 192.168.1/24, le domaine à ajouter est 1.168.192.in-addr.arpa. Toutes les autres requêtes seront transmises à WebTitan Web Filter cloud pour être résolues.

**Active Directory**

Afin qu'WebTitan Web Filter Cloud puisse rendre compte de l'activité des utilisateurs, vous devez d'abord importer tous vos utilisateurs depuis votre serveur Active Directory. Ils sont alors téléchargés de manière sécurisée vers WebTitan Web Filter Cloud, et des identifiants uniques sont renvoyés pour chaque utilisateur. Ensuite, lorsque le proxy DNS reçoit des requêtes DNS, s'il possède un nom d'utilisateur -> mappage IP (fourni par WebTitan Web Filter Active Directory Agent) pour l'adresse source de la requête DNS, alors ces identifiants uniques sont utilisés pour constituer les métadonnées ajoutées à la requête transmise à WebTitan Web Filter Cloud.

**Accédez à l'onglet Active Directory sous la section Configuration pour ajouter un domaine Active Directory. Cliquez sur « Ajouter », saisissez vos informations de serveur Active Directory et enregistrez.**




Pour pouvoir synchroniser les utilisateurs avec WebTitan Web Filter Cloud, vous devez indiquer vos références d'authentification d'WebTitan Web Filter Cloud.

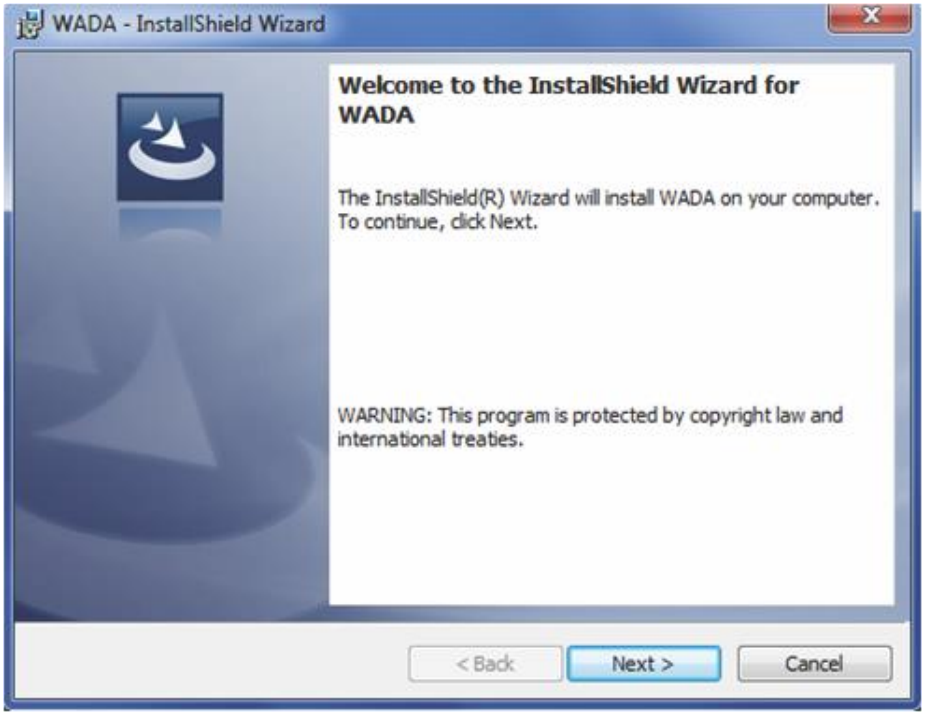
## WEBTITAN WEB FILTER ACTIVE DIRECTORY AGENT (WADA)

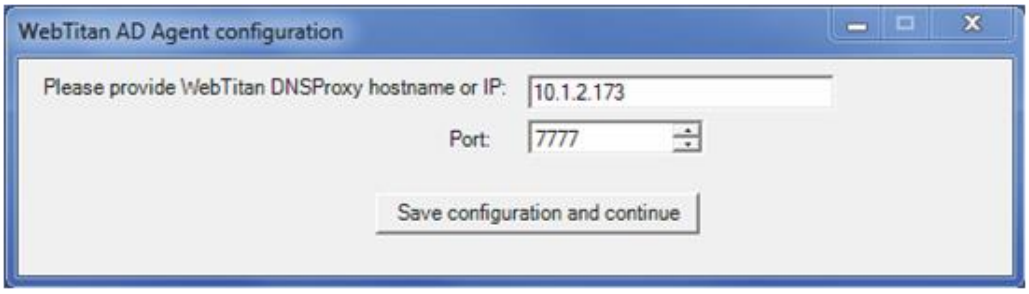
WebTitan Web Filter Active Directory Agent (WADA) est chargé de découvrir qui est connecté à quelle machine sur votre réseau Active Directory.
WADA doit être installé sur le contrôleur de domaine ou sur une machine depuis laquelle il peut communiquer avec :

- Windows Active Directory,
- le proxy DNS WebTitan Web Filter.

**Installation de WADA**

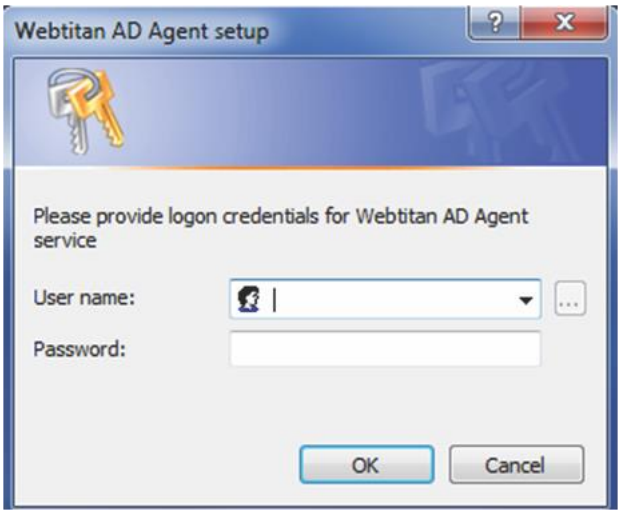
En tant qu'administrateur, lancez une invite de commandes avec élévation de privilèges et exécutez WADA.msi avec des privilèges d'administrateur. Suivez les étapes de l'assistant d'installation.

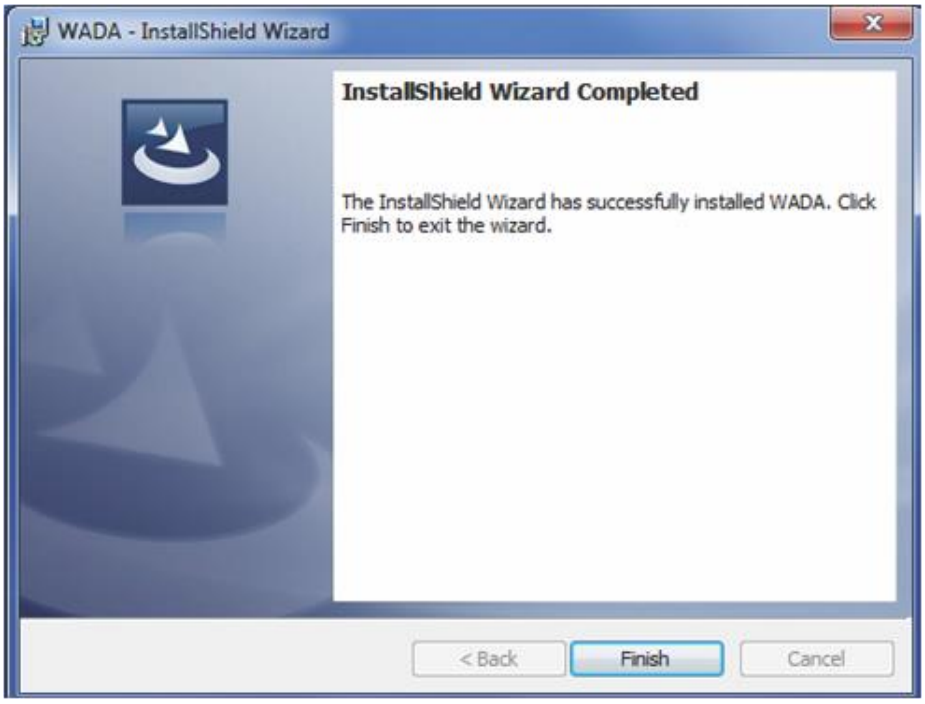



Vous êtes invité(e) à fournir le nom d'hôte ou l'adresse IP du proxy DNS WebTitan Web Filter ainsi que le numéro de port.

Vous êtes ensuite invité(e) à entrer le nom d'utilisateur et le mot de passe de WebTitan Web Filter AD Agent. Cet utilisateur doit être un membre du groupe Lecteurs des journaux des événements et du groupe Utilisateur du modèle COM distribué.




Le fichier de configuration WADA.ini se trouve sous C:\ProgramData\WebTitan Web FilterADAgent. Le fichier contient l'IP du proxy DNS WebTitan Web Filter et se présente comme suit :

```
[WADA]

WebTitanServers=http://10.1.2.173
```

Webtitan est le seul paramètre requis et peut contenir une liste d'URL séparées par « , » qui recevront la liste d'IP/utilisateurs dans les requêtes HTTP POST.

Les autres paramètres sont facultatifs mais peuvent se révéler utiles pour le débogage ou la personnalisation en fonction de besoins spécifiques :

- DiscoveryThreads (10 par défaut) – nombre de threads enfants utilisées dans le processus de découverte WMI. Chaque thread se connecte en parallèle à un ordinateur à l'aide de WMI pour accélérer le processus de découverte initial.

- DiscoveryIntMin (30) – nombre de minutes entre les découvertes (requêtes LDAP qui lisent la liste des ordinateurs disponibles, puis les contrôles WMI).

- LastLogonDays (365) – nombre maximal de jours depuis la dernière connexion à une machine afin d'être comparé aux sessions existantes avec WMI. Il est basé sur l'attribut LDAP lastLogon. Les ordinateurs dont le nombre de jours « d'inactivité » est supérieur sont omis.

- TTLMin (60) – nombre de minutes après lesquelles une paire IP/utilisateur est supprimée du mappage si la session de connexion active est introuvable sur une IP donnée au cours de cette durée (à partir des contrôles WMI, des événements du journal des événements ou de l'énumérateur des sessions réseau).

- EnumSessIntS (10) – nombre de secondes entre l'énumération des sessions réseau. Sachez que les sessions Windows XP ne sont visibles que 15 secondes environ, c'est pourquoi vous ne devez pas augmenter la valeur de ce paramètre car vous risqueriez de perdre des informations sur les sessions de connexion actives.

- WMICheckIntS (60) – nombre de secondes entre deux contrôles WMI sur un ordinateur donné. Cela sert à ne pas atteindre les ordinateurs Windows trop souvent pour éviter de les saturer.

- WMIMaxCheckRetry (10) – nombre de nouvelles tentatives lorsqu'une requête WMI à un ordinateur spécifique échoue. Si après ce nombre de nouvelles tentatives, la requête échoue toujours, une erreur est journalisée dans un fichier waderror.log et les sessions actives ne sont pas contrôlées sur cet ordinateur avec WMI, sauf en cas d'activité provenant d'autres sources (journal des événements, sessions réseau).

- DC – nom du contrôleur de domaine distant. Peut être utilisé pour exécuter WADA sur un autre ordinateur du réseau que le contrôleur de domaine lui-même.

- LogMinLevel – Niveau de débogage. 0 = débogage complet

## FAITES PASSER TOUT LE TRAFIC DNS PAR LE PROXY DNS WEBTITAN WEB FILTER

Pour rendre compte de l'activité des utilisateurs et appliquer des politiques sur celle-ci, tout le trafic DNS de tous les clients du réseau doit être acheminé à travers le proxy DNS WebTitan Web Filter. Si vous utilisez DHCP, cela peut être effectué facilement en modifiant les paramètres DNS de DHCP. Vous devrez attendre que les ordinateurs clients renouvellent leur bail ou qu'un utilisateur se connecte avant que les nouveaux paramètres soient appliqués.