Solution ESET Remote Administrator

Manuel d'installation
et Guide de l'utilisateur

we protect your digital worlds

sommaire

Solution ESET Remote Administrator

Service client Monde : www.eset.eu/support
Service client Amérique du Nord : www.eset.com/support

REV.20090514-010

1. Introduction

La solution ESET Remote Administrator (ERA) est une application permettant de gérer des produits d'ESET dans un environnement réseau comprenant des stations de travail et des serveurs à partir d'un emplacement central. Le système de gestion des tâches intégré dans la solution ESET Remote Administrator permet d'installer des solutions de sécurité ESET sur des ordinateurs distants et de réagir rapidement à de nouveaux problèmes et menaces.

La solution ESET Remote Administrator en elle-même n'offre pas d'autre forme de protection contre les codes malveillants (malware). ERA dépend de la présence sur des stations de travail ou des serveurs d'une solution de sécurité ESET telle qu'ESET NOD32 Antivirus ou ESET Smart Security.

Pour effectuer le déploiement complet d'un portefeuille de solutions de sécurité ESET, vous devez exécuter les étapes suivantes:
- Installation du serveur ERA (ERAS)
- Installation de la console ERA (ERAC)
- Installation de solutions de sécurité sur les postes clients (ESET NOD32 Antivirus, ESET Smart Security, Linux ESET Security client, etc...)

REMARQUE : Certaines parties de ce document utilisent des variables système faisant référence à l'emplacement précis de dossiers et de fichiers :
%ProgramFiles % = généralement C:\Program Files
%ALLUSERSPROFILE % = généralement C:\Documents and Settings\All Users

1.1 Architecture du programme

Techniquement, la solution ESET Remote Administrator comprend deux composants distincts : le serveur ERA (ERAS) et la console ERA (ERAC). Vous pouvez exécuter un nombre illimité de serveurs et consoles ERA au sein de votre réseau car le contrat de licence ne prévoit aucune limite à cet égard. La seule limite a trait au nombre total de clients que votre installation d'ERA peut administrer (voir la section 1.1.6, « Clés de licence »).

1.1.1 Serveur ERA (ERAS)

Le composant serveur d'ERA s'exécute comme service sous les systèmes d'exploitation de technologie Microsoft Windows® NT suivants : NT4, 2000, XP, 2003, Vista et 2008. La principale tâche de ce service est de collecter des informations de clients et de leur envoyer diverses requêtes. Ces requêtes, telles que des tâches de configuration et des demandes d'installation à distance, sont créées à l'aide de la console ERA (ERAC). ERAS est un point de rencontre entre ERAC et des ordinateurs clients, soit un emplacement où toutes les informations sont traitées, conservées ou modifiées avant leur transfert vers des clients ou vers ERAC.

1.1.2 Console ERA (ERAC)

ERAC est la console d'ERA, généralement installé sur une station de travail. Cette dernière est utilisée par l'administrateur pour contrôler à distance des solutions ESET sur des clients individuels. ERAC permet à l'administrateur de se connecter au composant serveur d'ERA sur le port TCP 2223. La communication est contrôlée par le processus console.exe, généralement situé dans le répertoire suivant :

%ProgramFiles %\ESET\ESET Remote Administrator\Console

Lors de l'installation d'ERAC, il se peut que vous deviez entrer un nom d'ERAS. Au démarrage, la console se connectera automatiquement à ce serveur. Il est également possible de configurer ERAC après l'installation.

ERAC génère des journaux graphiques au format HTML qui sont enregistrés localement. Toutes les autres informations sont envoyées à partir d'ERAS sur le port TCP 2223.

2. Installation du serveur ERA et de la console ERA

2.1 Configuration requise

ERAS fonctionne en tant que service. Il a donc besoin d'un système d'exploitation de technologie Microsoft Windows NT (NT4, 2000, XP, 2003, Vista ou 2008). ERAS n'a pas besoin de Microsoft Windows Server Edition pour fonctionner. Un ordinateur sur lequel ERAS est installé doit toujours être en ligne et accessible via un réseau informatique par :

- des clients (généralement des stations de travail) ;
- un PC avec une console ERA ;
- d'autres instances d'ERAS (en cas de réplication).

2.1.1 Configuration matérielle requise

L'effet sur les performances système est minime. Toutefois, il dépend du nombre de clients, du type de base de données utilisée par ERAS, du niveau de journalisation, etc. La configuration matérielle minimale pour le déploiement d'ERAS est identique à la configuration minimale recommandée pour le système d'exploitation Microsoft Windows utilisé sur l'ordinateur.

2.1.2 Ports utilisés

Le diagramme ci-dessous présente les communications réseau pouvant être utilisées une fois ERAS installé. Le processus EHttpSrv.exe écoute sur le port TCP 2221 et le processus era.exe sur les ports TCP 2222, 2223, 2224 et 2846. Les communications sont effectuées à l'aide des processus natifs du système d'exploitation (p. ex., « NetBIOS sur TCP/IP »).

Protocole	Port	Description
TCP	2221 (écoute d'ERAS)	Port par défaut utilisé par la fonctionnalité Miroir intégrée dans ERAS (version HTTP)
TCP	2222 (écoute d'ERAS)	Communication entre clients et ERAS
TCP	2223 (écoute d'ERAS)	Communication entre ERAC et ERAS

En cas d'utilisation de toutes les fonctionnalités du programme, les ports réseau suivants doivent être ouverts :

Protocole	Port	Description
TCP	2224 (écoute d'ERAS)	Communication entre l'agent einstaller.exe et ERAS durant une installation à distance
TCP	2846 (écoute d'ERAS)	Réplication ERAS
TCP	139 (port cible du point de vue d'ERAS)	Copie de l'agent einstaller.exe à partir d'ERAS vers un client à l'aide du partage admin$
UDP	137 (port cible du point de vue d'ERAS)	« Résolution de nom » durant une installation à distance
UDP	138 (port cible du point de vue d'ERAS)	« Navigation » durant une installation à distance
TCP	445 (port cible du point de vue d'ERAS)	Accès direct à des ressources partagées à l'aide du protocole TCP/IP durant une installation à distance (alternative à TCP 139)

Tous les ports figurant dans le tableau ci-dessus doivent être ouverts pour que tous les composants d'ERA fonctionnent correctement.

Il est possible de modifier les ports prédéfinis 2221, 2222, 2223, 2224 et 2846 s'ils sont déjà utilisés par d'autres applications.

Pour modifier les ports par défaut utilisés par ERA, cliquez sur ***Outils > Options du serveur...*** Pour modifier le port 2221, sélectionnez l'onglet ***Mises à jour***, puis modifiez la valeur ***Port du serveur HTTP***. Vous pouvez modifier les ports 2222, 2223, 2224 et 2846 dans la section ***Ports*** sous l'onglet ***Autres paramètres***.

Vous pouvez également modifier les ports 2222, 2223, 2224 et 2846 en mode d'installation avancée (ERAS).

2.2 Guide d'installation de base

2.2.1 Vue d'ensemble de l'environnement (structure du réseau)

Un réseau de société consiste généralement en réseau local (LAN). Nous suggérons donc d'installer un ERAS et un serveur Miroir. Vous pouvez créer le serveur Miroir soit dans ERAS soit dans ESET NOD32 Antivirus Business Edition ou ESET Smart Security Business Edition.

Supposons que tous les clients sont des stations de travail et des portables Microsoft Windows 2000/XP/Vista mis en réseau à l'intérieur d'un domaine. Le serveur nommé GHOST est en ligne en permanence et peut être une station de travail Windows Professionnel ou Windows Server (ce ne doit pas être un serveur Active Directory). En outre, supposons que les portables ne soient pas présents dans le réseau de la société durant l'installation des solutions client d'ESET. La structure du réseau pourrait ressembler à celle présentée ci-dessous :

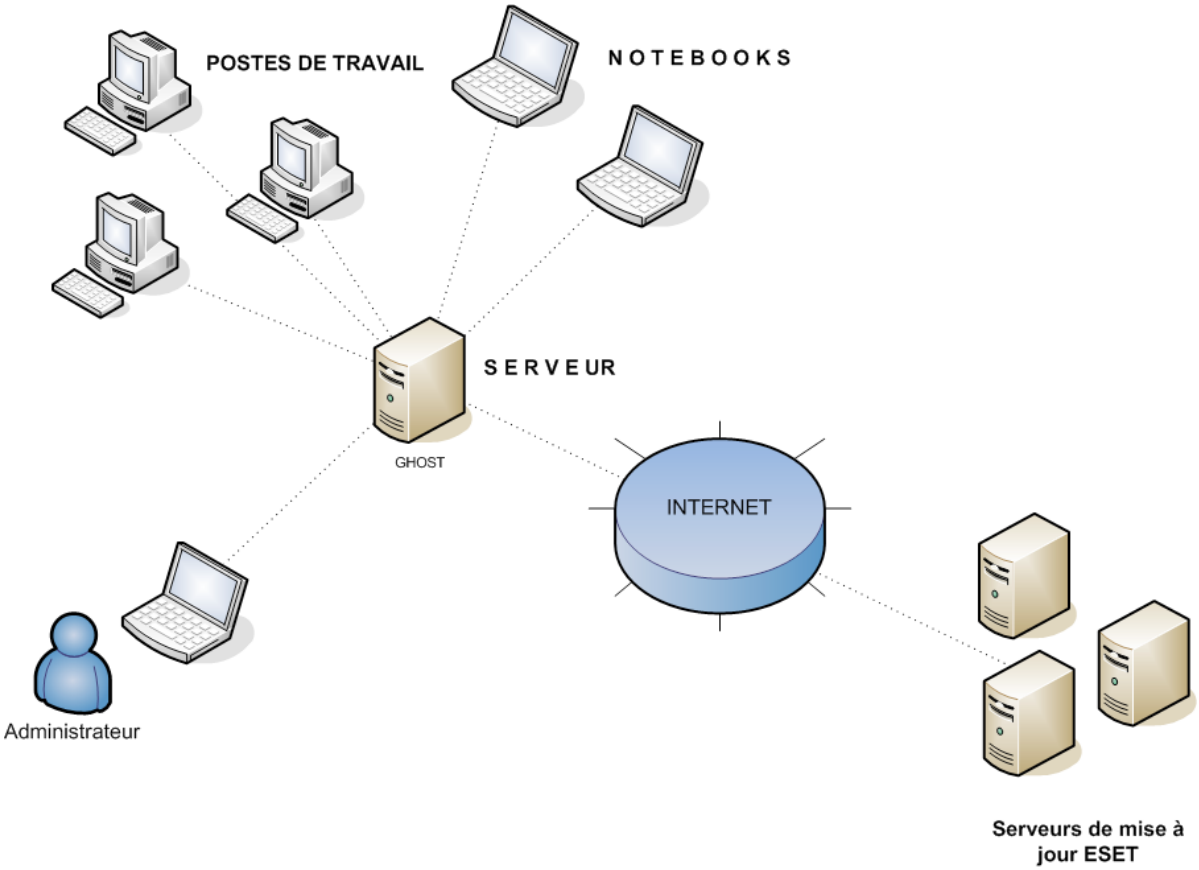


Figure 2-1

2.2.2 Avant l'installation

Avant de procéder à l'installation, vous devez télécharger les packages d'installation suivants du site Web d'ESET :

Composants d'ESET Remote Administrator :

ESET Remote Administrator – Serveur
ESET Remote Administrator – Console

Solutions client d'ESET :

ESET Smart Security
ESET NOD32 Antivirus 4.0
ESET NOD32 Antivirus 3.0
ESET NOD32 Antivirus 2.7

Ne téléchargez que les solutions correspondant à votre licence et que vous utiliserez sur les postes clients.

2.2.3 Installation

2.2.3.1 Installation du serveur ERA

Installez ERAS sur le serveur nommé GHOST. Vous pouvez sélectionner le mode d'installation Standard ou Avancé.

Si vous sélectionnez le mode Standard, le programme vous invite à insérer une clé de licence, fichier portant l'extension .lic qui assure le fonctionnement d'ERAS pendant la période définie dans la licence. Ensuite, le programme vous demande de définir les paramètres de mise à jour (nom d'utilisateur, mot de passe et serveur de mise à jour). Vous pouvez cependant passer à l'étape suivante et entrer les paramètres de mise à jour ultérieurement.

Si vous sélectionnez le mode d'installation Avancé, le programme d'installation propose de définir des paramètres supplémentaires. Vous pouvez modifier ces paramètres ultérieurement via ERAC, mais, dans la plupart des cas, ce n'est pas nécessaire. La seule exception est le nom de serveur qui doit être identique au nom DNS, soit la valeur %COMPUTERNAME % de votre système d'exploitation ou l'adresse IP attribuée à l'ordinateur. Il s'agit de l'élément d'information le plus essentiel pour l'exécution d'une installation à distance. Si le nom n'est pas spécifié durant l'installation, le programme d'installation fournit automatiquement la valeur de la variable système %COMPUTERNAME % qui suffit dans la plupart des cas.

Il est également important de sélectionner la base de données correcte dans laquelle stocker les informations d'ERAS. Pour plus d'informations, consultez la section 2.2.3.4 « *Types de base de données pris en charge par le serveur ERA.* »

Par défaut, les composants programme ERAS sont installés dans le dossier suivant :

%ProgramFiles %\ESET\ESET Remote Administrator\Server

Les autres composants de données, tels que les journaux, les packages d'installation, la configuration, etc. sont stockés dans :

%ALLUSERSPROFILE %\Application Data \ESET\ESET Remote Administrator\Server

Après l'installation, le service ERAS démarre automatiquement. L'activité du service ERAS est enregistrée dans l'emplacement suivant :

%ALLUSERSPROFILE %\Application Data\ESET\ESET Remote Administrator\Server\logs\era.log

2.2.3.2 Installation de la console ERA

Installez le console ESET Remote Administrator sur le PC/portable de l'administrateur (comme illustré dans la partie inférieure gauche de la figure 2-1). À la fin de l'installation en mode Avancé, entrez le nom du serveur ERA (ou son adresse IP) auquel l'ERAC se connecte automatiquement au démarrage. Elle est nommée GHOST dans notre exemple.

Après l'installation, lancez ERAC, puis contrôlez la connexion à ERAS. Par défaut, aucun mot de passe n'est requis pour se connecter à un serveur ERA (le champ de texte du mot de passe est vide) mais il est fortement recommandé d'en définir un. Pour créer un mot de passe pour se connecter à un serveur ERA :
cliquez sur ***Fichier*** > ***Modifier le mot de passe...***, puis modifiez le Mot de passe pour la console en cliquant sur le bouton Modifier...

L'administrateur peut spécifier un mot de passe pour l'accès administrateur et pour l'accès en lecture seule (qui permet uniquement d'afficher la configuration d'ERAS).

2.2.3.3 Activation et configuration du Miroir

Vous pouvez utiliser la console ERA pour activer le serveur de mise à jour du réseau local, appelé le Miroir dans le serveur ERA. Ce serveur peut faire office de source de fichiers de mise à jour pour les stations de travail situées dans le réseau local. En activant le Miroir, vous réduisez le volume des données transférées via votre connexion Internet.

Procédez comme suit :
1. Connectez la console ERA au serveur ERA en cliquant sur ***Fichier*** > ***Connexion***.
2. Dans la console ERA, cliquez sur ***Outils > Options du serveur...***, puis cliquez sur l'onglet ***Mises à jour***.
3. Dans le menu déroulant Serveur de mise à jour, sélectionnez ***Choisir automatiquement***, puis laissez la valeur Intervalle de mise à jour définie sur 60 minutes. Insérez **Nom d'utilisateur de mise à jour** (EAV-***), cliquez sur ***Définir le mot de passe...***, puis tapez ou collez le mot de passe que vous avez reçu avec votre nom d'utilisateur.
4. Sélectionnez l'option ***Créer un miroir de mise à jour***. Conservez le chemin d'accès par défaut pour les fichiers miroir et le port du serveur HTTP (2221). Laissez la valeur d'**Authentification** définie sur NONE.
5. Cliquez sur l'onglet ***Autres paramètres***, puis sur ***Modifier les paramètres avancés...*** Dans l'arborescence de la configuration avancée, accédez à ***Serveur ERA > Configuration > Miroir > Créer un miroir pour les composants programme sélectionnés***. Cliquez sur ***Edition*** du côté droit, puis sélectionnez les composants programme à télécharger. Vous devez sélectionner les composants pour toutes les versions linguistiques qui seront utilisées dans le réseau.
6. Sous l'onglet Mises à jour, cliquez sur ***Mettre à jour maintenant*** pour créer le Miroir.

Pour des options de configuration du Miroir plus détaillées, consultez la section 7.3.3, « *Activation et configuration du Miroir* ».

2.2.3.4 Types de base de données pris en charge par le serveur ERA

Par défaut, le programme utilise le moteur Microsoft Access (base de données Jet). ERAS 3.0 prend également en charge les bases de données suivantes :
- Microsoft SQL Server
- MySQL
- Oracle

Vous pouvez sélectionner le type de base de données durant l'installation en mode avancé d'ERAS. Après l'installation, il est impossible de modifier la version de base de données.

2.2.3.4.1 Configuration de base

Tout d'abord, il est nécessaire de créer la base de données sur un serveur de base de données. Le programme d'installation d'ERAS est capable de créer une base de données MySQL vide qui est automatiquement nommée *ESETRADB*.

Par défaut, le programme d'installation crée automatiquement une base de données. Pour créer la base de données manuellement, activez l'option ***Exporter le script***. Assurez-vous que l'option ***Créer automatiquement des tables dans la nouvelle base de données*** est désactivée.

2.2.3.4.2 Configuration de connexion de base de données

Après avoir créé une base de données, vous devez spécifier des paramètres de connexion pour le serveur de base de données à l'aide d'une des deux options suivantes :

1. En utilisant le DSN (nom de la source de données)
   Pour ouvrir le DSN manuellement, ouvrez l'administrateur de source de données OBCD (Cliquez sur ***Démarrer –> Exécuter –***, puis tapez ***odbcad32.exe***).

   Exemple de connexion DSN :
   DSN =ERASqlServer

2. Directement, en utilisant une chaîne de connexion complète
   Vous devez spécifier tous les paramètres requis – *pilote*, *serveur* et *nom de base de données*.

   Voici un exemple de chaîne de connexion complète pour MS SQL Server :
   Driver ={SQL Server}; Server =hostname; Database =ESETRADB

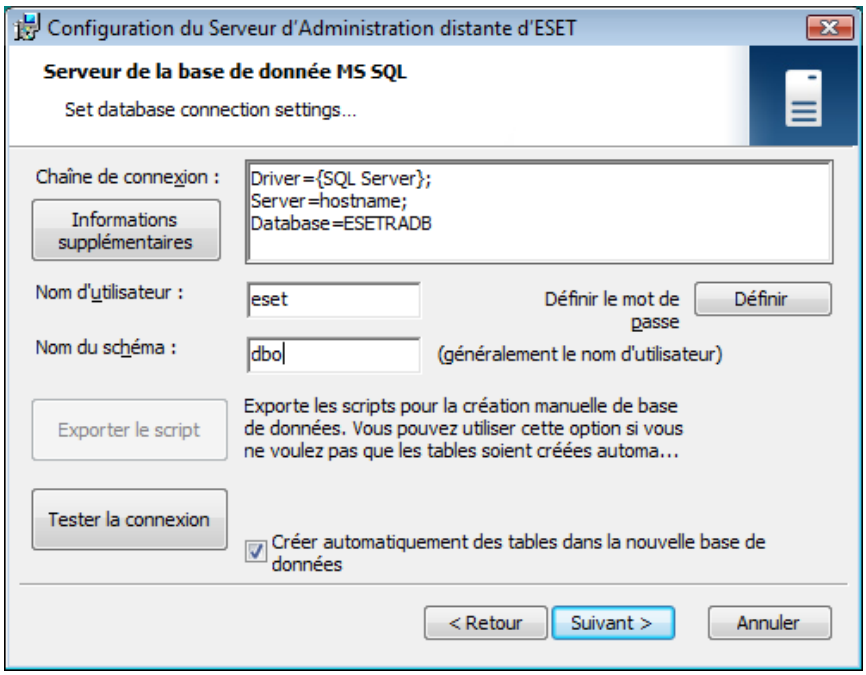


Figure 2-2

Voici un exemple de chaîne de connexion complète pour Oracle Server :
Driver ={Oracle in instantclient10_1}; dbq =hostname:1521/ESETRADB

Voici un exemple de chaîne de connexion complète pour MySQL Server :
Driver ={MySQL ODBC 3.51 Driver}; Server =hostname; Database =ESETRADB

Définissez ensuite le ***Nom d'utilisateur*** et le mot de passe pour la connexion (bouton ***Définir***). Les bases de données Oracle et MS SQL Server requièrent également un ***nom de schéma*** (pour MS SQL Server, il s'agit généralement du nom d'utilisateur).
Cliquez sur ***Tester la connexion*** pour vérifier la connexion au serveur de base de données.

2.2.3.4.3 Installation sur une base de données existante

Si la base de données contient des tables, le programme d'installation affiche une notification. Pour remplacer le contenu d'une table existante, sélectionnez ***Remplacer*** (avertissement : cette commande supprime le contenu de tables et remplace leur structure !). Sélectionnez ***Ignorer*** pour laisser les tables intactes.

*REMARQUE : Dans certaines conditions, l'activation de **Ignorer** peut entraîner des erreurs d'incohérence de base de données, en particulier quand des tables sont endommagées ou incompatibles avec la version actuelle.*

Pour annuler l'installation d'ERAS et analyser la base de données manuellement, cliquez sur ***Annuler***.

2.2.3.5 installation à distance sur des stations de travail client dans le réseau

En supposant que toutes les stations de travail sont actives, la méthode d'installation poussée (push install) est la plus efficace. Avant de commencer une installation poussée, vous devez télécharger les fichiers d'installation .msi pour ESET Smart Security ou ESET NOD32 Antivirus du site Web d'ESET et créer un package d'installation. Vous pouvez créer un fichier de configuration XML qui sera appliqué automatiquement lors de l'exécution du package. Pour plus d'informations sur l'installation à distance, consultez le chapitre 4. Installation des solutions client ESET ».

2.2.3.6 Installation à distance sur des portables non présents dans le réseau

Les portables situés hors du réseau local requièrent un autre type d'installation à distance, car l'installation doit avoir lieu après leur ouverture de session dans le domaine. Pour ces appareils, la méthode de script de connexion est conseillée.

Pour plus d'informations sur l'installation à distance à l'aide d'un script de connexion, consultez la section 4. Installation des solutions client ESET ».

2.3 Scénario – Installation dans un environnement d'entreprise

2.3.1 Vue d'ensemble de l'environnement (structure du réseau)

Vous pouvez voir ci-dessous une copie de la structure de réseau précédente avec une filiale supplémentaire, plusieurs clients et un serveur nommé LITTLE. Supposons qu'il y ait un canal VPN lent entre le siège central et la filiale. Dans ce scénario, le serveur Miroir doit être installé sur le serveur LITTLE. Nous allons également installer un second serveur ERA sur LITTLE pour créer un environnement plus convivial et réduire le volume des données transférées.

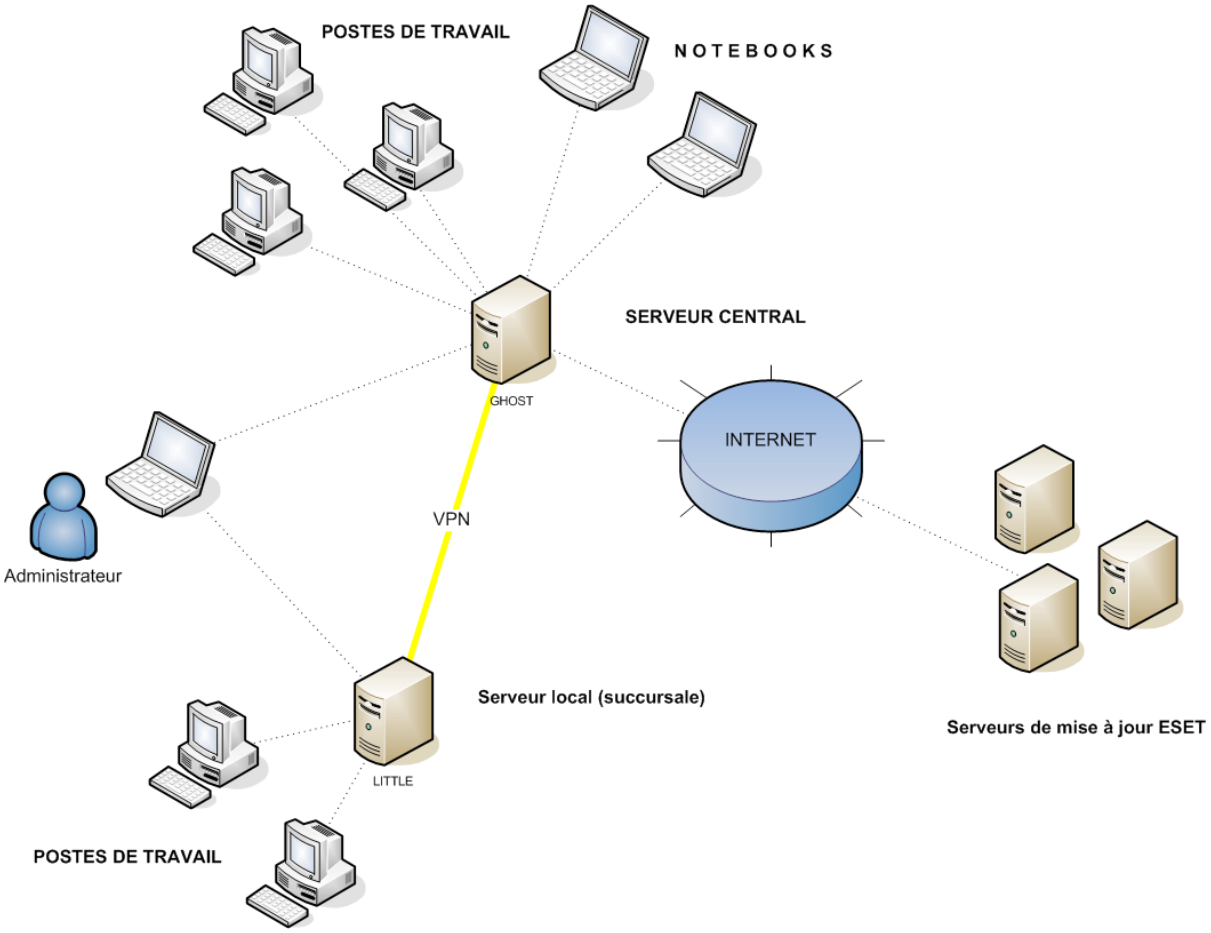


Figure 2-3

2.3.3 Installation

2.3.3.1 Installation au siège central

Les installations d'ERAS, d'ERAC et des stations de travail client sont très similaires au scénario précédent. La seule différence réside dans la configuration de l'ERAS maître (GHOST). Dans ***Outils > Options du serveur... > Réplication***, activez la case à cocher ***Activer la réplication « de »***, puis entrez le nom du serveur secondaire dans ***Serveurs autorisés***. Dans notre cas, le serveur de niveau inférieur est nommé LITTLE.

Si un mot de passe pour la réplication est défini sur le serveur de niveau supérieur (***Outils > Options du serveur... > Sécurité > Mot de passe pour la réplication***), ce mot de passe doit être utilisé pour l'authentification du serveur de niveau inférieur.

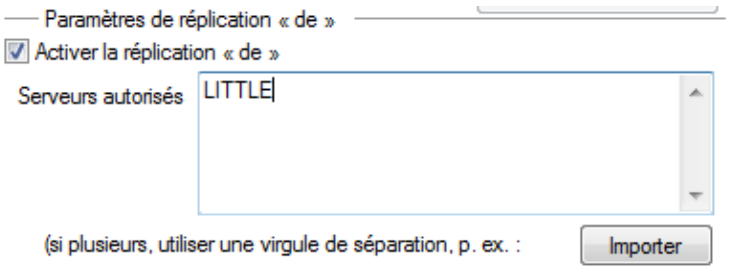


Figure 2-4

2.3.3.2 Filiale : Installation du serveur ERA

Comme dans l'exemple ci-dessus, installez le second ERAS et ERAC. Activez et configurez de nouveau les paramètres de réplication. Cette fois, activez la case à cocher Activer la réplication « sur » (***Outils > Options du serveur... > Réplication***), puis définissez le nom de l'ERAS maître. Il est recommandé d'utiliser l'adresse IP du serveur maître[1], qui est l'adresse IP du serveur GHOST.

Figure 2-5

2.3.3.3 Filiale : Installation du serveur Miroir HTTP

Vous pouvez également utiliser la configuration d'installation du serveur Miroir de l'exemple précédent dans ce cas. Les seuls changements figurent dans les sections définissant le nom d'utilisateur et le mot de passe.

Comme illustré à la figure 2-3, les mises à jour pour la filiale ne sont pas téléchargées des serveurs de mise à jour d'ESET, mais du serveur situé au siège central (GHOST). La source de mise à jour est définie par l'adresse URL suivante :

http://ghost:2221 (ou http://IP_adresse_de_ghost:2221)

Par défaut, il n'est pas nécessaire de spécifier un nom d'utilisateur ou un mot de passe parce le serveur HTTP intégré ne requiert pas d'authentification.

Pour plus d'informations sur la configuration du Miroir dans ERAS, consultez la section 7.3, « Serveur Miroir ».

2.3.3.4. Filiale : Installation à distance sur des clients

Une fois encore, vous pouvez utiliser le modèle précédent, si ce n'est qu'il ne convient pas pour effectuer toutes les opérations avec l'ERAC connectée directement à l'ERAS de la filiale (LITTLE) [2].

2.3.4 Autres exigences pour les environnements d'entreprise

Dans les grands réseaux, il est possible d'installer plusieurs serveurs ERA pour effectuer des installations à distance d'ordinateurs client à partir de serveurs plus accessibles. À cette fin, ERAS offre une fonctionnalité de « réplication » (voir les sections 2.3.3.1 et 2.3.3.2) qui permet de transférer des informations stockées à un parent ERAS (« serveur de niveau supérieur »). Il est possible de configurer la réplication à l'aide d'ERAC.

---

1 Afin d'éviter d'éventuels problèmes de translation DNS lors de la conversion de noms en adresses IP entre réseaux (en fonction de la configuration DNS).

2 Cela vise à empêcher le transfert des packages d'installation via le canal VPN qui est plus lent.

La fonctionnalité de réplication est très utile pour les sociétés disposant de plusieurs filiales ou bureaux distants. Le scénario de déploiement modèle serait le suivant : Installez ERAS dans chaque bureau et faites en sorte de répliquer chaque ERAS sur un ERAS central. L'avantage de cette configuration est particulièrement apparent dans les réseaux privés qui sont connectés via un VPN qui est habituellement plus lent ; l'administrateur doit uniquement se connecter à un ERAS central (la communication marquée par la lettre A dans la figure 2-6). Il n'est pas nécessaire d'utiliser de VPN pour accéder à des départements individuels (les communications B, C, D et E). Le canal de communication plus lent est contourné par l'utilisation de la réplication ERAS.

La configuration de la réplication permet à un administrateur de définir les informations à transférer aux serveurs de niveau supérieur automatiquement à un intervalle prédéfini, ainsi que les informations à envoyer sur demande de l'administrateur du serveur de niveau supérieur. La réplication rend ERA plus convivial et réduit le trafic réseau.

Un autre avantage de la réplication est que plusieurs utilisateurs peuvent se connecter avec divers niveaux d'autorisation. L'administrateur accédant à l'ERAS london2.company.com avec la console (communication E) ne peut contrôler que les clients se connectant à london2.company.com. L'administrateur accédant au central company.com (A) peut contrôler tous les clients se trouvant au siège central de la société et dans les différents départements/filiales.

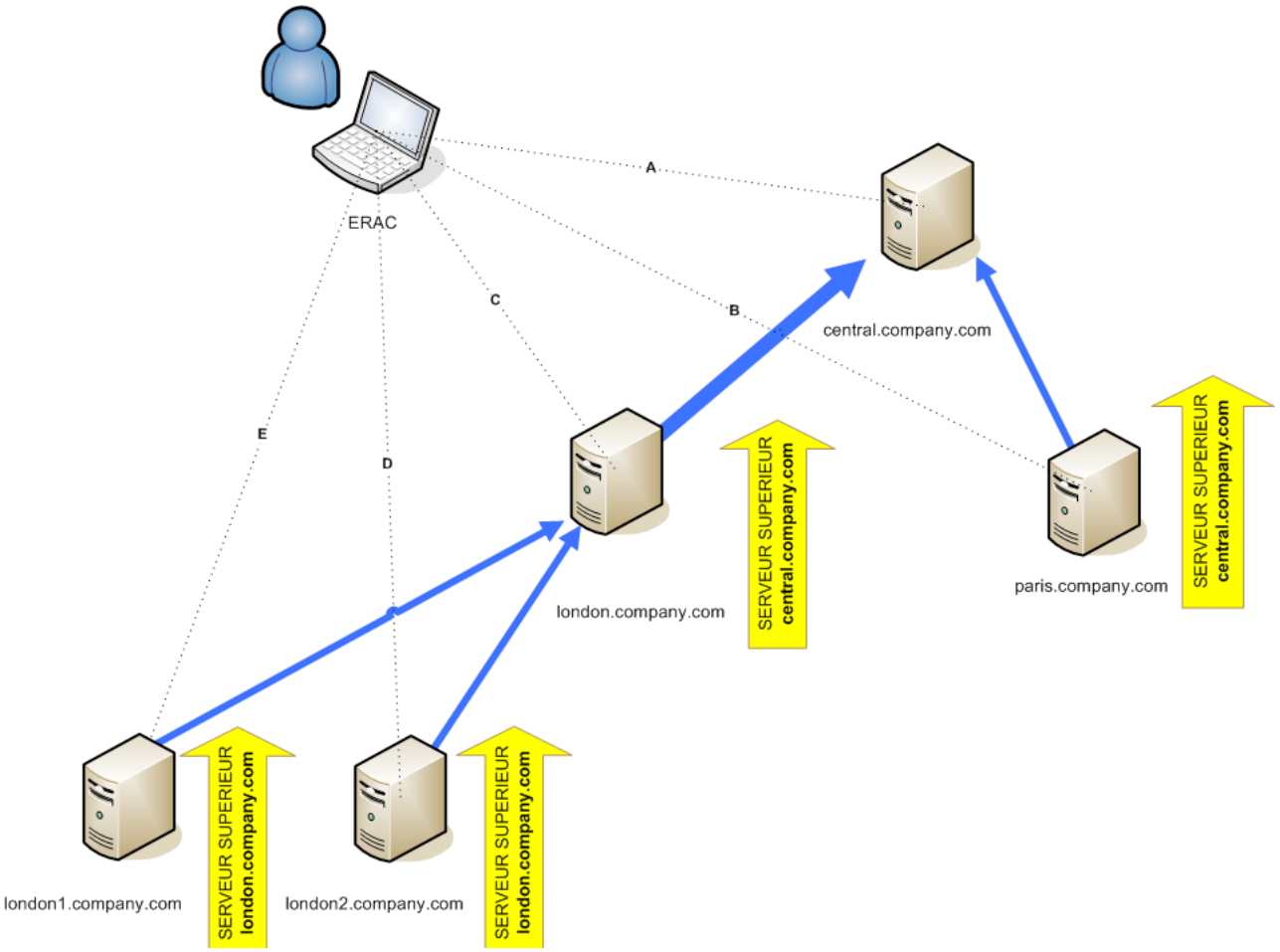


Figure 2-6

3. Utilisation d'ERAC

3.1 Connexion à ERAS

La plupart des fonctionnalités d'ERAC ne sont disponibles qu'après connexion à ERAS. Définissez le serveur par son nom ou son adresse IP avant la connexion :

Ouvrez l'ERAC, cliquez sur ***Fichier*** > ***Modifier les connexions***... (ou sur ***Outils*** > ***Options de la console...***), puis cliquez sur l'onglet ***Connexion***.

Cliquez sur le bouton ***Ajouter/Supprimer*** pour ajouter de nouveaux serveurs ERA ou modifier des serveurs actuellement répertoriés. Sélectionnez le serveur souhaité dans le menu déroulant **Sélectionner une connexion**. Cliquez ensuite sur le bouton **Connexion**.

Autres options de cette fenêtre :

- ***Connexion au serveur sélectionné au démarrage de la console***
  Si cette option est activée, la console se connecte automatiquement à l'ERAS sélectionné au démarrage.
- ***Afficher un message en cas d'échec de connexion***
  En cas d'erreur de communication entre ERAC et ERAS, un message d'alerte s'affiche.

Il est possible de protéger les connexions par mot de passe. Par défaut, aucun mot de passe n'est requis pour se connecter à un serveur ERAS, mais il est fortement recommandé d'en définir un. Pour créer un mot de passe pour se connecter à un serveur ERAS :

Cliquez sur ***Fichier*** > ***Modifier mot de passe***, puis cliquez sur le bouton ***Modifier...*** à droite de ***Mot de passe pour la console***.

Lors de l'entrée d'un mot de passe, vous pouvez activer l'option ***Mémoriser le mot de passe***. Songez au risque possible pour la sécurité lié à l'usage de cette option. Pour supprimer tous les mots de passe mémorisés, cliquez sur ***Fichier*** > ***Effacer les mots de passe en cache...***

Une fois la communication établie, l'en-tête du programme devient *Connecté [nom_serveur]*.
Vous pouvez également cliquer sur ***Fichier*** > ***Connexion*** pour vous connecter au serveur ERAS.
Au démarrage du programme, dans le menu déroulant **Accès**, sélectionnez le **Type d'accès** (**Administrateur** ou **Lecture seule**).

3.2 ERAC – Fenêtre principale

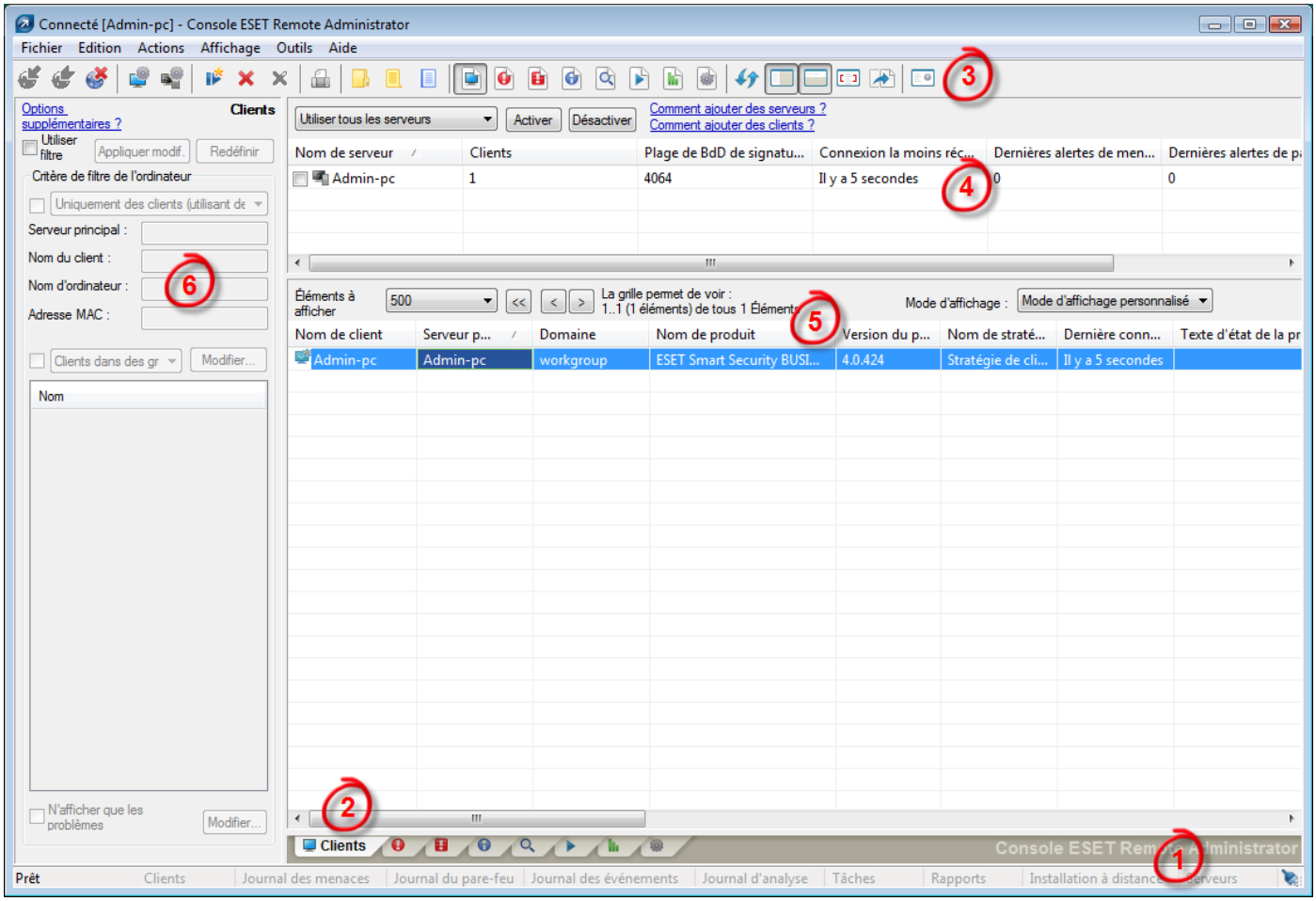


Figure 3-1 Fenêtre principale de la console ESET Remote Administrator

L'état de communication actuel entre ERAC et ERAS s'affiche dans la barre d'état (1). Toutes les données nécessaires d'ERAS sont actualisées régulièrement (par défaut à chaque minute ; voir **Outils > Options de la console...**). La progression de l'actualisation est également visible dans la barre d'état.

REMARQUE : Appuyez sur F5 pour actualiser les données affichées.

Les informations sont divisées en plusieurs onglets par ordre d'importance (2). Dans la plupart des cas, il est possible de trier les données en ordre croissant ou décroissant en cliquant sur un attribut (5), tandis qu'une opération glisser-déplacer permet d'effectuer une réorganisation. Si plusieurs lignes de données doivent être traitées, vous pouvez les limiter à l'aide du menu déroulant ***Éléments à afficher*** et des boutons de **navigation page par page**. Sélectionnez le Mode d'affichage pour présenter les attributs conformément à vos besoins (pour plus de détails, voir la section 3.3, « Filtrage des informations »).

La section Serveur (4) est importante si vous répliquez des serveurs ERA. Cette section affiche des informations résumées sur la Console à laquelle ERAS est connecté, ainsi que des informations sur les serveurs ERA enfant ou de niveau inférieur. Le menu déroulant Serveurs dans la section 4 influence la portée des informations affichées dans la section 5.

- ***Utiliser tous les serveurs***
  Affiche les informations de tous les serveurs ERA – section (5).

- ***N'utiliser que les serveurs contrôlés***
  Affiche les informations des serveurs ERA sélectionnés – section (5).

- ***Exclure les serveurs contrôlés***
  Exclut les informations des serveurs ERA sélectionnés.

Colonnes de la section 4 :

- ***Nom de serveur***
  Affiche le nom de serveur.
- ***Clients***
  Nombre total de clients se connectant à la base de données de l'ERAS sélectionné.
- ***Plage de Bd D de signatures de virus***
  Version des bases des signatures de virus parmi les clients de l'ERAS sélectionné.
- ***Connexion la moins récente***
  Version la plus ancienne de la base des signatures de virus parmi les clients de l'ERAS sélectionné.
- ***Dernières alertes de menace***
  Nombre total d'alertes de virus (voir l'attribut ***Dernière alerte de menace*** dans la section 5).
- ***Dernières alertes du pare-feu***
  Nombre total d'alertes de pare-feu.
- ***Derniers avertissements d'événement***
  Nombre total d'événements actuels (voir l'attribut ***Dernier événement*** dans la section 5).

Si vous n'êtes pas connecté actuellement, vous pouvez cliquer avec le bouton droit dans la section Serveur (4), puis sélectionner ***Connexion à ce serveur*** pour vous connecter à l'ERAS choisi.

Si la réplication est activée, des informations supplémentaires s'afficheront dans la section Serveur (4).

Les principales fonctionnalités d'ERAC sont accessibles dans le menu principal de la barre d'outils (3).

La dernière section est ***Critère de filtre de l'ordinateur*** (6) ; voir la section 3.3, « Filtrage des informations ».

3.3 Filtrage des informations

ERAC intègre plusieurs outils et fonctionnalités permettant d'administrer de façon conviviale les clients et les événements.

3.3.1 Groupes

Vous pouvez diviser des clients individuels en plusieurs groupes en cliquant sur ***Outils*** > ***Éditeur de groupes...*** dans l'ERAC. Vous pouvez ensuite utiliser des groupes lors de l'application de filtres ou de la création de tâches. Les groupes sont indépendants pour chaque ERAS et ne sont pas répliqués. La fonctionnalité ***Synchroniser avec Active Directory*** de l'Éditeur de groupes permet à l'administrateur de trier des clients en groupes, pour autant que le nom de client soit identique au type d'objet « ordinateur » à côté d'Active Directory (AD) et appartienne à des groupes dans l'AD[3].

Pour plus d'informations sur les gestion des groupes, consultez le chapitre 5.2, Groupes.

3.3.2 Filtre

Le filtre permet à l'administrateur de n'afficher des informations que sur des serveurs ou des postes client spécifiques. Pour afficher les options de filtre, dans le menu d'ERAC, cliquez sur ***Affichage*** > ***Afficher/Masquer le volet Filtre***.

Pour activer le filtrage, sélectionnez l'option ***Utiliser filtre*** du côté supérieur gauche de l'ERAC, puis cliquez sur le bouton ***Appliquer modif***. Toute modification future des critères de filtre mettra automatiquement à jour les données affichées, sauf configuration contraire sous l'onglet ***Outils > Options de la console... > Autres paramètres***. Dans la section ***Critère de filtre de l'ordinateur***, définissez les critères de filtrage (***Serveur principal, Nom du client, Nom d'ordinateur, Adresse MAC***).

Dans la section ***Critère de filtre de l'ordinateur***, vous pouvez filtrer les serveurs/clients ERA à l'aide des critères suivants :

- ***Uniquement des clients (utilisant des mots entiers)***
  Le résultat n'inclut que les clients dont le nom est identique à la chaîne entrée.
- ***Uniquement des clients commençant par (?,*)***
  Le résultat n'inclut que les clients dont le nom commence par la chaîne entrée.

[3] Pour qu'ERAS se synchronise avec Active Directory, ERAS ne doit pas nécessairement être installé sur votre contrôleur de domaine. Le contrôleur de domaine ne doit être accessible qu'à partir de l'ordinateur sur lequel ERAS est installé. Pour configurer l'authentification auprès de votre contrôleur de domaine, accédez à **Outils** > **Options du serveur** > **Autres paramètres** > **Modifier les options avancées** > **ESET Remote Administrator** > **Serveur ERA** > **Paramètres** > **Active directory**. Le format du nom de serveur est LDAP://nomdeserveur ou GC://nomdeserveur. Si le nom est vide, le catalogue global (GC) est utilisé.

- ***Uniquement des clients comme (?,*)***
  Le résultat n'inclut que les clients dont le nom contient la chaîne entrée.
- ***Exclure les clients (utilisant des mots entiers), Exclure les clients commençant par (?,*), Exclure les clients comme (?,*)***
  Ces options produisent des résultats opposés à ceux des trois options précédentes.

Les champs Serveur principal, Nom du client, Nom d'ordinateur et Adresse MAC acceptent des chaînes entières. Si l'un deux est renseigné, une requête de base de données est exécutée et les résultats sont filtrés en fonction de son contenu ; l'opérateur logique *ET* est utilisé.

La section suivante permet de filtrer les clients par groupes :

- ***Clients dans des groupes***
  N'affiche que les clients appartenant au(x) groupe(s) spécifié(s).
- ***Clients dans d'autres groupes ou n.a.***
  Le résultat n'inclut que les clients appartenant à d'autres groupes ou qui ne sont membres d'aucun groupe. Si un client appartient à la fois à des groupes spécifiés et non spécifiés, il s'affiche.
- ***Clients dans aucun groupe***
  N'affiche que les clients qui ne font partie d'aucun groupe.

La dernière option est un filtrage basé sur un problème ; les résultats n'incluent que les clients présentant le type de problème spécifié. Pour afficher la liste des problèmes, activez l'option ***N'afficher que les problèmes***, puis cliquez sur ***Modifier...*** Sélectionnez les problèmes à afficher, puis cliquez sur **OK** pour afficher les clients ayant les problèmes sélectionnés.

Toutes les modifications apportées à la configuration du filtrage seront appliquées après que vous aurez cliqué sur le bouton ***Appliquer modif.*** Pour restaurer les paramètres par défaut, cliquez sur ***Redéfinir***. Pour générer automatiquement de nouveaux résultats à chaque modification des paramètres de filtre, activez l'option ***Outils > Options de la console... > Autres paramètres... > Application automatique des modifications***.

3.3.3 Menu contextuel

Utilisez le bouton droit de la souris pour appeler le menu contextuel et ajuster la sortie dans les colonnes. Les options disponibles sont les suivantes :

- ***Sélectionner tout***
  Sélectionne toutes les entrées.
- ***Sélectionner par '...'***
  Cette option permet de cliquer avec le bouton droit -sur tout attribut, puis de sélectionner (mettre en surbrillance) automatiquement l'ensemble des autres stations de travail ou serveurs ayant le même attribut. La chaîne ... est automatiquement remplacée par la valeur figurant sous l'onglet actuel.
- ***Inverser la sélection***
  Effectue une sélection d'entrées inversée.
- ***Masquer éléments sélectionnés***
  Masque les entrées sélectionnées.
- ***Masquer éléments non sélectionnés***
  Masque toutes les entrées non sélectionnées dans la liste.

Les deux dernières options sont efficaces si un complément d'organisation est nécessaire suite à l'utilisation des méthodes de filtrage précédentes. Pour désactiver tous les filtres définis par le menu contextuel, cliquez sur ***Affichage > Vue détourée*** ou cliquez sur l'icône dans la barre d'outils d'ERAC. Vous pouvez également appuyer sur **F5** pour actualiser les informations affichées et désactiver les filtres.

Exemple :

- Pour afficher uniquement les clients présentant des alertes de menace :
  Sous l'onglet ***Clients*****, cliquez avec le bouton droit sur tout volet vide avec Dernière alerte de virus, puis, dans le menu contextuel, sélectionnez *Sélectionner par '...'*. Ensuite, toujours dans le menu contextuel, cliquez sur *Masquer éléments sélectionnés*.**

- Pour afficher les alertes de menace relatives aux clients « Joseph » et « Charles » :
  Cliquez sur l'onglet ***Journal des menaces***, puis cliquez avec le bouton droit sur tout attribut dans la colonne Nom du client contenant la valeur Joseph. Dans le menu contextuel, cliquez sur ***Sélectionner par 'Joseph'***. Ensuite, maintenez enfoncée la touche CTRL, cliquez avec le bouton droit, puis cliquez sur ***Sélectionner par 'Charles'***. Enfin,

cliquez avec le bouton droit, puis, dans le menu contextuel, sélectionnez ***Masquer éléments non sélectionnés*** et relâchez la touche CTRL.

La touche CTRL permet de sélectionner ou désélectionner des entrées spécifiques, et la touche MAJ de marquer un groupe d'entrées ou d'en annuler la marque.

REMARQUE : *Le filtrage peut faciliter la création de tâches pour des clients spécifiques (en surbrillance). Il existe de nombreuses manières d'utiliser le filtrage efficacement. Essayez plusieurs combinaisons.*

Affichages

Sous l'onglet ***Clients***, vous pouvez ajuster le nombre de colonnes affichées à l'aide du menu déroulant ***Mode d'affichage*** : situé à droite de la console. Le ***Mode d'affichage complet*** affiche toutes les colonnes, tandis que le ***Mode d'affichage minimal*** n'affiche que les plus importantes. Ces modes sont prédéfinis ; il est impossible de les modifier. Pour activer l'affichage personnalisé, sélectionnez ***Mode d'affichage personnalisé***. Vous pouvez le configurer sous l'onglet ***Outils > Options de la console...*** > ***Colonnes > Afficher/Masquer***.

3.4 Onglets dans ERAC

3.4.1 Description générale des onglets et des clients

La plupart des informations sous les onglets ont trait aux clients connectés. Chaque client connecté à ERAS est identifié par les attributs suivants :
Nom d'ordinateur (nom de client) + Adresse MAC + Serveur principal[4]

Le comportement d'ERAS par rapport à certaines opérations de réseau (telles que le changement de nom d'un PC) peut être défini dans Configuration avancée d'ERAS. Cela peut aider à empêcher des entrées en double sous l'onglet ***Clients***. Par exemple, si l'un des ordinateurs du réseau a été renommé, mais que son Adresse MAC est restée inchangée, vous pouvez éviter la création d'une entrée sous l'onglet **Clients**.

Les clients qui se connectent à ERAS pour la première fois sont désignés par la valeur **Oui** dans la colonne **Nouvel utilisateur**. Ils sont également marqués par un petit astérisque dans le coin supérieur droit de leur icône (voir la figure 3-2). Cette fonctionnalité permet à un administrateur de détecter aisément un ordinateur nouvellement connecté. Cet attribut peut avoir différentes significations en fonction des procédures opératoires de l'administrateur.

Figure 3-2

Si un client a été configuré et déplacé vers un certain groupe, il est possible de désactiver l'état Nouveau en cliquant avec le bouton droit sur le client, puis en sélectionnant ***Définir/Redéfinir des drapeaux > Redéfinir le drapeau « Nouveau »***. L'icône du client devient celle présentée à la figure 3-3, et la valeur de l'attribut ***Nouvel utilisateur*** devient ***Non***.

Figure 3-3

REMARQUE : *L'attribut Commentaire est facultatif sous les trois onglets. L'administrateur peut insérer une description ici (p. ex., « Bureau 129 »).*

ERAS permet d'afficher les valeurs de temps en mode relatif (« Il ya 2 jours »), en mode absolu (20. 5. 2008) ou en mode système (Paramètres régionaux).

Dans la plupart des cas, il est possible de trier les données en ordre croissant ou décroissant en cliquant sur un attribut, tandis qu'une opération glisser-déplacer permet d'effectuer une réorganisation.

Le fait de cliquer sur certaines valeurs active d'autres onglets afin d'afficher des informations plus détaillées. Par exemple, si vous cliquez sur une valeur dans la colonne ***Dernière alerte de menace***, le programme active l'onglet ***Journal des menaces*** et affiche les entrées du journal des menaces relatives au client donné. Si vous cliquez sur une valeur contenant trop d'informations pour qu'il soit possible de les présenter dans un affichage tabulaire, une boîte de dialogue s'ouvre, affichant des informations détaillées sur le client correspondant.

[4] Dans les versions précédentes d'ERA, les clients étaient identifiés par les attributs suivants : Nom d'ordinateur + Serveur principal

3.4.2 Réplication et informations sous les onglets individuels

Si ERAC est connecté à un ERAS opérant en tant que serveur de niveau supérieur, toutes les informations des serveurs de niveau inférieur s'affichent automatiquement, à moins que le serveur de niveau inférieur ne soit pas configuré pour le permettre.

Dans un tel scénario, les informations suivantes peuvent manquer :

- Journaux d'alertes détaillés (onglet ***Journal des menaces***)
- Journaux détaillés d'analyse à la demande (onglet ***Journal d'analyse***)
- Configurations de client actuel détaillées au format .xml (onglet ***Clients***, colonne ***Configuration***, ***État de la protection***, ***Fonctionnalités de protection***, ***Informations système***)

Des informations du programme ESET SysInspector peuvent également manquer. ESET SysInspector est intégré dans la génération de produits ESET 4.x et ultérieurs.

Dans les boîtes de dialogue où de telles informations devraient autrement figurer, le bouton ***Demande*** est disponible (Actions > Propriétés > Configuration). Un clic sur ce bouton entraîne le téléchargement d'informations manquantes d'un ERAS de niveau inférieur. Comme la réplication est toujours déclenchée par un ERAS de niveau inférieur, les informations manquantes doivent être livrées dans l'intervalle de réplication prédéfini.

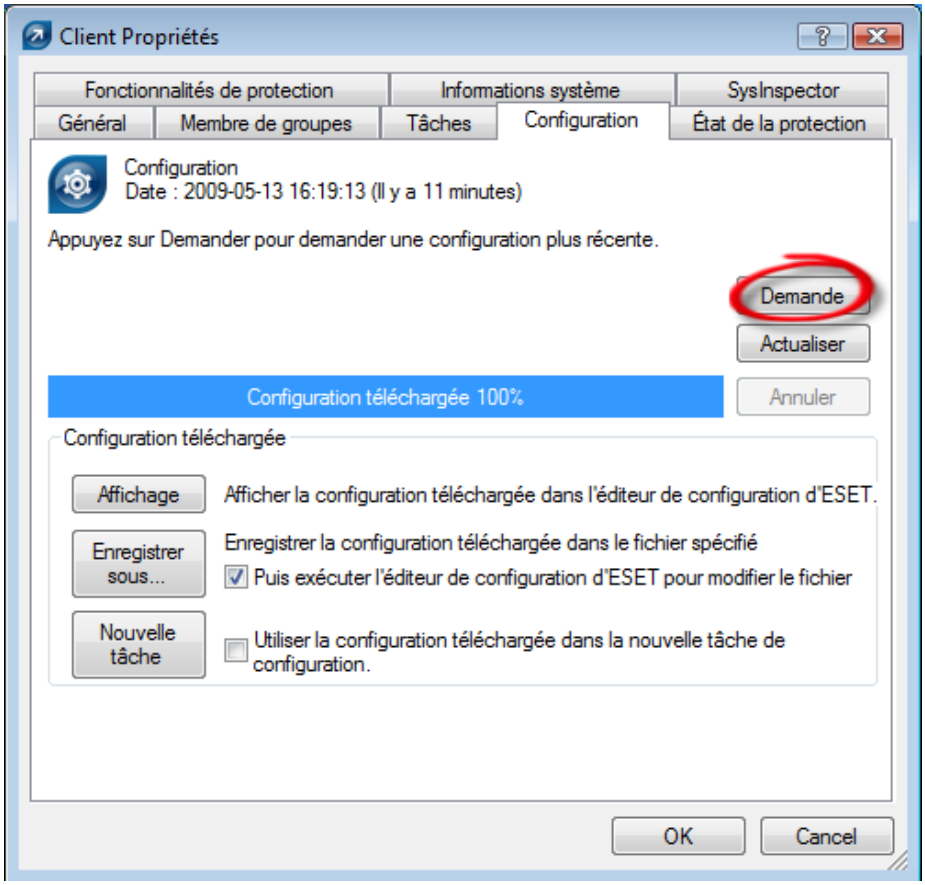


Figure 3-4 Cliquez sur Demande pour extraire des informations manquantes de serveurs ERA de niveau inférieur.

3.4.3 Onglet Clients

Cet onglet affiche des informations générales sur des clients individuels.

Attribut	Description
Nom d'ordinateur	Nom de la station de travail ou du serveur (nom d'hôte)
Adresse MAC	Adresse MAC (carte réseau)
Serveur principal	Nom du serveur ERA avec lequel un client communique
Domaine	Nom du domaine ou du groupe auquel un client appartient (il ne s'agit pas de groupes créés dans ERAS)
IP	Adresse IP
Nom de produit	Nom du produit de sécurité ESET
Version du produit	Version du produit de sécurité ESET

Attribut	Description
Nom de stratégie	Nom de la stratégie attribuée à un client
Dernière connexion	Heure à laquelle le client s'est connecté pour la dernière fois à ERAS (toutes les autres données collectées à partir de clients incluent cet horodateur, à l'exception de certaines données obtenues par réplication)
Texte d'état de la protection	État actuel du produit de sécurité ESET installé sur un client
BdD de signatures de virus	Version de la base des signatures de virus
Dernière alerte de menace	Dernier incident de virus
Dernière alerte du pare-feu	Dernier événement détecté par le pare-feu personnel d'ESET Smart Security (les événements à partir du niveau d'avertissement et au-delà s'affichent)
Dernier avertissement d'événement	Dernier message d'erreur
Derniers fichiers analysés	Nombre de fichiers analysés durant la dernière analyse à la demande
Derniers fichiers infectés	Nombre de fichiers infectés durant la dernière analyse à la demande
Derniers fichiers nettoyés	Nombre de fichiers nettoyés (ou supprimés) durant la dernière analyse à la demande
Date de dernière analyse	Heure de la dernière analyse à la demande
Demande de redémarrage	Indique si un redémarrage est requis (par exemple, après une mise à niveau du programme)
Date de demande de redémarrage	Heure de la première demande de redémarrage
Dernier démarrage du produit	Heure du dernier lancement du programme client
Date d'installation du produit	Date d'installation du produit de sécurité ESET sur le client
Utilisateur mobile	Les clients ayant cet attribut exécutent la tâche « Mettre à jour maintenant » chaque fois qu'ils établissent une connexion avec ERAS (recommandé pour les portables)
Nouveau client	Nouvel ordinateur connecté (voir la section 3.4.1, « Description générale des onglets et des clients »)
Nom de SE	Nom du système d'exploitation du client
Plateforme de SE	Plateforme du système d'exploitation (Windows / Linux…)
Plateforme matérielle	32 bits / 64 bits
Configuration	Configuration .xml actuelle du client (y compris la date et l'heure de création de la configuration)
État de la protection	Relevé d'état général (similaire par nature à l'attribut Configuration)
Fonctionnalités de protection	Relevé d'état général des composants programme (similaire à l'attribut Configuration)
Informations système	Le client soumet des informations système à ERAS (y compris l'heure à laquelle les informations système ont été soumises)
SysInspector	Les clients disposant de versions contenant l'outil ESET SysInspector peuvent soumettre des journaux à partir de cette application complémentaire
Informations personnalisées	Informations personnalisées à afficher spécifiées par l'administrateur.
Commentaire	Bref commentaire décrivant le client (entré par l'administrateur)

REMARQUE : *Certaines valeurs ont un caractère purement informatif et peuvent ne pas être à jour au moment où l'administrateur les consulte sur la console. Par exemple, il peut y avoir eu une erreur de mise à jour à 7 h 00, alors qu'à 8 h 00 la mise à jour a réussi. Ces valeurs peuvent être* ***Dernière alerte de menace*** *et* ***Dernier avertissement d'événement****. Si l'administrateur sait que ces informations sont obsolètes, il peut les effacer en cliquant avec le bouton droit, puis en sélectionnant Effacer les informations > Effacer les informations « Dernière alerte de menace » ou Effacer les informations « Dernier avertissement d'événement ». Les informations sur le dernier incident de virus ou le dernier événement système sont supprimées.*

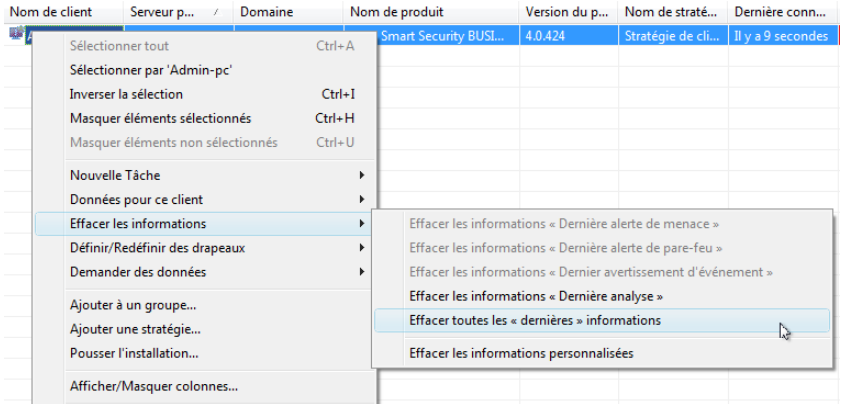


Figure 3-5 Il est facile de supprimer les événements obsolètes des colonnes Dernière alerte de menace et Dernier avertissement d'événement.

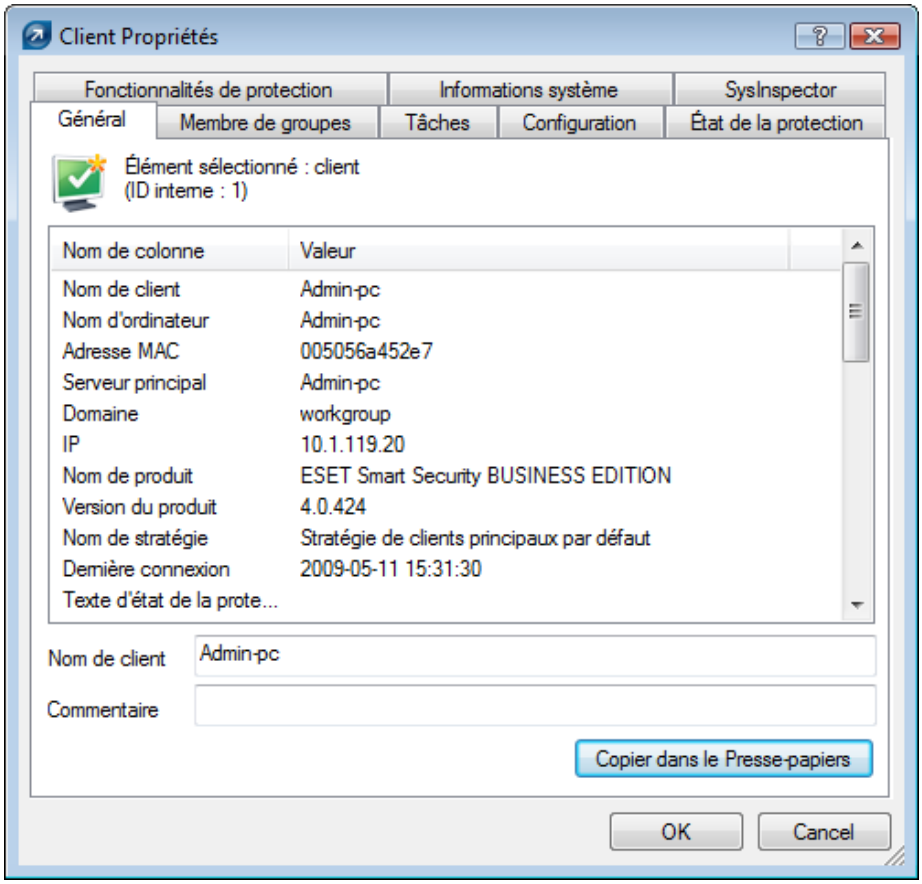


Figure 3-6 Informations détaillées sur une station de travail client.

Après que vous avez double-cliqué sur un client, l'onglet ***Clients*** affiche plusieurs options :

- ***Général***
  Contient des informations similaires à celles affichées sous l'onglet ***Clients***. Vous pouvez spécifier ici le ***Nom du client***, c'est-à-dire celui sous lequel ce client est visible dans ERA, ainsi qu'un commentaire facultatif.

- ***Membre de groupes***
  Cet onglet répertorie tous les groupes auxquels le client appartient. Pour plus d'informations, consultez la section 3.3, « Filtrage des informations ».

- ***Tâches***
  Tâches relatives au client indiqué. Pour plus d'informations, consultez la section 5.1, « Tâches ».

- ***Configuration***
  Cet onglet permet d'afficher ou d'exporter la configuration actuelle du client dans un fichier .xml. Ce manuel explique, plus loin, comment utiliser des fichiers .xml pour créer un modèle de configuration pour des fichiers de configuration .xml nouveaux ou modifiés. Pour plus d'informations, consultez la section 5.1, « Tâches ».

- ***État de la protection***
  Relevé d'état général concernant tous les programmes ESET. Certains relevés sont interactifs et permettent d'intervenir immédiatement. Cette fonctionnalité est utile car elle évite la nécessité de définir manuellement une nouvelle tâche pour résoudre un problème de protection donné.

- ***Fonctionnalités de protection***
  État du composant pour toutes les fonctionnalités de sécurité d'ESET (Blocage du courrier indésirable, Pare-feu personnel, etc.)

- ***Informations système***
  Informations détaillées sur le programme installé, sa version de composant, etc.

- Onglet **SysInspector**
  Informations détaillées sur les processus de démarrage et les processus s'exécutant à l'arrière-plan.

3.4.4 Onglet Journal des menaces

Cet onglet contient des informations sur des incidents de virus ou de menace individuels.

Attribut	Description
Nom de client	Nom du client signalant l'alerte de menace
Nom d'ordinateur	Nom de la station de travail ou du serveur (nom d'hôte)
Adresse MAC	Adresse MAC (carte réseau)
Serveur principal	Nom du serveur ERA avec lequel un client communique
Date de réception	Heure à laquelle ERAS a journalisé l'événement
Date de survenance	Heure à laquelle l'événement s'est produit
Niveau	Niveau d'alerte
Analyseur	Nom de la fonctionnalité de sécurité ayant détecté la menace
Objet	Type d'objet
Nom	Généralement un dossier dans lequel se trouve l'infiltration
Menace	Nom du code malveillant détecté
Action	Action exécutée par la fonctionnalité de sécurité donnée
Utilisateur	Nom de l'utilisateur identifié lorsque l'incident s'est produit
Informations	Informations sur la menace détectée
Détails	État de soumission du journal du client

3.4.5 Onglet Journal de pare-feu

Cet onglet affiche des informations sur l'activité du pare-feu du client.

Attribut	Description
Nom de client	Nom du client signalant l'événement
Nom d'ordinateur	Nom de la station de travail ou du serveur (nom d'hôte)
Adresse MAC	Adresse MAC (carte réseau)
Serveur principal	Nom du serveur ERA avec lequel un client communique
Date de réception	Heure à laquelle ERAS a journalisé l'événement
Date de survenance	Heure à laquelle l'événement s'est produit
Niveau	Niveau d'alerte
Événement	Description de l'événement
Source	Adresse IP source
Cible	Adresse IP cible
Protocole	Protocole concerné
Règle	Règle de pare-feu concernée
Application	Application concernée
Utilisateur	Nom de l'utilisateur identifié lorsque l'incident s'est produit

3.4.6 Onglet Journal des événements

Cet onglet présente la liste de tous les événements liés au système.

Attribut	Description
Nom de client	Nom du client signalant l'événement
Nom d'ordinateur	Nom de la station de travail ou du serveur (nom d'hôte)
Adresse MAC	Adresse MAC (carte réseau)
Serveur principal	Nom du serveur ERA avec lequel un client communique
Date de réception	Heure à laquelle ERAS a journalisé l'événement
Date de survenance	Heure à laquelle l'événement s'est produit
Niveau	Niveau d'alerte
Plugin	Nom du composant programme signalant l'événement
Événement	Description de l'événement
Utilisateur	Nom de l'utilisateur associé à l'événement

3.4.7 Onglet Journal d'analyse

Cet onglet répertorie les résultats des analyses d'ordinateur à la demande qui ont été lancées à distance, localement sur des ordinateurs client ou en tant que tâches planifiées.

Attribut	Description
Nom de client	Nom du client sur lequel l'analyse a été effectuée
Nom d'ordinateur	Nom de la station de travail ou du serveur (nom d'hôte)
Adresse MAC	Adresse MAC (carte réseau)
Serveur principal	Nom du serveur ERA avec lequel un client communique
Date de réception	Heure à laquelle ERAS a journalisé l'événement d'analyse
Date de survenance	Heure à laquelle l'analyse a eu lieu sur le client
Cibles analysées	Fichiers, dossiers et périphériques analysés
Analysés	Nombre de fichiers contrôlés
Infectés	Nombre de fichiers infectés
Nettoyés	Nombre d'objets nettoyés (ou supprimés)
État	État de l'analyse
Utilisateur	Nom de l'utilisateur identifié lorsque l'incident s'est produit
Type	Type d'utilisateur
Analyseur	Type d'analyseur
Détails	État de soumission du journal du client

3.4.8 Onglet Tâches

La signification de cet onglet est décrite dans le chapitre « Tâches ». Les attributs suivants sont disponibles :

Attribut	Description
État	État de la tâche (Active = en cours d'application, Terminée = tâche livrée aux clients)
Type	Type de tâche
Nom	Nom de la tâche
Description	Description de la tâche
Date de déploiement	Heure/date d'exécution de la tâche
Date de réception	Heure à laquelle ERAS a journalisé l'événement
Détails	État de soumission du journal des tâches
Commentaire	Bref commentaire décrivant le client (entré par l'administrateur)

3.4.9 Onglet Rapports

Cet onglet contient des fonctionnalités permettant d'archiver l'activité d'un réseau sur certaines périodes. L'onglet **Rapports** permet d'organiser des informations statistiques sous la forme d'un graphique ou d'un diagramme. Pour plus d'informations, consultez le chapitre 6, « Rapports ».

3.4.10 Onglet Installation à distance

Cet onglet offre des options pour plusieurs méthodes d'installation à distance d'ESET Smart Security ou d'ESET NOD32 Antivirus sur des clients. Pour plus d'informations, consultez la section 4.2, « Installation à distance ».

3.5 Configuration de la console ERA

Vous pouvez configurer ERAC dans le menu ***Outils > Options de la console...***

3.5.1 Onglet Connexion

Cet onglet permet de configurer la connexion d'ERAC à ERAS. Pour plus d'informations, consultez le chapitre 3, « Utilisation d'ERAC ».

3.5.2 Onglet Colonnes – Afficher/Masquer

Cet onglet permet de spécifier les attributs (colonnes) affichés sous les onglets individuels. Les modifications se reflètent dans le Mode d'affichage personnalisé (onglet **Clients**). Les autres modes ne peuvent pas être modifiés.

3.5.3 Onglet Couleurs

Cet onglet permet d'associer différentes couleurs à des événements spécifiques liés au système, afin de mieux mettre en évidence des clients problématiques (Mise en évidence conditionnelle). Par exemple, des clients avec une base des signatures de virus légèrement dépassée (**Clients : Version précédente**) pourraient être distingués de clients dont la base des signatures est obsolète (**Clients : Version plus ancienne ou n.a**).

3.5.4 Onglet Chemins

Cet onglet permet de spécifier le répertoire dans lequel ERAC enregistrera les rapports téléchargés à partir d'ERAS. Par défaut, les rapports sont enregistrés dans :

%ALLUSERSPROFILE %\Application Data\Eset\Eset Remote Administrator\Console\reports

3.5.5 Onglet Date/Heure

Apparence des colonnes de date/heure :

- ***Absolue***
  La console affichera l'heure absolue (p. ex., 14:30:00).

- ***Relative***
  La console affichera l'heure relative (p. ex., « Il y a 2 semaines »).

- ***Régionale***
  La console affichera l'heure en fonction des paramètres régionaux (paramètres de Windows).

- ***Recalculer l'heure UTC en heure locale (utiliser l'heure locale)***
  Activez cette case à cocher pour recalculer votre heure locale. Sinon, l'heure GMT – UTC sera affichée.

3.5.6 Onglet Autres paramètres

- ***Paramètres de filtre > Application automatique des modifications***
  Si cette option est activée, les filtres sous les différents onglets génèrent de nouveaux résultats à chaque modification des paramètres de filtre. Autrement, le filtrage n'a lieu qu'après que vous avez cliqué sur le bouton **Appliquer modif**.

- ***Mises à jour de la console Remote Administrator***
  Cette section permet de contrôler la disponibilité de nouvelles versions de la solution ESET Remote Administrator. Il est recommandé de laisser la valeur par défaut ***Mensuelle***. Si une nouvelle version est disponible, ERAC affiche une notification au démarrage du programme.

- ***Autres paramètres > Utiliser l'actualisation automatique***
  Si cette option est activée, les données sous les onglets individuels sont automatiquement actualisées conformément à l'intervalle indiqué.

- ***Autres paramètres > Vider les corbeilles de la console lors de la fermeture de l'application***
  Activez cette option pour vider automatiquement les éléments de la corbeille interne d'ERAC après sa fermeture. Vous pouvez également vider les éléments manuellement en cliquant dessus avec le bouton droit sous l'onglet ***Rapports***.

- ***Autres paramètres > Afficher le quadrillage***
  Activez cette option pour séparer les cellules individuelles sous tous les onglets à l'aide d'un quadrillage.

- ***Autres paramètres > Afficher le client comme « serveur/nom » plutôt que « serveur/ordinateur/MAC »***
  Affecte le mode d'affichage des clients dans certains boîtes de dialogue (p. ex., Nouvelle tâche). Cette option produit uniquement un effet visuel.

- ***Autres paramètres > Utiliser l'icône Systray***
  La console ERA sera représentée par une icône dans la zone de notification de Windows.

- ***Autres paramètres > Afficher dans la barre des tâches en cas de réduction***
  Si la fenêtre d'ERAC est réduite, elle sera accessible à partir de la barre des tâches de Windows.

- ***Autres paramètres > Icône Systray en surbrillance en cas de clients problématiques***
  Activez cette option conjointement avec le bouton **Modifier** pour définir les événements qui déclencheront un changement de couleur de l'icône ERAC dans la zone de notification.

Si l'ERAC sur le PC de l'administrateur doit être connectée en permanence à l'ERAS, il est recommandé de désactiver l'option ***Afficher dans la barre des tâches en cas de réduction*** et de laisser la console réduite en cas d'inactivité. En cas de problème, l'icône dans la zone de notification vire au rouge, ce qui constitue un signal d'intervention pour l'administrateur. Il est également recommandé d'ajuster l'option ***Icône Systray en surbrillance en cas de clients problématiques*** pour spécifier les événements déclenchant un changement de couleur de l'icône d'ERAC. Toutefois, l'ERAC se déconnectera si une compression de base de données est activée sur le serveur.

- ***Autres paramètres > Afficher tous les groupes dans les volets Filtre***
  Modifie le filtrage des groupes.

- ***Autres paramètres > Messages du didacticiel***
  Désactive (Désactiver tout) ou active (Activer tout) tous les messages d'informations.

3.6 Modes d'affichage

ERAC offre deux modes d'affichage :

- Mode administratif
- Mode lecture seule

Le **mode administratif** d'ERAC permet à l'utilisateur de contrôler totalement l'ensemble des fonctionnalités et paramètres, ainsi que d'administrer toutes les stations de travail client connectées.

Le **mode lecture seule** convient pour afficher l'état de solutions client ESET se connectant à ERAS ; la création de tâches pour des stations de travail client, la création de packages d'installation et l'installation à distance ne sont pas autorisées. Le Gestionnaire de licences, le Gestionnaire de stratégies et le Gestionnaire de notifications sont également inaccessibles. **Le mode lecture seule** permet à l'administrateur de modifier des paramètres d'ERAC et de générer des rapports.

Le mode d'affichage est sélectionné à chaque démarrage de la console dans le menu déroulant **Accès**, tandis que le mot de passe pour se connecter à ERAS peut être défini pour chaque mode d'affichage. La définition d'un mot de passe est particulièrement utile si vous voulez que certains utilisateurs aient un accès illimité à ERAS et d'autres un accès en lecture seule. Pour définir le mot de passe, cliquez sur **Outils > Options du serveur... > Sécurité**, puis sur le bouton Modifier... à côté de Mot de passe pour la console (accès administrateur) ou Mot de passe pour la console (Accès en lecture seule).

3.7 Éditeur de configuration d'ESET

L'éditeur de configuration d'ESET est un composant important d'ERAC utilisé à diverses fins. Parmi les plus importantes figurent la création des éléments suivants :

- Configurations prédéfinies pour les packages installation
- Configurations envoyées en tant que tâches aux clients
- Un fichier de configuration (.xml) général

L'éditeur de configuration fait partie d'ERAC et est représenté principalement par les fichiers cfgedit.*

L'éditeur de configuration permet à l'administrateur de configurer à distance un grand nombre des paramètres disponibles dans tout produit de sécurité ESET, en particulier ceux installés sur des stations de travail client. Il permet également à l'administrateur d'exporter des configurations dans des fichiers .xml utilisables ultérieurement à diverses fins, telles que la création de tâches dans ERAC, l'importation d'une configuration localement dans ESET Smart Security, etc.

La structure utilisée par l'éditeur de configuration est un modèle .xml qui contient la configuration dans une structure arborescente. Le modèle est stocké dans le fichier *cfgedit.exe*. C'est pourquoi il est recommandé de mettre à jour ERAS et ERAC régulièrement.

Avertissement : *L'éditeur de configuration permet de modifier tout fichier .xml. Évitez de modifier ou d'écraser le fichier source cfgedit.xml.*

Pour que l'éditeur de configuration fonctionne, les fichiers suivants doivent être disponibles : *eguiEpfw.dll*, *cfgeditLang.dll*, *eguiEpfwLang.dll et eset.chm*.

3.7.1 Superposition de configuration

Si une valeur est modifiée dans l'éditeur de configuration, la modification est marquée à l'aide d'un symbole bleu. Toute entrée associée à l'icône grise n'a pas été modifiée et ne sera pas écrite dans le fichier de configuration de sortie .xml.

Lors de l'application d'une configuration à des clients, seules les modifications enregistrées dans le fichier de configuration de sortie .xml sont appliquées () et tous les autres éléments () restent inchangés. Ce comportement permet une application progressive de plusieurs configurations différentes sans altération de modifications précédentes.

Un exemple est présenté à la figure 3-7. Dans cette configuration, le nom d'utilisateur AV-1234567 et le mot de passe sont insérés et l'utilisation d'un serveur proxy est interdite.

Figure 3-7

La seconde configuration (Figure 3-8) envoyée aux clients veillera à ce que les modifications précédentes soient préservées, dont le nom d'utilisateur EAV–1234567 et le mot de passe, mais autorisera également l'utilisation d'un serveur proxy dont elle définit l'adresse et le port.

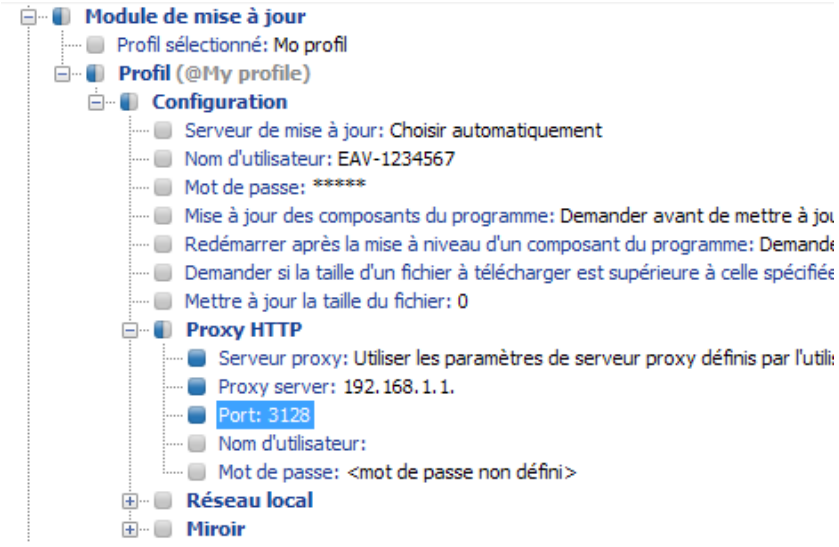


Figure 3-8

3.7.2 Entrées de configuration clés

Dans cette section, nous décrivons plusieurs entrées de configuration clés pour ESET Smart Security et ESET NOD32 Antivirus, disponibles via l'éditeur de configuration d'ESET :

- ***ESET Smart Security, ESET NOD32 Antivirus > Noyau ESET > Configuration > ESET Remote Administrator***
  Vous pouvez activer ici la communication entre les ordinateurs client et l'ERAS (***Connexion au serveur ESET Remote Administrator***). Entrez le nom ou l'adresse IP d'ERAS (***Adresse du serveur***). L'option ***Intervalle entre deux connexions au serveur*** doit rester définie sur sa valeur par défaut de cinq minutes. À des fins de test, vous pouvez réduire cette valeur à 0, ce qui a pour effet d'établir une connexion toutes les dix secondes. Si un mot de passe est défini, utilisez celui spécifié dans ERAS. Pour plus d'informations, consultez le chapitre sur la configuration d'ERAS (l'option ***Mot de passe pour les clients***). Si un mot de passe est utilisé, la communication entre les clients et ERAS est chiffrée. Pour plus d'informations sur la configuration du mot de passe, consultez la section 7.1, « Onglet Sécurité ».

- ***Noyau ESET > Configuration > Clés de licence***
  Les ordinateurs client ne nécessitent pas l'ajout ni la gestion de clés de licence. Les clés de licence ne sont utilisées que pour les produits serveur.

- ***Noyau ESET > Configuration > Threatsense. Net***
  Cette branche définit le comportement du système d'avertissement anticipé ThreatSense. Net qui permet de soumettre des fichiers suspects pour analyse aux laboratoires d'ESET. Lors du déploiement de solutions ESET sur un réseau de grande taille, les options ***Soumettre des fichiers suspects*** et ***Activer la soumission d'informations statistiques anonymes*** sont particulièrement importantes : Si ces options sont définies respectivement sur ***Ne pas soumettre*** ou sur **Non**, le système ThreatSense. Net est complètement désactivé. Pour soumettre des fichiers automatiquement sans intervention de l'utilisateur, sélectionnez respectivement ***Soumettre sans demander*** et **Oui**. Si un serveur proxy est utilisé avec la connexion Internet, spécifiez les paramètres de connexion sous ***Noyau ESET*** > ***Configuration*** > ***Serveur proxy***.
  Par défaut, les produits client soumettent les fichiers suspects à ERAS, qui les soumet aux serveurs d'ESET. C'est pourquoi, le serveur proxy doit être correctement configuré dans ERAS (**Outils > Options du serveur > Autres paramètres > Modifier les paramètres avancés > Serveur ERA > Configuration > Serveur proxy**).

- ***Noyau > Configuration > Protéger les paramètres de configuration***
  Permet à l'administrateur de protéger par mot de passe les paramètres de configuration. Si un mot de passe est défini, il sera requis pour pouvoir accéder aux paramètres de configuration sur les stations de travail client. Toutefois, le mot de passe n'affectera aucune modification de configuration effectuée à partir d'ERAC.

- **Noyau > Configuration > Planificateur/Programmateur**
  Cette clé contient les options de Planificateur/Programmateur qui permettent à l'administrateur de planifier des analyses antivirus régulières, etc.

REMARQUE : *Par défaut, toutes les solutions de sécurité ESET contiennent plusieurs tâches prédéfinies (dont une mise à jour automatique régulière et un contrôle automatique des fichiers importants au démarrage). Dans la plupart des cas, il n'est pas nécessaire de modifier ou d'ajouter des tâches.*

- ***Mise à jour***
  Cette branche de l'éditeur de configuration permet de définir la manière dont les profils de mise à jour sont appliqués. Normalement, il suffit de modifier le profil prédéfini ***Mon profil*** et de changer les paramètres ***Serveur de mise à jour***, ***Nom d'utilisateur*** et ***Mot de passe***. Si le paramètre Serveur de mise à jour est définie sur **Choisir automatiquement**, toutes les mises à jour seront téléchargées à partir des serveurs de mise à jour d'ESET. Dans ce cas, spécifiez les paramètres **Nom d'utilisateur** et **Mot de passe** fournis au moment de l'achat. Pour plus d'informations sur le paramétrage des stations de travail client pour la réception de mises à jour à partir d'un serveur local (Miroir), consultez la section 7.3, « Serveur Miroir ». Pour plus d'informations sur l'utilisation du planificateur, consultez la section 9.1, « Planificateur ».

REMARQUE : *Sur des périphériques mobiles, vous pouvez configurer deux profils, l'un pour effectuer une mise à jour à partir du serveur Miroir, et l'autre pour télécharger les mises à jour directement à partir des serveurs d'ESET. Pour plus d'informations, consultez la section 9.4, « Mise à jour combinée pour les portables et périphériques mobiles » à la fin de ce document.*

4. Installation des solutions client ESET

Ce chapitre traite de l'installation de solutions client ESET pour les systèmes d'exploitation Microsoft Windows. Vous pouvez effectuer des installations directement sur des stations de travail ou à distance à partir d'ERAS. Ce chapitre décrit également d'autres méthodes d'installation à distance.

REMARQUE : *Même si c'est techniquement réalisable, il n'est pas recommandé d'utiliser la fonctionnalité d'installation à distance pour installer des produits ESET sur des serveurs (stations de travail uniquement).*

4.1 installation directe

Dans le cas d'une installation directe, l'administrateur est présent devant l'ordinateur sur lequel le produit de sécurité ESET doit être installé. Cette méthode ne requiert aucune préparation supplémentaire et convient pour les petits réseaux informatiques ou pour les scénarios où ERA n'est pas utilisé.

Vous pouvez considérablement simplifier cette tâche à l'aide d'une configuration .xml prédéfinie. Aucune modification supplémentaire, telle que la définition d'un serveur de mise à jour (nom d'utilisateur et mot de passe, chemin d'accès du serveur Miroir, etc.), du mode sans assistance, d'une analyse planifiée, etc. n'est requise pendant ou après l'installation.

Il existe des différences dans l'application du format de configuration .xml entre les versions 3.x et 2.x des solutions client ESET :

- Téléchargez le fichier d'installation (p. ex., ess_nt32_enu.msi) à partir d'eset.com. Copiez le fichier de configuration .xml (cfg.xml) dans le répertoire où se trouve le fichier d'installation. Lors de son exécution, le programme d'installation adopte automatiquement la configuration du fichier .xml. Si le fichier de configuration .xml porte un autre nom ou se trouve ailleurs, vous pouvez utiliser le paramètre ADMINCFG ="path_to_xml_file" (p. ex., ess_nt32_enu.msi ADMINCFG ="\\server\xml\settings.xml" pour appliquer la configuration stockée sur un lecteur réseau).

- Version 2.x : Téléchargez le fichier d'installation (p. ex., ndntenst.exe) à partir d'eset.com. Extrayez le fichier téléchargé dans un dossier à l'aide d'un programme d'extraction de fichier tel que WinRAR. Le dossier contiendra les fichiers d'installation, dont setup.exe. Copiez le fichier de configuration nod32.xml dans le dossier. Exécutez le fichier setup.exe. La configuration contenue dans le fichier nod32.xml sera automatiquement appliquée. Si le fichier de configuration .xml porte un autre nom ou se trouve ailleurs, vous pouvez utiliser le paramètre /cfg ="path_to_xml_file" (p.ex., setup.exe /cfg ="\\server\xml\settings.xml" pour appliquer la configuration stockée sur un lecteur réseau).

4.2 Installation à distance

ERA offre plusieurs méthodes d'installation à distance. Vous pouvez distribuer des packages d'installation à des stations de travail cibles à l'aide des méthodes suivantes :

- Installation poussée à distance
- Installation à distance à l'aide d'un script d'ouverture de session
- installation à distance par Email

La procédure d'installation à distance à l'aide d'ERA est la suivante :

- création de packages d'installation ;
- distribution des packages aux stations de travail client (méthode d'installation poussée, script d'ouverture de session, Email, solution externe).

La première étape est lancée par ERAC, mais le package d'installation proprement dit se trouve dans ERAS, dans le répertoire suivant :

%ALLUSERSPROFILE %\Application Data\Eset\Eset Remote Administrator\Server\packages

Pour lancer les packages d'installation via ERAC, cliquez sur l'onglet ***Installation à distance***, puis sur le bouton ***Packages...***

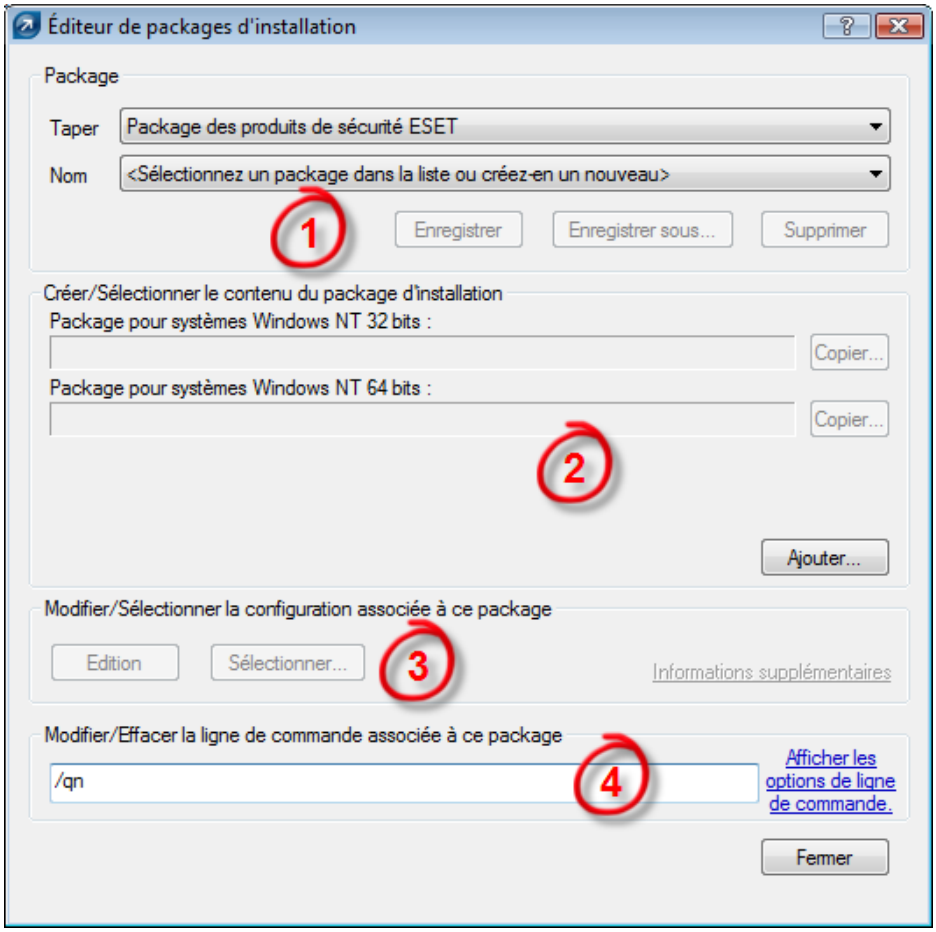


Figure 4-1 Boîte de dialogue de l'Éditeur de packages d'installation

Chaque package d'installation est défini par un nom. Voir (1) dans la figure 4-1 ci-dessus. Les autres sections de la boîte de dialogue ont trait au contenu du package qui est appliqué dès sa remise à une station de travail cible. Chaque package contient les éléments suivants :

- fichiers d'installation de la solution client ESET (2) ;
- fichier de configuration .xml pour les solutions client ESET (3) ;
- paramètres de ligne de commande attribués au package (4).

Le menu déroulant **Type** dans la section (1) étend les possibilités d'ERA. Outre l'installation à distance, il est possible de désinstaller à distance les produits de sécurité ESET à l'aide de l'option **Désinstaller les produits de sécurité ESET et NOD32 version 2**. Vous pouvez également installer à distance une application externe en sélectionnant **Package personnalisé**.

Un agent d'installation à distance d'ESET est automatiquement attribué à chaque package, ce qui permet une installation et une communication sans problème entre les stations de travail cibles et ERAS. L'agent d'installation à distance d'ESET est nommé einstaller.exe. Il contient le nom d'ERAS ainsi que le nom et le type de package auquel il appartient. Les chapitres suivants fournissent une description détaillée de l'agent.

Plusieurs paramètres peuvent affecter le processus d'installation. Ils sont utilisables soit durant une installation directe avec l'administrateur présent devant la station de travail, soit pour une installation distante. Pour les installations à distance, les paramètres sont sélectionnés durant le processus de configuration de packages d'installation. Les paramètres sélectionnés sont ensuite appliqués automatiquement aux clients cibles. Vous pouvez taper des paramètres supplémentaires pour ESET Smart Security et ESET NOD32 Antivirus après le nom du package d'installation .msi (p. ex., ea_nt64_ENU.msi /qn):

- **/qn**
  Mode d'installation silencieuse – aucune boîte de dialogue ne s'affiche.

- **/qb!**
  Aucune intervention de l'utilisateur n'est possible, mais le processus d'installation est indiqué par une barre de progression en %.

- **REBOOT ="ReallySuppress"**
  Supprime le redémarrage après installation du programme.

- **REBOOT ="Force"**
  Redémarre automatiquement après l'installation.

- **REBOOTPROMPT =""**
  Après installation, une boîte de dialogue invitant l'utilisateur à confirmer le redémarrage s'affiche (ne peut pas être utilisé avec */qn*).

- **ADMINCFG ="path_to_xml_file"**
  Durant l'installation, les paramètres définis dans les fichiers .xml spécifiés sont appliqués aux produits de sécurité ESET. Le paramètre n'est pas obligatoire pour une installation à distance. Les packages d'Installation contiennent leur propre configuration .xml qui est appliquée automatiquement.

Les paramètres pour ESET NOD32 Antivirus 2.x doivent être tapés après le nom de fichier *setup.exe*, qui peut être extrait avec d'autres fichiers du package d'installation (p. ex., *setup.exe /silentmode*) :

- **/SILENTMODE**
  Mode d'installation silencieuse – aucune boîte de dialogue ne s'affiche.

- **/FORCEOLD**
  Installe une version plus ancienne sur une version plus récente installée.

- **/CFG ="path_to_xml_file"**
  Durant l'installation, les paramètres définis dans les fichiers .xml spécifiés sont appliqués aux solutions client ESET. Le paramètre n'est pas obligatoire pour une installation à distance. Les packages d'Installation contiennent leur propre configuration .xml qui est appliquée automatiquement.

- **/REBOOT**
  Redémarre automatiquement après l'installation.

- **/SHOWRESTART**
  Après installation, une boîte de dialogue invitant l'utilisateur à confirmer le redémarrage s'affiche. Ce paramètre ne peut pas être utilisé en combinaison avec le paramètre *SILENTMODE*.

- **/INSTMFC**
  Installe les bibliothèques MFC pour le système d'exploitation Microsoft Windows 9x, qui sont requises pour le bon fonctionnement du programme. Ce paramètre peut toujours être utilisé, même si les bibliothèques MFC sont disponibles.

Sous Créer/Sélectionner le contenu du package d'installation (2), l'administrateur peut créer un package d'installation autonome avec une configuration prédéfinie d'un package d'installation existant et enregistré (le bouton **Copier**). Un tel package d'installation peut être exécuté sur la station de travail client sur laquelle le programme doit être installé. L'utilisateur doit uniquement exécuter le package pour installer le produit sans qu'il y ait de reconnexion à ERAS durant l'installation.

4.2.1 Configuration requise

La configuration de base pour l'installation à distance est un réseau TCP/IP correctement configuré, permettant une communication client-serveur fiable. L'installation d'une solution client à l'aide d'ERA impose des conditions plus strictes sur la station de travail client qu'une installation directe. Les conditions qui doivent être réunies pour une installation à distance sont les suivantes :

- client réseau Microsoft activé ;
- service de partage de fichiers et d'imprimantes activé ;
- ports de partage de fichiers (445, 135 – 139) accessibles ;
- protocole TCP/IP ;
- partage administratif ADMIN$ activé ;
- capacité du client à répondre à des requêtes PING ;
- connectivité d'ERAS et d'ERAC (ports –2224-2224 accessibles) ;

- nom d'utilisateur et mot de passe Administrateur existants pour les stations de travail client (le nom d'utilisateur ne peut pas rester vide) ;
- option Partage de fichiers simple désactivée ;
- service Serveur activé ;
- service Accès à distance au Registre activé.

Il est fortement recommandé de contrôler le respect de toutes les exigences avant installation, en particulier si le réseau comprend plusieurs stations de travail (sous l'onglet **Installation à distance**, cliquez sur **Installer... > Diagnostics**).

4.2.2 Configuration de l'environnement pour une installation à distance

Avant d'installer des produits de sécurité ESET sur des ordinateurs distants, l'administrateur doit préparer correctement l'environnement pour éviter des échecs d'installation.

Par exemple, l'outil de recherche intégré permet de parcourir le réseau pour trouver des stations de travail client non enregistrées. Les ordinateurs non enregistrés sont ceux qui ne sont pas connectés à ERAS.

Sous l'onglet Installation à distance, cliquez sur Chercher pour parcourir le réseau. Les ordinateurs non protégés s'affichent dans la partie droite de la fenêtre. Sur les ordinateurs trouvés et affichés dans la liste, vous pouvez tester des conditions pour les opérations ***Pousser l'installation, Copier,*** et ***Exporter***. L'option ***Chercher à partir du serveur*** permet de spécifier si les ordinateurs non protégés sont recherchés à partir d'ERAS ou d'ERAC. Il est recommandé de sélectionner cette option si vous vous connectez à un serveur ERA situé dans un autre réseau.

Après avoir trouvé des stations de travail appropriées pour l'installation d'une solution client, utilisez l'outil *Diagnostics d'installation à distance*.

Accédez à l'onglet ***Installation à distance***, puis cliquez sur le bouton ***Installer...***. Cliquez sur ***Diagnostics*** pour afficher la fenêtre **Diagnostics d'installation à distance** afin de contrôler les exigences d'installation et identifier des problèmes potentiels.

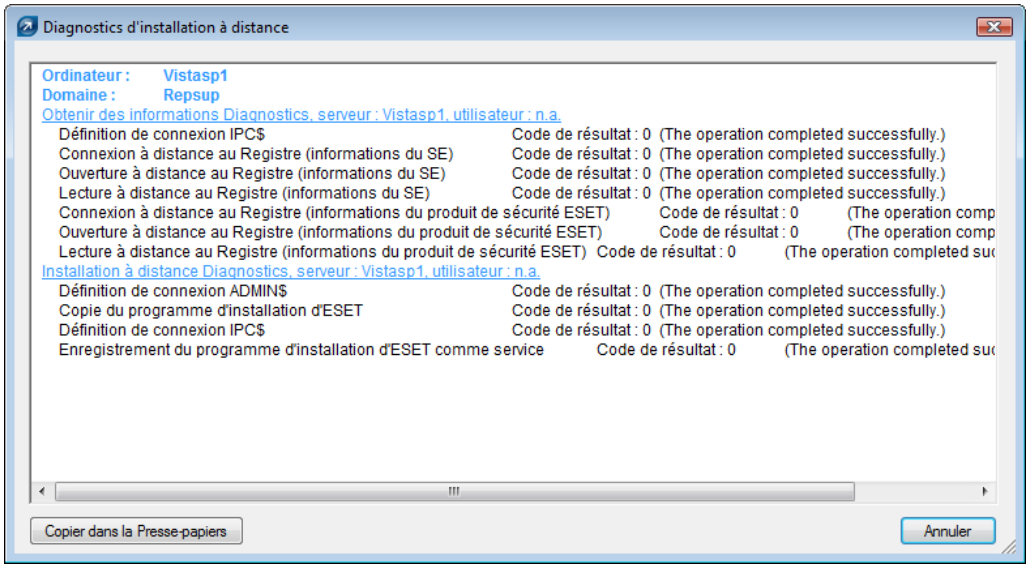


Figure 4-2 L'outil de diagnostic peut détecter des problèmes potentiels avant l'installation

La première partie de la section **Obtention de diagnostics d'information** présente des informations sur le produit de sécurité ESET installé sur l'ordinateur. La seconde partie indique si toutes les conditions d'installation du produit de sécurité ESET sont réunies.

4.2.3 Installation poussée à distance

Cette méthode d'installation à distance pousse instantanément des solutions client ESET sur des ordinateurs cibles distants. Les ordinateurs cibles doivent être en ligne. Ci-dessous figure une liste d'exigences (pour des exigences supplémentaires, voir la section 4.2.1, « **Configuration requise** »).

Pour lancer une installation poussée, procédez comme suit :

1) Dans ERAC (onglet **Installation à distance**), cliquez sur le bouton ***Installer...***. Dans la section **Favoris réseau** à gauche, accédez aux stations de travail sur lesquelles vous voulez pousser le package d'installation. Déplacez-les vers le volet vide à droite en les glissant-déplaçant.

2) Dans le menu déroulant ***Package***, sélectionnez le package d'installation à envoyer aux stations de travail cibles.

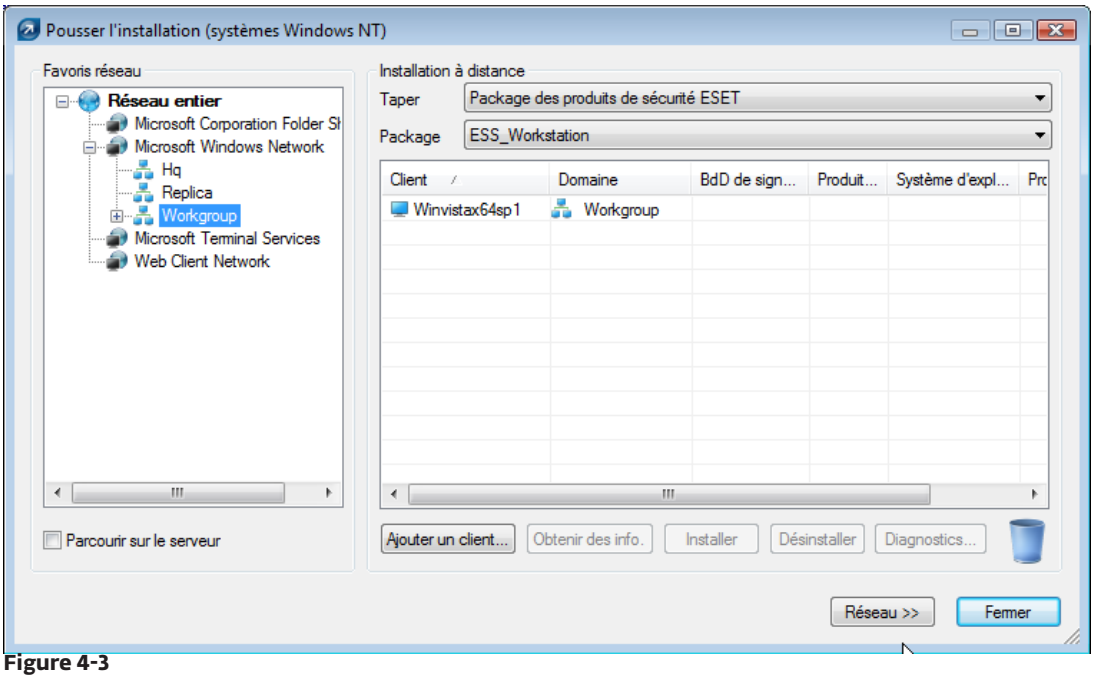


Figure 4-3

3) Dans le volet de droite, sélectionnez les stations de travail ayant besoin du package.

4) Cliquez sur Installer (vous pouvez également cliquer sur Obtenir des informations pour afficher des informations sur les clients sélectionnés).

5) Dans la plupart des cas, vous êtes invité à entrer le nom d'utilisateur et le mot de passe du compte utilisé pour accéder à la station de travail cible (ce compte doit bénéficier de droits d'administrateur).

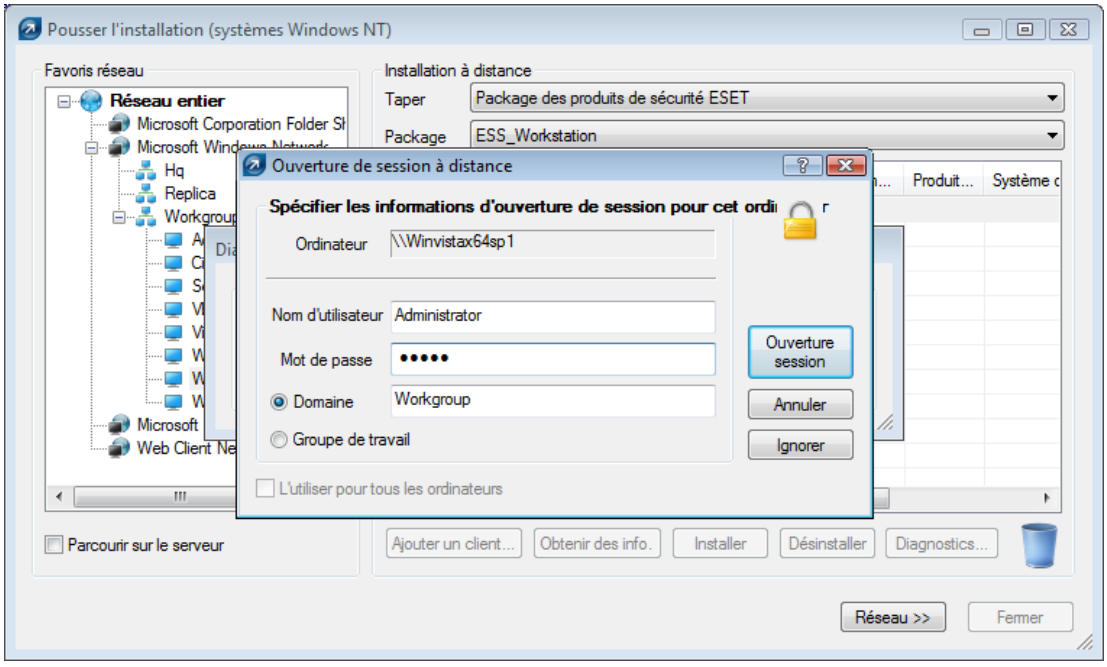


Figure 4-4

Les opérations suivantes sont indiquées par une barre de progression et un message texte. Les opérations sont décrites ci-dessous :

6) ERAS envoie l'agent einstaller.exe à la station de travail à l'aide du partage administratif admin$.

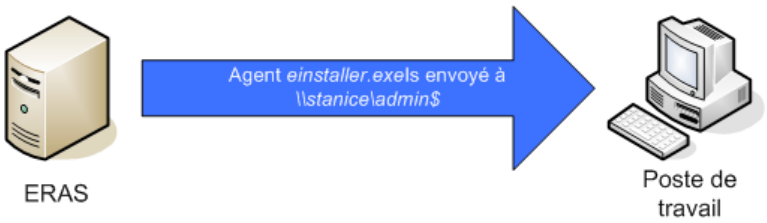
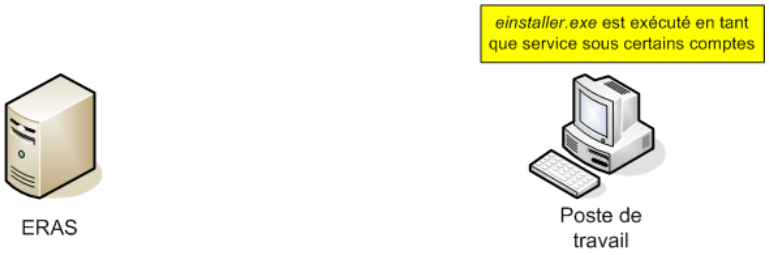
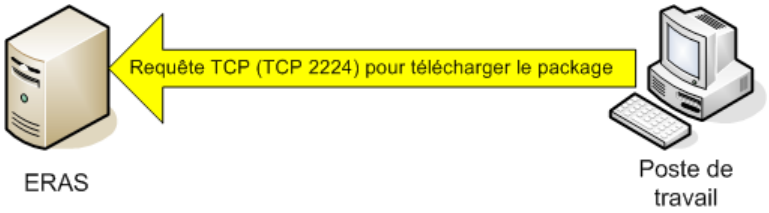


Figure 4-5

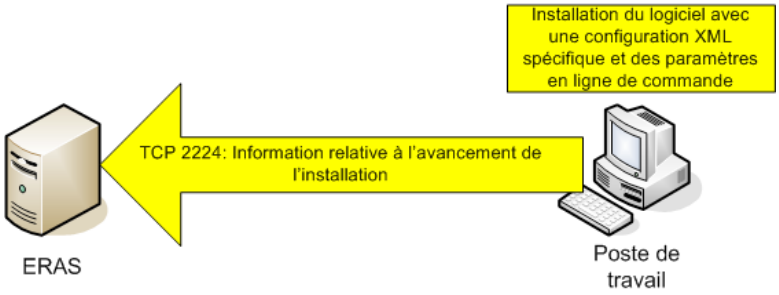
7) L'agent démarre en tant que service sous le compte système.



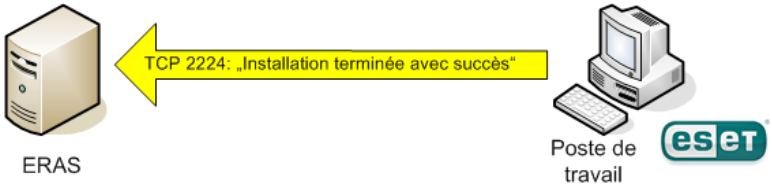
8) L'agent établit une communication avec son ERAS « parent » et télécharge le package d'installation correspondant sur le port TCP 2224.



9) L'agent installe le package sous le compte d'administrateur défini à l'étape 6 ; le fichier de configuration .xml correspondant et les paramètres de ligne de commande sont également appliqués.



10) Dès l'installation terminée, l'agent renvoie un message à ERAS. Certains produits de sécurité ESET requièrent un redémarrage et vous invitent à réagir si nécessaire.



Le menu contextuel (cliquez avec le bouton droit) de la boîte de dialogue **Pousser l'installation** offre les options suivantes :

- ***Obtenir des informations***
  Cette fonctionnalité détecte l'état actuel du produit de sécurité ESET sur les stations de travail sélectionnées (requiert un nom d'utilisateur et un mot de passe d'administrateur). Cette fonctionnalité utilise le partage admin$.
- ***Désinstaller***
  Suppression de programme. L'agent tente de désinstaller à distance le produit de sécurité ESET. L'option **Désinstaller** ne tient pas compte du package sélectionné dans le menu **Package**.
- ***Diagnostics***
  Contrôle la disponibilité des clients et services à utiliser durant l'installation à distance. Pour plus d'informations, consultez la section 4.2.2, « Configuration de l'environnement pour une installation à distance ».
- ***Supprimer les restes d'installation***
  Désenregistre les agents (einstaller.exe) du gestionnaire de services sur les stations de travail client et les supprime du disque dur. Si cette opération réussit, le drapeau empêchant des installations répétées du package est supprimé (voir la section 4.2.6, « Éviter des installations répétées »).
- ***Ouverture de session...***
  Ouvre une boîte de dialogue permettant de spécifier le nom d'utilisateur et le mot de passe d'administrateur qui, autrement, s'affiche automatiquement (étape 6). Cette fonctionnalité force une ouverture de session sur les stations de travail sélectionnées.
- ***Fermeture de session***
  Met fin à la session ouverte pour les stations de travail sélectionnées.
- ***Ajout d'un client...***
  Ajoute des stations de travail client individuelles à la liste. Entrez l'adresse IP ou le nom du client. Il est possible d'ajouter des clients supplémentaires simultanément.

4.2.4 Installation à distance par ouverture de session ou par Email

Les méthodes d'installation à distance par ouverture de session et par Email sont très similaires. Elles ne se différencient que par la manière dont l'agent einstaller.exe est envoyé aux stations de travail client. ERA permet d'exécuter l'agent via un script d'ouverture de session ou via Email. L'agent einstaller.exe peut également être utilisé individuellement et exécuté via d'autres méthodes (pour plus d'informations, consultez la section 4.2.5, « Installation à distance personnalisée »).

Si le script d'ouverture de session s'exécute automatiquement lorsque l'utilisateur ouvre une session, la méthode Email requiert une intervention de l'utilisateur qui doit lancer l'agent einstaller.exe à partir de la pièce jointe au message électronique. Si einstaller.exe est lancé plusieurs fois, il ne déclenche pas d'autre installation de solutions client ESET. Pour plus d'informations, consultez la section 4.2.6, « Éviter des installations répétées ».

La ligne appelant l'agent einstaller.exe à partir du script d'ouverture de session peut être insérée à l'aide d'un simple éditeur de texte ou de toute autre outil propriétaire. De même, einstaller.exe peut être envoyé en tant que pièce jointe de message électronique par tout client de messagerie. Quelle que soit la méthode utilisée, assurez-vous d'utiliser le fichier einstaller.exe approprié.

Pour le lancement d'einstaller.exe, l'utilisateur actuellement connecté ne doit pas nécessairement être un administrateur. L'agent adopte le nom d'utilisateur/mot de passe/domaine d'administrateur requis d'ERAS. Pour plus d'informations, consultez la fin de ce chapitre.

Entrez le chemin d'accès du fichier einstaller.exe dans le script d'ouverture de session :
- Sous l'onglet **Installation à distance**, cliquez sur ***Exporter...***, puis sélectionnez le **type** et le nom du **package** à installer.
- Cliquez sur le bouton **...** à côté de ***Dossier***, puis sélectionnez le répertoire où le fichier einstaller.exe sera situé et disponible au sein du réseau.
- Dans le champ ***Partager***, assurez-vous que le chemin d'accès est correct ou modifiez-le si nécessaire.
- Cliquez sur le bouton ... à côté de ***Dossier du script*** pour sélectionner le dossier où se trouve le script, puis modifiez le masque si nécessaire (***Fichiers***).
- Dans la section **Fichiers**, sélectionnez le fichier dans lequel insérer la ligne (invoquant einstaller.exe).
- Cliquez sur ***Export dans script d'ouverture de session*** pour insérer la ligne.
- Vous pouvez modifier l'emplacement de la ligne en cliquant sur ***Modifier >>***, puis l'enregistrer en cliquant sur le bouton ***Enregistrer***.

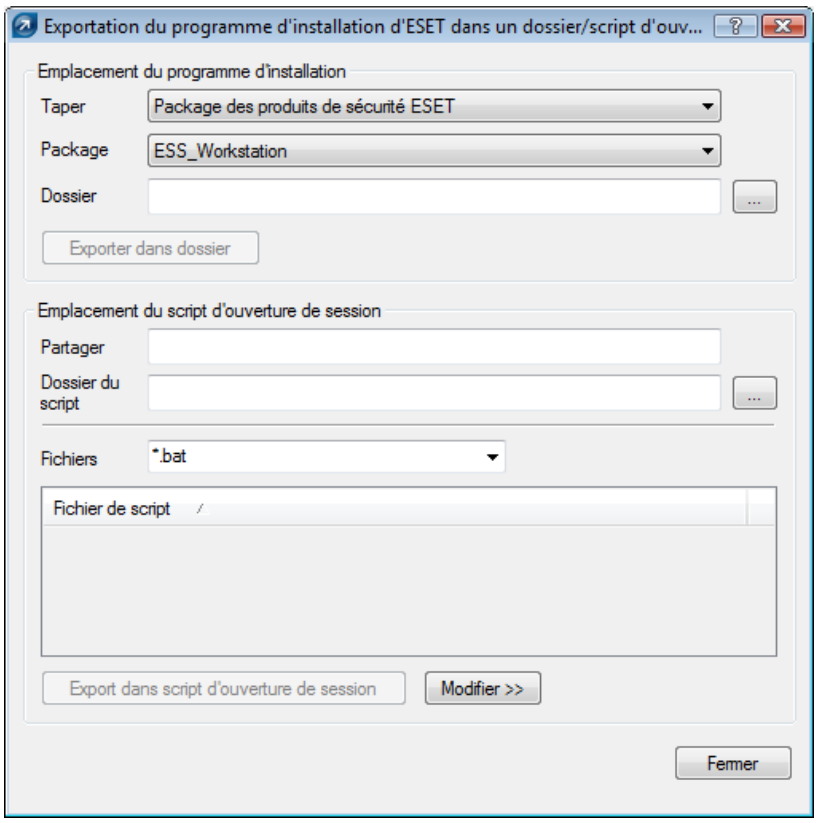


Figure 4-6 Boîte de dialogue Exportation du programme d'installation d'ESET dans un dossier/script d'ouverture de session

Joindre l'agent (einstaller.exe) à un Email :

- Sous l'onglet ***Installation à distance***, cliquez sur ***Email...***, puis sélectionnez le **Type** et le nom du **Package** à installer.
- Cliquez sur ***À...*** pour sélectionner des destinataires dans le carnet d'adresses (ou insérer des adresses individuelles).
- Entrez un ***Objet*** dans le champ correspondant.
- Tapez un message dans l'espace réservé au ***Corps*** du message.
- Cliquez sur ***Envoyer*** pour expédier le message[5].

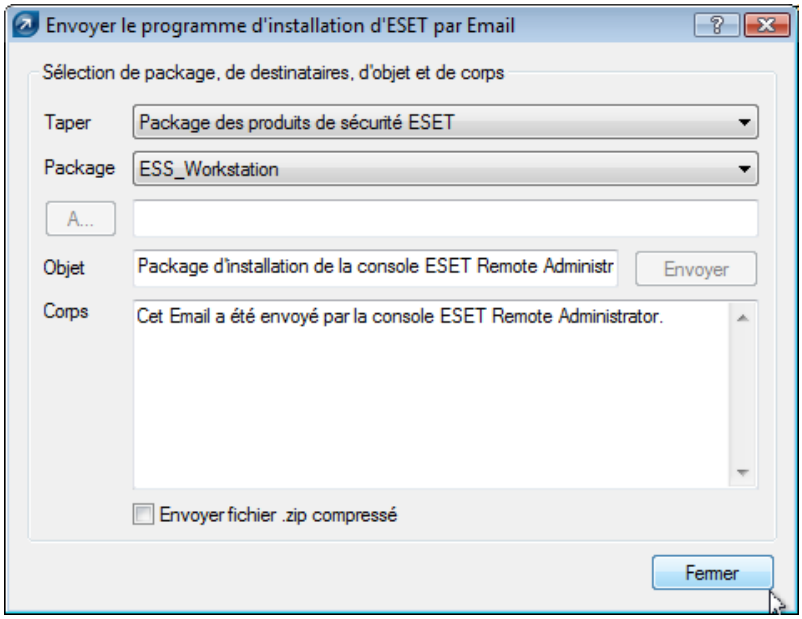


Figure 4-7 Boîte de dialogue Envoyer le programme d'installation d'ESET par Email

[5] Cette fonctionnalité utilise les paramètres SMTP définis sur ERAS.

Durant le processus d'installation à distance, une reconnexion à ERAS a lieu et l'agent (*einstaller.exe*) adopte les paramètres de l'option ***Ouverture de session par défaut pour installations par Email et script*** sous l'onglet ***Installation à distance***.

Figure 4-8

Cliquez sur ***Ouverture de session...*** pour spécifier le nom d'utilisateur et le mot de passe du compte sous lequel l'installation du package doit être effectuée. Il doit s'agir d'un compte disposant de droits d'administrateur ou, de préférence, d'un compte d'administrateur de domaine.

Les valeurs insérées dans la boîte de dialogue ***Ouverture de session...*** sont oubliées après chaque redémarrage du service (ERAS).

4.2.5 Installation à distance personnalisée

Il n'est pas obligatoire d'utiliser des outils ERA pour installer à distance des solutions client ESET. Finalement, l'aspect le plus important est de fournir et d'exécuter le fichier einstaller.exe sur les stations de travail client.

Pour le lancement d'einstaller.exe, l'utilisateur connecté ne doit pas nécessairement être un administrateur. L'agent adopte le nom d'utilisateur/mot de passe/domaine d'administrateur requis d'ERAS. Pour plus d'informations, consultez la fin de ce chapitre.

Le fichier einstaller.exe peut être obtenu comme suit :

- Sous l'onglet **Installation à distance**, cliquez sur ***Exporter...***, puis sélectionnez le **type** et le nom du **package** à installer.
- Cliquez sur le bouton **...** à côté de ***Dossier***, puis sélectionnez le répertoire dans lequel le fichier einstaller.exe sera exporté.
- Cliquez sur le bouton **Exporter dans dossier**.
- Utilisez le fichier einstaller.exe extrait.

REMARQUE : La méthode d'installation directe avec une configuration XML prédéfinie peut être utilisée dans des situations où il est possible de fournir des droits d'administrateur pour l'installation. Le package .msi est lancé à l'aide du paramètre /qn (version 3) ou du paramètre /silentmode (version 2). Ces paramètres exécuteront l'installation sans afficher d'interface utilisateur.

Durant le processus d'installation à distance, une reconnexion à ERAS a lieu et l'agent (*einstaller.exe*) adopte les paramètres de l'option ***Ouverture de session par défaut pour installations par Email et script*** sous l'onglet ***Installation à distance***.

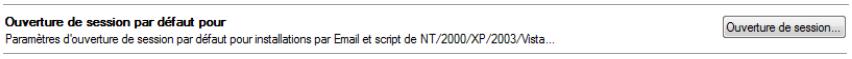


Figure 4-9

Cliquez sur ***Ouverture de session...*** pour spécifier le nom d'utilisateur et le mot de passe du compte sous lequel l'installation du package doit être effectuée. Il doit s'agir d'un compte disposant de droits d'administrateur ou, de préférence, d'un compte d'administrateur de domaine.

Si l'agent einstaller.exe est démarré manuellement sur une station de travail cible, l'installation à distance est gérée de la manière suivante :

- L'agent einstaller.exe envoie une demande à ERAS (port TCP 2224)

- ERAS démarre une nouvelle installation poussée (avec un nouvel agent) du package correspondant (envoyé via le partage *admin$*)[6]. Le nouvel agent commence ensuite à télécharger le package à partir d'ERAS via le protocole TCP/IP.

[6] L'agent attend une réponse d'ERAS (envoyant le package via le partage admin$). À défaut de réponse, l'agent tente de télécharger le package d'installation (via le port TCP/IP 2224). Dans ce cas, le nom d'utilisateur et le mot de passe d'administrateur spécifiés dans Installation à distance > Ouverture de session sur l'ERAS ne sont pas transférés et l'agent tente d'installer le package sous l'identité de l'utilisateur actuel. Sur les systèmes d'exploitation Microsoft Windows 9x/Me, il n'est pas possible d'utiliser le partage administratif, de sorte que l'agent établit automatiquement une connexion TCP/IP directe au serveur.

L'installation du package est lancée en appliquant les paramètres .xml associés sous le compte défini dans ERAS (bouton ***Ouverture de session...***)

4.2.6 Éviter des installations répétées

Dès que l'agent a terminé avec succès le processus d'installation à distance, il marque le client distant à l'aide d'un drapeau interdisant des installations répétées du même package d'installation. Le drapeau est inscrit dans la clé de registre suivante :

HKEY_LOCAL_MACHINE\Software\ESET\ESET Remote Installer

Si le type et le nom du package définis dans l'agent einstaller.exe correspondent aux données inscrites dans le Registre, aucune installation n'a lieu. Ce processus empêche des installations répétées sur les stations de travail cibles si l'agent einstaller.exe est lancé plusieurs fois.

REMARQUE : *La méthode d'installation poussée à distance ignore cette clé de registre.*

ERAS offre un niveau supplémentaire de protection contre des installations répétées, effectuées au moment où le programme d'installation établit une reconnexion à ERAS (TCP 2224). S'il y a un message d'erreur relatif à la station de travail, ou si l'installation a réussi, toute tentative d'installation supplémentaire est refusée.

L'agent enregistre l'erreur suivante dans le journal du programme d'installation situé dans *%TEMP %\einstaller.log* :

État 20 001 : Le serveur 'X:2224' a demandé la fermeture du programme d'installation d'ESET.

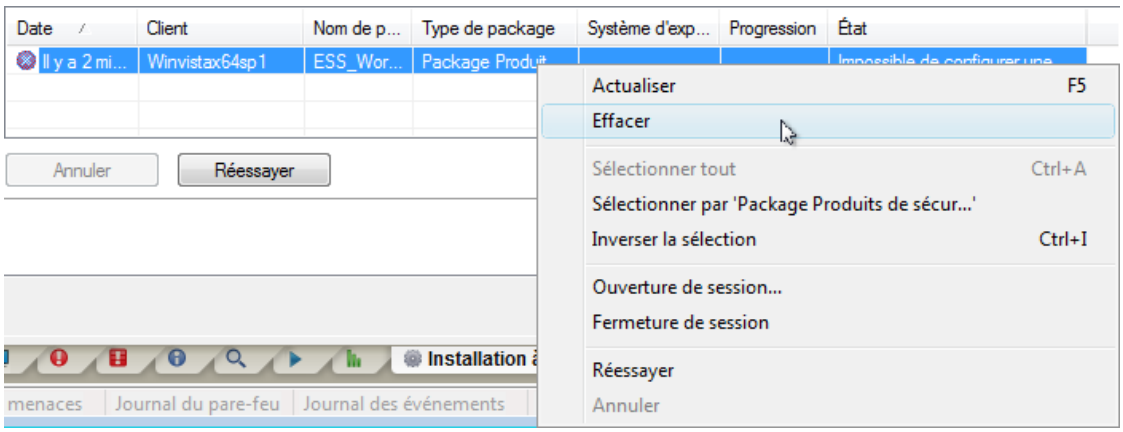


Figure 4-10

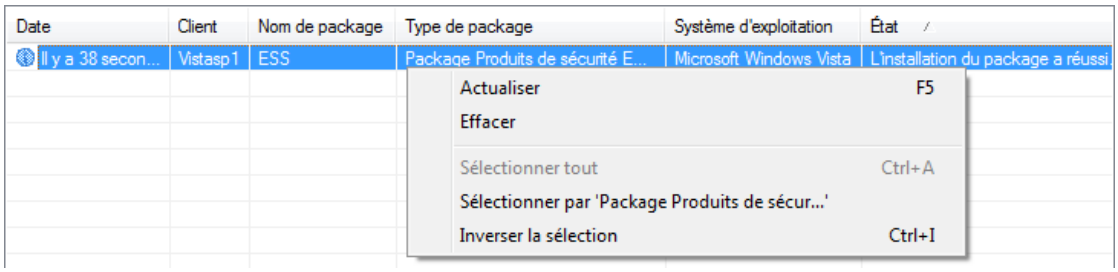


Figure 4-11

Pour empêcher ERAS de refuser des installations répétées, il faut supprimer les entrées correspondantes sous l'onglet ***Installation à distance***. Pour supprimer de telles entrées, cliquez avec le bouton droit, puis, dans le menu contextuel, activez l'option ***Effacer***.

4.3 Installation dans un environnement d'entreprise

Lors du déploiement de programmes dans un réseau de grande taille, il est important d'utiliser un outil capable d'effectuer des installations de programme à distance sur chaque ordinateur du réseau.

Installation via une stratégie de groupe

Dans l'environnement Active Directory, cette tâche peut être effectuée élégamment à l'aide d'une installation par stratégie de groupe. L'installation utilise le programme d'installation MSI qui est distribué directement à tous les clients se connectant au domaine via une stratégie de groupe.

Pour configurer un contrôleur de domaine pour installer automatiquement ESET Smart Security ou ESET NOD32 Antivirus sur chaque station de travail, après connexion, procédez comme suit :

1) Créez un dossier partagé sur votre contrôleur de domaine. Toutes les stations de travail doivent disposer d'une autorisation d'accès en lecture à ce dossier.

2) Copiez le package d'installation d'ESET Smart Security ou d'ESET NOD32 Antivirus (.msi) dans le dossier.

3) Insérez un fichier de configuration .xml à appliquer au programme dans le même dossier. Le fichier doit être nommé cfg.xml. Pour créer un fichier de configuration, vous pouvez utiliser l'éditeur de configuration d'ESET. Pour plus d'informations, consultez la section 3.7, « Éditeur de configuration d'ESET ».

4) Cliquez sur ***Démarrer > Programmes > Outils d'administration > Utilisateurs et ordinateurs Active Directory.***

5) Cliquez avec le bouton droit sur le nom de domaine, puis sélectionnez ***Propriétés > Stratégie de groupe > Modifier > Configuration utilisateur.***

6) Cliquez avec le bouton droit sur ***Paramètres du logiciel***, puis sélectionnez ***Nouveau > Package.***

7) Dans la fenêtre ***Ouvrir***, spécifiez le chemin UNC du package d'installation partagé, c.-à-d. *computer_name**path**installation_package.msi*, puis cliquez sur ***Ouvrir***. N'utilisez pas l'option **Parcourir** pour localiser le package d'installation, car elle afficherait un chemin de réseau local plutôt qu'un chemin de réseau UNC.

8) Dans la boîte de dialogue suivante, activez l'option ***Attribué***. Cliquez ensuite sur ***OK*** pour fermer la fenêtre.

En procédant de la manière décrite ci-dessus, le package du programme d'installation sera installé sur chaque ordinateur accédant au domaine. Pour installer le package sur des ordinateurs actuellement opérationnels, les utilisateurs doivent se déconnecter puis se reconnecter.

Si vous voulez donner à l'utilisateur la possibilité d'accepter ou de refuser l'installation du package, à l'étape 8, sélectionnez ***Publier*** au lieu de ***Attribué***. La prochaine fois que l'utilisateur se connectera, le package sera ajouté à ***Panneau de configuration > Ajout ou suppression de programmes > Ajouter un programme > Ajouter des programmes à partir de votre réseau.*** Le package sera alors à la disposition des utilisateurs pour des installations futures à partir de cet emplacement.

5. Administration d'ordinateurs client

5.1 Tâches

Vous pouvez configurer et administrer les stations de travail client correctement connectées à ERAS et affichées dans ERAC à l'aide de différents types de tâches. Vous pouvez appliquer des tâches à plusieurs clients ou à un ou plusieurs groupes de clients. Pour appliquer une tâche à une ou plusieurs stations de travail client, dans le volet ***Clients***, cliquez dessus avec le bouton droit. Cliquez ensuite sur ***Nouvelle tâche***, puis sélectionnez le type de tâche à exécuter. Vous pouvez également ouvrir l'Assistant Tâche à partir du menu principal d'ERAC en cliquant sur ***Actions > Nouvelle tâche***.

Les trois sections suivantes décrivent les types de tâches individuelles pour les stations de travail client et fournissent une exemple de scénario pour chacun d'eux.

5.1.1 Tâche de configuration

Les tâches de configuration permettent de modifier les paramètres de protection sur les stations de travail client. Ces tâches sont envoyées aux stations de travail client dans des packages de configuration contenant les paramètres de modification. Les fichiers .xml créés dans l'éditeur de configuration d'ESET ou exportés à partir de clients sont également compatibles avec les tâches de configuration. L'exemple ci-dessous montre comment créer une tâche de configuration qui modifie le nom d'utilisateur et le mot de passe sur des ordinateurs cibles. Les commutateurs et options non utilisés dans cet exemple sont décrits à la fin de ce chapitre.

Premièrement, désignez les stations de travail auxquelles la tâche doit être envoyée. Marquez-les dans le volet ***Clients*** d'ERAC.

1) Cliquez avec le bouton droit sur une station de travail sélectionnée, puis, dans le menu contextuel, sélectionnez ***Nouvelle tâche > Tâche de configuration***.

2) La fenêtre ***Configuration pour les clients*** s'ouvre, qui fait office d'Assistant Tâche de configuration. Vous pouvez spécifier la source du fichier de configuration en cliquant sur **Créer...**, **Sélectionner...** ou **Créer à partir d'un modèle...**

3) Cliquez sur le bouton ***Créer*** pour ouvrir l'éditeur de configuration d'ESET, puis spécifiez la configuration à appliquer. Accédez à ***ESET Smart Security, ESET NOD32 Antivirus > Module de mise à jour > Profil > Configuration > Nom d'utilisateur*** et ***Mot de passe.***

4) Insérez le nom d'utilisateur et le mot de passe fournis par ESET, puis cliquez sur ***Console*** à droite pour revenir à l'Assistant Tâche. Le chemin d'accès du package s'affiche dans le champ Créer/Sélectionner une configuration.

5) Si vous avez déjà un fichier de configuration contenant les modifications souhaitées, cliquez sur ***Sélectionner***, recherchez le fichier, puis attribuez-le à la tâche de configuration.

6) Vous pouvez également cliquer sur ***Créer à partir d'un modèle***, sélectionner le fichier .xml, puis apporter les modifications nécessaires.

7) Pour consulter ou modifier le fichier de configuration que vous venez de créer ou de modifier, cliquez sur le bouton ***Affichage*** ou ***Edition***.

8) Cliquez sur **Suivant** pour accéder à la fenêtre ***Clients sélectionnés*** qui présente les stations de travail auxquelles envoyer la tâche. À ce stade, vous pouvez ajouter des clients, des groupes de clients ou tous les clients. Cliquez sur ***Ajout spécial*** pour ajouter des clients à partir de serveurs ou de groupes sélectionnés. Cliquez sur ***Suivant*** pour passer à l'étape suivante.

9) La dernière boîte de dialogue, ***Rapport des tâches*** affiche un aperçu de la tâche de configuration. Entrez un nom ou une description pour la tâche (facultatif). L'option ***Appliquer la tâche après*** permet de définir la tâche à exécuter après une date/heure spécifiée. L'option ***Supprimer automatiquement les tâches terminées par nettoyage*** supprime toutes les tâches envoyées avec succès aux stations de travail cibles.

- Cliquez sur ***Terminer*** pour enregistrer la tâche à exécuter.

5.1.2 Tâches Analyse à la demande

L'option de menu contextuel ***Nouvelle tâche*** contient deux variantes de l'analyse à la demande. La première option est ***Analyse à la demande (nettoyage désactivé)***. Elle ne fait que créer un journal ; aucune action n'est appliquée aux fichiers infectés. La seconde option est ***Analyse à la demande (nettoyage activé).***

La fenêtre ***Analyse à la demande*** contient les mêmes paramètres par défaut pour les deux variantes, à l'exception de l'option ***Analyser sans nettoyer***. Cette option détermine si l'analyseur doit ou non nettoyer les fichiers infectés. L'exemple ci-dessous montre comment créer une tâche d'analyse à la demande

- Le menu déroulant ***Section de configuration*** permet de sélectionner le type de produit ESET pour lequel la tâche d'analyse à la demande est définie. Sélectionnez l'un des produits installés sur les stations de travail cibles.

- L'option ***Exclure cette section de l'analyse à la demande*** désactive tous les paramètres définis dans la fenêtre pour le type de produit sélectionné ; ils ne sont pas appliqués aux stations de travail sur lesquelles le type de produit défini dans Section de configuration est installé. Ainsi, tous les clients sur lesquels est installé le produit spécifié sont exclus de la liste des destinataires. Si l'administrateur marque des clients comme destinataires et exclut le produit à l'aide du paramètre précité, la tâche échoue et une notification s'affiche indiquant qu'il n'a pas été possible de l'exécuter. Pour éviter cela, l'administrateur doit toujours spécifier les clients auxquels attribuer la tâche.

- Dans ***Nom de profil***, vous pouvez sélectionner un profil d'analyse à appliquer pour la tâche.

- Dans la section ***Lecteurs à analyser***, sélectionnez les types de lecteur à analyser sur les ordinateurs client. Si la sélection est trop générale, vous pouvez ajouter le chemin d'accès exact des objets à analyser. À cette fin, utilisez le champ ***Chemin d'accès*** ou le bouton ***Ajouter un chemin***. Sélectionnez ***Effacer historique*** pour restaurer la liste d'origine des lecteurs à analyser.

- Cliquez sur ***Suivant*** pour accéder aux boîtes de dialogue ***Sélection de clients*** et ***Rapport des tâches*** qui sont identiques aux boîtes de dialogue de l'Assistant Tâche de configuration (voir la section 5.1.1, « Tâche de configuration »).

Une fois l'exécution de la tâche terminée sur les stations de travail client, les résultats sont renvoyés à ERAS où vous pouvez les consulter dans le volet ***Journal d'analyse***.

5.1.3 Tâche Mettre à jour maintenant

L'objectif de cette tâche est d'appliquer des mises à jour à des stations de travail cibles (mises à jour de base des signatures de virus ainsi que mises à niveau de composants de programme). Cliquez avec le bouton droit sur une station de travail dans le volet ***Clients***, puis sélectionnez ***Nouvelle tâche > Mettre à jour maintenant***. Pour exclure de la tâche certains types de produit de sécurité ESET, sélectionnez-les dans le menu déroulant ***Section de configuration***, puis activez l'option ***Exclure cette section de la tâche de mise à jour***. Pour utiliser un profil de mise à jour spécifique pour la tâche Mettre à jour maintenant, activez l'option ***Spécifier un nom de profil***, puis sélectionnez le profil souhaité. Vous pouvez également sélectionner ***Nom de profil défini par l'utilisateur***, puis entrer le nom de profil. Pour rétablir la valeur par défaut du champ, cliquez sur ***Effacer historique***. Cliquez ensuite sur ***Suivant*** pour accéder aux boîtes de dialogue ***Sélection de clients*** et ***Rapport des tâches***. Pour une description de ces boîtes de dialogue, consultez la section 5.1.1, « Tâche de configuration ».

5.2 Groupes

ERAC intègre plusieurs outils et fonctionnalités permettant d'administrer de façon conviviale les clients et les événements. L'une de ces fonctionnalités est l'Éditeur de groupes qui, lors de l'utilisation de filtres ou de la création de tâches, permet d'appliquer ces activités simultanément à un groupe entier de clients.

Vous pouvez diviser des clients individuels en plusieurs groupes à l'aide de l'Éditeur de groupes dans ERAC. Il est accessible sous ***Outils*** > ***Éditeur de groupes*** ou en appuyant sur CTRL + G.

La fenêtre **Éditeur de groupes** est divisée en deux parties. À gauche, figure la liste des groupes existants et, à droite, la liste des clients. Le volet de droite indique les clients affectés à un groupe sélectionné à gauche. De même, toutes les opérations représentées par des boutons au bas de cette fenêtre sont effectuées sur les groupes ou les clients sélectionnés.

Pour créer un groupe, cliquez sur ***Créer***, puis sélectionnez un nom pour le groupe. Il est recommandé d'utiliser un nom indiquant où se trouvent les ordinateurs (p. ex., Département commercial, Assistance technique, etc.). Le champ ***Description*** permet de décrire plus précisément le groupe (p.ex., « Ordinateurs du bureau C », « Stations de travail du siège », etc.). Vous pouvez modifier les groupes créés et configurés ultérieurement.

Cliquez sur ***OK*** pour créer le groupe. Son nom et sa description s'affichent à gauche et le bouton ***Ajouter/Supprimer*** devient actif. Cliquez sur ce bouton pour ajouter les clients à inclure dans le groupe (soit en double-cliquant dessus, soit en les glissant-déplaçant de gauche à droite). Pour trouver un client à ajouter, entrez son nom ou une partie de celui-ci dans le champ ***Recherche rapide***. Tous les clients contenant la chaîne saisie s'affichent. Pour marquer tous les clients, cliquez sur ***Sélectionner tout***. Cliquez sur le bouton ***Actualiser*** pour vérifier la présence de nouveaux clients connectés récemment au serveur.

Si la sélection manuelle de client ne convient pas, vous pouvez cliquer sur **Ajout spécial...** pour accéder à d'autres options.

Activez l'option ***Ajouter des clients dans le volet Clients*** pour ajouter tous les clients affichés dans la section Client, ou activez l'option ***Uniquement sélectionnés*** pour ajouter des clients appartenant déjà à un autre serveur ou groupe, sélectionnez-les dans les listes à gauche et à droite, puis cliquez sur ***Ajouter***.

Cliquez sur OK dans la boîte de dialogue Ajouter/Supprimer pour revenir à la fenêtre principale de l'Éditeur de groupes. Le nouveau groupe doit s'afficher avec les clients correspondants.

Cliquez sur le bouton ***Ajouter/Supprimer*** pour ajouter ou supprimer des clients dans des groupes, ou cliquez sur le bouton ***Supprimer*** pour supprimer un groupe entier. Cliquez sur le bouton ***Copier dans le Presse-papiers*** pour copier les listes de clients et de groupes.

La dernière option de l'Éditeur de groupes consiste à utiliser une création automatique de groupe (avec les clients correspondant) basée sur la structure définie par Active Directory. Notez que cette option n'est disponible que si ERAS est installé sur un système disposant également d'Active Directory. Pour adopter la structure d'Active Directory, cliquez sur ***Synchroniser avec Active Directory***. Vous pouvez également ajouter un client à un groupe en cliquant dessus avec le bouton droit sous l'onglet Clients, puis en sélectionnant ***Ajouter à un groupe...***

Avertissement : *Si vous utilisez l'option* ***Synchronisation complète****, tous les groupes existants seront supprimés ! Sinon, les nouveaux groupes et leur clients sont ajoutés, tandis que les groupes existants sont conservés.*

Vous pouvez effectuer une configuration détaillée de la synchronisation Active Directory à l'aide de l'éditeur de configuration (**Console ESET Remote Administrator** > **Serveur ERA** > **Paramètres** > **Active directory** > **Synchronisation de groupes/Active Directory**). Par défaut, seuls le **groupe de sécurité ordinateur** et les **unités d'organisation informatique** sont synchronisés. Toutefois, vous pouvez ajouter un autre objet Active Directory en activant l'option souhaitée.

5.2.1 Filtrage

Si le volet Clients contient un trop grand nombre de clients, vous pouvez utiliser des options de filtrage. Pour plus d'informations, consultez la section 3.3, « Filtrage des informations ».

5.3 Stratégies

Les stratégies sont, à maints égards, similaires aux tâches de configuration, sauf qu'il ne s'agit pas de tâches isolées envoyées à une ou plusieurs stations de travail. Elles assurent plutôt une maintenance continue de certains paramètres de configuration des produits de sécurité ESET. Autrement dit, une stratégie est une configuration appliquée à un client.

5.3.1 Principes de base et fonctionnement

Accédez au Gestionnaire de stratégies en cliquant sur ***Outils > Gestionnaire de stratégies...***. L'arborescence de stratégie à gauche répertorie les stratégies présentes sur les serveurs individuels. La partie droite est divisée en quatre sections ; ***Paramètres de stratégie, Configuration de stratégie, Action de stratégie*** et **Paramètres de stratégie globale**. Les options figurant dans ces sections permettent à un administrateur de gérer et de configurer des stratégies.

Les principales fonctions du gestionnaire de stratégies sont la création, la modification et la suppression de stratégies. Les clients reçoivent des stratégies d'ERAS. ERAS peut utiliser plusieurs stratégies pouvant hériter des paramètres les unes des autres ou de stratégies d'un serveur de niveau supérieur.

Le système d'adoption de stratégies d'un serveur de niveau supérieur est appelé ***héritage*** ; les stratégies créées à la suite d'un héritage sont appelées ***stratégies fusionnées***. L'héritage est basé sur le principe parent-enfant, à savoir qu'une stratégie enfant hérite des paramètres d'une stratégie parent. Par défaut, les paramètres spécifiés dans la stratégie enfant sont hérités et les paramètres existants remplacés.

5.3.2 Comment créer des stratégies

L'installation par défaut n'implémente qu'une seule stratégie appelée « Stratégie du serveur ». Vous pouvez modifier ce nom dans le champ ***Paramètres de stratégie > Nom de stratégie***. Vous pouvez configurer la stratégie proprement dite dans l'éditeur de configuration d'ESET en cliquant sur ***Modifier***, puis en définissant des paramètres pour le produit de sécurité ESET sélectionné (ou client). Tous les paramètres sont organisés dans une structure étendue et tous les éléments de l'Éditeur sont associés à une icône. Les clients n'adoptent que les paramètres actifs (marqués d'une icône bleue). Les paramètres inactifs (grisés) restent inchangés sur les ordinateurs cibles. Le même principe s'applique aux stratégies héritées et fusionnées ; une stratégie enfant n'adopte que les paramètres actifs d'une stratégie parent.

Les serveurs ERA autorisent plusieurs stratégies (***Ajouter une nouvelle stratégie enfant***). Les options disponibles pour les nouvelles stratégies sont les suivantes : nom de stratégie, liaison à une ***Stratégie parent*** et configuration (la configuration peut être vide, copiée à partir d'une stratégie existante ou copiée à partir d'un fichier de configuration .xml). Vous ne pouvez créer des stratégies que sur le serveur auquel vous êtes connecté via ERAC. Pour créer une stratégie sur un serveur de niveau inférieur, vous devez vous connecter directement à ce dernier.

Chaque stratégie a deux attributs de base ***Remplacer toute stratégie enfant*** et ***Stratégie réplicable vers le bas***. Ces attributs définissent la manière dont les stratégies enfant adoptent des paramètres de configuration actifs.

Remplacer toute stratégie enfant – Applique tous les paramètres actifs aux stratégies héritées. Si la stratégie enfant diffère, la stratégie fusionnée contient tous les paramètres actifs de la stratégie parent (même si l'attribut « ***Remplacer...*** » est actif pour la stratégie enfant). Tous les paramètres inactifs de la stratégie parent s'ajustent à la stratégie enfant. Si l'attribut ***Remplacer toute stratégie enfant*** n'est pas activé, les paramètres de la stratégie enfant ont la priorité sur ceux de la stratégie parent pour la stratégie fusionnée obtenue. De telles stratégies fusionnées s'appliquent à toutes les autres stratégies si elles y sont liées en tant que stratégies parent.

Stratégie réplicable vers le bas – Active la réplication vers les stratégies enfant. Cela signifie que la stratégie peut servir de stratégie par défaut pour des serveurs de niveau inférieur ainsi qu'être attribuée aux clients qui y sont connectés.

Figure 5-1 : Exemple d'héritage de stratégie

5.3.3 Stratégies virtuelles

Outre les stratégies créées et celles répliquées à partir d'autres serveurs (voir la section 7.4., « Réplication »), l'arborescence de stratégie contient une stratégie parent par défaut et une stratégie de clients principaux par défaut, appelées stratégies virtuelles.

La stratégie parent par défaut se trouve sur un serveur de niveau supérieur dans les Paramètres de stratégie globale et est sélectionnée comme ***Stratégie par défaut pour les serveurs de niveau inférieur***. Si le serveur n'est pas répliqué, cette stratégie est vide (cela sera expliqué ultérieurement).

La stratégie de clients principaux par défaut se trouve dans les Paramètres de stratégie globale du serveur donné (pas le serveur de niveau supérieur) et est sélectionnée dans Stratégie par défaut pour les clients principaux. Elle est automatiquement appliquée aux nouveaux clients connectés (clients principaux) de l'ERAS donné, à moins qu'ils aient déjà adopté une autre stratégie à partir des Règles de stratégie (pour plus d'informations, voir la section 5.3.6, « Attribution de stratégies à des clients »). Les stratégies virtuelles sont des liens vers d'autres stratégies situées sur le même serveur.

5.3.4 Stratégies et structure de l'éditeur de configuration d'ESET

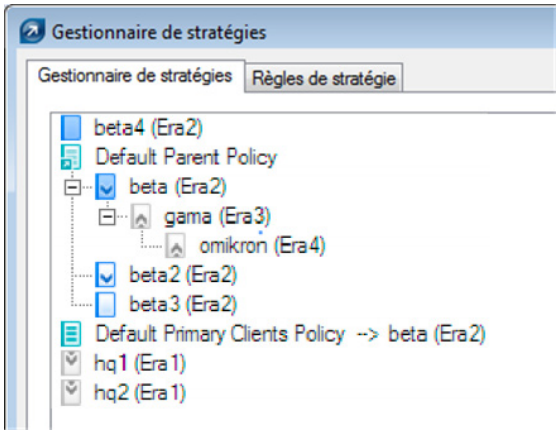


Figure 5-2

À chaque stratégie figurant dans l'arborescence de stratégie est affectée une icône à gauche. La signification des icônes est la suivante :

1) Les stratégies avec des icônes bleues sont celles présentes sur le serveur donné. Il y a trois sous-groupes d'icônes bleues :

Icônes avec cibles blanches – La stratégie a été créée sur ce serveur. En outre, elle n'est pas réplicable, ce qui signifie qu'elle n'est pas affectée à des clients de serveurs de niveau inférieur et qu'elle ne fait pas office de stratégie parent pour les serveurs enfant. Ces stratégies ne peuvent être appliquées qu'à l'intérieur du serveur, aux clients qui y sont connectés. Elles peuvent également servir de stratégie parent pour une autre stratégie du même serveur.

Icônes avec cibles bleues – La stratégie a également été créée sur le serveur, mais l'option ***Remplacer toute stratégie enfant*** est activée (pour plus d'informations, consultez la section 5.3.2, « Comment créer des stratégies »).

, Icônes avec flèches vers le bas – Ces stratégies sont répliquées ; l'option ***Stratégie réplicable vers le bas*** est activée. Vous pouvez les appliquer sur le serveur donné et sur ses serveurs enfants.

2) Les stratégies avec des icônes grises proviennent d'autres serveurs.

Icônes avec flèches vers le haut – Ces stratégies sont répliquées à partir de serveurs enfant. Il n'est possible de les afficher ou de les supprimer qu'avec l'option ***Supprimer une branche de stratégie***. Cette option ne supprime pas les stratégies proprement dites ; elles les supprime uniquement de l'arborescence de stratégie. Elles peuvent donc réapparaître après réplication. Si vous ne voulez pas afficher les stratégies de serveurs de niveau inférieur, utilisez l'option ***Masquer les stratégies de serveur étranger non utilisées dans l'arborescence de stratégie***.

Icônes avec flèches vers le bas – Ces stratégies sont répliquées à partir de serveurs de niveau supérieur. Vous pouvez les utiliser comme stratégies parent pour d'autres stratégies, les attribuer à des clients (***Ajouter***

des clients) ou les supprimer (***Supprimer la stratégie***). Notez qu'une suppression ne supprime que la stratégie qui réapparaîtra après réplication à partir du serveur de niveau supérieur (à moins que l'attribut ***Stratégie réplicable vers le bas*** ait été désactivé sur le serveur de niveau supérieur).

REMARQUE : *Pour déplacer et attribuer des stratégies à l'intérieur de la structure, vous pouvez soit sélectionner la stratégie parent, soit la glisser-déplacer à l'aide de la souris.*

5.3.5 Affichage des stratégies

Vous pouvez afficher les stratégies figurant dans l'arborescence de stratégie directement dans l'éditeur de configuration en cliquant sur ***Afficher...*** ou sur ***Affichage fusionné...***

Affichage fusionné – Affiche la stratégie fusionnée créée à la suite d'un héritage (le processus d'héritage applique les paramètres de la stratégie parent). Cet option s'affiche par défaut parce que la stratégie actuelle est déjà fusionnée.

Affichage – Affiche la stratégie d'origine avant sa fusion avec une stratégie parent.
Sur les serveurs de niveau inférieur, les options suivantes sont disponibles pour les stratégies héritées de serveurs de niveau supérieur :

Affichage fusionné – Comme ci-dessus

Afficher partie remplacée – Ce bouton s'applique aux stratégies avec l'attribut ***Remplacer toute stratégie enfant***. Cette option n'affiche que la partie forcée de la stratégie, c'est-à-dire celle qui a la priorité sur d'autres paramètres des stratégies enfant.

Afficher partie non forcée – a l'effet opposé de Afficher partie remplacée ; seuls s'affichent les éléments actifs auxquels l'option ***Remplacer...*** n'est pas appliquée.

5.3.6 Attribution de stratégies à des clients

Deux grandes règles régissent l'attribution de stratégies à des clients :

1) Vous pouvez attribuer à des clients locaux (principaux) toute stratégie locale ou toute stratégie répliquée à partir de serveurs de niveau supérieur.

2) Vous pouvez attribuer à des clients répliqués à partir de serveurs de niveau inférieur toute stratégie locale avec l'attribut ***Réplicable vers le bas*** ou toute stratégie répliquée à partir de serveurs de niveau supérieur. Il n'est pas possible de les forcer à adopter des stratégies de leur propre serveur principal (pour ce faire, vous devez vous connecter à ce serveur avec ERAC).

Un aspect important est qu'une stratégie est attribuée à chaque client (il n'y a pas de client sans stratégie). De même, vous ne pouvez pas supprimer une stratégie d'un client. Vous pouvez uniquement la remplacer par une autre. Si vous ne voulez pas appliquer de configuration à un client à partir d'une stratégie existante, créez une stratégie vide.

5.3.6.1 Stratégie de clients principaux par défaut

Une méthode d'attribution de stratégies est l'application automatique de la Stratégie de clients principaux par défaut, stratégie virtuelle configurable dans les Paramètres de stratégie globale. Cette stratégie s'applique aux clients principaux, c.-à-d. ceux qui sont directement connectés à cet ERAS. Pour plus d'informations, consultez la section 5.3.3, « Stratégies virtuelles ».

5.3.6.2 Attribution manuelle

Il y deux manières d'attribuer manuellement des stratégies : Cliquez avec le bouton droit sur un client dans le volet *Clients*, puis, dans le menu contextuel, sélectionnez ***Ajouter une stratégie***, ou, dans le Gestionnaire de stratégies, cliquez sur ***Ajouter des clients > Ajouter/Supprimer***.

Le fait de cliquer sur ***Ajouter des clients*** dans le Gestionnaire de stratégies ouvre la boîte de dialogue Ajouter/Supprimer. Les clients sont répertoriés à gauche au format Serveur/Client. Si la stratégie réplicable vers le bas est sélectionnée, la fenêtre présente également les clients répliqués à partir de serveurs de niveau inférieur. Sélectionnez les clients devant recevoir la stratégie en les glissant-déplaçant ou en cliquant sur >> pour les déplacer vers les Éléments

sélectionnés. Les nouveaux clients sélectionnés sont marqués à l'aide d'un astérisque jaune. Vous pouvez les supprimer de la liste Éléments sélectionnés en cliquant sur le bouton **<<** ou **C**. Cliquez sur **OK** pour confirmer la suppression.

REMARQUE : Après confirmation, si vous rouvrez la boîte de dialogue Ajouter/Supprimer, vous ne pouvez plus supprimer les clients de la liste Éléments sélectionnés, mais uniquement remplacer la stratégie.

La fonctionnalité ***Ajout spécial*** permet d'ajouter tous les clients en même temps, d'ajouter des clients sélectionnés ou d'ajouter des clients à partir de serveurs ou de groupes sélectionnés.

5.3.6.3 Règles de stratégie

L'outil ***Règles de stratégie*** permet à un administrateur d'attribuer automatiquement des stratégies à des stations de travail client de façon plus étendue. Les règles sont appliquées dès que le client se connecte au serveur ; elles ont la priorité sur la ***Stratégie de clients principaux par défaut*** et sur l'attribution manuelle. La ***Stratégie de clients principaux par défaut*** ne s'applique que si le client n'est régi par aucune des règles actuelles. De même, si une stratégie attribuée manuellement doit être appliquée, qui soit en conflit avec les règles de stratégie, la configuration forcée par les règles de stratégie est prioritaire.

Le Gestionnaire de stratégies contient un onglet permettant de créer et gérer les règles de stratégie. Le processus de création et d'application de règle est très similaire au processus de création et de gestion de règle dans les clients de messagerie : chaque règle contient un ou plusieurs critères ; plus la règle est haut placée dans la liste, plus elle est importante (vous pouvez la déplacer vers le haut ou le bas).

Pour créer une règle, cliquez sur le bouton ***Nouvelle...*** Complétez ensuite les champs ***Nom, Description***, ***Paramètres de filtre du client*** et ***Stratégie*** (stratégie qui sera appliquée à tous les clients correspondant aux critères spécifiés).

Pour configurer les critères de filtrage, cliquez sur le bouton ***Modifier***.

Les critères disponibles sont les suivants :

(PAS) DU serveur principal – Si (non) localisée sur le serveur principal
(N') EST (PAS) un nouveau client – S'il (ne) s'agit (pas) d'un nouveau client
(N') A un (PAS de) drapeau Nouveau – S'applique aux clients avec ou sans drapeau ***Nouveau client***.
Serveur principal (PAS) DANS (spécifier) – Si le nom du serveur principal contient/ne contient pas
GROUPES DANS (spécifier) – Si le client appartient au groupe...
GROUPES PAS DANS (spécifier) – Si le client n'appartient pas au groupe...
DOMAINE (PAS) DANS (spécifier) – Si le client appartient/n'appartient pas au domaine...
Nom d'ordinateur (spécifier) – Si le nom d'ordinateur est ...
Masque IP (spécifier) – Si le client appartient au groupe défini par l'adresse et le masque IP...
Plage IP (spécifier) – Si le client appartient au groupe défini par la plage IP...
(N') A (PAS) de stratégie définie (spécifier) – Si le client adopte (ou n'adopte pas) la stratégie...

Pour supprimer une règle de stratégie, dans la fenêtre Gestionnaire de stratégies, cliquez sur le bouton ***Supprimer***. Pour appliquer immédiatement toutes les règles, cliquez sur ***Exécuter les règles de stratégie maintenant***.

5.3.7 Suppression de stratégies

Comme la création de règle, une suppression n'est possible que pour des stratégies situées sur le serveur auquel vous êtes actuellement connecté. Pour supprimer des stratégies d'autres serveurs, vous devez vous y connecter directement avec ERAC.

REMARQUE : *Une stratégie peut être liée à d'autres serveurs ou stratégies (p. ex., stratégie parent, stratégie par défaut pour serveurs de niveau inférieur, stratégie par défaut pour clients principaux, etc.). C'est pourquoi, dans certains cas, il convient de la remplacer au lieu de supprimer. Pour voir les options de suppression et de remplacement, cliquez sur le bouton Supprimer la stratégie. Certains options décrites ci-dessous peuvent être indisponibles en fonction de la position de la stratégie concernée dans la hiérarchie des stratégies.*

Nouvelle stratégie pour les clients principaux dont la stratégie a été supprimée – Permet de sélectionner une nouvelle stratégie pour les clients principaux afin de remplacer celle que vous supprimez. Des clients principaux peuvent adopter la ***Stratégie par défaut pour les clients principaux***, ainsi que d'autres stratégies du même serveur (attribuées manuellement à l'aide de l'option ***Ajouter des clients***, ou forcées par des ***Règles de stratégie***). En remplacement, vous pouvez utiliser toute stratégie du serveur donné ou une stratégie répliquée.

Nouvelle stratégie parent pour les stratégies enfant (éventuelles) de la stratégie supprimée – Si une stratégie à supprimer faisait office de stratégie parent d'autres stratégies enfant, il convient également de la remplacer. Vous pouvez la remplacer par une stratégie de ce serveur, par une stratégie répliquée à partir de serveurs de niveau supérieur ou par le drapeau n.a. qui signifie qu'aucune stratégie de substitution ne sera attribuée aux stratégies enfant. Il est fortement recommandé d'attribuer une stratégie de substitution même s'il n'existe pas de stratégie enfant. Un autre utilisateur attribuant une stratégie enfant à cette stratégie durant le processus de suppression provoquerait un conflit.

Nouvelle stratégie pour les clients répliqués dont la stratégie a été supprimée ou modifiée – Vous pouvez sélectionner ici une nouvelle stratégie pour les clients répliqués à partir de serveurs de niveau inférieur (ceux appliqués à celle que vous supprimez actuellement). En remplacement, vous pouvez utiliser toute stratégie du serveur donné ou une stratégie répliquée.

Nouvelle stratégie par défaut pour les serveurs de niveau inférieur – Si la stratégie supprimée fait office de stratégie virtuelle (voir ***Paramètres de stratégie globale***), il convient de la remplacer par une autre (pour plus d'informations, voir la section 5.3.3, « Stratégies virtuelles »). En remplacement, vous pouvez utiliser toute stratégie du serveur donné ou le drapeau n.a.

Nouvelle stratégie par défaut pour les clients principaux – Si la stratégie supprimée fait office de stratégie virtuelle (voir ***Paramètres de stratégie globale***), il convient de la remplacer par une autre (pour plus d'informations, voir la section 5.3.3, « Stratégies virtuelles »). Vous pouvez utiliser une stratégie du même serveur en remplacement.

La même boîte de dialogue s'ouvre également si vous désactivez l'option ***Réplicable vers le bas*** pour une stratégie, puis cliquez sur ***OK***, ***Appliquer***, ou si vous sélectionnez une autre stratégie dans l'arborescence de stratégie. Cela active l'élément ***Nouvelle stratégie pour les clients répliqués dont la stratégie a été supprimée ou modifiée*** ou ***Stratégie par défaut pour les serveurs de niveau inférieur***.

5.3.8 Paramètres spéciaux

Les deux stratégies supplémentaires ne se trouvent pas dans le Gestionnaire de stratégies, mais dans ***Outils*** > ***Options du serveur*** > ***Autres paramètres*** > ***Modifier les paramètres avancés***) > ***Console ESET Remote Administrator*** > ***Serveur ERA*** > ***Configuration*** > ***Stratégies***.

Intervalle pour l'application de stratégie (minutes) :
Cette fonctionnalité s'applique aux stratégies dans l'intervalle spécifié. Il est recommandé de conserver le paramètre par défaut.

Désactiver l'utilisation de stratégie :
Activez cette option pour annuler l'application de stratégies aux serveurs. Il est recommandé d'utiliser cette option en cas de problème avec la stratégie. Pour éviter d'appliquer une stratégie à certains clients, une meilleure solution consiste à attribuer une stratégie vide.

5.3.9 Scénarios de déploiement de stratégie

5.3.9.1 Chaque serveur est une unité autonome et les stratégies sont définies localement

Dans le cadre de ce scénario, imaginons un petit réseau composé d'un serveur principal et de deux serveurs de niveau inférieur. Chaque serveur a plusieurs clients. Au moins une stratégie est créée sur chaque serveur. Les serveurs de niveau inférieur se trouvent dans les filiales de la société et tous les serveurs sont gérés par leur administrateur local. Chaque administrateur choisit les stratégies attribuées aux différents clients connectés à ses serveurs. L'administrateur principal n'intervient pas dans les configurations effectuées par les administrateurs locaux et n'attribue pas de stratégies aux clients de leurs serveurs. Dans la perspective d'une stratégie de serveur, cela signifie que le serveur A n'a pas de ***Stratégie par défaut pour les serveurs de niveau inférieur***. Cela signifie également que les serveurs B et C ont le drapeau n.a. ou une autre stratégie locale (outre la ***stratégie parent par défaut***) définie comme stratégie parent (p. ex., aucune stratégie parent n'est attribuée aux serveurs B et C à partir du serveur de niveau supérieur).

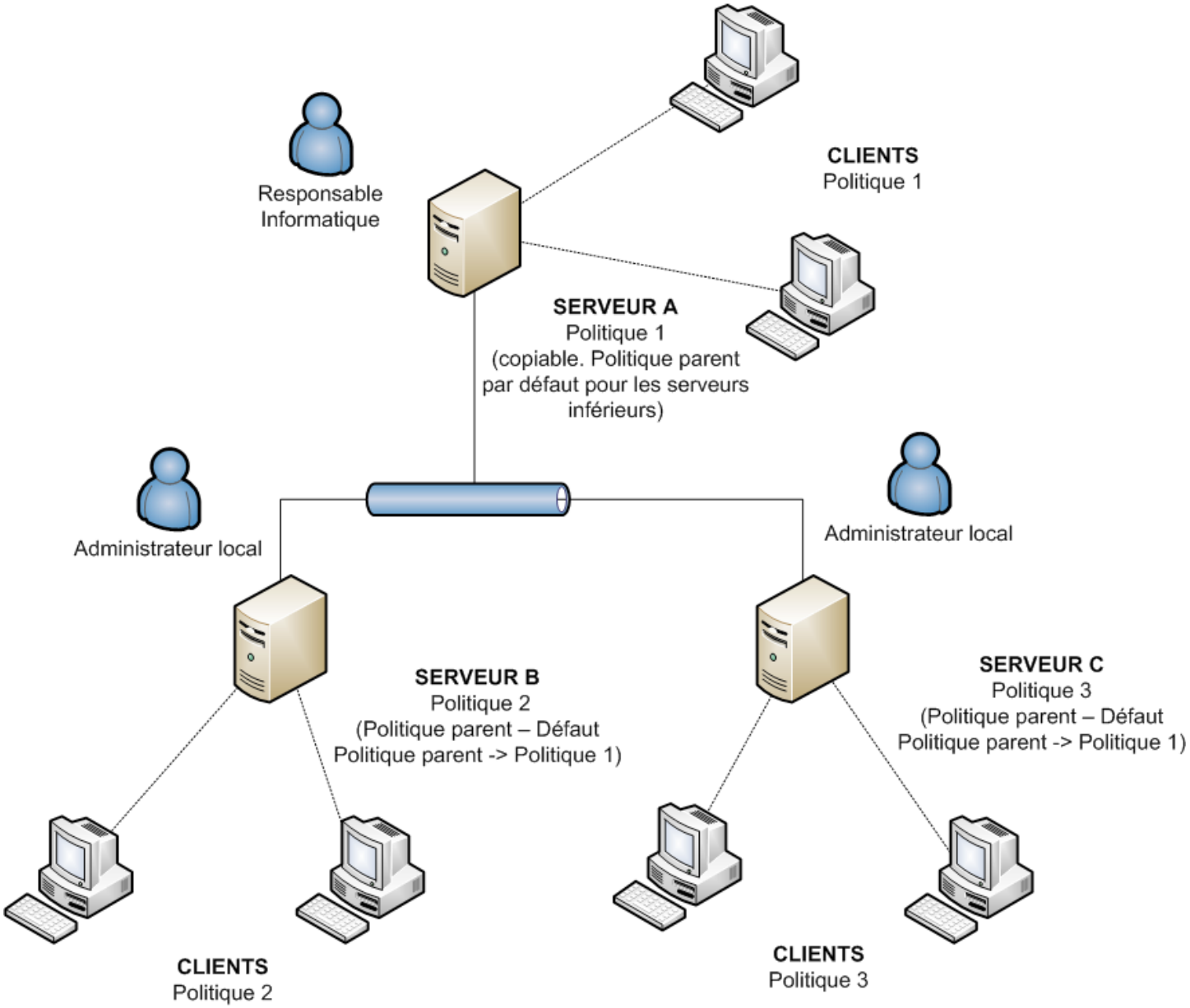


Figure 5-3

5.3.9.2 Chaque serveur est administré individuellement ; les stratégies sont gérées localement mais la stratégie parent par défaut est héritée du serveur de niveau supérieur

Tous les aspects mentionnés dans le scénario précédent s'appliquent également à ce scénario. Toutefois, l'option ***Stratégie par défaut pour les serveurs de niveau inférieur*** est activée sur le serveur A et les stratégies sur les serveurs de niveau inférieur héritent de la configuration de la ***stratégie parent par défaut*** du serveur maître. Dans ce scénario, les administrateurs locaux disposent d'une grande autonomie pour la configuration des stratégies. Si les ***stratégies enfant*** sur les serveurs de niveau inférieur peuvent hériter de la ***stratégie parent par défaut***, les administrateurs locaux ont la possibilité de la modifier à l'aide de leurs propres stratégies.

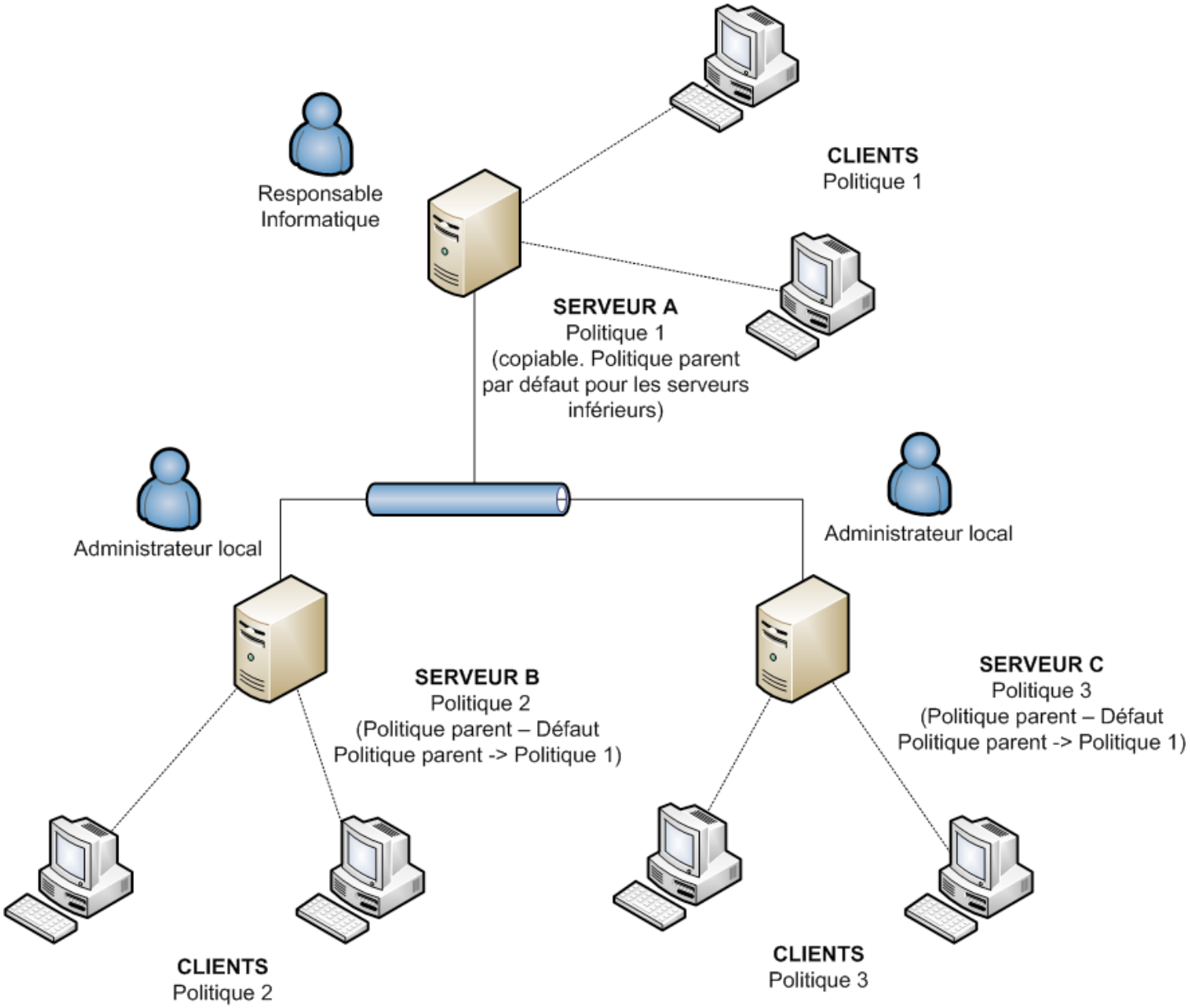


Figure 5-4

5.3.9.3 Héritage de stratégies d'un serveur de niveau supérieur

Le modèle de réseau pour ce scénario est le même que celui des deux scénarios précédents. En outre, le serveur maître, outre la ***stratégie parent par défaut***, contient d'autres stratégies réplicables vers le bas qui font office de stratégies parent sur les serveurs de niveau inférieur. Pour la stratégie 1 (voir la figure 5-5), l'attribut ***Remplacer toute stratégie enfant*** est activé. L'administrateur local dispose encore d'une certaine autonomie, mais l'administrateur principal définit les stratégies répliquées vers le bas, la méthode de réplication et celles qui font office de stratégies parent pour les stratégies locales. L'attribut ***Remplacer...*** indique que les configurations définies dans les stratégies sélectionnées remplacent celles définies sur les serveurs locaux.

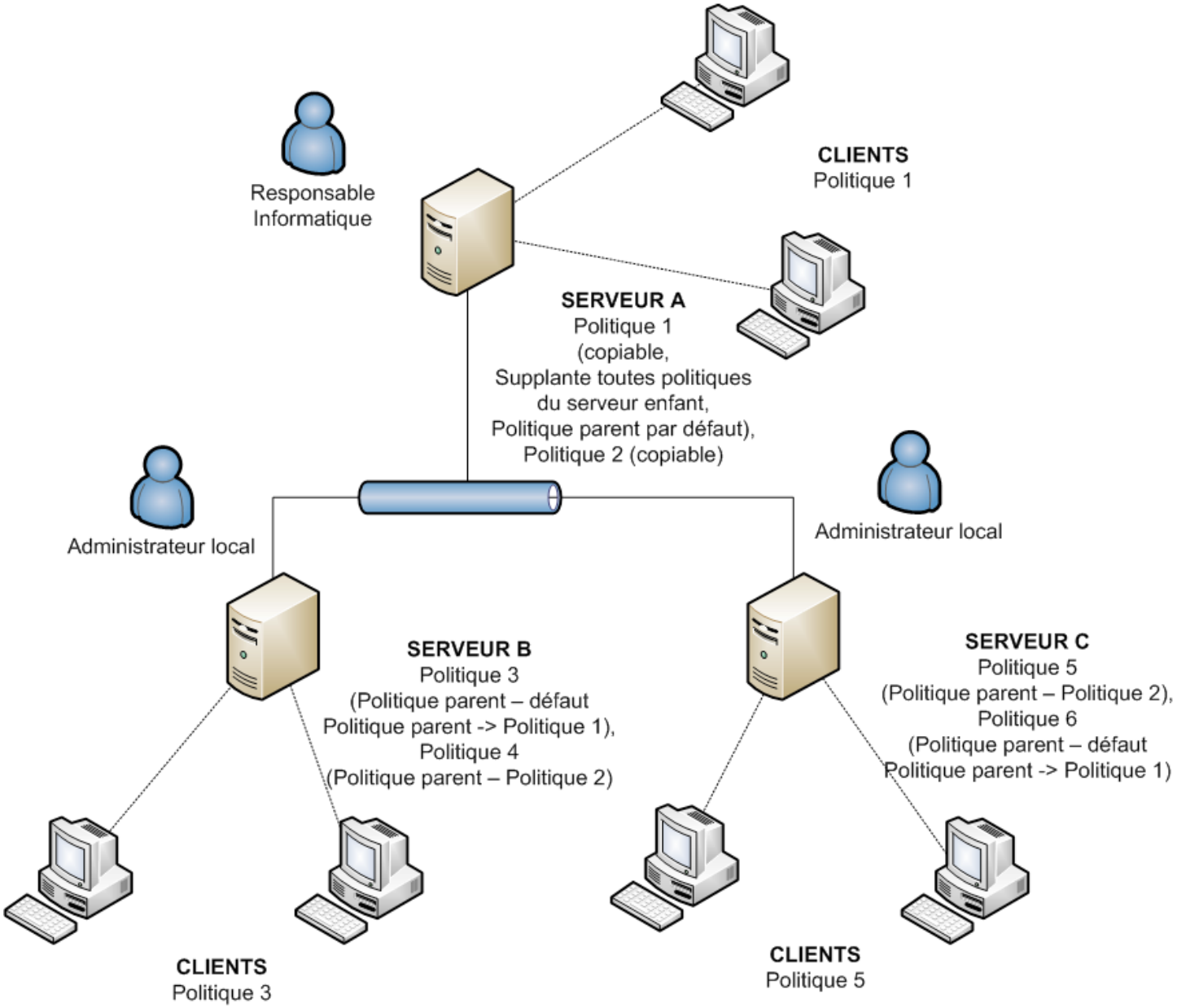


Figure 5-5

5.3.9.4 Attribution de stratégies uniquement à partir du serveur de niveau supérieur

Ce scénario représente un système centralisé de gestion des stratégies. Les stratégies destinées aux clients ne sont créées, modifiées et attribuées que sur le serveur principal ; l'administrateur local n'est pas autorisé à les modifier. Les serveurs de niveau inférieur n'ont qu'une stratégie de base qui est vide (nommée par défaut ***Stratégie du serveur***) et fait office de ***Stratégie parent par défaut pour les clients principaux***.

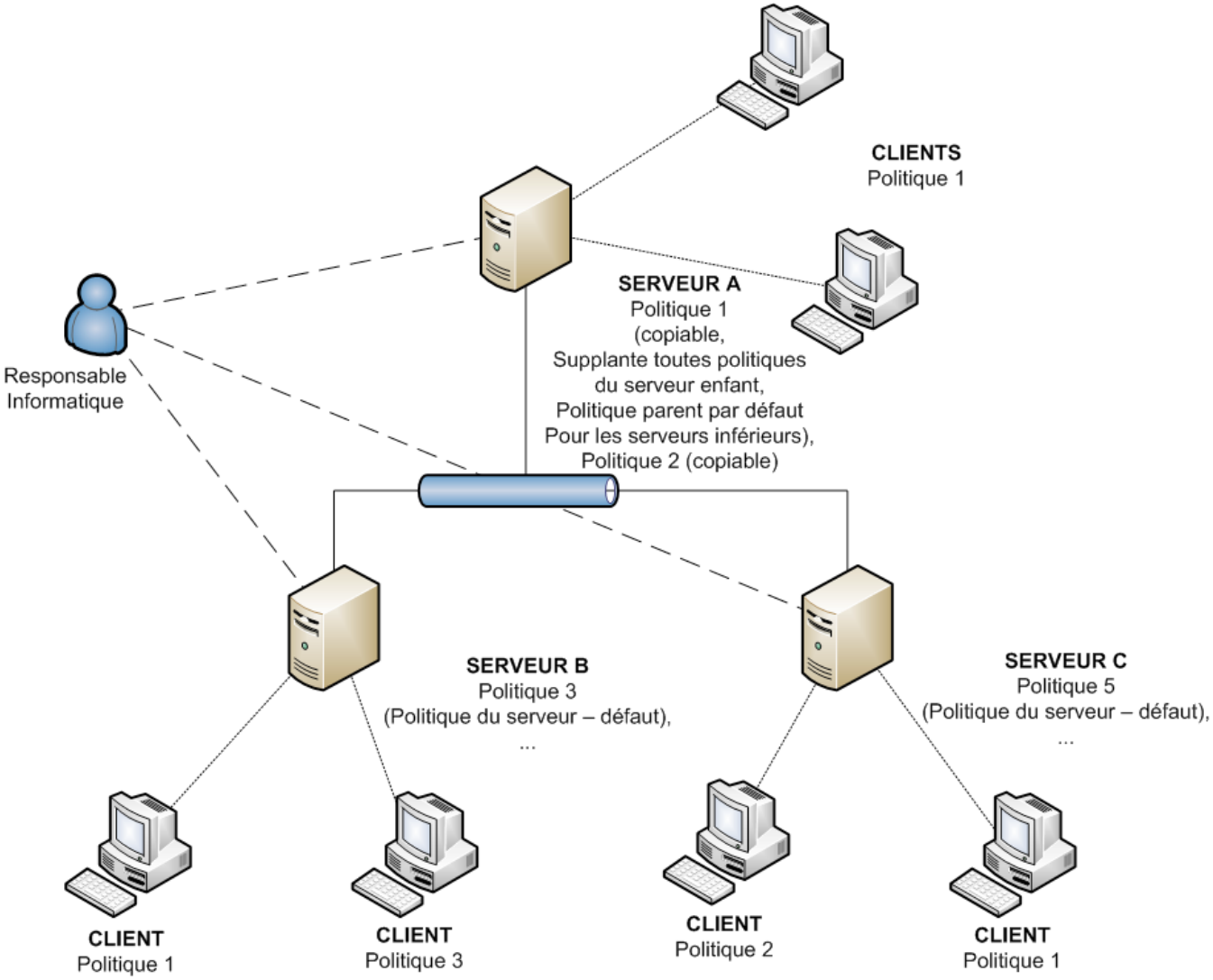


Figure 5-6

5.3.9.5 Utilisation de règles de stratégie

Notre exemple suivant inclut l'attribution automatique de stratégies basées sur des règles de stratégie. Cette méthode est complémentaire et doit être utilisée en combinaison avec les scénarios décrits précédemment, plutôt qu'en tant que scénario autonome.

Si chaque serveur est géré par un administrateur local, chaque administrateur peut créer des règles de stratégie individuelles pour ses clients. Dans ce scénario, il est important qu'il n'y ait aucun conflit entre les règles de stratégie, comme lorsque le serveur de niveau supérieur attribue une stratégie aux clients en fonction de règles de stratégie, tandis que le serveur de niveau inférieur attribue des stratégies distinctes sur la base de règles de stratégie locale.

En définitive, un système centralisé réduit considérablement la probabilité de conflits, car tout le processus de gestion a lieu sur le serveur principal.

5.3.9.6 Utilisation de groupes locaux

Dans certains cas, l'attribution de stratégies à des groupes de clients peut compléter les scénarios précédents. Vous pouvez créer des groupes manuellement ou à l'aide de l'option ***Synchroniser avec Active Directory*** (voir la section 5.2. « Groupes »). Pour ce faire, vous pouvez utiliser l'option d'attribution isolée (***Ajouter des clients*** > ***Ajout spécial***), ou fournir des stratégies automatiquement à l'aide de ***règles de stratégie***.

5.4 Notifications

La capacité de notifier aux administrateurs système et réseau des événements importants constitue un aspect essentiel de la sécurité et de l'intégrité du réseau. Un avertissement précoce concernant une erreur ou un code malveillant permet d'éviter les énormes pertes de temps et d'argent liées à l'élimination du problème ultérieurement. Les sections ci-après décrivent les options de notification d'ERA.

5.4.1 Gestionnaire de notifications

Pour ouvrir la fenêtre principale du Gestionnaire de notifications, cliquez sur ***Outils*** > ***Gestionnaire de notifications***.

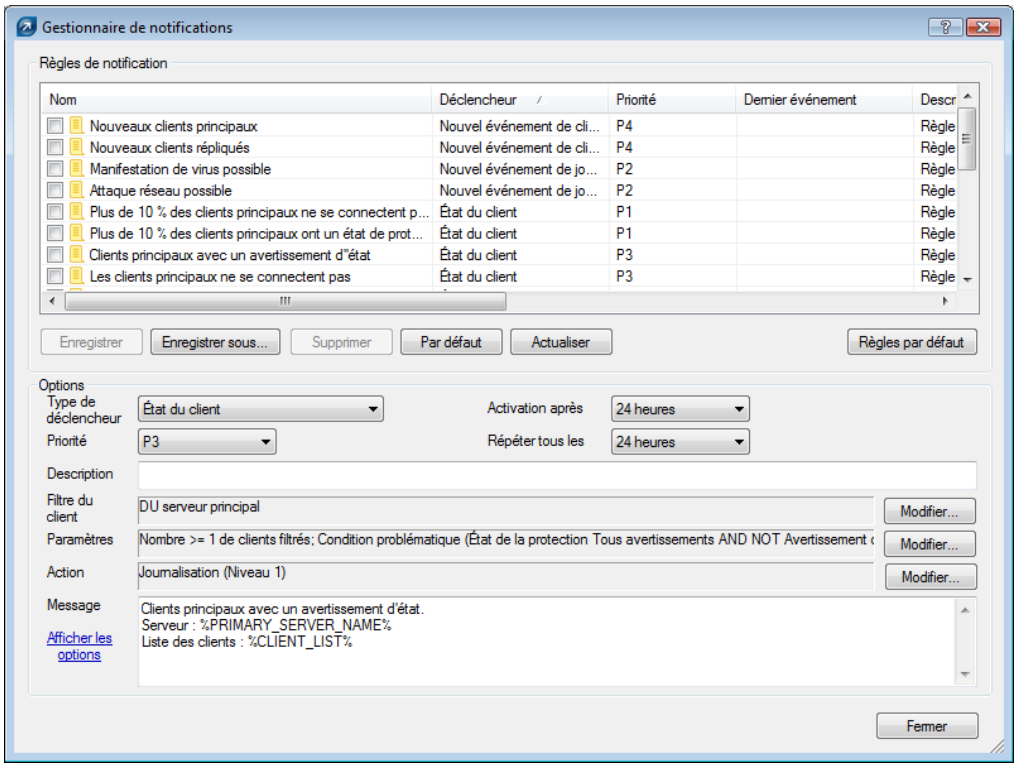


Figure 5-7 : Fenêtre Gestionnaire de notifications

La fenêtre principale comprend deux sections. La section Règles de notification dans la partie supérieure de la fenêtre contient la liste des règles existantes (prédéfinies ou définies par l'utilisateur). Vous devez sélectionner une règle dans cette section pour générer des messages de notification. Par défaut, aucune notification n'est activée. Il est donc recommandé de vérifier si les règles sont actives.

Les boutons fonctionnels sous la liste de règles sont les suivants : ***Enregistrer*** (enregistrer les modifications apportées à une règle), ***Enregistrer sous***...(enregistrer les modifications apportées à une règle sous un nouveau nom), ***Supprimer***, ***Par défaut*** (restaurer les paramètres par défaut d'une règle) et ***Actualiser*** (mettre à jour la liste avec les règles par défaut).

La section **Options** dans la moitié inférieure de la fenêtre fournit des informations sur la règle actuellement sélectionnée. L'ensemble des champs et options de cette section sont décrits à l'aide de l'exemple de règle de la section 5.4.2, « Création de règle ».

Dans chaque règle, vous pouvez spécifier les critères qui l'activent, également appelés déclencheurs.
Les déclencheurs suivants sont disponibles :

- ***État du client*** – La règle s'exécute en cas de problème sur certains clients
- ***État du serveur*** – La règle s'exécute en cas de problème sur certains serveurs
- ***Événement de tâche terminée*** – La règle s'exécute lorsque la tâche spécifiée est terminée
- ***Événement de nouveau client*** – La règle s'exécute si un nouveau client (y compris un client répliqué) se connecte au serveur
- ***Nouvel événement de journal*** – La règle s'exécute si l'événement spécifique figure dans certains journaux

En fonction du type de déclencheur, il est possible d'activer ou de désactiver d'autres options de règle. C'est pourquoi il est recommandé de commencer par créer des déclencheurs lors de la création de règles.

Le menu déroulant ***Priorité*** permet de définir la priorité de la règle. ***P1*** est la priorité la plus haute et ***P5*** la priorité la plus basse. La priorité n'affecte en rien la fonctionnalité des règles. Pour affecter une priorité aux messages de notification, vous pouvez utiliser la variable %PRIORITY%. Le menu ***Priorité*** contient un champ ***Description***. Il est recommandé d'attribuer à chaque règle une description compréhensible, telle que « règle avertissant sur les infiltrations détectées ».

Dès que le système détecte l'événement déclencheur pour un ou plusieurs clients donnés et trouve une règle à exécuter, il applique le filtre du client. Le filtre peut être attribué à toute règle impliquant des clients. Pour accéder à la configuration du filtre du client, dans la section ***Filtre du client***, cliquez sur ***Modifier***. Dans la fenêtre qui s'ouvre, définissez les paramètres de filtrage des clients. Lors de l'application d'une règle, seuls les clients répondant aux critères de filtre sont pris en considération. Les critères de filtrage sont les suivants :

- ***DU serveur principal*** – Uniquement les clients du serveur principal (il est également possible d'appliquer la forme négative PAS DU)
- ***Serveur principal DANS*** – Inclut le serveur principal dans le résultat
- ***A un nouveau drapeau*** – Clients marqués du drapeau « Nouveau » (il est également possible d'appliquer forme négative ***N'A PAS***)
- ***Groupe ERA IN*** – Clients appartenant au groupe spécifié
- ***Domaine/Groupe de travail DANS*** – Clients appartenant au domaine spécifié.
- ***Masque de nom d'ordinateur*** – Clients portant le nom d'ordinateur spécifié
- ***Masque IP*** – Clients correspondant au masque IP spécifié.
- ***Plage IP*** – Clients s'inscrivant dans la plage d'adresses IP spécifiée
- ***A défini une stratégie –*** Clients auxquels est attribuée la stratégie spécifiée (il est également possible d'appliquer la forme négative ***N'A PAS***).

Après avoir défini un filtre du client pour votre règle de notification, cliquez sur OK, puis passez aux paramètres de la règle. Les paramètres du client définissent la condition qu'un client ou un groupe de clients doit remplir pour exécuter l'action de notification. Pour afficher les paramètres disponibles, dans la section ***Paramètres***, cliquez sur le bouton ***Modifier...***

La disponibilité des paramètres dépend du type de déclencheur sélectionné. Vous trouverez ci-dessous la liste complète des paramètres disponibles par type de déclencheur.

Les paramètres suivants sont disponibles pour les déclencheurs État du client :

- ***Nombre –*** Pourcentage total de clients requis pour activer la règle.
- ***État de la protection Tous avertissements*** – Tout avertissement détecté dans la colonne État de la protection
- ***État de la protection Avertissements critiques*** – Avertissement critique détecté dans la colonne État de la protection
- ***Version de BdD de signatures de virus*** – Problème avec la base des signatures de virus (3 valeurs possibles)
  - ***Précédente*** – La base des signatures de virus est d'une version antérieure à celle présente sur le serveur.
  - ***Plus ancienne ou n.a.*** – La base des signatures de virus est antérieure de plusieurs versions à celle présente sur le serveur
  - ***Plus récente*** – La base des signatures de virus est postérieure à celle présente sur le serveur.
- ***Dernier avertissement de connexion*** – La dernière connexion a été établie avant la période spécifiée
- ***A un dernier événement de menace*** – La colonne Menace contient un avertissement de menace
- ***A un dernier événement –*** La colonne Dernier événement contient une entrée
- ***A un dernier événement de pare-feu*** – La colonne Événement de pare-feu contient une entrée d'événement de pare-feu
- ***A un nouveau drapeau*** – Le client a le drapeau « Nouveau »
- ***En attente de redémarrage*** – Le client attend un redémarrage
- ***Dernière menace trouvée par analyse*** – Sur le client, le nombre spécifié de menaces ont été détectées lors de la dernière analyse
- ***Dernière menace non nettoyée par analyse*** – Sur le client, le nombre spécifié de menaces non nettoyées ont été détectées lors de la dernière analyse

Tous les paramètres peuvent être formulés de façon négative, mais les négations ne sont pas toutes utilisables. Il convient de ne nier que les paramètres incluant deux valeurs logiques : vrai ou non vrai. Par exemple, le paramètre ***A un nouveau drapeau*** ne couvre que les clients marqués à l'aide du drapeau « nouveau ». Le paramètre négatif inclut donc tous les clients non marqués à l'aide de ce drapeau.

Toutes les conditions ci-dessus peuvent être combinées et inversées de façon logique. Le menu déroulant pour ***La règle est appliquée quand*** offre deux choix :

- ***Toutes les options sont vérifiées –*** La règle ne s'exécute que si **tous** les paramètres spécifiés sont vrais
- ***Une ou plusieurs options sont vérifiées –*** La règle s'exécute si au moins **une** condition est vraie

Les paramètres suivants sont disponibles pour les déclencheurs État du serveur :

- ***Serveur mis à jour –*** Le serveur est à jour
- ***Serveur non mis à jour*** – Le serveur n'est plus à jour depuis un temps supérieur à la valeur spécifiée
- ***Journaux du serveur*** – Le journal du serveur contient les trois types d'entrées suivants :
  - ***Erreurs*** – Messages d'erreur.
  - ***Erreurs + Avertissements*** – Messages d'erreur et d'avertissement
  - ***Filtrer les entrées de journal par type*** – Activez cette option pour spécifier des entrées d'erreur et d'avertissement à observer dans le journal du serveur. Notez que, pour que les notifications fonctionnent correctement, le niveau de détails du journal (***Outils > Options du serveur > Journalisation***) doit être correctement défini. Autrement, de telles règles de notification ne trouvent jamais de déclencheur dans le journal du serveur. Les entrées de journal suivantes sont disponibles :
    - ***ADSI_SYNCHRONIZE*** – Synchronisation de groupe Active Directory
    - ***CLEANUP*** – Tâches de nettoyage du serveur
    - ***CREATEREPORT*** – Génération de rapport à la demande.
    - ***DEINIT*** – Arrêt du serveur
    - ***INIT*** – Démarrage du serveur
    - ***INTERNAL*** – Message de serveur interne
    - ***LICENSE*** – Administration de licence
    - ***MAINTENANCE*** – Tâches de maintenance du serveur
    - ***NOTIFICATION*** – Gestion des notifications
    - ***PUSHINST*** – Installation poussée
    - ***RENAME*** – Changement du nom de structure interne
    - ***REPLICATION –*** Réplication du serveur
    - ***POLICY*** – Gestion des stratégies
    - ***POLICYRULES*** – Règles de stratégie
    - ***SCHEDREPORT*** – Rapports générés automatiquement
    - ***SERVERMGR*** – Gestion des menaces du serveur interne
    - ***SESSION*** – Connexions réseau du serveur
    - ***THREATSENSE*** – ThreatSense. NET – Soumission d'informations statistiques
    - ***UPDATER*** – Mise à jour du serveur et création de miroir

Un exemple de paramètre utile est UPDATER, qui envoie un message de notification quand le Gestionnaire de notifications détecte un problème lié à une mise à jour et à une création de miroir dans les journaux du serveur.

- ***Expiration de licence*** – La licence expirera dans le nombre de jours spécifié ou a déjà expiré. Activez l'option ***N'avertir que si cela entraîne une chute du nombre de clients sous licence au-dessous du nombre de clients réels dans la base de données du serveur*** pour envoyer une notification si l'expiration entraîne la chute du nombre clients sous licence au-dessous du nombre des clients actuellement connectés.
- ***Limiter la licence*** – Si le pourcentage de clients disponibles chute sous la valeur spécifiée

Les paramètres suivants sont disponibles pour les déclencheurs ***Nouvel événement de journal*** :

- ***Type de journal*** – Sélectionnez ***Journal des événements***, ***Journal des menaces*** ou ***Journal de pare-feu***
- ***Niveau de journalisation*** – Niveau d'entrée de journal dans le journal donné
  - ***Niveau 1*** – ***Avertissements critiques*** Erreurs critiques uniquement.
  - ***Niveau 2*** – ***Supérieur + Avertissements*** – Identique au niveau 1, plus notifications d'alerte.
  - ***Niveau 3*** – ***Supérieur + Normal*** – Identique au niveau 2, plus notifications informatives.
  - ***Niveau 4*** – ***Supérieur + Diagnostic*** – Identique au niveau 3, plus notifications de diagnostic.

- ***1000* occurrences en *60 minutes*** – Tapez le nombre d'occurrences, puis sélectionnez la période de temps pour spécifier la fréquence d'événements à atteindre pour que la notification soit envoyée. La fréquence par défaut est de 1000 occurrences par heure.
- ***Nombre*** – Nombre de clients (exprimé en valeur absolue ou en pour cent)

Les autres **types de déclencheurs** n'ont pas de paramètres spécifiques.

Si les paramètres spécifiés pour une règle se vérifient, l'action correspondante définie par l'administrateur est automatiquement exécutée. Pour configurer des actions, dans la section ***Actions***, cliquez sur ***Modifier...*** L'éditeur d'action offre les options suivantes :

- ***Email*** – Le programme envoie le texte de notification de la règle à l'adresse de messagerie spécifiée. Le champ **Objet** permet de spécifier l'objet du message. Cliquez sur **À** pour ouvrir le carnet d'adresses.
- ***Interruption SNMP*** – Génère et envoie une notification SNMP
- ***Exécuter (sur le serveur)*** – Activez cette option et spécifiez l'application à exécuter sur le serveur
- ***Journaliser dans un fichier*** – Génère des entrées de journal dans le fichier journal spécifié. Le niveau de ***Détails*** de ce journal est configurable.
- ***Journalisation*** – Enregistre les notifications dans les journaux du serveur. Le niveau de ***Détails*** des notifications est configurable.

Pour que cette fonctionnalité opère correctement, vous devez activer la journalisation dans le serveur ERA (**Outils > Options du serveur > Journalisation**).

Vous pouvez modifier le format de notification à l'aide du champ ***Message*** dans la section inférieure de la fenêtre principale du Gestionnaire de notifications. Dans le texte, vous pouvez utiliser des variables spéciales à l'aide de la syntaxe suivante : *%VARIABLE_NAME %*. Pour afficher la liste des variables disponibles, cliquez sur ***Afficher les options***.

- ***Server_Last_Updated*** – Dernière mise à jour du serveur
- ***Primary_Server_Name***
- ***Rule_Name***
- ***Rule_Description***
- ***Client_Filter*** – Paramètres de filtre du client
- ***Client_Filter_Short*** – Paramètres de filtre du client (sous forme abrégée)
- ***Client_List*** – Liste de clients
- ***Triggered*** – Date d'envoi de la dernière notification (répétitions exclues)
- ***Triggered Last*** – Date d'envoi de la dernière notification (répétitions inclues)
- ***Priority*** – Priorité de la règle de notification
- ***Log_Text_Truncated*** – Texte de journal ayant activé la notification (tronqué)
- ***Task_Result_List*** – Liste des tâches accomplies
- ***Parameters*** – Paramètres de la règle
- ***Last_Log_Date*** – Date du dernier journal
- ***License_Info_Merged*** – Informations de licence (résumé)
- ***License_Info_Full*** – Informations de licence (complètes)
- ***License_Days_To_Expiry*** – Jours restants avant l'expiration
- ***License_Clients_Left*** – Clients pouvant encore se connecter au serveur selon les termes de la licence actuelle
- ***Actual_License_Count*** – Nombre de clients actuellement connectés au serveur

Les derniers paramètres à spécifier sont l'heure et la date. Il est possible de retarder l'activation de la règle pendant une période comprise entre une heure et trois mois. Si vous voulez activer la règle le plus rapidement possible, dans le menu déroulant ***Activation après***, sélectionnez ***Dès que possible***. Par défaut, le Gestionnaire de notifications est activé toutes les 10 minutes. Ainsi, si vous sélectionnez **Dès que possible**, la tâche doit s'exécuter dans les 10 minutes. Si une période spécifique est sélectionnée dans ce menu, l'action est automatiquement exécutée à l'issue de celle-ci (pour autant que la condition de la règle se vérifie).

Le menu ***Répéter tous les...*** permet de spécifier un intervalle de temps à l'issue duquel l'action est répétée. Toutefois, la condition d'activation de la règle doit toujours être remplie. Dans ***Serveur > Autres paramètres > Modifier les paramètres avancés > Console ESET Remote Administrator > Serveur > Configuration > Notifications > Intervalle***

pour le traitement de notification (minutes), vous pouvez spécifier l'intervalle de temps pendant lequel le serveur contrôle et exécute les règles actives.

La valeur par défaut est 10 minutes. Il n'est pas recommandé de la réduire, car cela peut entraîner un ralentissement sensible du serveur.

Par défaut, la fenêtre Gestionnaire de notifications contient des règles prédéfinies. Pour activer une règle, sélectionnez la case à cocher située à côté. Les règles de notification suivantes sont disponibles. Si elles sont activées et que leurs conditions d'application sont remplies, elles génèrent des entrées de journal.

- ***Plus de 10 % des clients principaux ne se connectent pas*** – Si plus de 10 pour cent des clients ne se sont pas connectés au serveur depuis plus d'une semaine. La règle s'exécute dès que possible.
- ***Plus de 10 % des clients principaux ont un état de protection critique*** – Si plus de 10 pour cent des clients ont généré un avertissement critique sur l'état de la protection et qu'aucun d'eux ne s'est connecté au serveur depuis plus d'une semaine. La règle s'exécute dès que possible.
- ***Clients principaux avec un avertissement d'état*** – S'il y a au moins un client avec un avertissement d'état de protection qui ne s'est pas connecté au serveur depuis au moins une semaine
- ***Les clients principaux ne se connectent pas*** – S'il y a au moins un client qui ne s'est pas connecté au serveur depuis plus d'une semaine
- ***Client principaux dont la base des signatures de virus est obsolète*** – S'il y a un client avec une base des signatures de virus antérieure d'au moins deux versions à la base actuelle, qui ne s'est pas déconnecté du serveur depuis plus d'une semaine
- ***Clients principaux dont l'état de protection est critique*** – S'il y a un client avec un avertissement critique sur l'état de la protection qui ne s'est pas déconnecté depuis plus d'une semaine
- ***Clients principaux avec une base des signatures de virus plus récente que celle du serveur*** – S'il y a un client avec une base des signatures de virus plus récente que celle du serveur, qui ne s'est pas déconnecté depuis plus d'une semaine
- ***Clients principaux en attente de démarrage*** – S'il y a un client en attente de redémarrage qui ne s'est pas déconnecté depuis plus d'une semaine
- ***Une analyse de l'ordinateur révèle l'existence de clients principaux avec une infiltration non nettoyée*** – S'il y a un client sur lequel l'analyse de l'ordinateur n'a pas pu nettoyer au moins une infiltration et que le client ne s'est pas déconnecté depuis plus d'une semaine. La règle s'exécute dès que possible.
- ***Tâche accomplie*** – Si une tâche a été accomplie sur un client. La règle s'exécute dès que possible.
- ***Nouveaux clients principaux*** – Si un nouveau client s'est connecté au serveur. La règle s'exécute dès que possible.
- ***Nouveaux clients répliqués*** – Si un nouveau client répliqué figure dans la liste des clients. La règle s'exécute après une heure.
- Entrées de journal ***Manifestation de virus possible***.
- ***Attaque réseau possible*** – Si la fréquence d'entrées de journal du pare-feu personnel d'ESET sur tous les clients a dépassé 1000 avertissements critiques en une heure.
- ***Serveur mis à jour –*** Si le serveur a été mis à jour.
- ***Serveur non mis à jour*** – Si le serveur n'a pas été mis à jour depuis plus de cinq jours. La règle s'exécute dès que possible.
- ***Erreur dans le journal de texte du serveur*** – Si le journal du serveur contient une entrée d'erreur.
- ***Expiration de licence*** – Si la licence actuelle expire dans 20 jours et si, après expiration, le nombre maximal de clients disponibles sera inférieur au nombre actuel de clients. La règle s'exécute dès que possible.
- ***Limite de la licence*** – Si le nombre de clients disponibles chute sous 10 %.

Sauf spécification contraire, toutes les règles sont exécutées et répétées après 24 heures, et appliquées au serveur et aux clients principaux.

5.4.1.1 Notifications via interruption SNMP

SNMP (Simple Network Management protocol) est un protocole de gestion simple et largement répandu, approprié pour la surveillance et l'identification de problèmes réseau. L'une des opérations de ce protocole est l'interruption (TRAP) qui envoie des données spécifiques. ERA utilise une interruption pour envoyer des messages de notification.

Pour que l'outil d'interruption fonctionne efficacement, le protocole SNMP doit être correctement installé et configuré sur le même ordinateur qu'ERAS (***Démarrer > Panneau de configuration > Ajout ou suppression de programmes > Ajouter ou supprimer des composants Windows***). Le service SNMP doit être configuré de la manière décrite dans cet article : http://support.microsoft.com/kb/315154. Dans ERAS, vous devez activer une règle de notification SNMP.

Il est possible d'afficher des notifications dans le gestionnaire SNMP qui doit être connecté à un serveur SNMP sur lequel le fichier de configuration eset_ras.mib est importé. Le fichier est un composant standard d'une installation ERA et se trouve généralement dans le dossier C:\Program Files\ESET\ESET Remote Administrator\Server\snmp\.

5.4.2 Création de règle

Les étapes suivantes montrent comment créer une règle qui envoie une notification électronique à l'administrateur en cas de problème d'état de protection de stations de travail client. La notification sera également enregistrée dans un fichier nommé log.txt.

1) Dans le menu déroulant ***Type de déclencheur***, sélectionnez ***État du client***

2) Conservez les valeurs prédéfinies des options ***Priorité, Activation après*** et ***Répéter tous les***. La règle recevra automatiquement la priorité 3 et sera activée après 24 heures.

3) Dans le champ ***Description***, tapez **notification d'état de la protection pour les clients du siège**.

4) Cliquez sur ***Modifier...*** dans la section **Filtre du client** et n'activez que la condition de règle ***Groupes DANS***. Dans la partie inférieure de cette fenêtre, cliquez sur le lien ***spécifier***, puis, dans la nouvelle fenêtre, tapez ***Siège***. Cliquez sur ***Ajouter***, puis deux fois sur ***OK*** pour confirmer. Cela indique que la règle ne s'applique qu'aux clients du groupe Siège.

5) Spécifiez davantage les paramètres pour la règle dans ***Paramètres*** > ***Modifier...***. Désactivez toutes les options sauf ***État de la protection Tous avertissements***.

6) Accédez à la section ***Action***, puis cliquez sur le bouton ***Modifier...***. Dans la fenêtre **Action**, activez ***Email***, spécifiez les destinataires (***À...***) puis l'**Objet** de l'Email. Activez ensuite la case à cocher ***Journaliser dans un fichier***, puis entrez le nom et le chemin d'accès du fichier journal à créer. Vous avez la possibilité de sélectionner le niveau ***Détails*** du fichier journal. Cliquez sur **OK** pour enregistrer l'action.

7) Enfin, utilisez la zone de texte **Message** pour spécifier le contenu du corps du message électronique qui sera envoyé une fois la règle activée. Exemple : « Le client %CLIENT_LIST % signale un problème d'état de la protection ».

8) Cliquez sur ***Enregistrer sous...*** pour nommer la règle, p. ex., « problèmes d'état de la protection », puis sélectionnez la règle dans la liste des règles de notification.

La règle terminée devrait ressembler à celle présentée à la figure 5-8 :

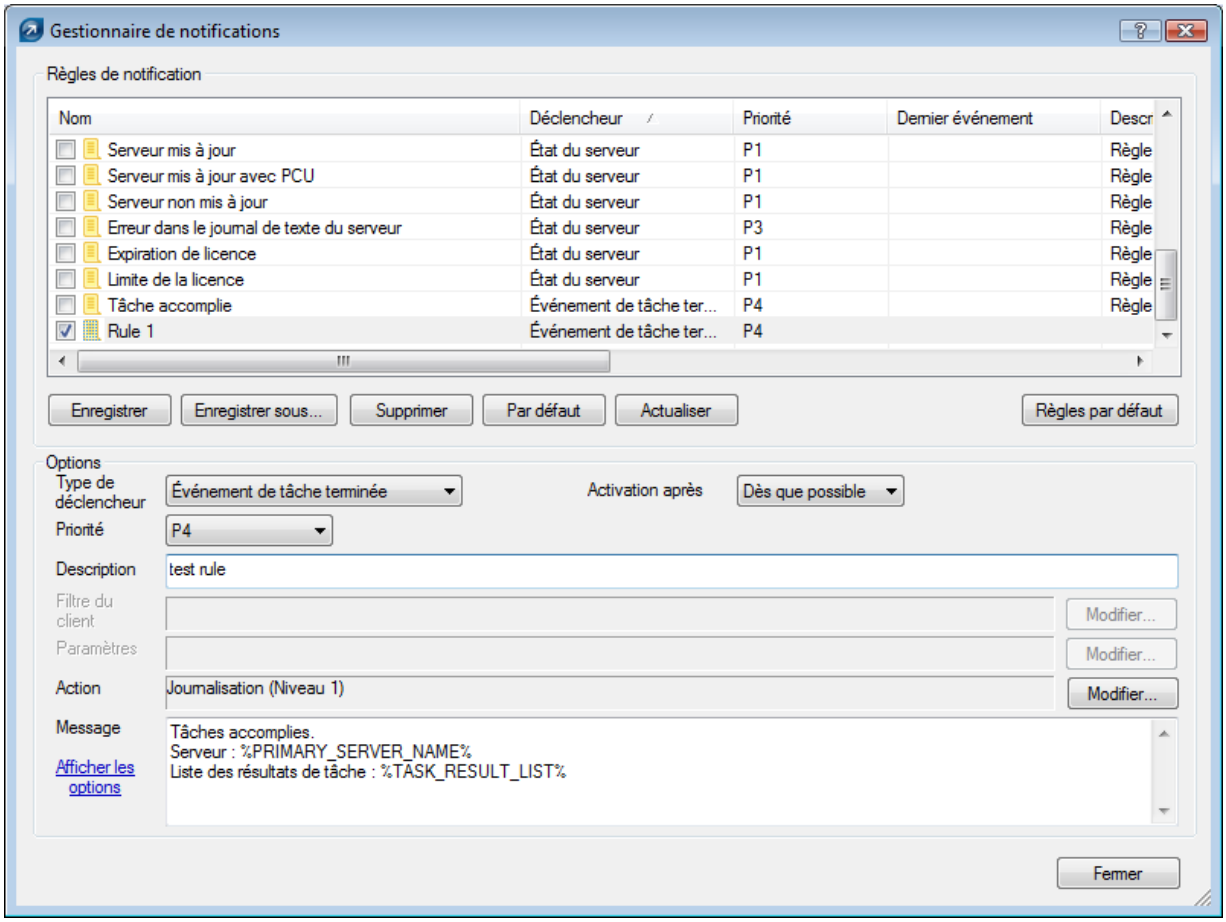


Figure 5-8 Exemple de règle de notification

La règle est désormais active. En cas de problème avec l'état de la protection sur un client du groupe Siège, la règle sera exécutée. L'administrateur recevra une notification électronique avec une pièce jointe contenant le nom du client problématique. Pour quitter le Gestionnaire de notifications, cliquez sur **Fermer**.

5.5 Informations détaillées de clients

ERA permet d'extraire des stations de travail client des informations sur les processus en cours d'exécution, les programmes de démarrage, etc. Ces informations peuvent être extraites à l'aide de l'outil ESET SysInspector intégré dans ERAS. Tout comme d'autres fonctions utiles, ESET SysInspector examine en profondeur le système d'exploitation et crée des journaux système. Pour l'ouvrir, dans le menu principal d'ERAC, cliquez sur ***Outils > ESET SysInspector***.

En cas de problèmes avec un client spécifique, vous pouvez demander son journal ESET SysInspector. Pour ce faire, dans le volet ***Clients***, cliquez avec le bouton droit sur le client, puis sélectionnez ***Demander des données*** – ***Demander les informations de SysInspector***. Il n'est possible d'obtenir des journaux que de produits à partir de la génération 4.x ; les versions antérieures ne prennent pas en charge cette fonctionnalité. Cliquez sur le lien **demande de journal** pour ouvrir une nouvelle fenêtre contenant les options suivantes :

- ***Créer un instantané (mémoriser le journal obtenu également sur le client)*** – Enregistre une copie du journal sur l'ordinateur client.

- ***Inclure une comparaison au dernier instantané avant l'heure spécifiée*** – Affiche un journal comparatif. Un journal comparatif est créé par fusion du journal actuel avec un journal précédent éventuellement disponible. ERA choisit le premier journal antérieur à la date spécifiée.

Cliquez sur ***OK*** pour obtenir les journaux sélectionnés et les enregistrer sur le serveur. Pour ouvrir et afficher les journaux procédez comme suit.

Les options d'ESET SysInspector pour des stations de travail client individuelles figurent sous l'onglet ***Propriétés du client*** – ***SysInspector***. La fenêtre est divisée en trois sections. La section supérieure présente des informations de texte sur les journaux les plus récents du client donné. Cliquez sur ***Actualiser*** pour charger les informations les plus récentes.

La section médiane de la fenêtre ***Options de demande*** est presque identique à la fenêtre qui s'affiche dans le processus de demande de journaux de stations de travail client décrit ci-avant. Le bouton ***Demande*** permet d'obtenir un journal ESET SysInspector du client.

La section inférieure comprend les boutons suivants :

- ***Affichage –*** Ouvre le journal indiqué dans la section supérieure directement dans ESET SysInspector

- ***Enregistrer sous...*** – Enregistre le journal actuel dans un fichier. L'option ***Puis exécuter la visionneuse d'ESET SysInspector pour afficher le fichier*** ouvre automatiquement le journal après son enregistrement (comme si vous cliquiez sur ***Affichage***).

La génération et l'affichage de nouveaux fichiers journaux sont parfois ralentis par le client local en raison de la taille du journal et de la vitesse de transfert de données. La date et l'heure affectées à un journal dans ***Propriétés du client*** > ***SysInspector*** sont la date et l'heure de remise au serveur.

6. Rapports

L'onglet Rapports (Outils > Volet Rapports) permet de convertir des informations statistiques en graphiques ou diagrammes. Vous pouvez enregistrer ces derniers au format .csv (valeurs séparées par des virgules) afin de les traiter ultérieurement à l'aide des outils ERA pour produire des graphiques et des sorties graphiques. Par défaut, ERA enregistre la sortie au format HTML. La plupart des rapports relatifs aux infiltrations sont générés à partir du journal des menaces.

Pour rechercher et sélectionner des styles graphiques, utilisez le menu déroulant ***Style*** de la section ***Rapport.***

ERA offre plusieurs modèles prédéfinis pour la création de rapports. Pour sélectionner un rapport, utilisez le menu déroulant ***Type*** :

- ***Principales menaces***
  Liste des menaces les plus fréquemment détectées.

- ***Principal client avec le plus de menaces***
  Répertorie les stations de travail client les plus « actives » (sur la base du nombre de menaces détectées).

- ***Progression des menaces***
  Progression des événements liés à des logiciels malveillants (sur la base du nombre).

- ***Progression comparative des menaces***
  Progression des événements liés à des logiciels malveillants par menace (sélectionnée à l'aide un filtre) en comparaison du nombre total de logiciels malveillants.

- ***Menaces par scanner***
  Nombre d'alertes de menace des différents modules du programme.

- ***Menaces par objet***
  Nombre d'alertes de menace en fonction de leur mode d'infiltration (message Email, fichiers, secteurs de démarrage).

- ***Principaux clients/Principales menaces combinés***
  Combinaison des types précités.

- ***Principales menaces/Progression des menaces combinées***
  Combinaison des types précités.

- ***Principales menaces/Progression comparative des menaces combinées***
  Combinaison des types précités.

- ***Rapport des clients, Rapport des menaces, Rapport des événements, Rapport des analyses, Rapport des tâches***
  Rapports standard visibles sous les onglets ***Clients, Journal des menaces, Journal des événements, Journal d'analyse*** ou ***Tâches***.

- ***Rapport complet***
  Résumé de
  – Principaux clients/Principales menaces combinés
  – Principales menaces/Progression comparative des menaces combinées
  – Progression des menaces

Dans la section ***Filtre***, vous pouvez utiliser les menus déroulants ***Clients cibles*** ou ***Menace*** pour sélectionner les clients ou virus à inclure dans le rapport.

Vous pouvez configurer d'autres détails en cliquant sur le bouton ***Paramètres supplémentaires...***. Ces paramètres s'appliquent principalement aux données figurant dans le titre et dans les types de diagrammes graphiques utilisés. Toutefois, vous pouvez également filtrer les données en fonction de l'état d'attributs choisis et choisir le format de rapport à utiliser (.html, .csv).

L'onglet Intervalle permet de définir un intervalle de temps pour lequel le rapport sera généré :

- ***Actuelle***
  Seuls les événements survenus au cours d'une période choisie seront inclus dans le rapport. Par exemple, si un rapport est créé un mercredi alors que l'intervalle est défini sur ***Semaine actuelle***, les événements des dimanche, lundi, mardi et mercredi seront inclus.

- ***Terminé***
  Seuls les événements survenus dans une période close choisie seront inclus dans le rapport (c.-à-d. tout le mois d'août ou une semaine entière du dimanche au samedi). Si l'option ***Ajouter aussi la période actuelle*** est activée, le rapport inclut les événements de la dernière période achevée jusqu'au moment de la création.

Exemple :

Nous souhaitons créer un rapport incluant les événements de la dernière semaine calendaire, c.-à-d. du dimanche au samedi suivant. Nous voulons que ce rapport soit généré le mercredi suivant (après le samedi).

Sous l'onglet ***Intervalle***, sélectionnez ***Terminé***, puis ***1 semaine***. Supprimez ***Ajouter aussi la période actuelle***. Sous l'onglet ***Planificateur***, définissez ***Fréquence*** sur ***Hebdomadaire***, puis sélectionnez ***Mercredi***. Les autres paramètres peuvent être configurés à la discrétion de l'administrateur.

- ***De/À***
  Ce paramètre permet de définir une période pour laquelle le rapport sera généré.

L'onglet Planificateur permet de définir et de configurer un rapport automatique à une heure ou à des intervalles choisis (à l'aide de la section ***Fréquence***).

La zone de sélection ***Exécuter à*** et le sélecteur de date **Début** permettent d'entrer l'heure et la date auxquelles le rapport doit être généré. Cliquez sur le bouton ***Sélectionner cible...***, puis, dans la section *Enregistrer le résultat dans*, spécifiez l'emplacement ou enregistrer le rapport. Vous pouvez enregistrer les rapports dans ERAS (par défaut), les envoyer par Email à une adresse choisie ou les exporter dans un dossier. Cette dernière option est utile si le rapport est envoyé à un dossier partagé sur l'intranet de votre organisation, où d'autres employés peuvent le consulter.

Pour envoyer les rapports générés par Email, vous devez entrer les informations de serveur SMTP et d'adresse d'expéditeur dans ***Outils > Options du serveur > Autres paramètres***, comme décrit dans la section 7.8.1, « Paramètres SMTP ».

Pour définir une plage de dates fixe pour le processus de génération de rapport, utilisez les options de la section ***Plage***. Vous pouvez définir le nombre de rapports générés (***Fin après***) ou une date que le processus de génération de rapport ne doit pas dépasser (***Fin pour***).

Pour enregistrer les paramètres de rapports définis dans un modèle, cliquez sur les boutons ***Enregistrer*** ou ***Enregistrer sous...***. Si vous créez un modèle, cliquez sur le bouton ***Enregistrer sous...***, puis attribuez-lui un nom.

En haut de la fenêtre de la console, dans la section Modèles de rapport, vous pouvez voir les noms des modèles déjà créés. À côté des noms de modèle, figurent des informations sur l'heure/les intervalles ainsi que sur le moment où les rapports sont générés en fonction du modèle prédéfini. Cliquez sur le bouton ***Générer maintenant*** (assurez-vous que l'onglet ***Options*** est sélectionné) pour générer un rapport à tout moment, indépendamment du planning.

Vous pouvez afficher des rapports générés précédemment sous l'onglet ***Rapports générés***. Pour accéder à des options supplémentaires, sélectionnez un ou plusieurs rapports, puis utilisez le menu contextuel (en cliquant avec le bouton droit).

Les modèles figurant dans la liste ***Favoris*** permettent de générer immédiatement de nouveaux rapports. Pour déplacer un modèle vers la liste Favoris, cliquez avec le bouton droit sur le rapport, puis, dans le menu contextuel, cliquez sur ***Ajouter aux favoris***.

7. Configuration du serveur ESET Remote Administrator (ERAS)

7.1 Onglet Sécurité

Les solutions de sécurité ESET version 3.x (ESET Smart Security, etc.) offrent une protection par mot de passe pour une communication déchiffrée entre le client et ERAS (communication avec le protocole TCP sur le port 2222).

Les versions antérieures (2.x) n'offrent pas cette fonctionnalité. Pour assurer une compatibilité descendante avec des versions antérieures, le mode ***Activer l'accès non authentifié de clients*** doit être activé.

L'onglet Sécurité contient des options permettant à l'administrateur d'utiliser des solutions de sécurité 2.x et 3.x simultanément sur le même réseau.

- ***Mot de passe pour la console (accès administrateur, accès en lecture seule)***
  Permet de spécifier un mot de passe pour l'administrateur et des utilisateurs limités afin de protéger la console contre des modifications non autorisées des paramètres d'ERAC.

- ***Mot de passe pour les clients* (produits de sécurité ESET)**
  Définit un mot de passe pour les clients accédant à l'ERAS.

- ***Mot de passe pour la réplication***
  Définit un mot de passe pour les serveurs ERA de niveau inférieur en cas de réplication sur un serveur ERAS donné.

- ***Mot de passe pour le programme d'installation à distance d'ESET (Agent)***
  Définit un mot de passe permettant à l'agent d'installation d'accéder à ERAS. Convient pour les installations à distance.

- ***Activer l'accès non authentifié de clients (produits de sécurité ESET)***
  Permet à des clients ne disposant pas d'un mot de passe valide (si le mot de passe actuel diffère du *Mot de passe pour les clients*) d'accéder à ERAS.

- ***Activer l'accès non authentifié pour la réplication***
  Permet à des clients de serveurs ERA de niveau inférieur ne disposant pas d'un mot de passe valide pour la réplication d'accéder à ERAS.

- ***Activer l'accès non authentifié pour le programme d'installation à distance d'ESET (Agent)***
  Permet à des clients de serveurs ERA de niveau inférieur ne disposant pas d'un mot de passe valide pour la réplication d'accéder à ERAS.

REMARQUE : *Si l'authentification est activée dans ERAS et sur tous les clients [génération 3.x], il est possible de désactiver l'option* ***Activer l'accès non authentifié de clients***.

7.2 Onglet Maintenance du serveur

Si la configuration est correcte sous l'onglet Maintenance du serveur, la base de données d'ERAS est automatiquement maintenue et optimisée, sans qu'aucune configuration supplémentaire soit nécessaire. Par défaut, les entrées et les journaux de plus de six mois sont supprimés et la tâche *Compactage et réparation* est effectuée tous les quinze jours. Toutes les options de maintenance du serveur sont accessibles sous ***Outils > Options du serveur*** > ***Maintenance du serveur***.

Les options disponibles sont les suivantes :

- ***Ne garder que les X dernières menaces pour chaque client***
  Ne conserve que le nombre spécifié d'incidents de virus pour chaque client.

- ***Ne garder que les X derniers journaux de pare-feu pour chaque client***
  Ne conserve que le nombre spécifié de journaux de pare-feu pour chaque client.

- ***Ne garder que les X derniers événements pour chaque client***
  Ne conserve que le nombre spécifié d'événements système pour chaque client.

- ***Ne garder que les X derniers journaux d'analyse pour chaque client***
  Ne conserve que le nombre spécifié de journaux d'analyse pour chaque client.

- ***Supprimer les clients non connectés depuis X mois (jours)***
  Supprime tous les clients qui ne se sont pas connecté à ERAS depuis un nombre de mois (ou de jours) supérieur à celui spécifié.

- ***Supprimer les journaux des menaces de plus de X mois (jours)***
  Supprime tous les incidents de virus plus anciens que le nombre de mois (jours) spécifié.

- ***Supprimer les journaux de pare-feu de plus de X mois (jours)***
  Supprime tous les journaux de pare-feu plus anciens que le nombre de mois (jours) spécifié.

- ***Supprimer les journaux des événements de plus de X mois (jours)***
  Supprime tous les événements système plus anciens que le nombre de mois (jours) spécifié.

- ***Supprimer les journaux d'analyse de plus de X mois (jours)***
  Supprime tous les journaux d'analyse plus anciens que le nombre de mois (jours) spécifié.

7.3 Serveur Miroir

La fonctionnalité Miroir permet à l'utilisateur de créer un serveur de mise à jour local. Les ordinateurs client ne téléchargeront pas les mises à jour des signatures de virus à partir des serveurs d'ESET sur Internet, mais se connecteront à un serveur Miroir local sur votre réseau. Les principaux avantages de cette solution sont qu'elle permet d'économiser de la bande passante Internet et de réduire le trafic réseau, car seul le serveur Miroir se connecte à Internet pour les mises à jour, au lieu de centaines d'ordinateurs client. Cette configuration signifie qu'il est important que le serveur Miroir soit toujours connecté à internet.

Avertissement : *Si un serveur Miroir qui a effectué une mise à niveau de composant programme et qui n'a pas été redémarré peut entraîner une panne. Dans un tel scénario, le serveur serait incapable de télécharger LA MOINDRE mise à jour ou d'en distribuer à des stations de travail client. NE DÉFINISSEZ PAS DE MISES À JOUR AUTOMATIQUES DE COMPOSANT PROGRAMME POUR LES PRODUITS SERVEUR ESET ! Cela ne s'applique pas au Miroir créé dans ERAS.*

La fonctionnalité Miroir est disponible dans deux emplacements :

- ESET Remote Administrator (Miroir s'exécutant physiquement dans ERAS, gérable à partir d'ERAC)

- ESET Smart Security Business Edition ou ESET NOD32 Antivirus Business Edition (pour autant que la « Business Edition » ait été activée par une clé de licence).

L'administrateur sélectionne la méthode d'activation de la fonctionnalité Miroir.

Dans des réseaux de grande taille, il est possible de créer plusieurs serveurs Miroir (p. ex., pour divers départements de la société) et d'en définir un comme central (au siège de la société) dans une structure de type cascade similaire à une configuration d'ERAS avec plusieurs clients.

L'administrateur doit insérer la clé de licence de produit pour un produit acheté et d'entrer le nom d'utilisateur et le mot de passe permettant d'activer la fonctionnalité Miroir dans ERAS. Si l'administrateur utilisant une clé de licence, un nom d'utilisateur et un mot de passe pour ESET NOD32 Antivirus Business Edition procède à une mise à niveau, la clé de licence, le nom d'utilisateur et le mot de passe doivent également être remplacés.

7.3.1 Utilisation du serveur Miroir

L'ordinateur hébergeant le serveur Miroir doit fonctionner et être connecté en permanence à Internet ou à un serveur Miroir de niveau supérieur pour la réplication. Vous pouvez télécharger les packages de mise à jour du serveur Miroir de deux manières :

1. En utilisant le protocole HTTP (recommandé)
2. En utilisant un lecteur réseau partagé (SMB)

Les serveurs de mise à jour d'ESET utilisent le protocole HTTP avec une authentification. Un serveur Miroir central doit accéder aux serveurs de mise à jour à l'aide d'un nom d'utilisateur (généralement) sous la forme suivante : EAV-XXXXXXX) et mot de passe.

Le serveur Miroir qui fait partie d'ESET Smart Security/ESET NOD32 Antivirus a un serveur HTTP intégré (variante 1).

REMARQUE : *Si vous décidez d'utiliser le serveur HTTP intégré (sans authentification), veillez à ce qu'il ne soit pas accessible à partir de l'extérieur de votre réseau (c.-à-d. à des clients non inclus dans votre licence). Le serveur ne peut pas être accessible à partir d'Internet.*

Par défaut, le serveur HTTP écoute le port TCP 2221. Assurez-vous que ce port n'est utilisé par aucune autre application.

Vous pouvez également utiliser tout autre type de serveur HTTP. ERA prend également en charge des méthodes d'authentification supplémentaires (p. ex., Apache Web Server utilise la méthode .htaccess).

La seconde méthode (dossier réseau partagé) requiert un partage (droits d'accès en lecture) du dossier contenant les packages de mise à jour. Dans ce scénario, il convient d'entrer, sur la station de travail client, un nom d'utilisateur et un mot de passe permettant d'accéder en lecture au dossier de mise à jour.

REMARQUE : *Les solutions client ESET utilisent le compte d'utilisateur SYSTEM et offrent donc des droits d'accès réseau différents de ceux d'un utilisateur actuellement connecté. Une authentification est requise même si le lecteur réseau est accessible à tous et si l'utilisateur actuel peut y accéder également. De même, utilisez des chemins UNC pour définir le chemin réseau du serveur local. Il est recommandé d'utiliser le format DISK:\.*

Si vous décidez d'utiliser la méthode de dossier réseau partagé (variante 2), il est recommandé de créer un nom d'utilisateur unique (p. ex., NODUSER). Ce compte sera utilisé sur tous les ordinateurs client uniquement pour le téléchargement de mises à jour. Le compte NODUSER doit avoir des droits d'accès en lecture sur le dossier réseau partagé contenant les packages de mise à jour.

Pour l'authentification d'accès à un lecteur réseau, entrez les données authentification sous leur forme complète : WORKGROUP\Utilisateur ou DOMAIN\Utilisateur.

Outre l'authentification, vous devez définir la source des mises à jour pour les solutions client ESET. Une source de mise à jour est soit l'adresse URL d'un serveur local (http://nom_serveur_miroir:port), soit le chemin UNC d'un lecteur réseau :(\\nom_serveur_miroir\nom_partage).

7.3.2 Types de mises à jour

Outre les mises à jour de base des signatures de virus (qui peuvent inclure des mises à jour de noyau logiciel d'ESET), des mises à niveau de composant programme sont également disponibles. Les mises à niveau de composant programme ajoutent des fonctionnalités aux produits de sécurité ESET et nécessitent un redémarrage.

Le serveur Miroir permet à un administrateur de désactiver le téléchargement automatique des mises à niveau de programme à partir des serveurs de mise à jour d'ESET (ou d'un serveur Miroir de niveau supérieur), et de désactiver sa distribution aux clients. L'administrateur peut ensuite déclencher une distribution manuellement (p. ex., s'il est certain qu'il n'y aura pas de conflit entre la nouvelle version et des applications existantes).

Cette fonctionnalité est particulièrement utile si l'administrateur souhaite télécharger et utiliser des mises à jour de base des signatures de virus quand une nouvelle version du programme est également disponible. Si une version plus ancienne du programme est utilisée conjointement avec la dernière version de base de données des virus, le programme continuera à offrir la meilleure protection possible. Il est cependant recommandé de télécharger et d'installer la dernière version du programme pour avoir accès à ses nouvelles fonctionnalités.

Par défaut, les composants programme ne sont pas téléchargés automatiquement et doivent être configurés manuellement dans ERAS. Pour plus d'informations, consultez la section 7.3.3., « Activation et configuration du Miroir ».

7.3.3 Activation et configuration du Miroir

Si le Miroir est directement intégré dans ERA (composant Business Edition), connectez-vous à ERAS à l'aide d'ERAC, puis procédez comme suit :

- Dans ERAC, cliquez sur ***Outils > Options du serveur...*** > ***Mises à jour***.
- Dans le menu déroulant ***Serveur de mise à jour***, sélectionnez **Choisir automatiquement** (les mises à jour seront téléchargées à partir des serveurs d'ESET), ou entrez l'adresse URL ou le chemin UNC d'un serveur Miroir.
- Définissez l'intervalle de mise à jour (idéalement, soixante minutes).

- Si vous avez sélectionné **Choisir automatiquement** à l'étape précédente, insérez le nom d'utilisateur (Nom d'utilisateur de mise à jour) et le mot de passe (Mot de passe de mise à jour) envoyés après l'achat. Si vous accédez à un serveur de niveau supérieur, entrez un nom d'utilisateur de domaine et un mot de passe valides pour ce serveur.

- Activez l'option ***Créer un miroir de mise à jour***, puis entrez le chemin d'accès du dossier qui contiendra les fichiers de mise à jour. Par défaut, il s'agit d'un chemin d'accès relatif au dossier Miroir, pour autant que l'option ***Fournir les fichiers de mise à jour via un serveur HTTP interne*** soit activée et disponible sur le port HTTP défini dans ***Port du serveur HTTP*** (par défaut, 2221).

Définissez ***Authentification*** sur **NONE**[7].

- Sélectionnez les composants à télécharger dans ***Autres paramètres > Modifier les paramètres avancés...*** branche ***Serveur ERA > Configuration > Miroir > Créer un miroir***. Vous devez sélectionner les composants pour toutes les versions linguistiques qui seront utilisées dans le réseau. Notez que le téléchargement d'une version linguistique non installée sur le réseau augmentera inutilement le trafic réseau.

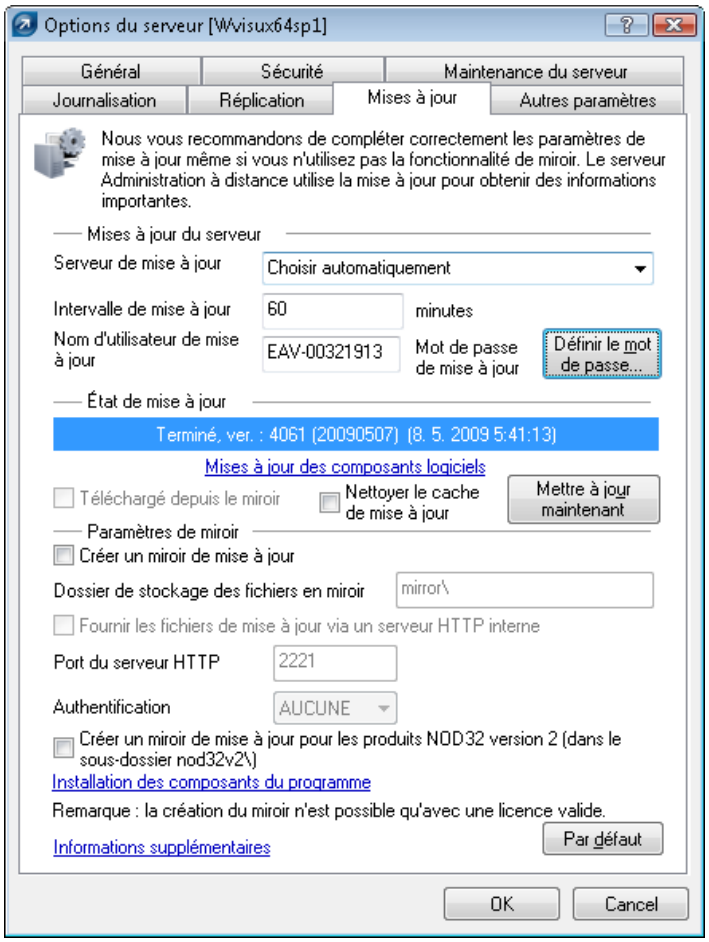


Figure 7-1

La fonctionnalité Miroir est également directement disponible au niveau de l'interface d'ESET Smart Security Business Edition et d'ESET NOD32 Antivirus Business Edition. Il appartient à l'administrateur de choisir la méthode utilisée pour implémenter le serveur Miroir.

Pour activer et lancer le serveur Miroir à partir d'ESET Smart Security Business Edition ou d'ESET NOD32 Antivirus Business Edition, procédez comme suit :

1) Installez ESET Smart Security Business Edition ou ESET NOD32 Antivirus Business Edition

2) Dans la fenêtre ***Configuration avancée*** (**F5**), cliquez sur ***Divers > Licences***. Cliquez sur le bouton ***Ajouter...***, recherchez le fichier *.lic, puis cliquez sur ***Ouvrir***. Cela aura pour effet d'installer la licence et de permettre la configuration de la fonctionnalité Miroir.

[7] Pour plus d'informations, consultez la section sur l'authentification dans le serveur ERA.

3) Dans la branche ***Mise à jour***, cliquez sur le bouton ***Configurer...***, puis sélectionnez l'onglet ***Miroir***.

4) Sélectionnez l'option ***Créer un miroir de mise à jour***, puis l'option ***Fournir les fichiers de mise à jour via un serveur HTTP interne***.

5) Entrez le chemin d'accès complet du dossier (***Dossier de stockage des fichiers en miroir***) dans lequel les fichiers de mise à jour doivent être stockés.

6) Les champs ***Nom d'utilisateur*** et ***Mot de passe*** servent de données d'authentification pour les stations de travail client tentant d'accéder au dossier Miroir. Dans la plupart des cas, il n'est pas obligatoire de les renseigner.

7) Définissez Authentification sur **NONE**[8].

8) Sélectionnez les composants à télécharger [9] (c.-à-d. les composants pour toutes les versions linguistiques qui seront utilisées dans le réseau).

REMARQUE : *Pour assurer une fonctionnalité optimale, il est recommandé d'activer le téléchargement et la mise en miroir des composants programme. Si cette option est désactivée, seule la base des signatures de virus est mise à jour, pas les composants du programme. Si vous utilisez la fonctionnalité Miroir d'ERA, vous pouvez configurer cette option dans ERAC en cliquant sur* ***Outils > Options du serveur... > onglet Autres paramètres > Modifier les paramètres avancés... > ESET Remote Administrator > Serveur ERA > Configuration > Miroir.*** *Activez toutes les versions linguistiques du programme présentes dans votre réseau.*

7.3.4 Miroir pour les clients avec NOD32 version 2.x

La solution ESET Remote Administrator permet à un administrateur de créer des copies de fichiers de mise à jour pour les ordinateurs client sur lesquels ESET NOD32 Antivirus 2.x est installé. Pour ce faire, cliquez sur ***Outils*** > ***Options du serveur*** > ***Mises à jour*** > **Créer un miroir de mise à jour pour les produits NOD32 version 2**. Cela s'applique uniquement à ERA ; le Miroir inclus dans la solution client de Business Edition (v 3.x) ne contient pas cette option.

Si vous disposez de clients 2.x et 3.x dans votre réseau, il est recommandé d'utiliser le Miroir intégré dans ERA. Si les deux miroirs sont activés sur le même ordinateur (un dans ERAS pour clients 2.x, l'autre dans un client Business Edition pour clients 3.x), cela peut entraîner un conflit entre deux serveurs HTTP utilisant le même port TCP.

Les mises à jour pour les clients 2.x sont stockées dans le dossier « nod32v2 », sous-dossier du dossier Miroir principal. Celui-ci est accessible via l'adresse URL suivante :

http://nom_serveur_miroir:port/nod32v2

ou le chemin UNC d'un lecteur réseau :

\\nom_serveur_miroir\nom_partage\nod32v2

ERA est également capable de télécharger des composants programme pour clients 2.x. Pour sélectionner les composants programme à télécharger, accédez à ***Outils > Options du serveur... > onglet Autres paramètres >***, cliquez sur ***Modifier les paramètres avancés... >***, branche ***ESET Remote Administrator > Serveur ERA > Configuration > Miroir pour NOD32 version 2***. Pour réduire le volume des données téléchargées, ne sélectionnez que les versions linguistiques présentes sur votre réseau.

7.4 Onglet Réplication

La réplication est utilisée dans des réseaux de grande taille où plusieurs serveurs ERA sont installés (p. ex., une société possédant plusieurs filiales). Pour plus d'informations, consultez la section 2.3.3, « Installation ».

Les options disponibles sous l'onglet Réplication (***Outils > Options du serveur...***) sont réparties dans deux sections :

- Paramètres de réplication « sur »
- Paramètres de réplication « de »

[8] Pour plus d'informations sur l'authentification, consultez la section 7.3.1., « Utilisation du serveur Miroir ».

[9] Les composants ne s'affichent que s'ils sont disponibles sur les serveurs de mise à jour d'ESET.

La section Paramètres de réplication « sur » permet de configurer des serveurs ERA de niveau inférieur. L'option *Activer la réplication « sur »* doit être activée et l'adresse IP ou le nom du serveur ERAS maître (serveur de niveau supérieur) doit être spécifié. Les données du serveur de niveau inférieur sont alors répliquées sur le serveur maître. Les *Paramètres de réplication « de »* permettent aux serveurs ERA maîtres (de niveau supérieur) d'accepter des données de serveurs ERA de niveau inférieur, ou de les transférer sur des serveurs maîtres. L'option *Activer la réplication « de »* doit être activée et les noms de serveurs de niveau inférieur doivent être définis (délimités par des virgules).

Ces deux options doivent être activées pour les serveurs ERA situés n'importe où au milieu de la hiérarchie de réplication (de façon à ce qu'ils aient des serveurs de niveau supérieur et de niveau inférieur).

Tous les scénarios précités sont visibles dans la figure ci-dessous. Les ordinateurs de couleur beige représentent des serveurs ERA individuels. Chaque serveur ERAS est représenté par son nom (qui doit être identique à %Computer Name %, afin d'éviter toute confusion) et par les paramètres correspondants dans la boîte de dialogue de réplication.

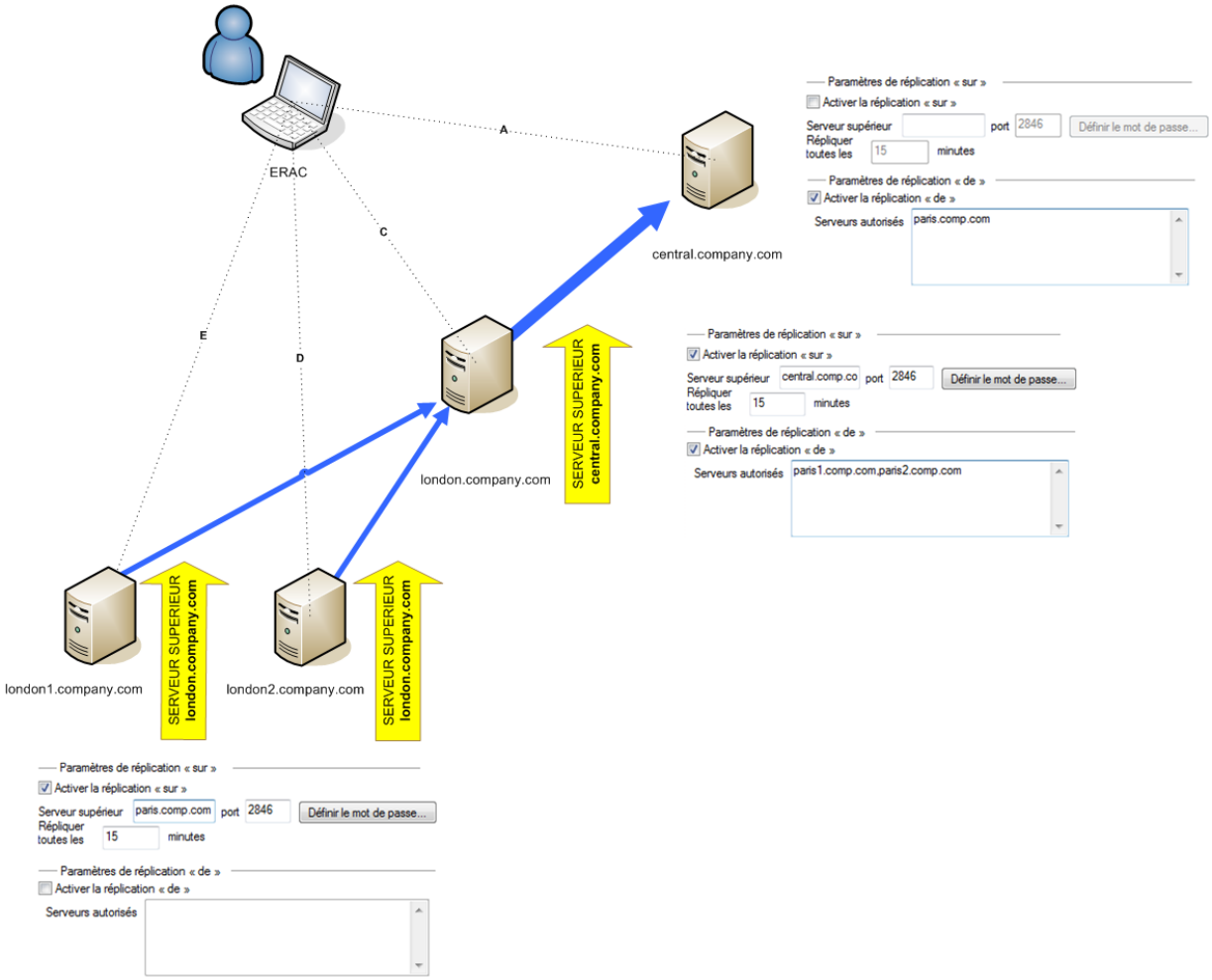


Figure 7-2

Les autres options qui influencent le comportement de réplication des serveurs sont les suivantes :

- **Répliquer journal des menaces, Répliquer journal de pare-feu, Répliquer journal des événements, Répliquer journal d'analyse**
  Si ces options sont activées, toutes les informations affichées sous les onglets **Clients, Journal des menaces, Journal de pare-feu, Journal des événements, Journal d'analyse** et **Tâches** sont répliquées dans des colonnes et des lignes individuelles. Il se peut que les informations non stockées directement dans la base de données mais dans des fichiers individuels (c.-à-d. au format .txt ou .xml) ne soient pas répliquées. Activez ces options pour répliquer également des entrées dans ces fichiers.

- ***Répliquer automatiquement détails du journal des menaces, Répliquer automatiquement détails du journal d'analyse, Répliquer automatiquement détails du client***
  Ces options activent la réplication automatique des informations complémentaires stockées dans des fichiers individuels. Il est également possible de télécharger ces informations à la demande en cliquant sur le bouton ***Demande***.

REMARQUE : *Certains journaux sont répliqués automatiquement, tandis que les journaux détaillés et les journaux de configuration de client ne le sont qu'à la demande. Cela est dû au fait que certains journaux peuvent contenir des quantités importantes de données dépourvues de pertinence. Par exemple, un journal d'analyse pour lequel l'option Journaliser tous les fichiers est activée utilise une quantité importante d'espace disque. De telles informations sont généralement superflues et peuvent être demandées manuellement. Les serveurs enfant ne soumettent pas automatiquement d'informations sur les clients supprimés. C'est pourquoi des serveurs de niveau supérieur peuvent continuer à stocker des informations sur des clients supprimés de serveurs de niveau inférieur. Pour supprimer un client de l'onglet Client sur un serveur de niveau supérieur, sélectionnez l'option Activer la suppression des clients répliqués sur le serveur sous-jacent accessible via* ***Options du serveur > Autres paramètres > Modifier les paramètres avancés > Configuration > Réplication.***

Pour définir le niveau de maintenance des journaux dans ERAS, cliquez sur ***Outils > Options du serveur*** > ***Autres paramètres*** > ***Modifier les paramètres avancés...*** > ***Configuration*** > ***Maintenance du serveur***.

Si vous ne voulez répliquer que les clients présentant un changement d'état, activez l'option ***Outils > Options du serveur > Réplication > Marquer tous les clients pour réplication par « Répliquer vers le haut maintenant »***.

7.5 Onglet Journalisation

En cours d'exécution, ERAS crée un journal (***Nom de fichier du journal***) concernant son activité, que vous pouvez configurer (Détails du journal). Si l'option ***Journaliser dans un fichier texte*** est activée, de nouveaux fichiers journaux sont créés (***Rotation quand taille supérieure à X Mo***) et supprimés sur une base quotidienne (***Supprimer les fichiers de rotation de plus de X jours***).

L'option ***Consigner dans le journal des applications du SE*** permet de copier les informations dans le journal de l'Observateur d'événements système (**Panneau de configuration de Windows > Outils d'administration > Observateur d'événements**).

Dans des circonstances normales, l'option ***Journal de débogage de base de données*** doit être désactivée.

Par défaut, le fichier texte est enregistré dans l'emplacement suivant :
%ALLUSERSPROFILE %\Application data\Eset\Eset Remote Administrator\Server\logs\era.log

Il est recommandé de laisser le paramètre Détails du journal défini sur Niveau 2 – Supérieur + Erreurs de session. Ne modifiez le niveau de journalisation que si vous rencontrez des problèmes ou sur demande du service client d'ESET.

Cliquez sur **Outils > Options du serveur > Autres paramètres > Modifier les paramètres avancés... > Configuration > Journalisation > Compression du journal de débogage soumis à rotation** pour configurer le niveau de compression des journaux soumis à rotation.

7.6 Gestion de licence

Pour qu'ERA fonctionne correctement, vous devez télécharger une clé de licence. Après l'achat, les clés de licence sont envoyées à votre adresse Email avec votre nom d'utilisateur et votre mot de passe. Le ***Gestionnaire de licences*** permet de gérer les licences.

À partir de la version 3.x, ERA prend en charge plusieurs clés de licence. Cette fonctionnalité facilite la gestion de clés de licence.

La fenêtre principale du Gestionnaire de licences est accessible à partir de ***Outils > Gestionnaire de licences.***

Pour ajouter une nouvelle clé de licence :

- Accédez à ***Outils > Gestionnaire de licences*** ou appuyez sur les touches **CTRL + L** de votre clavier.
- Cliquez sur ***Parcourir*** pour accéder au fichier de clé de licence souhaité (les fichiers de ce type portent l'extension .lic).
- Cliquez sur ***Ouvrir*** pour confirmer.
- Vérifiez que les informations de clé de licence sont correctes, puis sélectionnez ***Charger sur le serveur.***
- Cliquez sur **OK** pour confirmer.

Le bouton ***Charger sur le serveur*** n'est actif que si vous avez sélectionné une clé de licence (à l'aide du bouton ***Parcourir***). Les informations sur la clé de licence affichée sont présentées dans cette partie de la fenêtre. Cela permet d'effectuer un dernier contrôle avant de copier la clé sur un serveur.

La partie centrale de la fenêtre présente des informations sur la clé de licence actuellement utilisée par le serveur. Pour afficher des détails sur toutes les clés de licence présentes sur le serveur, cliquez sur le bouton ***Détails...***

ERAS est capable de sélectionner la clé de licence la plus appropriée et de fusionner plusieurs clés en une seule. Si plusieurs clés de licence ont été chargées, ERAS essaie toujours de trouver celle qui a le plus de clients et la date expiration la plus éloignée.

La capacité de fusionner plusieurs clés fonctionne si toutes les clés appartiennent au même client. La fusion de licences est un processus simple qui crée une clé contenant tous les clients concernés. La date d'expiration de la nouvelle clé de licence est celle de la clé qui expirera la première.

La partie inférieure de la fenêtre du Gestionnaire de licences est destinée aux notifications relatives aux problèmes de licence. Les options disponibles sont les suivantes :

- ***Avertir si la licence du serveur expirera dans 20 jours*** – Affiche un avertissement x jours avant l'expiration de la licence.
- ***N'avertir que si cela entraîne une chute du nombre de clients sous licence au-dessous du nombre de clients réels dans la base de données du serveur*** – Activez cette option pour n'afficher un avertissement que si l'expiration de la clé de licence ou d'une partie de la licence entraînera une chute du nombre clients sous le nombre de clients actuellement connectés ou de clients dans la base de données d'ERAS.
- ***Avertir s'il ne reste que 10 % de clients disponibles dans la licence du serveur*** – Le serveur affiche un message d'avertissement si le nombre de clients disponibles chute sous la valeur spécifiée (en %).

Le serveur ERAS peut fusionner plusieurs licences de plusieurs clients. Cette fonctionnalité doit être activée par une clé spéciale. Si vous avez besoin d'une telle clé, spécifiez-le dans votre commande ou contactez votre distributeur ESET local.

7.7 Paramètres avancés

Pour accéder au paramètres avancés d'ERA, cliquez sur ***Outils > Options du serveur > Autres paramètres > Modifier les paramètres avancés***.

Les paramètres avancés sont les suivantes :

- ***Utilisation d'espace disque maximale (pour cent)***
  En cas de dépassement, il se peut que certaines fonctionnalités du serveur soient indisponibles. Lorsqu'il se connecte à ERAS, ERAC affiche une notification en cas de dépassement de la limite**.**
- ***Codage du protocole de communication***
  Définit le type de codage. Il est recommandé de conserver le paramètre par défaut.
- ***Activer le changement de nom d'adresse MAC (d'inconnue en valide)***
  Après réinstallation à partir d'une solution client ESET qui ne prend pas en charge l'envoi d'adresse MAC (p. ex., ESET NOD32 Antivirus 2.x) à une solution client prenant en charge cette fonctionnalité (p. ex., un client 3.x), l'enregistrement de l'ancien client est converti en enregistrement du nouveau. Il est recommandé de conserver le paramètre par défaut (Oui).
- ***Activer le changement de nom d'adresse MAC (de valide en inconnue)***
  Après réinstallation à partir d'une solution client ESET qui prend en charge l'envoi d'adresse MAC (p. ex., ESET NOD32 Antivirus 3.x) à une solution client ne prenant pas en charge cette fonctionnalité (p. ex., un client 2.x), l'enregistrement de l'ancien client est converti en enregistrement du nouveau. Il est recommandé de conserver le paramètre par défaut (Non).
- ***Activer le changement de nom d'adresse MAC (de valide en une autre valide)***
  Active le changement de nom d'adresses MAC valides. La valeur par défaut ne permet pas le changement de nom, ce qui signifie que l'adresse MAC fait partie de l'identification unique des clients. Désactivez cette option s'il y a plusieurs entrées pour un seul PC. Il est également recommandé de désactiver cette option si un client est identifié comme étant le même client après modification de l'adresse MAC.
- ***Activer le changement de nom d'ordinateur***
  Permet de modifier le nom d'ordinateurs client. Si cette option est désactivée, le nom d'ordinateur fera partie de l'identification unique des clients.
- ***Utiliser aussi l'ouverture de session par défaut du serveur durant une installation poussée***
  ERAS permet à l'utilisateur de définir un nom d'utilisateur et un mot de passe uniquement pour une installation à distance par script d'ouverture de session et par Email. Activez cette option pour utiliser les valeurs prédéfinies également pour les installations poussées à distance.

7.8 Onglet Autres paramètres

7.8.1 Paramètres SMTP

- ***Paramètres SMTP*** (***Serveur, Adresse de l'expéditeur, Nom d'utilisateur, Mot de passe***)
  Certaines fonctionnalités d'ERA requièrent une configuration de serveur SMTP correcte. Ces fonctionnalités sont l'installation à distance par Email et la génération de rapports à envoyer par Email.

7.8.2 Ports

Ports (Console, Client, Port de réplication de ce serveur, Programme d'installation à distance d'ESET)

Permet de personnaliser les ports sur lesquels ERAS écoute les communications, établis par :

- ***Console*** (par défaut 2223)
- ***Client*** (par défaut 2222)
- Le processus de réplication (***Ports de réplication*** – par défaut 2846)
- ***Programme d'installation à distance d'ESET*** (par défaut 2224)

7.8.3 Nouveaux clients

- ***Autoriser nouveaux clients***
  Si cette option est désactivée, aucun nouveau client n'est ajouté sous l'onglet Clients. Même si de nouveaux clients communiquent avec des serveurs ERA, ils ne sont pas visibles sous l'onglet Clients.
- ***Redéfinir automatiquement le drapeau « Nouveau » pour les nouveaux clients***
  Si cette option est activée, le drapeau Nouveau est supprimé des clients se connectant pour la première fois à ERAS. Pour plus d'informations, consultez la section 3.4.3, « Onglet Clients ».

7.8.4 ThreatSense. Net

- ***Activer le transfert de données ThreatSense.Net aux serveurs ESET***
  Si cette option est activée, ERAS transfère les fichiers suspects et les informations statistiques des clients aux serveurs d'ESET. Notez que, selon la configuration du réseau, il n'est pas toujours possible pour des stations de travail client de soumettre ces informations directement.

8. Dépannage

8.1 FAQ

Ce chapitre contient des solutions aux questions les plus fréquemment posées et aux problèmes liés à l'installation et à l'utilisation d'ERA.

8.1.1 Problèmes d'installation de la solution ESET Remote Administrator sur un serveur Windows 2000/2003

Cause :
L'une des causes possibles est que le serveur Terminal Server soit en cours d'exécution sur le système en mode *execution*.

Solution :
Microsoft conseille de basculer le serveur Terminal Server en mode « install » lors de l'installation de programmes sur un système sur lequel le service Terminal Server est en cours d'exécution. Pour ce faire, accédez à ***Panneau de configuration > Ajout ou suppression de programmes***, ou ouvrez une invite de commandes, puis entrez la commande change user / install. Après installation, tapez change user / execute pour rétablir le mode execution du serveur Terminal Server. Pour obtenir des instructions pas à pas sur ce processus, consultez l'article suivant : http://support.microsoft.com/kb/320185.

8.1.2 Quelle est la signification du code d'erreur GLE ?

L'installation d'ESET Smart Security ou d'ESET NOD32 Antivirus via la console Remote Administrator génère parfois une erreur GLE. Pour connaître la signification d'un numéro d'erreur GLE, procédez de la manière décrite ci-dessous :

1) Ouvrez une invite de commandes en cliquant sur **Démarrer → Exécuter**. Tapez **cmd**, puis cliquez sur **OK**.
2) À l'invite de commandes, tapez : **net helpmsg numéro_erreur**

Exemple : « *net helpmsg* 55 »

Résultat : La ressource ou le périphérique réseau spécifié n'est plus disponible.

8.2 Codes d'erreur fréquemment rencontrés

Durant l'utilisation d'ERA, il se peut que vous rencontriez des messages d'erreur contenant des codes d'erreur indiquant un problème en relation avec une fonctionnalité ou une opération. La section 8.2.1 ci-dessous indique les codes d'erreur les plus fréquemment rencontrés lors de l'exécution d'installations poussées, ainsi que des erreurs qui peuvent être relevées dans le journal d'ERAS.

8.2.1 Messages d'erreur affichés lors de l'utilisation de la solution ESET Remote Administrator pour installer à distance ESET Smart Security ou ESET NOD32 Antivirus

Code d'erreur SC 6, code d'erreur GLE 53 Impossible de configurer une connexion IPC à un ordinateur cible
Pour configurer une connexion IPC, la configuration suivante est requise :
1. Pile TCP/IP installée sur l'ordinateur où ERAS est installé, ainsi que sur l'ordinateur cible.
2. Le Partage de fichiers et d'imprimantes pour Microsoft Network doit être installé.
3. Les ports de partage de fichiers doivent être ouverts (135 – 139, 445).
4. L'ordinateur cible doit répondre aux requêtes Ping.

Code d'erreur SC 6, code d'erreur GLE 67 Installation du programme d'installation d'ESET sur l'ordinateur cible impossible
Le partage administratif ADMIN$ doit être accessible sur le lecteur système du client.

Code d'erreur SC 6, Code d'erreur GLE 1326 Impossible de configurer une connexion IPC à l'ordinateur cible, probablement en raison d'un nom d'utilisateur ou d'un mot de passe erroné
Le nom d'utilisateur et le mot de passe de l'administrateur n'ont pas été tapés correctement ou n'ont pas été entrés du tout.

Code d'erreur SC 6, code d'erreur GLE 1327 Impossible de configurer une connexion IPC à un ordinateur cible
Le champ du mot de passe d'administrateur est vide. Une installation poussée à distance ne peut pas fonctionner avec un champ de mot de passe vide.

Code d'erreur SC 11, code d'erreur GLE 5 Installation du programme d'installation d'ESET sur l'ordinateur cible impossible
Le programme d'installation ne peut pas accéder à l'ordinateur client en raison de droits d'accès insuffisants (accès refusé).

Code d'erreur SC 11, code d'erreur GLE 1726 Impossible d'installer le programme d'installation de NOD32 sur l'ordinateur cible
Ce code d'erreur s'affiche après une tentative d'installation répétée si la fenêtre Pousser l'installation n'a pas été fermée après la première tentative.

8.2.2 Codes d'erreur fréquemment rencontrés dans era.log

0x1203 – UPD_RETVAL_BAD_URL
Erreur de module de mise à jour – nom de serveur de mise à jour entré incorrect.

0x1204 – UPD_RETVAL_CANT_DOWNLOAD
Cette erreur peut s'afficher :

- lors d'une mise à jour via HTTP
  - le serveur de mise à jour retourne un code d'erreur HTTP entre 400 – 500, sauf 401, 403, 404, et 407
  - si les mises à jour sont téléchargées à partir d'un serveur CISCO et que le format HTML de réponse d'authentification a été modifié
- lors d'une mise à jour à partir d'un dossier partagé :
  - l'erreur retournée ne s'inscrit pas dans les catégories « authentification incorrecte » ou « fichier introuvable » (p. ex., connexion interrompue ou serveur inexistant, etc.)
- les deux méthodes de mise à jour
  - si tous les serveurs répertoriés dans le fichier upd.ver sont introuvables (le fichier se trouve dans %ALLUSERSPROFILE\Application Data\ESET\ESET Remote Administrator\Server\updfiles)
  - échec de contact du serveur failsafe (probablement dû à la suppression des entrées ESET correspondantes dans le Registre)
- configuration du serveur proxy incorrecte dans ERAS
  - L'administrateur doit spécifier un serveur proxy dans le format

0x2001 – UPD_RETVAL_AUTHORIZATION_FAILED
Échec de l'authentification auprès du serveur de mise à jour, nom d'utilisateur ou mot de passe incorrect.

0x2102 – UPD_RETVAL_BAD_REPLY
Cette erreur de module de mise à jour peut se produire si un serveur proxy est utilisé comme intermédiaire pour une connexion Internet – à savoir proxy Webwasher.

0x2104 – UPD_RETVAL_SERVER_ERROR
Erreur de module de mise à jour indiquant un code d'erreur HTTP supérieur à 500. Dans le cas du serveur HTTP ESET, l'erreur 500 signifie qu'il y a un problème d'allocation de mémoire.

0x2105 – UPD_RETVAL_INTERRUPTED
Cette erreur de module de mise à jour peut se produire si un serveur proxy est utilisé comme intermédiaire pour une connexion Internet – à savoir proxy Webwasher.

8.3 Comment diagnostiquer des problèmes avec ERAS ?

Si vous pensez qu'il y a un problème avec ERAS ou s'il ne fonctionne pas correctement, il est recommandé de procéder comme suit :

1. Contrôlez le journal d'ERAS : Cliquez sur ***Outils > Options du serveur*** dans le menu principal d'ERAC. Dans la fenêtre **Options du serveur**, cliquez sur l'onglet ***Journalisation***, puis sur ***Afficher journal***.
2. Si vous ne voyez pas de message d'erreur, augmentez le niveau ***Détails du journal*** dans la fenêtre **Options du serveur** à 5. Après avoir identifié le problème, il est recommandé de rétablir la valeur par défaut.
3. Il se peut également que vous puissiez résoudre des problèmes en activant le journal de débogage de base de données sous le même onglet – voir ***Journal de débogage***. Il est recommandé de n'activer le ***Journal de débogage*** qu'en tentant de reproduire le problème.
4. Si vous voyez un code d'erreur autre que ceux mentionnés dans cette documentation, contactez le service clientèle d'ESET. Décrivez le comportement du programme, la manière de reproduire le problème et la manière de l'éviter. Il est très important d'inclure la version du programme de tous les produits de sécurité ESET concernés (c.-à-d. ERAS, ERAC, ESET Smart Security, ESET NOD32 Antivirus).

9. Conseils et astuces

9.1 Planificateur

ESET NOD32 Antivirus et ESET Smart Security contiennent un planificateur de tâches intégré permettant de planifier des analyses à la demande, mises à jour et opérations à intervalles réguliers. Toutes les tâches spécifiées sont répertoriées dans le Planificateur.

ERA permet de configurer les quatre types de tâches suivants :
- ***Exécuter une application externe***
- ***Contrôle des fichiers de démarrage du système***
- ***Analyse d'ordinateur à la demande***
- ***Mise à jour***

Dans la plupart des cas, il n'est pas nécessaire de configurer une tâche ***Exécuter une application externe***. La tâche ***Contrôle des fichiers de démarrage du système*** est une tâche par défaut. Il est recommandé de ne pas en modifier les paramètres[10]. Du point de vue d'un administrateur, les tâches ***Analyse d'ordinateur à la demande et Mise à jour sont probablement les plus utiles :***

- ***Analyse d'ordinateur à la demande***
  Cette tâche effectue une analyse antivirus régulière (généralement de lecteurs locaux) sur les clients.

- ***Mise à jour***
  Cette tâche est responsable de la mise à jour de solutions client ESET. Il s'agit d'une tâche prédéfinie qui, par défaut, s'exécute toutes les 60 minutes. Généralement, il n'y a aucune raison d'en modifier les paramètres. La seule exception a trait aux portables dont les propriétaires se connectent souvent à Internet sans passer par les réseaux locaux. Dans ce cas, il est possible de modifier la tâche de mise à jour afin d'utiliser deux profils de mise à jour à l'intérieur d'une seule tâche. Cela permet aux portables de se mettre à jour indifféremment à partir du serveur Miroir local ou des serveurs de mise à jour d'ESET.

La configuration du Planificateur est également accessible à l'aide de l'éditeur de configuration d'ESET dans ***ESET Smart Security / ESET NOD32 Antivirus*** > ***Noyau ESET*** > ***Configuration*** > ***Planificateur/Programmateur*** > ***Planificateur/Programmateur*** > ***Modifier***.

Pour plus d'informations, consultez la section 3.7, « Éditeur de configuration d'ESET ».

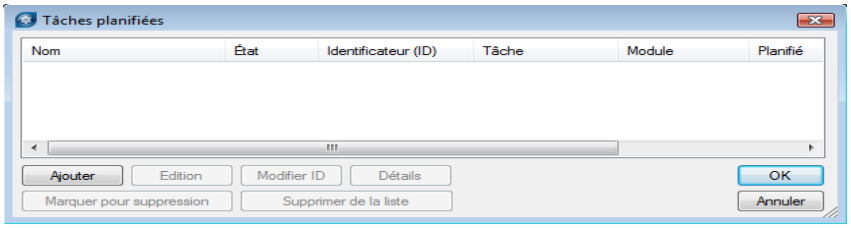


Figure 9-1

Il se peut que la boîte de dialogue contienne des tâches existantes (cliquez sur ***Edition*** pour les modifier) ou qu'elle soit vide. Cela dépend selon que vous avez ouvert une configuration à partir d'un client (p. ex., à partir d'un client précédemment configuré et opérationnel) ou ouvert un nouveau fichier avec le modèle par défaut ne contenant aucune tâche.

Un ID d'attribut est affecté à chaque nouvelle tâche. Les tâches par défaut ont des ID décimaux (1, 2, 3...) et les tâches personnalisées reçoivent des clés hexadécimales (p. ex., 4AE13D6C) qui sont générées automatiquement lors de leur création.

Si la case à cocher d'une tâche est activée, cela signifie que la tâche est active et qu'elle sera exécutée sur le client donné.

[10] Si aucune modification n'a été apportée après l'installation, ESET NOD32 et ESET Smart Security contiennent deux tâches prédéfinies de ce type. La première contrôle les fichiers systèmes à chaque ouverture de session de l'utilisateur, et la seconde fait la même chose après une mise à jour réussie de la base des signatures de virus.

Les boutons de la fenêtre Tâches planifiées fonctionnent comme suit :

- ***Ajouter*** – Ajoute une tâche
- ***Modifier*** – Modifie des tâches sélectionnées
- ***Modifier ID*** – Modifie l'ID des tâches sélectionnées
- ***Détails*** – Informations récapitulatives sur les tâches sélectionnées
- ***Marquer pour suppression*** – L'application du fichier .xml entraîne la suppression des tâches (ayant le même ID) sélectionnées en cliquant sur ce bouton au niveau des clients cibles.
- ***Supprimer de la liste*** – Supprime les tâches sélectionnées de la liste. Notez que les tâches supprimées de la liste dans la configuration .xml ne sont pas supprimées des stations de travail cibles.

Lors de la création d'une tâche (bouton ***Ajouter***) ou de la modification d'une tâche existante (***Modifier***), vous devez spécifier le moment de son exécution. La tâche peut se répéter après une certaine période (quotidiennement à 12 h, chaque vendredi, etc.) ou être déclenchée par un événement (après une mise à jour réussie, quotidiennement au premier démarrage de l'ordinateur, etc.).

La dernière étape de la tâche ***Analyse d'ordinateur à la demande*** affiche la fenêtre des paramètres spéciaux dans laquelle vous pouvez définir la configuration qui sera utilisée pour l'analyse, c.-à-d. le profil d'analyse et les cibles d'analyse qui seront utilisés.

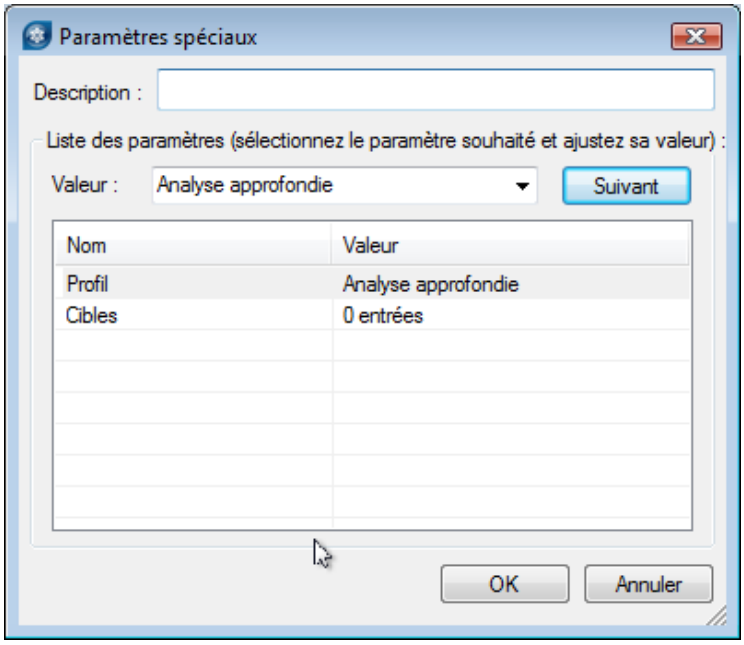


Figure 9-2

La dernière étape de la tâche ***Mise à jour*** spécifie les profils de mise à jour qui s'exécuteront dans le cadre de la tâche donnée. Il s'agit d'une tâche prédéfinie qui, par défaut, s'exécute toutes les 60 minutes. Généralement, il n'y a aucune raison d'en modifier les paramètres. La seule exception a trait aux portables dont les propriétaires se connectent à Internet sans passer par les réseaux de la société. La dernière boîte de dialogue permet de spécifier deux profils de mise à jour différents, couvrant les mises à jour à partir d'un serveur local ou des serveurs de mise à jour d'ESET.

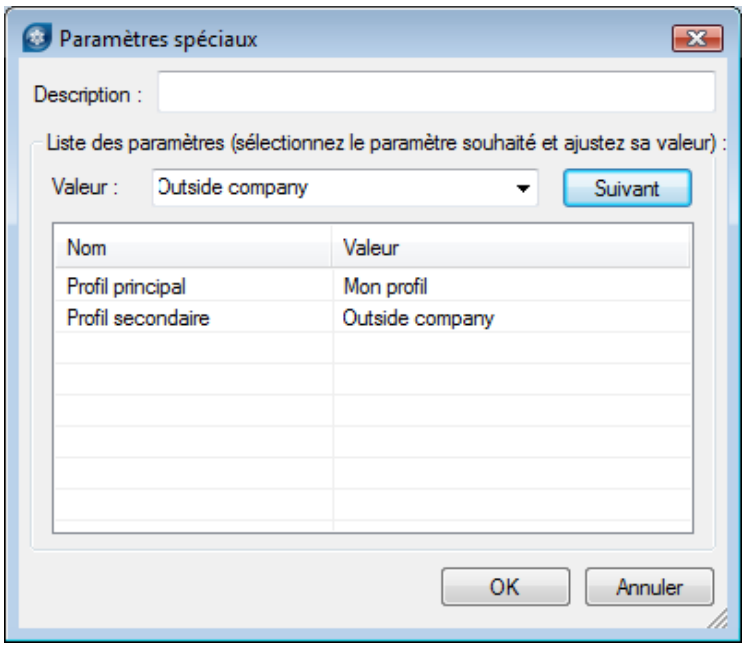


Figure 9-3

9.2 Suppression de profils

Il se peut que vous rencontriez occasionnellement des profils (de mise à jour ou d'analyse) en double créés par erreur. Pour supprimer ces profils à distance sans endommager d'autres paramètres du Planificateur, procédez comme suit :

- Dans ERAC, cliquez sur l'onglet ***Clients***, puis double-cliquez sur un client problématique.
- Dans la fenêtre **Propriétés du client**, cliquez sur l'onglet ***Configuration***. Activez les options ***Puis exécuter l'éditeur de configuration d'ESET pour modifier le fichier*** et ***Utiliser la configuration téléchargée dans la nouvelle tâche de configuration***, puis cliquez sur le bouton ***Nouvelle tâche***.
- Dans l'Assistant Nouvelle tâche, cliquez sur ***Modifier.***
- Dans l'éditeur de configuration, appuyez sur **CTRL + D** pour désélectionner (griser) tous les paramètres. Cela permet d'éviter des modifications accidentelles, car toute nouvelle modification apparaît en bleu.
- Cliquez avec le bouton droit sur le profil à supprimer, puis, dans le menu contextuel, sélectionnez ***Marquer profil pour suppression***. Le profil sera supprimé dès que la tâche aura été envoyée aux clients.

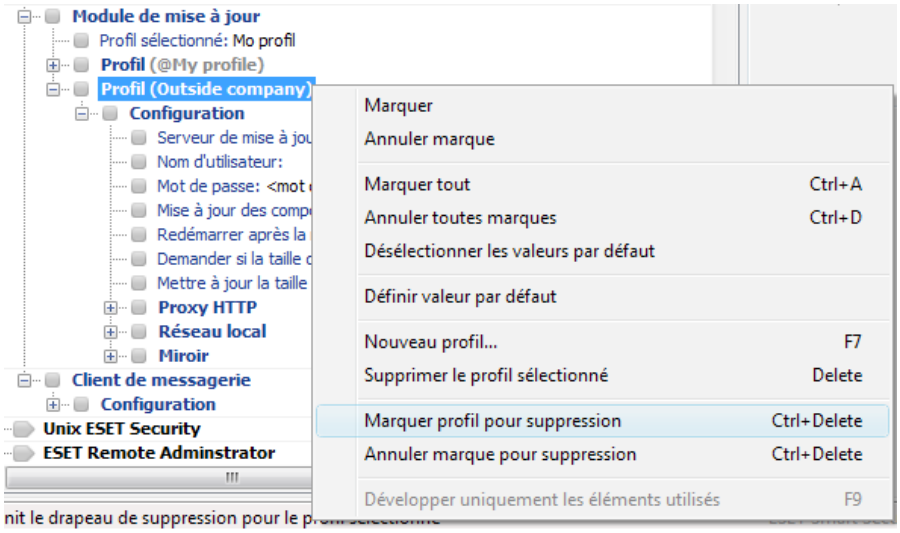


Figure 9-4

- Cliquez sur le bouton ***Console*** dans l'éditeur de configuration d'ESET, puis enregistrez les paramètres.
- Vérifiez que le client que vous avez sélectionné figure dans la colonne ***Éléments sélectionnés*** à droite. Cliquez sur ***Suivant***, puis sur ***Terminer***.

9.3 Exportation et autres fonctions de configuration XML des clients

Dans ERAC, sous l'onglet **Clients**, sélectionnez des clients. Cliquez avec le bouton droit, puis, dans le menu contextuel, sélectionnez **Configuration...**. Cliquez sur ***Enregistrer sous...*** pour exporter la configuration attribuée duclient donné dans un fichier .xml[11]. Vous pouvez ensuite utiliser le fichier .xml pour diverses opérations :

- Lors d'installations à distance, vous pouvez utiliser le fichier .xml comme modèle pour une configuration prédéfinie. Cela signifie qu'aucun fichier .xml n'est créé et que le fichier .xml existant est attribué (***Sélectionner...***) à un nouveau package d'installation.
- Pour configurer plusieurs clients, les clients sélectionnés reçoivent un fichier .xml téléchargé précédemment et adoptent les paramètres définis dans celui-ci (aucune configuration n'est créée ; la configuration est attribuée à l'aide du bouton ***Sélectionner...***).

Exemple : *Un produit de sécurité ESET n'est installé que sur une seule station de travail. Ajustez directement les paramètres via l'interface utilisateur du programme. Lorsque vous avez terminé, exportez les paramètres dans un fichier .xml. Vous pouvez ensuite utiliser ce fichier pour effectuer des installations à distance sur d'autres stations de travail. Cette méthode peut s'avérer très utile pour exécuter des tâches telles que le réglage fin des règles de pare-feu en cas d'application du mode « basé sur des règles personnalisées ».*

9.4 Mise à jour combinée pour les portables

Si votre réseau local comprend des périphériques mobiles (c.-à-d. des portables), il est recommandé de configurer une mise à jour combinée à partir de deux sources : les serveurs de mise à jour d'ESET et le serveur Miroir local. Les portables commencent par contacter le serveur Miroir local. Si la connexion échoue (ils se trouvent hors du bureau), ils téléchargent les mises à jour directement à partir des serveurs d'ESET. Pour permettre l'utilisation de cette fonctionnalité :

- Créez deux profils de mise à jour, l'un dirigé vers le serveur miroir (appelé « LAN » dans l'exemple suivant), et l'autre vers les serveurs de mise à jour d'ESET (INET)

- Créez une tâche de mise à jour ou modifiez une tâche existante à l'aide du Planificateur (***Outils > Planificateur*** dans la fenêtre principale du programme ESET Smart Security ou ESET NOD32 Antivirus).

La configuration peut être effectuée directement sur les portables ou à distance à l'aide de l'éditeur de configuration d'ESET. Elle peut être appliquée en cours d'installation ou ultérieurement en tant que tâche de configuration.

Pour créer des profils dans l'éditeur de configuration d'ESET, cliquez avec le bouton droit sur la branche ***Mise à jour***, puis, dans le menu contextuel, sélectionnez ***Nouveau profil***.

[11] Vous pouvez extraire des fichiers de configuration .xml directement à partir de l'interface du programme ESET Smart Security.

Le résultat des modifications doit ressembler à celui présenté ci-dessous :

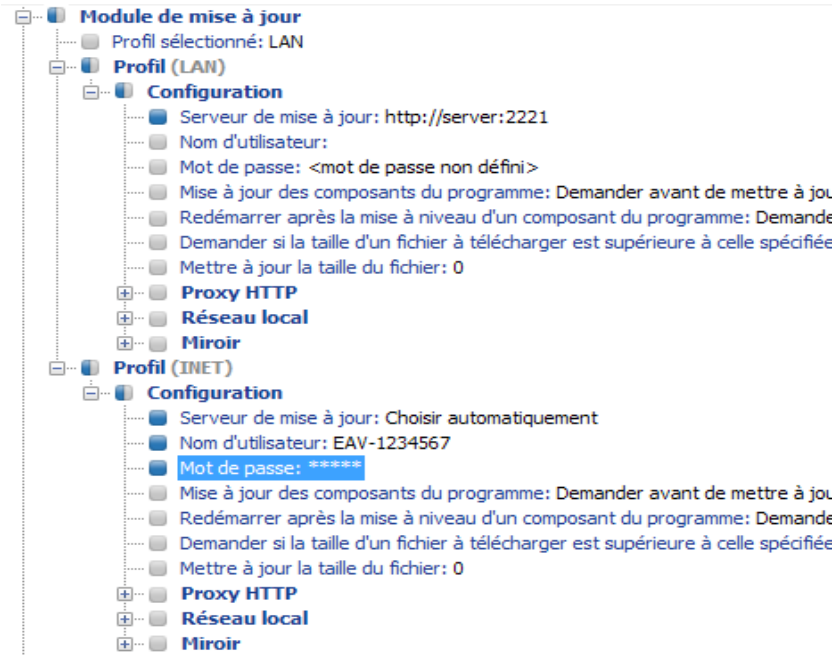


Figure 9-5

Le profil LAN télécharge les mises à jour à partir du serveur miroir local de la société (http://server:2221), tandis que le profil INET se connecte aux serveurs d'ESET (***Choisir automatiquement***). Ensuite, définissez une tâche de mise à jour exécutant successivement chaque profil de mise à jour. Pour ce faire, dans l'éditeur de configuration d'ESET, accédez à ***ESET Smart Security, ESET NOD32 Antivirus*** > ***Noyau*** > ***Configuration*** > ***Planificateur/Programmateur***. Cliquez sur le bouton **Edition** pour afficher la fenêtre **Tâches planifiées**.

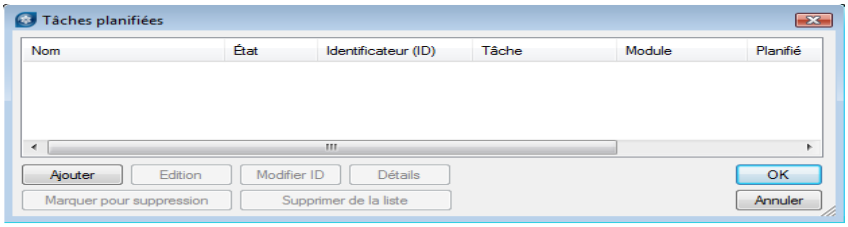


Figure 9-6

Pour créer une tâche, cliquez sur ***Ajouter***. Dans le menu déroulant **Tâche planifiée**, sélectionnez ***Mise à jour***, puis cliquez sur **Suivant**. Entrez le **nom de tâche** (p. ex., « mise à jour combinée »), sélectionnez **Toutes les 60 minutes**, puis procédez à la sélection des profils principal et secondaire.

Si les stations de travail portables doivent d'abord contacter le serveur Miroir, le profil principal doit être défini sur LAN et le profil secondaire sur INET. Le profil INET n'est appliqué qu'en cas d'échec de la mise à jour à partir du LAN.

Recommandation : Exportez la configuration .xml actuelle d'un client (pour plus d'informations, consultez la section 9.3), puis apportez les modifications précitées dans le fichier .xml exporté. Cela évite toute duplication entre le Planificateur et des profils non opérationnels.

9.5 Installation de produits tiers à l'aide d'ERA

Outre l'installation à distance de produits ESET, la console ESET Remote Administrator est capable d'installer d'autres programmes. La seule exigence est que le package d'installation personnalisée soit au format .msi. Vous pouvez effectuer l'installation à distance de packages personnalisés à l'aide d'un processus très similaire à celui décrit dans la section 4.2, « Installation à distance ».

La principale différence réside dans le processus de création du package qui se déroule comme suit :

- Dans ERAC, cliquez sur l'onglet ***Installation à distance***.
- Cliquez sur le bouton ***Packages...***.
- Dans le menu déroulant ***Type de package, sélectionnez Package personnalisé.***
- Cliquez sur ***Ajouter...***, sur ***Ajouter un fichier***, puis sélectionnez le package msi souhaité.
- Dans le menu déroulant ***Fichier d'entrée du package***, sélectionnez le fichier, puis cliquez sur ***Créer***.
- Une fois de retour dans la fenêtre d'origine, vous pouvez spécifier des paramètres de ligne de commande pour le fichier .msi. Les paramètres sont les mêmes que pour une installation locale du package concerné.
- Cliquez sur ***Enregistrer sous...*** pour enregistrer le package.
- Pour quitter l'éditeur de package d'installation, cliquez sur ***Fermer***.

Vous pouvez distribuer le nouveau package personnalisé à des stations de travail client en procédant de la même manière que pour les installations à distance décrites dans les chapitres précédents. Une installation poussée à distance, par ouverture de session ou Email, envoie le package aux stations de travail cibles. À partir du moment où le package est exécuté, l'installation est gérée par le service Microsoft Windows Installer.