ESET

REMOTE ADMINISTRATOR 5

Manuel d'installation et guide de l'utilisateur

Cliquez ici pour télécharger la dernière version de ce document

ESET **REMOTE ADMINISTRATOR 5**

Assistance à la clientèle internationale : www.eset.eu/support
Assistance à la clientèle Amérique du Nord : www.eset.com/support

RÉV. 5/19/2014

Table des matières

1. Introduction

La solution ESET Remote Administrator (ERA) est une application permettant de gérer des produits d'ESET dans un environnement de 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 aucune autre forme de protection contre le code malveillant. ERA dépend de la présence sur les stations de travail ou les serveurs d'une solution de sécurité ESET telle que ESET NOD32 Antivirus ou ESET Smart Security.

Pour effectuer le déploiement complet d'un portefeuille de solutions de sécurité ESET, procédez comme suit :

- Installation du ERA Server (ERAS),
- Installation de la ERA Console (ERAC),
- Installation sur des ordinateurs clients (ESET NOD32 Antivirus, ESET Smart Security, 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 Nouveautés

ESET Remote Administrator version 5.0

Nouvelles fonctionnalités

- Tableau de bord Web pour les administrateurs : vue d'ensemble complète des rapports dans votre navigateur Web
- Installation à distance ; nouvelle conception
- Fonctions de protection : nouvelle tâche pour la gestion des fonctions de protection sur les clients
- Exécution de la tâche planifiée : nouvelle tâche permettant de déclencher immédiatement une tâche planifiée sur un client
- Gestionnaire des utilisateurs : outil de gestion des comptes et des mots de passe pour l'accès à la console
- Onglet HIPS : informations sur les événements HIPS sur les clients
- Onglet Contrôle Web : informations sur les événements Contrôle Web sur les clients
- Onglet Contrôle de périphérique : informations sur les événements Contrôle de périphérique sur les clients
- Onglet Antispam : informations sur les événements liés au spam sur les clients
- Onglet Liste grise : informations sur les événements Liste grise sur les clients
- Recherche d'ordinateurs sur le réseau : nouvelles tâches de recherche et nouveau design
- Prise en charge de l'installation sur les versions ERA antérieures (4.x, 3.x), y compris la migration de données
- Rapports : nouveaux rapports, nouvelle conception, prise en charge des tableaux de bord Web

ESET Remote Administrator Version 4.0

- Prise en charge d'ESET Smart Security/ESET NOD32 Antivirus 4.2
- Prise en charge d'ESET Mail Security 4 for Microsoft Exchange Server
- Prise en charge d'ESET Mobile Security

Nouvelles fonctionnalités

- Installation à distance ; nouvelle conception
- Gestion de groupes ; nouvelle conception (groupes statiques, groupes paramétriques, synchronisation améliorée d'Active Directory)
- Filtre ; fonctionnalité améliorée (filtres de stratégie, filtres de groupes statiques et paramétriques)
- Stratégies ; nouveaux paramètres dans les règles de stratégie (prise en charge des groupes paramétriques), importation/exportation de stratégies et de règles de stratégie, fusion de tâches de planificateur, Assistant Règles de stratégie
- Notifications ; prise en charge des groupes paramétriques + plusieurs améliorations mineures
- Vue centralisée de la quarantaine des clients (pour clients ESS/EAV v4 et versions ultérieures)
- Rapports ; prise en charge des groupes statiques et paramétriques, nouveaux types de rapports (journal mobile, quarantaine, pare-feu), nouveaux modèles
- Assistant Fusion des règles de pare-feu ; Assistant pour fusionner les règles créées en mode d'apprentissage
- Authentification Windows/domaine des utilisateurs ERA Console
- Prise en charge du cluster passif Windows
- Prise en charge de l'installation sur les versions ERA antérieures (3.x, 2.x, 1.x), y compris la migration de données
- Chiffrement des communications selon AES-256

Nouveau Éditeur de configuration d'ESET

- Prise en charge des nouveaux produits de sécurité ESET
- Prise en charge des nouvelles fonctionnalités d'ERA Server
- Fichiers de licence compressés
- Possibilité d'ajouter des tâches planifiées prédéfinies

ESET Remote Administrator Version 3.0

- Prise en charge des produits de sécurité ESET 4.x
- Prise en charge des solutions Linux

Nouvelles fonctionnalités

- Gestion de stratégies
- Gestionnaire de notifications
- Accès en lecture seule à la console
- Prise en charge d'ESET SysInspector
- Modularité améliorée du transfert de données
- Suppression des clients répliqués
- Fusion de clés de licence/Gestionnaire de licences
- Miroir pour ESET NOD32 Antivirus 2.x
- Nouvelle configuration
- Option de filtrage basée sur le domaine ajoutée dans la recherche d'ordinateurs non enregistrés
- Compression des journaux du serveur (zip)
- Bogues mineurs corrigés et plusieurs fonctionnalités mineures ajoutées
- CD de récupération

Amélioration du serveur interne

- Prise en charge de bases de données supplémentaires (MS Access, MS SQL Server, Oracle, MySQL)

Nouveauté : Éditeur de configuration d'ESET

- Prise en charge des produits de sécurité ESET 4.x

ESET Remote Administrator Version 2.0

- Prise en charge des nouveaux produits de sécurité ESET version 3 (ESET Smart Security, ESET NOD32 Antivirus).
- Nouveaux journaux (nouvelles colonnes, journaux du pare-feu personnel ESET)
- Nouvelles informations d'état du client pour les clients version 3 (État de la protection, Fonctionnalités de protection, Informations système)
- Tâches (Configuration, Mettre à jour maintenant, Analyse à la demande, Tâche interactive)
- Prend encore en charge les produits NOD32 version 2.x

Nouvelles fonctionnalités

- Identification du client étendue (adresse MAC ajoutée)
- Installation à distance étendue (prise en charge de packages msi et personnalisés)

- Amélioration de la sécurité (possibilité de chiffrement de tous les nouveaux clients du serveur)
- Améliorations des performances (compression dans le protocole de communication)
- Ajout du transfert de données ESET Live Grid via ERA Server
- Amélioration de l'interface utilisateur graphique (nouveaux graphiques, coloration de l'état améliorée, filtres étendus, boîtes de dialogue redimensionnables)
- Nouveau modèle de rapport (configuration ESS)
- Surveillance des performances du serveur (données, requêtes)
- Fonctionnalité de mise à jour dans ERA Server (autorise la mise à jour d'informations importantes)
- Fonctionnalité de miroir dans ERA Server
- Installation à distance étendue (prise en charge des packages msi et personnalisés, possibilité d'installation à distance d'ERA, diagnostic)

Amélioration du serveur interne

- Amélioration de la réplication (priorité de réplication, meilleure réplication multiniveau)
- Nouvelle structure de base de données
- Nouvelle structure de répertoires
- Améliorations de la sécurité interne

Nouveauté : Éditeur de configuration d'ESET

- Prise en charge des produits de sécurité ESET versions 2 et 3
- Possibilité de configurer ERA Server
- Autres nouvelles fonctionnalités mineures (recherche, paramètres personnalisés)

Nouveau programme d'installation (MSI)

- Migration de base de données de versions précédentes
- Nouvelle documentation (aide, manuel)

1.2 Architecture du programme

Techniquement, ESET Remote Administrator comprend deux composants distincts : le ERA Server (ERAS) et la ERA Console (ERAC). Vous pouvez exécuter un nombre illimité de ERA Server et de consoles au sein de votre réseau car le contrat de licence ne prévoit aucune limite à cet égard. La seule limite imposée porte sur le nombre total de clients que votre installation d'ERA peut administrer.

ERA Server (ERAS)

Le composant serveur d'ERA s'exécute comme service sous les systèmes d'exploitation de technologie Microsoft Windows® NT suivants : 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, y compris les tâches de configuration, les requêtes d'installation à distance, etc., sont créées via la ERA Console (ERAC). ERAS est un point de rencontre entre l'ERAC et les ordinateurs client, un lieu où toutes les informations sont traitées, maintenues ou modifiées avant d'être transférées aux clients ou à l'ERAC.

ERA Console (ERAC)

ERAC est le composant client 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 saisir un nom d'ERAS. Au démarrage, la console sera automatiquement connectée à ce serveur. ERAC peut également être configurée après l'installation.

2. Installation de ERA Server et de la ERA Console

2.1 Configuration requise

ERAS fonctionne en tant que service. Il a donc besoin d'un système d'exploitation de technologie Microsoft Windows NT (2000, XP, 2003, Vista, 7 ou 2008). Bien que ERAS n'a pas besoin de Microsoft Windows Server Edition pour fonctionner, il est conseillé d'installer ERAS sur un système d'exploitation de technologie serveur pour garantir un bon fonctionnement. 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 ERA Console ;
- d'autres instances d'ERAS (en cas de réplication).

REMARQUE : ESET Remote Administrator 5 prend en charge l'installation sur des versions antérieures 18, y compris la migration des données.

2.1.1 Configuration logicielle

ERA Server

Systèmes d'exploitation 32 bits : Windows 2000 et versions ultérieures (voir la **remarque**)

Systèmes d'exploitation 64 bits : Windows XP et suivants

Bases de données :	Microsoft Access (intégré) Microsoft SQL Server 2005 et versions ultérieures MySQL 5.0 et versions ultérieures ORACLE 9i et versions ultérieures
Windows Installer :	2.0 et versions ultérieures
Tableau de bord Web :	Internet Explorer 7.0 et versions suivantes Mozilla Firefox 3.6 et versions suivantes Google Chrome 9 et versions suivantes
Serveur HTTP :	Identique aux exigences d'ERA Server, mais nécessite le Service Pack 2 ou ultérieur sur Windows XP

ERA Console

Systèmes d'exploitation 32 bits : Windows 2000 et versions ultérieures (voir la **remarque**)

Systèmes d'exploitation 64 bits :	Windows XP et suivants
Windows Installer :	2.0 et versions ultérieures
Internet Explorer :	7.0 et versions ultérieures

Remarque :

- ERA Console n'est pas pris en charge sur Microsoft Windows Server Core 2008 et Microsoft Windows Server Core 2012. ERA Server est pris en charge sur ces systèmes d'exploitation, mais ne prend pas en charge l'intégration avec les bases de données Microsoft Access.
- Pour démarrer ERA Console, l'éditeur de configuration ESET et l'outil de maintenance ERA sur Windows 2000, le fichier *gdiplus.dll* doit être présent dans votre système. Vous pouvez télécharger ce fichier ici. Extrayez le fichier du package d'installation et copiez-le dans le répertoire *C:\WINNT\system32*.
- Le rôle de serveur HTTPS n'est pas pris en charge sous Windows 2000 ; les fonctions de tableau de bord et de miroir ne sont donc pas opérationnelles en mode HTTPS sur ce système d'exploitation. Pour utiliser le tableau de bord sur un serveur Windows 2000, modifiez les paramètres de manière à ce que le tableau de bord ne s'exécute plus par défaut en mode HTTPS.

- L'installation à distance de produits de sécurité Linux/MAC n'est pas pris en charge sur Windows 2000.
- Pour certains systèmes d'exploitation, vous devrez mettre à jour les certificats racine de confiance avant d'effectuer une installation poussée. Vous pouvez mettre à jour ces certificats en exécutant le service Windows Update ou en important les dernières versions manuellement.
- Si vous utilisez un compte administrateur pour configurer l'accès SMTP dans **Outils** > **Options du serveur** > **Autres paramètres** (pour IIS ou Exchange), la messagerie sortante risque de ne pas fonctionner.
- Certaines fonctions (RDP, arrêt) exécutées depuis **Actions réseau**(option décrite dans la section Onglet Clients 29) ne sont pas disponibles sur Windows 2000.

2.1.2 Exigences de performances

Les performances du serveur peuvent varier en fonction des paramètres suivants :

1. Base de données utilisée

- Base de données MS Access, installée avec le serveur par défaut. Cette solution est recommandée pour plusieurs centaines de clients. Toutefois, la taille de la base de données est limitée à 2 Go. Par conséquent, il faudra activer les nettoyages sur le serveur et définir un intervalle (sous **Outils** > **Options du serveur** > **Maintenance du serveur**) pour la suppression des anciennes données.
- Les autres bases de données (MySQL, MSSQL, ORACLE) requièrent une installation séparée, mais cela peut améliorer les performances du serveur. Il est primordial d'utiliser le matériel adéquat pour chaque moteur de base de données (principalement ORACLE) selon les recommandations techniques du distributeur.
- Si vous choisissez ORACLE pour votre solution de base de données, vous devez définir un nombre de curseur supérieur à la valeur **Nombre maximum de connexions actives** (sous **Outils** > **Options du serveur** > **Paramètres avancés** > **Modifier les paramètres avancés** > **Paramètres avancés** ; la valeur par défaut est 500). Le nombre définitif de curseurs doit tenir compte du nombre de serveurs de niveau inférieur (en cas d'utilisation de la réplication) et de curseurs utilisés par d'autres applications qui accèdent au moteur de base de données.
- En général, les performances du serveur sont meilleures en cas d'utilisation de bases de données externes (à savoir, installées sur une autre machine).

2. Paramètres d'intervalle de connexion du client

- L'intervalle de connexion du client est de 10 minutes par défaut dans ESET Smart Security / ESET NOD32 Antivirus version 4.2 et supérieures. Si l'état du client doit être mis à jour plus ou moins fréquemment par rapport à l'intervalle par défaut, vous pouvez modifier cette configuration. N'oubliez pas qu'un intervalle de connexion des clients plus court aura des incidences sur les performances serveur.

3. Nombre moyen d'événements signalés par les clients par connexion

- Toute information envoyée par un client vers un serveur est reprise sous cet événement en particulier (par exemple, journal des menaces, journal des événements, journal d'analyse, modification de la configuration). Ce paramètre ne peut pas être directement modifié mais il peut être altéré si d'autres paramètres qui lui sont pertinents sont changés. Par exemple, dans la configuration avancée du serveur (sous **Outils** > **Options du serveur** > **Maintenance du serveur**) vous pouvez définir le nombre maximum de journaux qui peuvent être acceptés par le serveur (ce paramètre inclut les clients qui se connectent directement ainsi que les clients répliqués). Dans un contexte de fonctionnement régulier, la moyenne à long terme peut être estimée à 1 événement toutes les 4 heures par client.

4. Matériel utilisé

Pour **les petites installations (moins de 1 000 clients qui se connectent à ERA Server) :**

- Type de processeur – Processeur compatible Pentium IV, 2 GHz ou plus
- RAM - 2 Go
- Réseau - 1 Gbit

Pour **les installations moyennes (entre 1 000 et 4 000 clients qui se connectent à ERA Server)** il est recommandé de répartir l'installation sur deux ordinateurs :

ERA Server :

- Type de processeur – Processeur compatible Pentium IV, 2 GHz ou plus
- RAM - 2 Go
- Réseau - 1 Gbit

Serveur de base de données :

- Type de processeur – Processeur compatible Pentium IV, 2 GHz ou plus
- RAM - 2 Go
- Réseau - 1 Gbit

Vous pouvez également installer ERA Server et la base de données sur un même ordinateur :

- Type de processeur – Processeur compatible Pentium IV, multicœur, 3 GHz ou plus
- RAM - 4 Go
- Réseau - 1 Gbit
- Disque dur – Raid 0 ou disque SSD, ou les deux

REMARQUE :: Dans ce cas (ERA Server et base de données installés sur le même ordinateur), il n'est pas recommandé d'utiliser une base de données MS Access, car sa taille limitée à 2 Go suppose des nettoyages réguliers. N'oubliez pas non plus que la base de données MS SQL Express est limitée à 4 Go.

Pour **les installations de grande taille (entre 4 000 et 10 000 clients qui se connectent à ERA Server)** il est recommandé de répartir les installations sur 2 ordinateurs et d'utiliser une base de données MS SQL ou Oracle :

ERA Server :

- Type de processeur – Processeur compatible Pentium IV, multicœur, 3 GHz ou plus
- RAM - 4 Go
- Réseau - 1 Gbit

Serveur de base de données :

- Type de processeur – Processeur compatible Pentium IV, multicœur, 3 GHz ou plus
- RAM - 4 Go
- Réseau - 1 Gbit
- Disque dur – Raid 0 ou disque SSD, ou les deux

les installations de très grande taille (entre 10 000 et 20 000 clients sur un serveur ERA Server) il est recommandé de répartir les installations sur 2 ordinateurs et d'utiliser une base de données MS SQL ou Oracle :

ERA Server :

- Type de processeur – Processeur compatible Pentium IV, multicœur, 3 GHz ou plus
- RAM - 8 Go
- Réseau - 1 Gbit
- Disque dur – Raid 0 ou disque SSD, ou les deux

Serveur de base de données :

- Type de processeur – Processeur compatible Pentium IV, multicœur, 3 GHz ou plus
- RAM - 4 Go
- Réseau - 1 Gbit
- Disque dur – Raid 0 ou disque SSD, ou les deux

REMARQUE :: Toutes les configurations matérielles répertoriées ci-dessus représentent les conditions minimales requises pour l'exécution d'ERA. Il est recommandé d'utiliser des configurations plus puissantes pour obtenir de meilleures performances. Il est vivement conseillé d'utiliser la configuration matérielle minimale recommandée pour le système d'exploitation du serveur, en tenant compte du nombre de clients à servir. Pour obtenir des informations supplémentaires, consultez le chapitre Types de base de données pris en charge par ERA Server 17.

Surcharge

Si le serveur est surchargé (par exemple, nous connectons 20 000 clients à un serveur qui ne peut accepter que 10 000 clients toutes les 10 minutes), il passera certains des clients connectés. En moyenne, une connexion client sur deux sera traitée, comme si l'intervalle de connexion du client était de 20 minutes au lieu de 10. Chaque déni de service sera consigné de la manière suivante : "*<SERVERMGR_WARNING> ServerThread: nombre maximum de threads pour les connexions actives a été atteint (500), le serveur passera cette connexion*". Des dénis de service peuvent également se produire lors de surcharges temporaires du serveur.

Vous pouvez modifier la valeur du paramètre **Nombre maximum de connexions actives** (500 par défaut) dans les paramètres avancés du serveur, mais cette opération est à réserver aux cas exceptionnels (par exemple, pour la résolution de problèmes particuliers). En cas de surplus de ressources système et de performances du moteur de base de données, vous pouvez utiliser ce paramètre pour adapter les performances globales du serveur.

Transfert de données via un réseau

Pendant le fonctionnement standard d'un serveur, on estime qu'une client qui se connecte toutes les 10 minutes signalera 0,04 événement par connexion, soit 1 événement signalé toutes les 4 heures par client. Cela produira environ 2 Ko de trafic par connexion.

En cas d'épidémie de virus, lorsqu'un client signale 7 événements chaque fois qu'il se connecte, le trafic peut augmenter jusqu'à 240 Ko par connexion. Si vous utilisez la compression (par défaut), le poids des données transférées sera réduit d'environ 50 %, soit à peu près 120 Ko par connexion.

Les données portent sur les connexions client directes et ignorent les connexions répliquées. La réplication a lieu bien moins souvent et sert à envoyer de nouveaux événements depuis des serveurs de niveau inférieur. Les événements qui seront répliqués automatiquement et le niveau de détail peuvent être configurés dans les paramètres avancés du serveur (sous **Outils** > **Options du serveur** > **Paramètres avancés** > **Modifier les paramètres avancés** > **Réplication**). La section Maintenance du serveur permet de configurer le niveau maximum de journaux que le serveur de niveau supérieur acceptera. Ce paramètre s'applique aux clients qui se connectent directement et aux clients répliqués.

Exigences au niveau des capacités de stockage

L'installation neuve d'ESET Remote Administrator avec une base de données MS Access utilise jusqu'à 60 Mo sur le disque dur.

La majorité de l'espace de stockage est utilisée par les événements du client stockés dans la base de données et dans un référentiel sur le disque (le répertoire par défaut est *C:\Documents and Settings\All Users\Application Data\Eset\ESET Remote Administrator\Server*). ERA requiert au moins 5 % d'espace disponible sur le disque. Si ce minimum est dépassé, le serveur arrêtera de recevoir certains des événements des clients. Ce paramètre est accessible via **Outils** > **Option du serveur** > **Paramètres avancés** > **Modifier les paramètres avancés** > **Paramètres avancés** > **Utilisation d'espace disque maximale**. Il faut compter environ 10 Go d'espace disponible pour 1 000 clients en cas d'utilisation normale avec les paramètres de nettoyage par défaut (suppression d'événements de plus de 3 mois).

Étude de cas

Un serveur utilisant une base de données MS Access avec des clients qui se connectent toutes les 5 minutes et qui signalent en moyenne 7 événements (par exemple, journal des menaces, journal des événements, journal d'analyse, modification de la configuration, etc.) par connexion peut servir temporairement jusqu'à 3 000 clients. Ce scénario décrit une surcharge temporaire, par exemple la signalisation d'événements en cas d'épidémie de virus, etc.

Si le serveur utilise une base de données MySQL externe et que l'intervalle de connexion du client est de 10 minutes (donnant 0,02 événement par connexion), le nombre maximum de clients que le serveur sera en mesure de servir passe à 30 000. Un tel scénario démontre les performances optimales de la base de données avec des clients qui signalent un nombre relativement restreint d'événements.

Dans le cadre d'une utilisation normale, l'utilisation d'une base de données MS Access avec un intervalle de connexion de client de 10 minutes permet de servir un maximum de 10 000 clients.

2.1.3 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 autres communications sont effectuées à l'aide des processus natifs du système d'exploitation (p. ex., « NetBIOS sur TCP/IP »).

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

Pour que toutes les fonctionnalités du programme fonctionnent correctement, vérifiez que les ports réseau suivants sont ouverts :

Protocole	Port	Description
TCP	2224 (ERAS à l'écoute)	Communication entre l'agent *einstaller.exe* et ERAS durant une installation à distance
TCP	2225 (ERAS à l'écoute)	Communication entre le serveur HTTP du tableau de bord ESET et ERAS
TCP	2846 (ERAS à l'écoute)	réplication d'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).

Il est possible de modifier les ports prédéfinis 2221, 2222, 2223, 2224, 2225 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 du port du serveur HTTP. Vous pouvez modifier les ports 2222, 2223, 2224, 2225 et 2846 dans la section **Ports** de l'onglet Autres paramètres 106.

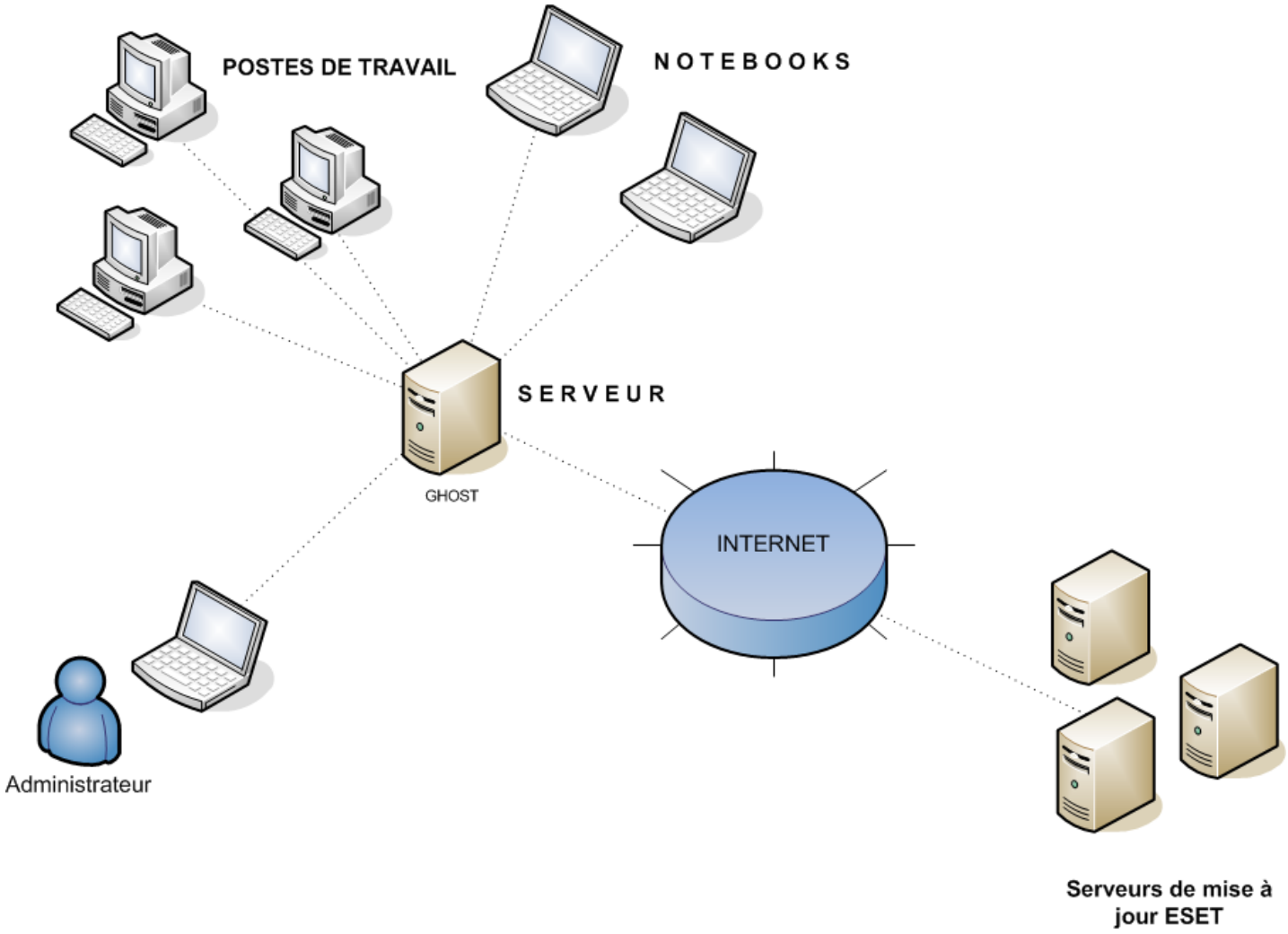
Vous pouvez également modifier les ports prédéfinis 2222, 2223, 2224 et 2846 en mode d'installation avancée (ERAS).

2.2 Guide d'installation de base

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

Un réseau de société est composé généralement d'un réseau local (LAN). Nous suggérons donc d'installer ERAS et un serveur Miroir. Le serveur Miroir peut être créé soit dans ERAS, soit dans ESET NOD32 Antivirus Business Edition/ESET Smart Security Business Edition.

Supposons que tous les clients sont des stations de travail et des portables Microsoft Windows 2000/XP/Vista/7 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 :



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 de ESET Remote Administrator :

ESET Remote Administrator - Serveur
ESET Remote Administrator - Console

Solutions client d'ESET :

ESET Endpoint Security
ESET Endpoint Antivirus
ESET Smart Security 4.x
ESET Smart Security 3.x
ESET NOD32 Antivirus 4.x
ESET NOD32 Antivirus 3.x
ESET NOD32 Antivirus 2.7

REMARQUE :: Ne téléchargez que les solutions client que vous utiliserez sur des stations de travail client.

2.2.3 Installation

2.2.3.1 installation du ERA Server

Installez ERAS sur le serveur nommé GHOST (voir l'exemple dans la section Vue d'ensemble de l'environnement 13). Commencez par sélectionner les composants à installer. Deux options sont disponibles : **ESET Remote Administrator Server** et **Serveur** de **tableau de bord** 38 **HTTP ESET**.

Les deux composants sont installés pour la plupart des applications. Vous pouvez choisir d'installer les deux composants sur des ordinateurs différents (par exemple, installer le serveur de tableau de bord HTTP ESET sur un ordinateur visible au public et installer ERAS sur un ordinateur accessible uniquement depuis un intranet local). Vous pouvez aussi décider de ne pas utiliser le serveur de tableau de bord HTTP ESET.

REMARQUE : Il est recommandé d'installer ERAS sur un ordinateur exécutant un système d'exploitation pour serveur.

REMARQUE : Le serveur de tableau de bord et le serveur de miroir font appel au même serveur HTTP, qui est installé automatiquement. Par conséquent, même si vous désélectionnez le serveur de tableau de bord au moment de l'installation, vous pouvez l'activer ultérieurement dans ESET Éditeur de configuration (**ERAC** > **Outils** > **Options du serveur** > **Paramètres avancés** > **Tableaux de bord** > **Utiliser le tableau de bord local**).

Après avoir choisi les composants voulus, sélectionnez le mode d'installation **par défaut** ou **avancée**.

- Si vous sélectionnez le **mode Par défaut**, le programme vous invite à insérer une clé de licence (fichier portant l'extension .lic ou .zip) qui autorise le fonctionnement du serveur 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 également passer à l'étape suivante et saisir les paramètres de mise à jour ultérieurement, en cochant la case à côté de **Définir les paramètres de mise à jour plus tard** et en cliquant sur **Suivant**.

- Le **mode d'installation avancée** vous permettra de configurer des paramètres d'installation 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, ou la valeur %COMPUTERNAME% de votre système d'exploitation ou l'adresse IP attribuée à l'ordinateur. Il s'agit de l'information essentielle pour l'exécution d'une installation à distance. Si aucun nom n'est défini pendant l'installation, le programme d'installation fournira automatiquement la valeur de la variable système %COMPUTERNAME%, ce qui suffit dans la plupart des cas. Il est également important de sélectionner la base de données dans laquelle les informations ERAS seront stockées. Pour obtenir des informations supplémentaires, consultez le chapitre Types de base de données pris en charge par le ERA Server 17.

REMARQUE : Lorsque le serveur ERAS est installé sur un système d'exploitation Windows 2000, il n'est pas recommandé d'utiliser de DNS. Utilisez plutôt la chaîne de connexion complète.

Important : Les stratégies de sécurité de Microsoft Windows limitent les autorisations des comptes des utilisateurs locaux. Vous risquez donc de ne pas pouvoir exécuter les opérations réseau connexes. Exécuter le service ERA sous un compte d'utilisateur local peut entraîner des problèmes d'installation poussée (par exemple, lors d'une installation à distance du domaine au groupe de travail). En cas d'utilisation de Windows Vista, Windows Server 2008 ou Windows 7,

il est conseillé d'exécuter le service ERA sous des comptes possédant des droits réseau suffisants. Vous pouvez désigner le compte d'utilisateur sous lequel vous souhaitez exécuter ERA dans le **mode d'installation avancée**.

Remarque: Malgré la prise en charge totale d'Unicode par ERA Server, le serveur convertit dans certains cas les caractères en caractères ANSI ou inversement (email ou nom d'ordinateur, par exemple). Dans ces cas-là, le paramètre de **langue pour programmes non-Unicode** doit être utilisé. Nous vous recommandons de modifier ce paramètre pour qu'il corresponde aux paramètres régionaux de l'environnement serveur, même si vous n'utilisez pas de version traduite d'ERA (si vous utilisez la version en anglais). Vous trouverez ce paramètre dans **Panneau de configuration** > **Options régionales et linguistiques**, dans l'onglet **Avancé**.

Par défaut, les composants du programme ERAS sont installés dans le répertoire 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 ce répertoire :

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

Une fois installé, ERAS se lance automatiquement. L'activité du service ERAS est enregistrée dans l'emplacement suivant :

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

Installation via la ligne de commande

ERAS peut être installé à l'aide des paramètres suivants de la ligne de commande :

/q : installation sans assistance. Aucune intervention de l'utilisateur n'est possible. Aucune boîte de dialogue n'apparaît.

/qb : aucune intervention de l'utilisateur n'est possible, mais l'avancement de l'installation est indiqué par une barre de progression.

Exemple : *era_server_nt32_ENU.msi /qb*

Les paramètres et la configuration de l'installation via la ligne de commande peuvent être complétés par le fichier « *cfg.xml* », le fichier de configuration *.xml* de l'administrateur qui doit se trouver dans le même dossier que le fichier d'installation *msi* d'ERA. Le fichier de configuration peut être créé dans Éditeur de configuration d'ESET et permet de configurer divers paramètres d'ERA. Consultez la section Éditeur de configuration d'ESET 50 pour plus d'informations.

2.2.3.1.1 Installation en mode cluster

Le scénario d'**installation avancée** permet également d'activer l'**installation en mode cluster**. Si l'installation en mode cluster est activée, il faudra désigner le chemin d'accès à un dossier de données partagé de cluster accessible par tous les nœuds du cluster (tous les nœuds doivent avoir un accès en lecture/écriture à ce dossier). Il peut s'agir d'un disque quorum ou d'un dossier partagé UNC. En cas d'utilisation d'un dossier partagé, il faut activer le partage pour les **ordinateurs** dans les propriétés du dossier partagé. Le nom du nœud du cluster doit ensuite être ajouté aux **Autorisations de partage** avec tous les privilèges.

REMARQUE :: L'utilisation d'une adresse IP n'est pas recommandée pour définir un dossier partagé pour le cluster.

Il faut installer le ERA Server individuellement sur chaque nœud du cluster. Après chaque installation ERA Server, le démarrage automatique du service ERA doit être défini sur manuel. Lorsque ERA Server est installé sur tous les nœuds, créez le service générique (era_server). Le service générique doit dépendre de la ressource de nom du réseau dans la console Cluster Administrator.

En cas d'utilisation d'une base de données autre que la base de données MS Access intégrée, il faut bien veiller à ce que tous les nœuds du serveur ERA Server se connectent à la même base de données. Au cours de l'étape suivante, il est important de définir le nom du nœud de cluster où ERA sera installé en tant que nom de serveur.

Important : il faut configurer le service ESET Remote Administrator Server (ERA_SERVER) en tant que service générique du cluster dans la console Cluster Administrator.

Désinstallation

Si vous envisagez de désinstaller ERA Server, le groupe de clusters doit être en ligne pour que la désinstallation s'effectue correctement :

1) Arrêtez le cluster en désactivant l'un de ses nœuds.

2) Laissez la reprise s'effectuer pour vérifier que l'autre ou les autres nœuds fonctionnent.

3) Désinstallez ESET Remote Administrator du nœud désactivé.

4) Redémarrez le nœud.

5) Reliez le nœud.

6) Répétez les étapes ci-dessus pour chaque nœud supplémentaire du cluster.

Mise à niveau d'ERA installé en mode cluster

Pour la réinstallation en mode cluster, il est nécessaire de mettre le groupe de service ERA de cluster hors ligne en sélectionnant **Mettre hors ligne** dans la console d'administration de cluster. Réinstallez ensuite ERA sur tous les nœuds du cluster et remettez en ligne le groupe du service ERA de cluster.

2.2.3.2 installation du ERA Console

Installez la ESET Remote Administrator Console sur le PC/portable de l'administrateur. À la fin de l'installation en mode Avancé, saisissez le nom du ERA Server (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 vérifiez la connexion à ERAS. Par défaut, aucun mot de passe n'est requis pour se connecter à un ERA Server (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 de connexion à un ERA Server, cliquez sur **Fichier** > **Modification du mot de passe...**, puis modifiez le Mot de passe pour la console en cliquant sur le bouton **Modifier....**.

REMARQUE : L'administrateur peut indiquer un compte utilisateur et un mot de passe avec accès à la console ESET Remote Administrator Console. Il peut aussi préciser le niveau d'accès. Pour plus d'informations, consultez le chapitre Gestionnaire des utilisateurs 95. La console ERAC doit être installée sur l'ordinateur à partir duquel vous voulez accéder au serveur ERAS avec le compte défini dans le Gestionnaire des utilisateurs.

2.2.3.3 Miroir

Vous pouvez utiliser la ERA Console pour activer le serveur de mise à jour du réseau local, appelé le Miroir dans le ERA Server. Ce serveur sert ensuite à mettre à jour les stations de travail du 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 Console au serveur ERA Server en cliquant sur Fichier > Connecter.

2) Dans la console ERA Console, 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 le 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). Conservez AUCUNE comme valeur d'authentification.

5) Cliquez sur l'onglet Paramètres avancés et cliquez sur Modifier les paramètres avancés. Dans l'arborescence de configuration avancée, accédez à ERA Server > Configuration > Miroir > Créer un miroir pour les composants du programme sélectionnés. Cliquez sur Modifier sur le côté droit, puis sélectionnez les composants du 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 le chapitre Activation et configuration du Miroir 105

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

Par défaut, le programme utilise le moteur Microsoft Access (base de données Jet). ERAS 5.0 prend également en charge les bases de données suivantes :

- Microsoft SQL Server 2005 et versions ultérieures
- MySQL 5.0 et versions ultérieures
- Oracle 9i et versions ultérieures

Vous pouvez sélectionner le type de base de données durant l'installation avancée d'ERAS. Après l'installation, il n'est pas possible de changer le type de base de données directement depuis ERA, toutefois, vous pouvez le faire à l'aide d' ERA Maintenance Tool 130.

REMARQUE :

- la base de données Microsoft Access n'est pas prise en charge sur Windows Server 2008 Core.
- Le volume de la base de données SQL Server Express est limité à 4 Go.
- Le volume de la base de données Microsoft Access est limité à 2 Go.
- Lors de l'utilisation de MySQL sur Microsoft Windows 2000, il est recommandé d'utiliser le pilote ODBC version 5.1.8 ou ultérieure afin d'établir la connexion à la base de données 18.

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.

Chaînes de classement

Le tri sera réalisé selon les paramètres par défaut de chaque base de données. Il faut activer la fonction de CASE IGNORÉE (CI).

Pour activer :

- Pour MS SQL et MySQL, il faut configurer un COLLATE avec l'option CI activée
- Pour ORACLE, il faut configurer un NLS_SORT avec l'option CI activée
- Pour MS Access, aucune action n'est requise car l'option CI est déjà activée

Jeu de caractères

Il est important d'utiliser le jeu de caractères UNICODE (UTF-8 est recommandé), surtout lorsque les clients ont des locales spéciales ou si l'ERA lui-même fonctionne dans une version localisée. S'il n'y a pas de plan pour la réplication et si tous les clients se connectent au même serveur, vous pouvez utiliser le jeu de caractères pour la locale de l'ERA que vous voulez installer.

MARS (Multiple Active Result Sets)

En cas d'utilisation d'une base de données MS SQL, vous aurez besoin d'un lecteur OBDC avec prise en charge de MARS pour un fonctionnement sans problème. Dans le cas contraire, le serveur fonctionnera moins efficacement et consignera le message d'erreur suivant dans le journal du serveur :

Database connection problem. It is strongly recommended to use odbc driver that supports multiple active result sets (MARS). The server will continue to run but the database communication may be slower. See the documentation or contact ESET support for more information.

Si le problème se produit avec une base de données autre que MS SQL, le serveur consigne le message suivant dans le journal et arrête :

Database connection problem. Updating the odbc driver may help. You can also contact ESET support for more information.

Pilotes sans prise en charge de MARS :

- SQLSRV32.DLL (2000.85.1117.00)

- SQLSRV32.DLL (6.0.6001.18000) - repris en mode natif dans Windows Vista et Windows Server 2008

Pilote natif avec prise en charge de MARS :

- SQLNCLI.DLL (2005.90.1399.00)

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 saisissez *odbcad32.exe*).

   Exemple de connexion DSN :
   DSN =ERASqlServer

   Important : l'utilisation de *System DSN* est recommandé pour que l'ERA fonctionne correctement.

Important : Sur un système d'exploitation 64 bits, le fichier *odbcad32.exe* doit être exécuté depuis le dossier *%SystemRoot%\SysWOW64*.

Pour que l'installation sous MSSQL avec authentification Windows/Domaine s'effectue correctement, veillez à utiliser un format DSN lors de la saisie de la chaîne de connexion.

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

   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

   Cliquez ensuite sur **Définir** et spécifiez le **nom d'utilisateur** et le **mot de passe** pour la connexion. Les connexions de base de données Oracle et MS SQL Server nécessitent également un **nom de schéma**.

   Cliquez sur **Tester la connexion** pour vérifier la connexion au serveur de base de données.

REMARQUE : nous vous recommandons d'utiliser l'authentification du serveur de base de données au lieu de l'authentification Windows/Domaine.

2.2.3.5 Installation sur des versions antérieures

ESET Remote Administrator 5 prend en charge de l'installation sur les versions antérieures, y compris la migration de données. Pour effectuer la mise à niveau d'ERA version 1.x ou 2.x, il est recommandé de commencer par migrer les données vers une installation 4.x, puis d'installer la version 5.x afin de conserver les données.

REMARQUE :: Il est recommandé de n'effectuer la réinstallation que si aucun client n'est connecté, car le service ERA Server est arrêté et toutes les connexions sont terminées pendant la réinstallation. La migration de la base de données peut être effectuée avant ou après la réinstallation (reportez-vous au chapitre Transfert de base de données 131 pour plus d'informations).

- **Installation d'ERA Server** :

1. Téléchargez le fichier d'installation sur votre serveur. Double-cliquez sur le fichier du programme d'installation pour commencer l'installation.

2. Sélectionnez l'installation standard ou avancée, comme vous le faites pour une installation neuve d'ERA Server 14.

- **Installation standard** : vous êtes invité à fournir votre fichier de clé de licence (*.lic), les mots de passe et les données de mise à jour. Deux modes de migration sont disponibles : **Importer uniquement la configuration** crée des tables vides dans une nouvelle base de données et **Importation complète** importe toutes les données de la base de données. La sélection de l'option **Créer une copie de sauvegarde de la base de données actuelle** (valeur par défaut) permet de créer une sauvegarde avant toute modification de la base de données. L'option **Activer le nettoyage automatique par défaut des anciens enregistrements** peut être sélectionnée pour améliorer la maintenance de la base de données.

- **Installation avancée** : vous êtes invité à indiquer votre fichier de clé de licence (*.lic), le compte utilisé pour exécuter le service ERA Server, les ports utilisés pour la communication, les mots de passe et les données de mise à jour, les paramètres de serveur SMTP (facultatif), les paramètres de journalisation 97 et ceux de migration de la base de données (décrite dans la section **Installation standard** ci-dessus). Pendant l'installation avancée, le système vous demande si vous souhaitez migrer d'anciennes règles (bureau Windows v3 et v4) vers de nouvelles règles (bureau Windows v5). La migration est effectuée à l'aide des paramètres par défaut ; si vous souhaitez configurer la migration, il est recommandé d'utiliser l'assistant de migration de règles 74 une fois la mise à niveau effectuée.

REMARQUE : Si le programme d'installation trouve des tables existantes dans la base de données courante, une invite s'affiche. Pour remplacer le contenu d'une table existante, cliquez sur **Remplacer** (***avertissement :*** cette commande supprime le contenu des tables et remplace leur structure !). Cliquez sur **Ignorer** pour laisser les tables intactes. Dans certaines conditions, le fait de cliquer sur **Ignorer** peut entraîner des erreurs d'incohérence de base de données, en particulier lorsque des tables sont endommagées ou incompatibles avec la version actuelle.

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

- **Installation d'ERA Console** :

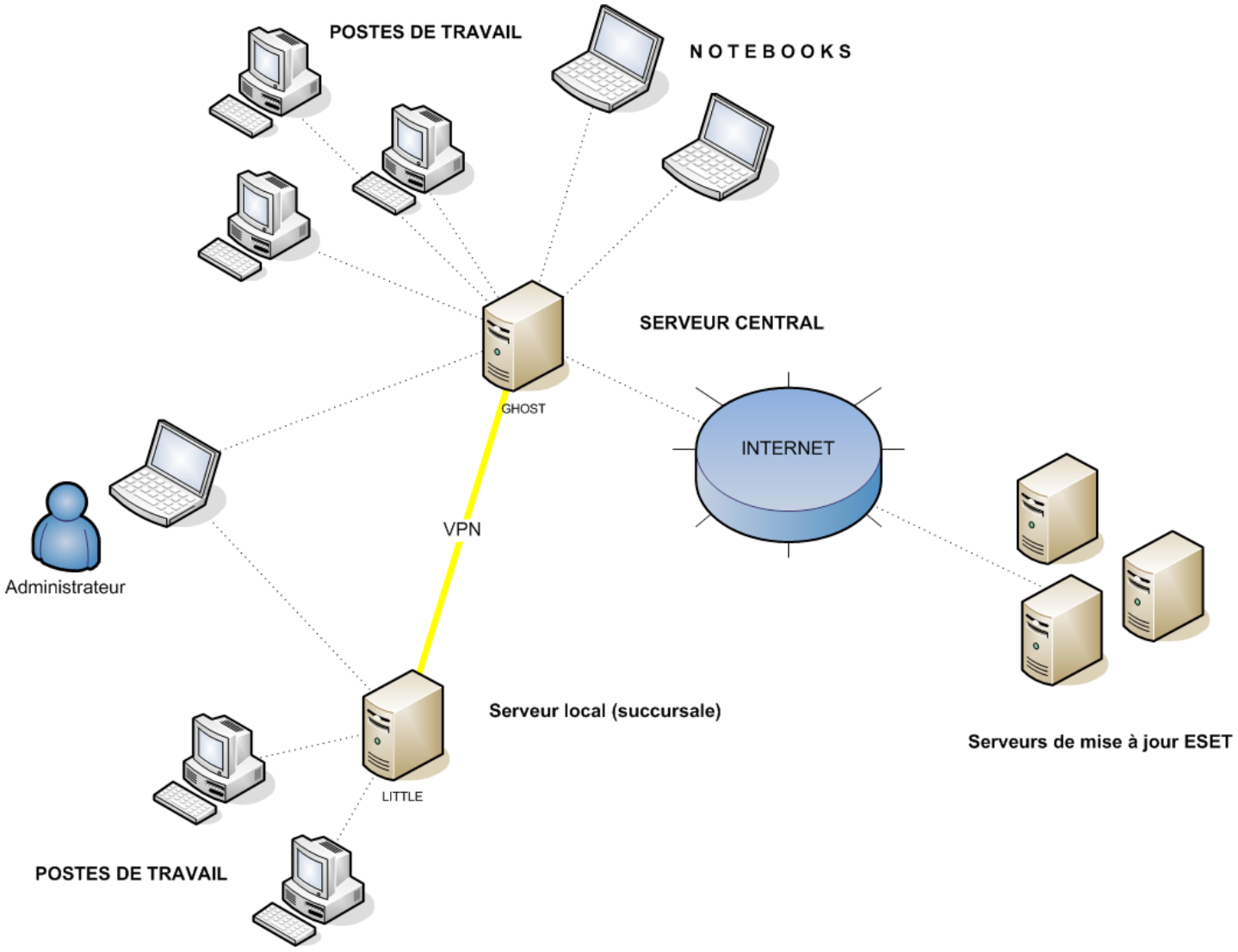
1. Téléchargez le fichier d'installation sur votre serveur. Double-cliquez sur le fichier d'installation pour commencer l'installation.

2. Suivez la procédure indiquée au chapitre Installation d'ERA Console 16.

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 ERA Server sur LITTLE pour créer un environnement plus convivial et réduire le volume des données transférées.

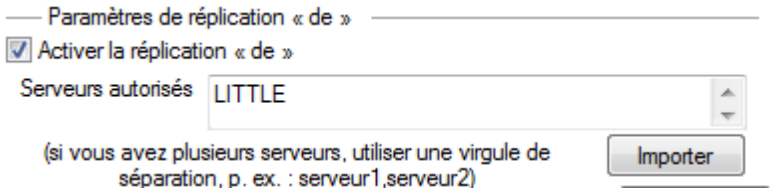


2.3.2 Installation

2.3.2.1 Installation au siège central

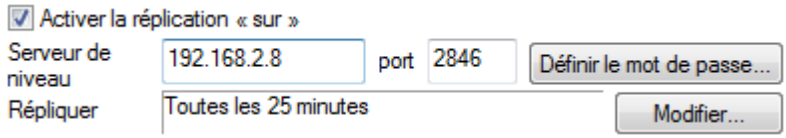
Les installations d'ERAS, d'ERAC et des stations de travail client sont très similaires au scénario précédent. La seule différence réside dans la configuration de l'ERAS maître (GHOST). Dans **Outils** > **Options du serveur...** > **Réplication**, activez la case à cocher **Activer la réplication « de »**, puis saisissez 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.



2.3.2.2 Filiale : installation du ERA Server

Comme dans l'exemple ci-dessus, installez le second ERAS et ERAC. Activez et configurez de nouveau les paramètres de réplication. Cette fois, cochez la case **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, qui est l'adresse IP du serveur GHOST.



2.3.2.3 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 Vue d'ensemble de l'environnement 20, 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 que le serveur HTTP intégré ne requiert pas d'authentification.

Pour obtenir des informations supplémentaires sur la configuration d'un miroir dans ERAS, consultez le chapitre intitulé Serveur Miroir 103.

2.3.2.4 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 (dans notre exemple, LITTLE). Cela vise à empêcher le transfert des packages d'installation via le canal VPN qui est plus lent.

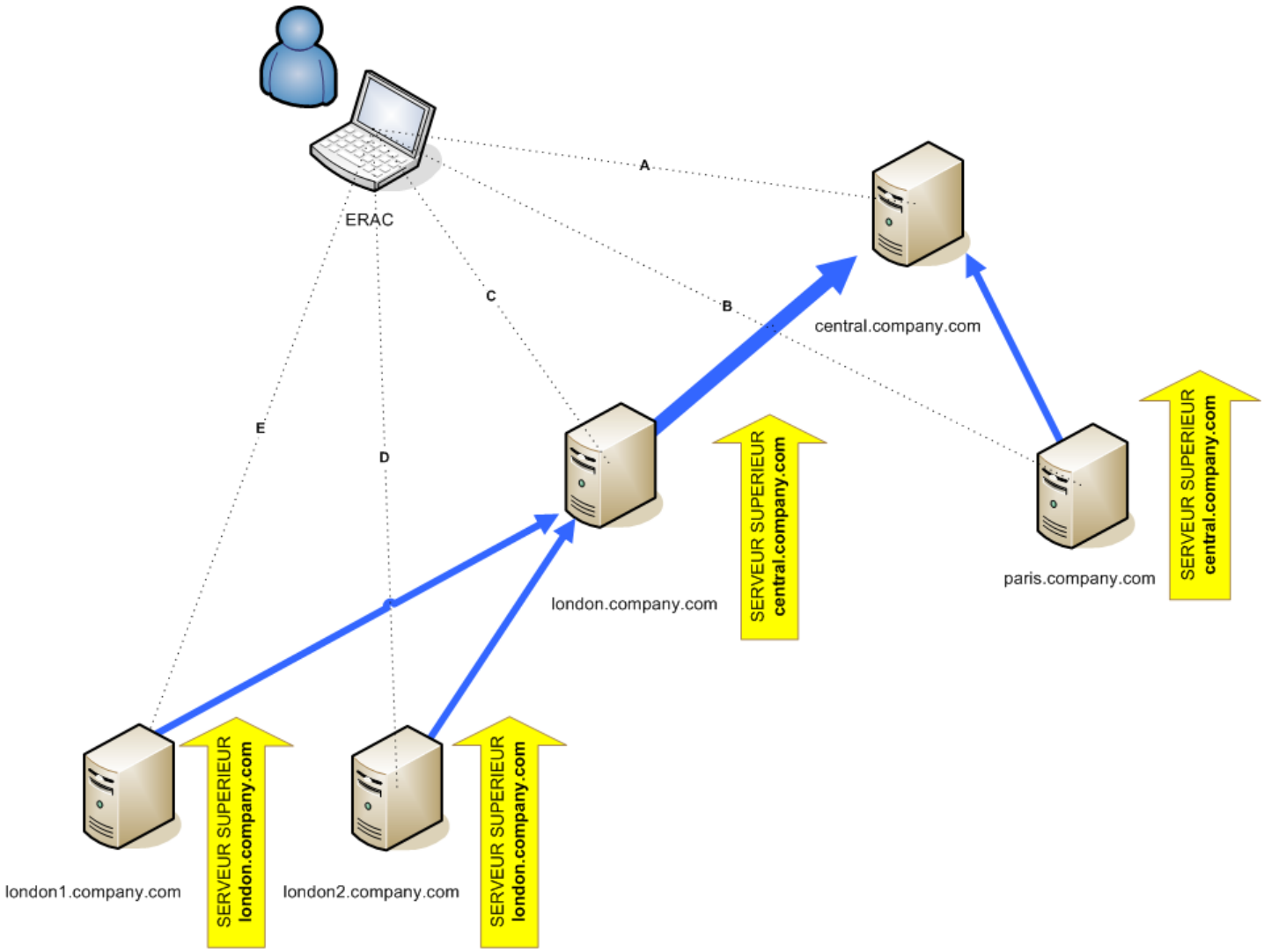
2.3.3 Autres exigences pour les environnements d'entreprise

Dans les grands réseaux, il est possible d'installer plusieurs ERA Server pour effectuer des installations à distance d'ordinateurs client à partir de serveurs plus accessibles. À cette fin, le ERAS propose la *réplication* (voir chapitre Installation au siège central 21 et Filiale : installation du ERA Server 21) qui permet de transférer les informations stockées vers un ERAS parent (*serveur de niveau supérieur*). Il est possible de configurer la réplication à l'aide d'ERAC.

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, d'habitude plus lent ; l'administrateur doit uniquement se connecter à un ERAS central (la communication marquée par la lettre A dans la figure ci-après). 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 ERAS london2.company.com avec la console (communication D) 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.



3. Utilisation de ERA Console

3.1 Connexion à ERA Server

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 ERA Server ou modifier des serveurs actuellement répertoriés. Sélectionnez le serveur souhaité dans le menu déroulant **Sélectionner une connexion**. Cliquez ensuite sur le bouton **Connecter**.

REMARQUE :: ERAC prend en charge le protocole IPv6. L'adresse doit être au format *[adresse_ipv6]:port*, par exemple *[::1]:2223*.

Autres options de cette fenêtre :

- **Connecter au serveur sélectionné au démarrage de la console** :si cette option est sélectionnée, la console se connecte automatiquement au serveur ERAS sélectionné au démarrage.
- **Afficher un message en cas d'échec de la connexion** : en cas d'erreur de communication entre ERAC et ERAS, un message d'alerte s'affiche.

Il existe deux types d'authentification :

ERA Server

L'authentification de l'utilisateur est réalisée à l'aide des informations d'identification ERAS. Par défaut, aucun mot de passe n'est requis pour se connecter à ERAS, mais il est fortement recommandé d'en définir un. Pour créer un mot de passe pour se connecter à ERAS :

Cliquez sur **Fichier** > **Modifier le mot de passe** (ou **Outils** > **Options du serveur** > **Sécurité**), puis cliquez sur le bouton **Modifier** à droite de **Mot de passe pour la console**.

Lors de la saisie d'un mot de passe, vous pouvez activer l'option **Mémoriser le mot de passe**. Songez aux risques possibles pour la sécurité liés à l'usage de cette option. Pour supprimer tous les mots de passe mémorisés, cliquez sur **Fichier** > **Effacer les mots de passe en cache...**

Si vous souhaitez définir ou modifier les comptes utilisateur pour l'authentification console-serveur, utilisez l'outil Gestionnaire des utilisateurs 95.

Windows/Domaine

Les utilisateurs s'authentifient à l'aide des informations d'identification utilisateur de Windows/Domaine. Pour que l'authentification Windows/Domaine fonctionne correctement, ERAS doit être installé sous un compte Windows/Domaine qui possède des privilèges suffisants. Il faut également activer cette fonctionnalité sous **Outils** > **Options du serveur...** > onglet **Paramètres avancés** > **Modifier les paramètres avancés...** > **ESET Remote Administrator** > **ERA Server** > **Configuration** > **Sécurité** :

Autoriser l'authentification de Windows/domaine : active/désactive l'authentification de Windows/domaine.

Groupes d'administrateurs : permet de définir les groupes pour lesquels l'authentification Windows/domaine sera activée.

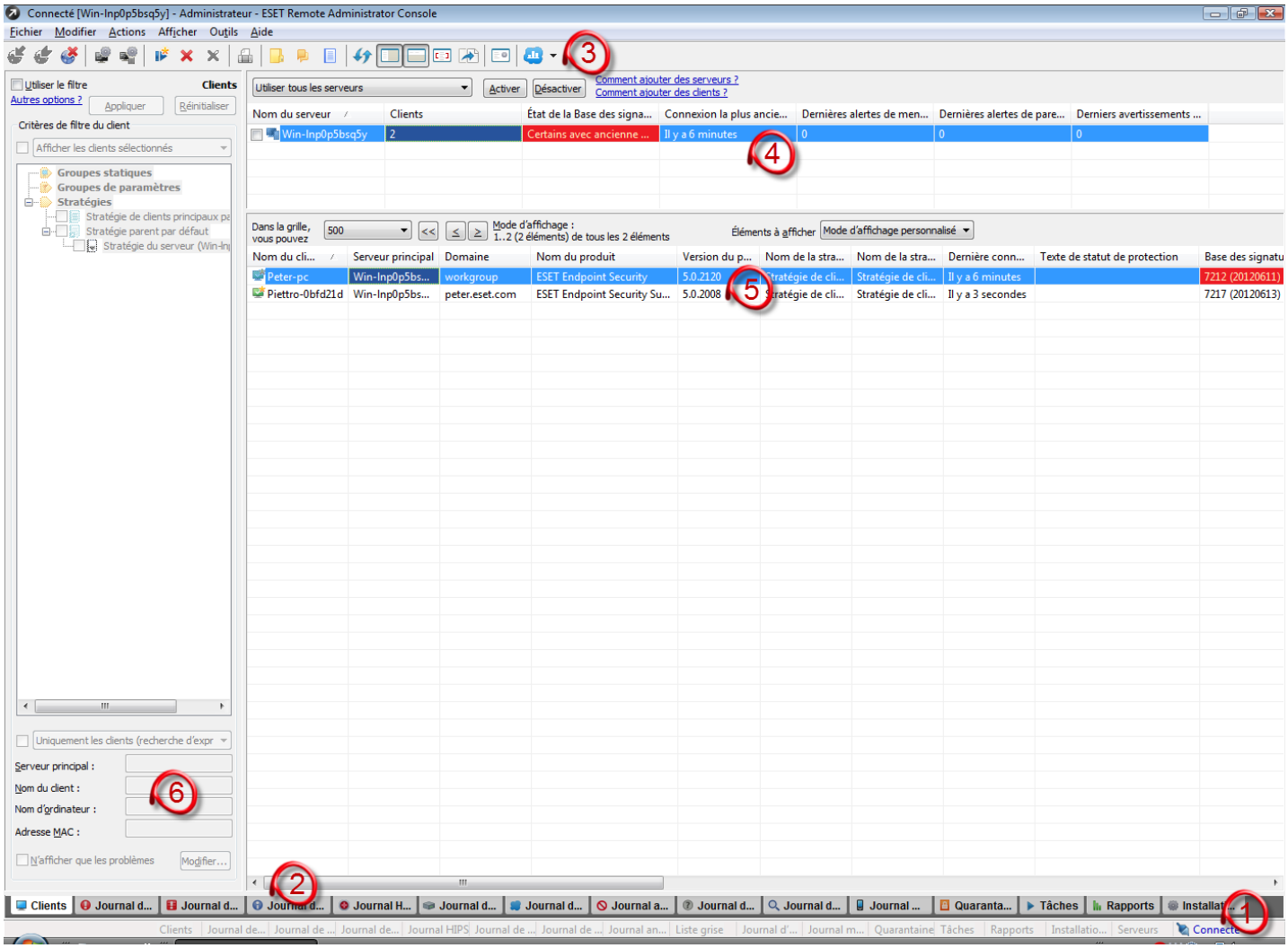
Groupes en lecture seule : permet de définir des groupes avec un accès en lecture seule.

Une fois la communication établie, l'en-tête du programme devient **Connecté [nom_serveur]**.

Vous pouvez également cliquer sur **Fichier** > **Connexion** pour vous connecter à l'ERAS.

REMARQUE : La communication entre ERAC et ERAS est chiffrée (AES-256).

3.2 ERA Console - fenêtre principale



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** > **Autres paramètres** > **Utiliser le rafraîchissement automatique (minutes)**). 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 28 par ordre d'importance (**2**). La plupart des informations sous les onglets ont trait aux clients connectés. 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 de 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 le chapitre Filtrage des informations 25). Si vous avez besoin d'imprimer certaines informations de ces onglets, reportez-vous au chapitre Mise en page 25 pour plus d'informations.

La section Serveur (**4**) est importante si vous répliquez des serveurs ERA Server. Elle affiche des informations de synthèse sur la console à laquelle ERAS est connecté, ainsi que des informations sur les serveurs ERA Server enfant ou de niveau inférieur. Le menu déroulant Serveurs de la section **4** influence les informations affichées à la section **5**.

- **Utiliser tous les serveurs** : affiche les informations de tous les serveurs ERA Server -section (**5**).
- **N'utiliser que les serveurs contrôlés** : affiche les informations des serveurs ERA Server sélectionnés - section (**5**).
- **Exclure les serveurs contrôlés** : exclut les informations des serveurs ERA Server 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 ERAS sélectionné.
- **Base de signatures des virus** : version des bases des signatures de virus parmi les clients du serveur ERAS sélectionné.
- **Connexion la plus ancienne** : temps écoulé depuis la connexion la plus ancienne au serveur.
- **Dernières alertes de menace** : nombre total d'alertes de virus (voir l'attribut **Dernière alerte de menace** dans la section **5**).
- **Dernières alertes de pare-feu** : nombre total d'alertes de pare-feu.
- **Derniers avertissements d'événement** : nombre total d'événements en cours (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 au serveur 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 ou depuis la barre d'outils ERAC (**3**).

La dernière section est **Critère de filtre de l'ordinateur** (**6**) ; voir le chapitre Filtrage des informations 25.

REMARQUE : Nous vous recommandons vivement d'utiliser le menu contextuel 27 pour administrer les clients et filtrer les informations. Il permet d'effectuer différentes opérations très rapidement : réalisation de tâches, gestion de groupes et de stratégies, filtrage de données, etc.

3.2.1 Mise en page

Dans la fenêtre **Mise en page**, vous pouvez configurer les paramètres d'impression du contenu des onglets de la console ERA Console :

WYSIWYG : imprime les onglets exactement comme vous les voyez (tel écran, tel écrit).

Imprimer : imprime les onglets en échelle de gris. Le noir et le blanc seulement sont utilisés.

Imprimer les icônes : imprime également les icônes affichées à côté des noms de client.

Imprimer l'en-tête : insère la chaîne définie dans le champ **En-tête** dans le coin supérieur gauche. Utilisez l'en-tête par défaut ou rédigez le vôtre dans le champ **En-tête**.

Imprimer le logo : insère la chaîne définie dans le champ **Chemin d'accès du logo** dans le coin supérieur droit. Le logo ESET est imprimé par défaut. Vous pouvez télécharger votre propre logo en cliquant sur le bouton **"..."** situé près de cette option et en choisissant le logo sur votre disque dur.

Numéroter les pages : insère le numéro de page dans la section inférieure de la page imprimée.

Aperçu avant impression : cliquez pour afficher une page en mode aperçu avant impression.

3.3 Filtrage des informations

ERAC intègre plusieurs outils et fonctionnalités permettant d'administrer de façon conviviale les clients et les événements. La disponibilité d'un système de filtrage avancé peut être inestimable, surtout sur les systèmes comptant un nombre important de clients lorsque les informations requises doivent être regroupées et gérées facilement. ERAC propose plusieurs outils qui permettent de trier et de filtrer efficacement les informations sur les clients connectés.

Le filtre 26 permet à l'administrateur d'afficher des informations uniquement relatives à des serveurs ou des stations de travail client spécifiques. Pour afficher les options de filtre, cliquez sur **Afficher** > **Afficher/Masquer le volet Filtre** dans le menu d'ERAC.

Mode d'affichage

Dans l'onglet **Clients**, le nombre de colonnes affichées peut être modifié via le menu déroulant **Mode d'affichage** situé à l'extrême 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 dans l'onglet **Outils** > **Options de la console** > **Colonnes**>**Afficher/Masquer**.

3.3.1 Filtre

Pour activer le filtrage, sélectionnez l'option **Utiliser le filtre** dans la partie supérieure gauche de la console ERAC. Toute modification des critères de filtre mettra automatiquement à jour les données affichées, sauf configuration contraire dans l'onglet **Outils** > **Options de la console** > **Autres paramètres**.

Définissez les critères de filtrage dans la section **Critères de filtre du client**. Les clients peuvent appartenir à plusieurs groupes et stratégies. L'affectation d'un client à un groupe statique ou paramétrique peut être très utile, non seulement pour le filtrage, mais également pour des activités telles que la génération de rapports. Pour en savoir plus sur la gestion de groupes, consultez le chapitre Gestionnaire de groupes 69. Le recours aux stratégies pour la séparation des clients peut également remplir diverses fonctions. Pour plus d'informations sur la création et la gestion de stratégies, consultez le chapitre Stratégies 71.

Le premier outil de filtrage est la section de sélection de groupes et de stratégies. Trois options sont disponibles :

- **Afficher les clients sélectionnés** : les clients repris dans les groupes/les stratégies sélectionnés apparaîtront dans le volet **Clients**.
- **Masquer les clients sélectionnés** : les clients figurant dans les groupes/les stratégies non sélectionnés et les clients n'appartenant à aucun groupe seront affichés dans le volet **Clients**. Si un client est membre de plusieurs groupes et que l'un des groupes est coché, le client n'est pas affiché.
- **Masquer les clients sélectionnés, ignorer les enregistrements multiples** : les clients figurant dans les groupes/les stratégies non sélectionnés et les clients n'appartenant à aucun groupe seront affichés. Si un client est membre de plusieurs groupes et que l'un des groupes est coché, le client est affiché.
- **Afficher les clients dans aucun groupe** : seuls les clients qui n'appartiennent à aucun groupe ni aucune stratégie seront affichés.

REMARQUE : lorsqu'un groupe est sélectionné dans la liste, tous les sous-groupes le sont également.

La partie inférieure de la section **Filtre** permet de définir un autre jeu de paramètres :

- **Uniquement des clients (utilisant des mots entiers)** : le résultat n'inclut que les clients dont le nom est identique à la chaîne saisie.
- **Uniquement des clients commençant par (?,*)** : le résultat n'inclut que les clients dont le nom commence par la chaîne indiquée.
- **Uniquement des clients comme (?,*)** : le résultat n'inclut que les clients dont le nom contient la chaîne indiquée.
- **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 les chaînes en fonction des critères définis dans le menu déroulant ci-dessus. 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). Vous pouvez également utiliser des chaînes complètes ou des caractères génériques (?,*).

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 certains problèmes, sélectionnez **N'afficher que les problèmes** et cliquez sur **Modifier**. Sélectionnez les problèmes à afficher et cliquez sur **OK** pour afficher la liste des clients présentant les problèmes sélectionnés.

Toutes les modifications apportées à la configuration du filtrage seront appliquées après que vous aurez cliqué sur le bouton **Appliquer les modifications**. Pour restaurer les paramètres par défaut, cliquez sur **Réinitialiser**. Pour générer automatiquement de nouveaux résultats à chaque modification des paramètres de filtre, cliquez sur **Outils** > **Options de la console** > **Autres paramètres**, puis sélectionnez **Appliquer les modifications automatiquement**.

REMARQUE : Les critères de filtre de la dernière section peuvent varier en fonction de l'onglet actif. Les critères sont personnalisés de manière à ce que les journaux soient triés correctement. Par exemple, vous pouvez trier les journaux en fonction du niveau de détail du journal du pare-feu afin de n'afficher que le type des journaux que vous devez examiner.

Vous pouvez également trier les données dans les onglets en sélectionnant l'intervalle pour lequel vous souhaitez que les éléments soient affichés. Pour obtenir des informations sur l'utilisation de l'option **Utiliser le filtre de date**, consultez le chapitre intitulé Filtre de date 27.

3.3.2 Menu contextuel

Cliquez avec le bouton droit de la souris pour appeler le menu contextuel et ajuster le résultat dans les colonnes. Le menu contextuel propose les options suivantes :

- **Sélectionner tout** : sélectionne toutes les entrées.
- **Sélectionner par '...'** : cette option permet de cliquer avec le bouton droit de la souris 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.
- **Sélection inverse** : effectue une sélection d'entrées inversée.
- **Masquer les éléments sélectionnés** : masque les entrées sélectionnées.
- **Masquer les éléments non sélectionnés** : masque toutes les entrées non sélectionnées dans la liste.

REMARQUE : Les options peuvent varier en fonction de la fenêtre active.

- **Afficher/Masquer les colonnes** : ouvre la fenêtre **Options de la console** > Colonnes - Afficher/Masquer 48 qui permet de définir les colonnes qui seront disponibles dans le volet sélectionné.

Les options **Masquer éléments sélectionnés/non sélectionnés** 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 **Afficher** > **Vue détourée** ou 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 de la souris sur n'importe quel volet vide avec Dernière alerte de virus, puis dans le menu contextuel, sélectionnez **Sélectionner par '...'**. Ensuite, toujours dans le menu contextuel, cliquez sur **Masquer les 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 de la souris sur tout attribut dans la colonne Nom du client contenant la valeur Joseph. Dans le menu contextuel, cliquez sur **Sélectionner par 'Joseph'**. Ensuite, maintenez la touche CTRL enfoncée, cliquez avec le bouton droit de la souris, puis cliquez sur **Sélectionner par 'Charles'**. Enfin, cliquez avec le bouton droit de la souris, puis, dans le menu contextuel, sélectionnez **Masquer les 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.

3.3.3 Filtre de date

Le **filtre de date** est situé dans le coin inférieur droit de chaque onglet de la console ERAC. Précisez un **intervalle DateHeure** pour pouvoir trier plus facilement les données d'une période sélectionnée.

Les X dernières heures/Les X derniers jours/Les X dernières semaines/Les X derniers mois/Les X dernières années : sélectionnez le nombre et la période spécifiés. Vous limiterez ainsi les éléments apparaissant dans l'onglet actuel et seuls les éléments situés dans cet intervalle seront affichés. Par exemple, si vous sélectionnez *Les 10 derniers jours*, tous les éléments survenus au cours des 10 derniers jours s'afficheront.

Derniers X/Dernières X : dans le menu déroulant, sélectionnez l'intervalle de temps prédéfini pour lequel vous souhaitez afficher les éléments.

Tout avant (inclus)/Tout après (inclus) : cochez la case près de **Tout avant (inclus)** ou **Tout après (inclus)**, et précisez la date et l'heure. Tous les éléments situés avant/après cette date et cette heure seront affichés.

Tout dans l'intervalle : sélectionnez une date et une heure de début et de fin. Les éléments situés dans cet intervalle de temps seront affichés.

REMARQUE : Vous pouvez utiliser un **filtre de date** dans chaque journal pour indiquer l'intervalle de temps pendant lequel vous voulez voir apparaître les données dans l'onglet. Vous avez aussi la possibilité de définir le niveau de détail dans les onglets (le cas échéant) afin de trier les données par pertinence. Le **filtre de date** affiche les données déjà

filtrées via le filtre **Éléments à afficher**. Ces filtres dépendent l'un de l'autre. Cela signifie qu'il appliquera le filtre uniquement aux données déjà filtrées.

3.4 Onglets dans ERA Console

3.4.1 Description générale des onglets et des clients

La plupart des informations figurant dans 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

Le comportement d'ERAS par rapport à certaines opérations de réseau (telles que le changement de nom d'un PC) peut être défini dans la 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, aucune nouvelle entrée ne sera créée dans l'onglet **Clients**.

Les clients qui se connectent à ERAS pour la première fois sont désignés par la valeur **Oui** dans la colonne **Nouveau client**. Ils sont également marqués par un petit astérisque dans le coin supérieur droit de leur icône (voir la figure ci-dessous). 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.

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 de la souris sur le client, puis en sélectionnant **Définir/Redéfinir des drapeaux** > **Redéfinir le drapeau « Nouveau »**. L'icône du client devient celle illustrée ci-dessous et la valeur dans la colonne **Nouveau client** devient **Non**.

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 y a 2 jours »*), en mode absolu (20.5.2012) 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.

Utilisez l'option **Éléments à afficher** pour trier les données que vous souhaitez afficher dans un onglet. Définissez le nombre de journaux que vous souhaitez afficher (la valeur par défaut est de 200, pour tous les journaux), ainsi que le début de la période pour laquelle vous souhaitez afficher les journaux (par défaut, au cours des 7 derniers jours). Il n'est pas recommandé de choisir **Ne pas limiter dans le temps** sur les réseaux importants, car cela pourrait provoquer une charge importante sur la base de données et éventuellement réduire les performances.

REMARQUE :: Vous pouvez également utiliser un **filtre de date** dans chaque journal afin d'indiquer l'intervalle pour lequel vous souhaitez que les éléments soient affichés. Vous pouvez également défini le niveau de détail dans les onglets (le cas échéant) pour trier les données par pertinence. Le **filtre de date** affiche les données déjà filtrées via le filtre **Éléments à afficher**. Ces filtres dépendent l'un de l'autre.

Le fait de double-cliquer sur certaines valeurs active d'autres onglets et affiche afin des informations plus détaillées. Par exemple, si vous double-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 double-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.

3.4.2 Réplication et informations sous les onglets individuels

Si ERAC est connecté à un ERAS qui fonctionne en tant que serveur de niveau supérieur, les clients des serveurs de niveau inférieur seront affichés automatiquement. Les types d'information répliquées peuvent être configurés sur le serveur inférieur dans **Outils** > **Options du serveur** > **Réplication** > **Paramètres répliqués « sûr »**.

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 actuelles détaillées au format .xml (onglet **Clients**, colonne **Configuration**, **État de la protection**, **Fonctionnalités de protection**, **Informations système**)

Il se peut également que les informations du programme ESET SysInspector manquent. ESET SysInspector est intégré à la génération 4.x et suivantes des produits ESET.

Si les informations sont introuvables dans la boîte de dialogue du programme, cliquez sur **Demande** (accessible sous **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.

Sur le serveur de niveau supérieur, vous pouvez définir le niveau des journaux reçus par le serveur (**Outils** > **Options du serveur** > **Paramètres avancés** > **Modifier les paramètres avancés...** > **ESET Remote Administrator** > **ERA Server** > **Configuration** > **Maintenance du serveur** > **Journaux .... à accepter**).

REMARQUE : cette option s'applique à tous les clients connectés au serveur (pas seulement les clients répliqués).

3.4.3 Onglet Clients

Cet onglet affiche des informations générales sur des clients individuels.

Attribut	Description
Nom du client	Nom du client (peut être modifié dans la boîte de dialogue des propriétés du client, onglet Général)
Nom de l'ordinateur	Nom de la station de travail ou du serveur (nom d'hôte)
Adresse MAC	Adresse MAC (carte réseau)
Serveur principal	Nom de l'ERAS 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 IPv4 ou IPv6
Nom du produit	Nom du produit ESET
Version du produit	Version du produit ESET
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 de 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 trouvés durant la dernière analyse à la demande
Derniers fichiers nettoyés	Nombre de fichiers nettoyés (ou supprimés) durant la dernière analyse à la demande

Attribut	Description
Date de la dernière analyse	Date 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 la 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 itinérant	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). La mise à jour est uniquement réalisée si la base des signatures de virus du client n'est pas à jour. Cette fonction est utile pour les utilisateurs qui n'ont pas été connectés à ERAS depuis un certain temps ; cette tâche déclenche la mise à jour immédiatement (même avant la tâche de mise à jour standard).
Nouveau client	Nouvel ordinateur connecté (voir le chapitre Description générale des onglets et des clients 28)
Nom du SE	Nom du système d'exploitation du client
Plateforme du 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 du 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 l'outil ESET SysInspector peuvent soumettre des journaux à partir de cette application.
Informations personnalisées 1, 2, 3	Informations personnalisées à afficher spécifiées par l'administrateur (cette option peut être configurée dans ERAC via Outils > Options du serveur... > onglet Paramètres avancés > Modifier les paramètres avancés > ESET Remote Administrator > ERA Server > Configuration > Autres paramètres > Informations personnalisées 1, 2, 3).
Commentaire	Bref commentaire décrivant le client (saisi par l'administrateur)

REMARQUE : Certaines de ces 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, les informations sur une erreur de mise à jour qui s'est produite à 7 heures du matin n'indiquent pas nécessairement que la mise à jour n'a pas été effectuée correctement à 8 heures. Les options **Dernière alerte de menace** et **Dernier avertissement d'événement** peuvent faire partie de ces valeurs. Si l'administrateur sait que ces informations sont obsolètes, il peut les effacer en cliquant dessus avec le bouton droit de la souris, 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.

Le fait de double-cliquer sur un client affiche des options supplémentaires dans l'onglet **Clients** :

- **Général** : contient des informations semblables à celles affichées dans l'onglet Clients. Vous pouvez spécifier ici le nom du client, c'est-à-dire le nom 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 obtenir des informations supplémentaires, consultez la rubrique Filtrage des informations 25.
- **Tâches** : affiche les tâches relatives au client indiqué. Pour obtenir des informations supplémentaires, consultez le chapitre Tâches 64.
- **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 obtenir des informations supplémentaires, consultez la rubrique Tâches 64.
- **État de la protection** : il s'agit d'un relevé d'état général concernant tous les programmes ESET. Certains relevés sont interactifs et permettent une intervention immédiate. 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 (antispam, pare-feu personnel, etc.)
- **Informations système** : informations détaillées sur le programme installé, la version de ses composants, etc.
- **SysInspector** : informations détaillées sur les processus de démarrage et les processus s'exécutant à l'arrière-plan.
- **Quarantaine** : contient la liste des fichiers mis en quarantaine. Les fichiers mis en quarantaine peuvent être sollicités sur un client et enregistrés sur un disque local.

Pour exécuter des opérations réseau pour un ou plusieurs clients spécifiques, cliquez avec le bouton droit sur un ou plusieurs clients et, dans le menu contextuel, sélectionnez **Action réseau**. Plusieurs options sont disponibles : **Ping**, **Wake On LAN**, **Partager**, **Arrêter/Redémarrer**, **Message**, **RDP** ou **Personnalisé**. Ces actions réseau correspondent aux actions réseau Windows et ont la même fonctionnalité. Chaque action réseau que vous exécutez (à l'exception de l'option Ping) vous informe sur l'état de l'action par l'intermédiaire d'une barre de progression dans la boîte de dialogue.

3.4.4 Onglet Journal des menaces

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

Attribut	Description
Nom du client	Nom du client signalant l'alerte de menace
Nom de l'ordinateur	Nom de la station de travail ou du serveur (nom d'hôte)
Adresse MAC	Adresse MAC (carte réseau)
Serveur principal	Nom de l'ERAS avec lequel un client communique
Date de réception	Moment auquel ERAS a journalisé l'événement
Date de survenance	Moment auquel l'événement s'est produit
Niveau	Niveau d'alerte
Scanneur	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 du client	Nom du client signalant l'événement
Nom de l'ordinateur	Nom de la station de travail ou du serveur (nom d'hôte)
Adresse MAC	Adresse MAC (carte réseau)
Serveur principal	Nom de l'ERAS avec lequel un client communique
Date de réception	Moment auquel ERAS a journalisé l'événement
Date de survenance	Moment auquel 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 (en fonction des composants de programme du produit de sécurité ESET).

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

3.4.7 Onglet Journal HIPS

Cet onglet affiche toute l'activité HIPS.

Attribut	Description
ID HIPS	ID de l'entrée correspondante dans la base de données (l'ID se présente sous cette forme : numéro HIPS)
Nom du client	Nom du client signalant le message HIPS
Serveur principal	Nom du serveur ERA Server avec lequel un client communique
Date de réception	Moment auquel ERAS a journalisé l'événement
Date de survenance	Moment auquel l'événement s'est produit
Niveau	Degré d'urgence de l'événement
Application	Nom de l'application qui a généré le journal HIPS. Le format est celui d'un chemin UNC vers l'exécutable de l'application.
Opération	Activité détectée ayant une incidence sur l'application cible
Cible	Fichier de l'application qui a généré le journal HIPS. Le format est celui d'un chemin vers le fichier dans le dossier d'installation de l'application.
Action	Action entreprise par HIPS en fonction de la règle/du mode actif

REMARQUE :: Par défaut, la journalisation de l'activité HIPS est désactivée. Pour pouvoir journaliser cette activité ou modifier les paramètres, sélectionnez **Outils** > **Options du serveur** > **Maintenance du serveur** > **Paramètres de collecte des journaux** 96.

3.4.8 Journal de contrôle des périphériques

Cet onglet affiche les journaux détaillés de l'activité de contrôle des périphériques.

Attribut	Description
ID de contrôle de périphérique	ID de l'entrée correspondante dans la base de données
Nom du client	Nom du client signalant l'événement
Serveur principal	Nom du serveur ERAS avec lequel un client communique
Date de réception	Moment auquel ERAS a journalisé l'événement
Date de survenance	Moment auquel l'événement s'est produit
Niveau	Niveau d'alerte
Utilisateur	Nom de l'utilisateur associé à l'événement
Groupe	Groupe dont fait partie le client ayant signalé l'activité
Classe de périphérique	Type de support amovible (clé USB, DVD...)
Périphérique	Nom donné et numéro de série (s'il est disponible) du support amovible
Événement	Événement signalé par la fonction de contrôle de périphérique
Action	Action exécutée par la fonctionnalité de sécurité donnée

REMARQUE :: Par défaut, la journalisation de l'activité de contrôle des périphériques est désactivée. Pour pouvoir journaliser cette activité ou modifier les paramètres, sélectionnez **Outils** > **Options du serveur** > **Maintenance du serveur** > **Paramètres de collecte des journaux** 96.

3.4.9 Journal de contrôle Web

Cet onglet affiche les journaux détaillés de l'activité de contrôle Web.

Attribut	Description
ID de contrôle Web	ID de l'entrée correspondante dans la base de données
Nom du client	Nom du client signalant l'événement
Serveur principal	Nom du serveur ERAS avec lequel un client communique
Date de réception	Moment auquel ERAS a journalisé l'événement
Date de survenance	Moment auquel l'événement s'est produit
Niveau	Niveau d'alerte
Utilisateur	Nom de l'utilisateur associé à l'événement
Groupe	Groupe dont fait partie le client ayant signalé l'activité
URL	URL de la page Web bloquée
Masque d'URL	Masque d'URL de la page Web bloquée
Catégorie d'URL	Catégorie d'URL de la page Web bloquée
Action	Action exécutée par la fonctionnalité de sécurité donnée

REMARQUE :: Par défaut, la journalisation de l'activité de contrôle Web est désactivée. Pour pouvoir journaliser cette activité ou modifier les paramètres, sélectionnez **Outils** > **Options du serveur** > **Maintenance du serveur** > **Paramètres de collecte des journaux** 96.

3.4.10 Onglet Journal antispam

Cet onglet affiche toute l'activité antispam.

Attribut	Description
ID antispam	ID de l'entrée correspondante dans la base de données (l'ID se présente sous cette forme : numéro antispam)
Nom du client	Nom du client signalant le message SpamAS
Serveur principal	Nom du serveur ERA Server avec lequel un client communique
Date de réception	Moment auquel ERAS a journalisé l'événement
Date de survenance	Moment auquel l'événement s'est produit
Expéditeur	Adresse électronique de l'expéditeur du message marqué comme spam
Destinataires	Destinataire du message marqué comme spam
Objet	Objet du message marqué comme spam
Score	Évaluation en tant que spam (probabilité que le message soit un message spam) en pourcentage

Raison	Raison pour laquelle ce message a été marqué comme spam
Action	Action entreprise pour ce message

REMARQUE :: Par défaut, la journalisation de l'activité antispam est désactivée. Pour pouvoir journaliser cette activité ou modifier les paramètres, sélectionnez **Outils** > **Options du serveur** > **Maintenance du serveur** > **Paramètres de collecte des journaux** 96.

3.4.11 Onglet Liste grise

Cet onglet affiche toute l'activité de liste grise.

Attribut	Description
Liste grise	ID de l'entrée correspondante dans la base de données (l'ID se présente sous cette forme : numéro de liste grise)
Nom du client	Nom du client signalant l'événement
Serveur principal	Nom du serveur ERAS avec lequel un client communique
Date de réception	Moment auquel ERAS a journalisé l'événement
Date de survenance	Moment auquel l'événement s'est produit
Domaine HELO	Nom de domaine utilisé par le serveur d'envoi pour s'identifier auprès du serveur de réception
Adresse IP	Adresse IP de l'expéditeur du message
Expéditeur	Adresse email de l'expéditeur du message
Destinataire	Adresse email du destinataire du message
Action	Action exécutée par la fonctionnalité de sécurité donnée
Temps restant	Temps restant avant le rejet ou la vérification et livraison du message

REMARQUE :: Par défaut, la journalisation de l'activité de liste grise est désactivée. Pour pouvoir journaliser cette activité ou modifier les paramètres, sélectionnez **Outils** > **Options du serveur** > **Maintenance du serveur** > **Paramètres de collecte des journaux** 96.

3.4.12 Onglet Journal d'analyse

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

Attribut	Description
ID d'analyse	ID de l'entrée correspondante dans la base de données (l'ID a la forme : numéro d'analyse)
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 ERA Server avec lequel un client communique
Date de réception	Moment auquel 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
Analysé	Nombre de fichiers contrôlés
Infecté	Nombre de fichiers infectés
Nettoyé	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
Scanneur	Type de scanneur
Détails	État de soumission du journal du client

3.4.13 Onglet Journal mobile

Cet onglet affiche des journaux détaillés pour les téléphones mobiles connecté à ERA Server.

Attribut	Description
ID Mobile	ID de réseau du périphérique mobile
Nom du client	Nom du client sur lequel l'action a été effectuée
Nom de l'ordinateur	Nom de la station de travail ou du serveur (nom d'hôte)
Adresse MAC	Adresse MAC (carte réseau)
Serveur principal	Nom du ERA Server avec lequel un client communique
Date de réception	Moment auquel ERAS a journalisé l'événement
Date de survenance	Moment auquel l'événement a eu lieu sur le client
Niveau	Niveau d'alerte
Type de journal	Type de journal (par exemple, journal de vérification de sécurité, journal du courrier indésirable expédié par SMS)
Événement	Description de l'événement
Type d'objet	Objet auquel l'événement est lié (par exemple, SMS, fichier...)
Nom d'objet	Objet particulier auquel l'événement est lié (par exemple, numéro de téléphone de l'expéditeur du SMS, fichier...)
Action	Action réalisée (ou erreur obtenue) pendant l'événement

3.4.14 Onglet Quarantaine

Cet onglet regroupe toutes les entrées en quarantaine de votre réseau.

Attribut	Description
ID de quarantaine	Identifiant de l'objet mis en quarantaine, attribué par ordre chronologique
Hachage	Code hash de fichier
Date de réception	Moment auquel ERAS a journalisé l'événement d'analyse
Première survenance	Temps écoulé depuis la première occurrence de l'élément mis en quarantaine
Dernière survenance	Temps écoulé depuis l'occurrence la plus récente de l'élément mis en quarantaine
Nom d'objet	Généralement un dossier dans lequel se trouve l'infiltration
Nom de fichier	Nom du fichier mis en quarantaine
Extension	Type d'extension du fichier mis en quarantaine
Taille	Taille du fichier mis en quarantaine
Raison	Raison pour la mise en quarantaine, en général la description du type de menace
Nombre de clients	Nombre de clients ayant mis l'objet en quarantaine
Résultats	Nombre de fois que l'objet a été mis en quarantaine
Fichier	Indique si l'objet a été sollicité pour un téléchargement sur le serveur

REMARQUE : Notez que les champs **Nom d'objet**, **Nom de fichier** et **Extension** affichent les trois premiers objets seulement. Pour obtenir des informations détaillées, ouvrez la fenêtre Propriétés en appuyant sur la touche **F3** ou en double-cliquant sur l'élément sélectionné.

La quarantaine centralisée offre un aperçu des fichiers mis en quarantaine qui sont stockés localement sur les clients avec la possibilité de les solliciter à la demande. Quand un fichier est sollicité, il est copié sur le serveur ERA Server sous une forme chiffrée et sûre. Pour des raisons de sécurité, le déchiffrement est réalisé au moment d'enregistrer le fichier sur le disque. Pour obtenir des instructions sur la manipulation des fichiers mis en quarantaine, consultez le chapitre Tâche Restaurer/Supprimer depuis la quarantaine 67.

REMARQUE : la quarantaine centralisée requiert l'installation d'EAV/ESS version 4.2 ou versions ultérieures sur les clients.

3.4.15 Onglet Tâches

La signification de cet onglet est décrite dans le chapitre Tâches 64. Les attributs suivants sont disponibles :

Attribut	Description
État	État de la tâche (Actif = en cours d'application, Terminé = 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	Moment auquel ERAS a journalisé l'événement
Détails	État de soumission du journal des tâches
Commentaire	Bref commentaire décrivant le client (saisi par l'administrateur)

3.4.16 Onglet Rapports

L'onglet **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 les résultats au format HTML. La plupart des rapports relatifs aux infiltrations sont générés à partir du journal des menaces.

1. **Modèles de** tableau de bord 38 : modèles de rapports de tableau de bord Web. Un tableau de bord est un ensemble de rapports disponible en ligne à l'aide d'un navigateur Web. La présentation du tableau de bord est entièrement personnalisable pour chaque administrateur. Double-cliquez sur un modèle pour afficher un aperçu du rapport utilisé dans le tableau de bord.

2. **Modèles de rapport** : modèles de rapports statiques. 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. Vous pouvez créer des modèles ou modifier les modèles prédéfinis existants (indiqués ci-dessous) :

- **Vue d'ensemble des clients** : affiche les états de protection de tous les clients.
- **Clients avec des menaces actives** : affiche les clients avec des menaces actives (menaces qui n'ont pas été nettoyées pendant l'analyse), ainsi que des informations sur ces menaces.
- **Rapport complet sur les attaques réseau** : affiche un rapport complet de toute l'activité des attaques réseau.
- **Rapport complet sur les SMS** : affiche un rapport complet de toute l'activité de spam expédié par SMS.
- **Rapport complet sur le spam** : affiche un rapport complet de toute l'activité de spam expédié par email.
- **Rapport complet des menaces** : affiche un rapport complet de toutes les menaces détectées.
- **Récapitulatif des informations personnalisées** : affiche un rapport complet contenant des informations définies par l'utilisateur (à définir en premier lieu).
- **Principaux clients problématiques** : affiche les clients ayant le plus grand nombre de problèmes (en fonction des reports ci-dessus).

Le fait de cliquer sur **Modèles par défaut** a pour effet de rétablir l'état d'origine des modèles prédéfinis (cette action n'a aucun effet sur les modèles personnalisés).

- **Options**

Cliquez sur le bouton **Générer maintenant** (assurez-vous que l'onglet **Options** est sélectionné) pour générer un rapport à tout moment, indépendamment de la planification. Sélectionnez le type de déclencheur dans le menu déroulant situé à côté de cette option. Cette option définit le type de fichier du rapport généré (HTML, ZIP ou PDF).

Rapport

Type : type de rapport basé sur les modèles prédéfinis. Il peut être modifié pour les modèles prédéfinis ou sélectionné pour les modèles créés et personnalisés. Le fait de cliquer sur **...** (à côté de cette option) affiche des rapports qui peuvent être utilisés pour le **rapport personnalisé complet**.

Style : vous pouvez modifier la couleur et la disposition du rapport à l'aide du menu déroulant.

Filtre

Clients cibles : vous pouvez indiquer si vous voulez que le rapport collecte **toutes** les données ou celles issues **uniquement des clients/serveurs/groupes sélectionnés**, ou qu'il **exclue les clients/serveurs/groupes sélectionnés**. Vous pouvez indiquer les clients/serveurs/groupes après avoir cliqué sur **...** à côté du menu déroulant **Clients cibles**, dans la boîte de dialogue **Ajouter**/**Supprimer**.

Menace : vous pouvez également indiquer si vous voulez que le rapport répertorie **toutes** les menaces ou **les menaces sélectionnées uniquement**, ou qu'il **exclue les menaces sélectionnées**. Vous pouvez indiquer les menaces après avoir cliqué sur **...** à côté du menu déroulant dans la boîte de dialogue **Ajouter**/**Supprimer**.

Vous pouvez configurer d'autres détails en cliquant sur **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).

- **Intervalle**

Actuelle : seuls les événements survenus au cours d'une période choisie sont 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 (par exemple 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, par exemple 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**. Désélectionnez l'option **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/A : ce paramètre permet de définir une période pour laquelle le rapport sera généré.

- **Planificateur**

Fréquence : permet de définir et de configurer un rapport automatique à une heure ou à des intervalles choisis.

Après avoir planifié le rapport, cliquez sur **Sélectionner cible...** pour désigner l'emplacement où le rapport sera enregistré. 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. Si vous utilisez cette option, sélectionnez le type de fichier de sortie (HTML, ZIP ou PDF). Vous pouvez utiliser des variables (%) dans le chemin du dossier. Les variables ne font pas la différence entre majuscules et minuscules. Ces variables ajoutent des informations personnalisées dans le rapport généré. Si vous saisissez le chemin du dossier avec le symbole "\", les rapports sont écrits directement dans ce dossier et les données sont remplacées. Les variables suivantes sont prises en charge :

Variable	Description
%INTERVAL%	Intervalle pour lequel le rapport est généré, tel qu'il est envoyé par CReport::GetIntervalString (INTERVALSTRING_FOLDER).
%DATE%	Date courante ("AAAA-MM-JJ").
%TIME%	Heure courante ("HH-MM-SS").
%DATETIME%	Date et heure courantes ("AAAA-MM-JJ HH-MM-SS").
%TIMESTAMP%	Date et heure courantes, temps unix, en hex, 8 chiffres.
%RND4%	Valeur aléatoire, 4 chiffres hex presque uniques (non recommandé).
%DDATE%	Date courante, dense ("AAAAMMJJ").
%DTIME%	Heure courante, dense ("HHMMSS").
%YEAR%, %MONTH%, %DAY%, %HOUR%, %MINUTE%, %SECOND%	Parties date/heure sous forme de chiffres (4 pour l'année, 2 pour les autres).
%COUNTER%	Nombre décimal sur 5 chiffres, à partir de 1.

%COUNTER1%, %COUNTER2%, %COUNTER3%, %COUNTER4%, %COUNTER5%	Nombre décimal sur 1/2/3/4/5 chiffres, à partir de 1.
%CCOUNTER%	Nombre conditionnel sur 5 chiffres (la 1e itération est effacée, la 2e itération est "00002")
%CCOUNTER1%, %CCOUNTER2%, %CCOUNTER3%, %CCOUNTER4%, %CCOUNTER5%	Nombre conditionnel décimal sur 1/2/3/4/5 chiffres.
%UCOUNTER%	Nombre avec caractère de soulignement sur 5 chiffres (la 1e itération est effacée, la 2e iteration est "_00002")
%UCOUNTER1%, %UCOUNTER2%, %UCOUNTER3%, %UCOUNTER4%, %UCOUNTER5%	Nombre avec caractère de soulignement décimal sur 1/2/3/4/5 chiffres.
%%	Signe % unique.

Par exemple, si vous saisissez le chemin sous la forme : *C:\Reports\%INTERVAL%_%COUNTER%*", les noms de dossier seront générés sous la forme *C:\Reports\Jour 2012-02-02_00001* ; *C:\Reports\Jour 2012-02-02_00002*, etc.

Pour envoyer les rapports créés à une adresse électronique, il faut saisir le serveur SMTP et l'adresse du destinataire dans **Outils** > **Options du serveur** > **Autres paramètres**.

3. **Rapports générés** : 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 sur le bouton droit de la souris). Vous pouvez trier les rapports en fonction du **nom**, de la **date** de génération, du **nom du modèle** et de l'**emplacement** du rapport. Cliquez sur **Ouvrir** ou double-cliquez dans la liste sur un rapport pour l'ouvrir. Le fait de cliquer sur un rapport dans la liste affiche un aperçu dans la section inférieure (si cette option est sélectionnée).

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, sélectionnez **Ajouter aux favoris**.

3.4.16.1 Tableau de bord

Un **tableau de bord** est un ensemble de rapports qui sont automatiquement mis à jour avec les nouvelles données et donne une vue d'ensemble complète de l'état du système. Chaque utilisateur ayant accès à ERAC et doté d'un nom d'utilisateur possède un ensemble individuel de tableaux de bord qu'il peut totalement personnaliser. Ces paramètres sont directement stockés sur le serveur, si bien que l'utilisateur a accès au même tableau de bord, quel que soit le navigateur employé.

La fonctionnalité de tableau de bord utilise le serveur HTTP ERA par défaut, en communiquant via le port 443. Il est possible de changer de port dans les **options avancées du serveur**, dans ERA Console. Le **tableau de bord** et les **options de connexion du tableau de bord** sont également accessibles depuis la fenêtre principale ERAC, dans la barre d'outils (icône de nuage bleu).

REMARQUE :: L'administrateur doit préparer un modèle pour chaque rapport avant de l'utiliser dans le tableau de bord. Sinon, les données des rapports risquent de ne pas s'afficher correctement.

REMARQUE :: Par défaut, le **tableau de bord** est démarré à l'aide du protocole https avec un certificat à signature automatique. Le message d'avertissement suivant s'affiche dans le navigateur Web : *Le certificat de sécurité présenté par ce site Web n'a pas été émis par une autorité de certification approuvée*. Notez que, lors de l'utilisation du protocole HTTP, vos noms d'utilisateur et vos mots de passe sont transmis en texte normal. Cela peut être particulièrement risqué si vous utilisez des informations de connexion Windows/Domaine.

Le programme d'installation peut générer un certificat avec signature automatique. Certains navigateurs peuvent afficher un avertissement lorsqu'ils détectent un certificat à signature automatique. Vous pouvez également fournir votre propre certificat pendant le mode d'installation avancée ou ultérieurement, par ESET Éditeur de configuration. Le certificat fourni peut être signé par une autorité de certification approuvée ou à l'aide de votre propre racine de certificat. Les formats suivants de certificat X.509 et de clé privée sont pris en charge :

- ASN - certificat codé ASN.1 DER et clé dans des fichiers distincts.
- PEM - ASN codé Base64 avec en-têtes supplémentaires, certificat et clé dans des fichiers distincts.
- PFX - certificat et clé privée dans un même fichier de conteneur.

Il n'est pas possible d'utiliser un certificat et une clé de formats différents. Vous pouvez modifier le protocole et choisir

http en cliquant sur **Tableau de bord** (icône de nuage bleu) dans la fenêtre principale du programme ERAC et en sélectionnant **Configurer...**. Vous pouvez également définir votre propre certificat (au format de fichier PEM, avec codage X.509 base64) à l'aide d'ESET Éditeur de configuration (**Outils** > **Serveur** > **Options** > **Paramètres avancés** > **Modifier les paramètres avancés...** > **Remote Administrator** > **ERA Server** > **Paramètres** > **Tableaux de bord** > **Clé du certificat local**/**Certificat local**).

REMARQUE :: Le tableau de bord prend également en charge le protocole IPv6. Par exemple, *http://[::1]:8080*.

Il existe un ensemble de modèles prédéfinis (indiqués ci-dessous) de **tableau de bord** ou vous pouvez créer un modèle personnalisé.

- **Rapport complet sur le spam** : affiche un récapitulatif de toute l'activité du moteur antispam.
- **Composition du score antispam** : affiche la composition du score de spam, ainsi que le nombre de messages évalués.
- **Vue d'ensemble de la connexion client** : affiche une vue d'ensemble des connexions client en fonction de l'heure et de l'état de leur connexion.
- **Récapitulatif InformationsPersonnalisées1 client** : affiche un rapport complet contenant des informations définies par l'utilisateur (à définir en premier lieu).
- **Récapitulatif InformationsPersonnalisées2 client** : affiche un rapport complet contenant des informations définies par l'utilisateur (à définir en premier lieu).
- **Récapitulatif InformationsPersonnalisées3 client** : affiche un rapport complet contenant des informations définies par l'utilisateur (à définir en premier lieu).
- **Clients de groupes** : indique le nombre de clients des groupes sélectionnés.
- **Clients des groupes vers Tout** : indique le rapport entre le nombre de clients des groupes sélectionnés et le nombre total de clients (sous forme de pourcentage).
- **Clients avec des menaces actives** : affiche les clients avec des menaces actives (non nettoyées pendant l'analyse), ainsi que des informations sur ces menaces.
- **Récapitulatif des actions de la liste grise** : affiche tous les messages de la liste grise, ainsi que l'action entreprise.
- **Ordinateurs gérés et non gérés** : affiche les ordinateurs connectés à ERA Server (ordinateurs gérés) et les ordinateurs non connectés (ordinateurs non gérés). Ces informations sont basées sur la recherche par défaut.
- **Récapitulatif des noms de SE** : affiche le nombre et le type de systèmes d'exploitation client.
- **Récapitulatif du produit** : affiche le nombre et le type de produits de sécurité client.
- **Récapitulatif de l'état de protection** : affiche le nombre de clients et l'état de leur sécurité.
- **Progression du spam expédié par SMS** : indique la progression du spam par SMS.
- **Chargement de base de données du serveur** : affiche la durée totale d'utilisation de la base de données par tous les threads.
- **Requêtes de base de données du serveur** : affiche le nombre de requêtes SQL effectuées sur la base de données.
- **Chargement du matériel du serveur** : affiche l'utilisation CPU et de la mémoire RAM du serveur.
- **Surveillance de l'état du serveur** : affiche l'état du serveur, ainsi que des informations sur la mise à jour de la base des signatures de virus.
- **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 menaces.
- **Progression des menaces** : progression des événements liés à des logiciels malveillants (sur la base du nombre).
- **Menaces par objet** : nombre d'alertes de menace en fonction de leur mode d'infiltration (emails, fichiers, secteurs d'amorçage).
- **Menaces par analyseur** : nombre d'alertes de menace des différents modules du programme.
- **Principaux clients par déconnexion** : affiche les principaux clients triés par la date de leur dernière connexion.
- **Principaux clients avec le plus d'attaques réseau** : affiche les principaux clients avec le plus grand nombre d'attaques réseau.
- **Principaux clients avec le plus de spam expédié par SMS** : affiche les principaux clients avec le plus de spam par SMS.
- **Principaux clients avec le plus de spam** : affiche les principaux clients avec le plus de messages de spam.
- **Principaux clients avec le plus de menaces** : répertorie les stations de travail client les plus « actives » (sur la base du nombre de menaces détectées).
- **Principaux destinataires d'emails de liste grise** : affiche les principaux destinataires avec le plus de messages en liste grise.
- **Principaux expéditeurs d'emails de liste grise** : affiche les principaux expéditeurs avec le plus de messages en liste grise.
- **Principales attaques réseau** : affiche les principales attaques réseau.
- **Sources des principales attaques réseau** : affiche les principales sources d'attaques réseau.
- **Principaux expéditeurs de spam par SMS** : indique les principaux expéditeurs de spam pour des cibles spécifiées.
- **Principaux destinataires de spam** : affiche les principaux destinataires de messages de spam.
- **Principaux expéditeurs de spam** : affiche les principaux expéditeurs de messages de spam.
- **Principales menaces** : liste des menaces les plus fréquemment détectées.
- **Principales menaces par propagation** : affiche les principales menaces par propagation.
- **Principaux utilisateurs avec le plus de menaces** : répertorie les utilisateurs les plus « actifs » (sur la base du nombre de menaces détectées).
- **Ordinateurs non enregistrés** : affiche tous les ordinateurs non gérés, c'est-à-dire ceux qui ne sont pas connectés à ERA Server. Cette option affiche également l'heure à laquelle un nouvel ordinateur non géré a été détecté.

Les modèles de rapport existant peuvent être importés/exportés depuis ou vers un fichier *.xml* en cliquant sur **Importer.../Exporter...** . Les conflits de noms qui se produisent pendant l'importation (modèles existants et importés

portant le même nom) sont résolus par l'ajout d'une chaîne aléatoire à la fin du nom d'un modèle importé.

Pour enregistrer les paramètres de rapports définis dans un modèle, cliquez sur **Enregistrer** ou**Enregistrer sous...** Si vous créez un modèle, cliquez sur **Enregistrer sous...**, puis attribuez-lui un nom. Le fait de cliquer sur **Modèles par défaut** a pour effet de rétablir l'état d'origine des modèles prédéfinis (cette action n'a aucun effet sur les modèles personnalisés).

- **Options**

Aperçu du rapport : le fait de cliquer sur ce bouton génère le tableau de bord et affiche une vue d'ensemble.

Rapport

Type : type de rapport basé sur les modèles prédéfinis. Il peut être modifié pour les modèles prédéfinis qui ont servi à la création des modèles personnalisés.

Filtre

Clients cibles : vous pouvez indiquer si vous voulez que le rapport collecte **toutes** les données ou celles issues **uniquement des clients/serveurs/groupes sélectionnés**, ou qu'il **exclue les clients/serveurs/groupes sélectionnés**. Vous pouvez indiquer les clients/serveurs/groupes après avoir cliqué sur le bouton **...** à côté du menu déroulant **Clients cibles**, dans la boîte de dialogue **Ajouter/Supprimer**.

Menace : vous pouvez également indiquer si vous voulez que le rapport répertorie **toutes** les menaces ou **les menaces sélectionnées uniquement**, ou qu'il **exclue les menaces sélectionnées**. Vous pouvez indiquer les menaces après avoir cliqué sur **...** à côté du menu déroulant dans la boîte de dialogue **Ajouter/Supprimer**.

Vous pouvez configurer d'autres détails en cliquant sur **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 des attributs sélectionnés. Vous pouvez également sélectionner le format de rapport utilisé (.html, .csv).

- **Intervalle**

Heure - Les X dernières minutes/Les X dernières heures/Les X derniers jours/Les X dernières semaines/Les X derniers mois/Les X dernières années : moment à partir duquel les données doivent figurer dans le rapport. L'heure est basée sur l'heure de l'incident signalée à ERA.

- **Rafraîchir**

Intervalle de rafraîchissement du navigateur : sélectionnez l'intervalle de rafraîchissement des nouvelles données reçues du serveur Web.

Intervalle de rafraîchissement du serveur : sélectionnez l'intervalle pendant lequel les données seront envoyées au serveur Web.

3.4.16.1.1 Liste des serveurs Web du tableau de bord

Cliquez sur la flèche en regard de l'icône Tableau de bord dans le menu principal pour configurer les options de connexion **Serveurs Web de tableau de bord**.

- **Serveurs Web de tableau de bord** : liste de tous les serveurs Web de tableau de bord disponibles.
- **Supprimer** : cliquez sur ce bouton pour supprimer le serveur Web du tableau de bord sélectionné de la liste.
- **Définir par défaut** : désigne le serveur Web du tableau de bord sélectionné comme serveur par défaut. Il apparaît en premier dans le menu déroulant (lorsque vous cliquez sur la flèche près de l'icône de tableau de bord) et s'ouvre en premier lorsque vous cliquez sur l'icône de tableau de bord proprement dite.
- **Protocole** : vous avez le choix entre les protocoles http et https avec un certificat auto-signé.
- **Nom ou adresse IP de l'hôte** : affiche le nom d'hôte ou l'adresse IP du serveur Web du tableau de bord sélectionné. Vous pouvez également saisir un nouveau nom d'hôte ou une nouvelle adresse IP et cliquer sur **Ajouter/Enregistrer** pour enregistrer les données et ajouter le serveur Web du tableau de bord à la liste.
- **Commentaire** : description ou commentaire facultatif du serveur Web du tableau de bord sélectionné.

REMARQUE : Le tableau de bord prend aussi en charge le protocole IPv6. Par exemple, *http://[::1]:8080*.

3.4.16.2 Scénario d'exemple de rapport

Pour maintenir la sécurité de réseau des clients au niveau le plus haut, il faut avoir un bonne vue d'ensemble de l'état de la sécurité du réseau. Vous pouvez créer facilement des rapports avec des détails complets sur les menaces, les mises à jour, les versions des produits client, etc. (pour de plus amples informations, consultez la rubrique Rapports 36). Normalement, un rapport hebdomadaire devrait fournir toutes les informations nécessaires. Toutefois, il peut arriver qu'une vigilance accrue s'impose, par exemple après la découverte d'une menace.

En guise d'exemple, nous allons créer un groupe paramétrique appelé *Quarantaine*. Ce groupe contiendra uniquement les ordinateurs dans lesquels une menace a été détectée et nettoyée lors de la dernière analyse à la demande. Définissez cette condition en cochant l'option **Menace détectée lors de la dernière analyse**. Pour créer ce groupe paramétrique, suivez les instructions reprises à la section Groupes paramétriques 70.

REMARQUE : lors de la création du groupe *Quarantaine*, assurez-vous que l'option **Sans suppression** est désactivée. De cette manière, l'ordinateur sera affecté dynamiquement et supprimé une fois que les conditions ne seront plus remplies.

Créez le rapport *Ordinateurs de quarantaine*. Pour créer un rapport pour ce groupe paramétrique, suivez les instructions reprises à la section Rapports 36.

Les paramètres spécifiques pour notre exemple sont les suivants :

- Paramètres de la section **Options** :

Type :	Rapport de quarantaine avec détails
Style :	Blue Scheme
Clients cibles :	Uniquement les groupes sélectionnés
Menace :	n.a

- Paramètres de l'onglet **Intervalle** :

Actuelle :	Jour

- Paramètres de l'onglet **Planificateur** :

Fréquence :	Quotidienne
Tous les :	1 jour

CONSEIL : vous pouvez stocker les résultats dans la base de données de rapports ou définir un dossier où les copies de rapport seront stockées. Les rapports peuvent également être envoyés par email. Tous ces paramètres sont disponibles après que vous avez cliqué sur **Sélectionner cible...**

Les rapports générés peuvent être consultés dans la section **Rapports générés**, dans la section **Rapports**.

Synthèse : nous avons créé le groupe paramétrique *Quarantaine* contenant des ordinateurs sur lesquels une menace a été détectée lors de l'analyse à la demande la plus récente. Ensuite, nous avons créé un rapport automatisé qui nous informera, chaque jour, des ordinateurs qui appartiennent au groupe *Quarantaine*. Nous aurons ainsi un bon aperçu de l'état de notre réseau de clients qui nous permettra de contrôler les menaces potentielles.

CONSEIL : pour voir les détails du dernier journal d'analyse, utilisez le type de rapport **Rapport des analyses avec détails**.

3.4.17 Onglet Installation à distance

Cet onglet propose des options pour plusieurs méthodes d'installation à distance d'ESET Smart Security ou d'ESET NOD32 Antivirus sur des clients. Pour obtenir des informations supplémentaires, consultez le chapitre Installation à distance 53.

1. Pour rechercher des ordinateurs, vous pouvez utiliser la recherche par défaut ou en créer une. Pour créer une recherche, cliquez sur **Nouvelle recherche** pour démarrer l'assistant de recherche réseau 43. Pour lancer une recherche, cliquez sur **Exécuter**.

2. Les résultats de la recherche peuvent être filtrés à l'aide du **filtre des résultats de la recherche** dans la section en dessous. Le filtrage des résultats est sans effet sur la recherche à proprement parler. Autres critères de recherche :

- **Ordinateurs non enregistrés** : affiche les ordinateurs qui ne sont pas répertoriés dans la base de données serveur actuelle.

- **Clients avec avertissement de dernière connexion** : affiche les ordinateurs répertoriés dans la base de données serveur actuelle et qui ont été l'objet de l'avertissement de dernière connexion.

- **Masquer les ordinateurs ignorés** : cette option est active par défaut. Elle masque les ordinateurs de la liste Ignorer créée par l'administrateur (dans le menu contextuel, vous pouvez modifier et importer cette liste).

3. Les résultats de la recherche actuelle apparaissent dans la section **Ordinateur** principale. À partir de là, vous pouvez gérer les packages d'installation 44 et exécuter l'installation poussée à distance 55 via le menu contextuel.

Le menu contextuel (clic droit) de l'onglet **Ordinateurs** offre les options suivantes :

- **Gérer les packages** exécute l'**éditeur de packages d'installation**. Consultez la section Installation à distance 44 pour plus de détails.
- **Mettre à niveau le client Windows** : exécute la mise à niveau. Utilisez cette option si vous souhaitez installer une version plus récente d'EES/EEV sur une version plus ancienne.
- **Diagnostics de l'installation poussée Windows** : contrôle la disponibilité des clients et services à utiliser durant l'installation à distance. Pour plus d'informations, consultez le chapitre Diagnostic de l'installation à distance 46.
- **Installation poussée Windows** : exécute l'installation poussée à distance 55 de Windows.
- **Installation poussée Linux/Mac** : exécute l'installation poussée de Linux/Mac. Consultez la rubrique Conditions requises pour une installation poussée Linux/Mac 55 pour plus de détails.
- **Exporter dans le dossier ou le script de connexion** : consultez la section Installation à distance par ouverture de session ou par email 57 pour en savoir plus.
- **Envoyer par email** : consultez la section Installation à distance par ouverture de session ou par email 57 pour en savoir plus.
- **Définir la connexion par défaut pour les installations par email et script de connexion** : ouvre la fenêtre **Connexion par défaut** où vous pouvez spécifier le nom de l'utilisateur et le mot de passe d'un compte d'administrateur pour les ordinateurs cibles.
- **Propriétés** : ouvre la fenêtre **Propriétés du client** qui reprend toutes les informations importantes sur un client.

Pour les autres options du menu contextuel, consultez le chapitre Menu contextuel 27.

3.4.17.1 Assistant de recherche réseau

Une **tâche de recherche** est un ensemble de paramètres qui permettent de rechercher des ordinateurs sur le réseau. Les tâches de recherche créées sont stockées directement sur le serveur et sont à la disposition de tous les administrateurs.

Vous pouvez utiliser la tâche de recherche par défaut prédéfinie ; elle est exécutée de manière périodique (et peut également être déclenchée manuellement) et porte sur l'intégralité du réseau. Les résultats de la recherche sont stockés sur le serveur. Cette tâche peut également être modifiée, mais une fois qu'elle est lancée, elle ne peut plus être arrêtée jusqu'à son déroulement complet.

Les paramètres de tâche personnalisés sont stockés sur le serveur, mais les résultats de la recherche ne sont envoyés qu'à la console depuis laquelle la recherche a été exécutée. Ces tâches de recherche ne peuvent être lancées que manuellement.

1. Tout d'abord, choisissez le type de tâche réseau :

- **Modèle d'analyse réseau** : crée une tâche de recherche dont le nom et l'ensemble de paramètres peuvent être stockés sur le serveur pour être réutilisés. Les résultats de la recherche ne sont pas stockés. L'exécution d'une nouvelle recherche actualise la liste des ordinateurs clients qui sont disponibles sur le réseau.
- **Recherche réseau temporaire** : crée une tâche de recherche temporaire qui n'est pas stockée sur le serveur et qui sera supprimée à la fin de la session en cours.

2. Choisissez ensuite les méthodes à utiliser pour effectuer une recherche sur le réseau (vous pouvez choisir plusieurs méthodes de recherche) :

- **Recherche Active Directory** : cette option permet de sélectionner les branches Active Directory sur lesquelles vous souhaitez rechercher des ordinateurs. Vous pouvez également **Inclure les ordinateurs désactivés**.
- **Windows Networking (WNet)** : recherche les ordinateurs sur le réseau Windows.
- **Shell** : recherche tous les ordinateurs dans tous les emplacements réseau (voisinage réseau de Windows).
- **Adresse IP** : permet de sélectionner la **plage IP**/**le masque IP** à utiliser pendant la recherche. Vous pouvez également

définir une **liste personnalisée d'adresses IP**. La recherche accède alors aux ordinateurs par les ports (ces derniers peuvent être configurés). Vous pouvez également utiliser une commande Ping (cette option est particulièrement recommandée pour les ordinateurs Linux).

- **Liste d'ordinateurs personnalisée** : importe une liste personnalisée d'ordinateurs. L'assistant de recherche réseau accepte les listes au format de fichier *.txt.

Le fait de cliquer sur **Terminer** enregistre la nouvelle recherche, de manière temporaire (recherche réseau temporaire) ou permanente (modèle d'analyse réseau). Pour terminer et lancer la tâche immédiatement, cliquez sur **Terminer et Exécuter**. Pour exécuter la tâche, cliquez sur **Exécuter** dans l'onglet **Installation à distance**.

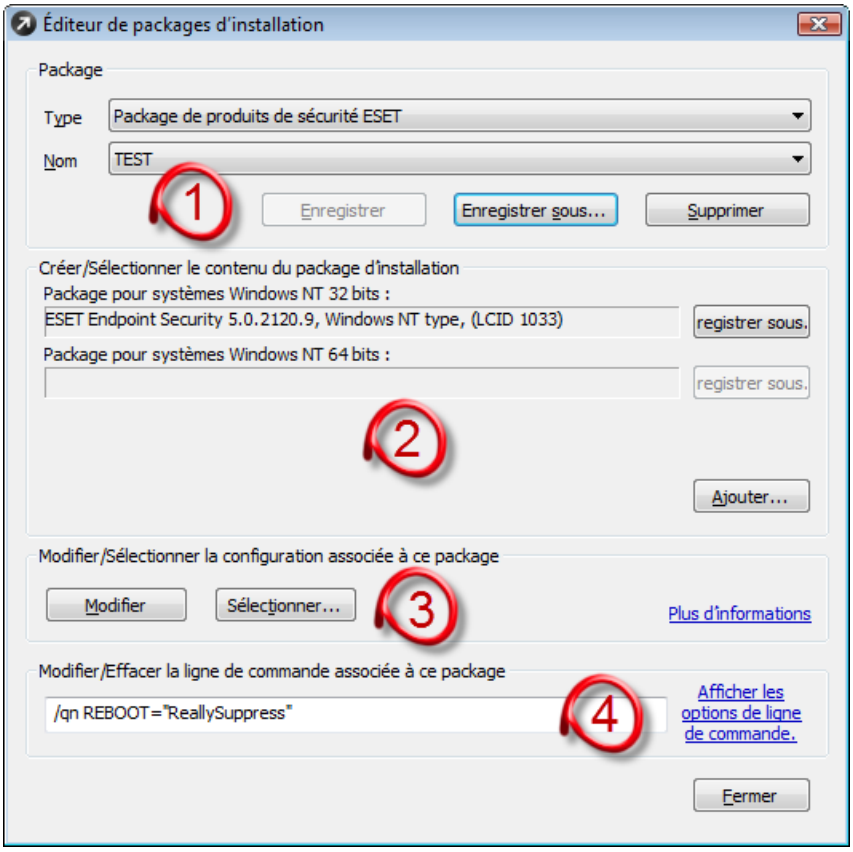
REMARQUE :: Si le service s'exécute sous le compte système local, aucun ordinateur n'est détecté à l'aide des recherches Shell et Wnet (réseau Windows). Cela provient du fait que le compte système local ne dispose pas des autorisations nécessaires pour effectuer ce type de recherche. Pour résoudre ce problème, changez les utilisateurs ou utilisez une autre méthode de recherche.

3.4.17.2 Packages d'installation

L'installation à distance est lancée via 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** et sélectionnez l'onglet **Ordinateurs**. Cliquez avec le bouton droit de la souris, puis sélectionnez **Gérer les packages** dans le menu contextuel. La fenêtre **Éditeur de packages d'installation** s'ouvre.



Chaque package d'installation est défini par un nom (voir (1) dans la figure 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 clients ESET (**3**)

Remarque : Lorsque vous créez un package d'installation, le mot de passe du serveur principal nécessaire à la connexion au serveur ERA n'est pas rempli. Cliquez sur **Modifier** pour modifier le fichier de configuration .xml de ce package et définissez le mot de passe (si nécessaire) dans la branche **Administration à distance** du produit concerné.

- Paramètres de ligne de commande attribués au package (**4**)

Le menu déroulant **Type** dans la section (1) permet d'accéder aux fonctionnalités complémentaires d'ERA. Outre l'installation à distance, il est également possible de désinstaller à distance les produits de sécurité ESET à l'aide de l'option **Désinstaller les produits de sécurité ESET pour Windows et NOD32 version 2**. Vous pouvez également installer à distance une application externe en sélectionnant **Package personnalisé**. Cette option est particulièrement utile si vous souhaitez exécuter plusieurs scripts et fichiers exécutables sur le client, y compris des outils de désinstallation pour des produits de sécurité d'éditeurs tiers ou des outils de nettoyage autonome. Vous pouvez indiquer des paramètres de ligne de commande personnalisés qui seront utilisés par le **Fichier d'entrée du package**. Consultez le chapitre Installation de produits tiers à l'aide d'ERA 140 pour plus de détails.

Un agent du programme 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 cible et ERAS. L'agent du programme d'installation à distance d'ESET est nommé *einstaller.exe*. Il contient le nom du serveur ERAS, ainsi que le nom et le type de package auquel il appartient. La section suivante fournit une description détaillée de l'agent du programme d'installation.

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. Les paramètres complémentaires pour ESET Smart Security et ESET NOD32 Antivirus peuvent être saisis après le nom du package d'installation *.msi* (par exemple, *eav_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.
- **REMOVE=...** : désactive l'installation d'un composant sélectionné. Les paramètres de commande de chaque composant sont répertoriés ci-dessous :

  Emon : protection du client de messagerie
  Antispam : protection antispam
  Dmon : protection de document
  ProtocolScan : filtrage des protocoles
  Firewall : pare-feu personnel
  eHttpServer : mettre à jour le dossier du miroir
  eDevmon : contrôle de périphérique
  MSNap : Microsoft NAP
  eParental : contrôle Web

- **REBOOTPROMPT =""** : après installation, une boîte de dialogue invitant l'utilisateur à confirmer le redémarrage s'affiche (ne peut pas être utilisé avec */qn*).
- **ADMINCFG ="chemin_vers_fichier_xml"** : durant l'installation, les paramètres définis dans les fichiers .xml spécifiés sont appliqués aux produits de sécurité ESET. Ce paramètre n'est pas obligatoire pour une installation à distance. Les packages d'installation contiennent leur propre configuration *.xml* qui est appliquée automatiquement.
- **PASSWORD="mot_de_passe"** : ajoutez ce paramètre si les paramètres ESS/EAV sont protégés par mot de passe.

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 (par exemple, *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 ="chemin_vers_fichier_xml"** : durant l'installation, les paramètres définis dans les fichiers *.xml* spécifiés sont appliqués aux solutions clients 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 qu'il souhaite redémarrer 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 d'ERA. Ce paramètre peut toujours être utilisé, même si les bibliothèques MFC sont disponibles.

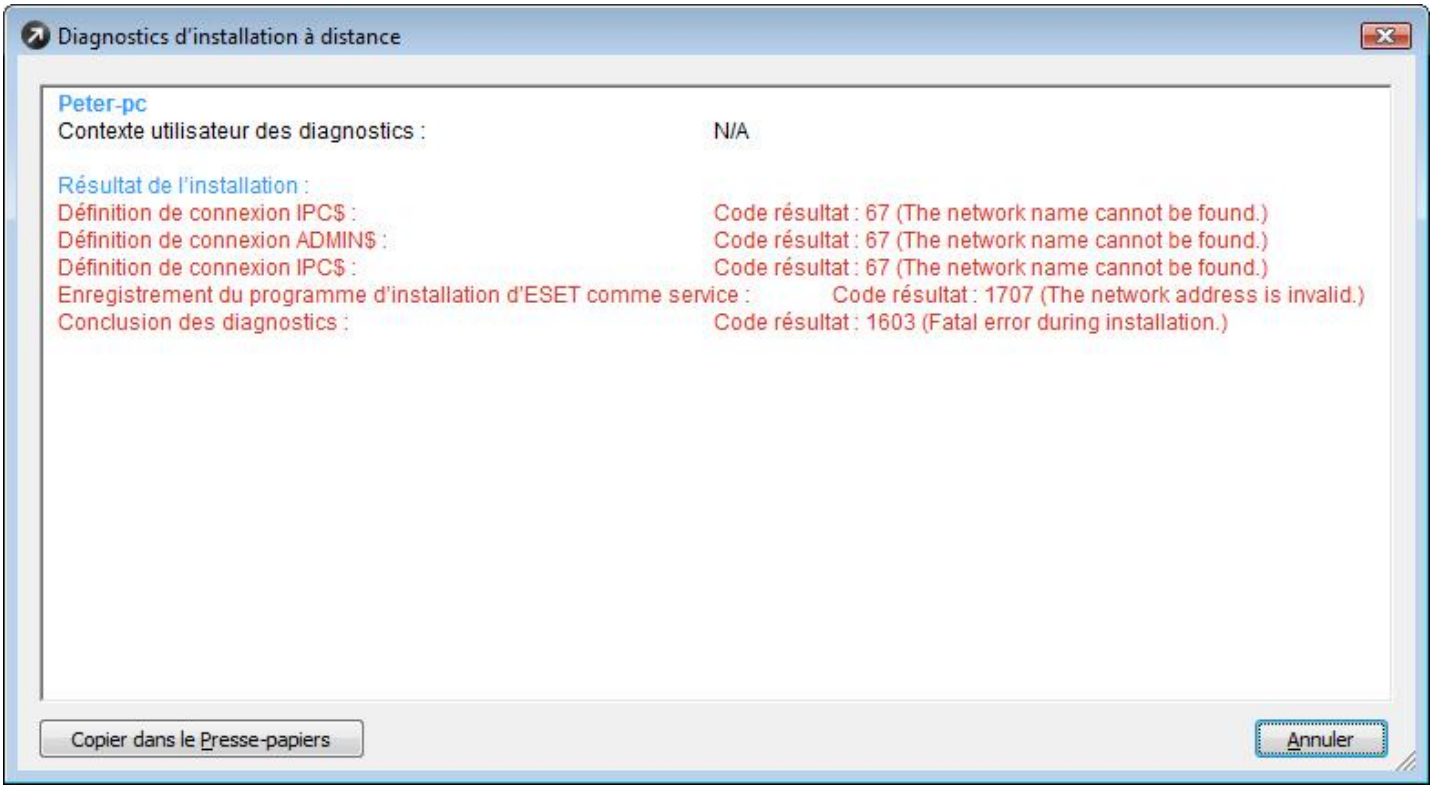
REMARQUE : Si le contrôle UAC est activé sur les solutions clients, les paramètres de sécurité UAC par défaut sur Windows Vista/7/2008 nécessitent la confirmation de l'utilisateur avant l'exécution du programme. Si vous essayez d'installer les solutions clients et que vous utilisez l'un des paramètres ci-dessus, une fenêtre contextuelle demandant l'intervention de l'utilisateur peut s'afficher sur le client. Afin d'éviter tout intervention de l'utilisateur, exécutez l'installation à l'aide de la commande suivante : *C:\Windows\System32\msiExec.exe -i chemin_vers_fichier_msi /qb! ADMINCFG="chemin_tp_vers_fichier_xml" REBOOT="ReallySupress"*, *C:\Windows\System32\msiExec.exe -i* étant l'exécutable du composant du programme d'installation Windows et le paramètre d'installation, et *chemin_vers_fichier_msi /qb! ADMINCFG="chemin_tp_vers_fichier_xml" REBOOT="ReallySupress"* est le chemin du fichier d'installation et le fichier de paramètre du produit de sécurité, suivi du paramètre de suppression de l'intervention de l'utilisateur.

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 (cliquez sur **Enregistrer sous**). Un tel package d'installation peut être exécuté manuellement 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.

REMARQUE : l'ajout d'une configuration au fichier d'installation *.msi* entraîne la fin de la validité de la signature numérique de ce fichier.

Important : Sous les systèmes d'exploitation Microsoft Windows Vista et ultérieurs, il est vivement conseillé de réaliser une installation à distance silencieuse (le paramètre */qn*, */qb*). Dans le cas contraire, l'interaction avec un utilisateur pourrait entraîner l'échec de l'installation à distance en raison du délai de connexion.

3.4.17.3 Diagnostics d'installation à distance



- **Définition de connexion IPC$** :

  L'administrateur doit disposer d'autorisations d'administration locales sur tous les ordinateurs clients.

  Les ressources partagées doivent être installées et activées sur le client.

  Les ressources partagées doivent être activées sur le pare-feu du réseau (ports 445 et 135-139).

  Le mot de passe de l'administrateur Windows ne doit pas être vierge.

  L'option « Utiliser le partage de fichiers simple » ne peut pas être activée dans un environnement combinant des groupes de travail et des domaines.

Assurez-vous que le service Serveur est exécuté sur l'ordinateur client.

- **Connexion à distance au Registre (informations du SE)** :

  Le service d'accès à distance au Registre doit être activé et démarré sur le client.

- **Ouverture à distance au Registre (informations du SE)** :

  Service ci-dessus + l'administrateur doit disposer d'un contrôle total sur le registre du client.

- **Lecture à distance au Registre (informations du SE)** :

  L'administrateur doit être autorisé à lire le registre du client. Si l'opération ci-dessus réussit, celle-ci doit réussir également.

- **Connexion à distance au Registre (informations du produit de sécurité ESET)** :

  L'administrateur doit disposer d'un contrôle total sur la clé HKEY_LOCAL_MACHINE/SOFTWARE/ESET (ou la branche HKEY_LOCAL_MACHINE/SOFTWARE entière).

- **Ouverture à distance au Registre (informations du produit de sécurité ESET)** :

  Assurez-vous que le service d'accès à distance au Registre est en cours d'exécution sur l'ordinateur client.

- **Définition de connexion ADMIN$** :

  Le partage administratif ADMIN$ doit être activé.

- **Copie du programme d'installation d'ESET** :

  Les ports 2222, 2223 et/ou 2224 doivent être ouverts sur le serveur et autorisés sur le pare-feu du réseau.

- **Définition de connexion IPC$** :

  Si cette opération a réussi lors de l'obtention de diagnostics d'information, elle doit également réussir ici.

- **Enregistrement du programme d'installation d'ESET comme service** :

  Assurez-vous que vous disposez des droits suffisants pour exécuter le fichier einstaller.exe sur les ordinateurs cibles.

REMARQUE : En cas d'erreur au cours des diagnostics, vous pouvez commencer à les résoudre sur la base de ces informations. Consultez le chapitre Configuration requise 54 avant l'installation et le chapitre Codes d'erreur fréquemment rencontrés 134 afin d'analyser les codes d'erreur.

3.4.17.4 Tâches d'installation

L'onglet **Tâches d'installation** de l'onglet **Installation à distance** reprend une liste de tâches et leurs attributs. Vous pouvez modifier le nombre d'éléments à afficher et cliquer avec le bouton droit de la souris sur les tâches de la liste afin de découvrir les options de gestion/de maintenance. Augmentez ou diminuez le nombre d'éléments affichés par page à l'aide du menu déroulant **Éléments à afficher** et des boutons de navigation adjacents pour naviguer entre les pages disponibles.

Vous pouvez également filtrer les informations figurant dans l'onglet Tâches d'installation. Cochez l'option **Utiliser le filtre** dans le volet de gauche pour activer le filtre. Définissez ensuite les critères de filtre des tâches : **Uniquement des clients comme (?,*)/Exclure les clients comme (?,*)**. Saisissez le nom d'ordinateur dans le champ **Nom d'ordinateur**. Vous pouvez également utiliser des caractères génériques, par exemple *ordi* au lieu d'indiquer le mot complet « ordinateur ». Si vous cliquez sur le bouton **Réinitialiser**, les paramètres de filtre sont supprimés et le filtre est désactivé.

- **Nom de la tâche** : nom de la tâche ; pour les tâches prédéfinies, il s'agit du même nom que le type de tâche.
- **Type de tâche** : type de la tâche. Pour plus d'informations, reportez-vous au chapitre Tâches 64.
- **État** : état d'avancement actuel de la tâche.
- **Description** : brève description de la tâche.
- **Date de déploiement** : temps restant avant l'exécution de la tâche ou écoulé depuis celle-ci.
- **Date de réception** : temps restant ou temps écoulé depuis la réception de la tâche jusqu'à son point d'exécution.
- **Commentaire** : remarque associée à la tâche d'installation.

Lorsque vous double-cliquez sur une tâche d'installation, elle s'affiche dans la fenêtre **Propriétés**.

3.5 Options ERA Console

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

3.5.1 Connexion

Pour accéder aux paramètres de la ERA Console, ouvrez le menu principal d'ERAC en cliquant sur **Outils** > **Options de la console...** ou **Fichier** > **Modifier les connexions**. Cet onglet permet de configurer la connexion d'ERAC à ERAS. Pour obtenir des détails, consultez le chapitre Connexion à l'ERAS 23

L'onglet **Connexion** permet de sélectionner le serveur auquel vous souhaitez vous connecter et d'indiquer si la connexion doit être établie au démarrage de la ERA Console. La console ne peut être connectée qu'à un seul serveur à la fois. Si vous voulez ajouter des serveurs répliqués, vous devez configurer une réplication dans le menu Outils/Options du serveur/Paramètres de réplication... 100.

REMARQUE : le port pour la connexion à ERA Server peut être personnalisé sous **Outils** > **Options du serveur** > onglet **Autres paramètres** (consultez le chapitre Autres paramètres 106).

Ajouter/Supprimer... : permet d'ajouter de nouveaux serveurs ERA Server ou de modifier des serveurs existants. Le fait de cliquer sur cette option permet d'ouvrir la fenêtre **Modification de connexion**. Pour ajouter une nouvelle connexion, saisissez l'adresse IP ou le nom d'hôte du serveur, le port à utiliser pour la connexion et un commentaire (facultatif). Cliquez sur le bouton **Ajouter/Supprimer** pour ajouter la connexion à la liste des serveurs, dans la partie supérieure de la fenêtre. Sélectionnez un serveur spécifique pour les options supplémentaires : vous pouvez le **supprimer**, utiliser l'option **Supprimer tout** ou modifier la connexion (semblable à la création d'une nouvelle connexion).

- **Connecter au serveur sélectionné au démarrage de la console** : la console se connecte automatiquement au serveur ERA Server prédéfini.
- **Afficher un message en cas d'échec de la connexion** : en cas d'erreur de communication, un message d'alerte s'affiche.

3.5.2 Colonnes

Cet onglet permet de spécifier les attributs (colonnes) affichés sous les différents onglets. Les modifications se reflètent dans le mode d'affichage personnalisé (Onglet Clients 29). Les autres modes ne peuvent pas être modifiés.

Pour afficher une colonne sur un onglet en particulier, cliquez sur son nom dans la liste des onglets, puis cochez la ou les colonnes à afficher.

- **Sélectionnez le volet** : choisissez le volet dont vous souhaitez changer la liste des colonnes à afficher.
- **Sélectionnez les colonnes à afficher** : choisissez les colonnes que vous souhaitez afficher dans le volet. Faites votre choix avec soin ; sélectionnez toutes les informations dont vous avez besoin, mais veillez en même temps à ce que l'affichage reste clair.
- **Effacer tout** : désélectionne toutes les cases à cocher de la fenêtre **Sélectionnez les colonnes à afficher** pour le volet sélectionné.
- **Définir tout** : sélectionne toutes les cases à cocher de la fenêtre **Sélectionnez les colonnes à afficher** pour le volet sélectionné.
- **Par défaut** : réinitialise toutes les cases à cocher de la fenêtre **Sélectionnez les colonnes à afficher** pour le volet sélectionné.
- **Définir tout par défaut** : réinitialise toutes les cases à cocher de la fenêtre **Sélectionnez les colonnes à afficher** pour le volet sélectionné.

3.5.3 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 : Ancienne version ou n.a**).

Vous pouvez affecter une couleur spécifique aux volets et aux colonnes en les sélectionnant dans la liste **Volet et colonne**. Sélectionnez ensuite leur couleur d'affichage.

REMARQUE : pour la colonne **Clients : ancienne version ou n.a.**, la couleur est utilisée quand la version de la base de données des virus d'ESET Smart Security sur le client n'a pas été ajoutée ou est plus ancienne que celle disponible sur le serveur. Elle est également utilisée lorsque la version du produit de sécurité ESET sur le serveur est plus ancienne que celle disponible sur le client ou n'a pas été ajoutée.

Dans la colonne **Clients : dernière connexion**, vous pouvez indiquer l'intervalle de la période de coloration.

3.5.4 Chemins

Pour accéder aux paramètres de la ERA Console, ouvrez le menu principal d'ERAC en cliquant sur **Outils** > **Options de la console...**

L'onglet **Chemins** permet de sélectionner l'emplacement où stocker les rapports générés par la ERA Console. Pour plus d'informations sur la génération et la consultation des rapports, reportez-vous au chapitre Rapports 36 de ce fichier d'aide.

3.5.5 Date/Heure

Le volet **Date/Heure** permet de personnaliser des options avancées pour la ERA Console. Il permet également de choisir le format d'affichage de l'heure dans les enregistrements de la fenêtre de la ERA Console.

- **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)** : cochez cette case pour recalculer l'heure en heure locale. Sinon, l'heure GMT - UTC sera affichée.

3.5.6 Autres paramètres

Le volet **Autres paramètres** permet de configurer des options avancées de la ERA Console d'ESET.

1. Paramètres de filtre

Appliquer les modifications automatiquement : quand cette option est activée, les filtres dans 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 les modifications**.

REMARQUE : Si la console ERA Console doit être connectée en permanence à un serveur ERA Server à partir du PC de l'administrateur, il est recommandé de sélectionner l'option **Afficher dans la barre des tâches en cas de réduction** et de laisser la console en mode d'affichage réduit lorsqu'elle est inactive. En cas de problème, l'icône Systray vire au rouge, ce qui constitue un signal d'intervention pour l'administrateur. Il est également recommandé d'ajuster l'option **Utiliser l'icône de la barre système en surbrillance en cas de clients problématiques** (événements déclenchant le changement de couleur de l'icône).

Mises à jour d'ESET Remote Administrator : cette section permet de contrôler la disponibilité de nouvelles versions de la console ESET Remote Administrator. Il est recommandé d'utiliser la valeur par défaut (mensuelle). Si une nouvelle version est disponible, la ERA Console affiche une notification au démarrage du programme.

2. Autres paramètres

- **Utiliser le rafraîchissement automatique (minutes)** : les données sont automatiquement actualisées sous les différents onglets dans l'intervalle choisi.
- **Afficher le quadrillage** : activez cette option pour séparer les cellules de tous les onglets à l'aide d'un quadrillage.
- **Afficher le client sous la forme « serveur/nom » plutôt que « serveur/ordinateur/MAC »**: affecte le mode

d'affichage des clients dans certaines boîtes de dialogue (p. ex., **Nouvelle tâche**). Ce changement est visuel uniquement.

- **Utiliser l'icône de la barre système** : la console ERA Console sera représentée par une icône dans la barre d'état système de Windows.
- **Afficher dans la barre des tâches en cas de réduction** : si la fenêtre de la console ERA Console est réduite, elle sera accessible via la barre des tâches Windows.
- **Utiliser l'icône de la barre système en surbrillance en cas de clients problématiques** : utilisez cette option, avec le bouton **Modifier** pour définir les événements qui déclencheront la modification de la couleur de l'icône dans la barre système.
- **Utiliser le nom d'hôte au lieu de l'adresse IP lors de l'exécution d'une action réseau** : lors de l'exécution d'actions réseau sur un client (décrites dans la section Onglet Clients 29), vous pouvez choisir d'utiliser un nom d'hôte au lieu d'une adresse IP.
- **Messages d'informations facultatifs** : désactive (option **Désactiver tout**) ou active (option **Activer tout**) tous les messages d'informations. Si cette option est activée, vous trouvez des messages soulignés et en bleu dans la console ERA Console. Si vous cliquez sur ces messages, ils ouvrent des conseils et astuces sur l'utilisation du produit.

3.6 Modes d'affichage

ERAC offre deux modes d'affichage :

- **Mode administratif** : 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.
- **Mode lecture seule** : 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 les paramètres de l'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 l'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), ou utilisez l'outil Gestionnaire des utilisateurs 95.

3.7 Éditeur de configuration d'ESET

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 ou stratégies aux clients
- Un fichier de configuration (.xml) général

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

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

Pour que Éditeur de configuration fonctionne, les fichiers suivants doivent être disponibles : *eguiHipsRa.dll*, *eguiHipsRaLang.dll*, *eguiRuleManagerRa.dll* et *eset.chm*.

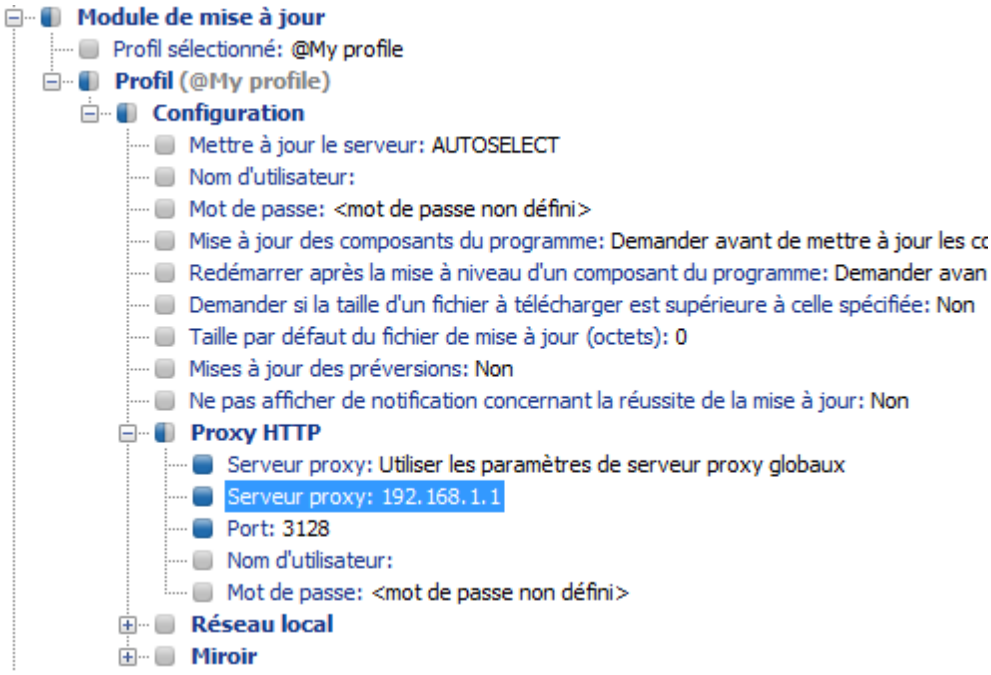
3.7.1 Superposition de configuration

Si une valeur est modifiée dans 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 annuler les modifications précédentes.

La figure ci-dessous reprend un exemple. Dans cette configuration, le nom d'utilisateur *EVA-12345678* et le mot de passe sont insérés et l'utilisation d'un serveur proxy est interdite.

La deuxième configuration (illustrée dans la figure ci-dessous) envoyée aux clients garantira la conservation des modifications antérieures, y compris le nom d'utilisateur *EVA-12345678* et le mot de passe. Cette configuration permet également d'utiliser un serveur proxy et définit son adresse et son port.



3.7.2 Entrées de configuration clés

Dans cette section, nous expliquons plusieurs des entrées de configuration clés pour la gamme de produits pour Windows versions 3 et 4 :

- **Gamme de produits Windows v3 et v4** > **Noyau ESET** > **Paramètres** > **Administration à distance**
  Vous pouvez activer ici la communication entre les ordinateurs client et l'ERAS (**Connexion au serveur d'administration à distance**). Saisissez le nom ou l'adresse IP d'ERAS (**Adresse du serveur principal/secondaire**). 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 obtenir des informations supplémentaires, consultez l'option **Mot de passe pour les clients** dans le chapitre Onglet Sécurité 94. Cette section propose également des informations supplémentaires sur la configuration du mot de passe.

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

- **Noyau ESET** > **Paramètres** > **ESET Live Grid**
  Cette branche définit le comportement du système d'avertissement anticipé ESET Live Grid 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 les fichiers suspects** et **Autoriser la soumission d'informations statistiques anonymes** sont particulièrement importantes : Si ces options sont définies respectivement sur **Ne pas soumettre** ou sur **Non**, le système ESET Live Grid 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 > Paramètres avancés > Modifier les paramètres avancés > ERA Server > Configuration > Serveur proxy**).

- **Noyau ESET** > **Paramètres** > **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 ESET** > **Paramètres** > **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.

- **Noyau ESET** > **Paramètres** > **Valeurs d'interface utilisateur par défaut**
  Les paramètres sous Valeurs d'interface utilisateur par défaut (à savoir, **Afficher l'écran de démarrage**/**Ne pas afficher l'écran de démarrage**) appliquent uniquement les modifications aux paramètres par défaut du client. Les paramètres du client peuvent être gérés ensuite par utilisateur et ne peuvent être modifiés à distance. Pour modifier les paramètres à distance, la valeur de l'option **Supprimer les paramètres utilisateur** doit être **Oui**. L'option **Supprimer les paramètres utilisateur** est disponible uniquement pour les clients qui utilisent des produits de sécurité ESET des versions 4.0 ou suivantes.

- **Module**
  Cette branche de 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 défini sur **Choisir automatiquement**, toutes les mises à jour seront téléchargées à partir des serveurs de mise à jour d'ESET. Dans ce cas, utilisez 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 le chapitre Serveur Miroir 103. Pour obtenir des informations supplémentaires sur l'utilisation du planificateur, consultez le chapitre Planificateur 137.

REMARQUE : Sur des périphériques mobiles tels que des ordinateurs portables, vous pouvez configurer deux profils, l'un pour effectuer la 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 obtenir des informations supplémentaires, consultez le chapitre Mise à jour combinée pour les portables 139 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 53 sur des stations de travail ou à distance 44 à partir d'ERAS. Ce chapitre décrit également d'autres méthodes d'installation à distance.

REMARQUE : bien que 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).

Important : Les administrateurs qui utilisent une connexion Microsoft Remote Desktop pour accéder aux clients distants doivent prendre connaissance de l'article suivant avant d'effectuer l'installation à distance d'ESET Smart Security.

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 5.x, 4.x, 3.x et 2.x des solutions client ESET :

- Version 5.x : appliquez les mêmes étapes que pour la version 4.x.

REMARQUE :: Vous pouvez ensuite installer les produits de sécurité ESET pour Linux et Mac après la sortie des clients de la version 5.

- Version 4.x : téléchargez le fichier d'installation (p. ex., *ess_nt32_enu.msi*) depuis *eset.com* et créez votre propre package d'installation dans **Éditeur de packages d'installation**. Modifiez/sélectionnez la configuration que vous voulez associer à ce package, cliquez sur le bouton **Copier...** à côté du champ **Package pour systèmes Windows NT xx bits** , puis enregistrez le package sous **Fichier Msi d'installation d'ESET avec configuration (*.msi)**.

  REMARQUE : l'ajout d'une configuration au fichier d'installation *.msi* entraînera la fin de la validité de la signature numérique de ce fichier. De plus, les étapes des versions 3.x s'appliquent également à la version 4.x.

- Version 3.x : téléchargez le fichier d'installation (p. ex., *ess_nt32_enu.msi*) depuis *eset.com*. Copiez le fichier de configuration (*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* possède un autre nom ou s'il se trouve à un autre endroit, le paramètre *ADMINCFG ="chemin_au_fichier_xml"* peut être utilisé (p. ex. :*ess_nt32_enu.msi ADMINCFG ="\\server\xml\settings.xml"* pour appliquer la configuration stockée sur un lecteur réseau).

REMARQUE : Si vous installez ESET Smart Security (pare-feu personnel inclus), vous devez autoriser le partage et l'administration à distance de ces solutions. Sinon, la communication réseau entre ces clients et ERA Server serait bloquée.

4.2 Installation à distance

L'installation à distance évite d'avoir à préinstaller ou à installer physiquement les produits de sécurité sur les ordinateurs clients. ERA offre plusieurs méthodes d'installation à distance.

La procédure d'installation à distance à l'aide d'ERA se compose des étapes suivantes :

- Création de packages d'installation

  Tout d'abord, vérifiez la configuration requise 54 pour l'installation à distance.

  Créez ensuite les packages d'installation 44 qui sont distribués sur les clients.

- Distribution des packages aux stations de travail client (méthode d'installation poussée, script d'ouverture de session, email, solution externe) :

  Vérifiez/Configurez l'environnement réseau pour une installation à distance.

Distribuez les packages d'installation sur des clients. Il existe plusieurs méthodes d'installation à distance :

Installation poussée à distance 55. C'est la méthode la plus efficace pour distribuer les produits de sécurité sur vos clients.

Vous pouvez également effectuer une installation à distance par ouverture de session ou par email 57.

Si vous ne souhaitez pas utiliser les méthodes ci-dessus, vous pouvez effectuer une installation distante personnalisée 60.

Si d'anciens produits de sécurité ESET sont installés sur des clients, vous devez les mettre à niveau vers la dernière version ; reportez-vous au chapitre Mettre à niveau le client 61. S'ils disposent déjà de la dernière version, consultez le chapitre Éviter des installations répétées 62. Pour installer les packages dans un environnement d'entreprise, reportez-vous au chapitre Installation dans un environnement d'entreprise 63.

4.2.1 Configuration requise

L'installation à distance nécessite 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 :

Windows

- 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

REMARQUE :: les versions récentes de Microsoft Windows (Windows Vista, Windows Server 2008 et Windows 7) appliquent des stratégies de sécurité qui limitent les autorisations des comptes des utilisateurs locaux, ce qui signifie que l'utilisateur ne pourra peut-être pas exécuter certaines opérations de réseau. Si votre service ERA est exécuté sous un compte d'utilisateur local, des problèmes d'installation poussée pourraient survenir dans certaines configurations de réseau (par exemple, lors de l'installation à distance depuis un domaine vers un groupe de travail). En cas d'utilisation de Windows Vista, Windows Server 2008 ou Windows 7, il est conseillé d'exécuter le service ERA sous des comptes possédant les privilèges de réseau suffisants. Pour désigner le compte utilisateur sous lequel vous souhaitez exécuter ERA, accédez au menu **Démarrer** ? **Panneau de configuration** ? **Outils d'administration** ? **Services**. Choisissez le service ESET Remote Administrator Server dans la liste et cliquez sur l'onglet **Ouverture de session**. ESET Remote Administrator 5 intègre ce paramètre dans le scénario d'installation avancé ; vous devez par conséquent choisir **Avancée** ? **Installation totalement personnalisée** lors de l'installation.

Important : Si vous utilisez l'**installation poussée** sur des stations de travail cible Windows Vista, Windows Server 2008 ou Windows 7, vérifiez que ERA Server et les stations de travail cible se trouvent dans un domaine.

Nous recommandons également à l'administrateur de désactiver le contrôle UAC (User Access Control) pour Windows Vista, Windows 7 et Windows Server 2008. Pour ce faire, cliquez sur **Démarrer** > **Panneau de configuration** > **Comptes utilisateur** > **Activer ou désactiver le contrôle des comptes d'utilisateurs**, ou cliquez sur **Démarrer** > saisissez **Msconfig** dans le champ de recherche, puis appuyez sur la touche **Entrée** > **Outils** > **Désactiver le Contrôle de compte d'utilisateur (nécessite un redémarrage)**.

Il est vivement conseillé de vérifier toutes les exigences avant l'installation, surtout si le réseau compte plusieurs stations de travail (dans l'onglet **Installation à distance**, sélectionnez l'onglet **Ordinateurs**, cliquez avec le bouton droit de la

souris sur le ou les clients pertinents, puis choisissez l'option **Diagnostics de l'installation poussée** dans le menu contextuel).

Important : Les administrateurs qui utilisent une connexion Microsoft Remote Desktop pour accéder aux clients distants doivent prendre connaissance de l'article suivant avant d'effectuer l'installation à distance d'ESET Smart Security.

4.2.1.1 Conditions requises pour une installation poussée Linux/Mac

Veillez à ce que tous les postes de travail client soient configurés correctement avant d'effectuer une installation distante.

- **Linux**

1. L'ordinateur doit pouvoir se connecter au serveur via SSH.
2. Le compte SSH doit disposer de droits d'administrateur. Autrement dit, vous devez exécuter l'installation en tant qu'utilisateur racine (UID=0) ou en tant qu'utilisateur doté de droits sudo.

- **Mac**

1. L'ordinateur doit pouvoir se connecter au serveur via SSH.
2. Le compte SSH doit disposer de droits d'administrateur. Autrement dit, vous devez exécuter l'installation en tant qu'administrateur.

Remarque: Cette fonctionnalité est prise en charge par ESET NOD32 Antivirus Business Edition pour Mac OS X 4.1.94 et ESET NOD32 Antivirus Business Edition pour Linux Desktop 4.0.79, ainsi que par toutes les versions ultérieures pour ces deux plateformes.

4.2.2 Installation poussée à distance

Cette méthode d'installation à distance pousse des solutions clients ESET sur des ordinateurs distants. L'installation poussée est la méthode d'installation la plus efficace. Pour qu'elle fonctionne, tous les postes de travail cibles doivent être en ligne. Avant de lancer une installation poussée, téléchargez les fichiers d'installation .msi pour ESET Smart Security ou ESET NOD32 Antivirus depuis le site Web d'ESET et créez un package d'installation. Vous pouvez créer un fichier de configuration .xml qui sera appliqué automatiquement lors de l'exécution du package. Consultez le chapitre sur la Configuration requise 54 avant de lancer l'installation.

Pour lancer une installation poussée, procédez comme suit :

1) Dès que les ordinateurs qui conviennent à l'installation à distance sont repris sous l'onglet **Ordinateurs**, vous pouvez les sélectionner tous ou quelques-uns et lancer une tâche d'installation poussée en cliquant avec le bouton droit de la souris dans la fenêtre et en sélectionnant l'option **Installation poussée** dans le menu contextuel.

2) Définissez les informations d'ouverture de session pour les ordinateurs dans la liste (**Définir**, **Définir tout**). Cette opération doit être réalisée à l'aide d'un compte possédant les privilèges d'administrateur. Vous pouvez toujours ajouter des clients à la liste dans cette étape grâce à la fonctionnalité spéciale **Ajouter des clients**.

3) Sélectionnez le package d'installation 44 souhaité à livrer aux postes de travail cibles.

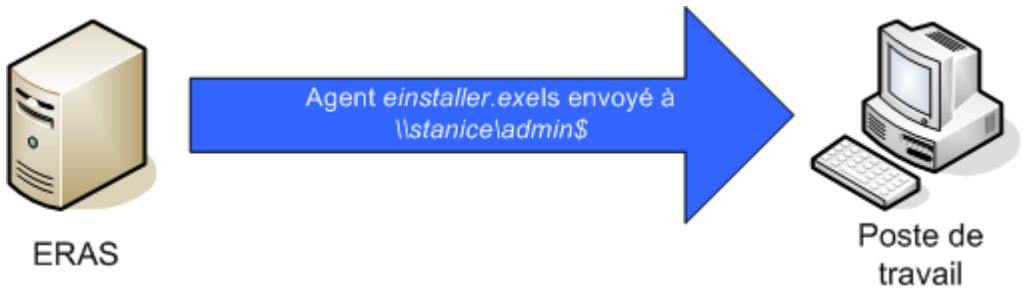
4) Définissez l'heure à laquelle la tâche doit être exécutée, puis cliquez sur **Terminer**.

L'état de la tâche d'installation poussée apparaît dans l'onglet Tâches d'installation 47. Pour les détails des résultats du diagnostic, sélectionnez la tâche souhaitée, puis enfoncez la touche F4. La fenêtre **Propriétés** s'ouvre sur l'onglet **Détails**. Vous pouvez y afficher les résultats du diagnostic d'installation à distance en cliquant sur **Afficher tous les journaux/Afficher les journaux sélectionnés**.

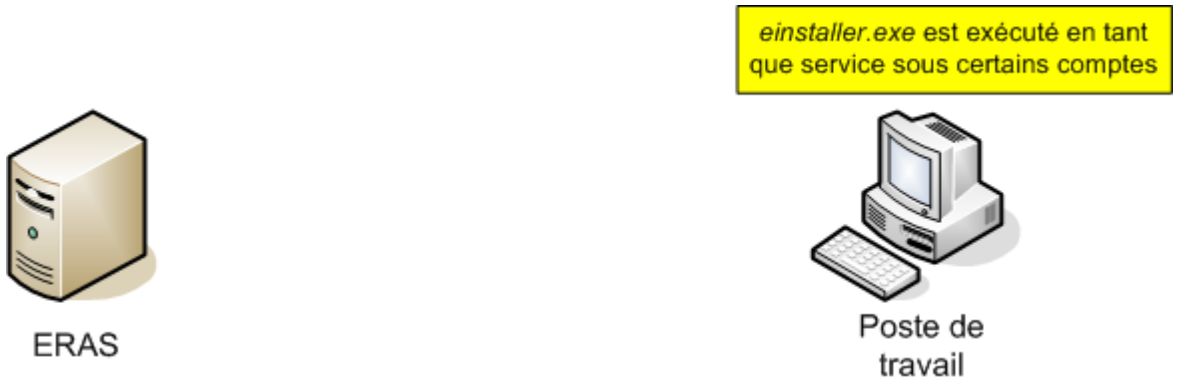
REMARQUE : par défaut, le nombre maximum de threads simultanés d'installation poussée est limité à 20. Si vous envoyez une tâche d'installation poussée à un nombre d'ordinateurs supérieur à cette limite, les ordinateurs excédentaires seront placés dans une file d'attente jusqu'à ce que des threads soient disponibles. Pour des raisons de performances, il est déconseillé d'augmenter cette valeur ; toutefois, si cela vous semble nécessaire, vous pouvez modifier la limite dans Éditeur de configuration (**ESET Remote Administrator** > **ERA Server** > **Configuration** > **Installation à distance**).

Les détails de la procédure d'installation à distance sont décrits ci-dessous :

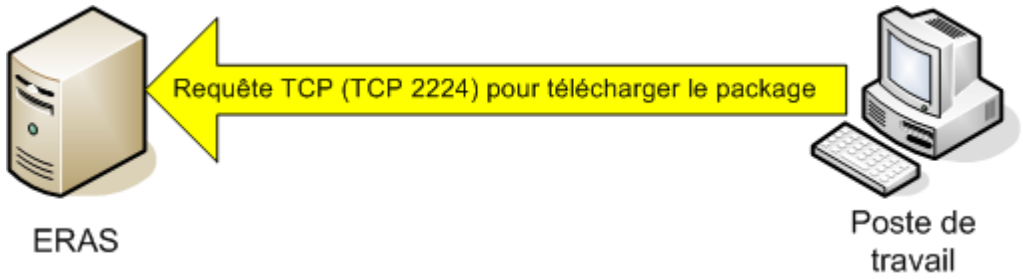
5) ERAS envoie l'agent *einstaller.exe* à la station de travail à l'aide du partage administratif admin$.



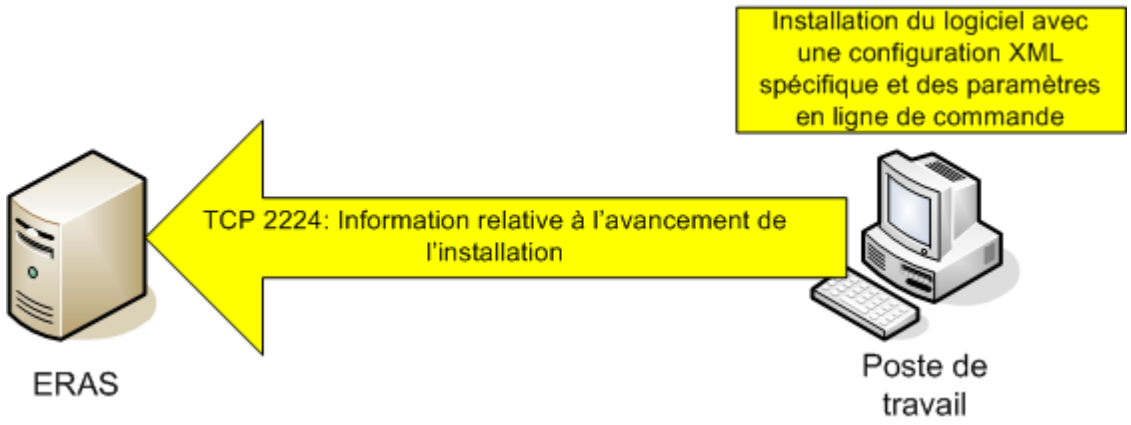
6) L'agent démarre en tant que service sous le compte système.



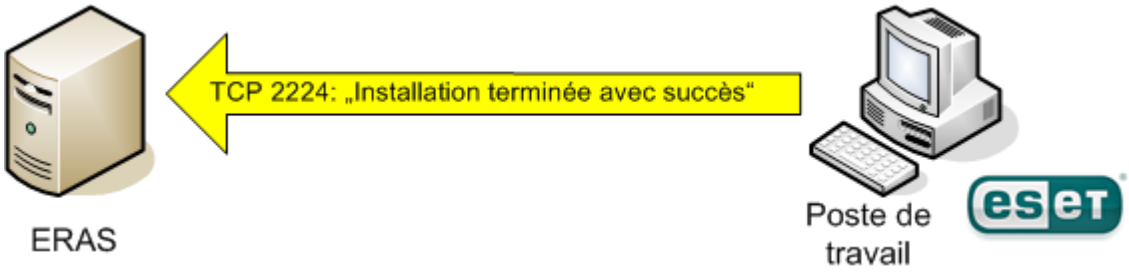
7) L'agent établit une communication avec son ERAS « parent » et télécharge le package d'installation correspondant sur le port TCP 2224.



8) L'agent installe le package sous le compte d'administrateur défini à l'étape 2 ; le fichier de configuration *.xml* correspondant et les paramètres de ligne de commande sont également appliqués.



9) 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.



4.2.3 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 le chapitre Installation à distance personnalisée 60).

La méthode par ouverture de session est bien adaptée aux ordinateurs portables qui sont souvent utilisés hors du réseau local. L'installation est exécutée après l'ouverture de session dans le domaine.

Alors que le script d'ouverture de session s'exécute automatiquement lorsque l'utilisateur ouvre une session, la méthode Email requiert l'intervention de l'utilisateur qui doit lancer l'agent einstaller.exe à partir de la pièce jointe à l'email. Si einstaller.exe est lancé plusieurs fois, il ne déclenche pas d'autre installation de solutions client ESET. Pour plus d'informations, consultez le chapitre Éviter des installations répétées 62.

Pour obtenir la procédure détaillée d'exportation du programme d'installation d'ESET dans un dossier/script de connexion, consultez ce chapitre 58.

Envoyer le programme d'installation d'ESET par email

Tout d'abord, choisissez le type du programme d'installation ESET.

- **Produits de sécurité ESET pour Windows**

1. Sélectionnez un package créé au préalable dans le menu déroulant **Package**.
2. Saisissez l'adresse email du destinataire dans le champ **À**.
3. Vous pouvez également modifier l'**objet** et la **description** de l'email, puis cliquer sur **Envoyer** pour envoyer l'agent *einstaller.exe* à l'utilisateur.

- **Désinstaller les produits de sécurité ESET pour Windows et NOD32 version 2**

Ce type permet de désinstaller tous les produits de sécurité ESET de l'ordinateur de l'utilisateur.

- **Produits de sécurité ESET pour Android**

Important : avant de poursuivre, lisez d'abord ce chapitre 76.

1. Cliquez sur **...** à côté du champ de **pièce jointe**, puis accédez à l'emplacement d'enregistrement du votre produit de sécurité ESET pour Android (fichier *.apk*). Sélectionnez cette application et cliquez sur **OK**.
2. Saisissez l'adresse email de l'utilisateur, vérifiez et modifiez le cas échéant les informations des champs **Objet** et **Description**, puis cliquez sur **...** à côté du lien de configuration. La fenêtre **Paramètres du lien de configuration** s'affiche et vous pouvez y configurer le mode de connexion du produit à ERA.

Remarque : Ce lien configure le produit de sécurité ESET pour Android qui doit être installé (vous pouvez envoyer à l'utilisateur un lien avec le fichier d'installation ou envoyer l'application directement en suivant les indications de l'étape 1).

3. Les champs **Serveur** et **Port** sont prédéfinis en fonction de votre serveur ERA actuel. Si les utilisateurs doivent fournir un mot de passe pour se connecter au serveur, saisissez-le dans le champ **Mot de passe**. Dans le cas contraire, ce champ peut rester vide. Si vous utilisez un mot de passe, l'option **Ajouter la carte SIM actuelle aux cartes de confiance** doit être sélectionnée. Cette option est sélectionnée par défaut pour éviter le verrouillage du téléphone portable lors d'une tentative de connexion au serveur ERA. Ces paramètres de base seront envoyés au client. Pour les paramètres avancés (par exemple le **nom d'utilisateur** et le **mot de passe** de la mise à jour), le client doit être connecté au serveur ERA et vous pouvez distribuer ces paramètres à l'aide d'une règle 71.

- **Package personnalisé**

Vous pouvez envoyer un package d'installation personnalisé (décrit ici 44) à un utilisateur sélectionné.

4.2.3.1 Exportation du programme d'installation d'ESET dans un dossier/script de connexion

Vous pouvez utiliser un éditeur de texte ou tout autre outil propriétaire pour insérer la ligne appelant *einstaller.exe* dans le script de connexion. De même, *einstaller.exe* peut être envoyé en tant que pièce jointe d'email via tout client de messagerie. Quelle que soit la méthode utilisée, veillez à 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.

Saisissez le chemin d'accès du fichier *einstaller.exe* dans le script de connexion :

1) Cliquez avec le bouton droit de la souris sur une entrée de l'onglet **Installation à distance**, cliquez sur **Exporter dans le dossier ou le script de connexion**, puis sélectionnez le **type** et le nom du **package** à installer.

2) Cliquez sur **...** près du champ **Dossier** pour sélectionner le répertoire où le fichier *einstaller.exe* est situé et disponible dans le réseau, puis cliquez sur **OK**.

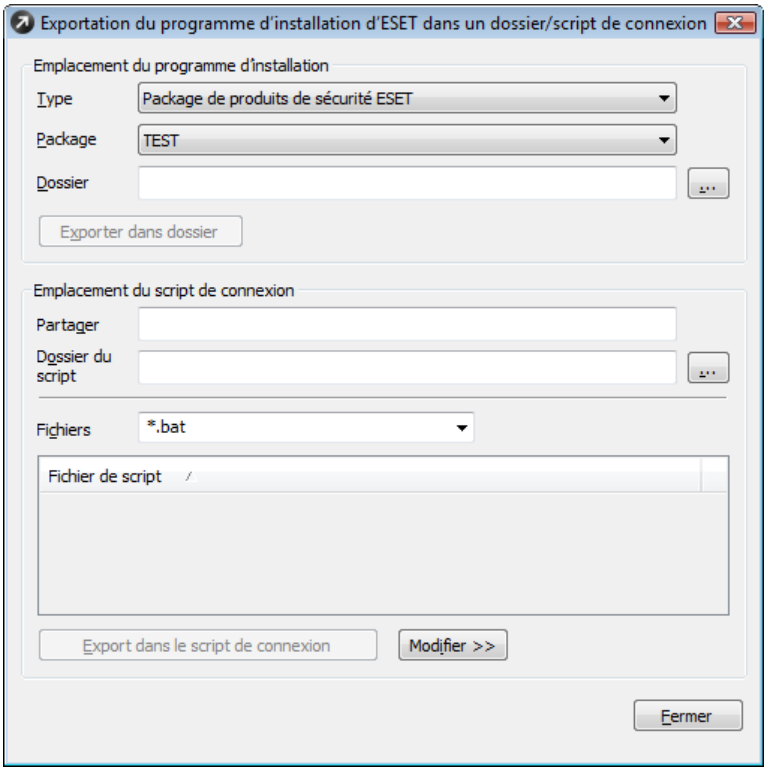
3) Dans le champ **Partager**, assurez-vous que le chemin d'accès est correct ou modifiez-le si nécessaire.

4) 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**).

5) Dans la section **Fichiers**, sélectionnez le fichier dans lequel insérer la ligne appelant *einstaller.exe*.

6) Cliquez sur **Export dans le script de connexion** pour insérer la ligne.

7) Vous pouvez modifier l'emplacement de la ligne en cliquant sur **Modifier >>**, puis l'enregistrer en cliquant sur le bouton **Enregistrer**.



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

1) Dans l'onglet **Installation à distance**, cliquez sur **Email...**, puis sélectionnez le **type** et le nom du **Package** que vous souhaitez installer.

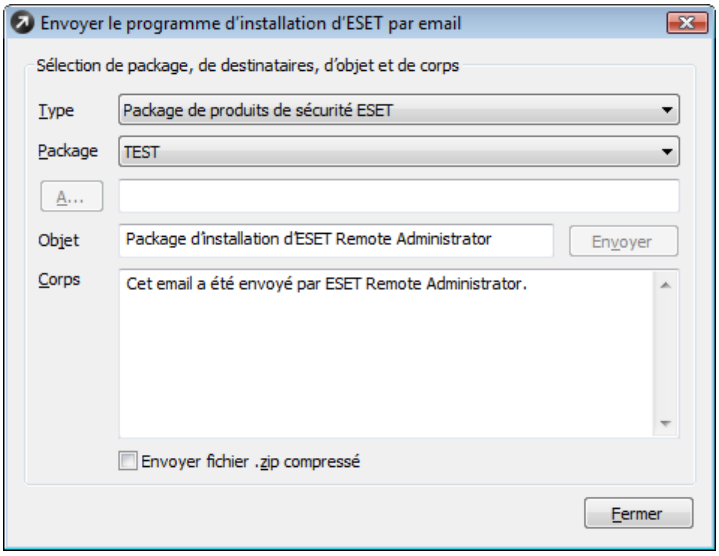
2) Cliquez sur **À...** pour sélectionner des destinataires dans le carnet d'adresses (ou insérer des adresses individuelles).

3) Saisissez un **objet** dans le champ correspondant.

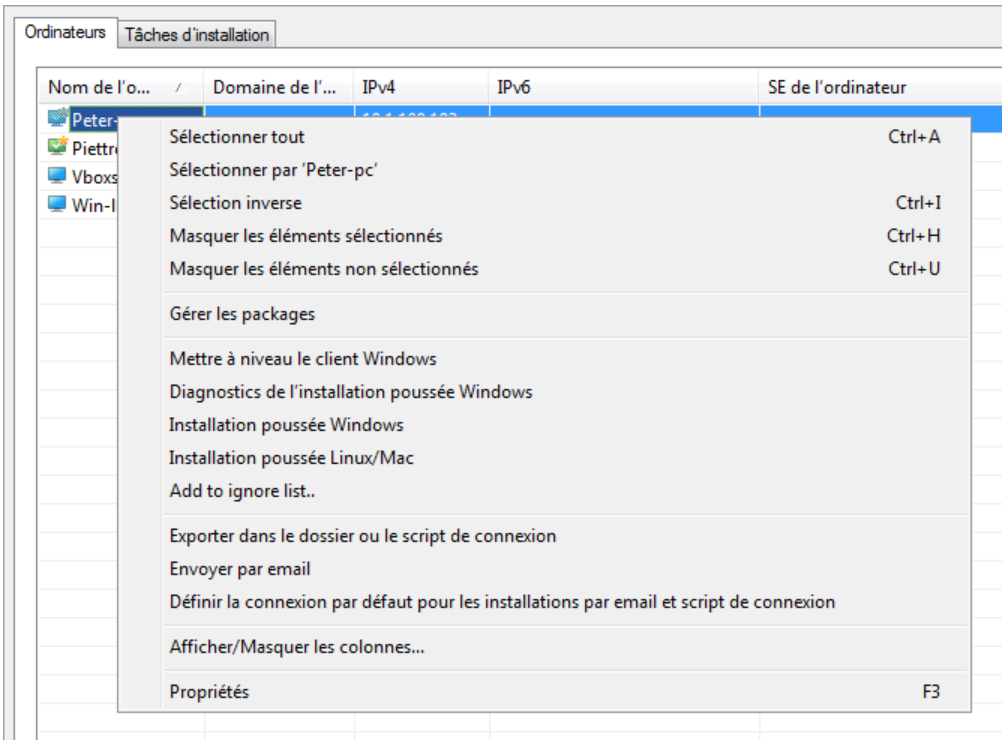
4) Tapez un message dans l'espace réservé au **corps** du message.

5) Cochez la case **Envoyer fichier .zip compressé** si vous voulez envoyer l'agent en tant que package compressé.

6) Cliquez sur **Envoyer** pour expédier le message.



Durant le processus d'installation à distance, une connexion inversée à ERAS a lieu et l'agent (*einstaller.exe*) adopte les paramètres de l'option [Définir la connexion par défaut pour les installations par email et script de connexion](60) dans le menu contextuel.



Le compte sous lequel l'installation du package sera réalisée doit bénéficier des droits d'administrateur ou correspondre à un administrateur de domaine. Les valeurs insérées dans la boîte de dialogue **Connexion par défaut** sont oubliées après chaque redémarrage du service (ERAS).

4.2.3.2 Ouverture de session par défaut

La fenêtre **Ouverture de session par défaut** permet de définir les informations d'identification de l'utilisateur et les informations du domaine requises pour accéder à l'ordinateur client sur le réseau et gérer les produits ESET installés.

Les données client requises sont les suivantes :

- **Nom d'utilisateur**
- **Mot de passe**
- **Domaine/Groupe de travail**

Une fois les données saisies, cliquez sur le bouton **Définir connexion** pour enregistrer les informations sur le serveur.

REMARQUE : ces informations ne sont stockées sur le serveur que jusqu'à son prochain redémarrage.

REMARQUE : Si le message *Les informations de connexion sont déjà stockées sur le serveur*. apparaît dans la fenêtre de **connexion par défaut**, les paramètres ont déjà été enregistrés sur le serveur. Si vous souhaitez modifier les paramètres stockés, cliquez sur le bouton **Remplacer** et poursuivez la configuration des nouvelles informations de connexion.

4.2.4 Installation à distance personnalisée

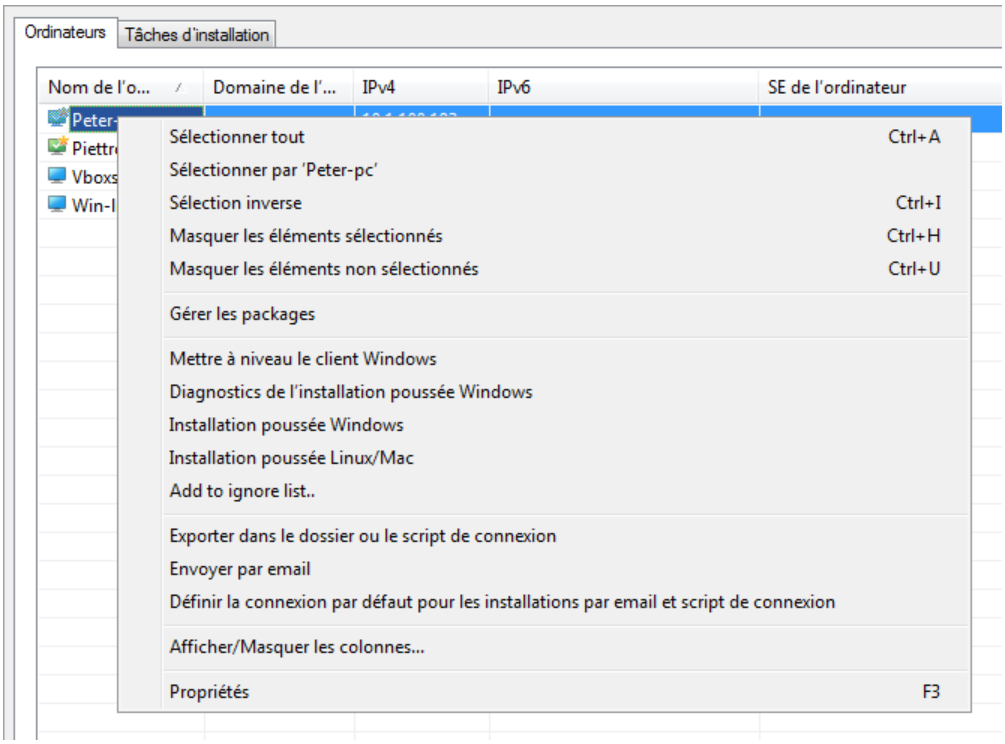
Il n'est pas obligatoire d'utiliser des outils ERA pour installer à distance des solutions client ESET. Finalement, l'aspect le plus important est de fournir et d'exécuter le fichier *einstaller.exe* sur les stations de travail client.

Pour le lancement d'*einstaller.exe*, l'utilisateur 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.

Le fichier *einstaller.exe* peut être obtenu comme suit :

- Dans l'onglet **Ordinateurs** (dans l'onglet **Installation à distance**), cliquez avec le bouton droit n'importe où et sélectionnez **Exporter dans le dossier ou le script de connexion** dans le menu contextuel. Sélectionnez le **type** et saisissez 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 « *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 exécuté avec le paramètre */qn* (versions 5.x, 4.x, 3.x). Ces paramètres exécuteront l'installation sans afficher d'interface utilisateur.



Le nom d'utilisateur et le mot de passe du compte sous lequel l'installation du package sera réalisée doivent correspondre à un compte bénéficiant des droits d'administrateur ou, de préférence, un compte d'administrateur de domaine.

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 d'ouverture de session** .

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$*). L'agent attend une réponse d'ERAS (envoyant le package via le partage *admin$*). 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. Le nouvel agent commence ensuite à télécharger le package à partir d'ERAS via le protocole TCP/IP.

L'installation du package est lancée et applique les paramètres .xml associés sous le compte défini dans l'ERAS (option **Ouverture de session par défaut pour installations par email et script d'ouverture de session**).

4.2.5 Mettre à niveau le client

Ce type d'installation est conçu pour les clients avec ESS/EAV version 4.2 et suivantes. Depuis la version 4.2, un nouveau mécanisme de mise à niveau a été mis en oeuvre et permet à ERA de lancer la mise à niveau du côté client sans agent *einstaller.exe*. Ce mécanisme fonctionne de la même manière que la mise à jour des composants du programme (PCU) qui installe la version la plus récente du programme sur les clients. Pour les clients ESS/EAV des versions 4.2 et suivantes, il est vivement conseillé d'utiliser ce type de mise à niveau.

REMARQUE : Si un fichier de configuration personnalisé a été défini pour le package d'installation, il sera ignoré lors de la mise à niveau.

La commande **Mettre à niveau le client** permet de mettre à niveau un client ou un groupe de clients à distance.

1) Cliquez sur le bouton **Ajout de clients spéciaux** à la première étape si vous souhaitez utiliser l'outil de sélection pour choisir les clients à mettre à niveau. Après avoir sélectionné les options voulues, cliquez sur **Suivant** pour continuer.

REMARQUE : un clic sur **Ajout de clients spéciaux** ouvre une nouvelle fenêtre dans laquelle vous pouvez ajouter des clients par serveur (dans la section **Serveurs**) ou par groupe (dans la section **Groupes**).

2) La fenêtre **Paramètres de package** permet d'utiliser les menus déroulants respectifs pour sélectionner le **type** et le **nom** d'un package de produit ESET qui servira à la mise à niveau de votre ou de vos clients. Après avoir sélectionné les options voulues, cliquez sur **Suivant** pour continuer.

3) La fenêtre **Paramètres de tâche** permet de changer le nom par défaut et la description de la tâche de mise à niveau, sélectionnez **Appliquer la tâche maintenant** pour exécuter la tâche immédiatement ou **Appliquer la tâche plus tard** si vous souhaitez choisir une date ultérieure pour l'exécution. Cliquez sur **Terminer** pour terminer la configuration de votre tâche de mise à jour du client.

REMARQUE : Cette tâche ne fonctionne que sur les clients qui se connectent directement au serveur principal. Les clients des serveurs répliqués seront ignorés.

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

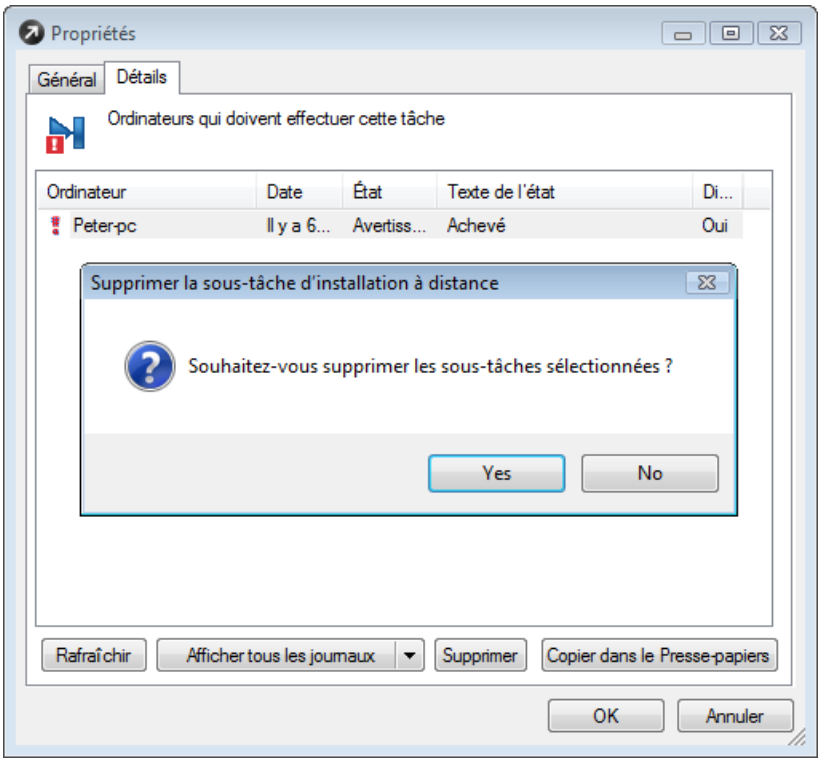
Si le type et le nom du package définis dans l'agent *einstaller.exe* correspondent aux données inscrites dans le Registre, aucune installation n'a lieu. Ceci empêche que les mêmes stations de travail soient ciblées en cas d'installations répétées.

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

ERAS propose une fonctionnalité complémentaire pour éviter les installations répétées. Celle-ci s'active lorsque le programme d'installation établit une reconnexion au 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* :

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



Pour empêcher ERAS de refuser des installations répétées, il faut supprimer les entrées correspondantes sous l'onglet **Détails de la tâche d'installation à distance**. Pour supprimer une entrée, sélectionnez-la, puis cliquez sur le bouton **Supprimer** et confirmer en cliquant sur **Oui**.

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 afin d'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 de ESET NOD32 Antivirus (*.msi*) dans le dossier.

3) Insérez un fichier de configuration *.xml* à appliquer au programme dans le même dossier. Ce fichier doit s'appeler *cfg.xml*. Pour créer un fichier de configuration, vous pouvez utiliser Éditeur de configuration d'ESET. Pour obtenir des informations supplémentaires, consultez le chapitre Éditeur de configuration d'ESET 50.

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 de la souris 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.

Étape I : **Nouvelle tâche**.

1) Pour appliquer une tâche à une ou plusieurs stations de travail client, dans le volet **Clients**, sélectionnez la ou les stations de travail et cliquez dessus avec le bouton droit de la souris pour ouvrir le menu contextuel 27.

2) Cliquez sur **Nouvelle tâche**, puis sélectionnez le type de tâche à exécuter.

REMARQUE : vous pouvez également ouvrir l'Assistant Tâche à partir du menu principal d'ERAC en cliquant sur **Actions > Nouvelle tâche**.

Étape II : sélectionnez une des tâches suivantes :

- Tâche de configuration 65
- Analyse à la demande (nettoyage désactivé/activé) 65
- Mettre à jour maintenant 66
- Tâche de script SysInspector 66
- Fonctionnalités de protection 66
- Exécuter la tâche planifiée 67
- Tâche Restaurer/Supprimer depuis la quarantaine 67
- Restauration de la base des signatures de virus 67
- Effacer le cache de mise à jour du client 68
- Générer un journal de vérification de sécurité 68
- Afficher la notification 68

3) Quand vous aurez choisi la tâche souhaitée, vous devrez réaliser les actions propres à chaque tâche décrites dans chacun des chapitres (cf. liens ci-après).

Étape III : **Sélectionner des clients**

4) Vous pouvez modifier vos sélections de clients dans la fenêtre **Sélectionner des clients** qui apparaît une fois que la tâche est configurée. Vous pouvez affiner la sélection de clients en ajoutant des clients de l'arborescence de présentation de clients **Tous les éléments** (moitié gauche de la fenêtre) vers la liste **Éléments sélectionnés** (moitié droite de la fenêtre) ou en supprimant les entrées de client qui figurent déjà dans la liste.

   REMARQUE : cliquez sur **Ajouter un élément spécial...** afin d'ouvrir une nouvelle fenêtre dans laquelle vous pouvez ajouter des clients depuis le **Volet clients** ou ajouter des clients par **Serveur** et/ou **Groupes**.

Étape IV : Achèvement de la tâche 68.

Les sous-chapitres suivants décrivent les types de tâches individuelles pour les stations de travail client et fournissent une exemple de scénario pour chacun d'eux.

REMARQUE :: La fenêtre **Contrôle de la mise à jour d'ESET Remote Administrator** s'ouvrira à l'issue de l'intervalle de temps défini ou lorsqu'une nouvelle version du produit est disponible. Pour télécharger la version la plus récente du produit depuis le site d'ESET, cliquez sur **Visiter le site Web de mise à jour**.

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 Éditeur de configuration d'ESET ou exportés depuis des 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 de la souris sur une station de travail sélectionnée, puis, dans le menu contextuel, cliquez sur **Nouvelle tâche** > **Tâche de configuration**.

2) La fenêtre **Configuration des 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 Éditeur de configuration d'ESET, puis désignez la configuration à appliquer. Accédez à **Gamme de produits Windows v3 et v4** > **Module de mise à jour** > **Profil** > **Paramètres** > **Nom d'utilisateur** et **Mot de passe**.

4) Saisissez 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 **Afficher** ou **Modifier**.

8) Cliquez sur **Suivant** pour accéder à la fenêtre **Sélectionner des clients** qui présente les stations de travail auxquelles il faut envoyer la tâche. À ce stade, vous pouvez ajouter des clients des serveurs ou des 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. Saisissez un nom ou une description pour la tâche (facultatif). L'option **Appliquer la tâche ultérieurement** permet de définir la tâche à exécuter après une date/heure spécifiée. L'option **Supprimer les tâches automatiquement par nettoyage si elles sont réalisées correctement** supprime toutes les tâches envoyées avec succès aux stations de travail cibles.

10) Cliquez sur **Terminer** pour enregistrer la tâche à exécuter.

5.1.2 Tâche 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.

1) 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 cible.

   REMARQUE : 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.

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

3) 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.

4) Cliquez sur **Suivant** pour accéder aux boîtes de dialogue **Sélectionner des clients** et **Rapport des tâches** qui sont décrites en détail dans le chapitre Tâches 64.

5) 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 l'ERAC 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 cible (mises à jour de base des signatures de virus ainsi que mises à niveau de composants du programme).

1) Cliquez avec le bouton droit sur une station de travail dans le volet **Clients**, puis sélectionnez **Nouvelle tâche** > **Mettre à jour maintenant**.

2) 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**.

3) 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 saisir le nom de profil. Pour rétablir la valeur par défaut du champ, cliquez sur **Effacer historique**.

4) Cliquez ensuite sur **Suivant** pour accéder aux boîtes de dialogue **Sélectionner de clients** et **Rapport des tâches**. Pour obtenir une description de ces boîtes de dialogue, consultez le chapitre Tâches 64.

5.1.4 Tâche de script SysInspector

La tâche de script SysInspector permet d'exécuter des scripts sur des ordinateurs cibles. Il permet de supprimer des objets indésirables du système. Pour plus d'informations, consultez la page d'aide sur ESET SysInspector 142.

1) Après avoir terminé les étapes I et II décrites au chapitre Tâches 64, cliquez sur **Sélectionner** pour choisir le script à exécuter sur la station de travail cible.

2) Cliquez sur **Afficher et modifier** pour adapter le script.

3) Cliquez sur **Suivant** pour accéder aux boîtes de dialogue **Sélectionner des clients** et **Rapport des tâches** qui sont décrites en détail dans le chapitre Tâches 64.

4) Quand la tâche est terminée sur la station de travail client, les informations sont affichées dans la colonne **État** du volet **Tâches**.

REMARQUE : les tâches de script SysInspector sont uniquement prises en charge à partir de ESET Smart Security/ESET NOD32 Antivirus version 4.0.

5.1.5 Fonctionnalités de protection

Cette tâche permet à l'administrateur de modifier l'état des fonctions de protection du produit de sécurité (produits de sécurité ESET pour Windows versions 5 et ultérieures).

1. Chaque fonction de protection se compose de trois étapes : **Ne pas modifier**, **Désactiver temporairement** et **Activer**. Vous pouvez passer d'une étape à l'autre en cochant la case située à côté de chaque fonction. Si la fonction de protection est désactivée (Désactiver temporairement), vous pouvez définir un **intervalle de désactivation temporaire**. Cet intervalle peut être défini entre 10 minutes et **Jusqu'au prochain redémarrage** (désactive la fonction complètement jusqu'au redémarrage de l'ordinateur).

2. Sélectionnez ensuite les clients dont vous souhaitez modifier les fonctions de protection et terminez la tâche 68.

REMARQUE :: Faites preuve de prudence lorsque vous désactivez les fonctions de protection, car cela peut provoquer des risques de sécurité. Le client est informé dès qu'une fonction de protection est désactivée.

5.1.6 Exécuter la tâche planifiée

Cette tâche déclenche une tâche planifiée qui s'exécute sur le client immédiatement. Vous pouvez sélectionner une tâche **prédéfinie** dans le planificateur du client ou une tâche **Par ID**. Chaque tâche planifiée disposant d'un ID, vous pouvez sélectionner la tâche dans le menu déroulant ou en saisissant un ID. Pour afficher chaque tâche du planificateur sur un client spécifique, démarrez cette tâche dans le menu contextuel dans l'onglet **Client**.

Sélectionnez la tâche à exécuter sur le ou les clients, puis sélectionnez les clients dont vous souhaitez modifier les fonctions de protection et terminez la tâche 68.

5.1.7 Tâche Restaurer/Supprimer depuis la quarantaine

Cette tâche permet de restaurer ou de supprimer de la quarantaine du client les objets désignés.

1) Après avoir ouvert la fenêtre **Restaurer/Supprimer depuis la quarantaine** (reportez-vous au chapitre Tâches 64), sélectionnez l'opération à effectuer sur l'objet mis en quarantaine : **Restaurer** ou **Supprimer**.

   REMARQUE : Si vous restaurez un objet mis en quarantaine qui est toujours détecté en tant que menace, pensez à exclure cet objet des prochaines analyses à l'aide de l'option **Ajouter également l'exclusion** afin d'éviter que l'objet soit à nouveau analysé et mis en quarantaine. Notez que tous les objets peuvent être exclus, notamment les chevaux de Troie ou les virus. Toute tentative d'exclusion de ce type de fichier génère une erreur. Si vous souhaitez exclure des fichiers nettoyés (non détectés comme menaces), effectuez l'opération directement sur le client ou à l'aide de l'éditeur de configuration ESET (stratégie, tâche, etc.).

2) Choisissez une condition pour désigner les objets mis en quarantaine que vous voulez restaurer/supprimer, puis cliquez sur **Suivant**.

   REMARQUE : Si vous avez ouvert la fenêtre Restaurer/Supprimer depuis la quarantaine en cliquant avec le bouton droit de la souris sur une entrée de la quarantaine directement dans l'onglet **Quarantaine** (et choisi l'option **Tâche Restaurer/Supprimer depuis la quarantaine**), vous ne devrez pas désigner de condition (l'option **Par hachage** sera choisie automatiquement et le code hash du fichier mis en quarantaine servira d'identifiant).

3) Sélectionnez les clients pour l'opération de restauration/suppression (reportez-vous au chapitre Tâches 64) et cliquez sur **Suivant**).

4) Vérifiez les paramètres dans la fenêtre **Rapport des tâches**, nommez votre tâche, indiquez l'heure à laquelle vous souhaitez qu'elle s'applique (le cas échéant, définissez les options de nettoyage), puis cliquez sur **Terminer** pour confirmer. Consultez le chapitre Tâches 64 pour plus d'informations.

5.1.8 Restauration de la base des signatures de virus

Si vous pensez que la nouvelle mise à jour de la base des signatures de virus est peut-être instable ou endommagée, vous pouvez rétablir la version antérieure et désactiver les mises à jour pendant une période donnée. Vous pouvez également activer les mises à jour désactivées précédemment.

1) Désactiver / Activer les mises à jour de la base des signatures de virus

Désactiver pendant X heures : les versions précédentes de la base des signatures de virus du ou des clients seront rétablies (en fonction d'un cliché créé par le client) et toute mise à jour du ou des clients sélectionnés sera désactivée pendant la période sélectionnée. Vous pouvez également sélectionner **Infini** et désactiver complètement les mises à jour. Utilisez cette option de désactivation permanente avec précaution, car cela peut provoquer des risques de sécurité.

Avertissement: L'option **Infini** reste active, même après le redémarrage d'un ordinateur client.

Activer les mises à jour désactivées précédemment : la mise à jour de la base des signatures de virus est à nouveau activée.

2) Sélectionnez les clients pour cette tâche et cliquez sur **Suivant**.

3) Vérifiez les paramètres dans la fenêtre **Rapport des tâches**, nommez votre tâche, indiquez l'heure à laquelle elle doit s'appliquer (le cas échéant, définissez les options de nettoyage), puis cliquez sur **Terminer** pour confirmer. Consultez le chapitre Tâches 64 pour plus d'informations.

5.1.9 Effacer le cache de mise à jour du client

Cette tâche est réservée aux produits de sécurité ESET versions 5 et ultérieures. Si vous pensez que la mise à jour de la base des signatures de virus n'a pas abouti, vous pouvez vider le cache de mise à jour du client, ce qui permettra le téléchargement de la dernière mise à jour.

1) Démarrez la tâche et cliquez sur **Suivant**.

2) Sélectionnez les clients pour cette tâche et cliquez sur **Suivant**.

3) Vérifiez les paramètres dans la fenêtre **Rapport des tâches**, nommez votre tâche, indiquez l'heure à laquelle elle doit s'appliquer (le cas échéant, définissez les options de nettoyage), puis cliquez sur **Terminer** pour confirmer. Consultez le chapitre Tâches 64 pour plus d'informations.

5.1.10 Tâche Générer un journal de vérification de sécurité

Cette tâche concerne uniquement ESET Mobile Security.

La vérification de sécurité contrôle : le niveau de la batterie, le statut Bluetooth, l'espace disque disponible, la visibilité des périphériques, le réseau domestique et les processus en cours. Un rapport détaillé est généré et indique si la valeur est en dessous ou non du seuil défini ou si elle constitue un risque potentiel pour la sécurité, p. ex., visibilité des périphériques activée, etc.).

Pour vérifier la sécurité du téléphone :

1) Cliquez avec le bouton droit de la souris sur le nom du client dans le volet **Clients** et choisissez l'option **Nouvelle tâche** > **Générer un journal de vérification de sécurité** dans le menu contextuel.

2) Cliquez ensuite sur **Suivant** pour accéder aux boîtes de dialogue **Sélectionner des clients** et **Rapport des tâches**. Pour obtenir une description de ces fenêtres, consultez le chapitre Tâches 64.

5.1.11 Tâche Afficher la notification

Cette tâche concerne uniquement ESET Mobile Security.

Pour envoyer une notification (p. ex., un message d'avertissement) à un téléphone :

1) Cliquez avec le bouton droit de la souris sur le nom du client dans le volet **Clients** et choisissez l'option **Nouvelle tâche** > **Afficher la notification** dans le menu contextuel.

2) Saisissez le **Titre** de la notification et **Corps** du message dans les champs appropriés et sélectionnez la **Verbosité** de la notification.

3) Cliquez ensuite sur **Suivant** pour accéder aux boîtes de dialogue **Sélectionner des clients** et **Rapport des tâches**. Pour obtenir une description de ces fenêtres, consultez le chapitre Tâches 64.

5.1.12 Achèvement de la tâche

La dernière boîte de dialogue présente un aperçu de la tâche. Elle contient tous les paramètres de la tâche et permet à l'utilisateur de cliquer sur **Précédent** pour apporter des modifications nécessaires.

La seconde partie de la fenêtre contient les paramètres suivants :

- **Nom** : nom de la tâche.
- **Description** : description de la tâche.
- **Appliquer la tâche ultérieurement** : moment du déploiement de la tâche sur les ordinateurs clients.
- **Supprimer les tâches automatiquement par nettoyage si elles sont réalisées correctement** : supprime automatiquement toutes les tâches exécutées.

5.2 Gestionnaire de groupes

Le gestionnaire de groupes est un puissant outil pour la gestion de vos clients. Il permet de les scinder en différents groups et d'appliquer différents paramètres, tâches, restrictions, etc. Vous pouvez y accéder facilement via le menu **Outils > Gestionnaire de groupes** ou la combinaison de touches **CTRL+G**. Les groupes sont indépendants pour chaque ERAS et ne dont pas répliqués.

Vous pouvez créer vos propres groupes pour répondre à vos besoins dans le réseau de votre société ou simplement synchroniser les groupes client ERAC avec Microsoft Active Directory en utilisant le caractère générique **Synchronisation Active Directory** de la fenêtre principale du gestionnaire de groupes.

Il existe deux groupes principaux de clients :

- Groupes statiques 69
- Groupes paramétriques 70

Aussi bien les groupes statiques que les groupes paramétriques peuvent être utilisés en divers endroits au sein de l'ERA, ce qui améliore considérablement les capacités de gestion des clients.

5.2.1 Groupes statiques

Les groupes statiques permettent de séparer les clients de votre réseau en groupes et sous-groupes nommés. Par exemple, vous pouvez créer un groupe Marketing contenant tous les clients marketing et également des sous-groupes spécialisés ; par exemple Ventes locales, Gestion EMOA, etc.

La fenêtre principale Groupes statiques est divisée en deux parties. La partie gauche reprend les groupes et les sous-groupes existants, affichés de façon hiérarchique. Les clients qui sont repris dans le groupe sélectionné apparaissent dans la partie droite de la fenêtre. Par défaut, seuls les clients du groupe sélectionné sont affichés. Si vous souhaitez voir les clients inclus dans les sous-groupes du groupe sélectionné, cochez la case **Afficher les clients en sous-groupes** dans la partie droite de la fenêtre.

Pour créer un groupe, cliquez sur **Créer**, puis saisissez un nom pour le groupe. Le nouveau groupe sera créé en tant que sous-groupe du groupe parent sélectionné. Si vous souhaitez créer un groupe principal, sélectionnez la racine de l'arbre hiérarchique **Groupes statiques**. Le champ **Groupe parent** contient le nom du groupe parent pour le groupe récemment créé (à savoir, « / » pour la racine). 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 ultérieurement les groupes créés et configurés.

REMARQUE : Lorsqu'une tâche est envoyée au groupe parent, toutes les stations de travail qui appartiennent aux sous-groupes accepteront la tâche également.

Il est également possible de créer des groupes vides pour une utilisation ultérieure.

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, saisissez 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 **Rafraîchir** pour vérifier la présence de nouveaux clients connectés récemment au serveur.

Si la sélection manuelle de client ne convient pas, vous pouvez cliquer sur **Ajouter un élément 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 du Gestionnaire de groupes statiques. 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 **Copier dans le Presse-papiers** pour copier les listes de clients et de groupes. Pour actualiser les clients du groupe, cliquez sur le bouton **Rafraîchir**.

Il est également possible d'**Importer/Exporter** les clients du groupe sélectionné dans un fichier *.xml*.

5.2.2 Groupes paramétriques

Outre les groupes statiques, les groupes paramétriques peuvent s'avérer très utiles. Les stations client sont affectées dynamiquement à un certain groupe paramétrique lorsque les conditions du groupe sont remplies. Les groupes paramétriques présentent l'avantage de pouvoir être utilisés à plusieurs endroits, y compris les filtres, les stratégies, les rapports et les notifications.

La fenêtre principale Groupes paramétriques comprend quatre parties. La section **Groupes paramétriques** reprend les groupes parents et les sous-groupes qui ont été créés. Une fois que vous avez sélectionné un certain groupe dans la **liste Groupes paramétriques**, les clients qui appartiennent au groupe sélectionné apparaissent dans la section **Groupe sélectionné**.

REMARQUE : quand un groupe parent est sélectionné, la liste reprend également les sous-groupes membres.

Les paramètres définis pour un groupe sélectionné sont repris dans la section **Paramètres** de la fenêtre. Vous pouvez modifier ou ajouter des paramètres à tout moment en cliquant sur le bouton **Modifier**.

La section **Statut de la synchronisation** affiche une barre de progression pour le processus de synchronisation.

1. Pour créer un groupe, cliquez sur **Créer**. Le nouveau groupe sera créé en tant que sous-groupe du groupe parent sélectionné. Si vous souhaitez créer un groupe principal, sélectionnez la racine de l'arbre hiérarchique **Groupes paramétriques**. Le champ **Groupe parent** contient le nom du groupe parent pour le groupe récemment créé (à savoir, « / » pour la racine). Saisissez un **nom** et une brève **description** pour le nouveau groupe.

2. L'étape suivante consiste à créer les **paramètres de filtre client**. Pour ce faire, dans l'**éditeur de règles**, sélectionnez les options voulues après avoir cliqué sur **Modifier** Vous pouvez spécifier ici les conditions nécessaires au déclenchement et à l'application de la règle. Sélectionnez la condition et **spécifiez-la** en cliquant sur l'option prévue en regard de la règle dans la fenêtre **Paramètres** en dessous. Vous pouvez également indiquer si vous voulez que cette règle s'applique uniquement lorsque **toutes les conditions sont remplies** ou dès que **l'une des conditions est remplie**.

3. Si vous cochez la case en regard de **Sans suppression**, les clients seront ajoutés automatiquement à ce groupe dès qu'ils répondront aux conditions, mais ils n'en seront jamais supprimés. Le contenu d'un groupe sans suppression peut être réinitialisé manuellement au niveau de la racine.

REMARQUE : ce paramètre peut être uniquement défini lors de la création d'un groupe.

Pour modifier un groupe existant, sélectionnez-le dans la **liste Groupes paramétriques**, puis cliquez sur le bouton **Modifier** dans la partie inférieure de la fenêtre. Pour supprimer un groupe, sélectionnez le groupe souhaité, puis cliquez sur le bouton **Supprimer**.

Vous pouvez actualiser manuellement la liste de groupes en cliquant sur le bouton **Rafraîchir**. Pour importer un groupe depuis un fichier, sélectionnez le groupe dans la section **Groupes paramétriques** dans laquelle vous souhaitez importer le nouveau groupe, puis cliquez sur **Importer**. Confirmez votre sélection en cliquant sur **Oui**. Localisez le fichier à importer, puis cliquez sur **Ouvrir**. Le groupe (et tous ses sous-groupes) sera importé à l'emplacement sélectionné. Pour exporter un groupe (et tous ses sous-groupes), sélectionnez-le dans la section **Groupes paramétriques**, cliquez sur la flèche du bouton **Importer**, puis sélectionnez **Exporter**. Cliquez sur **Oui** pour confirmer, sélectionnez un nom et un emplacement pour le fichier d'exportation, puis cliquez sur **Enregistrer**.

REMARQUE : vous pouvez déplacer des groupes déjà présents dans la section **Groupes paramétriques**, à l'aide de la méthode glisser-déposer.

REMARQUE : Les groupes paramétriques sont pratiques pour filtrer les données ou les clients. Supposons, par exemple, que vous voulez générer des rapports pour les ordinateurs sous Windows XP uniquement Créez un groupe paramétrique réservé aux ordinateurs équipés du système d'exploitation en question et utilisez ce groupe dans la cible du filtre. Vous pouvez également définir vos propres **données client personnalisées** lorsque vous créez un package d'installation 44 - (**Éditeur de configuration** > **Noyau** > **Paramètres** > **Administration à distance**). Définissez cette option (Données client personnalisées) en tant que paramètre d'un groupe paramétrique. Chaque utilisateur installant ce package devient membre de ce groupe.

5.2.3 Synchronisation Active Directory/LDAP

La synchronisation Active Directory utilise la création automatique de groupes (avec les clients correspondants) basée sur la structure définie par Active Directory. Elle permet à l'administrateur de répartir les clients dans des groupes, à condition que le nom du client corresponde au type d'objet *ordinateur* au niveau d'Active Directory (AD) et appartienne aux groupes dans Active Directory.

Il y a deux options principales qui déterminent le fonctionnement de la synchronisation :

- L'option **Synchroniser les groupes** permet de choisir les groupes Active Directory qui seront synchronisés. Sélectionnez l'option **Tous les groupes** pour synchroniser toute l'arborescence Active Directory, que les groupes Active Directory contiennent ou non des clients ERA. Les deux options suivantes (**Uniquement les groupes contenant des clients du ERA Server** et **Uniquement les groupes contenant des clients du serveur principal ERA**) synchronisent uniquement les groupes contenant des clients ERA existants.
- L'option **Type de synchronisation** permet de définir si les groupes Active Directory à synchroniser seront ajoutés aux groupes AD/LDAP existants (**Importer les groupes AD/LDAP**) ou si les groupes AD/LDAP existants seront complètement remplacés par ceux à synchroniser (**Synchroniser les groupes AD/LDAP**).
- L'option **Branches synchronisées** permet de choisir les branches **Active Directory** qui seront synchronisées. Cliquez sur **Configurer** pour sélectionner les branches Active Directory/LDAP synchronisées avec des groupes. Par défaut, toutes les branches sont marquées/sélectionnées.

Remarque: Cliquez sur **Plus d'informations** pour afficher d'autres informations concernant les paramètres et les règles de synchronisation Active Directory/LDAP.

- Pour configurer l'intervalle de synchronisation entre le serveur AD/LDAP et le serveur ERA, cliquez sur **Modifier** à côté de l'option Synchroniser. Sélectionnez la fréquence de synchronisation souhaitée dans la boîte de dialogue **Intervalle planifié de synchronisation AD/LDAP (en heure locale du serveur)**. La fréquence sélectionnée s'affiche à côté de l'option **Synchroniser**.

Vous pouvez configurer en détail la synchronisation Active Directory à l'aide de l'**Éditeur de configuration** (**Remote Administrator** > **ERA Server** > **Paramètres** > **Groupes** et **Active directory/LDAP**). Vous pouvez ajouter d'autres objets Active Directory/LDAP en cochant les options souhaitées.

Le fait de cliquer sur **Synchroniser maintenant** déclenche la synchronisation (en fonction des options configurées ci-dessus).

REMARQUE : Pour qu'ERAS puisse se synchroniser avec Active Directory, ERAS n'a pas besoin d'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** > **Paramètres avancés** > **Modifier les paramètres avancés** > **Remote Administrator** > **ERA Server** > **Paramètres** > **Active Directory/LDAP**.

5.3 Stratégies

Les stratégies sont, à maints égards, semblables aux **tâches de configuration**, à l'exception près qu'il ne s'agit pas de tâches isolées envoyées à un ou plusieurs postes 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 obtiennent les stratégies de l'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.

5.3.2 Comment créer des stratégies

L'installation par défaut n'implémente qu'une seule stratégie appelée « Stratégie du serveur ». Vous pouvez configurer la stratégie proprement dite dans Éditeur de configuration d'ESET en cliquant sur **Modifier une stratégie**, puis en définissant des paramètres pour le produit de sécurité ESET sélectionné (ou le client). Tous les paramètres sont organisés dans une structure étendue et tous les éléments de Éditeur de configuration 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 Server 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 à une **configuration de règles** (la configuration peut être vide ; vous pouvez copier une configuration de règles fusionnée depuis une règle du menu déroulant ou un fichier de configuration *.xml*, ou encore l'**assistant Fusion des règles de pare-feu**). 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 **Abaisser une stratégie réplicable**. 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'option **Remplacer toute stratégie enfant** n'est pas activée, 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 enfant de la stratégie modifiée.
- **Abaisser une stratégie réplicable** : active la réplication des stratégies sur les serveurs de niveau inférieur. Par exemple, une stratégie peut servir de stratégie par défaut pour des serveurs de niveau inférieur et être attribuée aux clients qui y sont connectés.

Les stratégies peuvent également être importée/exportée depuis/vers un fichier *.xml* ou importés depuis les groupes. Pour obtenir de plus amples informations, consultez le chapitre intitulé Importation/exportation de stratégies 73.

5.3.3 Stratégies virtuelles

Outre les stratégies créées et celles répliquées à partir d'autres serveurs (voir le chapitre Onglet Réplication 100), l'arborescence de stratégie contient une stratégie parent par défaut appelée stratégie virtuelle.

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 un serveur de niveau supérieur) et est sélectionnée dans le champ de stratégie par défaut pour les clients principaux. Elle est automatiquement appliquée aux nouveaux clients connectés (clients principaux) du serveur ERAS donné, à moins qu'ils aient déjà adopté une autre stratégie à partir des règles de stratégie (pour plus d'informations, voir le chapitre Attribution de stratégies à des clients 74). Les stratégies virtuelles sont des liens vers d'autres stratégies situées sur le même serveur.

5.3.4 Rôle et objectif des stratégies dans la structure arborescente de stratégie

Une icône, à gauche, est affectée à chaque stratégie figurant dans l'**arborescence de stratégie**. 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 vers le bas, 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 obtenir des informations supplémentaires, consultez le chapitre Comment créer des stratégies 72).

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

Icônes de la **stratégie serveur** par défaut.

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 supprimera pas la stratégie elle-même, mais la supprimera 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.

Les règles de stratégie existantes peuvent être importées/exportées depuis ou vers un fichier *.xml* en cliquant sur **Importer/exporter des stratégies**. Si une stratégie importée porte le même nom qu'une stratégie existante, une chaîne aléatoire est ajoutée automatiquement à la fin du nom de la stratégie importée.

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 la stratégie** > **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.

Afficher : 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 : cf. ci-dessus.

Afficher la partie ignorée : 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.

REMARQUE :: Vous pouvez double-cliquer sur un élément de l'arborescence pour obtenir l'affichage fusionné.

5.3.6 Importation/exportation de stratégies

Le Gestionnaire de stratégies permet d'importer/d'exporter des stratégies et des règles de stratégie. Les stratégies existantes peuvent être importées/exportées depuis ou vers un fichier *.xml* en cliquant sur **Importer/exporter des stratégies**. Les stratégies peuvent également être importées depuis des groupes en cliquant sur **Importer depuis des groupes...**. Les règles de stratégie peuvent être importées/exportées en cliquant sur **Importer** ou **Exporter**. Elles peuvent également être créées à l'aide de l'**assistant Règles de stratégie**.

Les conflits de nom (les noms de la stratégie existante et de la stratégie importée sont identiques) sont résolus pendant l'importation en ajoutant une chaîne aléatoire au nom de la stratégie importée. Si un conflit ne peut pas être résolu de cette manière (en général, lorsque le nouveau nom est trop long), l'importation se termine sur l'avertissement *Conflit de nom de stratégie non résolu*. La solution consiste à supprimer ou à renommer les stratégies ou les règles de stratégie en conflit.

5.3.7 Assistant de migration de règles

L'**Assistant de migration de règles** permet de créer une nouvelle **règle de bureau Windows v5** ou de mettre à jour une règle **de bureau Windows v5** existante à l'aide des paramètres des règles existantes des lignes de produits Windows v3 et v4. Vous pouvez migrer toutes les règles pendant l'installation sur une version antérieure, mais si vous souhaitez personnaliser tous les paramètres de la migration, il est recommandé d'utiliser l'**Assistant de migration de règles**.

Pour migrer des règles :

1. Cochez la case en regard des règles dont vous souhaitez migrer les paramètres.
2. Si une règle Endpoint existe, sélectionnez l'un des paramètres suivants :

- **Remplacer les règles Endpoint existante et utiliser uniquement les paramètres de la source** - la règle existante est entièrement remplacée par la nouvelle règle (**bureau Windows v5**) et les paramètres de la règle d'origine (**ligne de produits Windows v3 et v4**) sont utilisés.
- **Fusionner les règles et ne pas remplacer les paramètres Endpoint conflictuels** - les règles existantes et migrées sont fusionnées, et les paramètres existants de la règle de bureau Windows v5 ne sont pas remplacés par les paramètres de la règle de lignes de produits Windows v3 et v4.
- **Fusionner les règles et remplacer les paramètres Endpoint conflictuels** - les règles existantes et migrées sont fusionnées et les paramètres en conflit sont remplacés par les paramètres d'origine (v3/v4).

3. Patientez jusqu'à l afin du processus ; la durée varie en fonction du nombre de règles à migrer. Cliquez sur **Terminer** lorsque le message **Le processus de migration de règles est terminé** s'affiche.

5.3.8 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 **Abaisser une stratégie réplicable** 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.

5.3.8.1 Stratégie de clients principaux par défaut

Une méthode d'attribution de stratégies est l'application automatique de la **stratégie serveur**, 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 obtenir des informations supplémentaires, consultez la chapitre Stratégies virtuelles 72.

5.3.8.2 Attribution manuelle

Il y deux manières d'attribuer manuellement des stratégies : Cliquez avec le bouton droit de la souris 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 **Définir/Supprimer**. Les clients sont répertoriés à gauche au format Serveur/Client. Si la cas **Abaisser une stratégie réplicable** 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 **Définir/Supprimer**, vous ne pouvez plus supprimer les clients de la liste **Éléments sélectionnés** ; vous pouvez en revanche 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.

5.3.8.3 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 serveur** et sur les attributions manuelles. La **stratégie de serveur** 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.

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 aux clients une stratégie 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.

Les règles de stratégie peuvent être créées et gérées depuis l'onglet **Règles de stratégie** du Gestionnaire de stratégies. Le processus de création et d'application de règles ressemble beaucoup au processus de création et de gestion de règles 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 **Nouvelle règle** et choisissez si vous souhaitez **créer une nouvelle règle** ou utiliser l' Assistant Règles de stratégie 76. Complétez ensuite les champs **Nom**, **Description**, **Paramètres de filtre 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** :

DU (PAS DU) Serveur principal : si (non) localisée sur le serveur principal.
EST (N'EST PAS) Nouveau client : s'il (ne) s'agit (pas) d'un nouveau client.
A (N'A PAS) Nouveau drapeau : s'applique aux clients avec ou sans drapeau Nouveau client.
Serveur principal DANS (PAS DANS) (spécifier) : si le nom du serveur principal contient/ne contient pas...
GROUPES ERA DANS (spécifier) : si le client appartient au groupe...
GROUPES ERA PAS DANS (spécifier) : si le client n'appartient pas au groupe...
DOMAINE/GROUPE DE TRAVAIL DANS (PAS DANS) (spécifier) : si le client appartient/n'appartient pas au domaine...
Masque de nom d'ordinateur (spécifier) : si le nom d'ordinateur est ....
A un masque IPv4 (spécifier) : si le client appartient au groupe défini par l'adresse et le masque IPv4...
A une plage IPv4 (spécifier) : si le client appartient au groupe défini par la plage IPv4...
A un masque IPv6 (spécifier) : si le client appartient au groupe défini par l'adresse et le masque IPv6...
A une plage IPv6 (spécifier) : si le client appartient au groupe défini par la plage IPv6...
A (N'A PAS) défini une stratégie (spécifier) : si le client adopte (ou n'adopte pas) la stratégie...
Nom du produit DANS (PAS DANS) : si le nom du produit est...
Version du produit EST (N'EST PAS) : si la version du produit est...
Masque d'informations personnalisées du client 1, 2, 3 DANS (PAS DANS) : si les informations personnalisées du client contiennent...
Masque de commentaire client (PAS) DANS -
A (N'A PAS) État de la protection (spécifier) : si l'état de la protection du client est...
Version de la base des signatures de virus EST (N'EST PAS) : si la version de la base des signatures de virus est...
Dernière connexion EST (N'EST PAS) plus ancienne que (spécifier) : si la dernière connexion est plus ancienne que...
EST (N'EST PAS) En attente de redémarrage : si le client attend un redémarrage.

Les règles de stratégie peuvent être importées depuis ou exportées vers un fichier *.xml*. Les règles de stratégie peuvent également être créées automatiquement à l'aide de l'assistant de règles de stratégie 76, ce qui permet de créer une structure de stratégie basée sur la structure du groupe existant et d'associer les stratégies créées aux groupes en créant les règles de stratégie correspondante. Pour obtenir de plus amples informations sur l'importation et l'exportation de règles de stratégie, consultez le chapitre intitulé Importation/exportation de stratégies 73.

Pour supprimer une règle de stratégie, cliquez sur **Supprimer la règle**.

Pour appliquer immédiatement la règle activée, cliquez sur **Exécuter la règle de stratégie maintenant**.

5.3.8.3.1 Assistant Règles de stratégie

L'assistant Règles de stratégie permet la création d'une structure de stratégie basée sur la structure de groupe existante et d'associer les stratégies créées aux groupes en créant les règles de stratégie correspondantes.

1. Au cours de la première étape, vous êtes invité à organiser votre groupe. Si vous ne possédez pas de configuration pour la structure de groupe souhaitée, vous pouvez cliquer sur Gestionnaire de groupes 69 pour configurer vos groupes, puis cliquer sur **Suivant**.
2. À la deuxième étape, désignez les catégories de groupes clients auxquelles la nouvelle règle de stratégie sera appliquée. Après avoir coché les cases souhaitées, cliquez sur **Suivant**.
3. Choisissez une **stratégie parent**.
4. Un simple message de statut du processus apparaît à la dernière étape. Cliquez sur **Terminer** pour fermer la fenêtre **Assistant Règles de stratégie**.

La nouvelle règle de stratégie apparaît dans la liste de l'onglet **Règles de stratégie**. Cochez la case en regard du nom de la règle pour activer une règle spécifique.

Pour plus d'informations sur l'importation et l'exportation de règles de stratégie, ainsi que sur les conflits de noms, consultez le chapitre intitulé Importation/exportation de stratégies 73.

5.3.9 Stratégie pour les clients mobiles

Par rapport à un produit ESET installé sur un ordinateur de bureau/portable, l'utilisateur d'un produit installé sur un périphérique mobile dispose d'un contrôle plus précis des paramètres. Il est donc inutile de forcer en permanence une stratégie pour les utilisateurs mobiles, car ces derniers souhaiteront peut-être changer ou ajuster certains paramètres. Nous recommandons d'utiliser la technique ci-dessous pour créer une stratégie pour les clients mobiles :

Créez une stratégie vide (stratégie par défaut pour les clients)

1. Cliquez sur **Outils > Gestionnaire de stratégies**.
2. Cliquez sur **Ajouter une nouvelle stratégie** pour créer une stratégie vide sans aucun paramètre modifié. Dans la section de configuration de la stratégie, sélectionnez **Créer une configuration de stratégie vide**.
3. Cliquez sur **Ajouter des clients** et sélectionnez les utilisateurs mobiles que vous souhaitez gérer avec cette stratégie.
4. Cliquez sur l'onglet Règles de stratégie 75 et sur **Nouveau**.
5. Dans le menu déroulant **Stratégie**, sélectionnez cette stratégie, puis cliquez sur **Modifier**.
6. Sélectionnez la condition de règle **EST Nouveau client** dans le champ Paramètres : cliquez sur EST pour choisir N'EST PAS Nouveau client, pouis cliquez sur OK deux fois.
7. Cliquez sur OK, puis sur Oui lorsque le programme vous demande si vous souhaitez enregistrer les paramètres.
8. Cette stratégie sera appliquée au client à chaque connexion à ERA.

Créez une stratégie ponctuelle (stratégie de démarrage pour les clients)

1. Cliquez sur **Outils > Gestionnaire de stratégies**.
2. Cliquez sur **Ajouter une nouvelle stratégie** pour créer une stratégie vide sans aucun paramètre modifié. Dans la section de configuration de la stratégie, sélectionnez **Créer une configuration de stratégie vide**.
3. Configurez les paramètres à appliquer aux clients mobiles et enregistrez la configuration.
4. Cliquez sur **Ajouter des clients** et assignez les utilisateurs mobiles que vous souhaitez gérer avec cette stratégie.
5. Cliquez sur l'onglet Règles de stratégie 75 et sur **Nouveau**.
6. Dans le menu déroulant **Stratégie**, sélectionnez cette stratégie, puis cliquez sur **Modifier**.
7. Sélectionnez la condition de règle **EST Nouveau client** et cliquez sur OK deux fois.
8. Cliquez sur OK, puis sur Oui lorsque le programme vous demande si vous souhaitez enregistrer les paramètres.

Lorsque les clients mobiles se connectent à ERA pour la première fois, ils reçoivent les paramètres de la **stratégie ponctuelle**. Lors de leur connexion suivante à ERA, ils reçoivent une **stratégie vide** et leurs paramètres ne sont pas

modifiés.

5.3.10 Suppression de stratégies

Comme pour 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 les serveurs de niveau inférieur, stratégie par défaut pour les 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 **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 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 sélectionnée fait office de stratégie virtuelle (voir **Paramètres de stratégie globale**), il convient de la remplacer par une autre (pour plus d'informations, voir le chapitre Stratégies virtuelles 72). 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 sélectionnée fait office de stratégie virtuelle (voir **Paramètres de stratégie globale**), il convient de la remplacer par une autre (pour plus d'informations, voir le chapitre Stratégies virtuelles 72). Vous pouvez utiliser une stratégie du même serveur en remplacement.

La même boîte de dialogue s'ouvre également si vous désactivez l'option **Abaisser une stratégie réplicable** 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 **Nouvelle stratégie par défaut pour les serveurs de niveau inférieur**.

5.3.11 Paramètres spéciaux

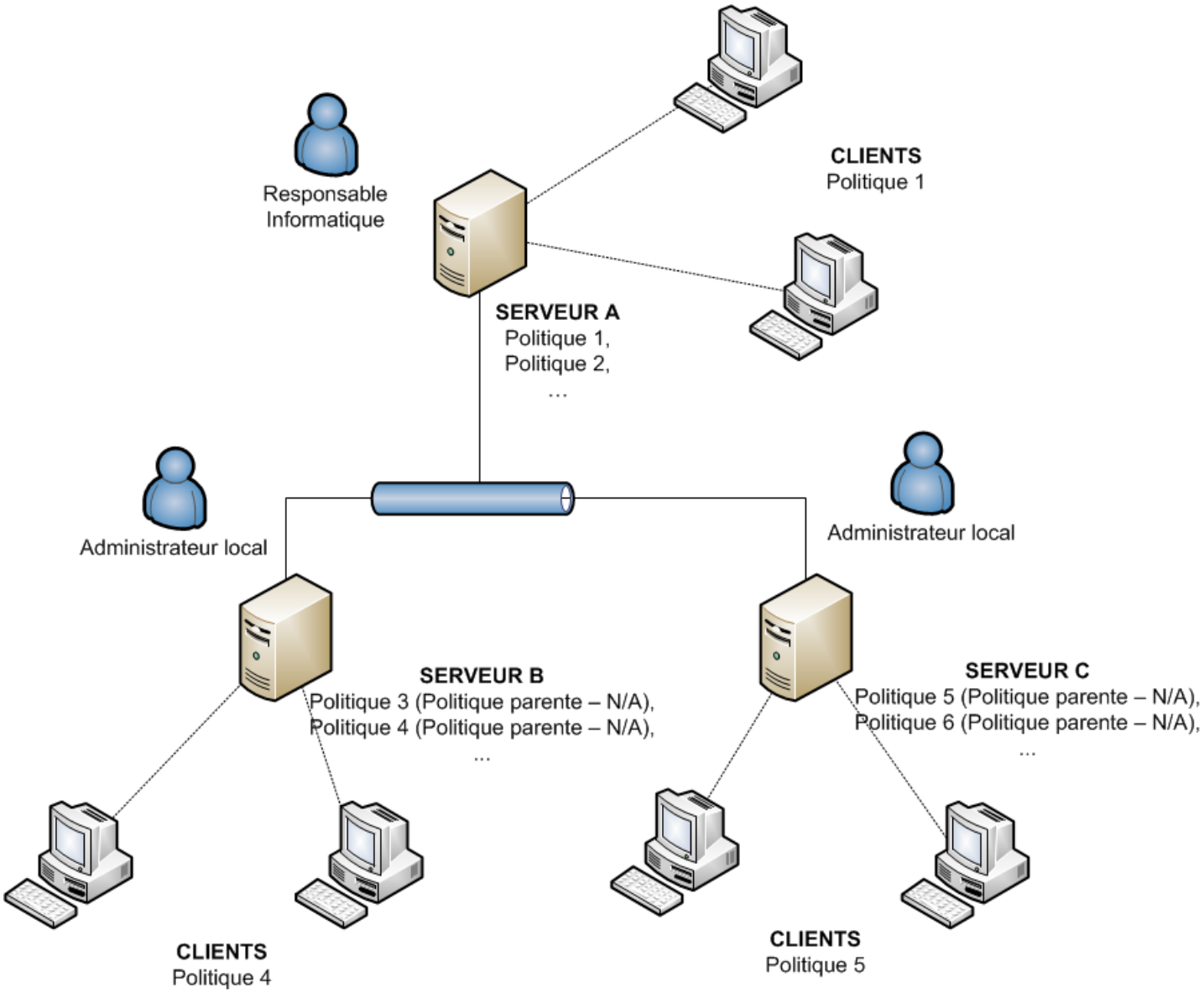
Deux stratégies supplémentaires ne se trouvent pas dans le Gestionnaire de stratégies, mais dans **Outils** > **Options du serveur** > **Paramètres avancés** > **Modifier les paramètres avancés** > **ESET Remote Administrator** > **ERA Server** > **Paramètres > Stratégies**.

- **Intervalle d'application de la 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 la 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, la meilleure solution consiste à leur attribuer une stratégie vide.

5.3.12 Scénarios de déploiement de stratégie

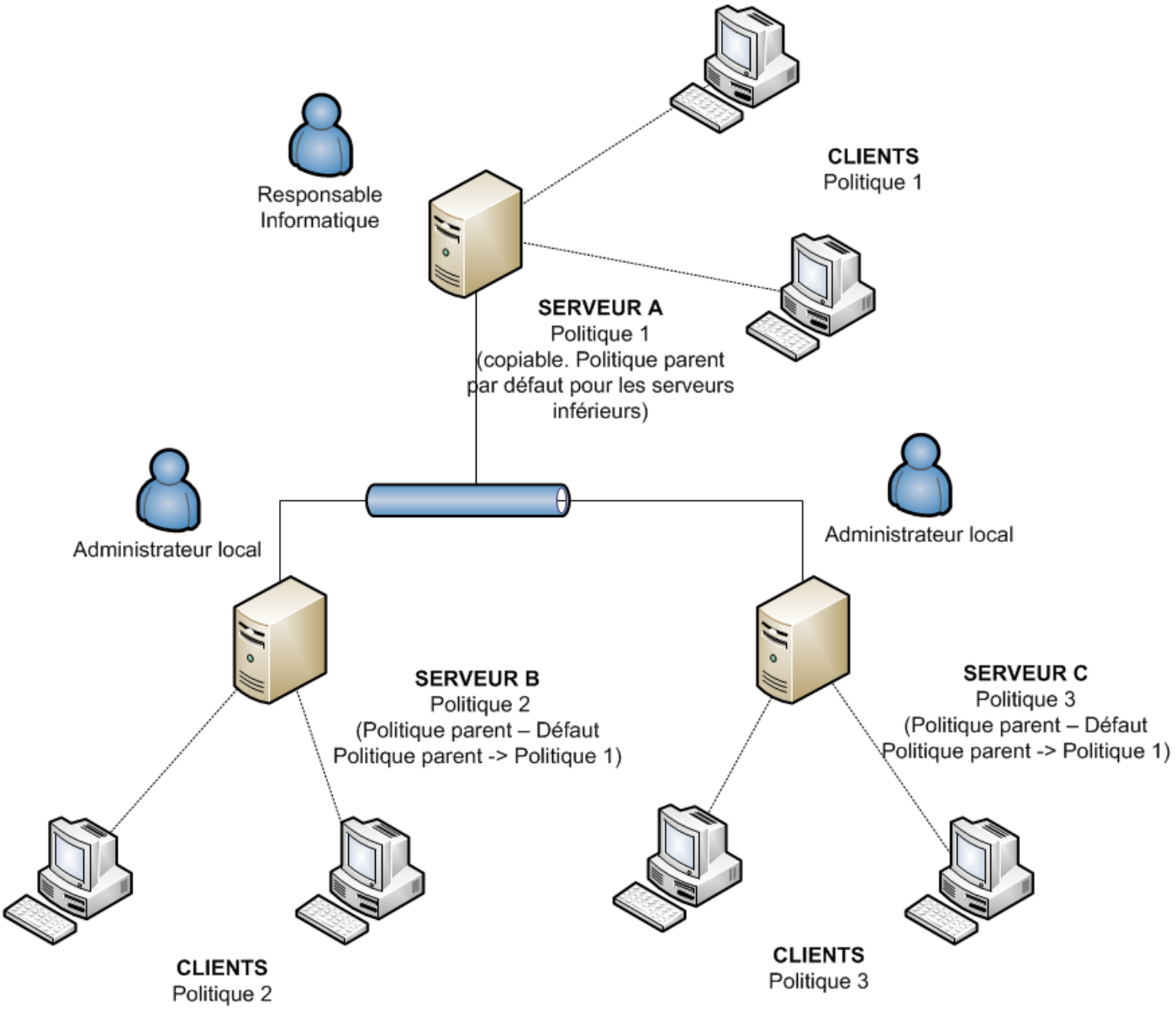
5.3.12.1 Chaque serveur est une unité autonome et les stratégies sont définies localement

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).



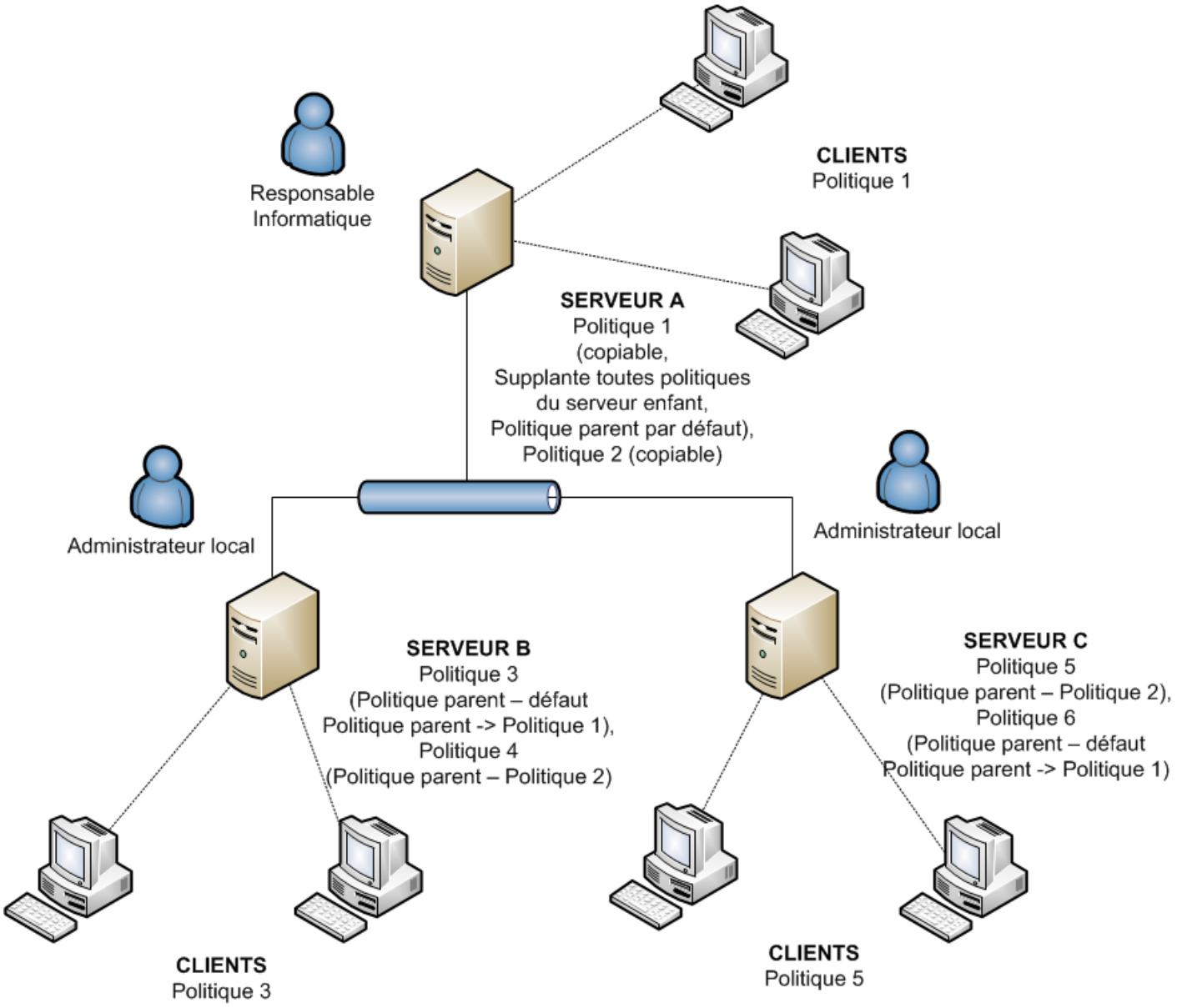
5.3.12.2 Chaque serveur est administré individuellement ; les stratégies sont gérées localement mais la stratégie parent par défaut est héritée du serveur de niveau supérieur

La configuration du scénario précédent s'applique 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.



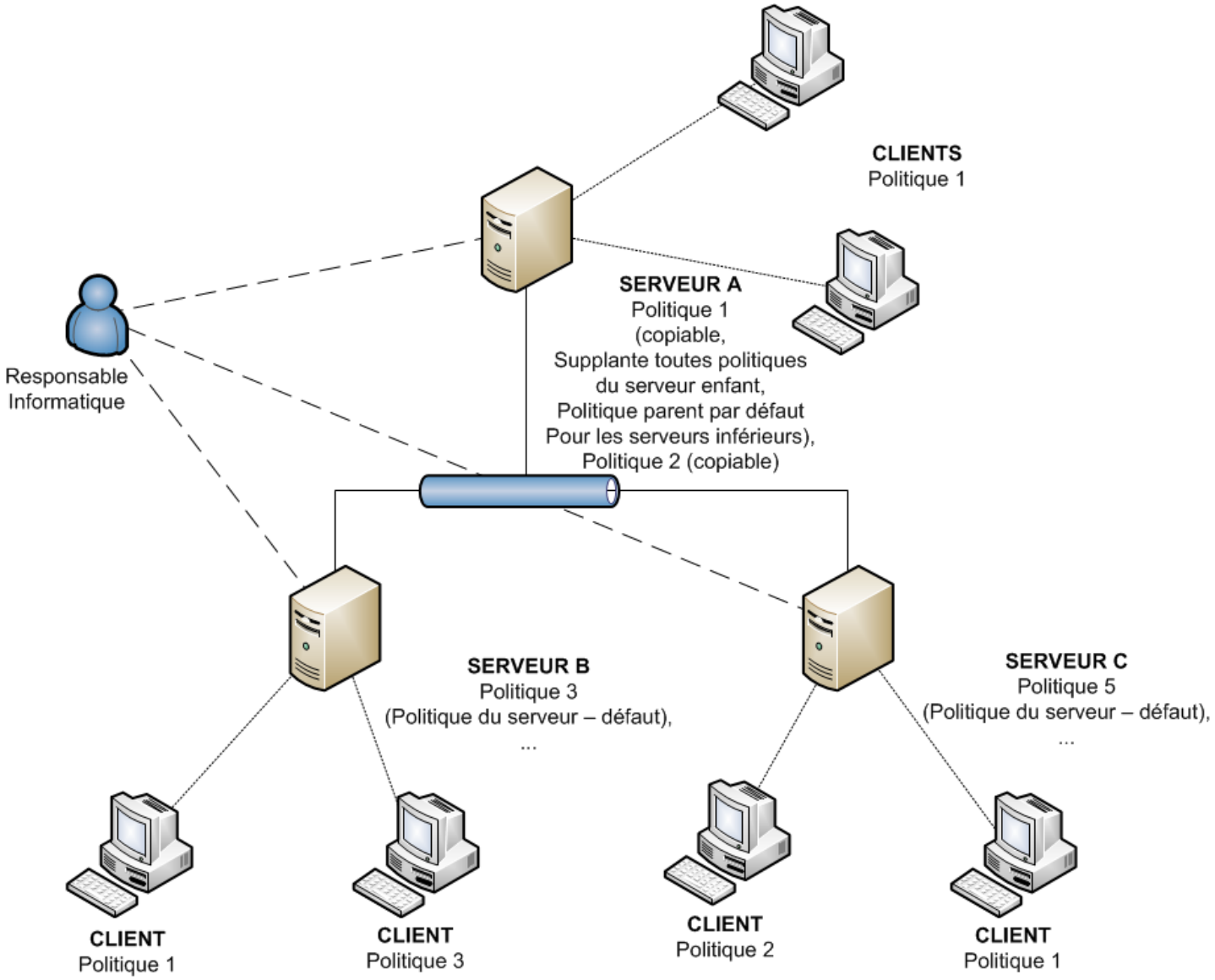
5.3.12.3 Héritage de stratégies d'un serveur de niveau supérieur

Le modèle de réseau pour ce scénario est le même que celui des deux scénarios précédents. De plus, 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 ci-dessous), 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 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.



5.3.12.4 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 (appelée par défaut Stratégie du serveur). Cette stratégie vide fait également office de stratégie parent par défaut pour clients principaux.



5.3.12.5 Utilisation de groupes

Dans certains cas, l'attribution de stratégies à des groupes de clients peut compléter les scénarios précédents. Il est possible de créer des groupes manuellement ou via l'option **Synchronisation Active Directory**.

Les clients peuvent être ajoutés aux groupes manuellement (**Groupes statiques**) ou automatiquement, selon les propriétés du groupe (**Groupes paramétriques**). Consultez le chapitre Gestionnaire de groupes 69 pour plus d'informations.

Pour attribuer une stratégie à un groupe de clients, vous pouvez utiliser l'option d'attribution ponctuelle sous **Gestionnaire de stratégies** (**Ajouter clients > Ajout spécial**) ou les livrer automatiquement via les **Règles de stratégie**).

Un scénario possible serait le suivant :

L'administrateur veut attribuer différentes stratégies à des clients qui appartiennent à différents groupes AD et changer automatiquement la stratégie du client lorsque celui est déplacé vers un autre groupe AD.

1) La première étape consiste à définir la **Synchronisation Active Directory** dans le **Gestionnaire de groupes** selon vos besoins. L'élément important ici est de planifier correctement la synchronisation AD (options possibles : tous les jours, quotidien, hebdomadaire ou mensuel).

2) Après la première synchronisation réussie, les groupes AD apparaissent dans la section **Groupes statiques**.

3) Créez une stratégie et choisissez **Groupes ERA DANS** et **Groupes ERA PAS DANS** en tant que condition de règle.

4) Désignez les groupes AD que vous souhaitez ajouter à la condition.

5) À l'étape suivante, définissez la stratégie qui sera appliquée aux clients qui répondent aux conditions de la règle et cliquez sur **OK** pour enregistrer la règle.

REMARQUE :: les étapes 3 à 5 peuvent être remplacée par l'utilisation de l'**Assistant Règles de stratégie** qui permet de créer une structure de stratégie basée sur la structure du groupe existant et d'associer les stratégies créées aux groupes en créant les règles de stratégie correspondante.

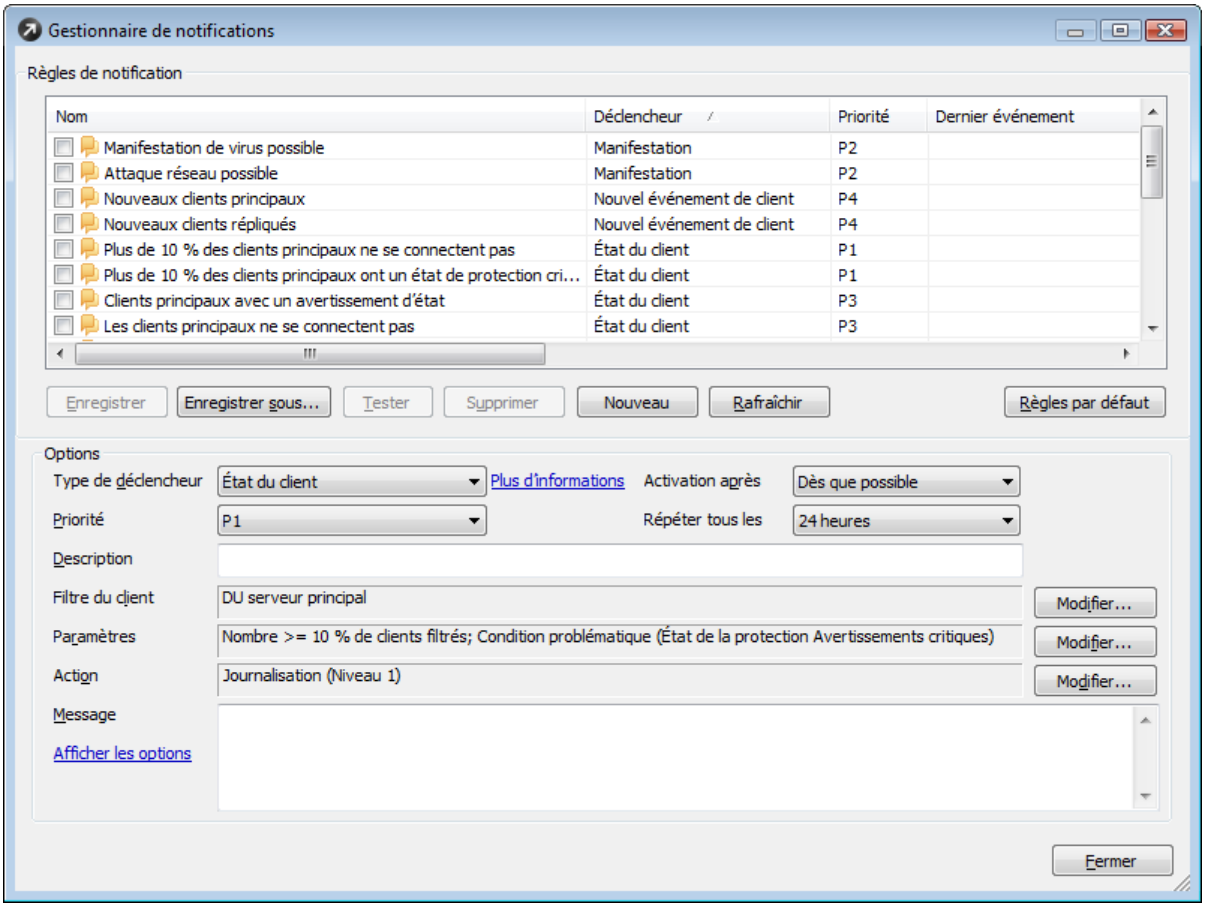
Il est ainsi possible de définir une règle de stratégie particulière pour chaque groupe AD. L'attribution d'une certaine stratégie à un certain client dépend maintenant de l'appartenance du client à un certain groupe AD. Dans la mesure où la synchronisation AD est planifiée pour une exécution régulière, toutes les modifications dans l'appartenance d'un client à un groupe AD sont actualisées et prises en compte lorsqu'une règle de stratégie est appliquée. En d'autres termes, les stratégies sont appliquées aux clients automatiquement en fonction de leur groupe AD. Une fois que les règles et les stratégies ont été définies en détail, l'administrateur n'a plus à intervenir au niveau de l'application de la stratégie.

Le principal avantage de cette approche est la liaison automatique et directe entre l'appartenance à un groupe AD et l'attribution d'une stratégie.

5.4 Gestionnaire de notifications

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

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



La fenêtre principale comprend deux sections :

1. 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 par conséquent conseillé de vérifier si les règles sont actives. Les boutons de fonction sous la liste des règles sont **Enregistrer** (enregistre les modifications dans une règle), **Enregistrer sous...** (enregistre les modifications dans une règle sous un nouveau nom), **Supprimer**, **Tester** (le fait de cliquer sur ce bouton déclenche immédiatement la règle et envoie une notification), **Nouveau** (utilisez ce bouton pour créer des règles), **Rafraîchir** et **Règles par défaut** (actualise la liste avec les règles par défaut).

Par défaut, la fenêtre **Gestionnaire de notifications** contient des règles prédéfinies. Pour activer une règle, cochez la case 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 est exécutée selon le paramètre 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 ne se sont pas connectés au serveur depuis plus d'une semaine, la règle est exécutée selon le paramètre Dès que possible.
- **Clients principaux avec un avertissement d'état** : si au moins un client avec un avertissement d'état de protection ne s'est pas connecté au serveur depuis au moins une semaine.
- **Les clients principaux ne se connectent pas** : si au moins un client ne s'est pas connecté au serveur depuis plus d'une semaine.
- **Client principaux dont la base des signatures de virus est obsolète** : si un client avec une base des signatures de virus antérieure d'au moins deux versions à la base actuelle ne s'est pas déconnecté du serveur depuis plus d'une semaine.
- **Clients principaux dont l'état de protection est critique** : si un client avec un avertissement critique sur l'état de la protection 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** : si un client avec une base des signatures de virus plus récente que celle du serveur ne s'est pas déconnecté depuis plus d'une semaine.
- **Clients principaux en attente de démarrage** : si un client en attente de redémarrage 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** : si un client sur lequel l'analyse de l'ordinateur n'a pas pu nettoyer au moins une infiltration ne s'est pas déconnecté depuis plus d'une semaine, la règle est exécutée selon le paramètre Dès que possible.
- **Tâche accomplie** : si une tâche a été accomplie sur un client, la règle est exécutée selon le paramètre Dès que possible.
- **Nouveaux clients principaux** : si un nouveau client s'est connecté au serveur, la règle est exécutée selon le paramètre Dès que possible.
- **Nouveaux clients répliqués** : si un nouveau client répliqué figure dans la liste des clients, la règle est exécutée au bout d'une heure.
- **Manifestation de virus possible** : si la fréquence des entrées dans le journal des menaces a dépassé 1 000 avertissements critiques en une heure sur au moins 10 % de tous les clients.
- **Attaque réseau possible** : si la fréquence des entrées dans le journal du pare-feu personnel ESET a dépassé 1 000 avertissements critiques en une heure sur au moins 10 % de tous les clients.
- **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 est exécutée selon le paramètre 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 est exécutée selon le paramètre Dès que possible.
- **Limite de la licence** : si le nombre de clients disponibles chute sous 10 % des clients.

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

2. La section **Options** dans la moitié inférieure de la fenêtre fournit des informations sur la règle actuellement sélectionnée. Les champs et options de cette section sont décrits à l'aide de l'exemple de règle de la section Création de règle 91.

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

- État du client 85 : la règle s'exécute en cas de problème sur certains clients.
- État du serveur 86 : la règle s'exécute en cas de problème sur certains serveurs.
- Événement de tâche terminée 88 : la règle s'exécute lorsque la tâche spécifiée est terminée.

- Nouvel événement de client 88 : la règle s'exécute si un nouveau client (y compris un client répliqué) se connecte au serveur.
- Manifestation 88 : la règle s'exécute si une vague d'incidents affecte un nombre significatif de clients.
- Événement de journal reçu 89 : la règle s'exécute si l'administrateur souhaite être informé des journaux dans un certain intervalle.

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 la définition du type des déclencheurs lors de la création de règles 91.

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 déroulant **Priorité** contient un champ **Description**. Il est recommandé d'attribuer à chaque règle une description compréhensible, telle que *« règle avertissant sur les infiltrations détectées »*.

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

- **Rule_Name**
- **Rule_Description**
- **Priority** : priorité de la règle de notification (P1 correspond à la priorité la plus élevée).
- **Triggered** : date d'envoi de la notification la plus récente (répétitions exclues).
- **Triggered_Last** : date d'envoi de la notification la plus récente (répétitions incluses).
- **Client_Filter** : paramètres de filtre du client.
- **Client_Filter_Short** : paramètres de filtre du client (sous forme abrégée).
- **Client_List** : liste de clients.
- **Parameters** : paramètres de la règle.
- **Primary_Server_Name**
- **Server_Last_Updated** : dernière mise à jour du serveur.
- **Virus_Signature_DB_Version** : version la plus récente de la base des signatures de virus.
- **Pcu_List** : dernière liste de tous les PCU.
- **Pcu_List_New_Eula** : dernière liste des PCU avec nouveau CLUF.
- **Last_Log_Date** : date du dernier journal.
- **Task_Result_List** : liste des tâches accomplies.
- **Log_Text_Truncated** : texte de journal ayant activé la notification (tronqué).
- **License_Info_Merged** : informations de licence (résumé).
- **License_Info_Full** : informations de licence (complètes).
- **License_Days_To_Expiry** : jours restants avant l'expiration.
- **License_Expiration_Date** : date d'expiration la plus proche.
- **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.

5.4.1 État du client

Définissez les paramètres de filtrage du client dans la fenêtre **Filtre du client**. 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 par le drapeau « *Nouveau* » (il est également possible d'appliquer forme négative N'A PAS).
- **Groupes ERA ENTRANTS** : clients appartenant au groupe spécifié.
- **Domaine/Groupe de travail ENTRANT** : clients appartenant au domaine spécifié.
- **Masque de nom d'ordinateur** : clients portant le nom d'ordinateur spécifié.
- **A un masque IPv4** : clients correspondant au masque IPv4 spécifié.
- **A une plage IPv4** : clients s'inscrivant dans la plage d'adresses IPv4 spécifiée.
- **A un préfixe réseau IPv6** : clients ayant le préfixe réseau IPv6.
- **A une plage IPv6** : clients s'inscrivant dans la plage d'adresses IPv6 spécifiée.
- **A défini une stratégie** : clients auxquels est attribuée la stratégie spécifiée (la négation de cette condition, N'A PAS, peut également être appliquée).

Après avoir défini un filtre de 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. Les paramètres suivants sont disponibles pour les déclencheurs État du client :

- **État de la protection Tous avertissement** : 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 la Base de signatures des virus** : problème avec la base des signatures de virus (6 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 ancienne que 5 versions ou n.a.** : la base des signatures de virus est antérieure de plus de 5 versions à celle présente sur le serveur.
  - **Plus ancienne que 10 versions ou n.a.** : la base des signatures de virus est antérieure de plus de 10 versions à celle présente sur le serveur.
  - **Plus ancienne que 7 jours ou n.a.** : la base des signatures de virus est antérieure de plus de 7 jours à celle présente sur le serveur.
  - **Plus ancienne que 14 jours ou n.a.** : la base des signatures de virus est antérieure de 14 jours au moins à celle présente sur le serveur.

- **Avertissement de dernière connexion** : la dernière connexion a été établie avant la période spécifiée.
- **A un événement de dernière menace** : la colonne Menace contient un avertissement de menace.
- **A un dernier événement** : la colonne Dernier événement contient une entrée.
- **A un événement de dernier 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.
- **Menace détectée lors de la dernière analyse** : sur le client, le nombre spécifié de menaces a été détecté lors de la dernière analyse.
- **Menace non nettoyée lors de la dernière analyse** : sur le client, le nombre spécifié de menaces non nettoyées a été détecté 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 **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.
- **l'une des options est vérifiée** : la règle s'exécute si au moins **une** condition est vraie.

Si les paramètres spécifiés pour une règle se vérifient, l'action correspondante définie par l'administrateur est exécutée automatiquement. Pour configurer des actions, dans la section Actions 90, cliquez sur **Modifier**.

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. L'intervalle de temps à l'issue duquel le serveur vérifiera l'existence de règles actives et les exécutera peut être défini dans **Serveur** > **Paramètres avancés** > **Modifier les paramètres avancés** > **ESET Remote Administrator** > **Serveur** > **Configuration** > **Notifications** > **Intervalle pour le traitement de notification (minutes)**.

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

5.4.2 État du serveur

La fenêtre **Paramètres de règle du serveur** permet de définir les paramètres qui déclencheront une règle liée à l'état du serveur particulier qui sera ensuite appliquée à l'envoi de notifications. Pour définir un paramètre, cliquez sur la case d'option en regard d'un état spécifique. Cette action activera les éléments adjacents actifs de l'interface utilisateur graphique afin que vous puissiez modifier le ou les paramètres d'une condition.

- **Serveur mis à jour** : le serveur est à jour.
- **Serveur non mis à jour** : le serveur n'est plus à jour depuis plus longtemps que la durée spécifiée.
- **Journal de vérification** : le **journal de vérification** surveille et journalise toutes les modifications apportées à la configuration, ainsi que toutes les opérations effectuées par les utilisateurs de la console ERAC. Vous pouvez filtrer les entrées du journal par type (voir **Journal du serveur**).
- **Journal du serveur** : le journal du serveur contient les types d'entrée suivants :
  - **Erreurs** : messages d'erreur.
  - **Erreurs+Avertissements** : messages d'erreur et d'avertissement.
  - **Erreurs+Avertissements+Infos (Verbosité)** : messages d'erreur, d'avertissement et d'information.

- **Filtrer les entrées de journal par type** : activez cette option pour spécifier les entrées d'erreur et d'avertissement à observer dans le journal du serveur. Notez que, pour que les notifications fonctionnent correctement, le niveau de détail du journal (**Outils > Options du serveur > Journalisation**) doit être correctement défini. Sinon, les 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 1** : message du serveur interne.
- **INTERNAL 2** : message du 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.
- **SESSION_USERACTION** : diverses actions du serveur.
- **THREATSENSE** - ESET Live Grid : soumission d'informations statistiques.
- **UPDATER** : mise à jour du serveur et création de miroir.

UPDATER est un exemple de paramètre utile, 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. Sélectionnez **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 de 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.

Si les paramètres spécifiés pour une règle se vérifient, l'action correspondante définie par l'administrateur est exécutée automatiquement. Pour configurer des actions, dans la section Actions 90, cliquez sur **Modifier**.

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. L'intervalle de temps à l'issue duquel le serveur vérifiera l'existence de règles actives et les exécutera peut être défini dans **Serveur** > **Paramètres avancés** > **Modifier les paramètres avancés** > **ESET Remote Administrator** > **Serveur** > **Configuration** > **Notifications** > **Intervalle pour le traitement de notification (minutes)**.

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

5.4.3 Événement de tâche terminée

La règle sera déclenchée une fois que les tâches sélectionnées seront terminées. Dans les paramètres **par défaut**, tous les types de tâche 64 sont sélectionnés.

Si les paramètres spécifiés pour une règle se vérifient, l'action correspondante définie par l'administrateur est exécutée automatiquement. Pour configurer des actions, dans la section Actions 90, cliquez sur **Modifier**.

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).

5.4.4 Événement de nouveau client

Définissez les nouveaux paramètres de filtrage du client dans la fenêtre **Filtre du client**. 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 par le drapeau « *Nouveau* » (il est également possible d'appliquer forme négative N'A PAS).
- **Groupes ERA ENTRANTS** : clients appartenant au groupe spécifié.
- **Domaine/Groupe de travail ENTRANT** : clients appartenant au domaine spécifié.
- **Masque de nom d'ordinateur** : clients portant le nom d'ordinateur spécifié.
- **A un masque IPv4** : clients correspondant au masque IPv4 spécifié.
- **A une plage IPv4** : clients s'inscrivant dans la plage d'adresses IPv4 spécifiée.
- **A un préfixe réseau IPv6** : clients s'inscrivant dans la plage d'adresses IPv6 spécifiée.
- **A une plage IPv6** : clients s'inscrivant dans la plage d'adresses IPv6 spécifiée.
- **A défini une stratégie** : clients auxquels est attribuée la stratégie spécifiée (la négation de cette condition, N'A PAS, peut également être appliquée).

Si les paramètres spécifiés pour une règle se vérifient, l'action correspondante définie par l'administrateur est exécutée automatiquement. Pour configurer des actions, dans la section Actions 90, cliquez sur **Modifier**.

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).

5.4.5 Manifestation

Cette notification est déclenchée dès que les critères définis pour une vague d'incidents sont remplis. Elle ne signale pas chaque incident isolé ni les incidents dépassant ces critères.

Définissez les paramètres de filtrage d'une manifestation dans la fenêtre **Filtre du client**. 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 par le drapeau « *Nouveau* » (il est également possible d'appliquer forme

négative N'A PAS).

- **Groupes ERA ENTRANTS** : clients appartenant au groupe spécifié.
- **Domaine/Groupe de travail ENTRANT** : clients appartenant au domaine spécifié.
- **Masque de nom d'ordinateur** : clients portant le nom d'ordinateur spécifié.
- **A un masque IPv4** : clients correspondant au masque IPv4 spécifié.
- **A une plage IPv4** : clients s'inscrivant dans la plage d'adresses IPv4 spécifiée.
- **A un préfixe réseau IPv6** : clients s'inscrivant dans la plage d'adresses IPv6 spécifiée.
- **A une plage IPv6** : clients s'inscrivant dans la plage d'adresses IPv6 spécifiée.
- **A défini une stratégie** : clients auxquels est attribuée la stratégie spécifiée (la négation de cette condition, N'A PAS, peut également être appliquée).

Après avoir défini un filtre de 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**.

- **Type de journal** : sélectionnez le type de journal à surveiller.
- **Niveau de journalisation** : niveau d'entrée de journal dans le journal donné.
  - Niveau 1 - Avertissements critiques : erreurs critiques uniquement.
  - Niveau 2 - Supérieur + Avertissement : 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.
- **1 000 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 1 000 occurrences par heure.
- **Nombre** : nombre de clients (exprimé en valeur absolue ou en pourcentage).

L'**intervalle d'accélération** correspond à l'intervalle de temps utilisé pour l'envoi des notifications. Par exemple, si l'intervalle d'accélération est fixé à 1 heure, les données sont collectées en arrière-plan et vous recevez la notification toutes les heures (en cas de manifestation et à condition que le déclencheur soit actif).

5.4.6 Événement de journal reçu

Cette option est utilisée lorsque vous voulez être informé de chaque journal dans un intervalle de temps précis.

Définissez les paramètres de filtrage du client dans la fenêtre **Filtre du client**. 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 par le drapeau « *Nouveau* » (il est également possible d'appliquer forme négative N'A PAS).
- **Groupes ERA ENTRANTS** : clients appartenant au groupe spécifié.
- **Domaine/Groupe de travail ENTRANT** : clients appartenant au domaine spécifié.
- **Masque de nom d'ordinateur** : clients portant le nom d'ordinateur spécifié.
- **A un masque IPv4** : clients correspondant au masque IPv4 spécifié.
- **A une plage IPv4** : clients s'inscrivant dans la plage d'adresses IPv4 spécifiée.
- **A un préfixe réseau IPv6** : clients s'inscrivant dans la plage d'adresses IPv6 spécifiée.
- **A une plage IPv6** : clients s'inscrivant dans la plage d'adresses IPv6 spécifiée.
- **A défini une stratégie** : clients auxquels est attribuée la stratégie spécifiée (la négation de cette condition, N'A PAS,

peut également être appliquée).

Après avoir défini un filtre de 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**.

- **Type de journal** : sélectionnez le type de journal à surveiller.
- **Niveau de journalisation** : niveau d'entrée de journal dans le journal donné.
  - Niveau 1 - Avertissements critiques : erreurs critiques uniquement.
  - Niveau 2 - Supérieur + Avertissement : 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.

Si les paramètres spécifiés pour une règle se vérifient, l'action correspondante définie par l'administrateur est exécutée automatiquement. Pour configurer des actions, dans la section Actions 90, cliquez sur **Modifier**.

L'**intervalle d'accélération** correspond à l'intervalle de temps utilisé pour l'envoi des notifications. Par exemple, si l'intervalle d'accélération est fixé à 1 heure, les données sont collectées en arrière-plan et vous recevez la notification toutes les heures (si le déclencheur est toujours actif).

5.4.7 Action

Si les paramètres spécifiés pour une règle se vérifient, l'action correspondante définie par l'administrateur est exécutée automatiquement. 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 email 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 des notifications SNMP.
- **Exécuter (sur le serveur)** : activez cette option et spécifiez l'application à exécuter sur le serveur. Saisissez le chemin d'accès complet à l'application.
- **Journaliser dans un fichier** : génère des entrées de journal dans le fichier journal spécifié. Indiquez le chemin d'accès complet au dossier. Le niveau de **détail** des notifications est configurable.
- **Connexion à Syslog** : enregistre les notifications dans les journaux système. Le niveau de **détail** des notifications est configurable.
- **Journalisation** : journalise les notifications dans les journaux du serveur. L'option **Verbosité** permet de configurer le niveau de détails de ce journal.
- **Exécuter le rapport** : après avoir sélectionné cette option, vous pouvez cliquer sur le menu déroulant **Nom du modèle**. Là, sélectionnez le modèle à utiliser pour le rapport. Pour plus d'informations sur les modèles, consultez le chapitre Rapports 36.

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

5.4.8 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*.

5.4.9 Exemple de 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**, puis activez seulement la condition de règle de la section **Groupes ERA 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 saisissez le nom et le chemin d'accès du fichier journal à créer. Vous avez la possibilité de sélectionner le niveau de **Verbosité** 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 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, cliquez sur **Outils** > **ESET SysInspector** dans le menu principal d'ERAC. 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 de la souris 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. Une fenêtre proposant les options suivantes s'ouvre :

- **Créer un instantané (enregistrer également le journal du résultat 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 **SysInspector** des **Propriétés du client**. 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 **Rafraîchir** 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 :

- **Afficher** : 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 **Afficher**).

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.

5.6 Assistant Fusion des règles de pare-feu

L'Assistant Fusion des règles de pare-feu permet de fusionner les règles de pare-feu pour les clients sélectionnés. Ceci est particulièrement utile si vous devez créer une configuration unique qui contient toutes les règles de pare-feu récoltées par les clients en mode d'apprentissage. La configuration obtenue peut être envoyée aux clients via une tâche de configuration ou peut être appliquée en tant que stratégie.

L'Assistant est accessible via le menu déroulant **Outils** et via le menu contextuel de l'onglet **Clients** après avoir cliqué avec le bouton droit de la souris sur les clients sélectionnés (les clients sélectionnés sont ensuite ajoutés automatiquement aux éléments sélectionnés à la première étape).

REMARQUE : Pour réaliser cette action correctement, tous les clients sélectionnés doivent stocker la configuration la plus récente (envoyée ou répliquée) sur le serveur. Vous devez choisir les clients ou les groupes de clients dont les règles de pare-feu seront fusionnées. L'étape suivante affiche la liste des clients sélectionnés et leur état de configuration. Si la configuration d'un client ne se trouve pas sur le serveur, vous pouvez la demander en cliquant sur le bouton **Demande**. Enfin, vous pourrez sélectionner les règles fusionnées à utiliser dans la configuration et les enregistrer dans un fichier *.xml*.

6. Options d'ERA Server

Vous pouvez configurer ERA Server directement à partir de la console ERA Console qui est connectée à ERA Server (option **Outils** > **Options du serveur**.

6.1 Général

L'onglet **Général** présente des informations générales sur ERA Server :

- **Informations sur le serveur** : cette section répertorie les informations de base d'ERA Server. Cliquez sur le bouton Modifier le mot de passe pour ouvrir l'onglet Sécurité 94 des options ERA Server.
- **Informations de licence** : indique le nombre de licences client de produit de sécurité ESET que vous avez achetées, ainsi que la version actuelle du système antivirus NOD32 ou d'ESET Smart Security installée sur le serveur. Si votre licence a expiré et que vous en avez acquis une nouvelle, cliquez sur le bouton Gestionnaire de licences 93 pour ouvrir une boîte de dialogue dans laquelle vous pouvez sélectionner la nouvelle licence pour activer ERA.
- **Version de la base de signatures des virus** : affiche la version de la base de signatures des virus (en fonction des informations de mise à jour fournies et des produits de sécurité utilisés).
- **Performances** : affiche la connexion serveur-client et les informations générales de performances.

6.1.1 Gestion de licences

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 :

1) Accédez à **Outils** > **Gestionnaire de licences** ou appuyez sur les touches **CTRL + L** de votre clavier.

2) Cliquez sur **Parcourir** pour accéder au fichier de clé de licence souhaité (les fichiers de ce type portent l'extension *.lic*).

3) Cliquez sur **Ouvrir** pour confirmer.

4) Vérifiez que les informations de clé de licence sont correctes, puis sélectionnez **Charger sur le serveur**.

5) 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 d'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 client disponibles chute sous la valeur spécifiée (en %).

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.

6.2 Sécurité

Les solutions de sécurité ESET (ESET Smart Security) versions 3.x et ultérieures 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 la rétrocompatibilité avec des versions antérieures, l'option **Activer l'accès non authentifié de clients** doit être sélectionnée. L'onglet **Sécurité** contient des options permettant à l'administrateur d'utiliser les solutions de sécurité 2.x et 3.x simultanément sur le même réseau.

Protection pour la communication avec un serveur ERA Server.

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

Paramètres de sécurité de la console

- **Utiliser l'authentification de Windows/domaine** : active l'authentification de Windows/domaine et permet de définir des groupes d'administrateurs (avec accès complet au serveur ERA Server) ainsi que des groupes avec accès en lecture seule (option **Traiter tous les autres utilisateurs comme s'ils avaient un accès en lecture seule**). Si cette case est cochée, l'option **Autoriser un accès en lecture seule pour les utilisateurs Windows/du domaine non assignés à un utilisateur du serveur ERA** devient active et peut être sélectionnée. Cette option garantit que ces utilisateurs ne peuvent pas modifier les paramètres de la console ERAC. Si vous souhaitez attribuer des utilisateurs de serveur ERA, cliquez sur **Gestionnaire des utilisateurs**.
- L'accès à la console utilisateur peut être géré au moyen de l'outil Gestionnaire des utilisateurs 95.

Paramètres de sécurité du serveur

- **Mot de passe pour les clients** : définit le mot de passe des clients qui accèdent au serveur ERAS.
- **Mot de passe pour la réplication** : définit le mot de passe des serveurs ERA Server 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 le mot de passe avec lequel l'agent d'installation accède au serveur ERAS (approprié pour les installations à distance).
- **Activer l'accès non authentifié de clients (produits de sécurité ESET)** : active l'accès au serveur ERAS pour les clients sans mot de passe valide (mot de passe actuel différent du **mot de passe pour les clients**).
- **Activer l'accès non authentifié pour la réplication** : active l'accès au serveur ERAS pour les clients de serveurs ERA Server de niveau inférieur n'ayant pas de mot de passe valide pour la réplication.
- **Activer l'accès non authentifié pour le programme d'installation à distance d'ESET (Agent)** : active l'accès au serveur ERAS pour les programmes d'installation à distance d'ESET qui ne disposent pas d'un mot de passe valide.

REMARQUE : L'option **Par défaut** concerne uniquement les paramètres prédéfinis. Elle ne permet pas de réinitialiser les mots de passe.

REMARQUE : Pour renforcer la sécurité, vous pouvez utiliser des mots de passe complexes. Sélectionnez **Outils** > **ESET Éditeur de configuration** > **Administration à distance** > **ERA Server** > **Paramètres** > **Sécurité** > **Nécessite un mot de passe complexe**, puis paramétrez cette option sur **Oui**. Lorsque cette option est activée, chaque nouveau mot de passe doit se composer d'au moins 8 caractères, et comporter une lettre minuscule, une lettre majuscule et un caractère non alphabétique.

6.2.1 Gestionnaire des utilisateurs

Les outils du **Gestionnaire des utilisateurs** permettent d'administrer les comptes utilisateurs pour l'authentification console-serveur. Les comptes Administrateur (accès complet) et Lecture seule sont prédéfinis.

Cliquez sur **Nouveau** afin d'ajouter un nouveau compte utilisateur pour l'authentification console-serveur. Définissez le **nom d'utilisateur** et le **mot de passe**, ainsi que les **autorisations** spécifiques.

Le champ **Description** est destiné aux descriptions personnalisées de l'utilisateur ; il n'est pas obligatoire.

Les **autorisations** définissent le niveau d'accès de l'utilisateur, ainsi que les tâches spécifiques qu'il peut effectuer. Vous pouvez modifier le mot de passe d'accès à la console 95 de chaque utilisateur ayant accès à la console en sélectionnant l'utilisateur et en cliquant sur l'option **Modifier...** située à côté de **Mot de passe d'authentification de la console**.

REMARQUE :: Les autorisations des comptes prédéfinis (Administrateur et Lecture seule) ne peuvent pas être modifiées.

Vous pouvez associer un ou plusieurs **groupes d'authentification de Windows/domaine** à un utilisateur ERA Server sélectionné. Si un groupe Windows/domaine est attribué à plusieurs utilisateurs, le premier utilisateur de la liste est utilisé. Les flèches vers le haut et vers le bas situées à côté de la liste des utilisateurs permettent de définir l'ordre des utilisateurs.

6.2.2 Mot de passe d'accès à la console

Pour modifier le mot de passe d'accès à la console, cliquez sur **Fichier** > **Modifier le mot de passe** ou modifiez le mot de passe à l'aide du Gestionnaire des utilisateurs 95. Saisissez l'ancien mot de passe, puis deux fois le nouveau mot de passe (pour le confirmer). Si vous cochez la case située à côté de l'option **Modifier également le mot de passe stocké en mémoire cache**, le mot de passe stocké en mémoire cache et utilisé au lancement de l'application (de manière à éviter que l'utilisateur ait à le saisir à chaque connexion à ERAC) est modifié.

REMARQUE : les mots de passe que vous définissez dans cette boîte de dialogue sont envoyés directement au serveur. Cela signifie que la modification est effectuée immédiatement après que vous cliquez sur **OK** et qu'elle ne peut pas être annulée.

6.3 Maintenance du serveur

Si la configuration est correcte dans l'onglet **Maintenance du serveur**, la base de données d'ERA Server est automatiquement maintenue et optimisée, sans qu'aucune configuration supplémentaire soit nécessaire. Vous pouvez définir les paramètres de nettoyage suivants :

- **Paramètres de collecte des journaux** : définit le niveau des journaux reçus par le serveur.
- **Paramètres de nettoyage** : supprime les journaux en fonction du paramètre d'intervalle de temps.
- **Paramètres de nettoyage avancés** : supprime les journaux en fonction du nombre d'enregistrements.

Indique le nombre d'entrées de journal qui doivent être conservées après le nettoyage, ainsi que le niveau des journaux reçus par le serveur. Par exemple, si vous choisissez **Supprimer tous les journaux des menaces, à l'exception des 600000 derniers enregistrements** dans Paramètres de nettoyage avancés par nombre d'enregistrements de journal 97 et si le niveau Paramètres de collecte des journaux 96 pour **Menaces** est défini sur **Niveau 3 - Supérieur + Normal**, les 600 000 derniers enregistrements contenant des informations sur les erreurs critiques, les notifications d'alerte et les notifications d'informations sont conservés dans la base de données. Vous pouvez également limiter les entrées de journal à l'aide du paramètre de nettoyage par intervalle de temps 96.

Planificateur de nettoyage : effectue les options sélectionnées ci-dessus à l'intervalle spécifié. Cliquez sur **Modifier...** près de cette option pour régler les paramètres de temps. Cliquez sur **Nettoyer maintenant** pour lancer le nettoyage immédiatement.

Planificateur de compactage et réparation : compacte la base de données dans l'intervalle de temps défini à l'heure spécifiée. Le compactage et la réparation éliminent les incohérences et les problèmes, et accélèrent la communication avec la base de données. Cliquez sur **Modifier...** près de cette option pour régler les paramètres de temps. Cliquez sur **Compacter maintenant** pour lancer un compactage et une réparation immédiatement.

REMARQUE : Les outils **Nettoyage** et **Compactage et réparation** prennent du temps et utilisent une grande quantité de ressources. Il est donc recommandé de les exécuter lorsque la charge sur le serveur est minimale (vous pouvez exécuter par exemple le nettoyage la nuit et le compactage et la réparation le week-end).

Par défaut, les entrées et les journaux de plus de trois/six mois sont supprimés et la tâche **Compactage et réparation** est effectuée tous les quinze jours.

6.3.1 Paramètres de collecte des journaux

Définissez le niveau des journaux envoyés au serveur. Sélectionnez le niveau de détail de chaque type de journal à l'aide des menus déroulants correspondants.

Aucun : aucun journal ne sera envoyé au serveur. Avec ce paramètre, le client n'enregistre aucune information dans le journal et ERA ne reçoit par conséquent aucun journal.

Niveau 1 - Avertissements critiques : erreurs critiques uniquement. Les erreurs critiques ne sont pas enregistrées dans les onglets **Contrôle Web** ou **Contrôle de périphérique**, car le client ne peut pas produire ces journaux.

Niveau 2 - Supérieur + Avertissements : identique au niveau 1, plus notifications d'alerte.

Niveau 3 - Supérieur + Normal : identique au niveau 2, plus notifications informatives. Ce niveau de détail est appelé **Informations** au lieu de **Normal** côté client.

Niveau 4 - Supérieur + Diagnostics : identique au niveau 3, plus notifications de diagnostic. Ce niveau de détail doit être défini également côté client. Le paramètre par défaut sur le client est le niveau de journalisation **Informations**.

Tout : tous les journaux seront reçus.

6.3.2 Nettoyage par paramètre d'intervalle de temps

Principaux paramètres de nettoyage par intervalle de temps :

- **Supprimer les clients non connectés pendant les X derniers mois (jours)** : supprime tous les clients qui ne se sont pas connectés à ERAS pendant une période supérieure au nombre de mois (ou jours) indiqué.
- **Supprimer les journaux des menaces de plus de X mois (jours)** : supprime tous les incidents de virus (menaces détectées) antérieurs au nombre de mois (ou jours) indiqué.
- **Supprimer les journaux de pare-feu de plus de X mois (jours)** : supprime tous les journaux de pare-feu antérieurs au nombre de mois (ou jours) indiqué.
- **Supprimer les journaux des événements de plus de X mois (jours)** : supprime tous les événements système antérieurs au nombre de mois (ou jours) indiqué.
- **Supprimer les journaux HIPS de plus de X mois (jours)** : supprime tous les journaux HIPS (Host-based Intrusion Prevention System) antérieurs au nombre de mois (ou jours) indiqué.
- **Supprimer les journaux de contrôle des périphériques de plus de X mois (jours)** : supprime tous les journaux de contrôle des périphériques antérieurs au nombre de mois (ou jours) indiqué.
- **Supprimer les journaux de contrôle Web de plus de X mois (jours)** : supprime tous les journaux de contrôle Web antérieurs au nombre de mois (ou jours) indiqué.
- **Supprimer les journaux antispam de plus de X mois (jours)** : supprime tous les journaux antispam antérieurs au nombre de mois (ou jours) indiqué.
- **Supprimer les journaux de liste grise de plus de X mois (jours)** : supprime tous les journaux de liste grise antérieurs au nombre de mois (ou jours) indiqué.
- **Supprimer les journaux d'analyse de plus de X mois (jours)** : supprime tous les journaux d'analyse antérieurs au nombre de mois (ou jours) indiqué.
- **Supprimer les journaux mobiles de plus de X mois (jours)** : supprime tous les journaux mobiles antérieurs au nombre de mois (ou jours) indiqué.
- **Supprimer les entrées de quarantaine sans clients de plus de X mois (jours)** : supprime toutes les entrées de quarantaine qui ne sont attribuées à aucun client et sont antérieures au nombre de mois (ou jours) indiqué.
- **Supprimer les entrées d'ordinateurs non enregistrés de plus de X mois (jours)** : supprime toutes les entrées d'ordinateurs non enregistrés (ordinateurs qui ne sont pas gérés par ERA) antérieures au nombre de mois (ou jours) indiqué.
- **Supprimer les entrées de tâche avec l'état Terminé de plus de X mois (jours)** : supprime toutes les entrées des tâches qui sont terminées et antérieures au nombre de mois (ou jours) indiqué.

- **Supprimer toutes les entrées de tâche de plus de X mois (jours)** : supprime toutes les entrées des tâches (quel que soit leur état) antérieures au nombre de mois (ou jours) indiqué.

6.3.3 Paramètres de nettoyage avancés par nombre d'enregistrements de journal

Paramètres de nettoyage avancés par nombre d'enregistrements de journal :

- **Supprimer tous les journaux des menaces, à l'exception des X derniers enregistrements** : supprime tous les incidents de virus (menaces détectées) à l'exception du nombre d'enregistrements spécifié.
- **Supprimer tous les journaux du pare-feu, à l'exception des X derniers enregistrements** : supprime tous les journaux du pare-feu à l'exception du nombre d'enregistrements spécifié.
- **Supprimer tous les journaux des événements, à l'exception des X derniers enregistrements** : supprime tous les événements système à l'exception du nombre d'enregistrements spécifié.
- **Supprimer tous les journaux HIPS, à l'exception des X derniers enregistrements** : supprime tous les journaux HIPS (Host-based Intrusion Prevention System) à l'exception du nombre d'enregistrements spécifié.
- **Supprimer tous les journaux de contrôle des périphériques, à l'exception des X derniers enregistrements** : supprime tous les journaux de contrôle des périphériques à l'exception du nombre d'enregistrements spécifié.
- **Supprimer tous les journaux de contrôle Web, à l'exception des X derniers enregistrements** : supprime tous les journaux de contrôle Web à l'exception du nombre d'enregistrements spécifié.
- **Supprimer tous les journaux antispam, à l'exception des X derniers enregistrements** : supprime tous les journaux antispam à l'exception du nombre d'enregistrements spécifié.
- **Supprimer tous les journaux de mise en liste grise, à l'exception des X derniers enregistrements** : supprime tous les journaux de mise en liste grise à l'exception du nombre d'enregistrements spécifié.
- **Supprimer tous les journaux d'analyse, à l'exception des X derniers enregistrements** : supprime tous les journaux d'analyse à l'exception du nombre d'enregistrements spécifié.
- **Supprimer tous les journaux mobiles, à l'exception des X derniers enregistrements** : supprime tous les journaux mobiles à l'exception du nombre d'enregistrements spécifié.

6.4 Journalisation

Pour définir les paramètres de maintenance de base de données, sélectionnez **Outils/Options du serveur**, dans le menu principal de la ERA Console.
La maintenance de base de données offre des options pour conserver les journaux transparents et permet de comprimer la base de données principale d'ERA à intervalles réguliers pour préserver l'espace disponible.

1. Journal de vérification

Le journal de vérification surveille et journalise toutes les modifications apportées à la configuration, ainsi que toutes les opérations effectuées par les utilisateurs ERAC.

- Si l'option **Journaliser dans un fichier texte** est activée, de nouveaux fichiers journaux sont créés (**Rotation quand la taille est supérieure à X Mo**) et supprimés sur une base quotidienne (**Supprimer les journaux de rotation de plus de X jours**). Vous pouvez également modifier le niveau de détail du journal dans le menu déroulant situé à gauche.

Cliquez sur Afficher le journal 99 pour afficher le journal temporaire actuel.

- 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**). Vous pouvez également modifier le niveau de détail du journal dans le menu déroulant situé à gauche.
- L'option **Connexion à syslog** envoie un message syslog au serveur syslog indiqué sur un port spécifié (le serveur par défaut est localhost et le port par défaut est 514). Pour accéder aux paramètres syslog avancés, sélectionnez **Outils** > **Options du serveur** > **Paramètres avancés** >**Modifier les paramètres avancés** > **Configuration** > **Journalisation**. Vous pouvez modifier les options syslog : nom du serveur syslog, port du serveur syslog, fonctionnalité syslog et détails de syslog.

REMARQUE :: La gravité de syslog doit être configurée pour chaque type de journal. Pour le journal du serveur, il s'agit du paramètre **Fonctionnalité syslog pour le journal du serveur** ; pour le journal de débogage, il s'agit du paramètre

Fonctionnalité syslog pour le journal de débogage. Pour ces journaux, la gravité syslog est la suivante :

Détails ERA	Gravité syslog
Niveau 1 (informations)	LOG_INFO //6
Niveau 2 (erreur)	LOG_INFO //3
Niveau 3 (avertissement)	LOG_INFO //4
Niveau 4,5 (débogage)	LOG_INFO //7

Les **détails** d'un journal représentent son niveau de détail et les informations incluses.

- **Niveau 1 - Utilisateurs et groupes** : activité des utilisateurs et des groupes du journal (groupes statiques, groupes paramétriques, ajout/suppression d'un client d'un groupe, etc.).
- **Niveau 2 - Supérieur + Actions client** : liste ci-dessus + toute l'activité concernant le client ERA (définition/suppression d'un drapeau, définition de la stratégie client, demande de données, etc.).
- **Niveau 3 - Supérieur + Tâches et notifications** : liste ci-dessus + toute l'activité concernant les tâches (création/suppression de tâche, création/suppression de notification, etc.).
- **Niveau 4 - Supérieur + Rapports** : liste ci-dessus + toute l'activité concernant les rapports (création/suppression de rapport, sélection/suppression de modèle de rapport).
- **Niveau 5 - Tous les événements** : toute l'activité concernant les journaux (suppression du journal HIPS, suppression du journal des menaces, etc.).

2. Journal du serveur

En cours d'exécution, ERA Server crée un journal serveur (**Nom de fichier du journal**) concernant son activité, que vous pouvez configurer (**Détails du journal**).

REMARQUE : par défaut, la sortie au format texte est enregistrée dans le fichier *%ALLUSERSPROFILE%\Application Data\Eset\ESET Remote Administrator\Server\logs\era.log*

- Si l'option **Journaliser dans un fichier texte** est activée, de nouveaux fichiers journaux sont créés (**Rotation quand la taille est supérieure à X Mo**) et supprimés sur une base quotidienne (**Supprimer les journaux de rotation de plus de X jours**).

REMARQUE : Dans la section **Journaliser dans un fichier texte**, il est recommandé de conserver le paramètre **Détails du journal** défini sur *Niveau 2 - Supérieur + Erreurs de session* et de n'augmenter sa valeur qu'en cas de problème ou sur demande du service client d'ESET.

- 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**).

- L'option **Connexion à syslog** envoie un message syslog au serveur syslog indiqué sur un port spécifié (le serveur par défaut est localhost et le port par défaut est 514). Pour accéder aux paramètres syslog avancés, sélectionnez **Outils** > **Options du serveur** > **Paramètres avancés** >**Modifier les paramètres avancés** > **Configuration** > **Journalisation.** Vous pouvez modifier les options syslog : nom du serveur syslog, port du serveur syslog, fonctionnalité syslog et détails de syslog.

Les **détails** d'un journal représentent son niveau de détail et les informations incluses.

- **Niveau 1 - Informations critiques** : comportement défaillant (dans ce cas, veuillez contacter le service client ESET).
- **Niveau 2 - Supérieur + Informations de session importantes** : informations sur la communication serveur (personne qui s'est connectée à ERA Server, heure de la connexion et motif).
- **Niveau 3 - Supérieur + Informations diverses** : informations sur les processus internes sur ERA Server.
- **Niveau 4 - Supérieur + Programme d'installation** : informations sur l'agent einstaller.exe (informations sur ERA Server, connexion/déconnexion de l'agent et résultats).
- **Niveau 5 - Supérieur + Clients** : informations sur le client (informations sur ERA Server, connexion/déconnexion du client et résultats).

REMARQUE : 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.

3. Dans des circonstances normales, l'option **Journal de débogage de base de données** doit être désactivée ; elle n'est utilisée que pour la résolution des problèmes de base de données. Cliquez sur **Outils** > **Options du serveur** > **Paramètres avancés** > **Modifier les paramètres avancés...** > **Configuration** > **Journalisation** > **Compression du**

journal de débogage soumis à rotation afin de configurer le niveau de compression pour des journaux soumis à rotation.

6.4.1 Visionneuse du journal de vérification

Le **journal de vérification** surveille et journalise toutes les modifications apportées à la configuration, ainsi que toutes les opérations effectuées par les utilisateurs ERAC. L'administrateur peut ainsi effectuer le suivi de toutes les activités concernant ERAC, y compris tout accès non autorisé potentiel.

REMARQUE :: La visionneuse du journal de vérification affiche les modifications journalisées dans la base de données. Le journal de vérification n'inclut pas d'autres journaux (journaux de fichiers et autres).

Dans la partie gauche figure le **filtre** utilisé pour filtrer les entrées du **journal de vérification**. Vous pouvez également sélectionner le nombre d'**éléments à afficher** dans le menu déroulant de ce module, dans la partie supérieure droite, en dessous de la liste des entrées du **journal de vérification**.

Filtre :

- **De**/**A** : sélectionnez les heures de début et de fin de la période pendant laquelle les journaux doivent être filtrés. La sélection des deux options et l'indication de deux heures créent un intervalle.
- **Utilisateur** : saisissez le ou les utilisateurs pour lesquels vous souhaitez afficher les journaux.
- **Nom de connexion au domaine** : saisissez le nom de connexion au domaine du ou des utilisateurs pour lesquels vous souhaitez afficher les journaux.
- **Adresse IP** : sélectionnez l'option souhaitée (**Adresse**, **Plage** ou **Masque**) et saisissez le ou les adresses dans les champs appropriés. Ces options sont communes pour les adresses IPv4 et IPv6.
- **Types d'action** : sélectionnez les actions à afficher dans les journaux de vérification. Par défaut, tous sont sélectionnés et affichés.
- **Appliquer le filtre** : lorsque vous cliquez sur ce bouton, les paramètres de filtre sont appliqués immédiatement au **journal de vérification**.
- **Par défaut** : lorsque vous cliquez sur ce bouton, les paramètres de filtre sont réinitialisés à leur état par défaut.

Liste des entrées du journal de vérification :

- **Date** : date d'exécution de l'action. La date et l'heure sont basées sur les paramètres du serveur.
- **Utilisateur** : utilisateur ERAC qui a effectué l'opération.
- **Nom de connexion** : nom de connexion du domaine Windows de l'utilisateur qui a effectué l'opération. Cette information n'apparaît que lorsque le type de connexion Windows/Domaine est utilisé.
- **Adresse IP de la console** : adresse IP de la console depuis laquelle l'opération a été effectuée par l'utilisateur ERAC.
- **Action** : action effectuée par l'utilisateur.
- **Objet** : nombre d'objets concernés par cette action.

REMARQUE :: D'autres informations (si elles sont disponibles) s'affichent lorsque vous double-cliquez sur une ligne du journal.

6.5 Réplication

Pour définir les paramètres du serveur ERA Server, cliquez sur **Outils** > **Options du serveur** dans le menu principal de la console ERA Console.

La réplication est utilisée dans des réseaux de grande taille où plusieurs ERA Server sont installés (p. ex., une société possédant plusieurs filiales). L'onglet **Paramètres de réplication** permet de configurer une réplication de données entre plusieurs ERA Server actifs au sein de votre réseau. Pour savoir comment configurer plusieurs ERA Server dans votre organisation, consultez le chapitre Paramétrage de serveurs RA dans des réseaux de grande taille 100.

Pour configurer la réplication, utilisez les options de réplication suivantes :

Paramètres de réplication « sur »

- **Activer la réplication « vers »** : active la réplication dans un réseau de grande taille conformément aux indications du

chapitre Réplication 100.

- **Serveur de niveau supérieur** : adresse IP ou nom du serveur ERA de niveau supérieur qui collecte des données du serveur ERA local.
- **Port** : spécifie le port utilisé pour la réplication.
- **Répliquer toutes les XX minutes** : définit l'intervalle de réplication.
- **Répliquer : journal des menaces**, **journal de pare-feu**, **journal des événements**, **journal d'analyse**, **journal mobile**, **journal de quarantaine** : quand ces options sont sélectionnées, toutes les informations qui figurent sous les onglets Clients, Journal des menaces, Journal de pare-feu, Journal des événements, Journal d'analyse, Tâches, Journal mobile et Journal de quarantaine sont répliquées dans des colonnes et sur 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 : les détails du client**, **les détails du journal des menaces**, **les détails du journal d'analyse**, **les détails du journal mobile**, **les fichiers de quarantaine** : ces options permettent la réplication automatique des informations complémentaires stockées dans des fichiers individuels, qui peuvent également être téléchargées à la demande en cliquant sur **Demander**.
- **Type de journal** : définit le type d'événement à répliquer (alerte, événement, analyse) sur ERA Server de niveau supérieur.
- **Répliquer automatiquement** : active la réplication périodique. Si cette option n'est pas activée, il est possible de déclencher la réplication manuellement.

Statut de la réplication « sur »

- **Répliquer vers le haut maintenant** : lance le processus de réplication.
- **Marquer tous les clients pour la réplication** : si l'option est activée, tous les clients sont répliqués, même ceux qui n'ont pas été modifiés.

Paramètres de réplication « de »

- **Activer la réplication « de »** : permet au serveur ERA de collecter des données à partir d'autres serveurs répertoriés dans le champ **Serveurs autorisés**. Utilisez une virgule pour séparer plusieurs serveurs ERA.
- **Autoriser la réplication depuis tout serveur** : si cette case est cochée, vous pouvez effectuer une réplication depuis n'importe quel serveur. Le fait de cocher cette case désactive le champ **Serveurs autorisés**.

6.5.1 Réplication dans des réseaux de grande taille

La réplication est utilisée dans des réseaux de grande taille où plusieurs ERA Server sont installés (p. ex., une société possédant plusieurs filiales). Pour obtenir des informations supplémentaires, consultez le chapitre Installation 21.

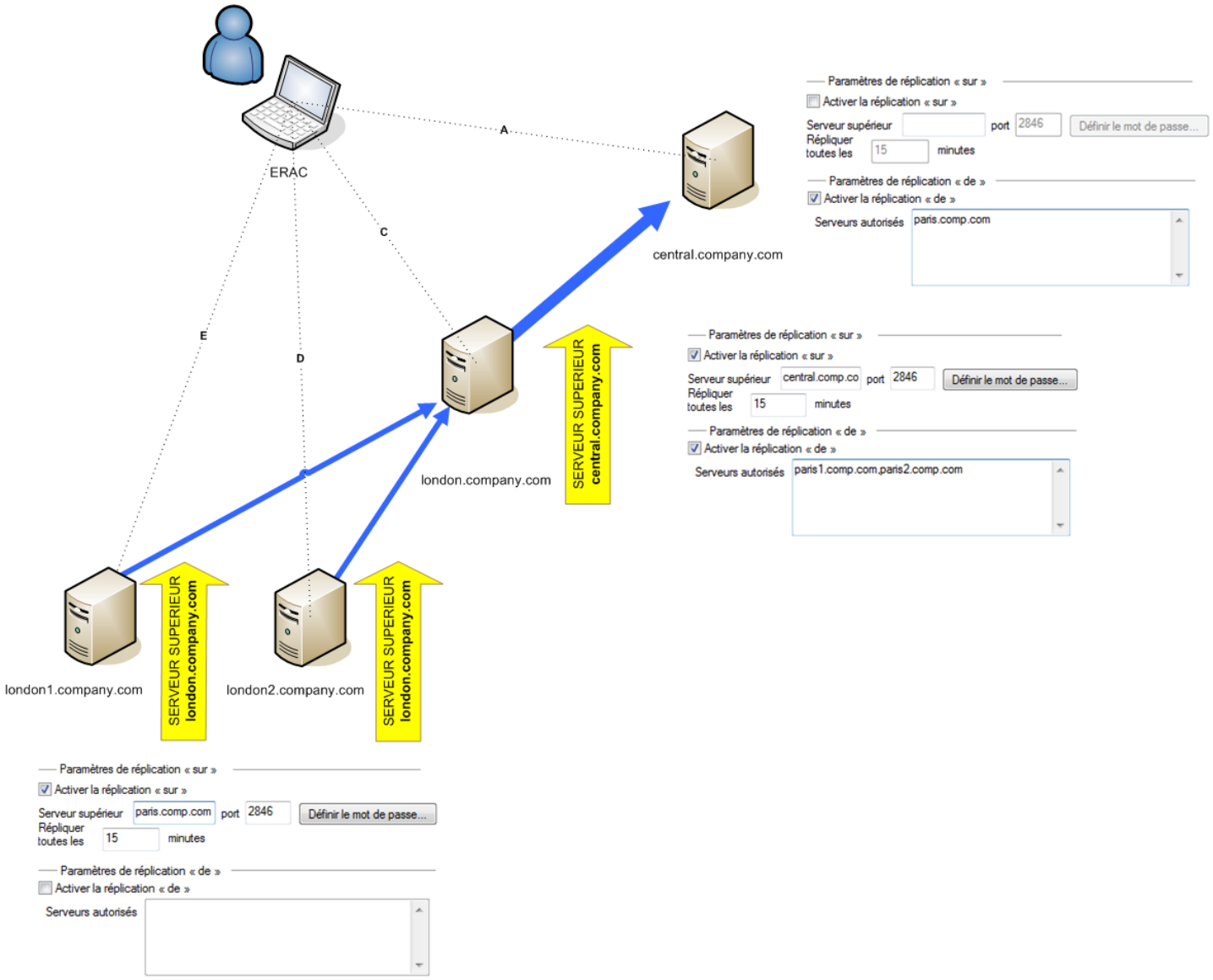
Les options disponibles sous l'onglet Réplication (**Outils > Options du serveur...**) sont réparties dans deux sections :

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

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

Ces deux options doivent être activées pour les ERA Server situés n'importe où au milieu dans 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 beiges représentent des ERA Server individuels. Chaque 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.



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**, **Répliquer journal mobile**, **Répliquer quarantaine**
  Quand ces options sont sélectionnées, toutes les informations affichées sur les onglets **Clients**, **Journal des menaces** , **Journal de pare-feu**, **Journal des événements**, **Journal d'analyse**, **Journal mobile**, **Quarantaine** 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**, **Répliquer automatiquement détails du journal mobile**, **Répliquer automatiquement fichiers de quarantaine**
  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 supprimés sur le serveur de niveau inférieur sous-jacent accessible via **Options du serveur** > **Paramètres avancés** > **Modifier les paramètres avancés** > **Configuration** > **Réplication**.

Pour définir le niveau de maintenance des journaux dans ERAS, cliquez sur **Outils** > **Options du serveur** > **Paramètres avancés** > **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 »**.

6.6 Mises à jour

La boîte de dialogue **Mises à jour**, située dans le modèle **Options du serveur**, sert à définir les paramètres de mise à jour pour ESET Remote Administrator Server. La fenêtre est divisée en deux sections : la section supérieure répertorie les options de mise à jour du serveur et la section inférieure est dédiée aux paramètres de miroir de mise à jour. Depuis la version 2.0, le serveur ESET Remote Administrator Server intègre la fonctionnalité serveur Miroir 103 qui crée un serveur de mise à jour local pour les postes de travail clients.

Voici la description de l'ensemble des éléments et fonctionnalités disponibles :

- **Serveur de mise à jour** : il s'agit du serveur de mise à jour d'ESET. Il est recommandé d'utiliser la valeur prédéfinie (Autoselect).
- **Intervalle de mise à jour** : spécifie l'intervalle maximal entre deux contrôles consécutifs de la disponibilité de nouveaux fichiers de mise à jour.
- **Nom d'utilisateur de mise à jour** : nom d'utilisateur employé par ESET Remote Administrator pour s'authentifier auprès des serveurs de mise à jour.
- **Mot de passe de mise à jour** : mot de passe lié au nom d'utilisateur donné.

La mise à jour régulière des composants du programme et de la base des signatures de virus est essentielle pour garantir la détection des menaces en temps voulu. Il arrive toutefois que les administrateurs gérant des réseaux de grande taille rencontrent des problèmes liés aux mises à jour tels que fausses alarmes ou problèmes de module. Trois options permettent de se connecter à un serveur de mise à jour :

- **Mise à jour régulière** : la base des signatures de virus est mise à jour depuis des serveurs de mises à jour régulières dès leur sortie.
- **Mise à jour des préversions** : si cette option est activée, les bêta-modules sont téléchargés lors de la mise à jour. Son utilisation n'est pas recommandée dans un environnement de production, mais uniquement à des fins de test.
- **Mise à jour retardée** : activez cette option pour recevoir les mises à jour avec un délai de 12 heures, c'est-à-dire des mises à jour testées dans un environnement de production et considérées comme stables.

Pour lancer une tâche de mise à jour permettant de télécharger tous les composants les plus récents pour ESET Remote Administrator, cliquez sur **Mettre à jour maintenant**. Les mises à jour pouvant contenir des fonctionnalités ou des composants essentiels, il est primordial de s'assurer qu'elles s'effectuent correctement et automatiquement. Si vous rencontrez des problèmes de mise à jour, sélectionnez **Vider le cache de mise à jour** pour vider le dossier des fichiers temporaires de mise à jour. L'option **Créer le miroir du PCU téléchargé** est activée lorsque la mise à niveau d'un PCU (*PCU - Mise à niveau d'un composant du programme*) est téléchargée et doit être confirmée manuellement. Cliquez sur ce bouton pour voir toutes les mises à jour de PCU disponibles et le CLUF. Pour configurer la création du miroir du PCU, ouvrez le menu **Paramètres avancés** > **Modifier les paramètres avancés** et configurez les paramètres dans **ESET Remote Administrator** > **ERA Server** > **Configuration** > **Miroir**.
La configuration d'un miroir dans le serveur ESET Remote Administrator Server est la même que dans les versions ESET NOD32 Antivirus Business Edition et ESET Smart Security Business Edition. Voici la description des éléments de miroir importants :

- **Créer un miroir de mise à jour** : active la fonctionnalité de miroir. Si cette option est désactivée, aucune copie de mise à jour n'est créée.
- **Créer un miroir pour les composants du programme sélectionnés** : permet à l'utilisateur de spécifier des variantes linguistiques et les types de composants du programme qui seront créés dans le miroir.
- **Ajouter au miroir les mises à jour des composants de programme sélectionnées uniquement sur demande** : quand cette option est activée, la création de miroir des PCU n'est pas automatique. Pour activer la création d'un miroir de PCU, sélectionnez l'option **Créer le miroir du PCU téléchargé** dans **Outils** > **Options du serveur** > **Mises à jour**
- **Dossier du miroir** : répertoire local ou réseau dédié au stockage des fichiers de mise à jour.
- **Activer la distribution de mise à jour via HTTP** : permet d'accéder aux mises à jour via un serveur HTTP interne.

- **Port du serveur HTTP** : définit le port sur lequel le serveur ESET Remote Administrator Server fournit des services de mise à jour.
- **Authentification du serveur HTTP** : définit la méthode d'authentification utilisée pour accéder aux fichiers de mise à jour. Les options disponibles sont les suivantes : **AUCUNE**, **De base**, **NTLM**. Sélectionnez **Basic** pour utiliser le codage base64 avec l'authentification de base. L'option **NTLM** fournit un codage utilisant une méthode fiable. Les utilisateurs créés sur la station de travail partageant les fichiers de mise à jour sont utilisés pour l'authentification.

Cliquez sur **Par défaut** dans la section inférieure pour restaurer les valeurs prédéfinies pour toutes les fonctionnalités de cette fenêtre.

REMARQUE : en cas d'utilisation de la méthode du serveur HTTP, le maximum de clients recommandés pour la mise à jour depuis un miroir est de 400. Dans les grands réseaux comptant plus de clients, il est conseillé de répartir les miroirs de mise à jour entre les serveurs miroir ERA (ou ESS/EAV). Si le miroir doit être centralisé sur un seul serveur, il est conseillé d'utiliser un autre type de serveur HTTP, comme Apache. ERA prend également en charge des méthodes d'authentification supplémentaires (p. ex., Apache Web Server utilise la méthode .htaccess).

L'administrateur doit insérer la clé de licence de produit pour un produit acheté et saisir le nom d'utilisateur et le mot de passe permettant d'activer la fonctionnalité Miroir dans ERAS. Si l'administrateur utilise une clé de licence, le nom d'utilisateur et le mot de passe pour ESET NOD32 Antivirus Business Edition, puis réalise ensuite la mise à niveau vers ESET Smart Security Business Edition, la clé de licence d'origine, le nom d'utilisateur et le mot de passe devront également être remplacés.

REMARQUE : les clients ESET NOD32 Antivirus peuvent également être actualisés à l'aide d'une licence ESET Smart Security, mais pas l'inverse.

6.6.1 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 clients. Cette configuration signifie qu'il est important que le serveur Miroir soit toujours connecté à Internet.

Avertissement : un serveur Miroir qui a effectué une mise à niveau de composants du 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 de la distribuer à des stations de travail client. NE DÉFINISSEZ PAS DE MISES À JOUR AUTOMATIQUES DES COMPOSANTS DU PROGRAMME POUR LES PRODUITS SERVEUR ESET !

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 version Business Edition ait été activée par une clé de licence).
- Le Miroir est également disponible dans ESET Endpoint Security et ESET Endpoint Antivirus. Consultez la documentation relative au produit client concerné pour en savoir plus.

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 saisir le nom d'utilisateur et le mot de passe permettant d'activer la fonctionnalité Miroir dans ERAS. Si l'administrateur utilise une clé de licence, le nom d'utilisateur et le mot de passe pour ESET NOD32 Antivirus Business Edition, puis réalise ensuite la mise à niveau à ESET Smart Security Business Edition, la clé de licence d'origine, le nom d'utilisateur et le mot de passe devront également être remplacés.

REMARQUE : les clients ESET NOD32 Antivirus peuvent également être actualisés à l'aide d'une licence ESET Smart Security, mais pas l'inverse. Cela s'applique aussi à ESET Endpoint Antivirus et à ESET Endpoint Security.

6.6.1.1 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 d'un 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.

REMARQUE : en cas d'utilisation de la méthode du serveur HTTP, le maximum de clients recommandé pour la mise à jour depuis un miroir est de 400. Dans les grands réseaux comptant plus de clients, il est conseillé de répartir les miroirs de mise à jour entre les serveurs miroir ERA (ou ESS/EAV). Si le miroir doit être centralisé sur un seul serveur, il est conseillé d'utiliser un autre type de serveur HTTP, comme Apache. 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 de saisir, 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, saisissez les données d'authentification sous leur forme complète : *WORKGROUP\User* ou *DOMAIN\User*.

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*).

6.6.1.2 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 des composants du programme sont également disponibles. Les mises à niveau des composants du 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 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 version la plus récente du programme pour avoir accès à ses nouvelles fonctionnalités.

Par défaut, les composants du programme ne sont pas téléchargés automatiquement et doivent être configurés manuellement dans ERAS. Pour plus d'informations, consultez le chapitre Activation et configuration du Miroir 105.

6.6.1.3 Activation et configuration du Miroir

Si le miroir est directement intégré dans ERA, connectez-vous à ERAS à l'aide d'ERAC, puis procédez comme suit :

- Dans la 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, saisissez un nom d'utilisateur de domaine et un mot de passe valides pour ce serveur.
- Choisissez l'option **Créer un miroir de mise à jour**, puis saisissez le chemin d'accès du dossier qui contiendra les fichiers de mise à jour. Par défaut, il s'agit d'un chemin relatif vers le dossier du miroir. Lorsque l'option **Fournir les fichiers de mise à jour via un serveur HTTP interne** est sélectionnée, les mises à jour sont disponibles sur le port HTTP défini dans le **Port du serveur HTTP)** (par défaut 2221). Définissez l'**Authentification** sur **AUCUNE** (pour de plus amples informations, consultez le chapitre Utilisation du serveur Miroir 104).

REMARQUE : en cas de problème de mise à jour, activez l'option **Vider le cache de mise à jour** pour vider le dossier contenant les fichiers temporaires de mise à jour.

- L'option **Créer le miroir du PCU téléchargé** permet d'activer la création de miroir de composants du programme. Pour configurer la création du miroir du PCU, ouvrez le menu **Paramètres avancés > Modifier les paramètres avancés** et configurez les paramètres dans **ESET Remote Administrator** > **ERA Server** > **Configuration > Miroir**.
- Sélectionnez les composants linguistiques à télécharger dans **Paramètres avancés** > **Modifier les paramètres avancés...** la branche **ERA Server** > **Configuration** > **Miroir** > **Créer un miroir pour les composants du programme sélectionnés**. 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.

La fonctionnalité du miroir est également disponible directement depuis l'interface du programme dans ESET Smart Security Business Edition et ESET NOD32 Antivirus Business Edition, ESET Endpoint Security ou ESET Endpoint Antivirus. Il appartient à l'administrateur de choisir la méthode utilisée pour implémenter le serveur Miroir.

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

1) Installez ESET Smart Security Business Edition, ESET NOD32 Antivirus Business Edition (client version 4.X), ESET Endpoint Security ou ESET Endpoint Antivirus.

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.

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

4) Cochez les cases des options **Créer un miroir de mise à jour** et **Fournir les fichiers de mise à jour via un serveur HTTP interne**.

5) Saisissez 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 **AUCUNE**.

8) Sélectionnez les composants à télécharger (c.-à-d. les composants pour toutes les versions linguistiques qui seront utilisées dans le réseau). Les composants ne s'affichent que s'ils sont disponibles sur les serveurs de mise à jour d'ESET.

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 le miroir est utilisé en tant que partie d'ERA, cette option peut être configurée dans ERAC via **Outils** > **Options du serveur...** > onglet **Paramètres avancés** > **Modifier les paramètres avancés...** > **ESET Remote Administrator** > **ERA Server** > **Configuration** > **Miroir**. Activez toutes les versions linguistiques du

programme présentes dans votre réseau.

REMARQUE :: Pour configurer le miroir afin qu'il utilise le protocole HTTPS pour les mises à jour du client, accédez à **ERAC** > **Outils** > **Options du serveur...** > onglet **Paramètres avancés** > **Modifier les paramètres avancés...** > **ESET Remote Administrator** > **ERA Server** > **Configuration** > **Miroir** > **Protocole** > **HTTPS**.

6.7 Autres paramètres

L'onglet **Autres paramètres** permet de configurer l'adresse de serveur **SMTP** à utiliser lors de l'envoi de packages d'installation par email ainsi que l'adresse email d'administrateur à utiliser dans l'email envoyé par l'administrateur. Si le serveur requiert une authentification, indiquez le nom d'utilisateur et le mot de passe appropriés.

Remarque : Vous pouvez sécuriser les connexions en sélectionnant un protocole de sécurité dans le menu déroulant **Connexion sécurisée**. Les options disponibles sont **TLS**, **SSL** et **Auto** ; cette dernière option sélectionne le protocole disponible automatiquement.

Nouveaux clients

- **Autoriser les nouveaux clients** : lorsque cette option est sélectionnée, les nouveaux clients sont ajoutés automatiquement à la liste de clients lors de leur première connexion au serveur ERA Server. Les clients importés par réplication à partir d'autres serveurs ERA sont automatiquement ajoutés à la liste de clients durant la réplication.
- **Redéfinir automatiquement le drapeau « Nouveau » par les nouveaux clients** : lorsque cette option est sélectionnée, les nouveaux clients ne sont pas automatiquement marqués comme tels lors de leur première connexion à ERAS. Pour plus d'informations, consultez la description de l'onglet **Clients**.

Ports : permet de personnaliser des ports.

- **Console** : port que la console ERA Console utilise pour se connecter au serveur ERA Server (2223 par défaut).
- **Client** : port que le client ESET utilise pour se connecter au serveur ERA Server (2222 par défaut).
- **Port de réplication de ce serveur** : port qu'ERA utilise pour la réplication sur un serveur ERA Server de niveau supérieur (2846 par défaut).
- **Programme d'installation à distance d'ESET (Agent)** : port qu'un agent d'installation utilise pour une installation à distance (Programme d'installation à distance d'ESET, par défaut 2224)
- **Serveur Web** : port utilisé pour la connexion au serveur Web (2225 par défaut).

REMARQUE : pour que les modifications de la configuration du port prennent effet, vous devez redémarrer le service ERA Server NOD32.

ESET Live Grid

- **Collection** : ERAS transfère les fichiers suspects et les informations statistiques des clients aux serveurs d'ESET dans l'intervalle de temps défini. Dans certains cas, il est impossible de recueillir ces informations directement à partir des clients.

Tableaux de bord

- **Configurer la liste des serveurs Web...** : cliquez ici pour accéder à la liste des serveurs Web de tableau de bord 41.

6.8 Paramètres avancés

L'onglet **Paramètres avancés** de la fenêtre **Options du serveur** permet d'accéder aux paramètres avancés du serveur et de les modifier via l'Éditeur de configuration d'ESET. Pour ouvrir Éditeur de configuration, cliquez sur le bouton **Modifier les paramètres avancés...** sur cet onglet. Lisez le message d'avertissement et soyez prudent.

Les paramètres avancés sont les suivants :

- **Utilisation d'espace disque maximale (pour cent)** : en cas de dépassement, certaines fonctionnalités du serveur risquent d'être indisponibles. Lorsqu'il se connecte à ERAS, ERAC affiche une notification en cas de dépassement de la limite.
- **Codage du protocole de communication préféré** : 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) vers 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 client. 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) vers 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 client. 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'adresse MAC. 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 pendant 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. Console à ligne de commande ERA

La console à ligne de commande ERA est un outil qui vous permet d'exécuter des tâches et de gérer des clients directement depuis la ligne de commande, soit en démarrant l'outil de console à ligne de commande ERA depuis le dossier dans lequel se trouve la console ERA, soit en saisissant *eracmd.exe* dans l'invite de commande.

Lorsque vous démarrez la console à ligne de commande ERA, vous êtes invité à envoyer les informations d'identification de connexion. Si ces paramètres ne sont pas définis, les valeurs par défaut sont utilisées.

Remarque: la console à ligne de commande ERA prend en charge la fonction de réalisation automatique. Commencez à saisir une commande dans la console et appuyez sur la touche TAB pour terminer la commande. Le fait d'appuyer plusieurs fois sur la touche TAB permet de parcourir toutes les options disponibles. Le fait d'appuyer sur les touches fléchées HAUT/BAS permet de parcourir l'historique des commandes saisies. Le fait d'appuyer sur la touche ÉCHAP permet de revenir au texte précédent et deux pressions consécutives sur cette même touche effacent complètement le texte.

Syntaxe de la ligne de commande :

eracmd.exe --paramètres_de_connexion [arguments de commande [-drapeaux_de_commande]] [;arguments de commande -drapeaux_de_commande]

Exemple :

eracmd.exe --s 127.0.0.1 version server -format csv

Une fois démarrée, la console à ligne de commande ERA essaie automatiquement de se connecter au serveur. Si la connexion est établie, eracmd démarre le traitement des commandes. Si aucune commande n'est spécifiée, eracmd démarre en mode shell, dans lequel l'utilisateur peut écrire des commandes et afficher le résultat directement. Pour afficher la liste des commandes disponibles, utilisez la commande HELP COMMANDS.

Syntaxe du mode shell :

[arguments de commande [-drapeaux_de_commande]] [;arguments de commande -drapeaux_de_commande]

Pour les arguments comportant des espaces, utilisez des guillemets pour intégrer tous les mots en un même argument. Pour ajouter des guillemets à l'intérieur d'un argument de ce type, utilisez des guillemets doubles. Par exemple, "Dites ""bonjour"" s'il vous plaît" est interprété comme 'Dites "bonjour" s'il vous plaît'.

Deux mots reliés entre eux (l'un d'eux étant entre guillemets) sont connectés. Par exemple, "Dites "bonjour est interprété comme 'Dites bonjour'.

Les commandes eracmd et les mots-clés ne font pas la différence entre les majuscules et les minuscules. Seuls les arguments utilisés pour interroger la base de données peuvent faire la différence entre les majuscules et les minuscules.

@-replacing :

toute partie d'une commande peut être exécutée depuis un fichier. Le chemin du fichier doit être placé entre symboles @. Si cette syntaxe est utilisée, le contenu du fichier spécifié est utilisé à la place. Si le fichier contient plusieurs lignes, ces lignes sont reliées entre elles par des virgules et sont utilisées comme une même ligne. De cette manière, il est possible d'enregistrer la liste des arguments de fichier qui sera utilisée dans la commande suivante. Les lignes vides sont ignorées. Pour supprimer cette fonctionnalité, le symbole @ doit être placé entre guillemets.

Exemples :

Le fichier *myconnection.txt* contient le texte '*--s 192.168.0.1*' et la commande

eracmd.exe @myconnection@ affiche l'ID des clients dont le nom *-like "*@*"*

est utilisé comme suit : *eracmd.exe --s 192.168.0.1 show clients id where name -like *@**

Cet exemple crée une tâche de configuration pour les clients dont le nom contient le terme 'portable' :

show client id where client_name -like *Notebook* -out notebookID.txt -format csv -header none

task config c:\task_config_01.xml @notebookID.txt@

Commandes[111] :

Saisissez HELP COMMANDS dans le terminal pour afficher la liste des commandes disponibles, puis HELP <commande> pour afficher les instructions propres à une commande spécifique. Les commandes peuvent avoir des paramètres

obligatoires et des paramètres facultatifs que vous pouvez indiquer à l'aide d'un mot-clé. Les paramètres facultatifs appelés par un mot-clé peuvent être utilisés dans n'importe quel ordre, après les paramètres obligatoires. Une commande démarre immédiatement après les paramètres de connexion ; aucun préfixe n'est nécessaire. Si aucune commande ne figure dans la ligne de commande, eracmd démarre en mode shell. Plusieurs commandes peuvent être indiquées sur une seule ligne. Pour les séparer, utilisez un point-virgule (;). Pour exécuter un fichier script contenant plusieurs commandes, utilisez la commande SCRIPT <nom_du_fichier_script>. Dans un fichier script, les commandes sont séparées par des sauts de ligne.

Drapeaux de commande :

Les drapeaux de commande définissent le comportement général d'une commande, par exemple un format de sortie ou une gestion d'erreur. Les drapeaux de commande doivent être ajoutés après une commande et ses arguments pour que le fonctionnement soit correct. Chaque mot-clé de drapeau est préfixé avec un tiret (-). Pour afficher la liste des drapeaux, saisissez la commande HELP FLAGS.

Commentaires :

En mode shell, les commentaires peuvent être utilisés dans des scripts ou des arguments de ligne de commande. Un commentaire commence par le caractère « # » et se poursuit jusqu'à la fin de la ligne en cours. Le séparateur de commande ne met pas fin à un commentaire. Si le caractère « # » est utilisé dans une séquence entre guillemets, il ne commence pas un commentaire et est plutôt utilisé en tant que partie standard du texte entre guillemets.

Mode shell :

En mode shell, appuyez sur la touche TAB pour activer la réalisation automatique contextuelle. Utilisez la commande HISTORY pour activer, désactiver ou supprimer l'historique des commandes. Pour choisir une commande dans l'historique, utilisez les touches fléchées HAUT et BAS. Pour annuler les modifications effectuées par l'intermédiaire de la touche TAB ou des touches fléchées HAUT/BAS, appuyez sur ÉCHAP.

Script de démarrage :

Le script de démarrage est un fichier dont les commandes sont exécutées automatiquement au début du mode shell.

Le fichier de script de démarrage par défaut se trouve dans ProgramData (All Users\Application Data) dans ESET\ESET Remote Administrator\Console\eracmd_startup.txt. Il est possible d'indiquer un autre chemin à l'aide de l'argument --startup eracmd.exe (par exemple, eracmd.exe --startup startup_script.txt).

Le script n'est pas exécuté en tant que sous-script distinct (comme c'est le cas de l'exécution à l'aide de la commande "script"). Il est exécuté comme si les commandes étaient saisies directement dans la console en mode shell (les drapeaux définis dans le script de démarrage à l'aide de la commande "définir" restent définis en mode shell).

La commande "définir enregistrement" peut également être utilisée pour enregistrer les valeurs actuelles des drapeaux dans le script de démarrage le cas échéant.

Si une commande de sortie est utilisée dans le script de démarrage, les commandes suivant cette commande ne sont pas exécutées, mais eracmd.exe ne quitte pas le mode shell.

Styles de formatage

Les drapeaux d'en-tête et de champ peuvent être utilisés pour indiquer des styles de formatage :

- mot-clé - les textes constants sont utilisés (adapté au post-traitement automatique)

- lisible - les textes traduisibles sont utilisés (convient à la sortie pour l'utilisateur)

Le drapeau d'en-tête a une incidence sur les en-têtes de table (noms de colonne). Le drapeau de champ a une incidence sur les valeurs des champs de table.

Paramètres de connexion

Les paramètres appartenant à la connexion au serveur ERA doivent être indiqués en tant que paramètres de ligne de commande. Eracmd.exe ne traite les commandes que si la connexion est correctement établie. Tous les paramètres de connexion utilisent le préfixe de double tiret (--).

--s serveur:port : serveur avec lequel s'établit la connexion. Valeur par défaut : localhost:2226
--u nom_utilisateur : nom d'utilisateur du serveur ERA. Si le nom d'utilisateur commence par un préfixe de domaine, il est utilisé comme nom d'utilisateur d'authentification de domaine. Cette commande ne peut pas être utilisée avec --ud ou --uc. Valeur par défaut : administrateur
--ud nom_utilisateur : nom d'utilisateur d'authentification de domaine. Cette commande ne peut pas être utilisée avec --u ou --uc.
--uc : utilise les informations d'identification de la session Windows. Cette commande ne peut pas être utilisée avec --u ou --ud.
--p mot_de_passe : mot de passe du serveur ERA ou d'authentification de domaine. Cette commande ne peut pas être utilisée avec --pa. Valeur par défaut : "" (mot de passe vide).
--pa : invite de mot de passe. Après le démarrage de la console, il est possible de saisir un mot de passe et de n'afficher que des caractères « * ». Cette commande ne peut pas être utilisée avec --p.
--aa : demande tous les paramètres de connexion. Si aucune valeur n'est spécifiée, aucun autre paramètre de connexion ne peut être indiqué.
--startup : autre chemin de script de démarrage. Le script de démarrage est exécuté automatiquement au début du mode shell.

7.1 Drapeaux de commande

Les drapeaux peuvent être utilisés pour définir certains comportements génériques des commandes ou pour spécifier la sortie de chaque commande. Pour définir la valeur par défaut de chaque drapeau, utilisez la commande SET. Les drapeaux sont ajoutés après la commande et ses arguments. La liste ci-dessous répertorie les drapeaux disponibles.

- *-format* : format de sortie. Valeurs possibles : *csv*, *table*. Valeur par défaut : *csv* (en mode ligne de commande), *table* (en mode shell).
- *-delim* : séparateur pour la sortie au format CSV. Si cette option est utilisée avec l'argument "", le séparateur système est utilisé (c'est également la valeur par défaut). Si aucun séparateur système n'est défini, le séparateur ',' est utilisé. Le point-virgule étant utilisé en tant que séparateur de commande, utilisez les guillemets pour le spécifier en tant que séparateur. Valeur par défaut : "" (séparateur système ; ',' si aucun séparateur n'est utilisé).
- *-out* : réachemine la sortie vers un fichier. Consultez également les drapeaux -mode et -enc. Si cette option est utilisée avec l'argument "", le réacheminement est désactivé (c'est également le comportement par défaut). Valeur par défaut : "" (réacheminement désactivé).
- *-mode* : mode de sortie du fichier. Valeurs possibles : o (remplace le fichier), a (ajoute à la fin du fichier). Valeur par défaut : o (remplace le fichier).
- *-enc* : Codage de la sortie dans un fichier. Valeurs possibles : *ansi*, *utf8*, *utf16*. Valeur par défaut : *utf8*.
- *-header* : type d'en-tête de table. Valeurs possibles : *mot-clé* (utilise les mots-clés comme dans les arguments de la commande SHOW, par exemple, nom_client), *lisible* (utilise des noms de colonne traduisibles et plus lisibles, par exemple Nom du client), *aucun* (l'en-tête n'est pas affiché). Valeur par défaut : *mot-clé*.
- *-paged* : sortie paginée. Si cette option est activée, l'utilisateur est invité à appuyer sur une touche après chaque page. Valeurs possibles : *vrai*, *faux*. Valeur par défaut : *faux*.
- *-tableclip* : coupe les tables pour qu'elles soient contenues dans l'écran. Cette option ne s'applique que lorsque la table est affichée dans une fenêtre de console. Valeurs possibles : *vrai*, *faux*. Valeur par défaut : *vrai*.
- *-color* : utilisez plusieurs couleurs lorsque vous affichez le contenu dans la fenêtre de console. Valeurs possibles : *vrai*, *faux*. Valeur par défaut : *vrai*.
- *-field* : style de formatage du champ de table. Valeurs possibles : *mot-clé* (utilise les mots-clés constants, par exemple terminé_avec_avertissement), *lisible* (utilise des textes traduisibles et plus lisibles, par exemple "Terminé avec avertissement"). Valeur par défaut : mot-clé.
- *-onerror* : Que faire si une erreur se produit lors de l'exécution d'une commande ? Si l'arrêt est défini, l'exécution d'une séquence de commande s'arrête immédiatement. Si la poursuite est définie, l'exécution se poursuit avec les commandes suivantes. L'intégralité de la séquence se termine avec un état d'erreur si l'une des commandes échoue. Valeurs possibles : *arrêter*, *continuer*. Valeur par défaut : *stop*.

7.2 Commandes

COMMANDE	DESCRIPTION	SYNTAXE	PARAMÈTRES	EXEMPLE
client comment	Définit le commentaire client.	client comment <client ID> <comment>	**client ID** ID du client pour lequel le commentaire sera défini. **comment** Commentaire pour le client.	client comment 1 Problematic
client new	Définit ou redéfinit le drapeau 'nouveau' pour un client sur le serveur.	client new <client ID> <action>	**client ID** Liste des ID clients séparés par des virgules pour la définition ou la redéfinition du drapeau 'nouveau'. **action** Indique si le drapeau 'nouveau' doit être défini ou redéfini. Valeurs possibles : définir, redéfinir	client new 1 reset
client rename	Renomme un client sur le serveur.	client rename <client ID> <name>	**client ID** ID du client à renommer. **name** Nouveau nom du client.	client rename 1 new_client_name
client roaming	Définit ou redéfinit le drapeau 'utilisateur itinérant' pour un client sur le serveur.	client roaming <client ID> <action>	**client ID** Liste des ID clients séparés par des virgules pour la définition ou la redéfinition du drapeau 'utilisateur itinérant'. **action** Indique si le drapeau 'utilisateur itinérant' doit être défini ou redéfini. Valeurs possibles : définir, redéfinir	client roaming 1 set
cls	Efface le résultat sur la console.	cls		cls
echo	Affiche un argument sous forme de message. Si l'argument est manquant, seule une nouvelle ligne est ajoutée au résultat.	echo [<message>]	**message** Message à afficher. Peut contenir plusieurs valeurs concaténées.	echo "hello world" echo "Report created with id: ",@reportId.csv@ echo

encrypt	Chiffre le mot de passe pour qu'il soit utilisé dans la configuration. Deux types de chiffrement sont utilisés : 'serveur', utilisé pour les mots de passe définis par le serveur ERA (réplication, client, programme d'installation, utilisateurs) et 'autre', utilisé pour les mots de passe définis par d'autres services (SMTP, mise à jour, etc.). En conséquence, cette commande affiche le mot de passe chiffré qui peut être utilisé pour la création des fichiers de configuration. Si aucun mot de passe n'est spécifié, l'utilisateur est invité à saisir les mots de passe. Les caractères apparaissent dans le champ de mot de passe sous forme d'astérisques.	encrypt <encryptionType> [<password>]	**encryptionType** Type de chiffrement. Valeurs possibles : serveur, autre **password** Mot de passe à chiffrer.	encrypt server MyReplicationPassword6578
errmsg	Affiche le message d'erreur d'un code d'erreur.	errmsg <code>	**code** Code d'erreur permettant de rechercher un message d'erreur.	errmsg 2001
exit	Met fin à la console à ligne de commande si elle est utilisée en mode shell. Arrête l'exécution du fichier de script actuel s'il est utilisé dans un fichier script.	exit		

getdata	Obtient l'ensemble spécifié d'informations depuis un client en particulier ou concernant une stratégie spécifique pour un fichier local. Certaines informations risquent de ne pas être disponibles sur le serveur. Pour actualiser ces informations, utilisez la commande REQUEST. Les informations concernant la configuration, les fonctionnalités de protection, l'état de la protection et le système sont actualisées automatiquement pour les clients sur le serveur principal.	getdata <data type> <data ID> <file>	**data type** Type des données à obtenir. Valeurs possibles : Client : sysinspector (journal SysInspector), configuration (configuration XML), état_protection (état de protection), fonctionnalités_protection (fonctionnalités de protection), informations_système (informations système) ; Stratégie : policy (stratégie XML, uniquement pour les stratégies qui ne sont pas répliquées depuis un serveur supérieur), policy_merged (stratégie XML fusionnée, créée en résultat d'un héritage par l'application de paramètres d'une stratégie supérieure), policy_override (partie ignorée de la stratégie XML, uniquement pour les stratégies répliquées depuis un serveur supérieur), policy_nonoverride (partie non ignorée de la stratégie XML) **data ID** ID de l'entité de données (client ou stratégie) à partir de laquelle les données sont téléchargées. **file** Chemin de destination du fichier local.	getdata configuration 1 c:\file.xml
group	Affiche les groupes définis et les informations sur le groupe.	group [<tree>]	**tree** Utilise le mode arborescence pour afficher les groupes avec héritage de groupe.	group
help	Affiche les informations concernant l'utilisation de la console à ligne de commande ERA. Utilisez l'argument pour sélectionner une aide plus spécialisée.	help [<command 1>] [<command 2>]	**command 1** Permet d'afficher l'aide correspondant à la commande (premier mot du nom de la commande). Valeurs possibles : <nom de la commande>, drapeaux, commandes **command 2** Permet	help version help commands help help

			d'afficher l'aide correspondant à la commande (deuxième mot du nom de la commande).	
history	Active ou désactive l'enregistrement permanent de l'historique des commandes en mode shell une fois la console fermée. Par défaut, cette commande est désactivée.	history [<action>]	**action** Si cette commande est omise, l'état actuel de l'historique d'enregistrement après la fin de la console s'affiche. Valeurs possibles : vrai (activer), faux (désactiver), effacer (effacer l'historique de commande), liste (affiche le contenu actuel de l'historique enregistré)	history true
license	Affiche les informations de licence du serveur.	license		license
license add	Télécharge le ou les fichiers de clés de licence spécifiés sur le serveur ERA.	license add <filename>	**filename** Liste des chemins des fichiers de clés de licence à télécharger, séparés par des virgules.	license add c:\era.lic
license details	Affiche les informations sur les clés de licence partielles chargées par le serveur ERA.	license details		license details
license replace	Télécharge un ou plusieurs fichiers de clés de licence sur le serveur ERA et remplace tous les anciens fichiers de licence par la ou les clés de licence téléchargées.	license replace <filename>	**filename** Liste des chemins des fichiers de clés de licence servant au remplacement, séparés par des virgules.	license replace c:\era.lic

logforward	Affiche ou définit les paramètres actuels de transfert de journal. Cette commande s'utilise de deux manières : 1. Pour afficher l'état d'un paramètre particulier de transfert de journal, utilisez le premier paramètre <type> ou la commande sans aucun paramètre afin d'afficher les paramètres actuels de transfert de journal pour tous les journaux. 2. Pour la définition des paramètres de transfert de journal, les paramètres <type> et <activer> sont obligatoires. Les autres paramètres ([level <niveau>], [severity <gravité>] et [facility <fonctionnalité>]) sont facultatifs. Si un paramètre facultatif est omis, la valeur n'est pas modifiée.	logforward [<type>] [<enable>] [level <level>] [severity <severity>] [facility <facility>]	**type** Type de journal à afficher ou à mettre à jour. Valeurs possibles : événement, menace, pare-feu, HIPS, antispam, liste grise, analyse, mobile, contrôle_périphérique, contrôle_web **enable** Détermine si le transfert doit être activé ou désactivé. Valeurs possibles : vrai, faux **level** Niveau du journal à traiter par transfert de journal. Valeurs possibles : critique, avertissement, normal, diagnostics **severity** Valeur de gravité SysLog. Valeurs possibles : informations, erreur, avertissement, débogage **facility** Valeur de fonctionnalité SysLog. Valeurs possibles : 0 à 23	logforward logforward scan logforward eventlog true level warning logforward threat false
password	Change le mot de passe de sécurité du serveur ERA. En cas d'absence de mot de passe, utilisez "". Si l'ancien ou le nouveau mot de passe n'est pas indiqué, l'utilisateur est invité à saisir les mots de passe. Les mots de passe saisis s'affichent sous forme d'astérisques. Cette commande ne peut pas définir de mots de passe faisant partie d'une configuration serveur. Pour ce type de mot de passe, utilisez la commande SERVERCFG SET ou SERVERCFG SETPWD.	password <passwordType> [<oldPassword> <newPassword>]	**passwordType** Type de mot de passe à définir. Valeurs possibles : réplication, client, programme_installation, utilisateur_actuel **oldPassword** Ancien mot de passe. Il est possible d'utiliser un mot de passe d'administrateur du serveur ERA. **newPassword** Nouveau mot de passe.	password currentuser password replication oldPass1 newPass2

path	Affiche ou définit le répertoire de travail actuel en tant que base de tous les chemins relatifs (lors de la spécification d'un chemin de script ou de chemins de fichiers de données).	path [<action>] [<path>]	**action** Action. Valeurs possibles : obtenir (affiche le répertoire de travail actuel), définir (définit le chemin spécifié en tant qu'argument suivant), script (définit le chemin du script en cours). Valeur par défaut : obtenir **path** Nouveau répertoire de travail. Si le chemin est relatif, il est relatif par rapport au répertoire de travail précédent.	path path set d:\scripts path script
policy	Affiche les stratégies définies avec les informations sur la stratégie. Si l'argument 'arborescence' est présent, afficher une arborescence des stratégies.	policy [<tree>]	**tree** Utilise le mode arborescence pour afficher les stratégies avec héritage de stratégie.	policy policy tree
policy assign	Affecte la stratégie spécifiée aux clients indiqués. Notez qu'il n'est pas possible d'affecter une stratégie à un client. Si la liste des clients contient des clients répliqués, la stratégie doit être réplicable vers le bas. La stratégie des serveurs de niveau inférieur ne peut pas être affectée.	policy assign <policy id> <clients>	**policy id** Stratégie affectée. Valeurs possibles : <ID de stratégie>, ! DefaultClientsPolicy **clients** Liste des ID client, séparés par des virgules (ou * pour tous les clients).	policy assign 10 1,2,5,9 policy assign ! DefaultClientsPolicy *

policy create	Crée une stratégie avec les paramètres spécifiés sur le serveur. Affiche l'ID de la nouvelle stratégie si elle est créée correctement.	policy create <name> <config XML> [parentID <parent ID>] [description <description>] [overrideAnyChild <override any child>] [downReplicable <down replicable>] [defaultForClients <default for clients>] [defaultForLowerServers <default for lower servers>]	**name** Nom de la nouvelle stratégie. **config XML** Fichier XML avec la configuration de la nouvelle stratégie. **parent ID** ID du parent de la nouvelle stratégie. **description** Description de la nouvelle stratégie. **override any child** Définit le drapeau 'Remplacer toute stratégie enfant' pour la nouvelle stratégie. Valeurs possibles : vrai, faux. Valeur par défaut : faux **down replicable** Définit le drapeau 'Abaisser une stratégie réplicable' pour la nouvelle stratégie. Valeurs possibles : vrai, faux. Valeur par défaut : faux **default for clients** Définit la stratégie comme étant la stratégie par défaut pour les clients. Valeurs possibles : vrai, faux. Valeur par défaut : faux **default for lower servers** Définit la stratégie comme étant la stratégie par défaut pour les serveurs de niveau inférieur. Valeurs possibles : vrai, faux. Valeur par défaut : faux	policy create new_policy policy.xml

policy delete	Supprime une stratégie et vous permet de définir des remplacements pour la stratégie supprimée. Les remplacements non nécessaires sont ignorés.	policy delete <policy id> [child_policies <child policies parent replacement>] [primary_clients <primary clients policy replacement>] [replicated_clients <replicated clients policy replacement>] [primary_clients_default <primary clients default policy replacement>] [lower_servers_default <lower servers default policy replacement>] [whole_branch <delete whole branch>]	**policy id** ID de la stratégie à supprimer. **child policies parent replacement** Nouvelle stratégie parent pour les stratégies enfant de la stratégie supprimée. Valeurs possibles : <ID de stratégie>, !DefaultUpperServerPolicy, !NotAvailable **primary clients policy replacement** Nouvelle stratégie pour les clients principaux dont la stratégie a été supprimée. Valeurs possibles : <ID de stratégie>, !DefaultClientsPolicy **replicated clients policy replacement** ID de la nouvelle stratégie pour les clients répliqués dont la stratégie a été supprimée. **primary clients default policy** ID de remplacement de la nouvelle stratégie par défaut pour les clients principaux. **lower servers default policy** Nouvelle stratégie par défaut pour les serveurs de niveau inférieur. Valeurs possibles : <ID de stratégie>, !NotAvailable **delete whole branch** Si la branche doit être supprimée dans son intégralité (la stratégie indiquée, y compris les stratégies enfant). Valeurs possibles : vrai, faux. Valeur par défaut : faux	policy delete 2 primary_clients 4
rule	Affiche les règles de stratégie.	rule		rule

rule create	Crée une nouvelle règle de stratégie.	rule create <xml> <nom> <ID de stratégie> [desc <description>] [priority <priorité>] [enabled <activé>]	**xml** Fichier XML source créé par l'exportation de la règle existante. **nom** Nom de la règle de stratégie. **ID de stratégie** ID de la stratégie associée. Seuls les types suivants peuvent être utilisés : stratégie de client par défaut, stratégies locales, stratégies réplicables vers le bas depuis un serveur de niveau supérieur. Valeurs possibles : ! DefaultClientsPolicy **description** Description de la règle de stratégie. **priorité** Priorité de la règle de stratégie. Valeurs possibles : haut, bas. Valeur par défaut : bas **activer** État initial de la règle de stratégie créée. Valeurs possibles : vrai, faux. Valeur par défaut : vrai	rule create "c:\my data\exportedPolicy.xml" myNewPolicy 3 desc "New policy rule" priority top enabled false
rule delete	Supprime une règle de stratégie.	rule delete <ID de règle de stratégie>	**ID de règle de stratégie** ID de la règle de stratégie à supprimer.	rule delete 3
rule import	Importe les règles de stratégie à partir d'un fichier XML. Les règles déjà définies ne sont pas modifiées. Si un nom de règle existe déjà, la nouvelle règle (importée) est renommée.	rule import <chemin du fichier>	**chemin du fichier** Chemin du fichier XML d'où sont importées les règles.	rule import d:\rule.xml
rule export	Exporte les règles de stratégie dans un fichier XML.	rule import <règles> <chemin du fichier>	**règles** Liste des règles, séparées par des virgules (ou * pour toutes les règles). **chemin du fichier** Chemin du fichier XML vers lequel sont importées les règles.	rule export 1,2 d:\rule.xml

rule update	Change les paramètres ou la configuration d'une règle de stratégie. Les paramètres non spécifiés ne sont pas modifiés.	rule update <ID de règle de stratégie> [xml <config xml>] [desc <description>] [policy <ID de stratégie>] [priority <priorité>] [enabled <activé>]	**ID de règle de stratégie** ID de la règle de stratégie à mettre à jour. **config xml** Fichier XML de configuration créé par l'exportation de la règle existante. **description** Nouvelle description de la règle de stratégie. **ID de stratégie** ID de la nouvelle stratégie associée. Valeurs possibles : ! DefaultClientsPolicy **priorité** Changement de priorité de la règle de stratégie. Valeurs possibles : niveau supérieur, niveau inférieur, haut, bas **activer** Nouvel état de la règle de stratégie. Valeurs possibles : vrai, faux	rule update 2 xml d:\rule.xml enabled true

policy update	Met à jour une configuration de stratégie avec les paramètres spécifiés.	policy update <ID> [name <name>] [parentID <parent ID>] [configXML <config XML>] [description <description>] [overrideAnyChild <override any child>] [downReplicable <down replicable>] [defaultForClients <default for clients>] [defaultForLowerServers <default for lower servers>] [replicated_clients <replicated clients policy replacement>] [lower_servers_default <lower servers default policy replacement>] [primary_clients_default <primary clients default policy replacement>]	**ID** ID de la stratégie mise à jour. **name** Nouveau nom de la stratégie mise à jour. **parent ID** Nouvel ID du parent de la stratégie mise à jour. Valeurs possibles : <ID de stratégie>, !NoPolicy (la stratégie mise à jour n'a pas de parent) **config XML** Fichier XML avec la nouvelle configuration de la stratégie mise à jour. **description** Nouvelle description de la stratégie mise à jour. **override any child** Nouvelle valeur du drapeau 'Remplacer toute stratégie enfant' pour la stratégie mise à jour. Valeurs possibles : vrai, faux **down replicable** Nouvelle valeur du drapeau 'Abaisser une stratégie réplicable' pour la stratégie mise à jour. Valeurs possibles : vrai, faux **default for clients** Définit la stratégie comme étant la stratégie par défaut pour les clients. Valeurs possibles : vrai, faux **default for lower servers** Définit la stratégie comme étant la stratégie par défaut pour les serveurs de niveau inférieur. Valeurs possibles : vrai, faux **replicated clients policy replacement** Nouvelle stratégie pour les clients répliqués dont la stratégie a été mise à jour. Valeurs possibles : <ID de stratégie>, !DefaultClientsPolicy, !NotAvailable	policy update 123 name policy1 parentID 1 configXML policy.xml overrideAnyChild TRUE defaultForLowerServers FALSE

			lower servers default policy replacement Nouvelle stratégie par défaut pour les serveurs de niveau inférieur. Valeurs possibles : <ID de stratégie>, ! DefaultClientsPolicy, ! NotAvailable **primary clients default policy replacement** ID de la nouvelle stratégie par défaut pour les clients principaux.	
report	Affiche les modèles de rapport statique ou de tableau de bord, ou encore les rapports générés. Dans le cas des rapports générés, seuls les rapports situés sur le serveur sont affichés.	report <type>	**type** Type de rapport. Valeurs possibles : statique, tableau de bord, généré	report static
request	Demande la version en cours des différentes données à transférer d'un client vers le serveur ERA. Il est possible de demander des informations sur SysInspector, sur la configuration, l'état de la protection, les fonctionnalités de protection et les informations système. Les données demandées sont reçues dès que le client se connecte au serveur principal et que les données sont disponibles. Sur les clients répliqués, la demande doit d'abord être répliquée. Les informations concernant la configuration, les fonctionnalités de protection, l'état de la protection et le système sont actualisées automatiquement pour les clients sur le serveur principal.	request <data type> <clients> [si_compare <compare date>] [<si_snapshot>]	**data type** Liste des types de données à demander, séparés par des virgules. Valeurs possibles : sysinspector, configuration, état_protection, fonctionnalités_protection, informations_système **clients** Liste des ID client, séparés par des virgules (ou * pour tous les clients). **compare date** Si cet argument est utilisé, compare le journal demandé à un journal précédent en fonction de sa date et de son heure UTC, au format AAAA-MM-JJ hh:mm:ss (par exemple "2014-01-21 10:43:00"). Utilisé uniquement lors de la demande d'informations sur SysInspector. **si_snapshot** Enregistre le journal localement sur le poste de travail du client. Utilisé uniquement lors de la demande d'informations sur SysInspector.	request protection_features * request sysinspector,config 1,2,8 si_compare "2014-01-01 01:02:03" si_snapshot

scanlog	Affiche le contenu du journal d'analyse spécifié.	scanlog <id>	**id** ID d'un journal d'analyse demandé.	scanlog 1
script	Exécute un lot de commande dans un fichier externe.	script <filename>	**filename** Chemin vers le fichier contenant des commandes. Les commandes peuvent être séparées par une ligne ou un point-virgule.	script c:\eraGetClientsInfo.txt
servercfg get	Télécharge la configuration serveur actuelle dans le fichier local spécifié.	servercfg get <filename>	**filename** Chemin du fichier local dans lequel enregistrer la configuration téléchargée.	servercfg get d:\era_config.xml
servercfg list	Affiche les paramètres de configuration disponibles qui peuvent être modifiés directement par les commandes SERVERCFG SET et SERVERCFG SETPWD.	servercfg list		servercfg list
servercfg put	Télécharge la configuration serveur depuis un fichier XML local.	servercfg put <filename>	**filename** Chemin du fichier XML local à télécharger.	servercfg put d: ew_config.xml
servercfg set	Affecte une valeur à un paramètre de configuration particulier. Utilisez la commande HELP SERVERCFG LIST pour afficher tous les paramètres disponibles.	servercfg set <name=value>	**name=value** Nom du paramètre et valeur à assigner.	servercfg set port_con=2223 servercfg set mirror_enabled=1
servercfg setpwd	Affecte une valeur à un paramètre de configuration particulier par l'intermédiaire d'une invite de mot de passe. Les valeurs saisies s'affichent sous forme d'astérisques, ce qui est très utile pour la saisie des mots de passe. Utilisez la commande HELP SERVERCFG LIST pour afficher tous les paramètres disponibles. Cette commande ne peut pas définir les mots de passe de sécurité serveur. Utilisez pour cette définition la commande PASSWORD.	servercfg setpwd <name>	**name** Nom du paramètre à définir.	servercfg setpwd ps_password_smtp

set	Permet d'obtenir, de définir ou d'enregistrer les valeurs des drapeaux. Les drapeaux permettent de spécifier le résultat d'une commande et d'autres paramètres communs. Pour afficher la liste des drapeaux disponibles, utilisez la commande HELP FLAGS. La définition d'un drapeau est effective pour toutes les commandes suivantes du fichier de script actuel ou pour toutes les commandes suivantes en mode shell (s'il est utilisé directement dans ce mode). Le drapeau peut être remplacé pour une seule commande par l'indication d'un drapeau de commande après la commande.	set [<flag name>] [<flag value>]	**flag name** Utilisez le nom d'un drapeau sans le tiret initial. Utilisez la commande HELP FLAGS pour afficher la liste des drapeaux disponibles. Si aucune information n'est spécifiée, les valeurs actuelles de tous les drapeaux sont affichées. L'argument "enregistrer" peut également être utilisé pour enregistrer l'état actuel des drapeaux dans le fichier de démarrage (utilisez le second argument pour indiquer un autre chemin de fichier de démarrage). **flag value** Utilisez la commande HELP FLAGS pour les valeurs disponibles. Si aucune information n'est spécifiée, la valeur actuelle du drapeau est affichée.	set set enc set enc utf8 set format table set paged true set save set save startup.txt
show	Affiche les données de la table spécifiée. Utilisez l'argument "nombre" au lieu de la liste des colonnes pour obtenir uniquement le nombre de lignes.	show <table name> <list of columns> [where <where>] [group by <group by>] [order by <order by>] [skip <skip>] [limit <limit>]	**table name** Utilisez la commande SHOW TABLES pour afficher les tables disponibles. **list of columns** Liste séparée par des virgules. Utilisez la commande SHOW COLUMNS pour afficher la liste des colonnes de la table spécifiée. Utilisez * pour toutes les colonnes. Utilisez l'argument "nombre" pour obtenir uniquement le nombre de lignes. Valeurs possibles : <nom de colonne>, *, nombre des conditions, séparées par des virgules, dans une liste au format <colonne><opérateur de comparaison><valeur> (par exemple id>3) ou <colonne> <opérateur IN> (<liste_de_valeurs_séparées_par_des_virgules>	show client * show client client_name show client id, client_name WHERE id>4, configuration -IN (ready, requested) ORDER BY client_name LIMIT 5 show client * WHERE product_name -LIKE *endpoint* show client count WHERE id>4 show client * where group_id=4 show client * where requested_policy_id -IN (2,3) show event * where client_group_id=4 show event * where client_requested_policy_id -IN (2,3)

			). Les opérateurs de comparaison suivants sont autorisés : = (ou -EQ), != (ou -NE), <= (ou -LE), >= (ou -GE), < (ou -LT), > (ou -GT). Les opérateurs IN suivants sont autorisés : -IN ou -NOTIN. Pour les colonnes de texte, -LIKE et -NOTLIKE avec une valeur de texte avec caractères génériques (* - zéro caractère ou plus, ? - exactement un caractère) peuvent être utilisés à la place d'un opérateur de comparaison. **group by** Liste des colonnes servant au regroupement, séparées par des virgules. Les lignes ayant des valeurs correspondantes dans toutes ces colonnes s'affichent sur une seule ligne. **order by** Liste des colonnes servant au tri, séparées par des virgules. Après chaque nom de colonne, les arguments -ASC (option par défaut) ou -DESC peuvent être spécifiés pour le tri croissant ou décroissant. **skip** Nombre de lignes à ignorer au début. **limit** Nombre maximum de lignes à afficher.	
show columns	Affiche les colonnes disponibles pour la table spécifiée.	show columns [for] <table name>	**table name** Table dont les colonnes doivent être affichées. Utilisez la commande SHOW TABLES pour obtenir les noms des tables disponibles.	show columns for client
show tables	Affiche les tables disponibles qui peuvent être utilisées dans la commande SHOW.	show tables		show tables
task config	Crée une tâche de configuration à l'aide d'un fichier de	task config <configuration file> <clients> [name	**configuration file** Fichier XML issu de l'éditeur de	task config d:\task_config_01.xml 1,4,5 name "Config01" description

	configuration. Affiche l'ID de la nouvelle tâche si elle est créée correctement.	<name>] [description <description>] [applyAfter <apply after>] [deleteIfCompleted <delete if completed>]	configuration. **clients** Liste des ID client, séparés par des virgules (ou * pour tous les clients). **name** Nom de la tâche. **description** Description de la tâche. **apply after** Heure UTC à laquelle la tâche doit être appliquée, dans l'un des formats suivants : AAAA-MM-JJ hh:mm:ss, AAAA-MM-JJ hh:mm, AAAA-MM-JJ hh, AAAA-MM-JJ. Par exemple (date et heure) : "2014-01-21 10:43". Exemple (date sans heure) : "2014-01-21". **delete if completed** Utilisez cet argument si la tâche doit être supprimée après sa réalisation. Valeurs possibles : vrai, faux. Valeur par défaut : faux.	"email client protection config"
task scan	Crée une tâche d'analyse. Affiche l'ID de la nouvelle tâche si elle est créée correctement.	task scan <clients> [name <name>] [description <description>] [applyAfter <apply after>] [deleteIfCompleted <delete if completed>] [exclude <exclude>] [windows_profile <profile>] [windows_targets <windows targets>] [windows_no_cleaning <no cleaning>] [windows_shutdown_after_scan <shutdown>] [windows_allow_shutdown_cancel <allow cancel>] [linux3_targets <linux3 targets>] [linux3_no_cleaning <no cleaning>] [linux_profile <profile>] [linux_targets <linux targets>] [linux_no_cleaning <no cleaning>] [mobile_targets <mobile targets>] [mobile_no_cleaning <no cleaning>]	**clients** Liste des ID client, séparés par des virgules (ou * pour tous les clients). **name** Nom de la tâche. **description** Description de la tâche. **apply after** Heure UTC à laquelle la tâche doit être appliquée, dans l'un des formats suivants : AAAA-MM-JJ hh:mm:ss, AAAA-MM-JJ hh:mm, AAAA-MM-JJ hh, AAAA-MM-JJ. Par exemple (date et heure) : "2014-01-21 10:43". Exemple (date sans heure) : "2014-01-21". **delete if completed** Utilisez cet argument si la tâche doit être supprimée après sa réalisation. Valeurs possibles : vrai, faux. Valeur par défaut : faux. **exclude** Liste des	task scan 1,3

		[max_delay <max delay>]	sections à exclure de la tâche d'analyse, séparées par des virgules. Valeurs possibles : windows, linux3, linux, mobile. **profile** Nom du profil d'analyse. Valeurs possibles : !InDepthScan, !MyProfile, !SmartScan, !ContextMenuScan, <nom de profil défini par l'utilisateur>. Valeur par défaut : !InDepthScan **windows targets** Liste des cibles Windows à analyser, séparées par des virgules. Valeurs possibles : !Memory, !RemovableDrivesBoot, !RemovableDrives, !LocalDrivesBoot, !LocalDrives, !RemoteDrives, !AllDrivesBoot, !AllDrives, <chemin personnalisé> Valeur par défaut : !Memory, !LocalDrivesBoot, !LocalDrives **no cleaning** Analyser sans nettoyer. Valeurs possibles : vrai, faux. Valeur par défaut : faux **shutdown** Arrêter l'ordinateur après l'analyse. Valeurs possibles : vrai, faux. Valeur par défaut : faux **allow cancel** Autoriser un utilisateur à annuler l'arrêt. Valeurs possibles : vrai, faux. Valeur par défaut : faux **linux3 targets** Liste des chemins Linux3 à analyser, séparés par des virgules. Valeur par défaut : / **linux targets** Liste des chemins Linux à analyser, séparés par des virgules. Valeur par défaut : /	

			mobile targets Liste des cibles mobiles à analyser, séparées par des virgules. Valeurs possibles : !All, <chemin personnalisé>. Valeur par défaut : !All **max delay** Retard aléatoire maximal en minutes.	
task update	Crée une tâche de mise à jour. Affiche l'ID de la nouvelle tâche si elle est créée correctement.	task update <clients> [name <name>] [description <description>] [applyAfter <apply after>] [deleteIfCompleted <delete if completed>] [exclude <exclude>] [windows_profile <windows profile>] [max_delay <max delay>]	**clients** Liste des ID client, séparés par des virgules (ou * pour tous les clients). **name** Nom de la tâche. **description** Description de la tâche. **apply after** Heure UTC à laquelle la tâche doit être appliquée, dans l'un des formats suivants : AAAA-MM-JJ hh:mm:ss, AAAA-MM-JJ hh:mm, AAAA-MM-JJ hh, AAAA-MM-JJ. Par exemple (date et heure) : "2014-01-21 10:43". Exemple (date sans heure) : "2014-01-21". **delete if completed** Utilisez cet argument si la tâche doit être supprimée après sa réalisation. Valeurs possibles : vrai, faux. Valeur par défaut : faux **exclude** Liste des sections à exclure de la tâche de mise à jour, séparées par des virgules. Valeurs possibles : windows, linux3, linux, mobile. **windows profile** Nom de profil de la section Windows. **max delay** Retard aléatoire maximal en minutes.	task update 2,4,6 name "Update01" exclude windows task update *
version	Affiche la version actuelle de la console à ligne de commande, de l'API et du serveur ERA.	version [<component>]	**component** Affiche la version du composant. Si aucune valeur n'est indiquée, toutes les versions sont affichées. Valeurs possibles :	version version cmd

			commande, API, serveur	

8. ERA Maintenance Tool

ESET Remote Administrator Maintenance Tool sert à exécuter des tâches spécifiques pour l'exploitation et la maintenance du serveur. Pour y accéder, cliquez sur **Démarrer** > **Programmes** > **ESET** > **ESET Remote Administrator Server** > **ESET Remote Administrator Maintenance Tool**. Quand vous lancez ERA Maintenance Tool, un Assistant s'ouvre pour vous aider à réaliser les tâches requises.

Après avoir démarré ESET Remote Administrator Maintenance Tool, cliquez sur **Suivant** ; la fenêtre d'informations ERA Server s'affiche. L'outil affiche des informations de synthèse sur le serveur ERA Server installé. Les informations affichées peuvent être consultées plus en détail dans une fenêtre séparée ; il suffit de cliquer sur **Informations supplémentaires**. Vous pouvez les copier en cliquant sur **Copier dans le Presse-papiers** et les actualiser en cliquant sur **Rafraîchir**. Après avoir vérifié les informations, passez à l'étape suivante en cliquant sur **Suivant** et sélectionnez une tâche :

À la fin de la configuration de chaque tâche, vous pouvez enregistrer les paramètres de la tâche actuelle en cliquant sur **Enregistrer tous les paramètres dans un fichier**. Ces paramètres pourront ensuite être utilisés à tout moment à l'avenir en cliquant sur **Charger tous les paramètres d'un fichier**. Pour chaque étape de configuration d'une tâche, il est également possible de choisir les options **Enregistrer tous les paramètres dans un fichier** ou **Charger tous les paramètres d'un fichier**.

8.1 Arrêter le ERA Server

Cette tâche arrête le service de ESET Remote Administrator Server.

REMARQUE :: Le service s'intitule ERA_SERVER. Le fichier exécutable de ce service est le suivant : *C:\Program Files\ESET\ESET Remote Administrator\Server\era.exe*.

8.2 Démarrer le ERA Server.

Cette tâche démarre le service de ESET Remote Administrator Server.

REMARQUE :: Le service s'intitule ERA_SERVER. Le fichier exécutable de ce service est le suivant : *C:\Program Files\ESET\ESET Remote Administrator\Server\era.exe*.

8.3 Transfert de base de données

Cette tâche permet de convertir le format de la base de données. L'outil peut assurer des conversions entre les bases de données suivantes :

- MS Access
- MS SQL Server
- Oracle
- MySQL

La première étape consiste à vérifier la connexion de la base de données. Cette étape est propre à toutes les tâches, sauf lors du chargement d'une nouvelle clé de licence et de la modification de la configuration du serveur.

S'il s'agit d'une base de données MS Access, indiquez le chemin d'accès au fichier *.mdb*. Le chemin indiqué lors de l'installation d'ERA Server est utilisé par défaut.

Tous les autres formats de bases de données requièrent la définition de paramètres complémentaires :

- Chaîne de connexion : chaîne spéciale utilisée pour identifier la base de données source.
- Nom d'utilisateur : nom d'utilisateur pour accéder à la base de données.
- Mot de passe : mot de passe pour accéder à la base de données.
- Nom du schéma : nom d'un schéma (disponible pour Oracle et MS SQL uniquement)

Cliquez sur **Charger la configuration de serveur actuelle** pour utiliser les paramètres actuels de ERA Server. Cliquez sur **Tester la connexion** pour tester la connexion de la base de données. S'il est impossible d'établir une connexion, vérifiez si les paramètres sont corrects. Quand le test de la base de données a réussi, continuez en cliquant sur **Suivant**.

Sélectionnez ensuite la base de données cible. Choisissez l'option **Remplacer les paramètres de connexion du serveur** pour connecter le serveur et utiliser la nouvelle base de données après la conversion. Si vous ne choisissez pas cette option, la nouvelle base de données sera créée sans que le serveur n'adopte la nouvelle version de la base de données.

Pour tous les autres types de bases de données à l'exception de MS Access, décidez s'il faut créer les tables de la base de données automatiquement (**Créer automatiquement des tables dans la nouvelle base de données**) ou s'il faut introduire les tables dans la base de données ultérieurement (**Afficher le script** > **Enregistrer dans fichier**) à l'étape suivante. Pour une base de données MySQL, l'option **Créer automatiquement une base de données (ESETRADB)** crée automatiquement une base de données MS SQL appelée ESETRADB. La dernière étape consiste à confirmer la conversion de la base de données.

8.4 Sauvegarde d'une base de données

Cet outil permet de créer un fichier de sauvegarde de la base de données. Les paramètres de la première fenêtre sont très semblables à ceux de la conversion d'une base de données (voir chapitre Transfert de base de données 131) ; lade base de données source est sélectionnée dans cette fenêtre. La base de données source sera copiée dans un fichier de sauvegarde défini à l'étape suivante.

Les paramètres facultatifs de la partie inférieure de la fenêtre permettent d'écraser le fichier existant (**Écraser si existe**) ainsi que d'arrêter ESET Remote Administrator Server lors de la sauvegarde (**Arrêter le serveur pendant le traitement de la tâche**). Cliquez sur **Suivant** pour confirmer l'exécution de la tâche.

8.5 Restauration de la base de données

Cette tâche permet de restaurer la base de données depuis un fichier de sauvegarde. Les paramètres de la première fenêtre sont très semblables à ceux de la conversion d'une base de données (voir chapitre Transfert de base de données 131) ; le type de base de données est sélectionné dans cette fenêtre.

Pour tous les autres types de bases de données à l'exception de MS Access, décidez s'il faut créer les tables de la base de données automatiquement (**Créer automatiquement des tables dans la nouvelle base de données**) ou s'il faut introduire les tables dans la base de données ultérieurement (**Afficher le script** > **Enregistrer dans fichier**) à l'étape suivante. Dans le cas d'une base de données MS SQL, l'option **Créer automatiquement une base de données (ESETRADB)** crée automatiquement une base de donnés MS SQL appelée ESETRADB. La dernière étape consiste à confirmer la restauration de la base de données.

Sélectionnez le fichier à partir duquel la base de données sera restaurée à l'étape suivante. Les paramètres facultatifs de la partie inférieure de la fenêtre permettent d'importer un fichier d'un type de base de données différent de celui sélectionné à l'étape précédente (**Autoriser l'importation d'un type de base de données différent**) ainsi que d'arrêter ESET Remote Administrator Server lors de la restauration de la base de données (**Arrêter le serveur pendant le traitement de la tâche**). Cliquez sur **Suivant** pour confirmer l'exécution de la tâche.

8.6 Supprimer des tables

Ceci supprime les tables actuelles dans la base de données. Par conséquent, la base de données retrouve l'état qu'elle avait juste après l'installation d'ERA Server. Les paramètres de la première fenêtre sont très semblables à ceux de la conversion d'une base de données (voir chapitre Transfert de base de données 131) ; le type de base de données est sélectionné dans cette fenêtre. Vous serez invité à confirmer l'action à l'étape suivante. Choisissez **Oui, j'accepte**, puis cliquez sur **Suivant** pour confirmer l'action.

REMARQUE : En cas d'utilisation d'une base de données MS SQL, MySQL ou Oracle, il est conseillé d'arrêter ERA Server avant de supprimer les tables.

En cas d'utilisation d'une base de données MS Access, celle-ci sera remplacée par la base de données vide par défaut.

8.7 Sauvegarde de stockage

Cette tâche effectue une sauvegarde du stockage et enregistre toutes les données du dossier du stockage (*C:\ProgramData\ESET\ESET Remote Administrator\Server\storage* par défaut) dans un fichier d'image mémoire externe (*.dmp). Ce dossier stocke des configurations et des journaux serveurs importants. Cliquez sur le symbole de l'enveloppe, dans la partie inférieure, pour accéder au dossier dans lequel vous souhaitez que le stockage soit sauvegardé, puis saisissez un nom de fichier. Vous pouvez également indiquer si vous souhaitez **Remplacer si existant**, auquel cas vous souhaitez remplacer un fichier .dmp existant. Il est recommandé de ne pas désélectionner l'option **Arrêter le serveur pendant le traitement de la tâche**, car la tâche de sauvegarde de stockage peut réduire les performances du serveur. Cliquez sur **Suivant**, puis sur **Démarrer** pour lancer la tâche.

8.8 Restauration de stockage

Cette tâche effectue une restauration de stockage à partir d'un fichier d'image mémoire (*.dmp) enregistré. Pour plus d'informations, reportez-vous à la tâche de sauvegarde de stockage. Cliquez sur le symbole de l'enveloppe, dans la partie inférieure, pour accéder au dossier dans lequel le fichier d'image mémoire est stocké. Il est recommandé de ne pas désélectionner l'option **Arrêter le serveur pendant le traitement de la tâche**, car la tâche de restauration de stockage peut réduire les performances du serveur. Cliquez sur **Suivant**, puis sur **Démarrer** pour lancer la tâche.

8.9 Installer une nouvelle clé de licence

Pour introduire une nouvelle clé de licence qui sera utilisée par le serveur, saisissez l'emplacement de la nouvelle clé.

Le cas échéant, écraser la clé existante (**Écraser si existe**) et redémarrez le serveur si nécessaire (**Forcer le démarrage du serveur (s'il ne tourne pas)**). Cliquez sur **Suivant** pour confirmer l'action et terminer.

8.10 Modifier la configuration du serveur

Cette tâche lance Éditeur de configuration (si installé). Quand vous terminez la tâche, la fenêtre Éditeur de configuration s'ouvre et permet de modifier les paramètres avancés de ERA Server. Ces paramètres sont également accessibles via **Outils** > **Options du serveur** > **Paramètres avancés** > **Modifier les paramètres avancés**.

REMARQUE : pour que cette fonctionnalité puisse marcher, ERA Console doit être installée. Vous pouvez également enregistrer les paramètres du serveur dans un fichier .xml et le charger ultérieurement à l'aide de l'option **Charger tous les paramètres du fichier**.

8.11 Interface de ligne de commande

ESET Remote Administrator Maintenance Tool (ERAtool.exe) peut également être utilisé comme outil à ligne de commande qui s'intègre dans les scripts. Lorsque l'outil est exécuté, il analyse les paramètres et exécute chaque action dans l'ordre indiqué. Si aucun argument n'est fourni, l'assistant interactif est exécuté.

Les commandes suivantes sont prises en charge :

- */startserver* ou */startservice* - démarre le service ESET Remote Administrator Server
- */stopserver* ou */stopservice* - arrête le service ESET Remote Administrator Server
- */gui* - lance l'assistant interactif après toutes les tâches

Tout paramètre qui ne commence pas par une barre oblique (/) est interprété comme un nom de fichier du script de configuration qui doit être exécuté. Les scripts de configuration sont créés par l'enregistrement des paramètres dans l'assistant interactif.

REMARQUE :: ERAtool.exe nécessite des droits d'administrateur ; si le script qui appelle ERAtool.exe ne dispose pas des droits nécessaires, Windows peut afficher une invite interactive permettant d'augmenter les droits et d'exécuter un processus de console distinct (l'affichage de l'outil est perdu).

9. Dépannage

9.1 FAQ

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

9.1.1 Problèmes d'installation d'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 saisissez 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.

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

L'installation de ESET Smart Security ou de ESET NOD32 Antivirus via ESET Remote Administrator Console peut parfois engendrer un code d'erreur GLE. Pour connaître la signification d'un numéro d'erreur GLE, procédez de la manière suivante :

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 pour l'exemple : la ressource ou le périphérique réseau spécifié n'est plus disponible.

9.2 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. Les chapitres suivants indiquent 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.

9.2.1 Messages d'erreur affichés lors de l'utilisation de 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 disque système du client.

Code d'erreur SC 6, code d'erreur GLE 1326 Impossible de configurer la connexion IPC à l'ordinateur cible. Le nom d'utilisateur ou le mot de passe fourni est probablement erroné
Le nom d'utilisateur et le mot de passe de l'administrateur n'ont pas été saisis correctement ou n'ont pas été saisis 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 Installation du programme d'installation de ESET sur l'ordinateur cible impossible
Ce code d'erreur s'affiche après une tentative d'installation répétée si la fenêtre Installation poussée n'a pas été fermée après la première tentative.

9.2.2 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 saisi 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 HTTP de réponse d'authentification a été modifié
- lors d'une mise à jour à partir d'un dossier partagé :
  - l'erreur renvoyée 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 adéquat.

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. En cas d'utilisation 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.

9.3 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 le journal**.

2) Si vous ne voyez pas de message d'erreur, augmentez le niveau **Verbosité du journal** dans la fenêtre **Options du serveur** sur 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 et ESET NOD32 Antivirus).

10. Conseils et astuces

10.1 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 types de tâches suivants :

- Exécuter une application externe
- Maintenance des journaux
- Analyse d'ordinateur
- Créer un instantané du statut de l'ordinateur
- Mise à jour
- Vérification automatique des fichiers de démarrage

Dans la plupart des cas, il n'est pas nécessaire de configurer une tâche **Exécuter une application externe**. La tâche **Vérification automatique des fichiers de démarrage** est une tâche par défaut. Il est recommandé de ne pas en modifier les paramètres. 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, la seconde fait la même chose après une mise à jour réussie de la base des signatures de virus. Du point de vue d'un administrateur, les tâches **Analyse d'ordinateur** et **Mise à jour** sont probablement les plus utiles :

- **Analyse d'ordinateur** : effectue une analyse antivirus régulière (généralement de lecteurs locaux) sur les clients.
- **Mise à jour** : cette tâche est chargée 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 dans **Éditeur de configuration d'ESET**, dans **Gamme de produits Windows v3 et v4** > **Noyau ESET** > **Paramètres** > **Planificateur/Programmateur** > **Modifier**.

Pour obtenir des informations supplémentaires, consultez le chapitre Éditeur de configuration d'ESET 50.

Il se peut que la boîte de dialogue contienne des tâches existantes (cliquez sur **Modifier** pour les modifier) ou qu'elle soit vide. Cela dépend si 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.

Les boutons de la fenêtre Tâches planifiées fonctionnent comme suit :

- **Ajouter** : ajoute une tâche.
- **Modifier** : modifie les 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.).

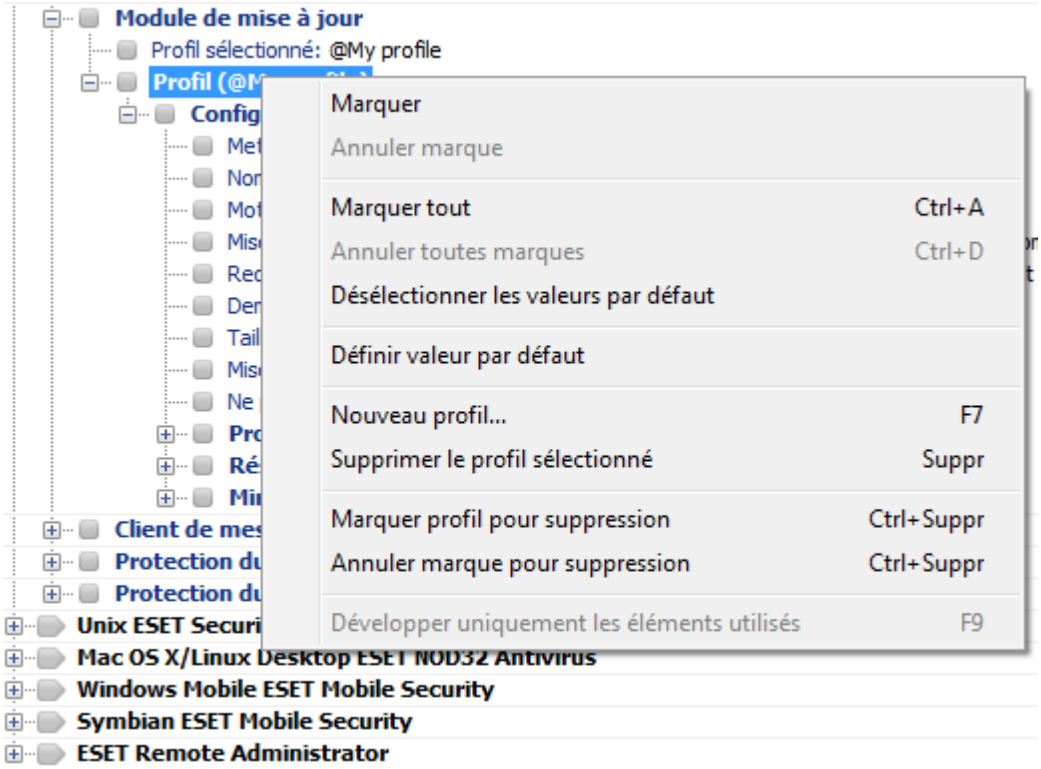
La dernière étape de la tâche **Analyse d'ordinateur à la demande** affiche la fenêtre des paramètres spéciaux dans laquelle vous pouvez définir la configuration qui sera utilisée pour l'analyse, c.-à-d. le profil d'analyse et les cibles d'analyse qui seront utilisés.

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.

10.2 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 le client problématique.
- Dans la fenêtre **Propriétés du client**, cliquez sur l'onglet **Configuration**. Activez les options **Puis exécuter 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 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 de la souris 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.



- Cliquez sur le bouton **Console** dans 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**.

10.3 Exportation et autres fonctions de configuration XML des clients

Dans ERAC, sous l'onglet **Clients**, sélectionnez n'importe quel client. Cliquez avec le bouton droit de la souris, puis dans le menu contextuel, sélectionnez**Configuration...**. Cliquez sur **Enregistrer sous...** pour exporter la configuration attribué au client donné dans un fichier *.xml* (les fichiers de configuration *.xml* peuvent également être extraits directement de l'interface du programme ESET Smart Security). 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. Vous pouvez extraire des fichiers de configuration *.xml* directement à partir de l'interface du programme ESET Smart Security.
- 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, elle est uniquement 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 *.xml* 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 »*.

10.4 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, Exportation et autres fonctions de configuration XML des clients 139, 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 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 Éditeur de configuration d'ESET, cliquez avec le bouton droit de la souris sur la branche **Mise à jour**, puis, dans le menu contextuel, sélectionnez **Nouveau profil**.

Le résultat des modifications doit ressembler à ce qui suit :

- **Module de mise à jour**
  - Profil sélectionné: Mon profil
  - **Profil** (Profile (LAN))
    - **Configuration**
      - Mettre à jour le serveur: AUTOSELECT
      - Nom d'utilisateur:
      - Mot de passe: <mot de passe non défini>
      - Mise à jour des composants du programme: Demander avant de mettre à jour les composants du programme
      - Redémarrer après la mise à niveau d'un composant du programme: Demander avant de redémarrer l'ordinateur, si nécessaire
      - Demander si la taille d'un fichier à télécharger est supérieure à celle spécifiée: Non
      - Taille par défaut du fichier de mise à jour (octets): 0
      - Mises à jour des préversions: Non
      - Ne pas afficher de notification concernant la réussite de la mise à jour: Non
      - **Proxy HTTP**
      - **Réseau local**
      - **Miroir**
  - **Profil** (Profile (INET))
    - **Configuration**
      - Mettre à jour le serveur: AUTOSELECT
      - Nom d'utilisateur: EAV-123456789
      - Mot de passe: *****
      - Mise à jour des composants du programme: Demander avant de mettre à jour les composants du programme
      - Redémarrer après la mise à niveau d'un composant du programme: Demander avant de redémarrer l'ordinateur, si nécessaire
      - Demander si la taille d'un fichier à télécharger est supérieure à celle spécifiée: Non
      - Taille par défaut du fichier de mise à jour (octets): 0
      - Mises à jour des préversions: Non
      - Ne pas afficher de notification concernant la réussite de la mise à jour: Non
      - **Proxy HTTP**
      - **Réseau local**
      - **Miroir**

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, accédez à **Gamme de produits Windows v3 et v4** > **Noyau ESET** > **Paramètres** > **Planificateur/Programmateur** dans Éditeur de configuration d'ESET. Cliquez sur le bouton **Modifier** pour afficher la fenêtre **Tâches planifiées**.

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 : exporter la configuration actuelle *.xml* depuis un client (pour obtenir des informations supplémentaires, consultez le chapitre Comment diagnostiquer des problèmes avec ERAS ? 135) et introduisez les modifications citées ci-dessus dans le fichier *.xml* exporté. Cela évite toute duplication entre le Planificateur et des profils non opérationnels.

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

Outre l'installation à distance de produits ESET, 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 semblable à celui décrit à la section Installation poussée à distance 55.

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

1) Dans ERAC, cliquez sur l'onglet **Installation à distance**.

2) Sélectionnez l'onglet **Ordinateurs**, puis cliquez avec le bouton droit dans son contenu. Sélectionnez l'option **Gérer les packages** dans le menu contextuel.

3) Dans le menu déroulant Type de package, sélectionnez **Package personnalisé**.

4) Cliquez sur **Ajouter...**, sur **Ajouter un fichier**, puis sélectionnez le package *.msi* souhaité.

5) Dans le menu déroulant **Fichier d'entrée du package**, sélectionnez le fichier, puis cliquez sur **Créer**.

6) 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.

7) Cliquez sur **Enregistrer sous...** pour enregistrer le package.

8) 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. Lorsque le package est ouvert, l'installation est gérée par le service Microsoft Windows Installer. Une fois l'installation personnalisée effectuée, ERAS peut télécharger un fichier depuis le client contenant les données de résultat de l'installation. Pour spécifier un fichier résultat, ajoutez le paramètre **/eResult** à la ligne de commande associée au package après l'enregistrement du package personnalisé. Une fois l'installation personnalisée effectuée, vous pouvez télécharger les fichiers de résultats depuis ERAS dans la fenêtre **Détails de la tâche**.

REMARQUE : les packages d'installation personnalisée tiers ne doivent pas dépasser la taille limite de 100 Mo.

11. ESET SysInspector

11.1 Présentation de ESET SysInspector

ESET SysInspector est une application qui inspecte votre ordinateur en profondeur et qui affiche les données obtenues de manière exhaustive. Des information telles que les pilotes et applications installés, les connexions réseau ou les entrées de registre importantes peuvent vous aider à élucider un comportement suspect du système, qu'il soit dû à une incompatibilité logicielle ou matérielle, ou à une infection par logiciel malveillant.

ESET SysInspector est accessible de deux manières : depuis la version intégrée dans les solutions ESET Security ou par téléchargement gratuit de la version autonome (SysInspector.exe) depuis le site d'ESET. Les deux versions ont les mêmes fonctions et les mêmes contrôles de programme. La seule différence réside dans le mode de gestion des résultats. La version autonome et la version intégrée permettent d'exporter des instantanés du système dans un fichier *.xml* et de les enregistrer sur le disque. Toutefois, la version intégrée permet également de stocker les instantanés système directement dans **Outils** > **ESET SysInspector** (à l'exception d'ESET Remote Administrator).

Patientez quelques instants pendant qu'ESET SysInspector analyse votre ordinateur. L'opération peut prendre entre 10 secondes et quelques minutes en fonction de la configuration matérielle, du système d'exploitation et du nombre d'applications installées sur votre ordinateur.

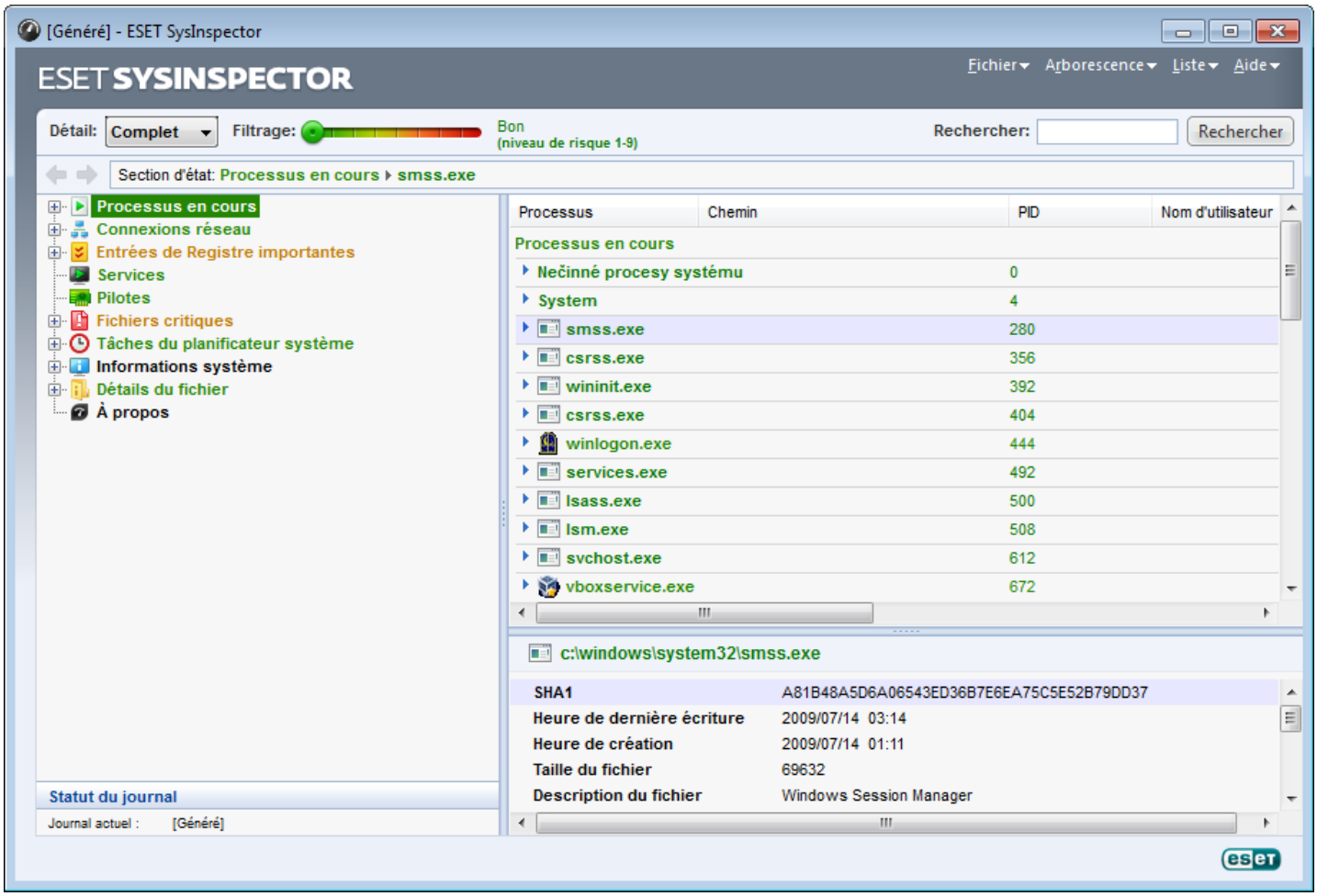
11.1.1 Démarrer ESET SysInspector.

Pour démarrer ESET SysInspector, il suffit de lancer le fichier exécutable *SysInspector.exe* téléchargé depuis le site d'ESET.

Patientez pendant que l'application vérifie le système, une opération qui pourrait durer plusieurs minutes en fonction du matériel et des données à recueillir.

11.2 Interface utilisateur et utilisation de l'application

Pour des raisons de clarté, la fenêtre principale est scindée en quatre grandes sections : contrôles du programme dans la partie supérieure de la fenêtre principale, fenêtre de navigation à gauche, fenêtre de description à droite au centre et fenêtre des détails à droite en bas de la fenêtre principale. La section État du journal reprend les paramètres de base d'un journal (filtre utilisé, type de filtre, le journal est-il le résultat d'une comparaison ?, etc.)



11.2.1 Contrôles du programme

Cette section contient la description de tous les contrôles du programme disponible dans ESET SysInspector.

Fichier

En cliquant sur **Fichier**, vous pouvez enregistrer l'état actuel du système en vue d'une enquête ultérieure ou ouvrir un journal déjà enregistré. Pour la publication, il est conseillé de créer un journal **approprié pour envoi**. Sous cette forme, le journal omet les informations sensibles (nom d'utilisateur, nom d'ordinateur, nom de domaine, privilèges actuels de l'utilisateur, variables d'environnement, etc.).

REMARQUE : vous pouvez ouvrir des rapports enregistrés de ESET SysInspector en les faisant glisser et en les déposant sur la fenêtre principale.

Arborescence

Permet de développer ou de réduire tous les nœuds et d'exporter les sections sélectionnées dans le script de service.

Liste

Contient les fonctions pour une navigation simplifiée dans le programme et diverses autres fonctions comme l'obtention d'informations en ligne.

Aide

Contient des informations sur l'application et ses fonctions.

Détails

Ce paramètre a une incidence sur les informations affichées dans la fenêtre principale afin de simplifier leur utilisation. En mode de base, vous avez accès aux informations utilisées pour trouver les solutions aux problèmes communs dans votre système. En mode « Moyen », l'application affiche moins de détails utilisés. En mode « Complet », ESET SysInspector affiche toutes les informations requises pour résoudre des problèmes très particuliers.

Filtrage des éléments

Le filtrage des éléments est particulièrement adapté à la recherche de fichiers suspects ou d'entrées de Registre dans le système. En déplaçant le curseur, vous pouvez filtrer les éléments en fonction de leur niveau de risque. Quand le curseur est en position maximale vers la gauche (niveau de risque 1), tous les éléments sont affichés. En déplaçant le curseur vers la droite, l'application filtre tous les éléments dont le risque est inférieur au niveau de risque actuel et affiche uniquement les éléments qui sont plus suspects que le niveau affiché. Si le curseur est en position maximale à droite, le programme affiche uniquement les éléments nuisibles connus.

Tous les éléments qui appartiennent aux catégories de risque 6 à 9 peuvent poser un risque pour la sécurité. Si vous n'utilisez pas de solution de sécurité ESET, nous vous conseillons d'analyser votre système à l'aide de ESET Online Scanner si ESET SysInspector a détecté un élément de ce type. ESET Online Scanner est un service gratuit.

REMARQUE : le niveau de risque d'un élément peut être rapidement déterminé en comparant sa couleur à celle du curseur de niveau de risque.

Rechercher

La fonction de recherche peut être utilisée pour trouver rapidement un élément en particulier sur la base de son nom ou d'une partie de celui-ci. Les résultats de la recherche sont affichés dans la fenêtre Description.

Retour

En cliquant sur la flèche arrière ou avant, vous pouvez revenir aux informations affichées précédemment dans la fenêtre Description. Vous pouvez utiliser la touche de retour arrière et la barre d'espace au lieu de cliquer sur les flèches arrière ou avant.

Section d'état

Affiche le nœud actuel dans la fenêtre Navigation.

Important : les éléments surlignés en rouge sont inconnus et c'est la raison pour laquelle l'application les marque comme potentiellement dangereux. Si un élément est rouge, cela ne signifie pas automatiquement que vous pouvez supprimer le fichier. Avant de le supprimer, assurez-vous que les fichiers sont bel et bien dangereux ou qu'ils ne sont pas nécessaires.

11.2.2 Navigation dans ESET SysInspector

ESET SysInspector répartit divers types d'informations en plusieurs sections élémentaires baptisées nœuds. Le cas échéant, vous pouvez obtenir des détails complémentaires en développant chaque nœud afin d'afficher les sous-nœuds. Pour développer ou réduire un nœud, il suffit de double-cliquer sur son nom ou de cliquer sur ⊞ ou sur ⊟ en regard du nom du nœud. Quand vous parcourez la structure arborescente des nœuds et des sous-nœuds dans la fenêtre de navigation, vous pouvez voir différents détails pour chaque nœud dans la fenêtre Description. Si vous parcourez les éléments de la fenêtre Description, des détails supplémentaires pour chaque élément peuvent être affichés dans la fenêtre Détails.

Voici les descriptions des principaux nœuds de la fenêtre Navigation et des informations qui s'y rapportent dans les fenêtres Description et Détails.

Processus en cours

Ce nœud reprend les informations sur les applications et les processus en cours d'exécution au moment de la création du journal. La fenêtre Détails reprend des détails complémentaires pour chaque processus tels que les bibliothèques dynamiques utilisées par les processus et leur emplacement dans le système, le nom de l'éditeur de l'application, le niveau de risque du fichier, etc.

La fenêtre Détails contient des informations complémentaires sur les éléments sélectionnés dans la fenêtre Description telles que la taille du fichier ou son hachage.

REMARQUE : un système d'exploitation contient plusieurs noyaux importants qui fonctionnent en permanence et qui assurent des fonctions élémentaires et vitales pour d'autres applications utilisateur. Dans certains cas, ces processus sont repris dans l'outil ESET SysInspector avec un chemin d'accès au fichier commençant par \??\. Ces symboles

garantissent l'optimisation préalable au lancement pour ce processus ; ils ne présentent aucun danger pour le système.

Connexions réseau

La fenêtre Description contient la liste des processus et des applications qui communiquent via le réseau à l'aide du protocole sélectionné dans la fenêtre navigation (TCP ou UDP), ainsi que l'adresse distante à laquelle l'application est connectée. Vous pouvez également vérifier les adresses IP des serveurs DNS.

La fenêtre Détails contient des informations complémentaires sur les éléments sélectionnés dans la fenêtre Description telles que la taille du fichier ou son hachage.

Entrées de Registre importantes

Contient la liste des entrées de registre sélectionnées qui sont souvent liées à divers problèmes du système telles que celles qui indiquent les applications de démarrage, les objets application d'assistance du navigateur, etc.

La fenêtre Description peut indiquer les fichiers en rapport avec les entrées de Registre particulières. Vous pouvez voir des détails complémentaires dans la fenêtre Détails.

Services

La fenêtre Description contient la liste des fichiers enregistrés en tant que services Windows. Vous pouvez consulter la manière dont le service doit démarrer avec des détails spécifiques sur le fichier dans la fenêtre Détails.

Pilotes

Liste des pilotes installés sur le système.

Fichiers critiques

La fenêtre Description affiche le contenu des fichiers critiques liés au système d'exploitation Microsoft Windows.

Tâches système du planificateur

Contient la liste des tâches déclenchées par le planificateur de tâches Windows à une heure/un intervalle spécifiés.

Informations système

Contient des informations détaillées sur le matériel et le logiciel, ainsi que des informations sur les variables d'environnement, les droits de l'utilisateur et les journaux d'événement système définis.

Détails du fichier

Liste des fichiers système importants et des fichiers du dossier Program Files. Des informations complémentaires spécifiques sur les fichiers sont disponibles dans les fenêtres Description et Détails.

À propos

Informations sur la version d'ESET SysInspector et sur la liste des modules de programme.

11.2.2.1 Raccourcis clavier

Voici les raccourcis clavier disponibles dans ESET SysInspector :

Fichier

Ctrl+O	ouvre un journal existant
Ctrl+S	enregistre les journaux créés

Générer

Ctrl+G	génère un instantané du statut de l'ordinateur
Ctrl+H	génère un instantané de l'état du système qui pourrait également consigner des informations sensibles

Filtrage des éléments

1, O	acceptable, les éléments de niveau de risque 1 à 9 sont affichés
2	acceptable, les éléments de niveau de risque 2 à 9 sont affichés
3	acceptable, les éléments de niveau de risque 3 à 9 sont affichés
4, U	inconnu, les éléments de niveau de risque 4 à 9 sont affichés
5	inconnu, les éléments de niveau de risque 5 à 9 sont affichés

6	inconnu, les éléments de niveau de risque 6 à 9 sont affichés
7, B	risqué, les éléments de niveau de risque 7 à 9 sont affichés
8	risqué, les éléments de niveau de risque 8 à 9 sont affichés
9	risqué, les éléments de niveau de risque 9 sont affichés
-	diminue le niveau de risque
+	augmente le niveau de risque
Ctrl+9	mode de filtrage, niveau égal ou supérieur
Ctrl+O	niveau de filtrage, niveau égal uniquement

Afficher

Ctrl+5	afficher par éditeur, tous les éditeurs
Ctrl+6	afficher par éditeur, uniquement Microsoft
Ctrl+7	afficher par éditeur, tous les autres éditeurs
Ctrl+3	appliquer tous les détails
Ctrl+2	afficher les détails moyens
Ctrl+1	affichage de base
Retour arrière	revient une étape en arrière
Barre d'espace	avance d'une étape
Ctrl+W	développe l'arborescence
Ctrl+Q	réduit l'arborescence

Autres commandes

Ctrl+T	va à l'emplacement d'origine de l'élément après la sélection dans les résultats de recherche
Ctrl+P	affiche des informations élémentaires sur un élément
Ctrl+A	affiche des informations complètes sur un élément
Ctrl+C	copie l'arborescence de l'élément
Ctrl+X	copie les éléments
Ctrl+B	trouve des informations sur les fichiers sélectionnés sur Internet
Ctrl+L	ouvre le dossier où se trouve le fichier sélectionné.
Ctrl+R	ouvre l'entrée correspondante dans l'éditeur de registre
Ctrl+Z	copie un chemin d'accès à un fichier (si l'élément est lié à un fichier)
Ctrl+F	passe au champ de recherche
Ctrl+D	ferme les résultats de la recherche
Ctrl+E	exécute le script de service

Comparaison

Ctrl+Alt+O	ouvre le journal d'origine/de comparaison
Ctrl+Alt+R	annule la comparaison
Ctrl+Alt+1	affiche tous les éléments
Ctrl+Alt+2	affiche uniquement les éléments ajoutés, le journal indiquera les éléments présents dans le journal actuel
Ctrl+Alt+3	affiche uniquement les éléments supprimés, le journal indiquera les éléments présents dans le journal précédent
Ctrl+Alt+4	affiche uniquement les éléments remplacés (fichiers inclus)
Ctrl+Alt+5	affiche uniquement les différences entre les journaux
Ctrl+Alt+C	affiche la comparaison
Ctrl+Alt+N	affiche le journal actuel
Ctrl+Alt+P	ouvre le journal précédent

Divers

F1	afficher l'aide
Alt+F4	quitter l'application
Alt+Maj+F4	quitter l'application sans demander
Ctrl+I	statistiques du journal

11.2.3 Comparer

La fonctionnalité Comparer permet de comparer deux journaux. Cette fonctionnalité met en évidence les éléments qui ne sont pas communs aux deux journaux. Cet outil est utile si vous souhaitez assurer le suivi des modifications dans le système, car il permet de détecter l'activité d'un code malveillant.

Après son lancement, l'application crée un journal qui apparaît dans une nouvelle fenêtre. Accédez au menu **Fichier** > **Enregistrer le journal** pour enregistrer le journal dans un fichier. Les fichiers journaux peuvent être ouverts et consultés ultérieurement. Pour ouvrir un journal existant, utilisez le menu **Fichier** > **Ouvrir le journal**. Dans la fenêtre principale de l'application, ESET SysInspector affiche toujours un journal à la fois.

La comparaison de deux journaux permet d'afficher un journal actif et un journal enregistré dans un fichier. Pour comparer des journaux, choisissez l'option **Fichier** > **Comparer les journaux**, puis choisissez **Sélectionner un fichier**. Le journal sélectionné sera comparé au journal actif dans les fenêtres principales de l'application. Le journal des comparaisons n'affiche que les différences entre les deux journaux.

REMARQUE : si vous comparez deux fichiers journaux, que vous choisissez **Fichier** > **Enregistrer le journal** et que vous l'enregistrez dans un fichier ZIP, les deux fichiers sont enregistrés. Si vous ouvrez ce fichier ultérieurement, les journaux qu'il contient seront comparés automatiquement.

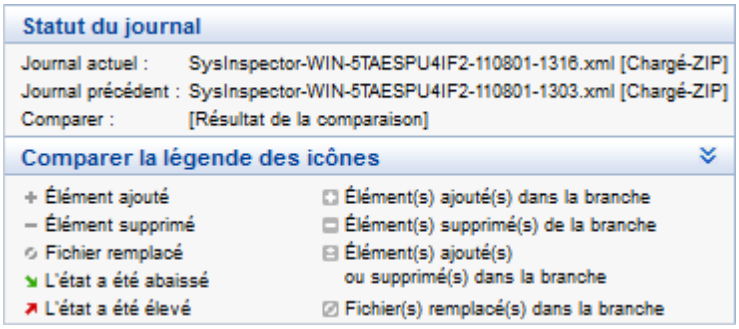
En regard des éléments affichés, ESET SysInspector affiche les symboles qui identifient les différences entre les journaux comparés.

Les éléments marqués par – se trouvent uniquement dans le journal actif et sont absents du journal de comparaison ouvert. En revanche, les éléments marqués par + se trouvent uniquement dans le journal ouvert et ne figurent pas dans le journal actif.

Description de tous les symboles qui peuvent être affichés à côté des éléments :

- + nouvelle valeur, absente du journal précédent.
- la section de la structure arborescente contient de nouvelles valeurs.
- – valeur supprimée, présente uniquement dans le journal précédent.
- la section de la structure arborescente contient des valeurs supprimées.
- la valeur/le fichier a été modifié.
- la section de la structure arborescente contient des valeurs/des fichiers modifiés.
- le niveau de risque a diminué/il était supérieur dans le journal précédent.
- le niveau de risque a augmenté/il était inférieur dans le journal précédent.

La section d'explication affichée dans le coin inférieur gauche décrit tous les symboles et affiche le nom des journaux comparés.



Les journaux de comparaison peuvent être enregistrés dans un fichier et ouverts plus tard :

Exemple

Créez un journal reprenant des informations d'origine sur le système et enregistrez-le dans un fichier appelé précédent.xml. Après avoir modifié le système, ouvrez ESET SysInspector et laissez-le créer un nouveau journal. Enregistrez ce journal sous *actuel.xml*.

Pour voir les différences entre ces deux journaux, utilisez l'option **Fichier** > **Comparer les journaux**. Le programme crée un journal de comparaison qui indique les différences entre les journaux.

Un résultat identique peut être obtenu si vous utilisez l'option de ligne de commande suivante :

SysInspector.exe actuel.xml précédent.xml

11.3 Paramètres de la ligne de commande

ESET SysInspector prend en charge la création de rapports via la ligne de commande à l'aide de ces paramètres :

/gen	crée un journal directement depuis la ligne de commande sans exécuter l'interface utilisateur.
/privacy	crée un journal qui exclut les informations sensibles.
/zip	stocke le journal obtenu directement sur le disque dans un fichier compressé.
/silent	supprime l'affichage de la barre d'état de la création du journal.
/help, /?	affiche des informations sur les paramètres de la ligne de commande.

Exemples

Pour charger un journal en particulier directement dans la navigateur, saisissez : *SysInspector.exe "c:\clientlog.xml"*
Pour créer un journal à l'emplacement actuel, saisissez : *SysInspector.exe /gen*
Pour créer un journal dans un dossier en particulier, saisissez : *SysInspector.exe /gen="c:\dossier\"*
Pour créer un journal dans un fichier/un dossier en particulier, saisissez : *SysInspector.exe /gen="c:\dossier\monnouveaujournal.xml"*
Pour créer un journal qui exclut les informations sensibles directement dans un fichier compressé, utilisez : *SysInspector.exe /gen="c:\monnouveaujournal.zip" /privacy /zip*
Pour comparer deux journaux, utilisez : *SysInspector.exe "actuel.xml" "original.xml"*

REMARQUE : si le nom du fichier/du dossier contient un espace, vous devez le saisir entre guillemets.

11.4 Script de service

Le script de service est un outil qui vise à offrir une aide aux clients qui utilisent ESET SysInspector en leur permettant de supprimer les objets indésirables du système.

Le script de service permet à l'utilisateur d'exporter l'ensemble du journal ESET SysInspector ou des parties sélectionnées uniquement. Après l'exportation, vous pouvez marquer les objets indésirables pour la suppression. Vous pouvez ensuite exécuter le journal modifié pour supprimer les objets marqués.

Le script de service convient aux utilisateurs expérimentés qui connaissent les problèmes des systèmes de diagnostic. Des modifications erronées pourraient endommager le système d'exploitation.

Exemple

si vous pensez que votre ordinateur est infecté par un virus qui n'est pas détecté par votre logiciel antivirus, suivez les instructions ci-après :

- Exécutez ESET SysInspector pour obtenir un nouvel instantané du système.
- Sélectionnez le premier élément de la section à gauche (dans la structure arborescente), appuyez sur la touche Maj, puis sélectionnez le dernier élément afin de marquer tous les éléments.
- Cliquez avec le bouton droit de la souris sur les objets sélectionnés, puis choisissez l'option **Exporter les sections sélectionnées dans un script de service** dans le menu contextuel.
- Les objets sélectionnés seront exportés dans un nouveau journal.
- Il s'agit de l'étape la plus importante de toute la procédure : ouvrez le nouveau journal et remplacez l'attribut + par - pour tous les objets que vous souhaitez supprimer. Veillez à ne marquer aucun objet/fichier important du système d'exploitation.
- Ouvrez ESET SysInspector, cliquez sur **Fichier** > **Exécuter le script de service**, puis saisissez le chemin d'accès au script.
- Cliquez sur **OK** pour lancer le script.

11.4.1 Création d'un script de service

Pour créer un script, cliquez avec le bouton droit de la souris sur n'importe quel élément de l'arborescence de menus (dans le volet de gauche) dans la fenêtre principale de ESET SysInspector. Dans le menu contextuel, choisissez l'option **Exporter toutes les sections dans un script de service** ou **Exporter les sections sélectionnées dans un script de service**.

REMARQUE : il est impossible d'exporter le script de service lorsque deux journaux sont comparés.

11.4.2 Structure du script de service

La première ligne de l'en-tête du script reprend des informations sur la version du moteur (ev), la version de l'interface utilisateur graphique (gv) et la version du journal (lv). Ces données permettent d'identifier d'éventuelles modifications dans le fichier .xml qui génère le script et d'éviter toute incohérence durant l'exécution. Cette partie du script ne peut être modifiée.

Le reste du fichier est scindé en sections dont les éléments peuvent être modifiés (indique ceux qui seront traités par le script). Pour marquer un élément à traiter, remplacez le caractère « - » qui le précède par « + ». Les sections du script sont séparées par une ligne vide. Chaque section possède un numéro et un titre.

01) Running processes (processus en cours)

Cette section contient la liste de tous les processus en cours d'exécution dans le système. Chaque processus est identifié par son chemin UNC et, ensuite, par son code de hachage CRC16 entre astérisques (*).

Exemple :

```
01) Running processes:
- \SystemRoot\System32\smss.exe *4725*
- C:\Windows\system32\svchost.exe *FD08*
+ C:\Windows\system32\module32.exe *CF8A*
[...]
```

Dans cet exemple, un processus, à savoir module32.exe, a été sélectionné (marqué par le caractère « + ») ; le processus s'arrêtera à l'exécution du script.

02) Loaded modules (modules chargés)

Cette section reprend une liste des modules système en cours d'utilisation :

Exemple :

```
02) Loaded modules:
- c:\windows\system32\svchost.exe
- c:\windows\system32\kernel32.dll
+ c:\windows\system32\khbekhb.dll
- c:\windows\system32\advapi32.dll
[...]
```

Dans cet exemple, le module khbekhb.dll a été marqué par un « + ». Quand le script est exécuté, il reconnaît les processus qui utilisent ce module en particulier et les arrête.

03) TCP connections (connexions TCP)

Cette section contient des informations sur les connexions TCP existantes.

Exemple :

```
03) TCP connections:
- Active connection: 127.0.0.1:30606 -> 127.0.0.1:55320, owner: ekrn.exe
- Active connection: 127.0.0.1:50007 -> 127.0.0.1:50006,
- Active connection: 127.0.0.1:55320 -> 127.0.0.1:30606, owner: OUTLOOK.EXE
- Listening on *, port 135 (epmap), owner: svchost.exe
+ Listening on *, port 2401, owner: fservice.exe Listening on *, port 445 (microsoft-ds), owner:
System
[...]
```

Lorsque le script est exécuté, il trouve le propriétaire du socket dans les connexions TCP marquées et arrête le socket, ce qui libère des ressources système.

04) UDP endpoints (points de terminaison UDP)

Cette section contient des informations sur les points de terminaison UDP existants.

Exemple :

```
04) UDP endpoints:
- 0.0.0.0, port 123 (ntp)
+ 0.0.0.0, port 3702
- 0.0.0.0, port 4500 (ipsec-msft)
- 0.0.0.0, port 500 (isakmp)
[...]
```

Lorsque le script est exécuté, il isole le propriétaire du socket aux points de terminaison UDP marqués et arrête le socket.

05) DNS server entries (entrées du serveur DNS)

Cette section contient des informations sur la configuration actuelle du serveur DNS.

Exemple :

```
05) DNS server entries:
+ 204.74.105.85
- 172.16.152.2
[...]
```

Les entrées du serveur DNS marquées seront supprimées à l'exécution du script.

06) Important registry entries (entrées de registre importantes)

Cette section contient des informations relatives aux entrées de registre importantes.

Exemple :

```
06) Important registry entries:
* Category: Standard Autostart (3 items)
 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HotKeysCmds = C:\Windows\system32\hkcmd.exe
- IgfxTray = C:\Windows\system32\igfxtray.exe
 HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Google Update = "C:\Users\antoniak\AppData\Local\Google\Update\GoogleUpdate.exe" /c
* Category: Internet Explorer (7 items)
 HKLM\Software\Microsoft\Internet Explorer\Main
+ Default_Page_URL = http://thatcrack.com/
[...]
```

Les entrées marquées seront supprimées, réduites à des valeurs de 0 octet ou réinitialisées à leur valeur par défaut lors de l'exécution du script. L'action à appliquer à une entrée en particulier dépendra de la catégorie de l'entrée et de la valeur de la clé dans ce registre en particulier.

07) Services (services)

Cette section reprend les services enregistrés dans le système.

Exemple :

```
07) Services:
- Name: Andrea ADI Filters Service, exe path: c:\windows\system32\aeadisrv.exe, state: Running,
startup: Automatic
- Name: Application Experience Service, exe path: c:\windows\system32\aelupsvc.dll, state: Running,
startup: Automatic
- Name: Application Layer Gateway Service, exe path: c:\windows\system32\alg.exe, state: Stopped,
startup: Manual
[...]
```

Les services marqués et les services dépendants seront arrêtés et désinstallés après l'exécution du script.

08) Drivers (pilotes)

Cette section reprend les pilotes installés.

Exemple :

```
08) Drivers:
- Name: Microsoft ACPI Driver, exe path: c:\windows\system32\drivers\acpi.sys, state: Running,
startup: Boot
- Name: ADI UAA Function Driver for High Definition Audio Service, exe path: c:\windows\system32
\drivers\adihdaud.sys, state: Running, startup: Manual
[...]
```

Lorsque vous exécutez le script, les pilotes sélectionnés seront arrêtés. Notez que certains pilotes ne s'arrêtent pas.

09) Critical files (fichiers critiques)

Cette section contient des informations sur les fichiers critiques pour le fonctionnement adéquat du système d'exploitation.

Exemple :

```
09) Critical files:
* File: win.ini
- [fonts]
- [extensions]
- [files]
- MAPI=1
[...]
* File: system.ini
- [386Enh]
- woafont=dosapp.fon
- EGA80WOA.FON=EGA80WOA.FON
[...]
* File: hosts
- 127.0.0.1 localhost
- ::1 localhost
[...]
```

Les éléments sélectionnés seront soit supprimés, soit restaurés à leur valeur d'origine.

11.4.3 Exécution des scripts de service

Marquez tous les éléments souhaités, puis enregistrez et fermez le script. Exécutez le script modifié directement depuis la fenêtre principale ESET SysInspector en choisissant l'option **Exécuter le script de service** dans le menu Fichier. Lorsque vous ouvrez un script, le programme affiche le message suivant : **Voulez-vous vraiment exécuter le script de service « %Scriptname% » ?** Après avoir confirmé votre sélection, un autre avertissement peut apparaître et vous indique que le script de service que vous essayez d'exécuter n'a pas été signé. Cliquez sur **Exécuter** pour lancer le script.

Une boîte de dialogue confirme que le script s'est exécuté correctement.

Si le script n'a pu être traité que partiellement, une boîte de dialogue avec le message suivant apparaîtra : **Le script de service n'a été exécuté que partiellement. Voulez-vous afficher le rapport d'erreurs ?** Choisissez **Oui** pour afficher un rapport des erreurs complexe qui reprend les opérations qui n'ont pas été exécutées.

Si le script n'a pas été reconnu, une boîte de dialogue s'affiche avec le message suivant : **Le script de service sélectionné n'est pas signé. L'exécution de scripts sans signature et inconnus peut nuire sérieusement aux données de votre ordinateur. Êtes-vous certain de vouloir exécuter le script et les actions ?** Ceci peut être le résultat d'incohérences au sein du script (en-tête endommagé, titre de section endommagé, ligne vide manquante entre les sections, etc.). Vous pouvez soit rouvrir le fichier de script et corriger les erreurs qu'il contient, soit créer un autre script de service.

11.5 FAQ

L'exécution de ESET SysInspector requiert-elle des privilèges d'administrateur ?

Bien que ESET SysInspector puisse être exécuté sans privilèges d'administrateur, certaines des informations qu'il recueille peuvent être consultées uniquement via un compte administrateur. Une exécution en tant qu'utilisateur standard ou utilisateur disposant d'un accès restreint entraînera la collecte d'un volume inférieur d'informations sur l'environnement d'exploitation.

ESET SysInspector crée-t-il un fichier journal ?

ESET SysInspector peut créer un fichier journal sur la configuration de votre ordinateur. Pour l'enregistrer, choisissez **Fichier** > **Enregistrer le journal** dans le menu principal. Les journaux sont enregistrés au format XML. Par défaut, les

fichiers sont enregistrés dans le répertoire *%USERPROFILE%\My Documents* selon la nomenclature « SysInspector-%COMPUTERNAME%-AAMMJJ-HHMM.XML ». Vos pouvez changer l'emplacement et le nom du fichier avant la sauvegarde si vous le souhaitez.

Comment puis-je consulter le fichier journal de ESET SysInspector ?

Pour consulter un fichier journal créé par ESET SysInspector, exécutez le programme et choisissez **Fichier** > **Ouvrir le journal** dans le menu principal. Vous pouvez également faire glisser les fichiers journaux et les déposer sur l'application ESET SysInspector. Si vous devez consulter fréquemment les fichiers journaux ESET SysInspector, il est conseillé de créer un raccourci vers le fichier SYSINSPECTOR.exe sur le Bureau ; vous pourrez ensuite faire glisser les fichiers et les déposer sur ce raccourci. Pour des raisons de sécurité, Windows Vista/7 peut ne pas autoriser la fonction glisser-déposer entre des fenêtres dont les autorisations diffèrent.

Existe-t-il une spécification pour le format du fichier journal ? Ou un SDK ?

Pour l'instant, il n'existe ni spécifications pour le fichier journal, ni SDK, car le programme en est toujours au stade du développement. Après la diffusion du programme, nous fournirons ces éléments sur la base des commentaires et des demandes des clients.

Comment ESET SysInspector évalue-t-il le risque que pose un objet en particulier ?

Dans la majorité des cas, ESET SysInspector attribue des niveaux de risque aux objets (fichiers, processus, clés de Registre, etc.) sur la base d'une série de règles heuristiques qui examinent les caractéristiques de chaque objet, puis qui évaluent le potentiel d'activité malveillante. Cette analyse heuristique attribue aux objets un niveau de risque allant de 1 - OK (vert) à 9 - Risqué (rouge). Dans le volet de navigation gauche, la couleur des sections est définie par le niveau de risque le plus élevé d'un des objets qu'elles contiennent.

Un niveau de risque « 6 - Inconnu (rouge) » signifie-t-il que l'objet est dangereux ?

Les évaluations de ESET SysInspector ne garantissent pas qu'un objet est malveillant. Cette réponse doit être apportée par l'expert en sécurité. ESET SysInspector a été développé pour fournir aux experts en sécurité une évaluation rapide afin qu'ils puissent identifier les objets d'un système qui devront faire l'objet d'un examen plus approfondi en cas de comportement étrange.

Pourquoi ESET SysInspector se connecte-t-il à Internet ?

À l'instar de nombreuses applications, ESET SysInspector possède un « certificat » avec une signature numérique qui permet de garantir que le logiciel a bien été diffusé par ESET et qu'il n'a pas été modifié. Afin de vérifier le certificat, le système d'exploitation contacte une autorité de certification pour confirmer l'identité de l'éditeur de logiciels. Il s'agit d'un comportement normal pour tous les programmes avec signature numérique sous Microsoft Windows.

Qu'est ce que la technologie Anti-Stealth ?

La technologie Anti-Stealth offre une détection efficace des rootkits.

Quand un système est attaqué par un code malveillant qui se comporte comme un rootkit, l'utilisateur est exposé à la perte ou au vol de données. Sans outil spécial de lutte contre les rootkits, il est pratiquement impossible de les détecter.

Pourquoi y-a-t-il parfois des fichiers marqués comme « Signé par MS » avec une valeur différente dans le champ « Nom de la société » ?

Lorsque ESET SysInspector tente d'identifier la signature numérique d'un fichier exécutable, il vérifie d'abord si le fichier intègre une signature numérique. Si une signature numérique est détectée, le fichier est validé à l'aide de ces informations. Si aucune signature numérique n'est détectée, ESET SysInspector lance la recherche du fichier CAT correspondant (Catalogue de sécurité - *%systemroot%\system32\catroot*) qui contient les informations sur le fichier exécutable traité. Si le fichier CAT pertinent est trouvé, la signature numérique du fichier CAT est appliquée dans la procédure de validation du fichier exécutable.

C'est la raison pour laquelle les fichiers sont parfois marqués « Signé par MS » mais ont un « Nom de la société » différent.

Exemple :

Windows 2000 reprend l'application HyperTerminal qui se trouve dans *C:\Program Files\Windows NT*. Le fichier exécutable principal de l'application n'a pas de signature numérique, mais ESET SysInspector l'indique comme étant un fichier signé par Microsoft. Ceci s'explique par une référence dans *C:\WINNT\system32\CatRoot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\sp4.cat* qui pointe vers *C:\Program Files\Windows NT\hypertrm.exe* (le fichier exécutable principal de l'application HyperTerminal) et *sp4.cat* possède une signature numérique de Microsoft.

12. ESET SysRescue

ESET SysRescue est un utilitaire qui permet de créer un disque d'amorçage contenant l'une des solutions ESET Security : ESET NOD32 Antivirus, ESET Smart Security ou même certains des produits orientés serveur. Le principal avantage de ESET SysRescue réside dans le fait que la solution ESET Security est exécutée indépendamment du système d'exploitation hôte, tout en ayant un accès direct au disque et à l'ensemble du système de fichiers. Il est ainsi possible de supprimer les infiltrations qui ne pourraient normalement pas être supprimées, par exemple lorsque le système d'exploitation est en cours d'exécution, etc.

12.1 Configuration minimale requise

ESET SysRescue fonctionne dans l'environnement de préinstallation Microsoft Windows (Windows PE) version 2.x qui repose sur Windows Vista.

Windows PE fait partie du Kit d'installation automatisée de Windows (Windows AIK) et par conséquent, Windows AIK doit être installé avant de créer ESET SysRescue (http://go.eset.eu/AIK). En raison de la prise en charge de la version 32 bits de Windows PE, il est nécessaire d'utiliser un package d'installation 32 bits de la soution ESET Security lors de la création d'ESET SysRescue sur des systèmes 64 bits. ESET SysRescue prend en charge Windows AIK 1.1 et les versions ultérieures.

REMARQUE : la taille de Windows AIK étant supérieure à 1 Go, le téléchargement nécessite une connexion Internet haut débit.

ESET SysRescue est disponible dans les solutions ESET Security version 4.0 et ultérieures.

Systèmes d'exploitation pris en charge

- Windows 7
- Windows Vista
- Windows Vista Service Pack 1
- Windows Vista Service Pack 2
- Windows Server 2008
- Windows Server 2003 Service Pack 1 avec KB926044
- Windows Server 2003 Service Pack 2
- Windows XP Service Pack 2 avec KB926044
- Windows XP Service Pack 3

12.2 Procédure de création d'un CD de dépannage

Pour lancer l'assistant ESET SysRescue, cliquez sur **Démarrer** > **Programmes** > **ESET** > **ESET Remote Administrator** > **ESET SysRescue**.

Tout d'abord, l'assistant vérifie si Windows AIK est installé et si un périphérique adapté pour la création du support d'amorçage est présent. Si Windows AIK n'est pas installé sur l'ordinateur (ou si l'installation est endommagée ou incorrecte), l'assistant vous proposera de l'installer ou de saisir le chemin d'accès à votre dossier Windows AIK (http://go.eset.eu/AIK).

REMARQUE : la taille de Windows AIK étant supérieure à 1 Go, le téléchargement nécessite une connexion Internet haut débit.

Au cours de l'étape suivante 154, sélectionnez le support cible où ESET SysRescue sera créé.

12.3 Sélection de la cible

Outre la sauvegarde sur un CD/DVD/périphérique USB, vous pouvez enregistrer ESET SysRescue dans un fichier ISO. Par la suite, vous pourrez graver l'image ISO sur un CD/DVD ou l'utiliser d'une autre manière (p. ex., dans un environnement virtuel tel que VMware ou Virtualbox).

Si vous choisissez un support cible USB, le démarrage peut ne pas fonctionner sur certains ordinateurs. Certaines versions de BIOS peuvent signaler des problèmes de communication entre BIOS et le gestionnaire de démarrage (p. ex., sous Windows Vista) et le démarrage arrête sur l'erreur suivante :

```
file : \boot\bcd
status : 0xc000000e
info : une erreur s'est produite pendant la tentative de lecture des données de configuration du démarrage
```

Si vous êtes confronté à ce message, il est conseillé de sélectionner CD au lieu d'USB en tant que support.

12.4 Paramètres

Avant de commencer la création du CD ESET SysRescue, l'assistant d'installation affiche la compilation des paramètres qui peuvent être modifiés dans la dernière étape de l'assistant ESET SysRescue. Vous pouvez les modifier en cliquant sur le bouton **Modifier**. Les options disponibles sont les suivantes :

- Dossiers 154
- Antivirus ESET 155
- Paramètres avancés 155
- Protocole Internet 155
- Périphérique USB d'amorçage 155 (lorsqu'un périphérique USB cible est sélectionné)
- Gravure 156 (lorsque le lecteur de CD/DVD cible est sélectionné)

Le bouton **Créer** est inactif si aucun package d'installation MSI n'a été défini ou si aucune solution ESET Security n'est installée sur l'ordinateur. Pour sélectionner un package d'installation, cliquez sur le bouton **Modifier**, puis accédez à l'onglet **Antivirus ESET**. Si vous ne saisissez pas le nom d'utilisateur et le mot de passe (**Modifier Antivirus ESET**), le bouton **Créer** est inactif.

12.4.1 Dossiers

Le **dossier temporaire** est un dossier de travail pour les fichiers requis lors de la compilation de ESET SysRescue.

Le **dossier ISO** est un dossier dans lequel le fichier ISO est enregistré après la fin de la compilation.

La liste sous cet onglet reprend tous les disques de réseau locaux et mappés ainsi que l'espace disponible. Si certains des dossiers sont situés sur un lecteur manquant d'espace, il est conseillé de sélectionner un autre lecteur avec plus d'espace disponible. Dans le cas contraire, la compilation pourrait s'arrêter prématurément en raison d'un manque d'espace sur le disque.

Applications externes : permet d'indiquer des programmes supplémentaires qui seront exécutés ou installés après l'amorçage depuis un support ESET SysRescue.

Inclure les applications externes : permet d'ajouter des programmes externes à la compilation ESET SysRescue.

Dossier sélectionné : dossier dans lequel se trouvent les programmes qui doivent être ajoutés à ESET SysRescue.

12.4.2 Antivirus ESET

Pour créer le CD ESET SysRescue, vous pouvez sélectionner deux sources de fichiers ESET à utiliser par le compilateur.

Dossier ESS/EAV : fichiers déjà contenus dans le dossier dans lequel la solution ESET Security est installée sur l'ordinateur.

Fichier MSI : les fichiers contenus dans le programme d'installation MSI sont utilisés.

Vous pouvez ensuite choisir de mettre à jour l'emplacement des fichiers (.nup). Normalement, l'option par défaut **Dossier ESS/EAV/Fichier MSI** doit être défini. Dans certains cas, un **dossier de mise à jour** personnalisé peut être choisi, par exemple pour utiliser une version de base des signatures de virus plus ancienne ou plus récente.

Vous pouvez utiliser l'une des deux sources suivantes pour le nom d'utilisateur et le mot de passe :

ESS/EAV installé : le nom d'utilisateur et le mot de passe sont copiés depuis la version installée de la solution ESET Security.

De l'utilisateur : le nom d'utilisateur et le mot de passe saisis dans les zones de texte correspondantes sont utilisés.

REMARQUE : la solution ESET Security du CD ESET SysRescue est mise à jour soit depuis Internet, soit depuis la solution ESET Security installée sur l'ordinateur sur lequel le CD ESET SysRescue est exécuté.

12.4.3 Paramètres avancés

L'onglet **Avancé** permet d'optimiser le CD ESET SysRescue en fonction de la quantité de mémoire disponible sur l'ordinateur. Sélectionnez **576 Mo et plus** pour écrire le contenu du CD dans la mémoire vive (RAM). Si vous choisissez **moins de 576 Mo**, l'accès au CD de récupération aura lieu en permanence lorsque WinPE est en exécution.

Dans la section **Pilotes externes**, vous pouvez indiquer les pilotes de votre matériel (en général, une carte de réseau). Bien que WinPE repose sur Windows Vista PS1 qui prend en charge un large éventail de matériel, il arrive parfois que le matériel ne soit pas reconnu. Le pilote doit alors être ajouté manuellement. Un pilote peut être indiqué de deux manières dans la compilation ESET SysRescue : manuellement (à l'aide du bouton **Ajouter**) et automatiquement (à l'aide du bouton **Recherche auto**.) En cas d'intégration manuelle, vous devez choisir le chemin d'accès au fichier .inf correspondant (le fichier *.sys applicable doit se trouver également dans le dossier). En cas d'introduction automatique, le pilote est trouvé automatiquement dans le système d'exploitation de l'ordinateur donné. Il est conseillé d'utiliser l'intégration automatique uniquement si ESET SysRescue est utilisé sur un ordinateur qui possède la même carte de réseau que l'ordinateur sur lequel le CD ESET SysRescue a été créé. Lors de la création de ESET SysRescue, le pilote est introduit dans la compilation, si bien que l'utilisateur n'a pas besoin de le chercher ultérieurement.

12.4.4 Protocole Internet

Cette section permet de configurer les informations réseau de base et de configurer des connexions prédéfinies après ESET SysRescue.

Sélectionnez **Adresse IP privée automatique** pour obtenir l'adresse IP automatiquement du serveur DHCP (Dynamic Host Configuration Protocol).

Cette connexion réseau peut également utiliser une adresse IP spécifiée manuellement (appelée également adresse IP statique). Sélectionnez **Personnaliser** pour configurer les paramètres IP appropriés. Si vous sélectionnez cette option, vous devez indiquer une **adresse IP** et, pour les connexions LAN et Internet haut débit, un **masque de sous-réseau**. Dans les zones **Serveur DNS préféré** et **Serveur DNS auxiliaire**, saisissez les adresses des serveurs DNS principal et secondaire.

12.4.5 Périphérique USB d'amorçage

Si vous avez choisi le périphérique USB en tant que support cible, vous pouvez choisir un des supports USB disponibles sous l'onglet **Périphérique USB d'amorçage** (si plusieurs périphériques USB existent).

Sélectionnez le **périphérique** cible approprié sur lequel ESET SysRescue sera installé.

Avertissement : le périphérique USB sélectionné sera formaté pendant la création d'ESET SysRescue. Toutes les données du périphérique seront supprimées.

Si vous choisissez l'option **Formatage rapide**, le formatage supprime tous les fichiers de la partition, mais ne recherche pas les secteurs défaillants. Utilisez cette option si votre périphérique USB a été formaté au préalable et que vous êtes certain qu'il n'est pas endommagé.

12.4.6 Graver

Si vous avez choisi CD/DVD en tant que support cible, vous pouvez définir les paramètres de gravure complémentaires sous l'onglet **Graver**.

Supprimer fichier ISO : cochez cette case pour supprimer le fichier ISO temporaire après la création du CD ESET SysRescue.

Suppression activée : permet de choisir entre la suppression rapide et la suppression complète.

Graveur : choisissez le lecteur à utiliser pour la gravure.

Avertissement : il s'agit de l'option par défaut. En cas d'utilisation d'un CD/DVD réinscriptible, toutes les données sur le CD/DVD seront supprimées.

La section Support contient des informations sur le support dans le lecteur de CD/DVD.

Vitesse de gravure : sélectionnez la vitesse souhaitée dans le menu déroulant. Les capacités du périphérique de gravure et le type de CD/DVD utilisé doivent être pris en compte lors de la sélection de la vitesse de gravure.

12.5 Utilisation de ESET SysRescue

Pour que les supports de récupération CD/DVD/USB fonctionnent efficacement, l'ordinateur doit être démarré depuis le support d'amorçage ESET SysRescue. La priorité d'amorçage peut être modifiée dans le BIOS. Vous pouvez aussi utiliser le menu d'amorçage lors du démarrage de l'ordinateur, généralement à l'aide d'une des touches entre F9 et F12 en fonction de la version de la carte mère/du BIOS.

Après l'amorçage à partir du support d'amorçage, la solution ESET Security démarre. Dans la mesure où ESET SysRescue est utilisé uniquement dans des situations particulières, certains modules de protection et fonctionnalités de l'application présents dans la version standard d'ESET Security ne sont pas requis ; la liste est réduite à **Analyse de l'ordinateur**, **Mise à jour** et certaines sections de **Configuration**. La capacité d'actualiser la base de signature des virus est la fonctionnalité la plus importante de ESET SysRescue ; nous vous recommandons de mettre à jour le programme avant de démarrer l'analyse de l'ordinateur.

12.5.1 Utilisation d'ESET SysRescue

Supposons que les ordinateurs du réseau ont été infectés par un virus qui modifie les fichiers exécutables (.exe). La solution ESET Security peut nettoyer tous les fichiers infectés, à l'exception de *explorer.exe* qui ne peut pas être nettoyé, même en mode sans échec. En tant que processus essentiel de Windows, le fichier *explorer.exe* est en effet lancé en mode sans échec également. La solution ESET Security ne pourrait effectuer aucune opération sur ce fichier et ce dernier resterait infecté.

Dans ce type de scénario, vous pouvez utiliser ESET SysRescue pour résoudre le problème. ESET SysRescue ne requiert aucun composant du système d'exploitation hôte et peut traiter (nettoyer, supprimer) n'importe quel fichier du disque.

13. Annexe – Licence tierce

ESET reconnaît que le Logiciel contient du code tiers sous les licences tierces suivantes :

3-clause BSD License ("New BSD License")
