ESET

REMOTE ADMINISTRATOR 6

Guide d'installation, de mise à niveau et de migration

Cliquez ici pour accéder à la dernière version de ce document.

ENJOY SAFER TECHNOLOGY™

ESET **REMOTE ADMINISTRATOR 6**

Service client : www.eset.com/support

RÉV. 19/01/2016

Table des

1. Installation/Mise à niveau....4

1.1 Fonctionnalités....4

1.2 Architecture....5

1.2.1 Serveur....5

1.2.2 Console Web....6

1.2.3 Agent....6

1.2.4 Proxy....7

1.2.5 Rogue Detection Sensor....8

1.2.6 Connecteur de périphérique mobile....9

1.2.7 Scénarios de déploiement....10

1.2.7.1 Serveur unique (petite entreprise)....10

1.2.7.2 Filiales distantes avec proxy....11

1.2.7.3 Haute disponibilité (entreprise)....12

1.2.8 Exemples pratiques de déploiement....13

1.3 Produits et langues pris en charge....14

2. Configuration système requise....16

2.1 Systèmes d'exploitation pris en charge....16

2.1.1 Windows....16

2.1.2 Linux....18

2.1.3 OS X....18

2.2 Matériel....19

2.3 Base de données....19

2.4 Ports utilisés....19

3. Processus d'installation....22

3.1 Installation sous Windows....22

3.1.1 Installation pas à pas sous Windows....23

3.1.1.1 Désinstaller des composants....33

3.1.2 Installation sur Windows SBS / Essentials....34

3.1.3 Installation du package....37

3.1.4 Installation de composants sur Windows....39

3.1.4.1 Installation du serveur - Windows....40

3.1.4.1.1 Conditions préalables requises pour le serveur - Windows....42

3.1.4.2 Microsoft SQL Server - Windows....43

3.1.4.3 Installation de l'Agent - Windows....43

3.1.4.4 Installation de la console Web - Windows....45

3.1.4.4.1 Navigateurs Web pris en charge....45

3.1.4.5 Installation du proxy - Windows....45

3.1.4.5.1 Conditions préalables requises pour le proxy - Windows....46

3.1.4.6 Installation de RD Sensor - Windows....46

3.1.4.6.1 Conditions préalables requises pour RD Sensor - Windows....46

3.1.4.7 Installation du Connecteur de périphérique mobile - Windows....47

3.1.4.7.1 Conditions préalables requises pour le Connecteur de périphérique mobile - Windows....50

3.1.4.8 Installation du proxy HTTP Apache - Windows....52

3.1.4.9 Outil Miroir....53

3.1.5 Cluster de basculement - Windows....55

3.2 Installation de composants sur Linux....56

3.2.1 Installation pas à pas sous Linux....56

3.2.2 Configuration MySQL....57

3.2.3 Configuration ODBC....58

3.2.4 Installation du serveur - Linux....58

3.2.4.1 Conditions préalables requises pour le serveur - Linux....61

3.2.5 Installation de l'Agent - Linux....62

3.2.5.1 Conditions préalables requises pour l'Agent - Linux....64

3.2.6 Installation d'ERA Web Console - Linux....64

3.2.6.1 Conditions préalables requises pour ERA Web Console - Linux....65

3.2.7 Installation du proxy - Linux....65

3.2.7.1 Conditions préalables requises pour le proxy - Linux....67

3.2.8 Installation et conditions préalables requises pour RD Sensor - Linux....67

3.2.9 Installation du Connecteur de périphérique mobile - Linux....68

3.2.9.1 Conditions préalables requises pour le Connecteur de périphérique mobile - Linux....69

3.2.10 Installation du proxy HTTP Apache - Linux....70

3.2.11 Installation du proxy HTTP Squid sur Ubuntu Server 14.10....73

3.2.12 Outil Miroir....73

3.2.13 Cluster de basculement - Linux....75

3.2.14 Comment désinstaller ou réinstaller un composant - Linux....77

3.3 Base de données....78

3.3.1 Sauvegarde du serveur de base de données....78

3.3.2 Mise à niveau du serveur de base de données....78

3.3.3 Migration de la base de données ERA....79

3.3.3.1 Processus de migration de SQL Server....79

3.3.3.2 Processus de migration de MySQL Server....87

3.4 Image ISO....88

3.5 Enregistrement du service DNS....89

4. Outil de migration....90

4.1 Scénario de migration 1....92

4.2 Scénario de migration 2....94

4.3 Scénario de migration 3....97

5. Procédures de mise à niveau....100

5.1 Mise à niveau des composants....100

5.2 scénario 2....106

6. Premières étapes....107

6.1 Ouverture d'ERA Web Console....108

7. Outil de diagnostic....109

8. FAQ....110

1. Installation/Mise à niveau

ESET Remote Administrator (ERA) est une application qui permet de gérer les produits ESET de manière centralisée sur les postes de travail clients, les serveurs et les périphériques mobiles dans un environnement réseau. Grâce au système de gestion de tâches intégré d'ESET Remote Administrator, vous pouvez installer les solutions de sécurité ESET sur des ordinateurs distants et réagir rapidement face à de nouveaux problèmes ou de nouvelles menaces.

ESET Remote Administrator ne protège pas directement contre les codes malveillants. La protection de votre environnement dépend de la présence d'une solution de sécurité ESET comme ESET Endpoint Security sur les postes de travail et les périphériques mobiles, ou ESET File Security pour Microsoft Windows Server sur les ordinateurs serveurs.

ESET Remote Administrator repose sur deux principes :

1. **Gestion centralisée** : tout le réseau peut être configuré, géré et surveillé à partir d'un seul et même emplacement.
2. **Évolutivité** : le système peut être déployé dans un réseau de petite taille et dans des environnements d'entreprise de grande taille. ESET Remote Administrator est conçu pour s'adapter à la croissance de votre infrastructure.

ESET Remote Administrator prend en charge la nouvelle génération de produits de sécurité ESET et est également compatible avec la génération précédente de produits.

Les pages d'aide d'ESET Remote Administrator incluent un guide complet d'installation et de mise à niveau :

- Architecture d'ESET Remote Administrator
- Outil de migration
- Processus d'installation
- ESET License Administrator
- Processus de déploiement et Déploiement de l'Agent à l'aide de GPO ou SCCM
- Premières étapes après l'installation d'ESET Remote Administrator
- Tâches de post-installation
- Administration

1.1 Fonctionnalités

Les fonctions et fonctionnalités suivantes sont nouvelles dans la version 6 :

- Indépendance des plateformes : ERA Server fonctionne sous Windows et Linux.
- Tâches de post-installation : vous indiquent comment tirer pleinement parti d'ESET Remote Administrator et vous guident tout au long des étapes recommandées pour une expérience utilisateur optimale.
- ERA Web Console, l'interface utilisateur principale d'ESET Remote Administrator, est accessible à l'aide de votre navigateur Web. Vous pouvez ainsi l'utiliser facilement à partir de n'importe quel emplacement et sur tous les périphériques.
- ESET License Administrator : ESET Remote Administrator doit être activé à l'aide d'une clé de licence émise par ESET avant de pouvoir être utilisé. Reportez-vous à la section ESET License Administrator pour des instructions sur l'activation de votre produit, ou consultez l'aide en ligne d'ESET License Administrator pour en savoir plus sur l'utilisation d'ESET License Administrator.
- Un tableau de bord entièrement personnalisable vous donne une vue d'ensemble de l'état de sécurité du réseau. En outre, la section Admin de la console Web d'ESET Remote Administrator (console Web ERA) constitue un outil convivial puissant pour gérer les produits ESET.
- ERA Agent : ERA Agent doit être installé sur tous les ordinateurs clients qui communiquent avec ERA Server.
- Les notifications vous donnent des informations pertinentes en temps réel et les rapports vous permettent de trier efficacement divers types de données que vous pouvez utiliser ultérieurement.

1.2 Architecture

ESET Remote Administrator est une nouvelle génération de système de gestion à distance, très différente des versions précédentes de ESET Remote Administrator. Parce que son architecture est totalement différente, la solution n'est pas rétrocompatible avec l'ancienne génération d'ESET Remote Administrator. Toutefois, la compatibilité est maintenue avec les versions précédentes des produits de sécurité ESET.

En même temps que le nouvel ESET Remote Administrator, ESET a aussi lancé une nouvelle génération de produits de sécurité avec un nouveau système de licences.

Pour effectuer un déploiement complet du portefeuille de solutions de sécurité ESET, les composants suivants doivent être installés (plates-formes Windows et Linux) :

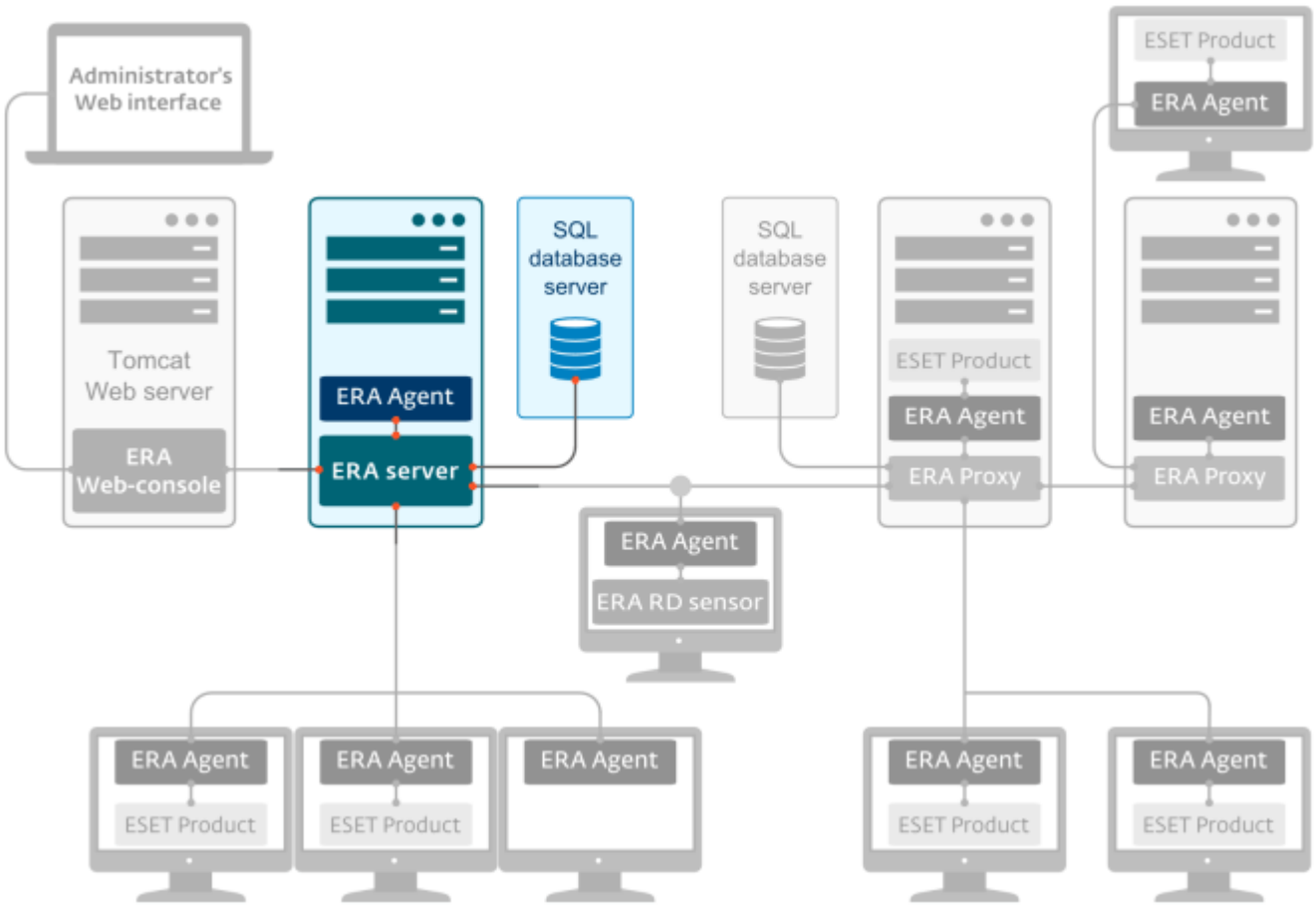
- ERA Server
- ERA Web Console
- ERA Agent

Bien que les composants de prise en charge suivants soient facultatifs, il est recommandé de les installer pour optimiser les performances de l'application sur le réseau :

- ERA Proxy
- RD Sensor
- Connecteur de périphérique mobile

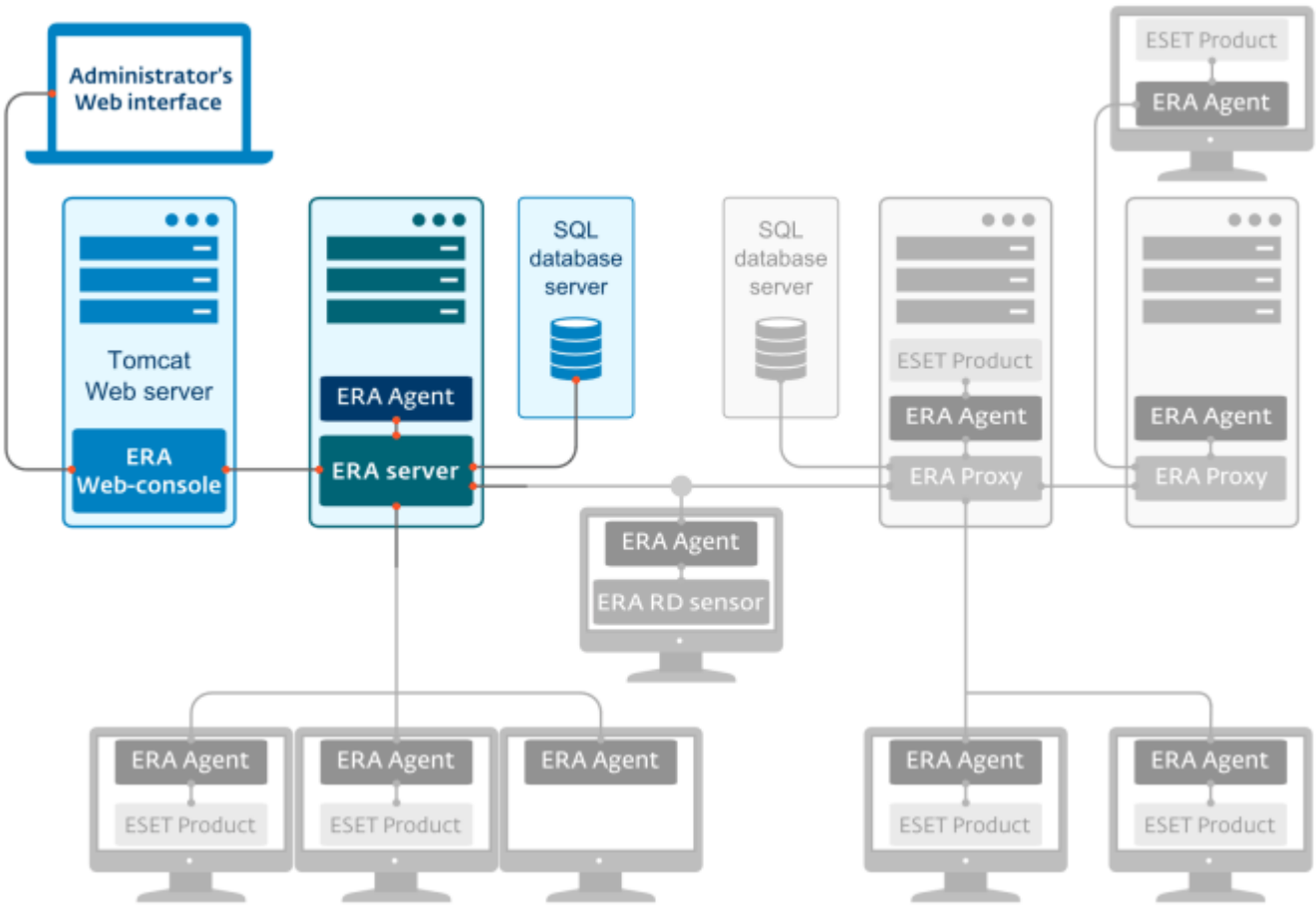
1.2.1 Serveur

ESET Remote Administrator Server (ERA Server) est l'application d'exécution qui traite toutes les données reçues des clients se connectant au serveur (par le biais d'ERA Agent). Pour traiter correctement les données, ERAS requiert une connexion stable à un serveur de base de données où sont stockées les données réseau. Il est recommandé d'installer le serveur de base de données sur un autre ordinateur pour des performances optimales.



1.2.2 Console Web

ERA Web Console est une interface utilisateur Web qui vous permet de gérer les solutions de sécurité ESET dans votre environnement. Elle affiche une vue d'ensemble de l'état des clients sur le réseau et peut être utilisée pour déployer à distance les solutions ESET sur des ordinateurs non gérés. Elle est accessible à l'aide de votre navigateur (voir Navigateurs Web pris en charge). Si vous décidez de rendre le serveur Web accessible à partir d'Internet, vous pouvez utiliser ESET Remote Administrator à partir de presque n'importe quel emplacement, sur presque tous les périphériques.



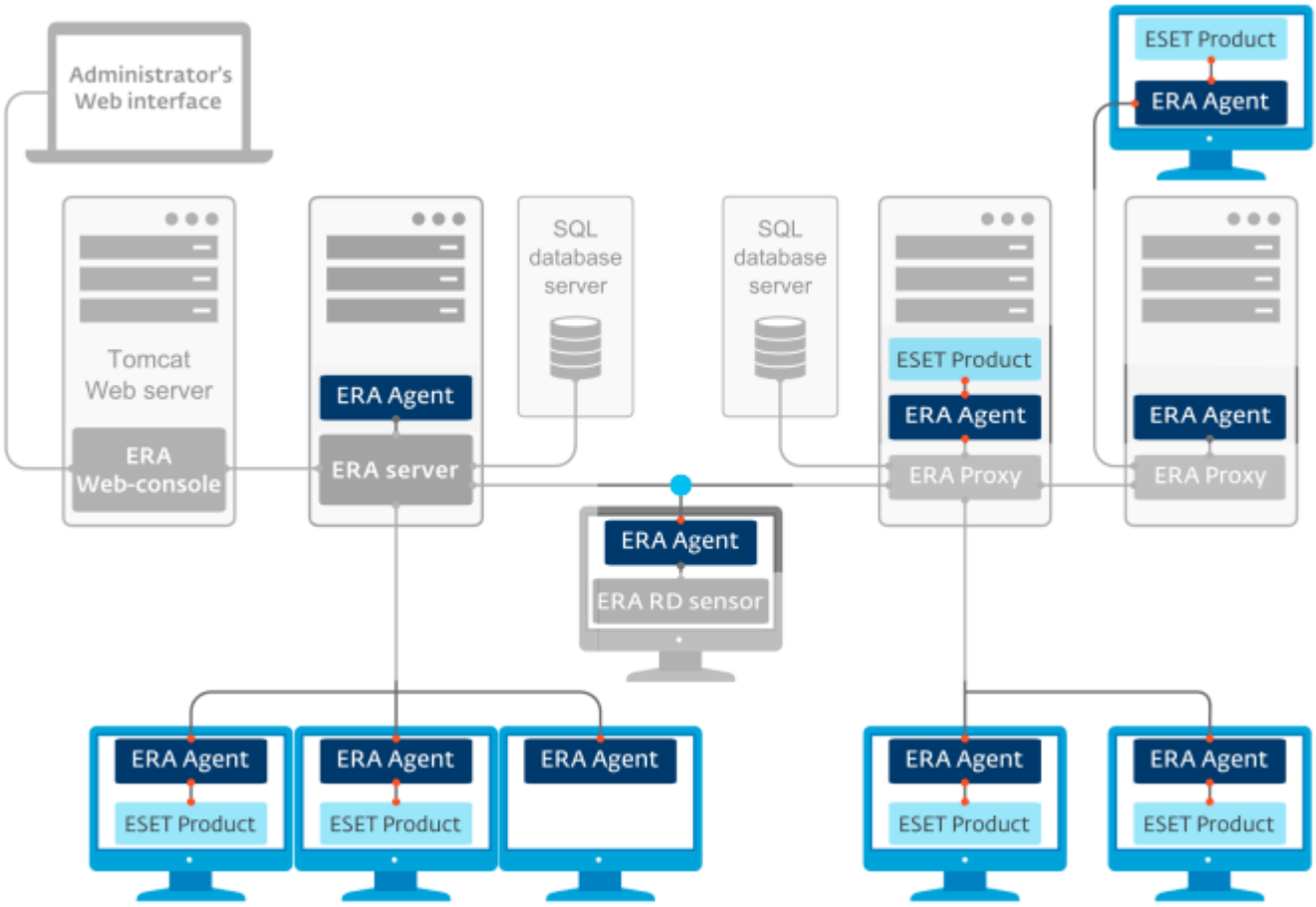
1.2.3 Agent

ESET Remote Administrator Agent (ERA Agent) est un composant essentiel d'ESET Remote Administrator 6. Les clients ne communiquent pas directement avec le serveur, c'est l'Agent qui facilite cette communication. L'Agent collecte les informations du client et les envoie à ERA Server. Si ERA Server envoie une tâche destinée au client, celle-ci est envoyée à l'Agent qui l'envoie à son tour au client.

Pour simplifier la mise en œuvre de la protection des points de terminaison, le composant ERA Agent autonome est inclus dans la suite ERA (à partir de la version 6). Il s'agit d'un service simple, léger et hautement modulaire qui couvre toutes les communications entre ERA Server et les autres produits ESET ou systèmes d'exploitation. Au lieu de communiquer directement avec ERA Server, les produits ESET communiquent par le biais de l'Agent. Les ordinateurs clients qui disposent d'ESET Agent et qui peuvent communiquer avec ERA Server sont appelés ordinateurs administrés. Vous pouvez installer l'Agent sur n'importe quel ordinateur, qu'un autre logiciel ESET soit installé ou non.

Les avantages sont les suivants :

- Installation aisée : il est possible de déployer l'Agent dans le cadre d'une installation d'entreprise standard.
- Gestion de la sécurité sur place : dans la mesure où l'Agent peut être configuré pour stocker plusieurs scénarios de sécurité, le temps de réaction face aux menaces est considérablement réduit.
- Gestion de la sécurité hors ligne : l'Agent peut répondre à un événement s'il n'est pas connecté à ERA Server.



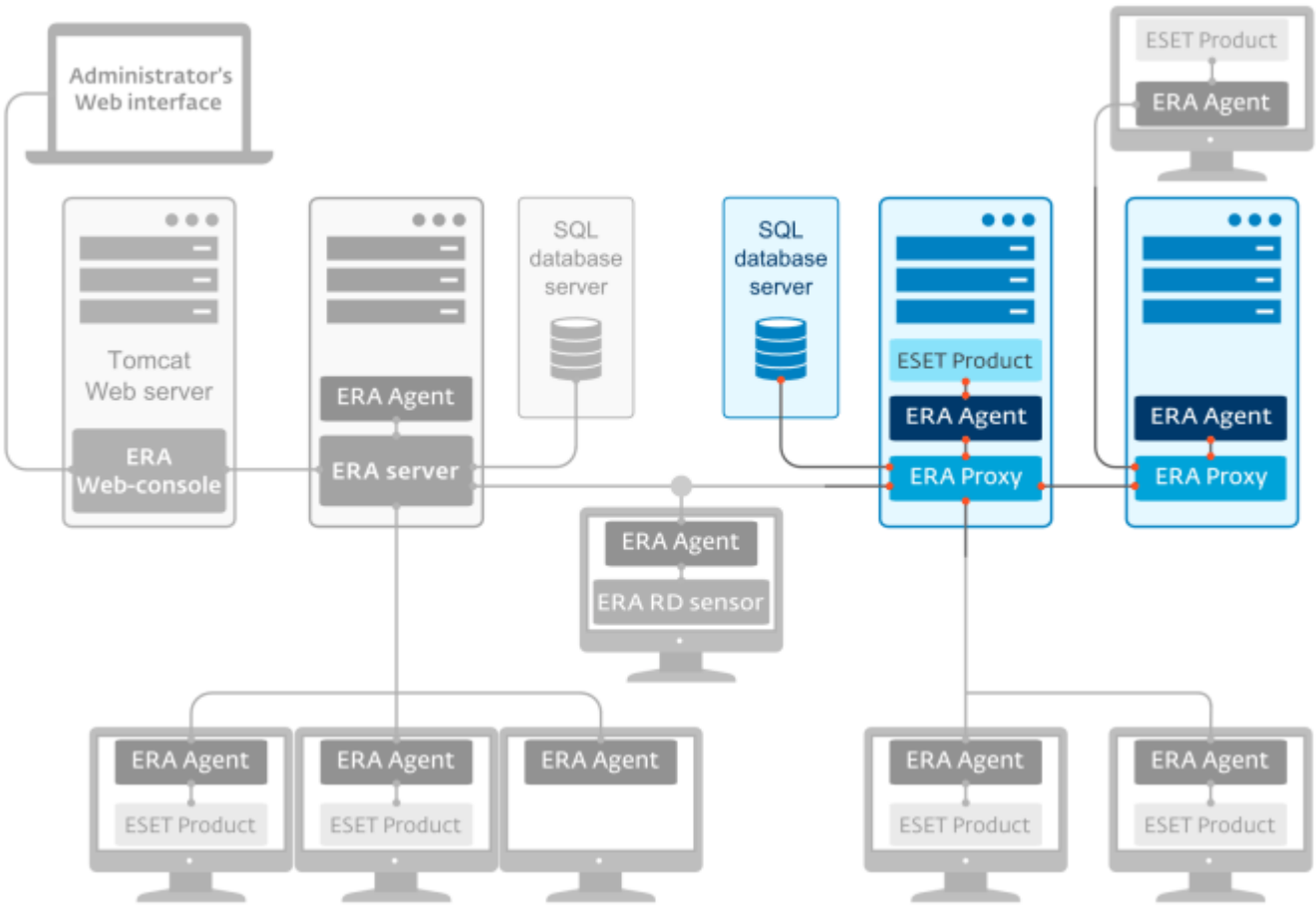
1.2.4 Proxy

Le serveur **ERA Proxy** est une version légère du composant serveur. Ce type de serveur est utilisé pour offrir un degré élevé d'évolutivité. Le serveur ERA Proxy permet de concentrer le trafic des Agents clients. Il autorise la connexion de plusieurs Agents et il redistribue ensuite le trafic à ERA Server. Les requêtes de base de données sont ainsi optimisées. ERA Proxy peut également se connecter à d'autres serveurs proxy puis à ERA Server. Cela dépend de l'environnement réseau et de sa configuration.

ERA Proxy est également chargé de la distribution passive des données de configuration (groupes, stratégies, tâches, etc.) aux Agents. Ce transfert est effectué sans aucune implication d'ERA Server.

Le seul moyen de configurer ERA Proxy (et tous les autres composants) est par le biais d'une stratégie envoyée par ERA Server. Cela signifie que l'Agent doit être installé sur l'ordinateur ERA Proxy pour remettre la configuration d'ERA Server au composant ERA Proxy.

REMARQUE : ERA Server ne peut pas se connecter directement au serveur ERA Proxy sans l'Agent.



ERA Proxy est un autre composant d'ESET Remote Administrator qui a un double objectif. Dans le cas d'un réseau d'entreprise de taille moyenne qui comprend de nombreux clients (10 000 clients ou plus), ERA Proxy peut servir à répartir la charge entre plusieurs ERA Proxy, et décharger ainsi ERA Server. L'autre avantage d'ERA Proxy est que vous pouvez l'utiliser lors de la connexion à une filiale distante qui possède une liaison faible. Cela signifie qu'ERA Agent sur chaque client ne se connecte pas directement à ERA Server mais par le biais d'ERA Proxy qui se trouve sur le même réseau local que la filiale. Cette configuration améliore les communications avec la filiale. ERA Proxy accepte les connexions de tous les ERA Agents locaux, compile leurs données et les télécharge sur ERA Server (ou un autre ERA Proxy). Votre réseau peut ainsi prendre en charge davantage de clients sans compromettre les performances du réseau et des requêtes de base de données.

Pour qu'ERA Proxy fonctionne correctement, l'ordinateur hôte sur lequel vous avez installé ERA Proxy doit disposer d'un ESET Agent et être connecté au niveau supérieur (ERA Server ou ERA Proxy supérieur, le cas échéant) du réseau.

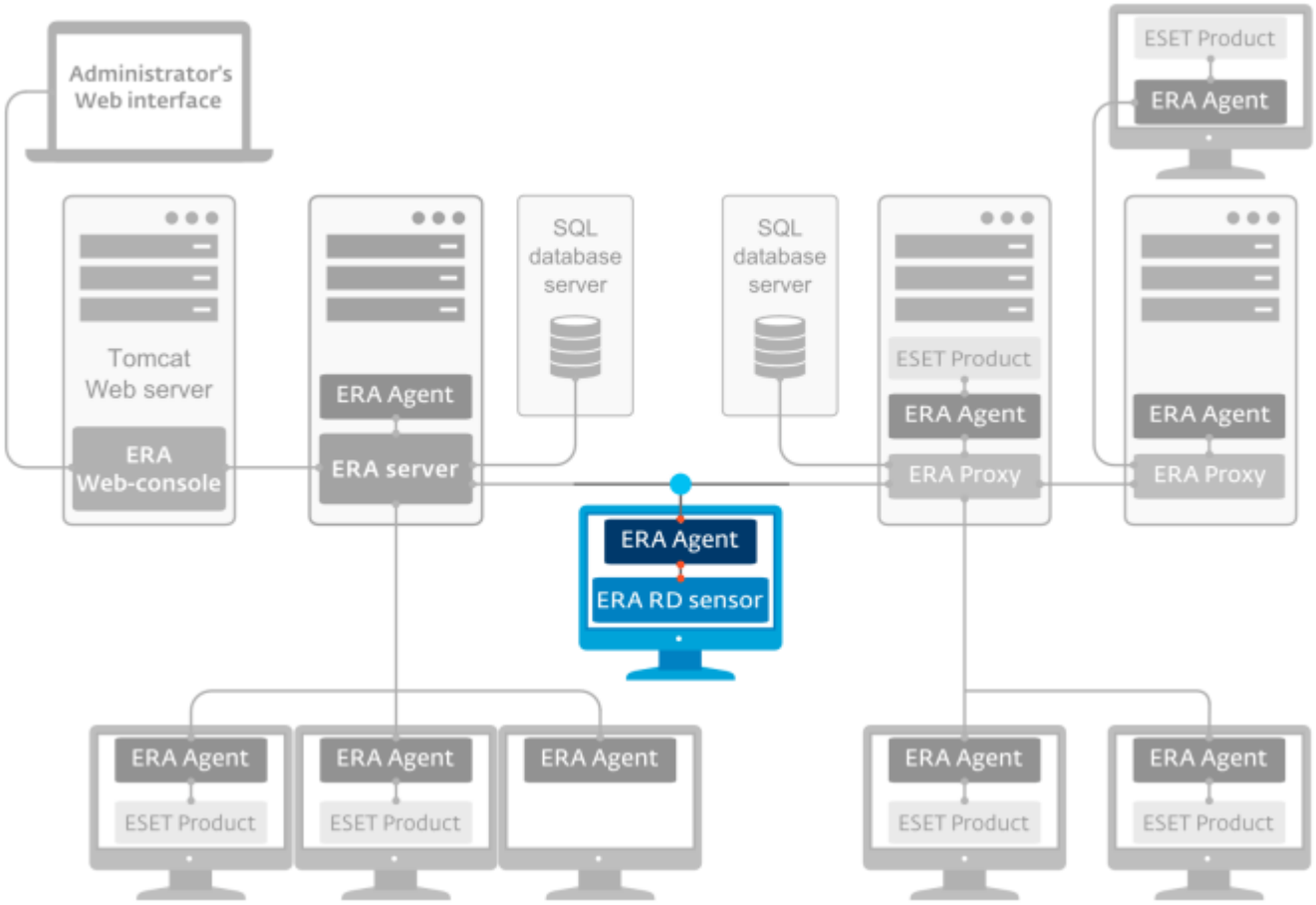
REMARQUE : reportez-vous au scénario de déploiement avec ERA Proxy.

1.2.5 Rogue Detection Sensor

Rogue Detection Sensor (RD Sensor) est un outil de détection de serveurs non autorisés qui recherche des ordinateurs sur le réseau. Il s'avère très utile, car il peut détecter de nouveaux ordinateurs à partir d'ESET Remote Administrator sans avoir à les rechercher et à les ajouter manuellement. Les ordinateurs détectés sont immédiatement localisés et signalés dans un rapport prédéfini, ce qui permet de les déplacer vers des groupes statiques spécifiques et d'effectuer des tâches de gestion.

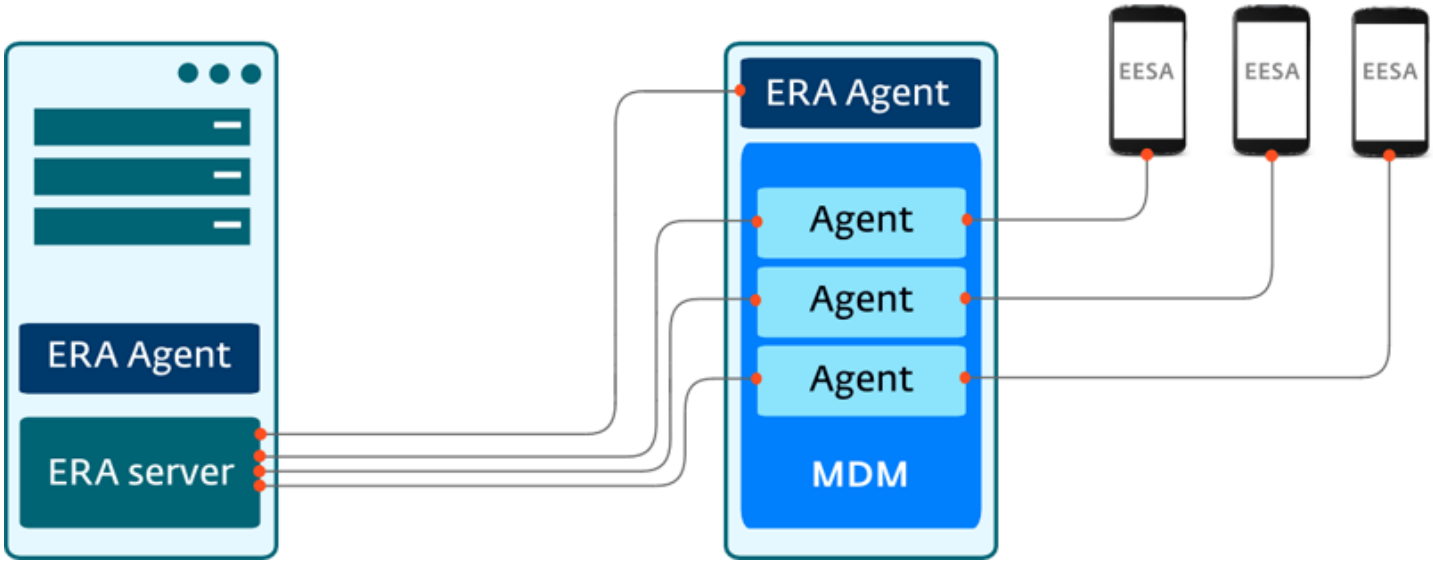
RD Sensor est un écouteur passif qui détecte les ordinateurs qui se trouvent sur le réseau et envoie des informations sur ces derniers à ERA Server. ERA Server évalue ensuite si les ordinateurs trouvés sur le réseau sont inconnus ou déjà gérés.

Chaque ordinateur au sein de la structure réseau (domaine, LDAP, réseau Windows) est ajouté automatiquement à la liste des ordinateurs d'ERA Server par le biais d'une tâche de synchronisation de serveur. Utiliser RD Sensor s'avère utile pour détecter les ordinateurs ne se trouvant pas dans le domaine ou une autre structure réseau et pour les ajouter à ESET Remote Administrator Server. Cet outil mémorise les ordinateurs déjà découverts et n'envoie pas deux fois les mêmes informations.



1.2.6 Connecteur de périphérique mobile

Le **Connecteur de périphérique mobile (ESET MDC)** est une application qui vous permet de gérer les périphériques mobiles et d'administrer ESET Endpoint Security pour Android.



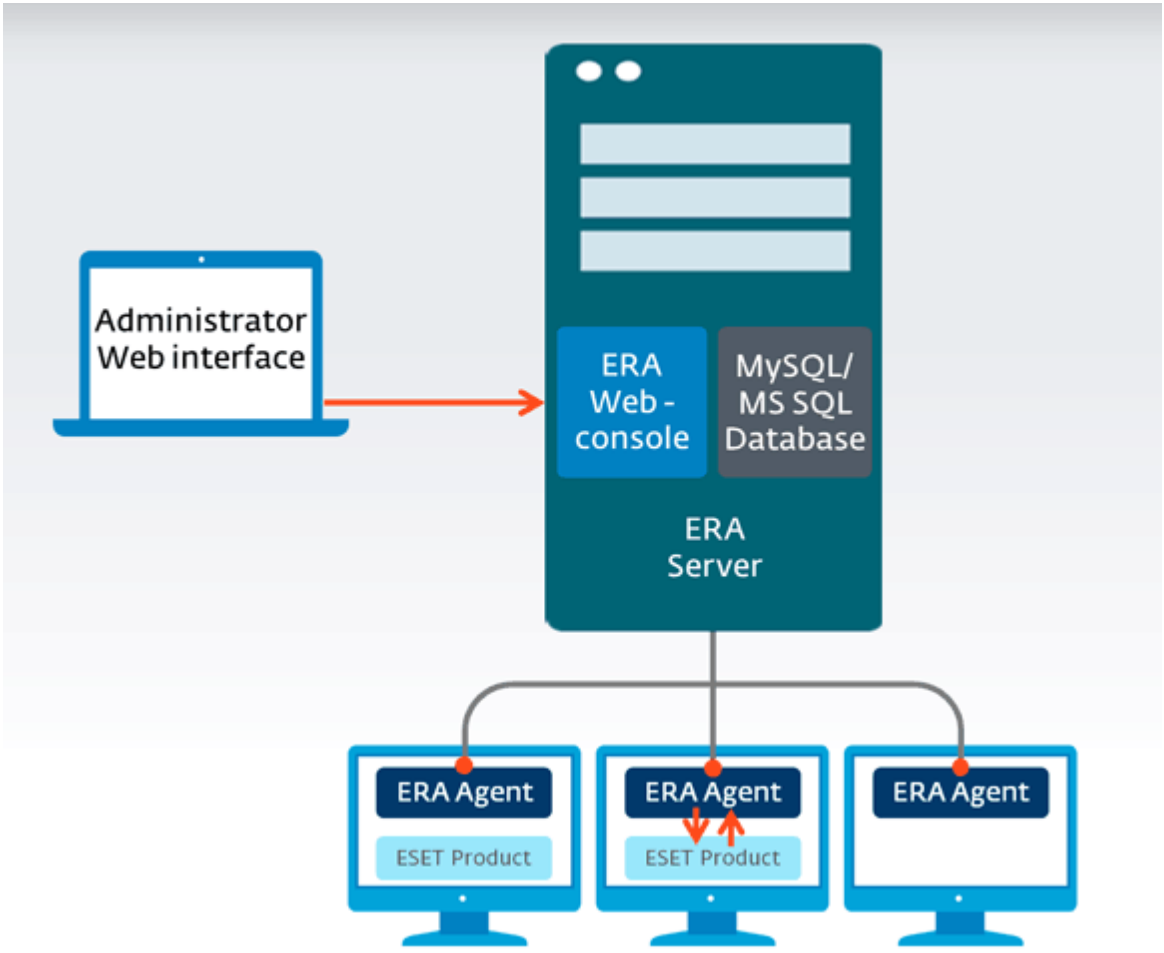
1.2.7 Scénarios de déploiement

Les chapitres suivants traitent de scénarios de déploiement pour différents environnements réseau. Pour obtenir des instructions détaillées, reportez-vous au chapitre adéquat :

- Serveur unique (petite entreprise)
- Haute disponibilité (entreprise)
- Filiales distantes avec proxy

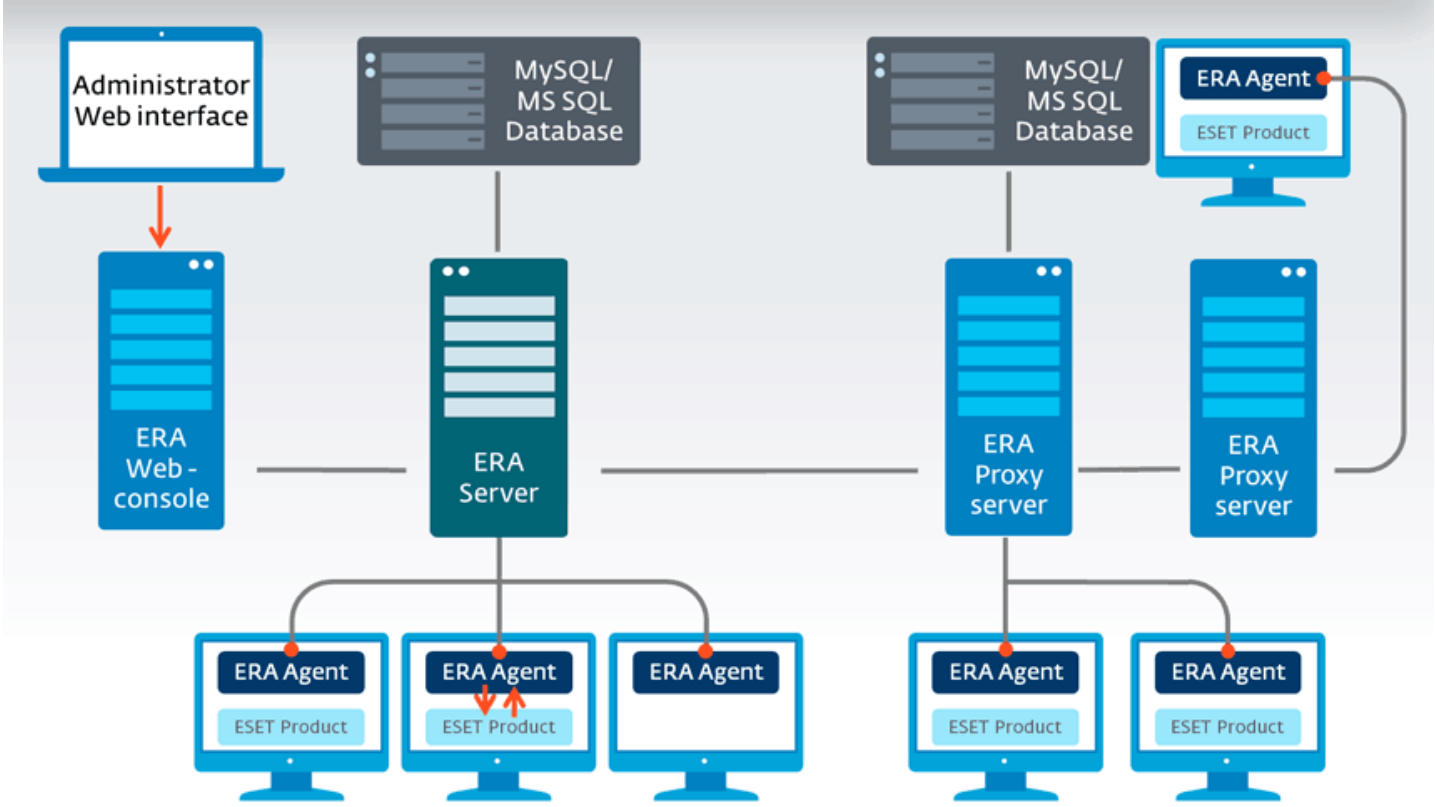
1.2.7.1 Serveur unique (petite entreprise)

Pour gérer des réseaux de petite taille (1 000 clients ou moins), un ordinateur unique sur lequel est installé ERA Server et tous les composants (serveur Web, base de données) est généralement suffisant. Vous pouvez comparer cette configuration à une installation autonome ou de serveur unique. Tous les clients administrés sont directement connectés à ERA Server par le biais d'ERA Agent. L'administrateur peut se connecter à ERA Web Console par l'intermédiaire d'un navigateur Web depuis n'importe quel ordinateur du réseau ou exécuter directement la console Web à partir d'ERA Server.



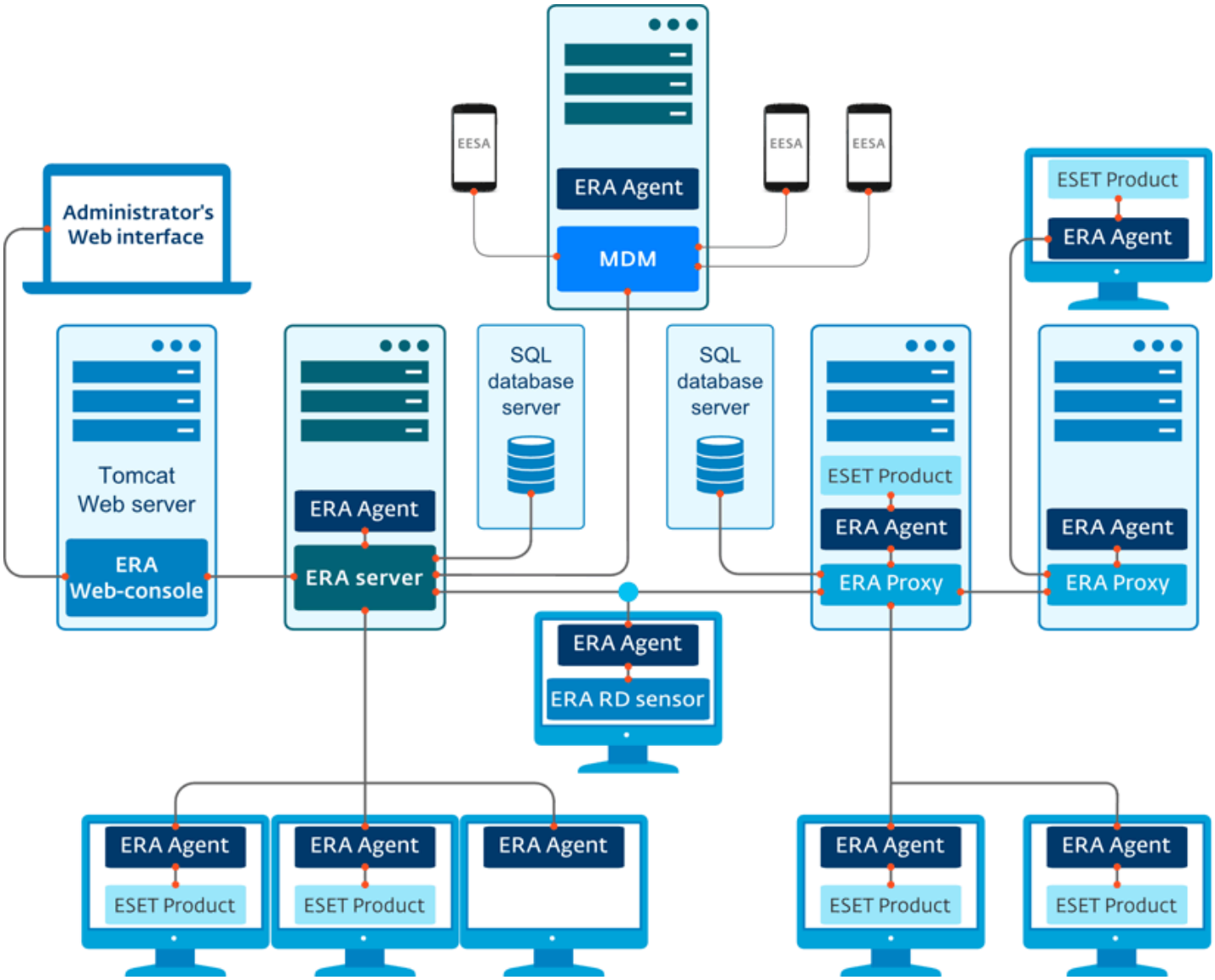
1.2.7.2 Filiales distantes avec proxy

Dans un réseau de taille moyenne (10 000 clients par exemple), une couche supplémentaire composée de serveurs ERA Proxy est ajoutée. Les ERA Agents sont connectés au serveur ERA Proxy. La raison de l'ajout du serveur ERA Proxy peut être une liaison faible au site distant (filiale). Il est toutefois toujours possible de connecter les ERA Agents (situés à un site distant) directement au serveur principal.



1.2.7.3 Haute disponibilité (entreprise)

Pour les environnements d'entreprise (100 000 clients, par exemple), d'autres composants ERA doivent être utilisés. L'un de ces composants est RD Sensor. Il permet de découvrir de nouveaux ordinateurs sur votre réseau. Un autre ajout est une couche de serveurs proxy ERA. Les ERA Agents sont connectés au serveur proxy ERA, ce qui permet d'équilibrer la charge sur le serveur principal (ce qui est important pour les performances). À l'aide de cette configuration, il est toujours possible de connecter les ERA Agents directement au serveur principal. Une base de données SQL est également mise en œuvre sur un cluster de basculement pour assurer la redondance.



1.2.8 Exemples pratiques de déploiement

Pour des performances optimales, il est recommandé d'utiliser Microsoft SQL Server en tant que base de données ESET Remote Administrator. Bien qu'ESET Remote Administrator soit compatible avec MySQL, l'utilisation de MySQL peut avoir un impact négatif sur les performances du système lors de l'utilisation de grandes quantités de données (tableaux de bord, menaces et clients compris). Avec Microsoft SQL Server, un même matériel est capable de gérer 10 fois plus de clients qu'avec MySQL.

À des fins de test, chaque client stocke environ 30 journaux dans la base de données. Microsoft SQL Server utilise de grandes quantités de mémoire vive (RAM) pour mettre en cache les données de la base de données. Il est donc recommandé de disposer d'autant de mémoire que Microsoft SQL Server sur disque.

Comme les ressources varient selon la configuration réseau, il est difficile de calculer la quantité exacte de ressources utilisées par ESET Remote Administrator. Vous trouverez ci-dessous des résultats de test pour des configurations réseau courantes :

- Cas de test : 5 000 clients au maximum se connectant à ERA Server
- Cas de test : 100 000 clients au maximum se connectant à ERA Server

Pour une configuration optimale répondant à vos besoins, il est recommandé d'effectuer un test avec un plus petit nombre de clients et un matériel plus lent, puis d'évaluer la configuration système requise selon les résultats du test.

CAS DE TEST (5 000 CLIENTS)

Matériel/logiciels

- Windows Server 2003 R2, architecture de processeur x86
- Microsoft SQL Server Express 2008 R2
- Intel Core2Duo E8400 cadencé à 3 GHz
- 3 Go de mémoire vive (RAM)
- Seagate Barracuda 7 200 tours/min, 500 Go, 16 Mo de cache, Sata 3,0 Gb/s

Résultats

- ERA Web Console est très réactif (moins de 5 s).
- Utilisation de la mémoire :
  - Apache Tomcat : 200 Mo
  - ERA Server : 200 Mo
  - Base de données SQL Server : 1 Go
- Performances de réplication du serveur : 10 réplications par seconde
- Taille de la base de données sur disque : 1 Go (5 000 clients, chacun avec 30 journaux dans la base de données)

Dans cet exemple, SQL Server Express 2008 R2 a été utilisé. En dépit des limites de SQL Server Express 2008 R2, (base de données de 10 Go, 1 CPU et 1 Go d'utilisation de RAM), cette configuration était fonctionnelle et performante. L'utilisation de SQL Server Express est recommandée pour les serveurs prenant en charge moins de 5 000 clients. Vous pouvez déployer initialement SQL Server Express et effectuer ensuite une mise à niveau vers Microsoft SQL Server (version complète) lorsqu'une base de données plus volumineuse devient nécessaire. Notez que les anciennes versions de SQL Server Express (postérieures à la version 2008 R2) présentent une limite de taille de base de données de 4 Go sur disque.

Les performances de réplication du serveur définissent un intervalle de réplication pour les clients. 10 réplications par seconde équivalent à 600 réplications par minute. Dans un cas idéal, l'intervalle de réplication sur 5 000 clients doit donc être défini sur 8 minutes. Comme cela implique toutefois une charge de 100 % sur le serveur, un intervalle plus long est donc nécessaire. Dans cet exemple, un intervalle compris entre 20 et 30 minutes est recommandé.

CAS DE TEST (100 000 CLIENTS)

Matériel/logiciels

- Windows Server 2012 R2 Datacenter, architecture de processeur x64
- Microsoft SQL Server 2012
- Intel Xeon E5-2650v2 cadencé à 2,60 GHz
- 64 Go de mémoire vive (RAM)
- Carte réseau Intel NIC/PRO/1000 PT Dual
- 2 lecteurs SSD Micron RealSSD C400 de 256 Go (un pour le système+logiciels, l'autre pour les fichiers de données SQL Server)

Résultats

- La console Web est réactive (moins de 30 s).
- Utilisation de la mémoire :
  - Apache Tomcat : 1 Go
  - ERA Server : 2 Go
  - Base de données SQL Server : 10 Go
- Performances de réplication du serveur : 80 réplications par seconde
- Taille de la base de données sur disque : 10 Go (100 000 clients, chacun avec 30 journaux dans la base de données)

Dans ce cas, tous les composants (Apache Tomcat + console Web, ERA Server et SQL Server) ont été installés sur un ordinateur pour tester les capacités d'ERA Server.

En raison du grand nombre de clients, l'utilisation du disque et de la mémoire par Microsoft SQL Server a augmenté. Pour des performances optimales, SQL Server effectue une mise en cache presque intégrale à partir de la base de données stockée dans la mémoire. Comme Apache Tomcat (console Web) et ERA Server mettent également en cache les données, cela explique l'augmentation de l'utilisation de la mémoire dans cet exemple.

ERA Server est capable de prendre en charge 80 réplications par seconde (288 000 par heure). Dans un cas idéal, l'intervalle de réplication sur les 100 000 clients doit être défini sur 30 minutes (charge de 200 000 réplications par heure). Pour éviter une charge de 100 % sur le serveur, l'intervalle de réplication doit être toutefois défini sur 1 heure (100 000 réplications par heure).

L'utilisation des données réseau dépend du nombre de journaux collectés par les clients. Dans ce test, ce nombre était environ de 20 Ko par réplication, soit une vitesse du réseau de 1 600 Ko/s (20 Mbps) pour 80 réplications par seconde.

Dans cet exemple, un serveur unique a été utilisé. La charge réseau et de CPU est mieux répartie en utilisant plusieurs ERA Proxy (plus ils sont nombreux, mieux c'est). La charge réseau et de CPU est ainsi répartie lors de la diffusion des réplications clientes. Répartir la charge réseau est conseillé, tout particulièrement pour les clients distants. L'intervalle de réplication des proxy vers le serveur peut être défini en dehors des heures de travail lorsque la vitesse du réseau depuis des emplacements distants est plus rapide.

1.3 Produits et langues pris en charge

ESET Remote Administrator peut déployer, activer et gérer les produits ESET suivants :

Gérable par le biais d'ESET Remote Administrator 6	Version du produit	Méthode d'activation
ESET Endpoint Security pour Windows	6.x et 5.x	6.x - Clé de licence 5.x - Nom d'utilisateur/mot de passe
ESET Endpoint Antivirus pour Windows	6.x et 5.x	6.x - Clé de licence 5.x - Nom d'utilisateur/mot de passe
ESET Endpoint Security pour OS X	6.x	Clé de licence

Gérable par le biais d'ESET Remote Administrator 6	Version du produit	Méthode d'activation
ESET Endpoint Antivirus pour OS X	6.x	Clé de licence
ESET Endpoint Security pour Android	2.x	Clé de licence
ESET File Security pour Windows Server	6.x	Clé de licence
ESET Mail Security pour Microsoft Exchange Server	6.x	Clé de licence
ESET File Security pour Microsoft Windows Server	4.5.x	Nom d'utilisateur/mot de passe
ESET NOD32 Antivirus 4 Business Edition pour Mac OS X	4.x	Nom d'utilisateur/mot de passe
ESET NOD32 Antivirus 4 Business Edition pour Linux Desktop	4.x	Nom d'utilisateur/mot de passe
ESET Mail Security pour Microsoft Exchange Server	4.5.x	Nom d'utilisateur/mot de passe
ESET Mail Security pour IBM Lotus Domino	4.5.x	Nom d'utilisateur/mot de passe
ESET Security pour Microsoft Windows Server Core	4.5.x	Nom d'utilisateur/mot de passe
ESET Security pour Microsoft SharePoint Server	4.5.x	Nom d'utilisateur/mot de passe
ESET Security pour Kerio	4.5.x	Nom d'utilisateur/mot de passe
ESET NOD32 Antivirus Business Edition	4.2.76	Nom d'utilisateur/mot de passe
ESET Smart Security Business Edition	4.2.76	Nom d'utilisateur/mot de passe

REMARQUE : les versions des produits ESET Windows Server antérieures à celles indiquées dans le tableau ci-dessus ne sont pas actuellement gérables à l'aide de ESET Remote Administrator.

Langues prises en charge

Langue	Code
Anglais (États-Unis)	en-US
Arabe (Égypte)	ar-EG
Chinois simplifié	zh-CN
Chinois traditionnel	zh-TW
Croate (Croatie)	hr-HR
Tchèque (République tchèque)	cs-CZ
Français (France)	fr-FR
Français (Canada)	fr-FC
Allemand (Allemagne)	de-DE
Italien (Italie)	it-IT
Japonais (Japon)	ja-JP
Coréen (Corée)	ko-KR
Polonais (Pologne)	pl-PL
Portugais (Brésil)	pt-BR
Russe (Russie)	ru-RU
Espagnol (Chili)	es-CL
Espagnol (Espagne)	es-ES
Slovaque (Slovaquie)	sk-SK

2. Configuration système requise

Pour installer ESET Remote Administrator, vous devez remplir un ensemble de conditions préalables requises en ce qui concerne le matériel, la base de données et les logiciels.

2.1 Systèmes d'exploitation pris en charge

Les sections suivantes indiquent les versions de système d'exploitation prises en charge sous Windows, Linux et Mac OS par un composant spécifique d'ESET Remote Administrator.

2.1.1 Windows

Le tableau ci-après répertorie tous les systèmes d'exploitation pris en charge pour chaque composant ESET Remote Administrator. Il est également possible d'installer ERA Server, ERA Proxy et MDM sur un système d'exploitation client (*Microsoft Windows 7, 8, 8.1, 10), mais **uniquement à des fins d'évaluation**.

Système d'exploitation	Serveur	Agent	Proxy	RD Sensor	MDM
Windows XP x86 SP3		X		X	
Windows XP x64 SP2		X		X	
Windows Vista x86 SP2		X		X	
Windows Vista x64 SP2		X		X	
Windows 7 x86 SP1	*	X	*	X	*
Windows 7 x64 SP1	*	X	*	X	*
Windows 8 x86	*	X	*	X	*
Windows 8 x64	*	X	*	X	*
Windows 8.1 x86	*	X	*	X	*
Windows 8.1 x64	*	X	*	X	*
Windows 10 x86	*	X	*		
Windows 10 x64	*	X	*		
Windows HomeServer 2003 SP2		X		X	
Windows HomeServer 2011 x64		X		X	
Windows Server 2003 x86 SP2	X	X	X	X	
Windows Server 2003 x64 SP2	X	X	X	X	
Windows Server 2003 x86 R2 SP2	X	X	X	X	
Windows Server 2003 x64 R2 SP2	X	X	X	X	
Windows Server 2008 x64 R2 SP1	X	X	X	X	X
Windows Server 2008 x64 R2 CORE	X	X	X	X	X
Windows Server 2008 x86		X		X	
Windows Server 2008 x86 SP2	X	X	X	X	X
Windows Server 2008 x64		X		X	
Windows Server 2008 x64 SP2	X	X	X	X	X
Windows Server 2012 x64	X	X	X	X	X
Windows Server 2012 x64 CORE	X	X	X	X	X
Windows Server 2012 x64 R2	X	X	X	X	X
Windows Server 2012 x64 R2 CORE	X	X	X	X	X
Microsoft SBS 2003 x86 SP2 **	X	X	X	X	X

Microsoft SBS 2003 x86 R2 **	X	X	X	X	X
Microsoft SBS 2008 x64		X		X	
Microsoft SBS 2008 x64 SP2 **	X	X	X	X	X
Microsoft SBS 2011 x64 Standard	X	X	X	X	X
Microsoft SBS 2011 x64 Essential	X	X	X	X	X

*** Les composant ERA s'exécutant sur les systèmes d'exploitation clients (à des fins d'évaluation uniquement).**

**** Microsoft SQL Server Express inclus avec Microsoft Small Business Server (SBS) n'est pas pris en charge par ESET Remote Administrator**. Si vous souhaitez exécuter la base de données ERA sur SBS, vous devez utiliser une version plus récente de Microsoft SQL Server. Pour obtenir des informations supplémentaires et des instructions, reportez-vous à la section Installation sur Windows SBS / Essentials**.**

Sur les systèmes anciens, tels que Windows Server 2003, il est possible que le chiffrement de protocole ne soit pas entièrement pris en charge du côté du système d'exploitation. Pour cette raison, TLSv1.0 est utilisé à la place de TLSv1.2, (TLSv1.0 est considéré comme étant moins sûr que les versions plus récentes). Cette situation peut également se produire lorsque le système d'exploitation prend en charge TLSv1.2 mais pas le client. Dans ce cas, les communications sont établies à l'aide de TLS1.0. Afin de renforcer la sécurité de vos communications, il est conseillé d'utiliser des systèmes d'exploitation plus récents (Windows Server 2008 R2 et versions ultérieures pour les serveurs, Windows Vista et versions ultérieures pour les clients).

REMARQUE : il est possible d'installer sur un système d'exploitation de bureau et de déployer l'appliance virtuelle d'ESET Remote Administrator. Vous pouvez ainsi exécuter ESET Remote Administrator sur un système d'exploitation autre que serveur sans ESXi.

2.1.2 Linux

Système d'exploitation	Serveur	Agent	Proxy	RD Sensor	MDM
Ubuntu 12.04 LTS x86 Desktop	X	X	X	X	X
Ubuntu 12.04 LTS x86 Server	X	X	X	X	X
Ubuntu 12.04 LTS x64 Desktop	X	X	X	X	X
Ubuntu 12.04 LTS x64 Server	X	X	X	X	X
Ubuntu 14.04 LTS x86 Desktop	X	X	X	X	X
Ubuntu 14.04 LTS x86 Server	X	X	X	X	X
Ubuntu 14.04 LTS x64 Desktop	X	X	X	X	X
Ubuntu 14.04 LTS x64 Server	X	X	X	X	X
RHEL 5 x86		X			
RHEL 5 x64		X			
RHEL Server 6 x86	X	X	X	X	X
RHEL Server 6 x64	X	X	X	X	X
RHEL Server 7 x86	X	X	X	X	X
RHEL Server 7 x64	X	X	X	X	X
CentOS 5 x86		X			
CentOS 5 x64		X			
CentOS 6 x86	X	X	X	X	X
CentOS 6 x64	X	X	X	X	X
CentOS 7 x86	X	X	X	X	X
CentOS 7 x64	X	X	X	X	X
SLED 11 x86	X	X	X	X	X
SLED 11 x64	X	X	X	X	X
SLES 11 x86	X	X	X	X	X
SLES 11 x64	X	X	X	X	X
OpenSUSE 13 x86	X	X	X	X	X
OpenSUSE 13 x64	X	X	X	X	X
Debian 7 x86	X	X	X	X	X
Debian 7 x64	X	X	X	X	X
Fedora 19 x86	X	X	X	X	X
Fedora 19 x64	X	X	X	X	X
Fedora 20 x86	X	X	X	X	X
Fedora 20 x64	X	X	X	X	X

2.1.3 OS X

Système d'exploitation	Agent
OS X 10.7 Lion	X
OS X 10.8 Mountain Lion	X
OS X 10.9 Mavericks	X
OS X 10.10 Yosemite	X

REMARQUE : OS X est pris en charge en tant que client uniquement. Il est impossible d'installer ERA Server sous OS X.

2.2 Matériel

Pour garantir le fonctionnement correct du produit ESET Remote Administrator, votre système doit répondre à la configuration matérielle suivante :

Mémoire	4 Go de mémoire vive (RAM)
Disque dur	20 Go au minimum d'espace libre
Processeur	Double cœur, cadencé à 2,0 GHz ou plus rapide
Connexion réseau	1 Gbit/s

2.3 Base de données

ESET Remote Administrator prend en charge deux types de serveurs de base de données :

- Microsoft SQL Server (y compris les éditions Express et autres qu'Express) 2008, 2008 R2, 2012, 2014
- MySQL (version 5.5 et ultérieure)

Vous pouvez spécifier le serveur de base de données à utiliser lors de l'installation du serveur ou du proxy. Microsoft SQL Server 2008 R2 Express est installé par défaut et fait partie du package d'installation. Notez que Microsoft SQL Server 2008 R2 Express présente une limite de taille de base de données de 10 Go et ne peut pas être installé sur un contrôleur de domaine. Si vous utilisez par exemple Microsoft SBS, il est recommandé d'installer ESET Remote Administrator sur un autre serveur ou de ne pas sélectionner le composant SQL Server Express pendant l'installation (vous devez alors utiliser votre serveur SQL ou MySQL Server existant pour exécuter la base de données ERA).

Si vous décidez d'utiliser Microsoft SQL Server, la version la plus ancienne prise en charge est **Microsoft SQL Server 2008**. Vous pouvez utiliser une version de Microsoft SQL Server s'exécutant dans votre environnement, à condition qu'elle réponde à la configuration minimale requise.

REMARQUE : Comme ERA Server et ERA Proxy ne comportent pas d'outil de sauvegarde intégré, il est vivement recommandé d'effectuer une sauvegarde du serveur de base de données pour éviter toute perte de données.

Configuration matérielle requise pour le serveur de base de données :

Mémoire	1 Go de mémoire vive (RAM)
Disque dur	10 Go au minimum d'espace libre
Vitesse du processeur	Processeur x86 : 1,0 GHz Processeur x64 : 1,4 GHz **Remarque** : pour des performances optimales, un processeur cadencé à 2,0 GHz ou plus rapide est recommandé.
Type de processeur	Processeur x86 : processeur compatible Pentium III ou plus rapide Processeur x64 : AMD Opteron, AMD Athlon 64, Intel Xeon avec prise en charge d'Intel EM64T, Intel Pentium IV avec prise en charge d'EM64T

2.4 Ports utilisés

Les diagrammes ci-dessous répertorient tous les ports de communication utilisés lorsqu'ESET Remote Administrator et ses composants sont installés dans votre infrastructure. Les autres communications ont lieu via les processus du système d'exploitation natif (NetBIOS sur TCP/IP, par exemple).

ERA Server :

Protocole	Port	Utilisation	Descriptions
TCP	2222	Écoute d'ERA Server	Communication entre les ERA Agents et ERA Server

Protocole	Port	Utilisation	Descriptions
TCP	2223	Écoute d'ERA Server	Communication entre ERA Web Console et ERA Server utilisée pour l'installation assistée.

Serveur Web ERA Web Console :

Protocole	Port	Utilisation	Descriptions
TCP	443	Ecoute	Appel à la console Web HTTP SSL

ERA Proxy :

Protocole	Port	Utilisation	Descriptions
TCP	2222	Ecoute	Communication entre les ERA Agents et ERA Proxy

Proxy HTTP :

Protocole	Port	Utilisation	Descriptions
TCP	3128	Ecoute	Proxy HTTP (mise à jour de la mise en cache)

ERA Agent :

Protocole	Port	Utilisation	Descriptions
UDP	1237	Ecoute	Appel de mise en éveil

Connecteur de périphérique mobile :

Protocole	Port	Utilisation	Descriptions
TCP	9977		Communication interne entre le Connecteur de périphérique mobile et ERA Agent
TCP	9978		Communication interne entre le Connecteur de périphérique mobile et ERA Agent
TCP	9980	Inscription de périphérique mobile	Port d'inscription
TCP	9981	Communication avec ERA	Le Connecteur de périphérique mobile se connecte à ERA Server.

ERA Agent - utilisé pour le déploiement à distance d'ERA Agent sur un ordinateur cible doté d'un système d'exploitation Windows :

Protocole	Port	Utilisation	Descriptions
TCP	139	Port cible du point de vue d'ERA Server	Utilisation du partage ADMIN$
TCP	445	Port cible du point de vue d'ERA Server	Accès direct aux ressources partagées à l'aide de TCP/IP lors de l'installation à distance (une autre solution que TCP 139)
UDP	137	Port cible du point de vue d'ERA Server	Résolution des noms lors de l'installation à distance
UDP	138	Port cible du point de vue d'ERA Server	Navigation lors de l'installation à distance

Les ports 2222 et 2223 prédéfinis peuvent être modifiés s'ils sont déjà utilisés par d'autres applications.

REMARQUE : pour qu'ESET Remote Administrator fonctionne correctement, aucun des ports ci-dessus ne doit être utilisé par d'autres applications.

REMARQUE : veillez à configurer les pare-feu au sein de votre réseau pour permettre les communications via les ports répertoriés ci-dessus.

3. Processus d'installation

Les programmes d'installation ESET Remote Administrator sont disponibles en différents formats pour les différentes méthodes d'installation. Ils sont disponibles dans la section des téléchargements du site Web ESET, sous **Remote Administrator 6** (cliquez sur le signe + pour développer la catégorie). Vous pouvez télécharger les éléments suivants :

- Package de programmes d'installation ERA tout en un compressé
- Image ISO contenant tous les programmes d'installation d'ESET Remote Administrator (excepté l'appliance virtuelle ERA)
- Appliances virtuelles (fichiers OVA)
- Programmes individuels d'installation de chaque composant - pour les plates-formes Windows et Linux

REMARQUE : le déploiement de l'appliance virtuelle ERA est conseillée aux utilisateurs souhaitant exécuter ESET Remote Administrator dans un environnement virtualisé ou désireux d'opter pour une installation sans souci. Reportez-vous à notre Guide de déploiement de l'appliance virtuelle ERA pour des instructions détaillées.

Pour obtenir des instructions sur la mise à niveau de votre installation ERA existante, voir Procédures de mise à niveau.

3.1 Installation sous Windows

L'installation d'ESET Remote Administrator peut être effectuée de plusieurs manières différentes. Choisissez le type d'installation qui répond à vos besoins et votre environnement. La méthode la plus simple consiste à utiliser le programme d'installation tout en un ESET Remote Administrator (ERA). Cette méthode permet d'installer ESET Remote Administrator et ses composants sur un seul ordinateur.

L'installation de composants permet d'installer différents composants d'ESET Remote Administrator sur des ordinateurs différents. Vous disposez ainsi de plus de liberté pour personnaliser votre installation. Vous pouvez installer chaque composant sur un ordinateur souhaité, à condition qu'il réponde à la configuration système requise.

- Installation du package (Installation du package tout en un)
- Installation par étapes
- Installation sur Windows Small Business Server (SBS) / Essentials
- Installation de composants

De nombreux scénarios d'installation nécessitent d'installer différents composants ESET Remote Administrator sur des ordinateurs différents pour tenir compte des architectures réseau, pour satisfaire aux exigences de performance ou pour d'autres raisons. Les packages d'installation suivants sont disponibles pour les composants ESET Remote Administrator distincts :

Composants principaux

- ERA Server
- ERA Web Console
- ERA Agent (doit être installé sur les ordinateurs clients ; ce composant est facultatif sur ERA Server)

Composants facultatifs

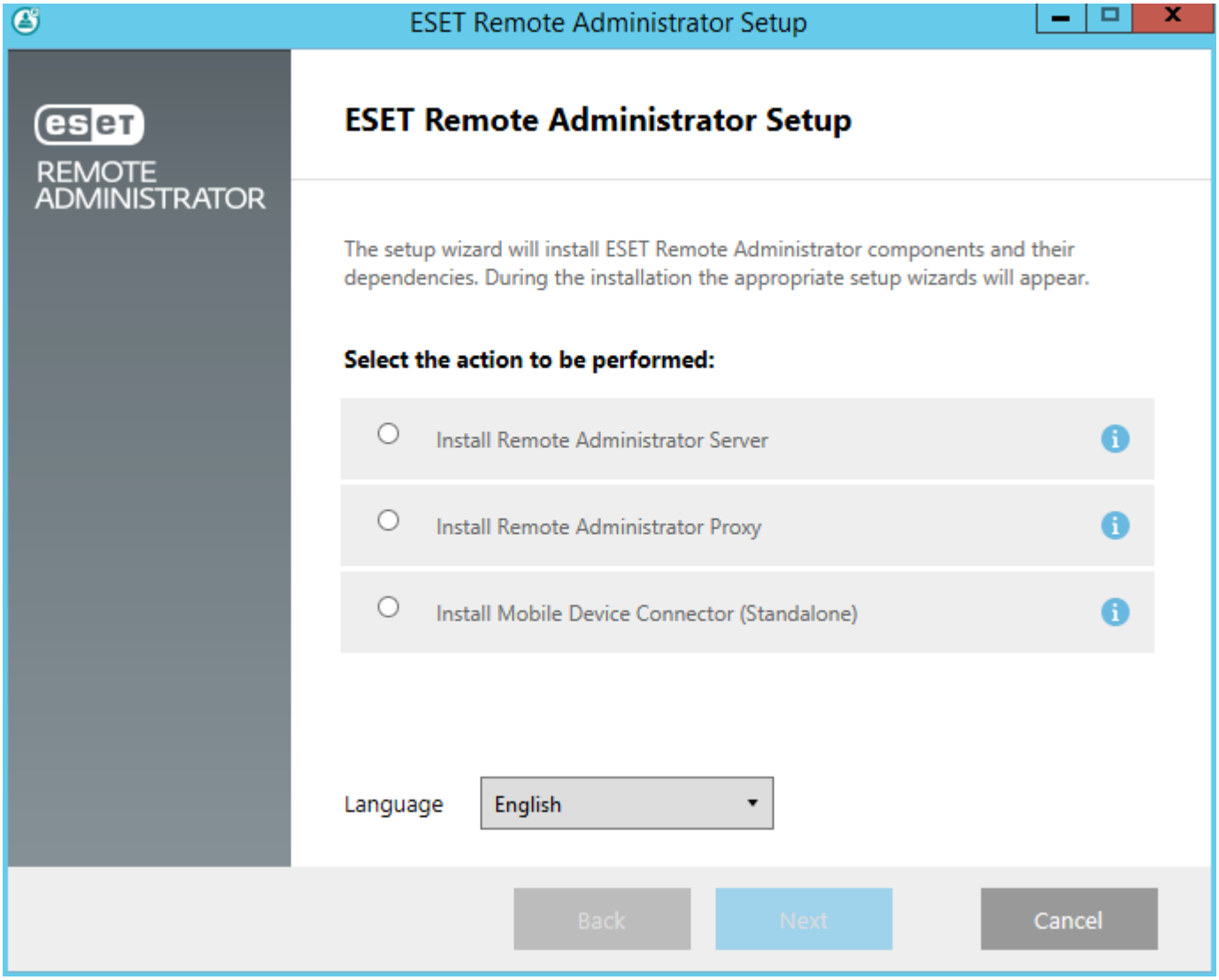
- ERA Proxy
- RD Sensor
- Connecteur de périphérique mobile
- Proxy HTTP Apache
- Outil Miroir

Pour obtenir des instructions afin d'effectuer une mise à niveau d'ESET Remote Administrator vers la dernière version (6.x), consultez l'article de la base de connaissances.

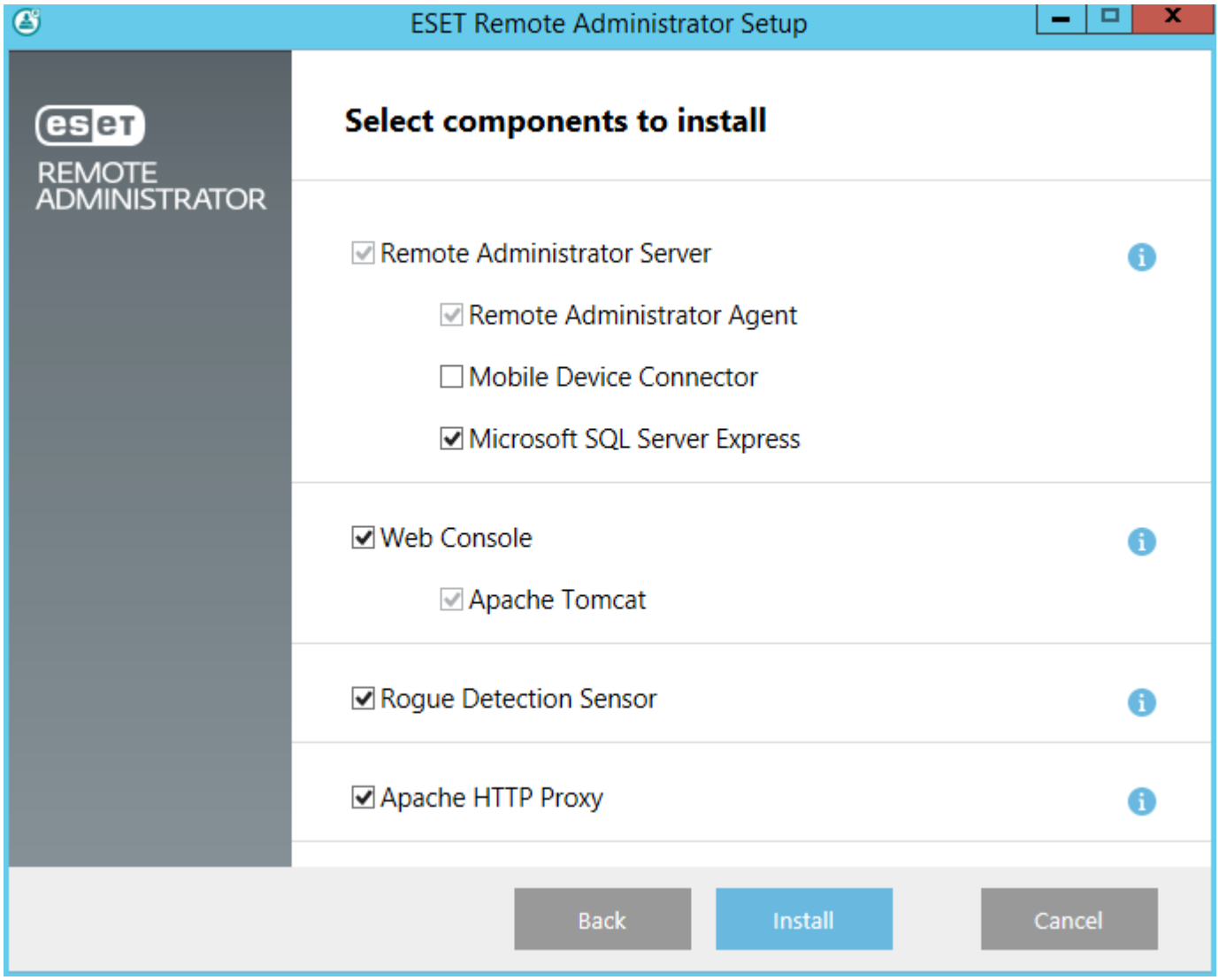
3.1.1 Installation pas à pas sous Windows

Le programme d'installation ERA (tout en un) est uniquement disponible pour les systèmes d'exploitation Windows. Il vous permet d'installer tous les composants ERA à l'aide de l'assistant d'installation ERA. Lorsque vous exécutez le package d'installation, trois options vous sont proposées.

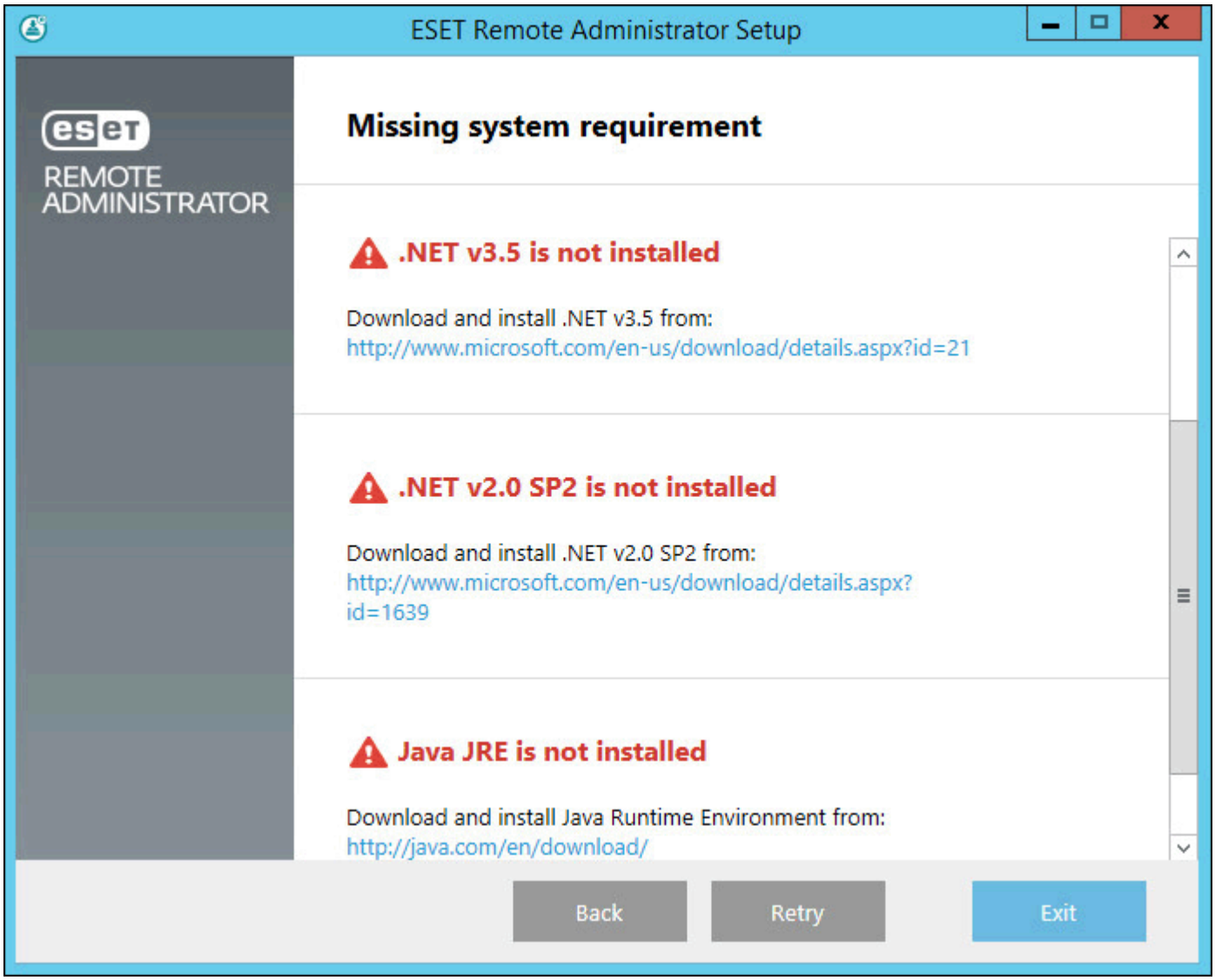
1. Sélectionnez **Remote Administrator Server** et cliquez sur **Suivant**. Vous pouvez également sélectionner la **langue** dans le menu déroulant avant de continuer.



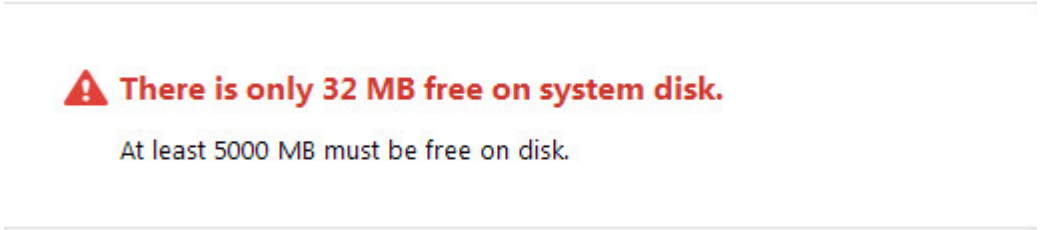
2. Après acceptation des termes du CLUF, cliquez sur **Suivant**. Il est recommandé d'installer les composants sélectionnés par défaut.


ESET Remote Administrator Setup
REMOTE ADMINISTRATOR
Select components to install
Remote Administrator Server
Remote Administrator Agent
Mobile Device Connector
Microsoft SQL Server Express
Web Console
Apache Tomcat
Rogue Detection Sensor
Apache HTTP Proxy
Back
Install
Cancel

3. Si des erreurs sont détectées lors de la vérification des conditions préalables requises, corrigez-les. Vérifiez que le système répond à toutes conditions préalables requises.

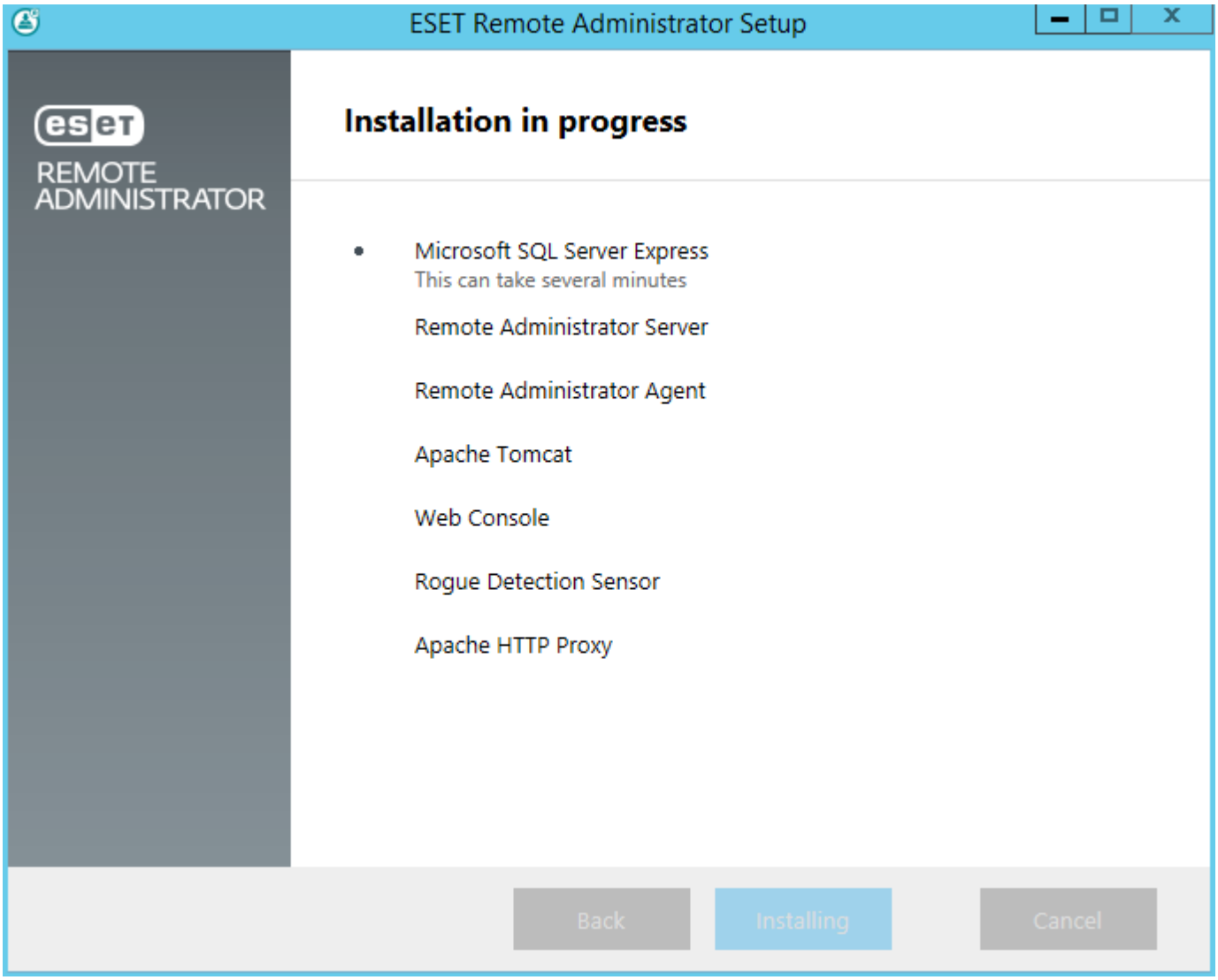


La notification suivante peut s'afficher si votre système ne dispose pas de l'espace disque requis par l'installation d'ERA :

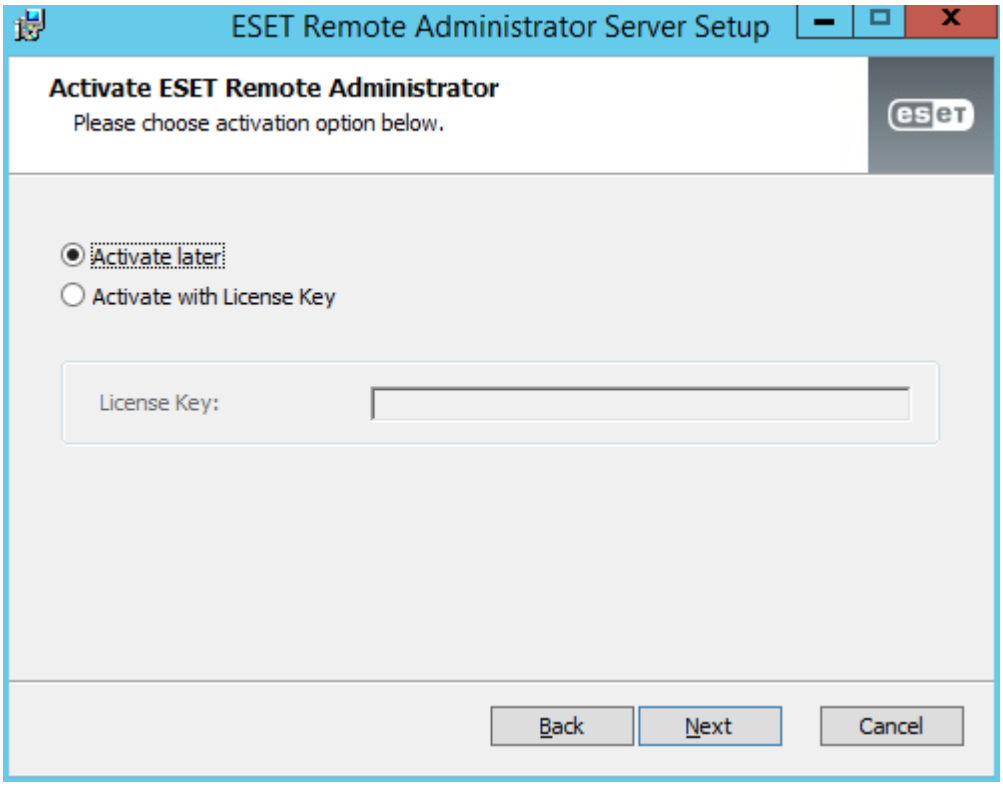


REMARQUE : si vous choisissez d'installer Microsoft SQL Server Express lors de l'installation d'ESET Remote Administrator, vous ne serez pas en mesure de l'installer sur un contrôleur de domaine. Cela risque de se produire si vous utilisez Windows SBS / Essentials. Si vous utilisez SBS / Essentials, il est recommandé d'installer ESET Remote Administrator sur un autre serveur ou de ne pas sélectionner le composant SQL Server Express lors de l'installation (vous devez dans ce cas utiliser un serveur SQL Server ou MySQL existant pour exécuter la base de données ERA).

4. Lorsque la vérification des conditions préalables requises est terminée et que votre environnement répond à toutes les exigences, l'installation démarre.

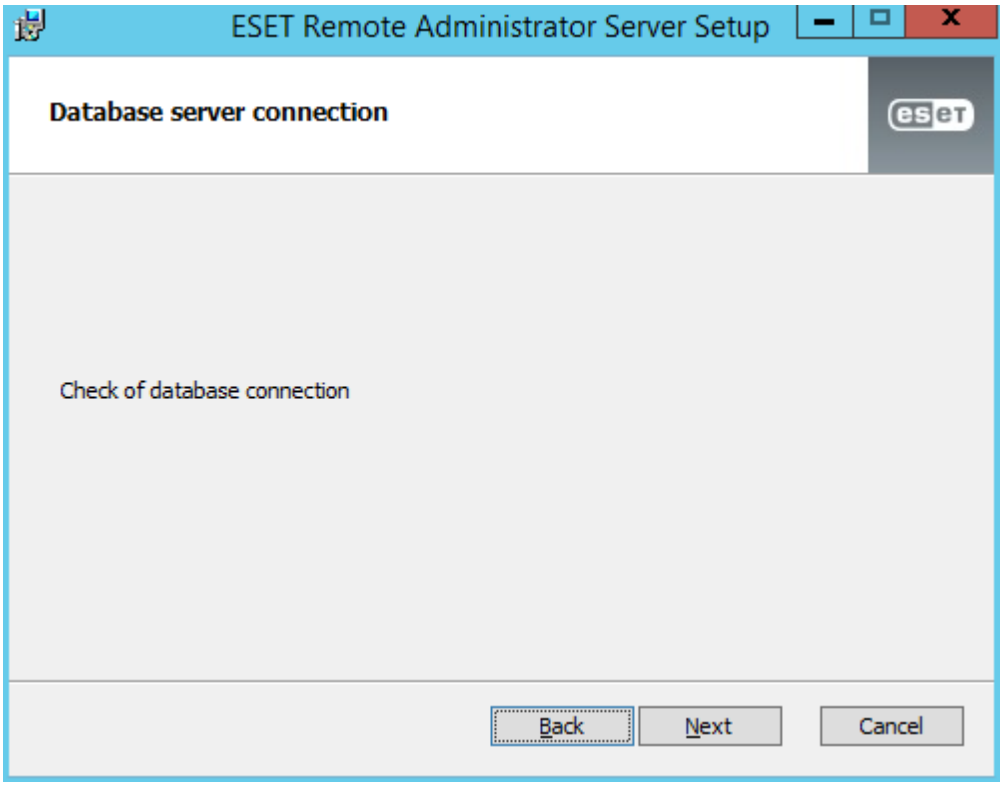


5. Saisissez une **clé de licence** valide, que vous devez avoir reçue lors de l'achat de votre solution de sécurité ESET. Si vous utilisez des informations d'identification de licence héritée (nom d'utilisateur et mot de passe), convertissez-les en clé de licence. Vous pouvez également sélectionner **Activer ultérieurement**. Si vous choisissez **Activer ultérieurement**, reportez-vous au chapitre Activation pour obtenir des instructions supplémentaires.

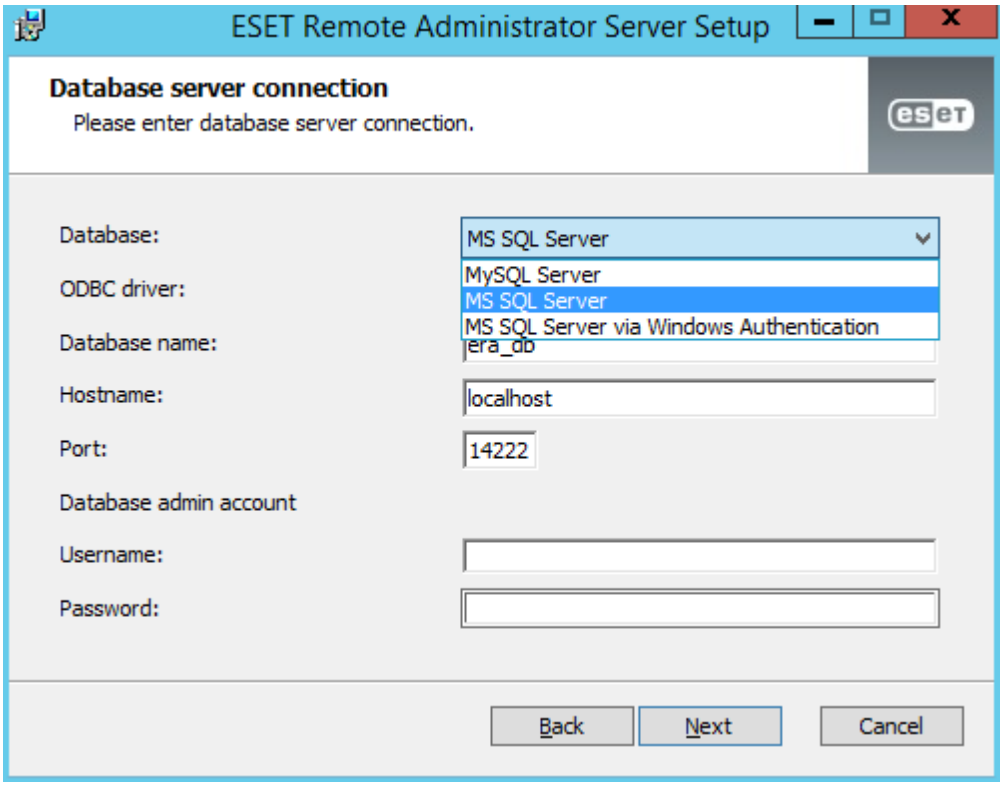


6. Si vous avez choisi d'installer Microsoft SQL Server Express (à l'étape 2), une vérification de la connexion de la base de données est effectuée. Vous pouvez passer à l'étape 10.

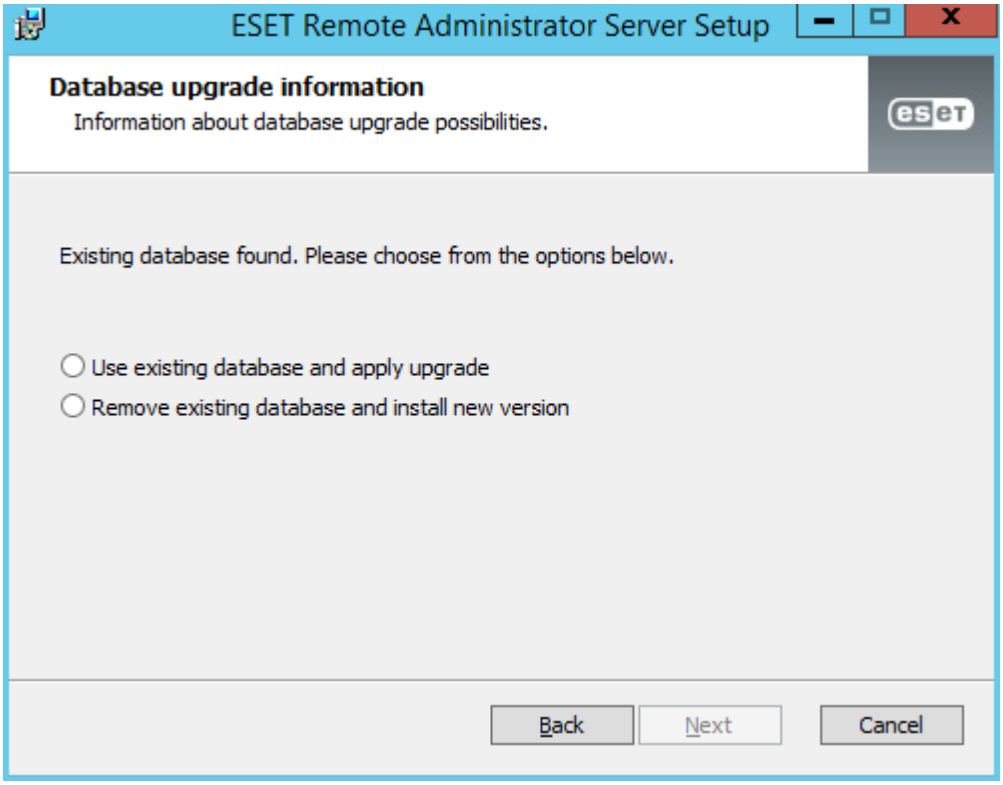
   - Si vous disposez d'un serveur de base de données existant, vous êtes invité à saisir les informations de connexion à la base de données à l'étape suivante.



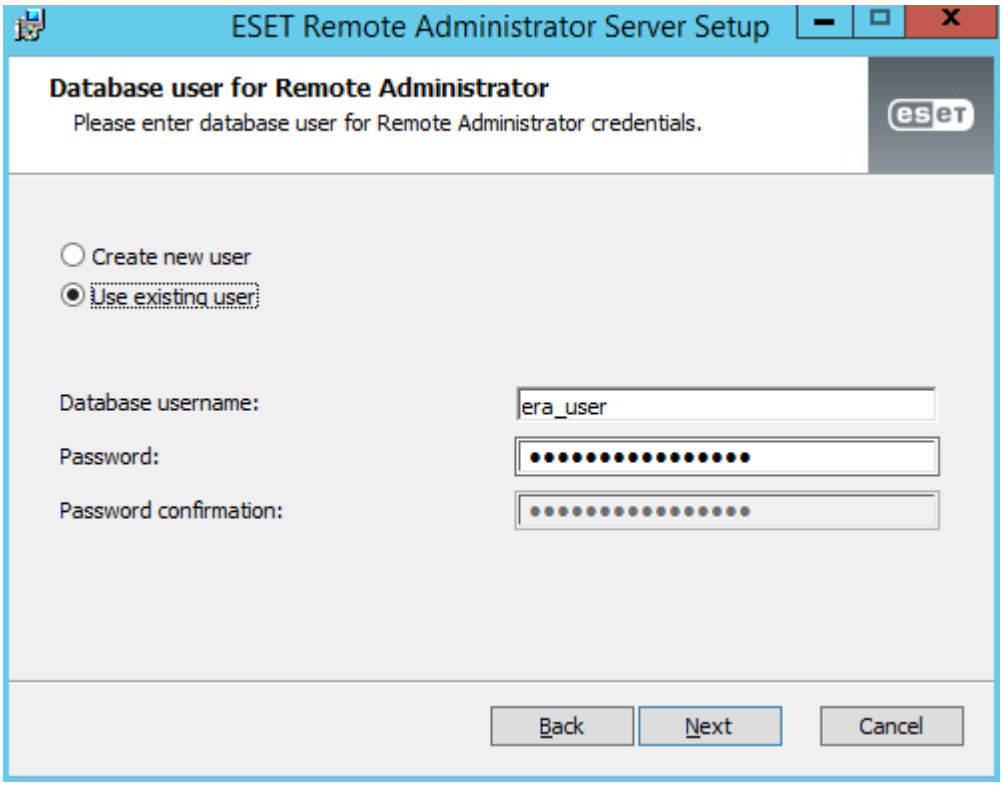
7. Si vous utilisez un serveur SQL Server ou MySQL existant, configurez les paramètres de connexion en conséquence. Saisissez le **nom de la base de données**, le **nom d'hôte** et le numéro de **port** (vous pouvez trouver ces informations dans le Gestionnaire de configuration Microsoft SQL Server) et les détails du compte de l'administrateur de base de données (nom d'utilisateur et mot de passe) dans les champs appropriés, puis cliquez sur Suivant. La connexion à la base de données est vérifiée.



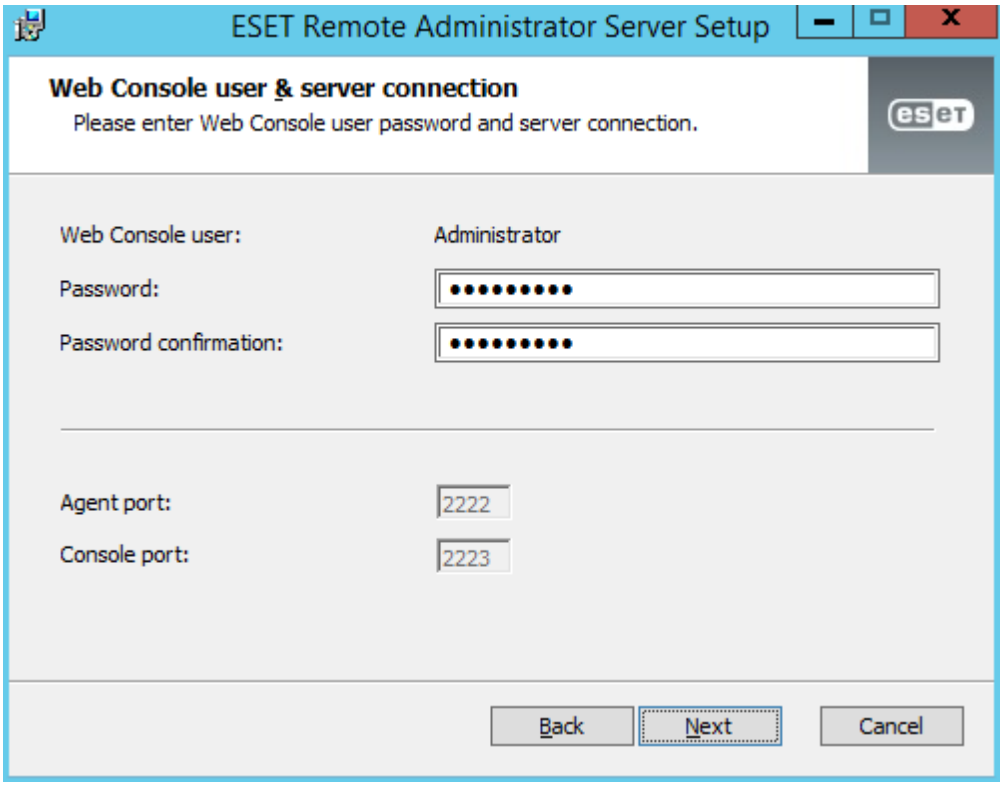
8. La présence d'une base de données ERA existante (provenant d'une installation ERA précédente) sur votre serveur de base de données est détectée. Vous pouvez sélectionner **Utiliser la base de données existante et appliquer une mise à niveau** ou **Supprimer la base de données existante et installer une nouvelle version**.



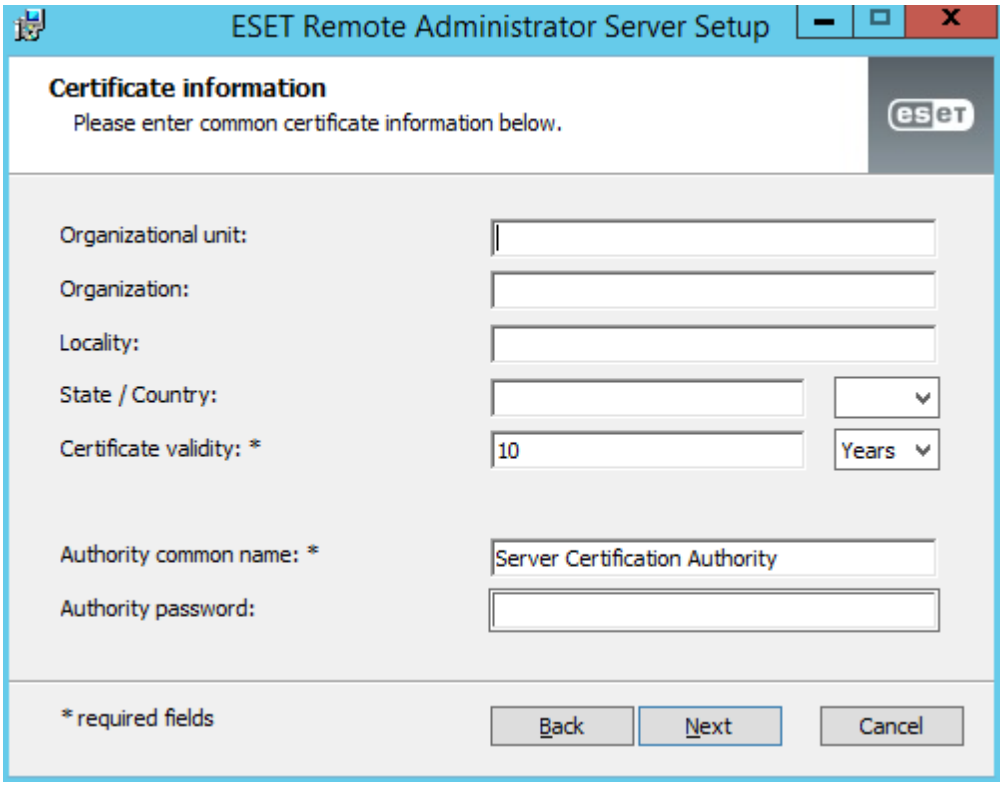
9. Indiquez si vous souhaitez utiliser l'utilisateur de base de données existant ou en créer un nouveau. Si vous avez sélectionné **Utiliser l'utilisateur existant**, entrez le **nom d'utilisateur de base de données** et le **mot de passe**. Si un message d'erreur s'affiche, choisissez de créer un nouvel utilisateur.



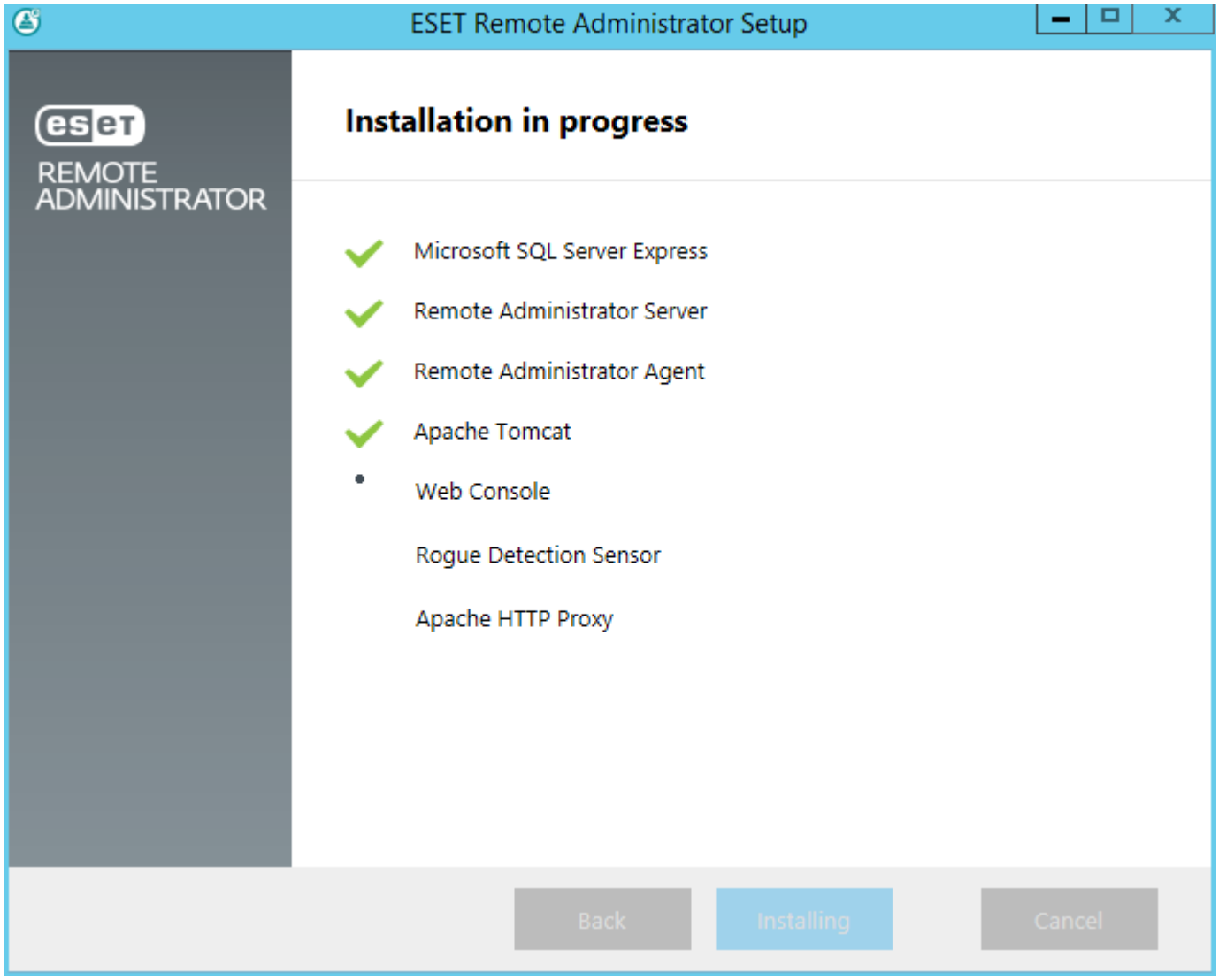
10. Vous êtes invité à saisir un mot de passe pour le compte Administrateur de la console Web. Ce mot de passe est important, car il vous permet de vous connecter à la console Web ERA.



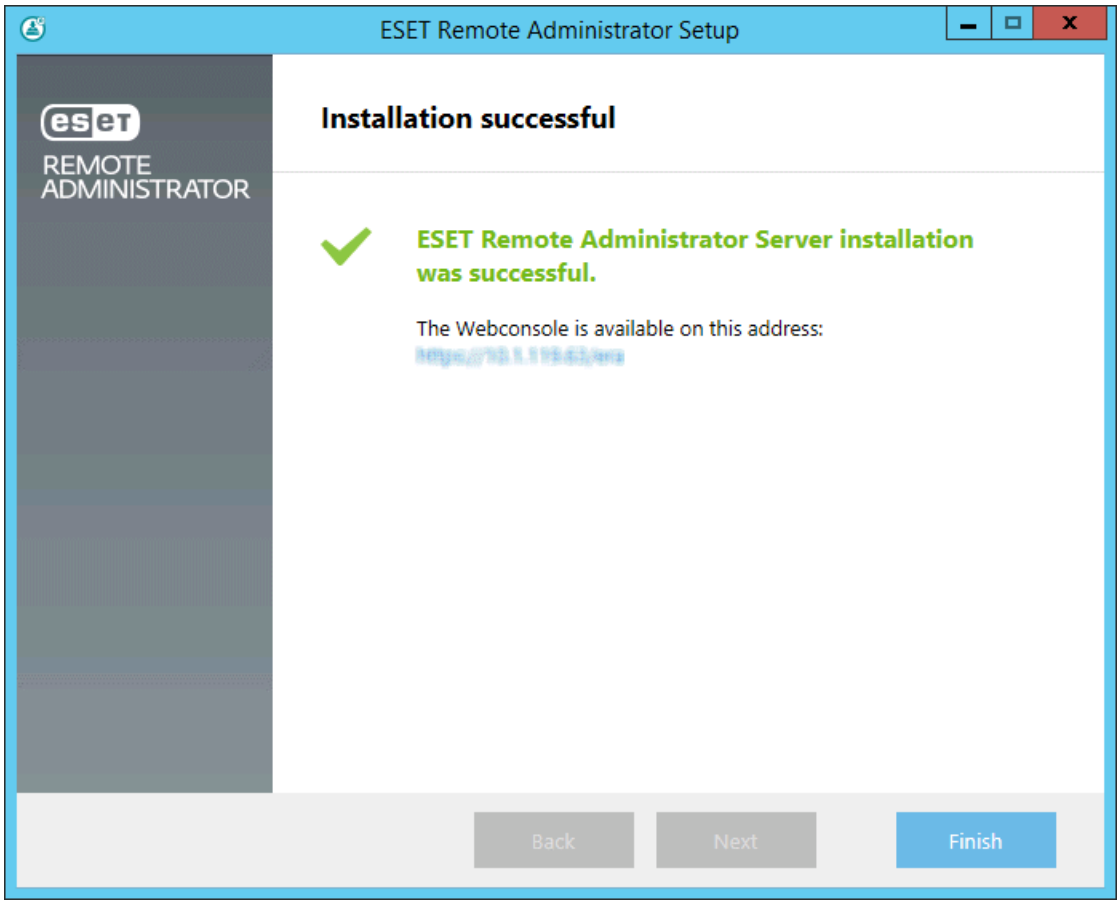
11. Créez une autorité de certification pour ESET Remote Administrator, puis cliquez sur **Suivant**. Vous pouvez éventuellement indiquer des informations supplémentaires sur le certificat (ces informations ne sont pas obligatoires). Vous pouvez laisser le champ **Mot de passe de l'autorité** vide. Si vous saisissez un mot de passe, veillez à le mémoriser.



12. Après avoir cliqué sur **Suivant**, la progression de l'installation s'affiche.

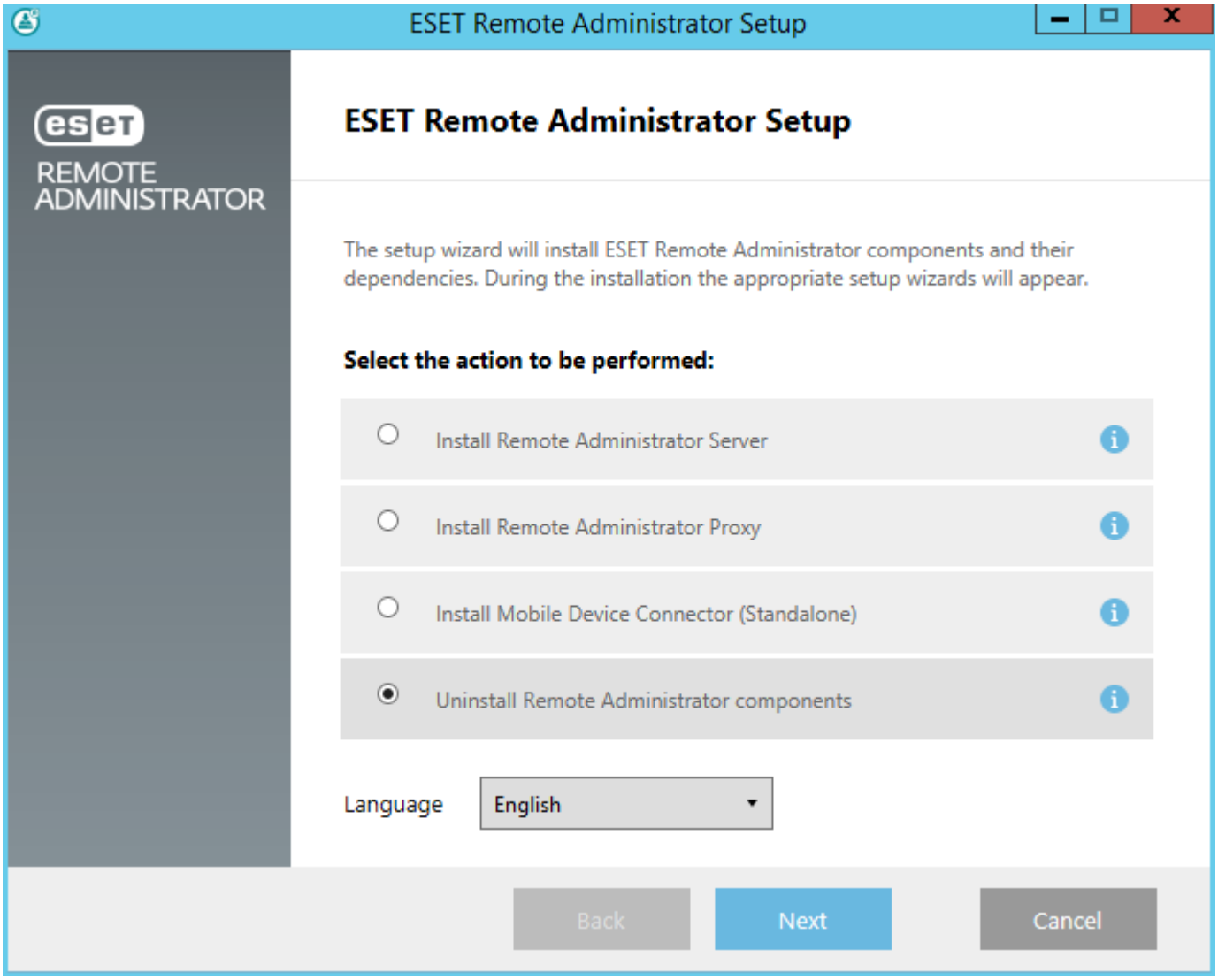

ESET Remote Administrator Setup
REMOTE ADMINISTRATOR
Installation in progress
Microsoft SQL Server Express
Remote Administrator Server
Remote Administrator Agent
Apache Tomcat
Web Console
Rogue Detection Sensor
Apache HTTP Proxy
Back
Installing
Cancel

13. Lorsque vous avez terminé, le message « L'installation d'ESET Remote Administrator Server a réussi » s'affiche avec l'adresse URL de la console Web ERA. Cliquez sur l'adresse URL pour ouvrir la console Web ou sur **Terminer**.

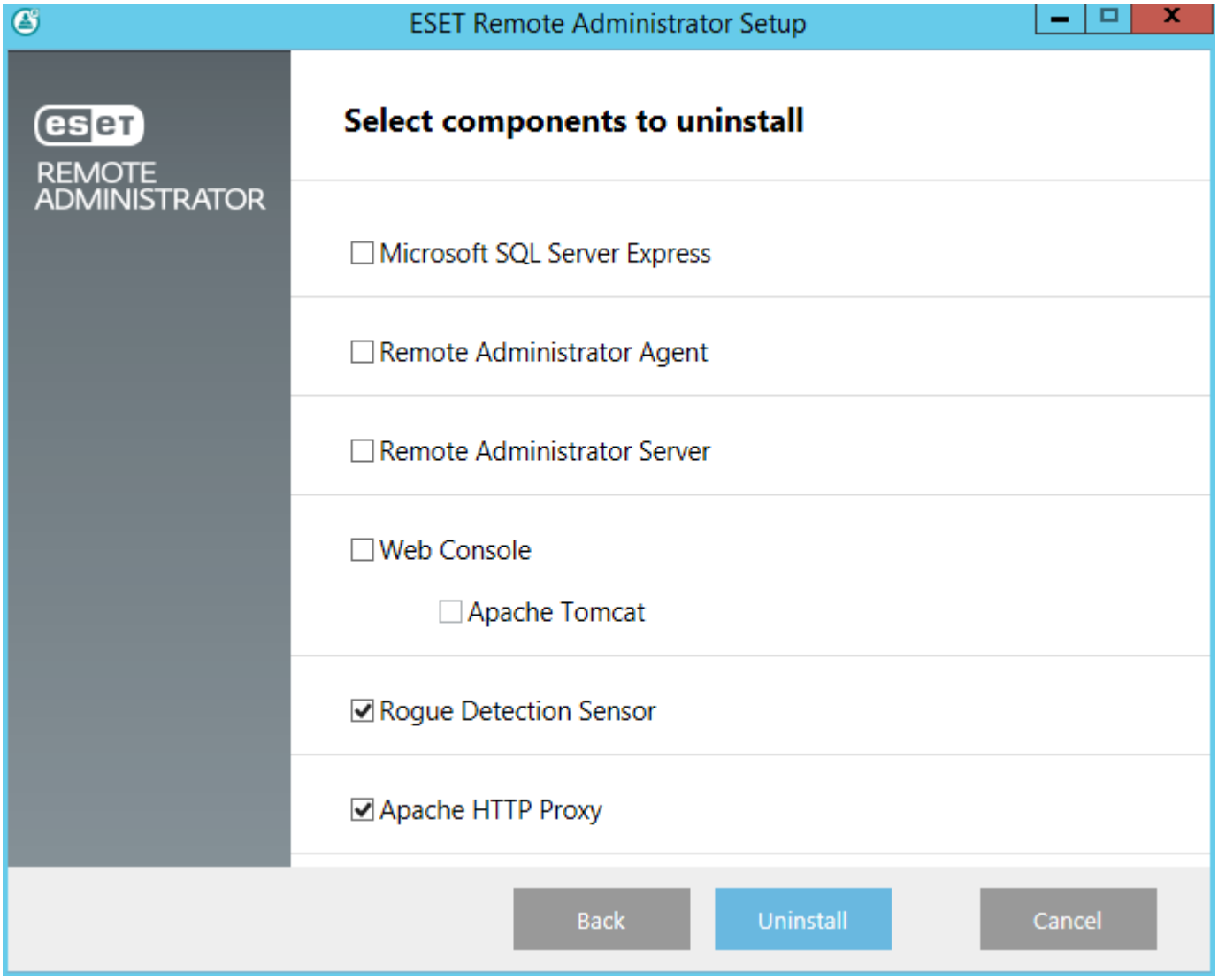


3.1.1.1 Désinstaller des composants

Pour désinstaller des composants ERA, exécutez le programme d'installation tout en un ERA que vous avez utilisé durant l'installation d'ERA et sélectionnez Désinstaller les composants Remote Administrator. Vous pouvez également sélectionner la **langue** dans le menu déroulant avant de continuer.



Après acceptation des termes du CLUF, cliquez sur **Suivant**. Sélectionnez le ou les composants que vous souhaitez désinstaller, puis cliquez sur **Désinstaller**.



REMARQUE : il est recommandé de redémarrer le serveur après la désinstallation de composants.

3.1.2 Installation sur Windows SBS / Essentials

Veillez à ce que toutes les conditions requises soient réunies, en particulier que le système d'exploitation soit pris en charge.

REMARQUE :: certaines anciennes versions de Microsoft SBS comprennent des versions de Microsoft SQL Server Express qui ne sont pas prises en charge par ESET Remote Administrator :

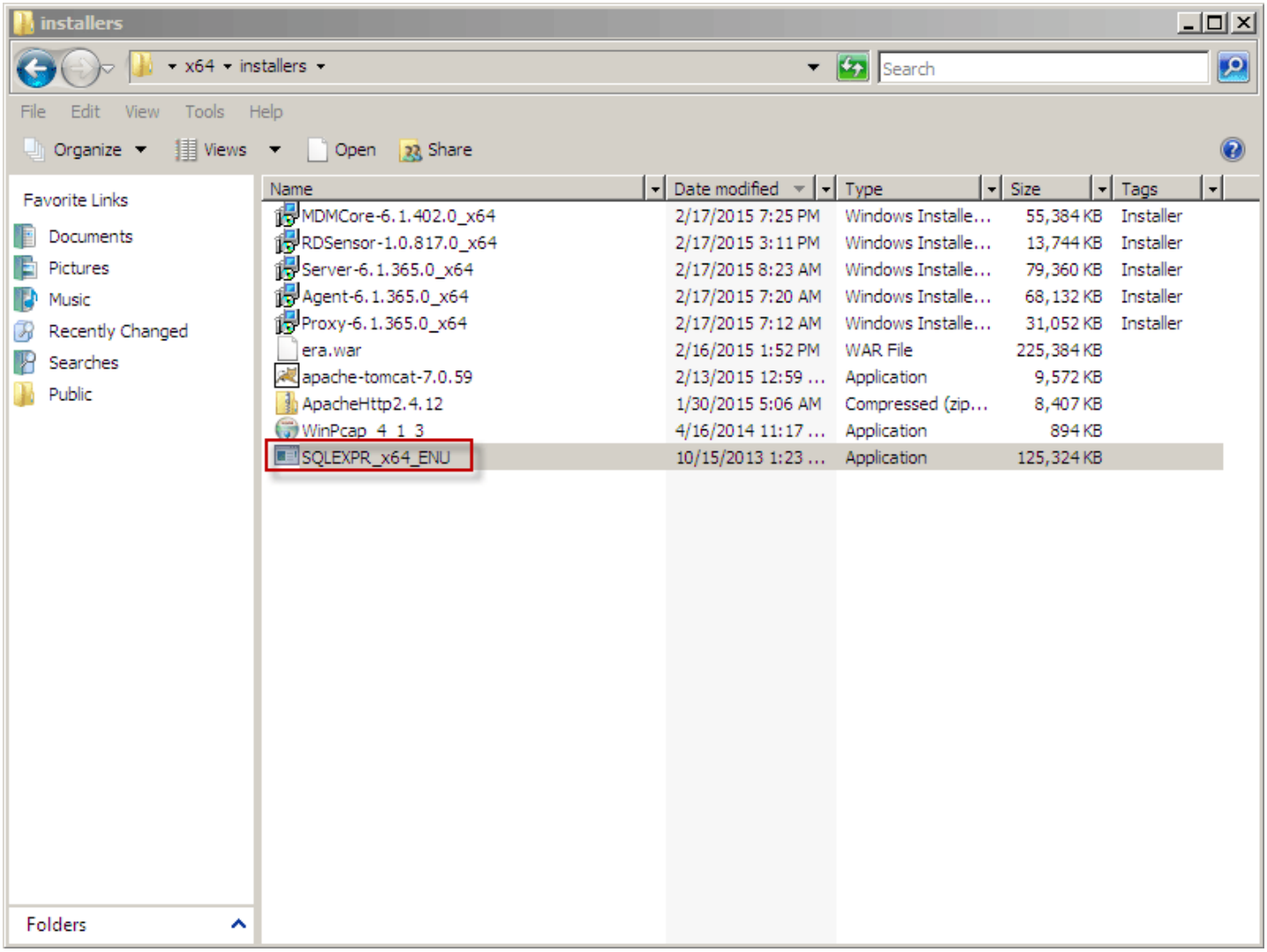
Microsoft SBS 2003 x86 SP2
Microsoft SBS 2003 x86 R2
Microsoft SBS 2008 x64 SP2

Si vous possédez l'une des versions de Windows Small Business Server répertoriées ci-dessus et si vous souhaitez installer la base de données ERA sur Microsoft SBS, vous devez utiliser une version plus récente de Microsoft SQL Server Express.

- Si Microsoft SQL Express n'est pas installé sur SBS, suivez la procédure décrite ci-après.
- Si Microsoft SQL Express est installé sur SBS mais que vous n'utilisez pas le programme, désinstallez-le, puis suivez la procédure décrite ci-après.
- Si vous utilisez la version de Microsoft SQL Server Express fournie avec SBS, migrez votre base de données vers une version de SQL Express compatible avec ERA Server. Pour ce faire, sauvegardez vos bases de données, désinstallez Microsoft SQL Server Express et suivez la procédure décrite ci-après pour installer une version compatible de Microsoft SQL Server Express et restaurer les bases de données, si nécessaire.

1. Téléchargez le package d'installation d'ERA sous une forme compressée à partir de la section des téléchargements du site Web ESET, sous **Remote Administrator 6** (cliquez sur le signe + pour développer la catégorie).

2. Décompressez le fichier d'installation que vous avez téléchargé à l'étape 1, ouvrez le dossier des programmes d'installation, puis double-cliquez sur **SQLEXPR_x64_ENU**.

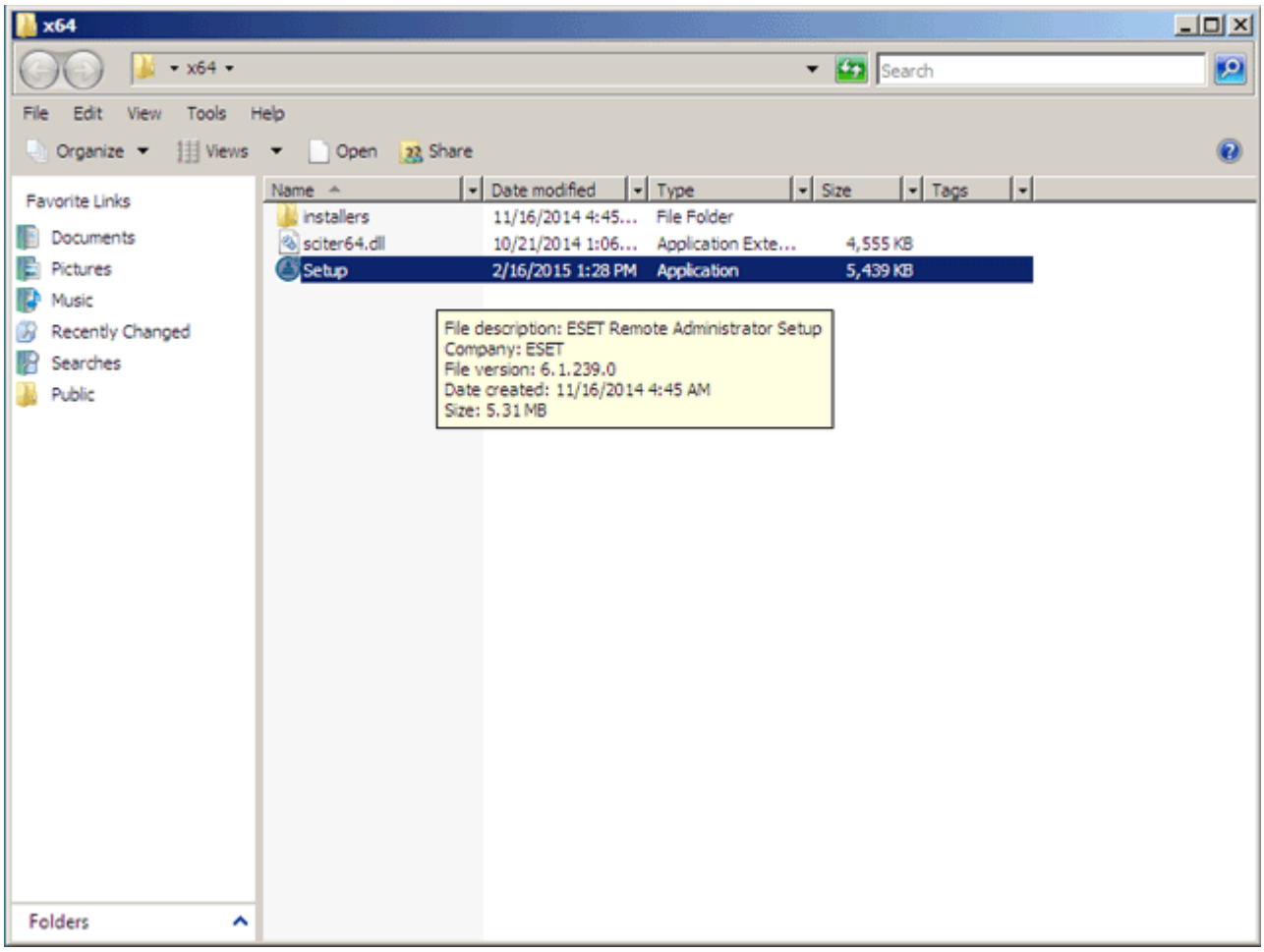


- Le Centre d'installation est lancé. Cliquez sur **Nouvelle installation ou ajout de fonctionnalités à une installation existante** pour démarrer l'Assistant Installation.

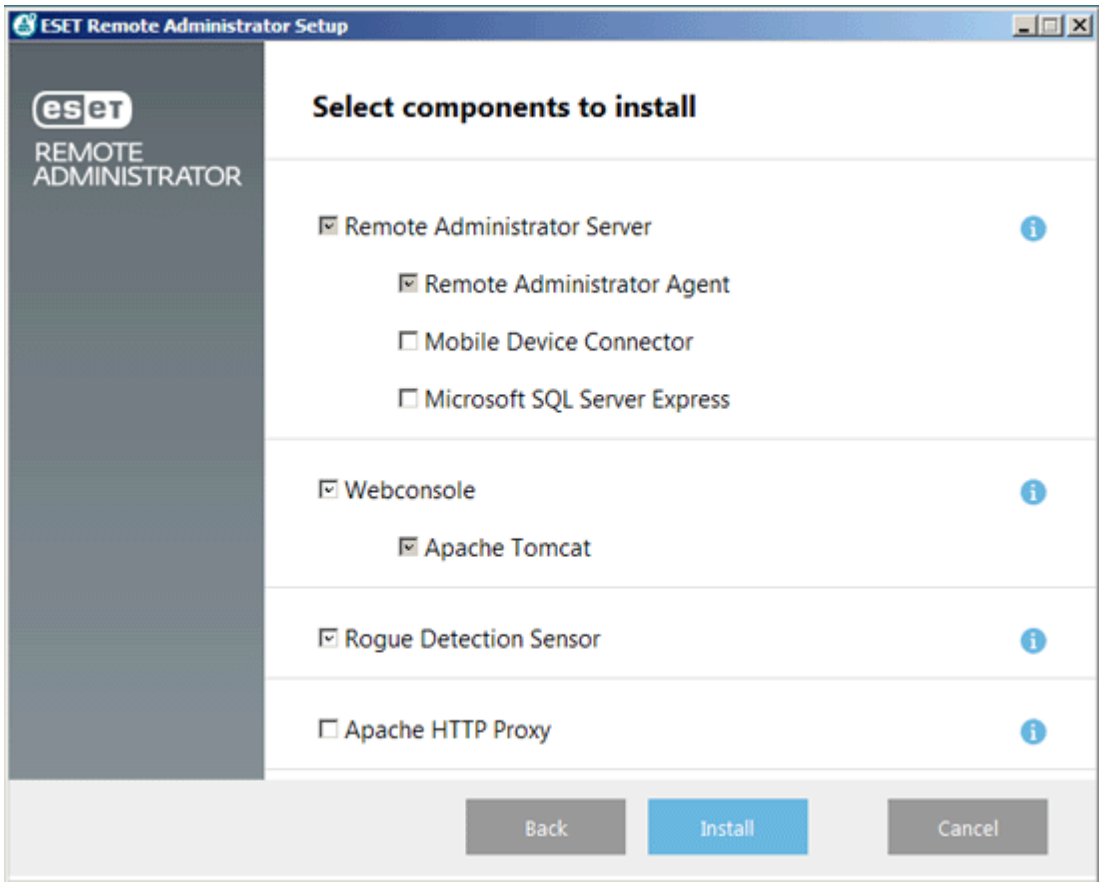
REMARQUE : à l'étape 8 du processus d'installation, définissez le mode d'authentification sur **Mode mixte (authentification SQL Server et authentification Windows)**.

REMARQUE : pour installer ERA Server sur SBS, vous devez autoriser les connexions TCP/IP à SQL Server.

3. Installez ESET Remote Administrator en exécutant le fichier **Setup.exe**.



4. Sélectionnez les composants à installer, veillez à désélectionner Microsoft SQL Server Express, puis cliquez sur **Installer**.



3.1.3 Installation du package

Installation de Remote Administrator Server

Suivez les instructions ci-après ou regardez la vidéo d'instructions de la base de connaissance. Vous pouvez également consulter l'article de la base de connaissances pour obtenir des instructions détaillées et illustrées afin d'effectuer l'installation à l'aide du programme d'installation tout en un.

1. Double-cliquez sur le package d'installation pour commencer l'installation. Sélectionnez **Remote Administrator Server**.

REMARQUE : si vous souhaitez installer ERA dans un environnement de cluster de basculement, une installation de composant est nécessaire.

2. Sélectionnez les composants à installer. Si vous ne disposez pas d'un serveur de base de données, vous pouvez installer Microsoft SQL Server 2008 R2 Express, compris dans le package d'installation. Notez que Microsoft SQL Server 2008 R2 Express présente une limite de taille de base de données de 10 Go. Vous pouvez également installer ERA Web Console, le Connecteur de périphérique mobile, le proxy HTTP Apache et Rogue Detection Sensor à l'aide de la méthode d'installation du package.
3. Saisissez une clé de licence valide ou sélectionnez **Activer ultérieurement**.
4. Si vous utilisez une base de données SQL Express, la connexion à celle-ci est vérifiée. Vous êtes également invité à saisir un mot de passe pour ERA Web Console (étape 8) et votre mot de passe de certificat (étape 10).
5. En cas d'utilisation d'un autre système de base de données : sélectionnez **Compte d'utilisateur du service**. Ce compte est utilisé pour exécuter le service ESET Remote Administrator Server. Les options disponibles sont les suivantes :

   a. Compte de service réseau
   b. Compte personnalisé/Utilisateur spécifique : DOMAINE/NOMUTILISATEUR

6. Connectez-vous à une base de données. Toutes les données, du mot de passe de la console Web aux journaux des ordinateurs clients, y sont stockées.

   a. **Base de données** : MySQL Server/MS SQL Server/MS SQL Server via l'authentification Windows
   b. **Pilote ODBC** : pilote MySQL ODBC 5.1/pilote Unicode MySQL ODBC 5.2/pilote unicode MySQL ODBC 5.3/ SQL Server/client natif SQL Server 10.0/pilote ODBC 11 pour SQL Server
   c. **Nom de la base de données :** vous pouvez conserver le nom prédéfini ou le modifier en cas de besoin
   d. **Nom de l'hôte** : nom d'hôte ou adresse IP du serveur de base de données
   e. **Port** utilisé pour la connexion au serveur
   f. **Nom d'utilisateur/Mot de passe** du compte d'administrateur de base de données

Cette étape vérifie la connexion à la base de données. Si la connexion est correcte, vous pouvez passer à l'étape suivante.

7. Sélectionnez un utilisateur ESET Remote Administrator ayant accès à la base de données. Vous pouvez utiliser un utilisateur existant ou en créer un.
8. Saisissez un mot de passe pour l'accès à **console Web**.
9. ESET Remote Administrator utilise des certificats pour les communications client-serveur. Vous pouvez sélectionner vos propres certificats. Le **serveur** peut également en créer.
10. Définissez un mot de passe pour l'**autorité de certification. Veillez à le mémoriser.** Pour créer une autorité de certification pour ESET Remote Administrator, cliquez sur **Suivant**. Un serveur de certificat est créé. Définissez un nom d'hôte de serveur et un mot de passe pour celui-ci.
11. Définissez un mot de passe pour le **certificat homologue**. Vous pouvez éventuellement indiquer des informations supplémentaires sur le certificat (ces informations ne sont pas obligatoires). Vous pouvez laisser le champ **Mot de passe de l'autorité** vide. Si vous saisissez un mot de passe, **veillez à le mémoriser**.

12. La configuration peut effectuer une tâche Synchronisation des groupes statiques initiale. Sélectionnez la méthode (**Ne pas synchroniser**, **Synchroniser avec Réseau Windows** ou **Synchroniser avec Active Directory**), puis cliquez sur **Suivant**.

13. Cliquez sur **Suivant** pour procéder à l'installation dans le dossier par défaut ou sélectionnez **Modifier...** le dossier de destination.

14. Cliquez sur **Installer** pour installer ERA Server.

15. Lorsque l'installation est terminée, cliquez sur le lien affiché dans l'assistant de configuration pour ouvrir la console Web (il est recommandé de mettre en signet cette URL), puis cliquez sur **Terminer**.

REMARQUE : si l'installation se termine avec l'erreur 2068052081, consultez le FAQ pour trouver des solutions.

Installation de Remote Administrator Proxy

1. Démarrez le package d'installation. Sélectionnez **Remote Administrator Proxy**.

2. Sélectionnez les composants à installer. Si vous ne disposez pas d'un serveur de base de données, vous pouvez installer Microsoft SQL Server 2008 R2 Express, compris dans le package d'installation. Notez que Microsoft SQL Server 2008 R2 Express présente une limite de taille de base de données de 10 Go. Vous pouvez également installer RD Sensor à partir du package d'installation.

3. Connectez-vous à une base de données :

   a. **Base de données** : MySQL Server/MS SQL Server/MS SQL Server via l'authentification Windows
   b. **Pilote ODBC** : pilote MySQL ODBC 5.1/pilote Unicode MySQL ODBC 5.2/pilote unicode MySQL ODBC 5.3/ SQL Server/client natif SQL Server 10.0/pilote ODBC 11 pour SQL Server
   c. **Nom de l'hôte** : nom d'hôte ou adresse IP du serveur de base de données
   d. **Port** utilisé pour la connexion au serveur
   e. **Nom d'utilisateur/Mot de passe** du compte d'administrateur de base de données

Cette étape vérifie la connexion à la base de données. Si la connexion est correcte, vous pouvez passer à l'étape suivante.

4. Sélectionnez un port de communication proxy. Par défaut, le port 2222 est utilisé.

5. Configurez la connexion du proxy à ESET Remote Administrator. Saisissez un **hôte de serveur** (nom d'hôte/ adresse IP du serveur) et un **port de serveur** (2222).

6. Sélectionnez un certificat homologue et un mot de passe pour ce certificat. Vous pouvez éventuellement ajouter une autorité de certification. Elle n'est nécessaire que pour les certificats non signés.

7. Sélectionnez éventuellement un dossier d'installation du Proxy, puis cliquez sur Installer.

8. ERA Agent est installé en plus du proxy.

3.1.4 Installation de composants sur Windows

De nombreux scénarios d'installation nécessitent d'installer différents composants ESET Remote Administrator sur des ordinateurs différents pour tenir compte des architectures réseau, pour satisfaire aux exigences de performance ou pour d'autres raisons. Les packages d'installation suivants sont disponibles pour les composants ESET Remote Administrator distincts :

Composants principaux

- ERA Server
- ERA Web Console
- ERA Agent (doit être installé sur les ordinateurs clients ; ce composant est facultatif sur ERA Server)

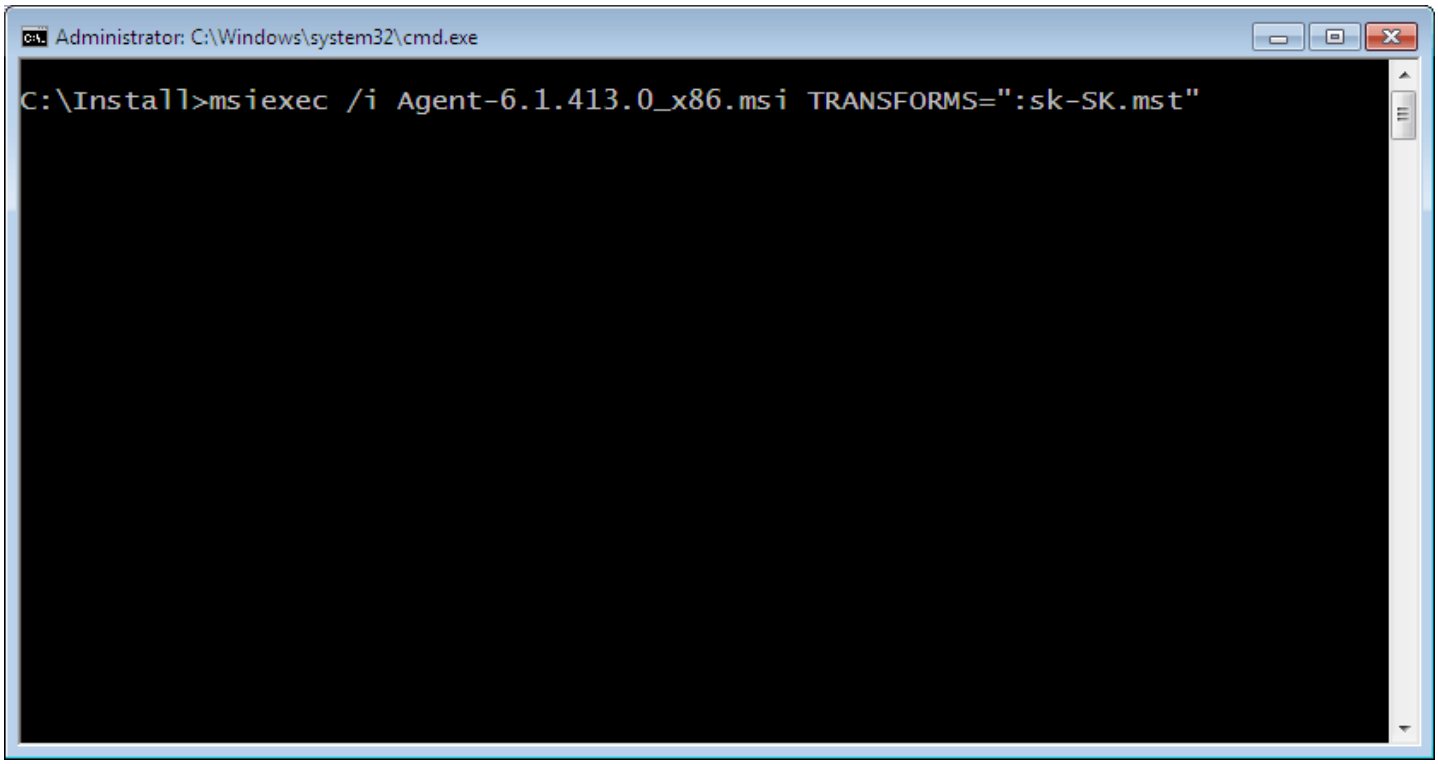
Composants facultatifs

- ERA Proxy
- RD Sensor
- Connecteur de périphérique mobile
- Proxy HTTP Apache
- Outil Miroir

Pour obtenir des instructions afin d'effectuer une mise à niveau d'ESET Remote Administrator vers la dernière version (6.x), consultez l'article de la base de connaissances.

Si vous souhaitez exécuter l'installation dans votre langue, vous devez démarrer le programme d'installation MSI d'un composant ERA spécifique via une ligne de commande.

Voici un exemple d'exécution de l'installation dans la langue slovaque :



Pour sélectionner la langue dans laquelle exécuter le programme d'installation, spécifiez le paramètre TRANSFORMS correspondant selon ce tableau :

Langue	Code
Anglais (États-Unis)	en-US
Arabe (Égypte)	ar-EG
Chinois simplifié	zh-CN
Chinois traditionnel	zh-TW

Croate (Croatie)	hr-HR
Tchèque (République tchèque)	cs-CZ
Français (France)	fr-FR
Français (Canada)	fr-FC
Allemand (Allemagne)	de-DE
Italien (Italie)	it-IT
Japonais (Japon)	ja-JP
Coréen (Corée)	ko-KR
Polonais (Pologne)	pl-PL
Portugais (Brésil)	pt-BR
Russe (Russie)	ru-RU
Espagnol (Chili)	es-CL
Espagnol (Espagne)	es-ES
Slovaque (Slovaquie)	sk-SK

3.1.4.1 Installation du serveur - Windows

Pour installer le composant ERA Server sur Windows, procédez comme suit :

1. Vérifiez que toutes les conditions préalables requises sont remplies.
2. Exécutez le programme d'installation d'ERA Server et acceptez les termes du CLUF si vous êtes d'accord avec ces derniers.

REMARQUE: si vous installez ERA Server sur un cluster de basculement, cochez la case en regard de l'option **Il s'agit d'une installation de cluster**. Dans le cas contraire, ne la cochez pas.

3. Si vous procédez à l'installation sur un cluster de basculement, indiquez le **chemin d'accès aux données de l'application personnalisée** pour pointer vers le stockage partagé du cluster. Les données doivent être stockées à un emplacement accessible par tous les nœuds du cluster.
4. Saisissez une clé de licence ERA valide ou sélectionnez **Activer ultérieurement**.
5. Sélectionnez un **compte d'utilisateur du service**. Ce compte est utilisé pour exécuter le service ESET Remote Administrator Server. Les options disponibles sont les suivantes :
   - Compte de service réseau
   - Spécifié par l'utilisateur : DOMAINE/NOMUTILISATEUR
4. Connectez-vous à une base de données. Toutes les données y sont stockées (mot de passe ERA Web Console, journaux des ordinateurs clients, etc.) :
   - **Base de données** : MySQL Server/MS SQL Server/MS SQL Server via l'authentification Windows
   - **Pilote ODBC** : pilote MySQL ODBC 5.1/pilote Unicode MySQL ODBC 5.2/pilote unicode MySQL ODBC 5.3/ SQL Server/client natif SQL Server 10.0/pilote ODBC 11 pour SQL Server
   - **Nom de la base de données** : vous pouvez conserver le nom prédéfini ou le modifier en cas de besoin
   - **Nom de l'hôte** : nom d'hôte ou adresse IP du serveur de base de données
   - **Port :** utilisé pour les connexions au serveur de base de données
   - **Nom d'utilisateur/Mot de passe** du compte d'administrateur de base de données

REMARQUE : ERA Server stocke des blobs de données volumineux dans la base de données. Pour qu'ERA s'exécute correctement, il est donc nécessaire de configurer MySQL pour accepter des paquets de grande taille. Pour plus d'informations sur cette configuration, reportez-vous au FAQ.

Cette étape vérifie la connexion à la base de données. Si la connexion est correcte, vous pouvez passer à l'étape suivante.

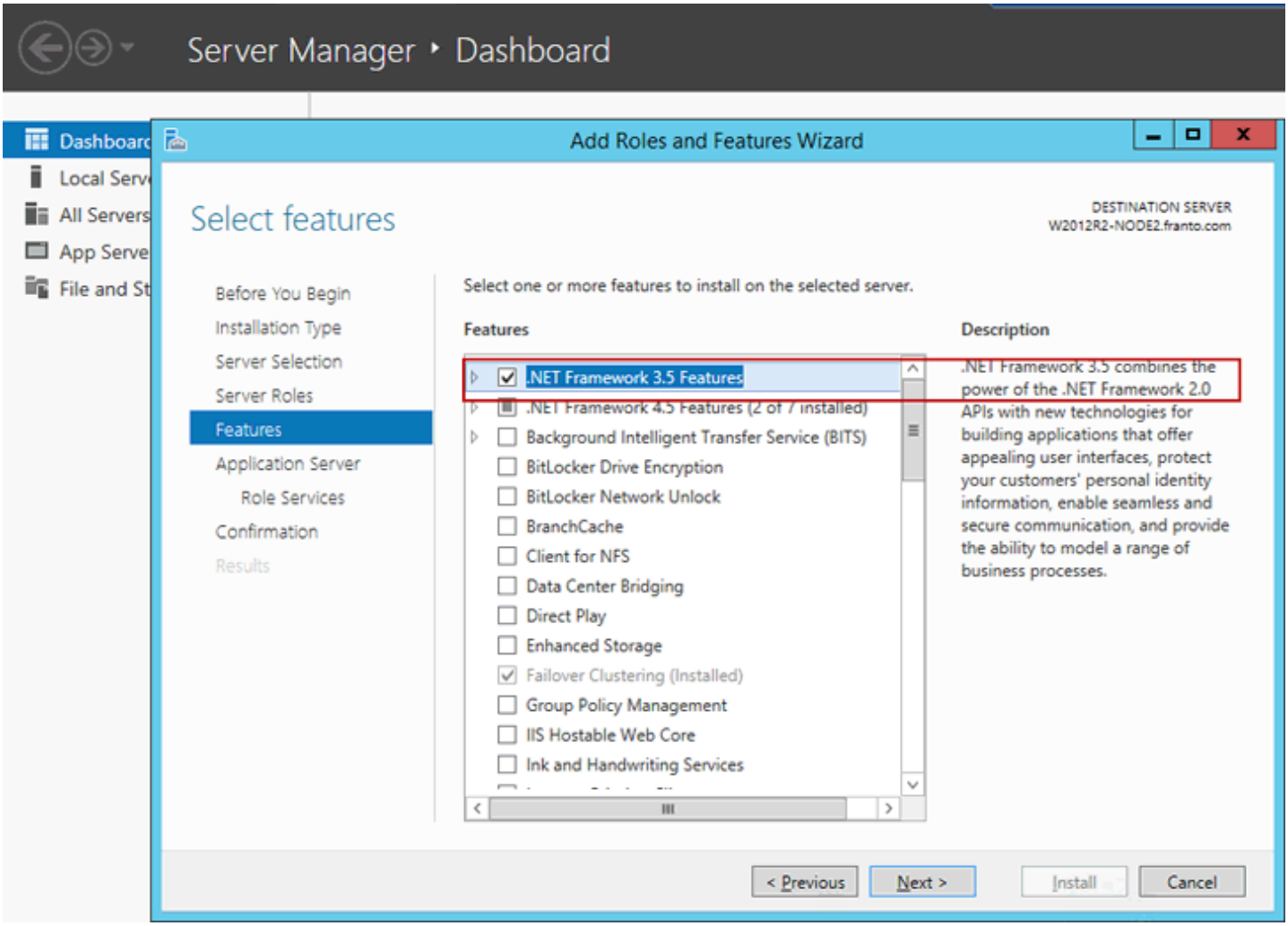
5. Sélectionnez un utilisateur ESET Remote Administrator ayant accès à la base de données. Vous pouvez utiliser un utilisateur existant. Un utilisateur peut être également automatiquement créé.
6. Saisissez un mot de passe pour l'accès à la **console Web**.
7. ESET Remote Administrator utilise des certificats pour les communications client-serveur. Vous pouvez sélectionner vos propres certificats. Le **serveur** peut également en créer.
8. Saisissez le mot de passe de l'**autorité de certification**. Veillez à le mémoriser.
9. Un serveur de certificat est créé. Sélectionnez également un mot de passe pour celui-ci.
10. À l'étape suivante, sélectionnez un mot de passe pour votre **certificat homologue**. Vous pouvez éventuellement indiquer des informations supplémentaires sur le certificat (ces informations ne sont pas obligatoires). Vous pouvez laisser le champ **Mot de passe de l'autorité** vide. Si vous saisissez un mot de passe, **veillez à le mémoriser**.
11. La configuration peut effectuer une tâche Synchronisation des groupes statiques initiale. Sélectionnez la méthode (**Ne pas synchroniser**, **Synchroniser avec Réseau Windows** ou **Synchroniser avec Active Directory**), puis cliquez sur **Suivant**.
12. Validez le dossier d'installation pour le serveur ou modifiez-le, puis cliquez sur **Suivant**.
13. Cliquez sur **Installer** pour installer le serveur.

REMARQUE : une fois que vous avez terminé l'installation d'ERA Server, veillez à installer ERA Agent sur le même ordinateur (facultatif). Vous pourrez ainsi gérer le serveur comme un ordinateur client.

3.1.4.1.1 Conditions préalables requises pour le serveur - Windows

Pour installer ERA Server sous Windows, les conditions préalables requises suivantes doivent être remplies :

- Vous devez disposer d'une licence valide.
- Les ports requis doivent être ouverts et disponibles. Consultez la liste complète des ports ici.
- Le serveur de base de données (Microsoft SQL Server ou MySQL) est installé et en cours d'exécution. Pour plus d'informations, reportez-vous à la configuration requise pour la base de données. Si vous ne disposez pas d'un serveur de base de données, il est recommandé de consulter les informations de configuration de SQL Server pour configurer SQL correctement afin de l'utiliser avec ESET Remote Administrator.
- Java Runtime Environment (JRE) doit être installé (vous pouvez le télécharger à l'adresse http://java.com/en/download/). Utilisez toujours la dernière version officielle de Java.
- Microsoft .NET Framework 3.5 doit être installé. Si vous exécutez Windows Server 2008 ou 2012, vous pouvez l'installer à l'aide de **l'Assistant Ajout de rôles et de fonctionnalités** (comme illustré ci-dessous). Si vous utilisez Windows Server 2003, vous pouvez télécharger .NET 3.5 à l'adresse suivante : http://www.microsoft.com/en-us/download/details.aspx?id=21



REMARQUE : si vous choisissez d'installer Microsoft SQL Server Express lors de l'installation d'ESET Remote Administrator, vous ne serez pas en mesure de l'installer sur un contrôleur de domaine. Cela risque de se produire si vous utilisez Microsoft SBS. . Dans ce cas, il est recommandé d'installer ESET Remote Administrator sur un autre serveur ou de ne pas sélectionner le composant SQL Server Express lors de l'installation (vous devez dans ce cas utiliser un serveur SQL Server ou MySQL existant pour exécuter la base de données ERA). Pour obtenir des instructions afin d'installer ERA Server sur un contrôleur de domaine, consultez l'article de la base de connaissances.

REMARQUE : ERA Server stocke des blobs de données volumineux dans la base de données. Pour qu'ERA s'exécute correctement, il est donc nécessaire de configurer MySQL pour accepter des paquets de grande taille. Pour obtenir des instructions afin d'apporter cette modification, reportez-vous au FAQ.

3.1.4.2 Microsoft SQL Server - Windows

L'une des conditions préalables requises pour l'installation d'ERA Server est l'installation et la configuration de Microsoft SQL Server en vue de son utilisation avec ESET Remote Administrator. Les conditions requises suivantes doivent être remplies :

- Installez Microsoft SQL Server 2008 R2 ou version ultérieure. Vous pouvez autrement installer Microsoft SQL Server 2008 R2 Express ou version ultérieure. Pendant l'installation, choisissez l'authentification en **mode mixte**.
- Si Microsoft SQL Server est déjà installé, définissez l'authentification sur **Mode mixte (authentification SQL Server et authentification Windows)**. Pour ce faire, suivez les instructions de cet article de la base de connaissances.
- Autorisez les connexions TCP/IP à SQL Server. Pour ce faire, suivez les instructions de cet article de la base de connaissances à partir de la section **II. Allow TCP/IP connections to the SQL database**.

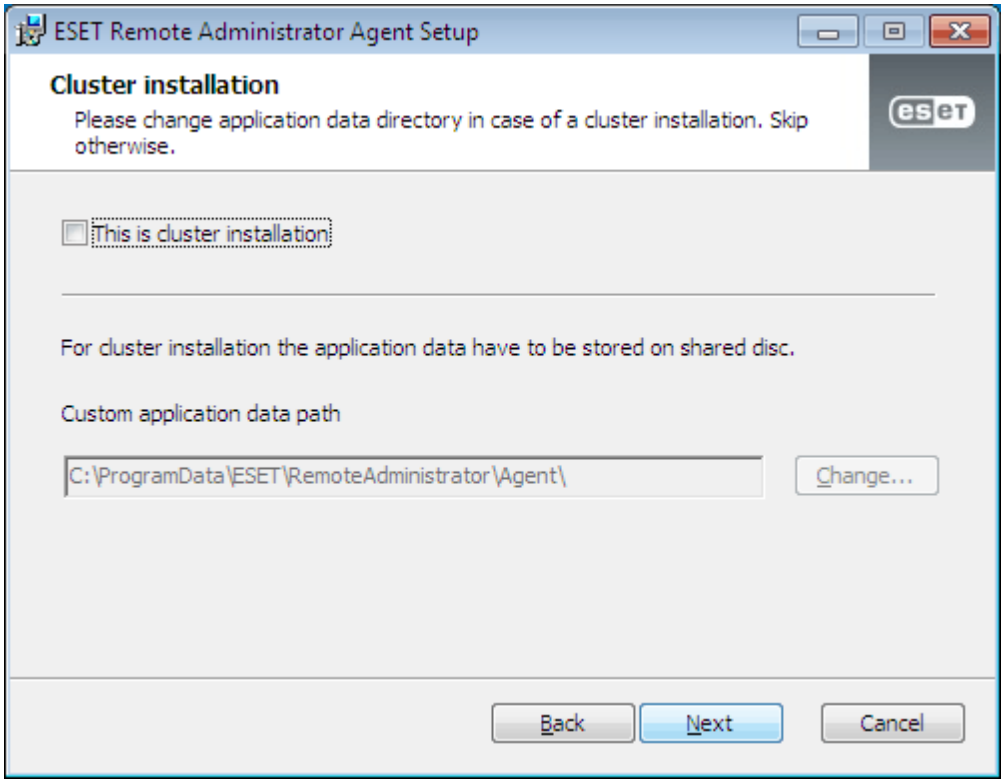
3.1.4.3 Installation de l'Agent - Windows

Cette rubrique concerne l'installation locale d'ERA Agent sur un poste de travail client. Reportez-vous au Guide d'administration pour d'autres méthodes d'installation d'ERA Agent sur des clients.

Pour installer le composant ERA Agent localement sur Windows, procédez comme suit :

1. Exécutez le programme d'installation d'ERA Agent et acceptez les termes du CLUF si vous êtes d'accord avec ces derniers.

REMARQUE : si vous installez ERA Agent sur un cluster de basculement, cochez la case en regard de l'option **Il s'agit d'une installation de cluster**. Dans le cas contraire, ne la cochez pas.



2. Si vous procédez à l'installation sur un cluster de basculement, indiquez le **chemin d'accès aux données de l'application personnalisée** pour pointer vers le stockage partagé du cluster. Les données doivent être stockées à un emplacement accessible par tous les nœuds du cluster.
3. Saisissez l'**hôte du serveur** (nom ou adresse IP d'ERA Server) et le **port du serveur** (le port par défaut est 2222 ; si vous utilisez un autre port, remplacez le port par défaut par votre numéro de port personnalisé).

IMPORTANT : assurez-vous que l'**hôte du serveur** correspond à au moins une des valeurs (idéalement FQDN) définies dans le champ **Hôte** du **certificat de serveur**. Dans le cas contraire, une erreur se produira indiquant que « Le certificat de serveur reçu n'est pas valide ». Une exception cependant : si un caractère générique (*) est placé dans le champ Hôte du certificat de serveur, il fonctionnera avec n'importe quel **hôte de serveur**.

4. Sélectionnez l'une des options d'installation suivantes, puis suivez la procédure de la section adéquate :

   - **Installation assistée du serveur** : vous devez indiquer les informations d'identification de l'administrateur d'ERA Web Console (le programme d'installation télécharge automatiquement les certificats requis).
   - **Installation hors connexion** : vous devez indiquer un **certificat d'agent** qui peut être exporté depuis ESET Remote Administrator. Vous pouvez également utiliser un certificat personnalisé.

Installation assistée du serveur :

1. Saisissez le nom ou l'adresse IP d'ERA Server dans le champ Hôte du serveur. Laissez le **port de la console Web** sur le port par défaut 2223 si vous n'utilisez pas de port personnalisé. Saisissez aussi les informations d'identification du compte de l'administrateur de la console Web dans les champs **Nom d'utilisateur** et **Mot de passe**.

IMPORTANT : assurez-vous que l'**hôte du serveur** correspond à au moins une des valeurs (idéalement FQDN) définies dans le champ **Hôte** du **certificat de serveur**. Dans le cas contraire, une erreur se produira indiquant que « Le certificat de serveur reçu n'est pas valide ». Une exception cependant : si un caractère générique (*) est placé dans le champ Hôte du certificat de serveur, il fonctionnera avec n'importe quel **hôte de serveur**.

2. Cliquez sur Oui lorsque le système vous demande si vous souhaitez accepter le certificat.

3. Sélectionnez **Ne pas créer d'ordinateur** ou **Choisir un groupe statique personnalisé**. Si vous cliquez sur **Choisir un groupe statique personnalisé**, vous pourrez effectuer une sélection dans une liste de groupes statiques existants dans ERA. L'ordinateur sera ajouté au groupe sélectionné.

4. Indiquez un dossier de destination pour ERA Agent (il est recommandé d'utiliser l'emplacement par défaut), cliquez sur **Suivant**, puis sur **Installer**.

Installation hors connexion :

1. Cliquez sur **Parcourir** et accédez à l'emplacement de votre certificat homologue (il s'agit du certificat de l'Agent que vous avez exporté depuis ERA). Laissez le champ **Mot de passe du certificat** vide dans la mesure où ce certificat ne requiert pas de mot de passe. Il n'est pas nécessaire de rechercher une **autorité de certification**. Vous pouvez laisser le champ correspondant vide.

REMARQUE : si vous utilisez un certificat personnalisé avec ERA (au lieu des certificats par défaut qui ont été automatiquement générés pendant l'installation d'ESET Remote Administrator), utilisez-le en conséquence.

2. Cliquez sur **Suivant** pour procéder à l'installation dans le dossier par défaut. Vous pouvez cliquer sur **Modifier** pour sélectionner un autre dossier d'installation (il est recommandé d'utiliser l'emplacement par défaut).

3.1.4.4 Installation de la console Web - Windows

Pour installer le composant ERA Web Console sur Windows, procédez comme suit :

1. Vérifiez que les conditions préalables requises suivantes sont remplies :
   - Java - utilisez toujours la dernière version officielle de Java (la console Web ERA requiert Java version 7 au minimum, mais il est vivement recommandé d'utiliser la dernière version).
   - Apache Tomcat (version 6 ou ultérieure)
   - Le fichier de la console Web (*era.war*) est enregistré sur votre disque dur local.
2. Copiez *era.war* dans le dossier des applications Web Tomcat (sur la plupart des systèmes d'exploitation : *C:\Program Files (x86)\Apache Software Foundation\Tomcat 7.0\webapps\).*
3. Redémarrez le service *Apache Tomcat*.
4. Ouvrez https://localhost/era/ dans votre navigateur sur localhost. Un écran de connexion s'affiche alors.

3.1.4.4.1 Navigateurs Web pris en charge

Navigateur Web	Version
Mozilla Firefox	20+
Internet Explorer	10+
Chrome	23+
Safari	6+
Opera	15+

3.1.4.5 Installation du proxy - Windows

Pour installer le composant serveur ERA Proxy sur Windows, procédez comme suit :

1. Vérifiez que toutes les conditions préalables requises sont remplies.

REMARQUE : si vous installez le serveur ERA Proxy sur un cluster de basculement, cochez la case en regard de l'option **Il s'agit d'une installation de cluster**. Dans le cas contraire, ne la cochez pas.

2. Si vous procédez à l'installation sur un cluster de basculement, indiquez le **chemin d'accès aux données de l'application personnalisée** pour pointer vers le stockage partagé du cluster. Les données doivent être stockées à un emplacement accessible par tous les nœuds du cluster.
3. Sélectionnez un compte d'utilisateur du service. Ce compte est utilisé pour exécuter le service ESET Remote Administrator Server. Les options disponibles sont les suivantes :
   a. Compte de service réseau
   b. Compte personnalisé : DOMAINE/NOMUTILISATEUR
4. Connectez-vous à une base de données. Toutes les données, du mot de passe ERA Web Console aux journaux des ordinateurs clients, y sont stockées. Vous serez invité à entrer les informations suivantes :
   a. **Base de données** : MySQL Server/MS SQL Server/MS SQL Server via l'authentification Windows
   b. **Pilote ODBC** : pilote MySQL ODBC 5.1/pilote ANSI MySQL ODBC 5.2/SQL Server
   c. **Nom de l'hôte :** nom d'hôte ou adresse IP de votre serveur de base de données
   d. **Port** utilisé pour la connexion au serveur
   e. **Nom de la base de données** : nom d'hôte ou adresse IP de votre serveur de base de données
   f. Nom d'utilisateur et mot de passe du compte d'administrateur de la base de données
   g. Votre nom d'utilisateur et **mot de passe** de la base de données ERA

Cette étape vérifie la connexion à la base de données. Si la connexion est correctement établie, vous pouvez passer à l'étape suivante. Un message d'erreur s'affiche si aucune connexion ne peut être établie.

5. Sélectionnez un port de communication proxy. Par défaut, le port 2222 est utilisé.

6. Configurez la connexion du proxy à ESET Remote Administrator Server. Saisissez un **hôte de serveur** (nom d'hôte/ adresse IP d'ERA Server) et le **port du serveur** (2222).

IMPORTANT : assurez-vous que l'**hôte de serveur** correspond à au moins une des valeurs (idéalement FQDN) définies dans le champ **Hôte** du **certificat de serveur**. Dans le cas contraire, une erreur se produira indiquant que « Le certificat de serveur reçu n'est pas valide ». Une exception cependant : si un caractère générique (*) est placé dans le champ Hôte du certificat de serveur, il fonctionnera avec n'importe quel **hôte de serveur**.

7. Sélectionnez un certificat homologue et un mot de passe pour ce certificat. Vous pouvez éventuellement ajouter une autorité de certification. Elle n'est nécessaire que pour les certificats non signés.
8. Sélectionnez un dossier d'installation pour le **proxy** ou conservez le dossier prédéfini.
9. Cliquez sur **Installer**. Le **proxy** est installé sur votre ordinateur.

REMARQUE : l'installation assistée du serveur n'est pas prise en charge lors de l'installation d'ERA Proxy.

3.1.4.5.1 Conditions préalables requises pour le proxy - Windows

Pour installer le composant serveur ERA Proxy sur Windows, les conditions préalables requises suivantes doivent être remplies :

- **ERA Server** et **ERA Web Console** sont installés (sur un ordinateur serveur).
- Le certificat de proxy est créé et téléchargé sur le lecteur local.
- L'autorité de certification est préparée sur le lecteur local.
- Vous disposez d'une licence valide.
- Un serveur de base de données est déjà installé et configuré.
- Un pilote ODBC destiné à la connexion au serveur de base de données (MySQL / MS SQL) est installé sur l'ordinateur.
- L'Agent doit être installé sur un ordinateur local pour prendre entièrement en charge toutes les fonctionnalités du programme.

3.1.4.6 Installation de RD Sensor - Windows

Pour installer le composant RD Sensor sur Windows, procédez comme suit :

1. Vérifiez que toutes les conditions préalables requises sont remplies.
2. Double-cliquez sur le fichier d'installation de RD Sensor pour commencer l'installation.
3. Sélectionnez l'emplacement d'installation de RD, puis cliquez sur **Suivant** > **Installer**.

3.1.4.6.1 Conditions préalables requises pour RD Sensor - Windows

Pour installer le composant RD Sensor sous Windows, les conditions préalables requises suivantes doivent être remplies :

- WinPcap : utilisez la dernière version de WinPcap (version 4.1.0 ou ultérieure).
- Le réseau doit être correctement configuré (les ports adéquats doivent être ouverts, les communications entrantes ne doivent pas être bloquées par un pare-feu, etc.).
- ERA Server doit être accessible.
- ERA Agent doit être installé sur l'ordinateur local pour prendre entièrement en charge toutes les fonctionnalités du programme.
- Le fichier journal de Rogue Detection Sensor figure à cet emplacement : *C:\ProgramData\ESET\Rouge Detection Sensor\Logs\trace.log*

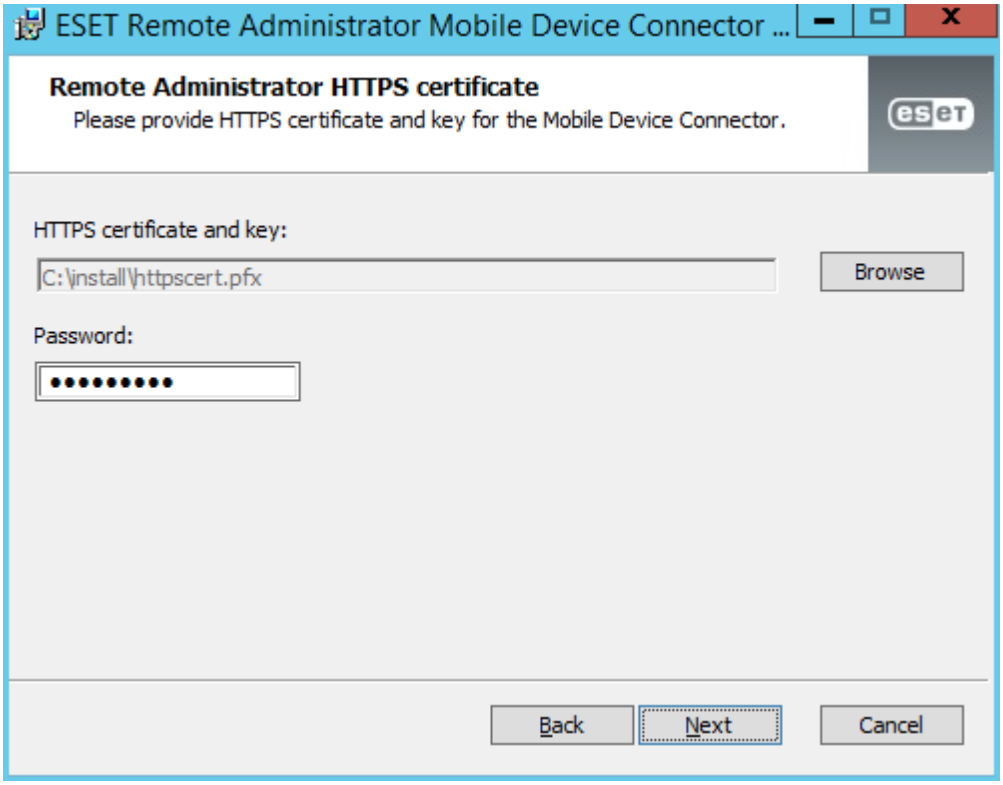
3.1.4.7 Installation du Connecteur de périphérique mobile - Windows

Vous pouvez installer le composant Connecteur de périphérique mobile sur un autre ordinateur que celui sur lequel s'exécute ERA, par exemple lorsque vous souhaitez que le Connecteur de périphérique mobile soit accessible depuis Internet pour que les périphériques mobiles de l'utilisateur puissent être gérés à tout moment, indépendamment de leur emplacement.

REMARQUE : Tenez compte du fait que le périphérique mobile communique avec le Connecteur de périphérique mobile, ce qui affecte inévitablement l'utilisation des données mobiles. C'est notamment le cas en itinérance.

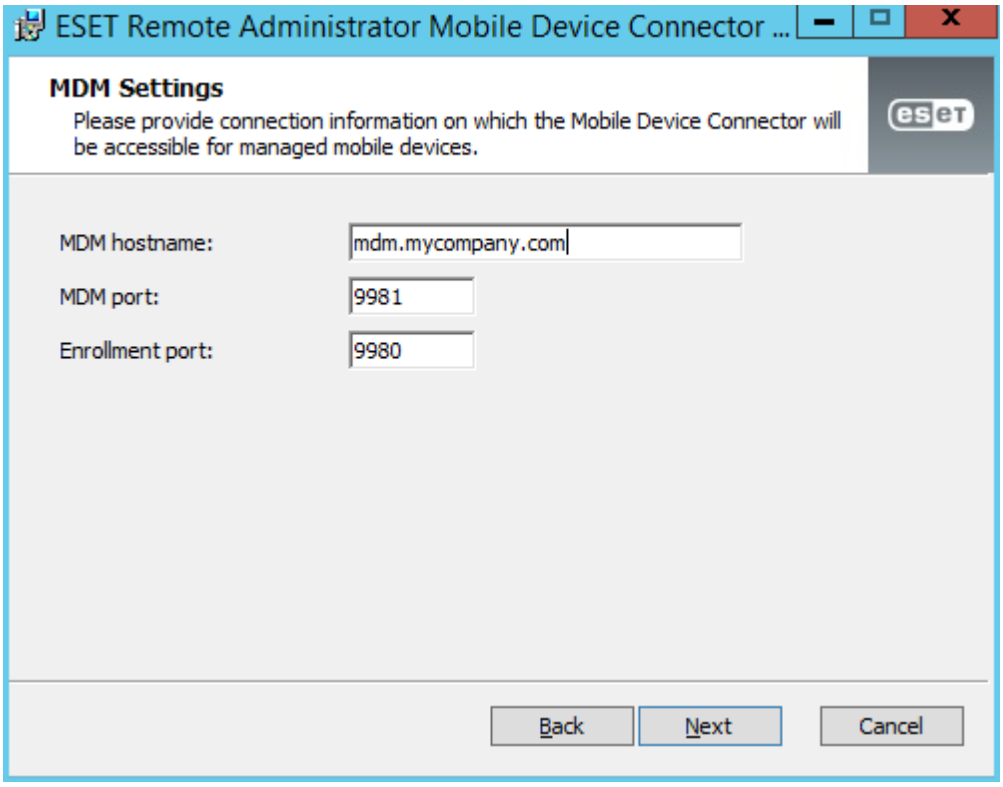
Pour installer le Connecteur de périphérique mobile sur Windows, procédez comme suit :

1. Vérifiez que toutes les conditions préalables requises sont remplies.
2. Exécutez le programme d'installation du Connecteur de périphérique mobile et acceptez les termes du CLUF si vous êtes d'accord avec ces derniers.
3. Cliquez sur **Parcourir**, accédez à l'emplacement de votre certificat SSL pour les communications via HTTPS, puis saisissez le mot de passe de ce certificat :



4. Indiquez le **Nom d'hôte MDM :** il s'agit du nom de votre serveur MDM tel qu'il est visible et accessible par des périphériques mobiles depuis l'extérieur. Si vous devez changer le nom d'hôte de votre serveur MDM, faites-le dans son fichier de configuration. Il est conseillé d'utiliser les numéros de ports par défaut 9981 et 9980, mais ceux-ci peuvent également être modifiés dans le fichier de configuration de votre serveur MDM si nécessaire.

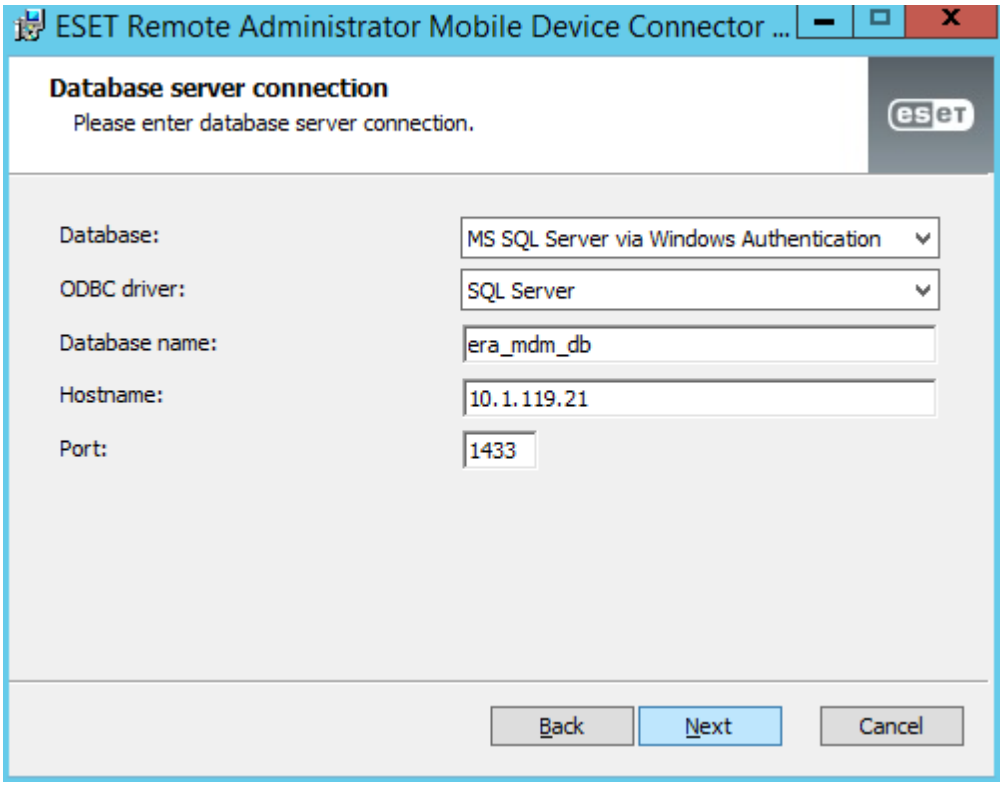
REMARQUE : vérifiez que les périphériques mobiles sont en mesure de se connecter via ces deux ports au serveur sur lequel vous installez le Connecteur de périphérique mobile. Modifiez les paramètres du pare-feu et/ou du réseau (le cas échéant) pour rendre cette connexion possible.



5. Le programme d'installation doit créer une base de données qui sera utilisée par le Connecteur de périphérique mobile. Vous devez donc indiquer les informations de connexion :

- **Base de données** : MySQL Server/MS SQL Server/MS SQL Server via l'authentification Windows
- **Pilote ODBC** : pilote MySQL ODBC 5.1/pilote Unicode MySQL ODBC 5.2/pilote unicode MySQL ODBC 5.3/ SQL Server/client natif SQL Server 10.0/pilote ODBC 11 pour SQL Server
- **Nom de la base de données** : vous pouvez conserver le nom prédéfini ou le modifier en cas de besoin
- **Nom de l'hôte** : nom d'hôte ou adresse IP du serveur de base de données
- **Port :** utilisé pour les connexions au serveur de base de données
- **Nom d'utilisateur/Mot de passe** du compte d'administrateur de base de données

REMARQUE : il est recommandé d'utiliser le même serveur de base de données que celui utilisé pour la base de données ERA. Ce serveur peut être toutefois différent si nécessaire. Lorsque vous cliquez sur le bouton Suivant, le programme d'installation du Connecteur de périphérique mobile crée sa base de données.



6. Indiquez l'utilisateur de la base de données Connecteur de périphérique mobile nouvellement créée. Vous pouvez **créer un utilisateur** ou **utiliser un utilisateur de base de données existant**. Saisissez le mot de passe de l'utilisateur de la base de données.

7. Saisissez l'**hôte du serveur** (nom ou adresse IP d'ERA Server) et le **port du serveur** (le port par défaut est 2222 ; si vous utilisez un autre port, remplacez le port par défaut par votre numéro de port personnalisé).

Vous disposez maintenant de deux options pour continuer l'installation :

- **Installation assistée du serveur** : vous devez indiquer les informations d'identification de l'administrateur d'ERA Web Console (le programme d'installation télécharge automatiquement les certificats requis).
- **Installation hors connexion** : vous devez indiquer un **certificat d'agent** qui peut être exporté depuis ESET Remote Administrator. Vous pouvez également utiliser un certificat personnalisé.

Cette procédure s'applique si vous choisissez **Installation assistée du serveur** :

8. Saisissez l'**hôte du serveur** (nom ou adresse IP d'ERA Server) et le **port de la console Web** (conservez le port 2223 par défaut si vous n'utilisez pas de port personnalisé). Indiquez également les informations d'indentification du compte d'administrateur de la console Web : **Nom d'utilisateur/Mot de passe**.

9. Lorsque le système vous demande d'**accepter le certificat**, cliquez sur **Oui**.

10. Indiquez un dossier de destination pour le Connecteur de périphérique mobile (il est recommandé d'utiliser l'emplacement par défaut), cliquez sur **Suivant**, puis sur **Installer**.

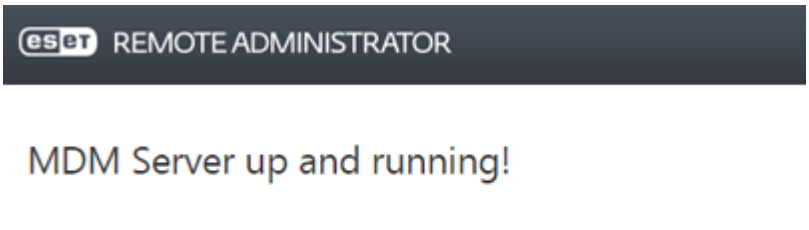
Cette procédure s'applique si vous choisissez **Installation hors connexion** :

8. Cliquez sur **Parcourir** et accédez à l'emplacement de votre certificat homologue (il s'agit du certificat de l'Agent que vous avez exporté depuis ERA). Laissez le champ **Mot de passe du certificat** vide dans la mesure où ce certificat ne requiert pas de mot de passe.

REMARQUE : si vous utilisez vos certificats personnalisés avec ERA (au lieu de ceux qui ont été automatiquement générés pendant l'installation d'ESET Remote Administrator), utilisez-les en conséquence.

9. Cliquez sur **Suivant** pour procéder à l'installation dans le dossier par défaut. Vous pouvez cliquer sur **Modifier...** pour sélectionner un autre dossier d'installation (il est recommandé d'utiliser l'emplacement par défaut).

Une fois l'installation terminée, vérifiez si le Connecteur de périphérique mobile fonctionne correctement en ouvrant https://*votre-nom_hôte-mdm*:*port-inscription* (https://eramdm:9980, par exemple) dans votre navigateur Web. Si l'installation a été effectuée correctement, le message suivant s'affiche :



Vous pouvez également utiliser cette URL pour vérifier la disponibilité du serveur Connecteur de périphérique mobile depuis Internet (en cas de configuration adéquate) en la visitant à partir d'un périphérique mobile par exemple. Si vous ne parvenez pas à accéder à la page, vérifiez votre pare-feu et d'autres configurations de votre infrastructure réseau.

Une fois que vous avez installé le Connecteur de périphérique mobile, vous devez l'activer à l'aide de la licence ESET Endpoint Security pour Android :

1. Ajoutez la licence **ESET Endpoint Security pour Android** à ERA License Management en suivant les étapes décrites ici.
2. Activez le Connecteur de périphérique mobile à l'aide de la tâche de client Activation de produit. La procédure est identique à celle permettant d'activer un produit de sécurité ESET sur un ordinateur client (dans le cas présent, le Connecteur de périphérique mobile correspond à l'ordinateur client).

3.1.4.7.1 Conditions préalables requises pour le Connecteur de périphérique mobile - Windows

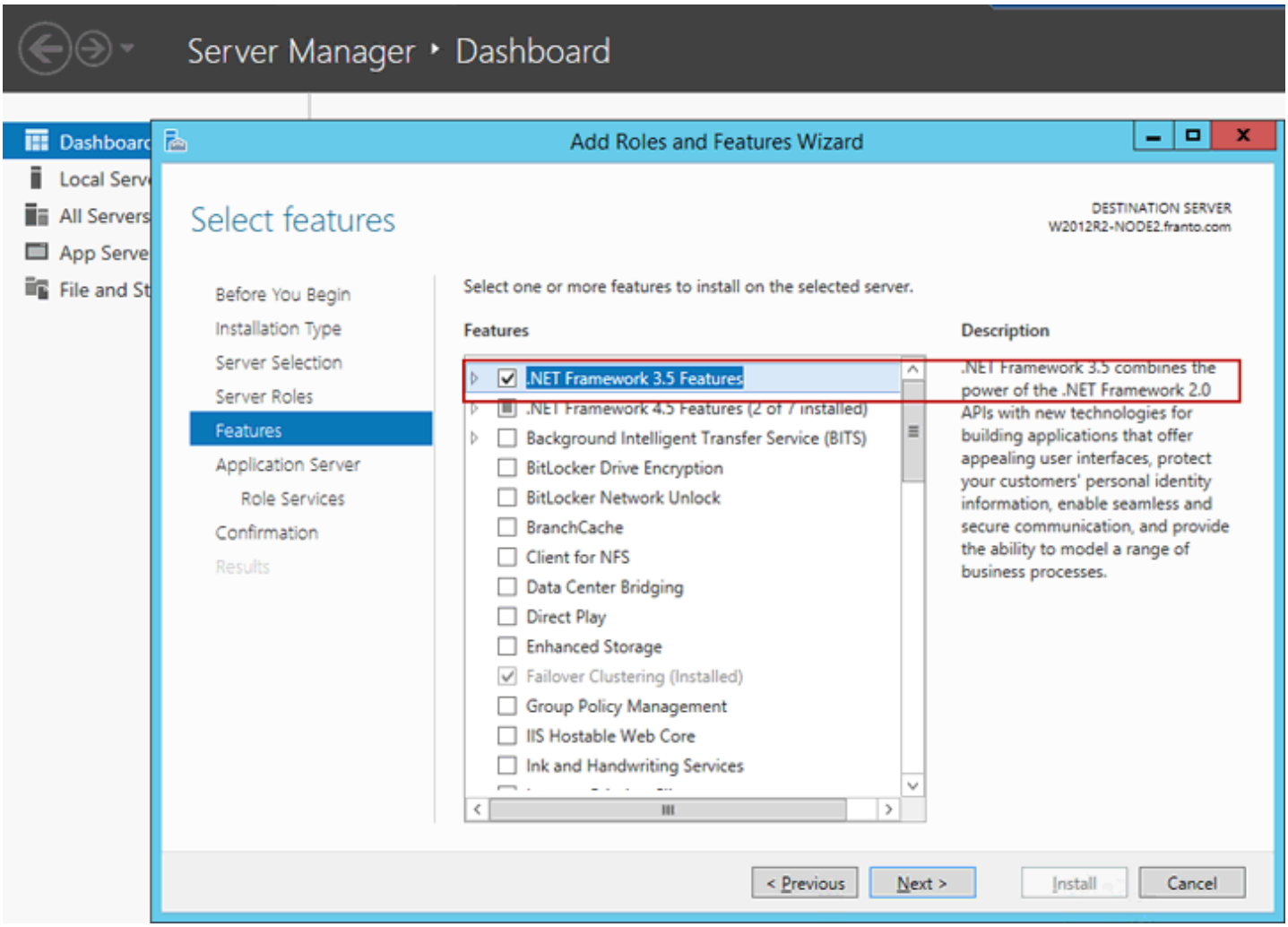
Pour installer le Connecteur de périphérique mobile sur Windows, les conditions préalables requises suivantes doivent être remplies :

- Les ports sont ouverts et disponibles. Consultez la liste complète des ports ici.
- Paramètres de pare-feu : si vous installez le Connecteur de périphérique mobile sur un système d'exploitation autre que serveur comme Windows 7 (à des fins d'évaluation uniquement), veillez à autoriser les ports de communication en créant des règles du pare-feu pour :
  C:\Program Files\ESET\RemoteAdministrator\MDMCore\ERAMDMCore.exe, port TCP 9980
  C:\Program Files\ESET\RemoteAdministrator\MDMCore\ERAMDMCore.exe, port TCP 9981
  C:\Program Files\ESET\RemoteAdministrator\Server\ERAServer.exe, port TCP 2222

REMARQUE : les chemins d'accès actuels aux fichiers `.exe` peuvent varier selon l'installation de chaque composant ERA sur le système d'exploitation client.

- Java Runtime Environment (JRE) doit être installé (vous pouvez le télécharger à l'adresse http://java.com/en/download/). Utilisez toujours la dernière version officielle de Java.

- Microsoft .NET Framework 3.5 doit être installé. Si vous exécutez Windows Server 2008 ou 2012, vous pouvez l'installer à l'aide de **l'Assistant Ajout de rôles et de fonctionnalités** (comme illustré ci-dessous). Si vous utilisez Windows Server 2003, vous pouvez télécharger .NET 3.5 à l'adresse suivante : http://www.microsoft.com/en-us/download/details.aspx?id=21



REMARQUE : si vous choisissez d'installer Microsoft SQL Server Express lors de l'installation d'ESET Remote Administrator, vous ne serez pas en mesure de l'installer sur un contrôleur de domaine. Cela risque de se produire si vous utilisez Microsoft SBS. . Dans ce cas, il est recommandé d'installer ESET Remote Administrator sur un autre serveur ou de ne pas sélectionner le composant SQL Server Express lors de l'installation (vous devez dans ce cas utiliser un serveur SQL Server ou MySQL existant pour exécuter la base de données ERA).

REMARQUE : ERA Server stocke des blobs de données volumineux dans la base de données. Pour qu'ERA s'exécute correctement, il est donc nécessaire de configurer MySQL pour accepter des paquets de grande taille. Pour obtenir des instructions pour cette configuration, reportez-vous au FAQ.

IMPORTANT : vous avez besoin d'un **certificat SSL** au format `.pfx` pour sécuriser les communications sur HTTPS. Il est recommandé d'utiliser le certificat fourni par l'autorité de certification. Les certificats signés automatiquement ne sont pas recommandés, car les périphériques mobiles ne permettent pas tous de les accepter. Les certificats signés par l'autorité de certification ne posent pas de problèmes, car ils sont approuvés et ne nécessitent pas d'être acceptés par l'utilisateur.

IMPORTANT : en cas d'installation hors connexion , vous avez également besoin d'un **certificat d'agent** exporté depuis ESET Remote Administrator. Vous pouvez également utiliser un certificat personnalisé avec ERA.

3.1.4.8 Installation du proxy HTTP Apache - Windows

Le proxy HTTP Apache est un service qui peut être utilisé conjointement avec ESET Remote Administrator 6 (et version ultérieure) pour distribuer des mises à jour aux ordinateurs clients et des packages d'installation à ERA Agent. Le proxy HTTP joue un rôle similaire au serveur miroir de ESET Remote Administrator 5 et version antérieure. Le proxy HTTP offre les avantages suivants :

- Il télécharge les mises à jour de la base des signatures de virus et des composants du produit, puis les distribue aux clients du réseau.
- Il peut mettre en cache les packages d'installation des produits ESET.
- Il permet de réduire le trafic sur votre réseau.

REMARQUE : pour les mises à jour de la base de données de virus hors connexion, utilisez l'outil Miroir au lieu du proxy HTTP Apache. Cet outil est disponible pour les deux plates-formes (Windows et Linux).

Pour installer le proxy HTTP Apache sous Windows, procédez comme suit :

1. Ouvrez le fichier ApacheHttp.zip et extrayez les fichiers dans le dossier *C:\Program Files\Apache HTTP Proxy*
2. Ouvrez une invite de commande d'administration et placez-vous dans le dossier *C:\Program Files\Apache HTTP Proxy\bin*
3. Exécutez la commande suivante :

```
httpd.exe -k install -n ApacheHttpProxy
```

4. À l'aide d'un éditeur de texte comme le Bloc-notes, ouvrez le fichier httpd.conf et ajoutez les lignes suivantes dans la partie inférieure du fichier :

```
ServerRoot "C:\Program Files\Apache HTTP Proxy"
DocumentRoot "C:\Program Files\Apache HTTP Proxy\htdocs"
<Directory "C:\Program Files\Apache HTTP Proxy\htdocs">
Options Indexes FollowSymLinks
AllowOverride None
Require all granted
</Directory>
CacheRoot "C:\Program Files\Apache HTTP Proxy\cache"
```

5. Démarrez le service proxy HTTP Apache à l'aide de la commande suivante :

```
sc start ApacheHttpProxy
```

6. Vous pouvez vérifier que le service proxy HTTP Apache est en cours d'exécution dans le composant logiciel enfichable services.msc (recherchez ApacheHttpProxy). Par défaut, le service est configuré pour démarrer automatiquement.

Suivez les étapes ci-dessous pour configurer un nom d'utilisateur et un mot de passe pour le proxy HTTP Apache (recommandé) :

1. Vérifiez la présence des modules suivants dans *Apache HTTP Proxy\conf\httpd.conf* :

```
LoadModule authn_core_module modules\mod_authn_core.dll
LoadModule authn_file_module modules\mod_authn_file.dll
LoadModule authz_groupfile_module modules\mod_authz_groupfile.dll
LoadModule auth_basic_module modules\mod_auth_basic.dll
```

2. Ajoutez les lignes suivantes à *Apache HTTP Proxy\conf\httpd.conf* sous `<Proxy *>` :

```
AuthType Basic
AuthName "Password Required"
AuthUserFile password.file
AuthGroupFile group.file
Require group usergroup
```

3. Utilisez la commande `htpasswd` pour créer un fichier appelé `password.file` dans le dossier *Apache HTTP Proxy\bin* (vous serez invité à fournir un mot de passe) :

```
htpasswd.exe -c ..\password.file username
```

4. Créez manuellement le fichier `group.file` dans le dossier *Apache HTTP Proxy* avec le contenu suivant :

```
usergroup:username
```

5. Testez la connexion au proxy HTTP en accédant à l'URL suivante dans votre navigateur :

   http://localhost:3128/index.html

REMARQUE : après avoir terminé avec succès l'installation du proxy HTTP Apache, vous pouvez autoriser uniquement les communications ESET (en bloquant le reste du trafic) ou autoriser tout le trafic. Effectuez les changements de configuration requis comme indiqué ici :

- Transfert pour les communications ESET uniquement
- Chaînage du proxy (ensemble du trafic)

La commande suivante affiche une liste de contenus actuellement mis en cache dans le proxy :

C:\Apache_HTTP_Proxy_Install_Folder\bin>htcacheclean.exe -a -p"C:\ProgramData\Apache HTTP Proxy\cache"

Utilisez l'outil htcacheclean pour nettoyer le cache de disque. Cet outil peut s'exécuter manuellement ou en mode démon. Indiquez la limite de taille totale du cache de disque. Par défaut, la valeur est exprimée en octets (associez O au nombre). Ajoutez un K pour kilo-octets et un M pour mégaoctets.

Pour plus d'informations, consultez cet article de la base de connaissances ou la documentation Apache Authentication and Authorization.

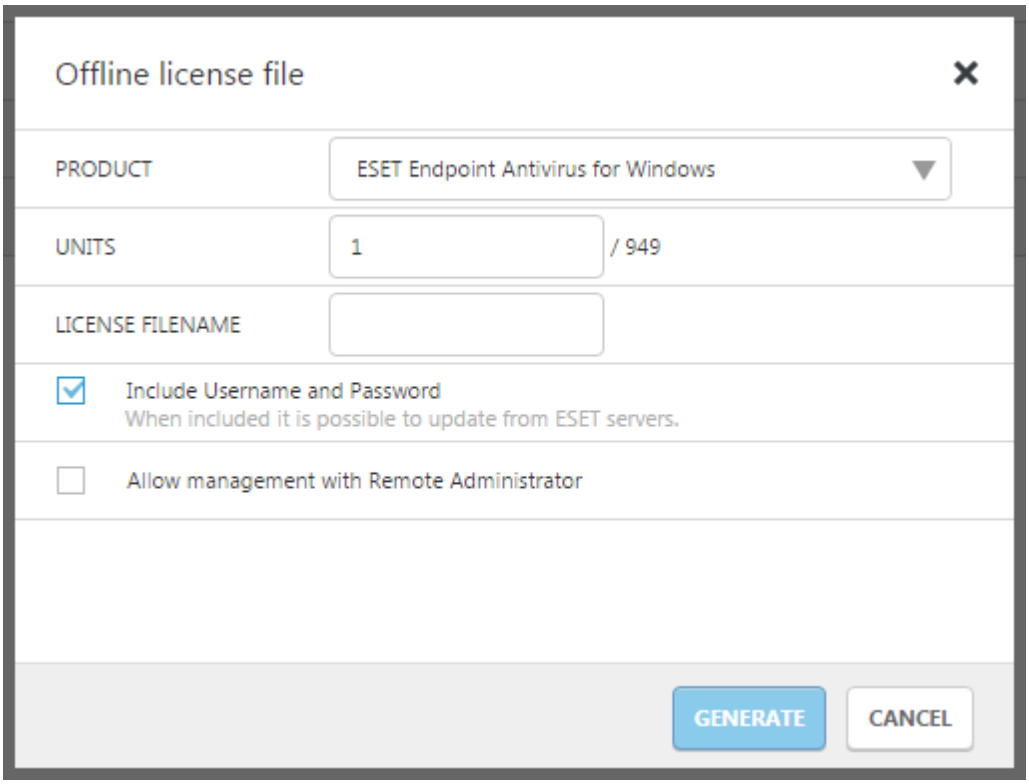
3.1.4.9 Outil Miroir

L'outil Miroir est nécessaire pour les mises à jour de la base de données de virus hors connexion. Si vos ordinateurs clients ne disposent pas d'une connexion Internet et nécessitent des mises à jour de la base de données de virus, vous pouvez utiliser l'outil Miroir pour télécharger les fichiers de mise à jour depuis les serveurs de mise à jour ESET et les stocker localement.

REMARQUE : l'outil Miroir télécharge uniquement les définitions de la base de données de virus, mais ne télécharge pas les mises à jour des composants du programme (PCU). Pour effectuer la mise à jour d'un produit de sécurité ESET sur des ordinateurs clients hors connexion, il est conseillé de mettre le produit à niveau à l'aide de la tâche d'installer un logiciel sur un client dans ERA. Vous pouvez également mettre les produits à niveau individuellement.

Conditions préalables requises :

- Le dossier cible doit être disponible en partage, Samba/Windows ou un service HTTP/FTP, selon la manière dont vous souhaitez accéder aux mises à jour.
- Vous devez disposer d'un fichier de licence hors connexion incluant le nom d'utilisateur et le mot de passe. Durant la génération d'un fichier de licence, veillez à sélectionner la case à cocher en regard du champ Inclure le nom d'utilisateur et le mot de passe. Vous devez aussi indiquer un nom de fichier de licence.



- L'outil Miroir nécessite que Visual C++ Redistributables for Visual Studio 2012 soit installé sur le système.
- L'installation ne comporte aucune étape, l'outil est composé de deux fichiers :

Windows :
`MirrorTool.exe` et `updater.dll`

Linux :
`MirrorTool` et `updater.so`

Utilisation :

- Pour afficher l'aide de l'outil Miroir, exécutez `MirrorTool --help` afin de voir toutes les commandes disponibles pour l'outil :

```
C:\Users\administrator.FRANTO\Desktop\1.0.136.0\Win32>MirrorTool.exe --help
Mirror Tool, Copyright (c) ESET, spol. s r.o. 1992-2015. All rights reserved.
Allowed options:
  --mirrorType arg                      [required]
                                        Type of mirror. Possible values (case
                                        insensitive): regular, pre-release,
                                        delayed.
  --intermediateUpdateDirectory arg     [required]
                                        Files will be downloaded to this directory
                                        to create mirror in output directory.
  --offlineLicenseFilename arg          [required]
                                        Offline license file.
  --updateServer arg                    [optional]
                                        Update server. (e.g.:http://update.eset.com
                                        /eset_upd/ep6/) Mirror will be created in
                                        output directory, only specified path in
                                        server will be mirrored.
  --outputDirectory arg                 [required]
                                        Directory where mirror will be created.
  --proxyHost arg                       [optional]
                                        Http proxy address (fqdn or IP).
  --proxyPort arg                       [optional]
                                        Http proxy port.
  --proxyUsername arg                   [optional]
                                        Http proxy username.
  --proxyPassword arg                   [optional]
                                        Http proxy password.
  --excludedProducts arg                [optional]
                                        Disable creating mirror for specified
                                        products. Possible values:ep4 ep5 ep6 era6.
  --help                                [optional]
                                        Display this help and exit
```

- Le paramètre `--updateServer` est facultatif. Si vous l'utilisez, vous devez spécifier l'URL complète du serveur de mise à jour.
- Le paramètre `--offlineLicenseFilename` est obligatoire. Vous devez indiquer un chemin d'accès à votre fichier de licence hors connexion (comme mentionné plus haut).
- Pour créer un miroir, exécutez `MirrorTool` avec au moins les paramètres minimums requis. Voici un exemple :

Windows :

```
MirrorTool.exe --mirrorType regular --intermediateUpdateDirectory c:\temp\mirrorTemp --
offlineLicenseFilename c:\temp\offline.lf --outputDirectory c:\temp\mirror
```

Linux :

```
sudo ./MirrorTool --mirrorType regular --intermediateUpdateDirectory /tmp/mirrorTool/mirrorTemp
--offlineLicenseFilename /tmp/mirrorTool/offline.lf --outputDirectory /tmp/mirrorTool/mirror
```

Paramètre de l'outil miroir et de mise à jour :

- Pour automatiser la distribution des mises à jour de la base de données de virus, vous pouvez créer une planification pour l'exécution de l'outil Miroir. Pour ce faire, ouvrez la console Web et accédez à **Tâches client** > **Système d'exploitation** > **Exécuter une commande**. Sélectionnez **Ligne de commande à exécuter** (avec un chemin d'accès à `MirrorTool.exe`) et un déclencheur raisonnable (par exemple, une expression CRON pour toutes les heures 0 0 * * * ? *). Vous pouvez également utiliser le Planificateur de tâches Windows ou CRON dans Linux.
- Pour configurer les mises à jour sur un ordinateur client, créez une stratégie et configurer le **serveur de mise à jour** afin qu'il pointe sur l'adresse miroir ou un dossier partagé.

3.1.5 Cluster de basculement - Windows

Vous trouverez ci-dessous les étapes générales nécessaires pour installer ESET Remote Administrator dans un environnement de cluster de basculement.

1. Créez un cluster de basculement. Il doit disposer d'un disque partagé, d'une adresse IP et d'un nom de cluster.
   a. Instructions pour créer un cluster de basculement dans Windows Server 2012
   b. Instructions pour créer un cluster de basculement dans Windows Server 2008
2. Installez ERA Server et ERA Agent sur le nœud actif. Sélectionnez le disque partagé en tant que stockage de données d'application.
3. Modifiez le nœud actif, puis répétez l'étape 2.
4. Dans le gestionnaire de configuration de cluster, créez 2 services de cluster : ERA Agent et ERA Server.
5. Définissez les dépendances adéquates : les services doivent démarrer après l'initialisation des ressources de l'étape 1. ERA Agent doit être également dépendant d'ERA Server.
6. La base de données et le serveur Web ne sont pas pris en charge sur un cluster.

REMARQUE : il n'est pas possible d'installer ERA Server sur un cluster de basculement via le programme d'installation d'ERA. Pour installer ESET Remote Administrator sur un cluster de basculement, effectuez une installation de composants.

3.2 Installation de composants sur Linux

Dans la plupart des scénarios d'installation, vous devez installer différents composants ESET Remote Administrator sur des ordinateurs différents pour tenir compte des architectures réseau différentes, pour satisfaire aux exigences de performance ou pour d'autres raisons. Votre installation peut varier en fonction de la distribution Linux prise en charge qui s'exécute sur le serveur.

Composants principaux

- ERA Server
- ERA Web Console
- ERA Agent

Composants facultatifs

- ERA Proxy
- RD Sensor
- Connecteur de périphérique mobile
- Proxy HTTP Apache
- Outil Miroir

Si vous devez effectuer une mise à niveau d'ESET Remote Administrator vers la dernière version (6.x), consultez l'article de la base de connaissances.

3.2.1 Installation pas à pas sous Linux

Ce scénario d'installation simule l'installation pas à pas d'ERA Server et d'ERA Web Console. Votre installation peut varier en fonction de la distribution Linux prise en charge qui s'exécute sur le serveur. L'installation requiert que l'utilisateur soit en mesure d'utiliser la commande sudo ou d'effectuer l'installation avec les privilèges root.

Pour consulter les étapes d'installation, cliquez sur la distribution Linux que vous avez utilisée sur le serveur :

- Distributions Debian et Ubuntu
- Distributions CentOS, Red-Hat et Fedora

Avant de procéder à l'installation, vérifiez la présence du serveur de base de données et assurez-vous d'y avoir accès sur le serveur local/distant. Si aucun serveur de base de données n'est installé, vous devez en installer un et le configurer. Ce scénario simule une installation qui utilise MySQL.

Distributions Debian et Ubuntu

1. Installez les packages nécessaires pour ERA Server :

```
sudo apt-get install xvfb cifs-utils unixodbc libmyodbc
```

2. Accédez au dossier dans lequel vous avez téléchargé ERA Server et rendez le package d'installation exécutable :

```
chmod +x Server-Linux-x86_64.sh
```

3. Configurez la connexion au serveur MySQL comme indiqué dans la rubrique Configuration de MySQL.
4. Configurez le pilote MySQL ODBC comme indiqué dans la rubrique Configuration d'ODBC.
5. Personnalisez les paramètres d'installation et exécutez l'installation d'ERA Server. Pour plus d'informations, reportez-vous à la section Installation du serveur - Linux.
6. Installez les packages **java** et **tomcat** nécessaires pour la console Web ERA :

```
sudo apt-get install openjdk-7-jdk tomcat7
```

7. Déployez le package de la console Web era.war dans le dossier de l'application Web tomcat :

```
sudo cp era.war /var/lib/tomcat7/webapps/
```

8. Redémarrez le service tomcat :

```
sudo service tomcat7 restart
```

9. Testez la connexion à ERA Web Console (voir les instructions en bas de cette rubrique).

Distributions CentOS, Red-Hat et Fedora

1. Installez les packages nécessaires pour ERA Server :

```
sudo yum install mysql-connector-odbc xvfb xorg-x11-server-Xvfb cifs-utils
```

2. Accédez au dossier dans lequel vous avez téléchargé ERA Server et rendez le package d'installation exécutable :

```
chmod +x Server-Linux-x86_64.sh
```

3. Modifiez le fichier de configuration MySQL */etc/mysql/my.cnf* (ou */etc/my.cnf*) et ajoutez les lignes suivantes :

```
[mysqld]
max_allowed_packet=33M
```

4. Redémarrez le service MySQL :

```
sudo service mysql restart
```

5. Personnalisez les paramètres d'installation et exécutez l'installation d'ERA Server. Pour plus d'informations, reportez-vous à la section Installation du serveur - Linux.

6. Installez les packages **java** et **tomcat** nécessaires pour la console Web ERA :

```
yum install java-1.8.0-openjdk tomcat
```

7. Déployez le package de la console Web era.war dans le dossier de l'application Web tomcat :

```
sudo cp era.war /var/lib/tomcat/webapps/
```

8. Redémarrez le service tomcat :

```
sudo service tomcat restart
```

Testez la connexion à ERA Web Console après l'installation. Ouvrez le lien suivant dans votre navigateur sur localhost (un écran de connexion doit s'afficher) :

`http://localhost:8080/era` ou, si vous accédez à distance au serveur : `http://ADRESSE_IP_OU_NOM_HÔTE:8080/era`

3.2.2 Configuration MySQL

Pour installer **MySQL**, exécutez la commande suivante depuis la ligne de commande d'un terminal :

```
sudo apt-get install mysql-server
```

Saisissez un mot de passe pour l'utilisateur **racine** d'administration de MySQL quand vous y êtes invité. Si vous laissez le champ vide, le mot de passe n'est pas modifié. Vous êtes invité à répéter le mot de passe que vous avez saisi.

Le serveur MySQL doit démarrer automatiquement quand l'installation est terminée.
Tapez la commande suivante pour vérifier si le serveur MySQL est en cours d'exécution :

```
sudo netstat -tap | grep mysql
```

Si le serveur MySQL est exécuté, la ligne suivante sera affichée. Notez que l'identifiant du processus PID (7668 dans l'exemple suivant) est différent :

```
tcp 0 0 localhost:mysql *:* LISTEN 7668/mysqld
```

Si vous ne voyez pas cette ligne, cela signifie que le serveur MySQL ne fonctionne pas correctement. Tapez la commande suivante pour le redémarrer.

```
sudo service mysql restart
```

Exécutez la commande suivante pour ouvrir le fichier **my.cnf** dans un éditeur de texte :

```
sudo nano /etc/mysql/my.cnf
```

Copiez la configuration suivante dans le fichier **my.cnf**, puis enregistrez et fermez le fichier :

```
[mysqld]
max_allowed_packet=33M
```

3.2.3 Configuration ODBC

Pour installer le pilote **MySQL ODBC** (Open Database Connectivity), exécutez la commande suivante depuis un terminal :

```
sudo apt-get install libmyodbc libodbc1
```

Exécutez la commande suivante pour ouvrir le fichier **odbcinst.ini** dans un éditeur de texte :

```
sudo nano /etc/odbcinst.ini
```

Copiez la configuration suivante dans le fichier **odbcinst.ini**, puis enregistrez et fermez le fichier :

```
[MySQL]
Description = ODBC for MySQL
Driver = /usr/lib/x86_64-linux-gnu/odbc/libmyodbc.so
Setup = /usr/lib/x86_64-linux-gnu/odbc/libodbcmyS.so
FileUsage = 1
```

Les produits ERA nécessitent le pilote MySQL pour la prise en charge du multi-threading. Il s'agit du package par défaut pour les dernières versions du package unixODBC (2.3.0 ou plus récentes). Les versions plus anciennes exigent l'utilisation d'une configuration de threading explicite. Si vous disposez d'une version ancienne, ajoutez le paramètre suivant au fichier **odbcinst.ini file** :

```
Threading = 0
```

Mettez à jour les fichiers de configuration qui contrôle l'accès ODBC aux serveurs de base de données sur l'hôte actuel en exécutant la commande suivante :

```
sudo odbcinst -i -d -f /etc/odbcinst.ini
```

REMARQUE : si vous utiliser Ubuntu version 32 bits, utilisez les clés **Pilote** et **Configuration** et modifiez le chemin en « */usr/lib/i386-linux-gnu/odbc/* ». Assurez-vous que les chemins d'accès au **pilote** et à la **configuration** sont corrects.

Exécutez la commande suivante pour ouvrir le fichier **odbc.ini** dans un éditeur de texte :

```
sudo nano /etc/odbc.ini
```

Copiez la configuration suivante dans le fichier **odbc.ini**, puis enregistrez et fermez le fichier :

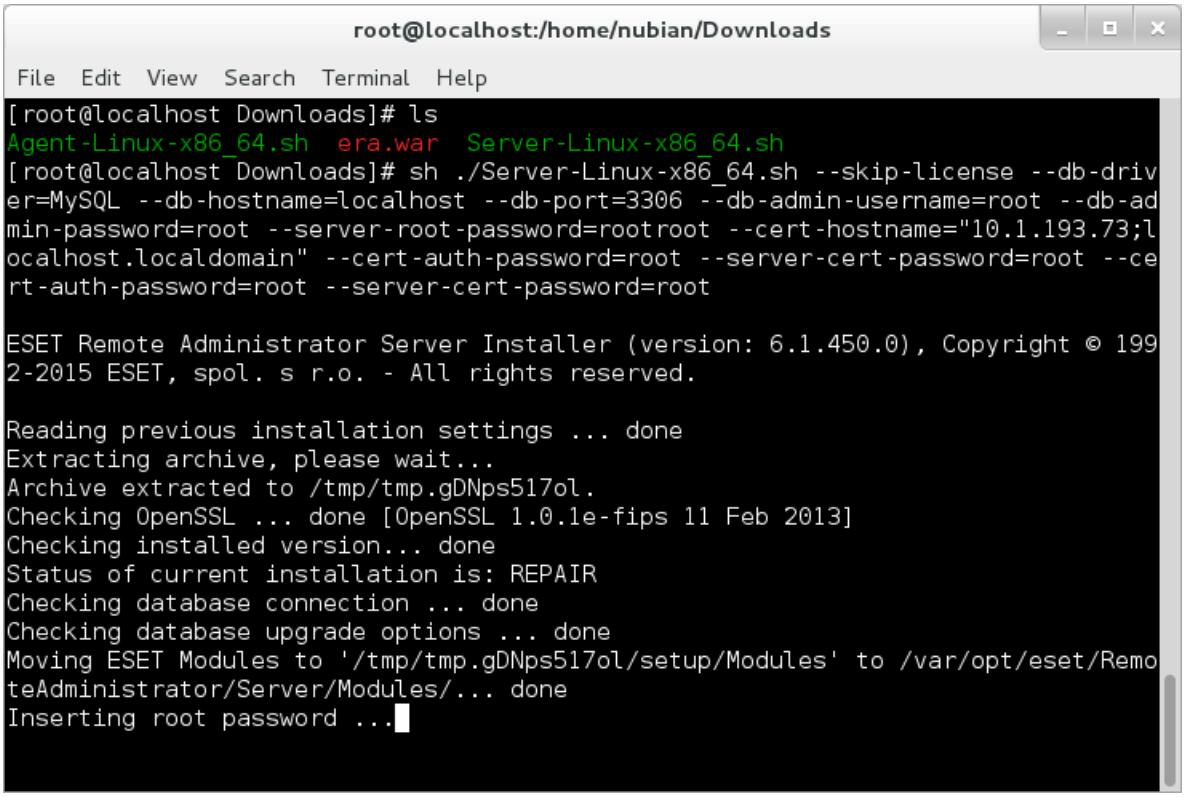
```
[MySQLconnection]
Description = MySQL connection
Driver = MySQL
Server = 10.1.179.4
Port = 3306
```

3.2.4 Installation du serveur - Linux

L'installation du composant ERA Server sur Linux est effectuée à l'aide d'une commande dans le terminal. Vérifiez que toutes les conditions préalables requises sont remplies. Vous pouvez préparer un script d'installation et l'exécuter ensuite à l'aide de *sudo*.

Exemple de script d'installation
(Les nouvelles lignes sont séparées par une barre « \ » pour copier la commande intégrale dans le terminal.)

```
sudo ./Server-Linux-x86_64.sh \
--skip-license \
--db-driver=MySQL \
--db-hostname=127.0.0.1 \
--db-port=3306 \
--db-admin-username=root \
--db-admin-password=Admin123 \
--server-root-password=Admin123 \
--db-user-username=root \
--db-user-password=Admin123 \
--cert-hostname="10.1.179.46;Ubuntu64-bb;Ubuntu64-bb.BB.LOCAL"
```



ERA Server et le service `eraserver` sont installés à l'emplacement suivant :
/opt/eset/RemoteAdministrator/Server

Vous pouvez modifier les attributs suivants :

Attribut	Description	Obligatoire
--uninstall	Désinstalle le produit.	-
--locale	Identificateur de paramètres régionaux (LCID) du serveur installé (la valeur par défaut est `en_US`). Pour connaître les options possibles, reportez-vous à la section des langues prises en charge. **Remarque :** vous pouvez définir une langue pour chaque session ERA Web Console.	Oui
--skip-license	L'installation ne demande pas à l'utilisateur de confirmer le contrat de licence.	-
--skip-cert	Ignore la génération des certificats (à utiliser avec le paramètre --server-cert-path).	-
--license-key	Clé de licence ESET. Elle peut être définie ultérieurement.	-
--product-guid	Identificateur unique global du produit. S'il n'est pas défini, il est généré.	-
--server-port	Port de ESET Remote Administrator (ERA) Server (`2222` par défaut).	-
--console-port	Port de la console ESET Remote Administrator (`2223` par défaut).	-

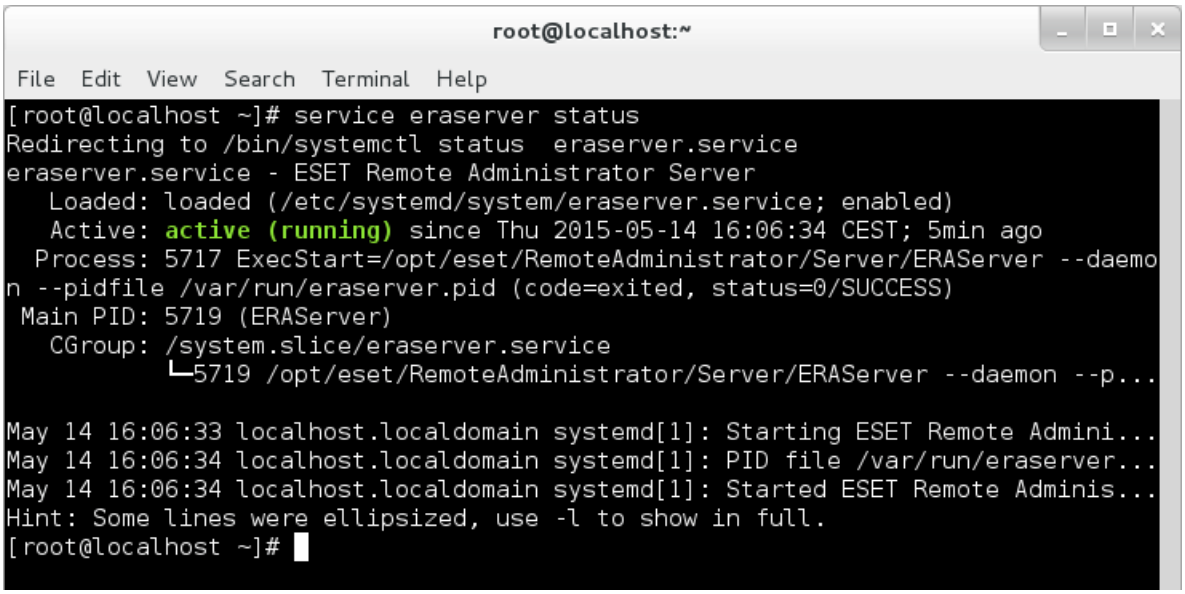
Attribut	Description	Obligatoire
--server-root-password	Mot de passe de l'utilisateur Administrateur pour la connexion à la console Web. Il doit contenir au moins 8 caractères.	Oui
--db-type	Type de base de données utilisé (les valeurs possibles sont : `MySQL Server`, `Microsoft SQL Server`)	-
--db-driver	Pilote ODBC utilisé pour la connexion à la base de données (`MySQL ODBC 5.3 ANSI Driver`, par exemple).	Oui
--db-hostname	Nom de l'ordinateur ou adresse IP du serveur de base de données.	Oui
--db-port	Port du serveur de base de données (`3306` par défaut).	Oui
--db-name	Nom de la base de données ERA Server (`era_db` par défaut).	-
--db-admin-username	Nom d'utilisateur de l'administrateur de base de données (utilisé par l'installation pour créer et modifier la base de données).	Oui
--db-admin-password	Mot de passe de l'administrateur de base de données.	Oui
--db-user-username	Nom d'utilisateur de l'utilisateur de la base de données ERA Server (utilisé par ERA Server pour la connexion à la base de données). Il ne doit pas comporter plus de 16 caractères.	Oui
--db-user-password	Mot de passe de l'utilisateur de la base de données ERA Server.	Oui
--cert-hostname	Contient tous les noms et/ou les adresses IP de l'ordinateur sur lequel ERA Server sera installé. Le nom doit correspondre au nom de serveur spécifié dans le certificat de l'Agent se connectant au serveur.	Oui
--server-cert-path	Chemin d'accès au certificat homologue du serveur (utilisez cette option si vous avez également spécifié `--skip-cert`).	-
--server-cert-password	Mot de passe du certificat homologue du serveur.	-
--agent-cert-password	Mot de passe du certificat homologue de l'Agent.	-
--cert-auth-password	Mot de passe de l'autorité de certification.	-
--cert-auth-path	Chemin d'accès au fichier d'autorité de certification du serveur.	-
--cert-auth-common-name	Nom commun de l'autorité de certification (utilisez des "").	-
--cert-organizational-unit	-	-
--cert-organization	-	-
--cert-locality	-	-
--cert-state	-	-
--cert-country	-	-
--cert-validity	Validité du certificat en jours ou années (unité spécifiée dans l'argument `--cert-validity-unit`)	-
--cert-validity-unit	Unité de la validité du certificat. Les valeurs possibles sont « Years » ou « Days » (la valeur par défaut est `Years`).	-
--ad-server	Serveur Active Directory	-
--ad-user-name	Nom de l'utilisateur disposant des droits pour effectuer des recherches sur le réseau AD.	-
--ad-user-password	Mot de passe de l'utilisateur Active Directory.	-
--ad-cdn-include	Chemin d'accès à l'arborescence Active Directory qui fera l'objet d'une synchronisation. Utilisez des guillemets vides "" pour synchroniser toute l'arborescence.	-

Journal du programme d'installation

Le journal du programme d'installation peut s'avérer utile pour résoudre des problèmes éventuels. Il figure à l'emplacement suivant :
/var/log/eset/RemoteAdministrator/EraServerInstaller.log

Une fois l'installation terminée, vérifiez que le service ERA Server est en cours d'exécution :

```
service eraserver status
```



3.2.4.1 Conditions préalables requises pour le serveur - Linux

Pour installer ERA Server sous Linux, les conditions préalables requises suivantes doivent être remplies :

- Vous devez disposer d'une licence valide.
- Un serveur de base de données doit être installé et configuré avec un compte racine. Il n'est pas nécessaire de créer un compte d'utilisateur avant l'installation ; le programme d'installation peut le créer.
- **ODBC Pilote** : ODBC Le pilote permet d'établir une connexion avec le serveur de base de données (MySQL / MS SQL).

REMARQUE : vous devez utiliser le package **unixODBC_23** (et non le package unixODBC par défaut) pour qu'ERA Server se connecte à la base de données MySQL sans aucun problème. Cela est particulièrement vrai pour SUSE Linux.

- Le fichier d'installation du serveur est défini en tant qu'exécutable. Pour ce faire, utilisez la commande suivante :

```
chmod +x Server-Linux-x86_64.sh
```

- La version minimum de openSSL prise en charge est **openssl-1.0.1e-30**
- **Xvfb** : requis pour imprimer correctement les rapports (Générer un rapport) sur les systèmes Linux Server sans interface graphique.
- **Cifs-utils** : requis pour déployer correctement l'agent sur un Windows OS.
- **Qt4 WebKit libraries** : utilisée pour imprimer les rapports aux formats PDF et PS (doivent être de la version 4.8, et non 5). Toutes les autres dépendances Qt4 sont automatiquement installées.

REMARQUE : en ce qui concerne CentOS, il est possible qu'il n'y ait pas de package dans les référentiels officiels. Vous pouvez l'installer à partir d'un référentiel tiers (les référentiels EPEL, par exemple) ou le compiler par vous-même sur un ordinateur cible.

- **Kinit + klist** : utilisés pour l'authentification Kerberos pendant la tâche de synchronisation d'Active Directory et la connexion avec un utilisateur du domaine. Une configuration Kerberos correcte est également requise (*/etc/krb5.conf*).

- **Wbinfo + ntlm auth** - utilisés pour l'authentification avec les comptes de domaine + l'authentification NTLM avec le serveur SMTP (envoi de messages électroniques).
- **Ldapsearch** : utilisé dans la tâche de synchronisation d'Active Directory.
- **Snmptrap** : Utilisé pour envoyer des interceptions SNMP. Facultatif si cette fonctionnalité n'est pas utilisée. SNMP doit aussi être configuré.
- **SELinux devel package** : utilisé pendant l'installation du produit pour créer les modules de stratégie SELinux. Ceci est uniquement requis sur les systèmes où SELinux est activé (CentOS, Fedora, RHEL).

Le tableau suivant présente les commandes de terminal appropriées pour chaque package décrit ci-dessus, pour les distributions Debian et Ubuntu et les distributions Centos, Red-Hat et Fedora :

Package	Distributions **Debian et Ubuntu**	Distributions **CentOS, Red-Hat et Fedora**
ODBC Driver	`apt-get install unixodbc libmyodbc`	`yum install mysql-connector-odbc`
xvfb	`apt-get install xvfb`	`yum install xorg-x11-server-Xvfb`
cifs-utils	`apt-get install cifs-utils`	`yum install cifs-utils`
Qt4 WebKit libraries	`apt-get install libqtwebkit4`	-
kinit + klist	`apt-get install krb5-user`	`yum install krb5-workstation`
wbinfo + ntlm_auth	`apt-get install winbind`	`yum install samba-winbind-clients`
ldapsearch	`apt-get install ldap-utils`	`yum install openldap-clients`
snmptrap	`apt-get install snmp`	`yum install net-snmp-utils`
SELinux devel package	`apt-get install selinux-policy-dev`	`yum install policycoreutils-devel`

REMARQUE : ERA Server stocke des blobs de données volumineux dans la base de données. Pour qu'ERA s'exécute correctement, il est donc nécessaire de configurer MySQL pour accepter des paquets de grande taille. Pour plus d'informations sur cette configuration, reportez-vous au FAQ.

3.2.5 Installation de l'Agent - Linux

La connexion à ERA Server est résolue à l'aide des paramètres --hostname et --port (le port n'est pas utilisé lorsqu'un enregistrement SRV est fourni). Les formats de connexion possibles sont les suivants :

- **Nom d'hôte** et **port**
- **Adresse IPv4** et **port**
- **Adresse IPv6** et **port**
- Enregistrement de service (enregistrement SRV) : pour configurer l'enregistrement de ressource DNS dans Linux, l'ordinateur doit se trouver dans un domaine avec un serveur DNS opérationnel. Voir Enregistrement de ressource DNS.

L'enregistrement SRV doit comporter le préfixe « _NAME._tcp », où « NAME » représente le nom personnalisé (era, par exemple).

Exemple de script d'installation
(Les nouvelles lignes sont séparées par une barre « \ » pour copier la commande intégrale dans le terminal.)

```
./Agent-Linux-x86_64.sh \
--skip-license \
--cert-path=/home/admin/Desktop/agent.pfx \
--cert-auth-path=/home/admin/Desktop/CA.der \
--cert-password=N3lluI4#2aCC \
--hostname=10.1.179.36 \
--port=2222
```

Attribut	Description	Obligatoire
`--skip-license`	L'installation ne demande pas à l'utilisateur de confirmer le contrat de licence.	Oui
`--cert-path`	Chemin d'accès au fichier de certificat de l'Agent.	Oui
`--cert-auth-path`	Chemin d'accès au fichier d'autorité de certification du serveur.	Oui
`--cert-password`	Mot de passe de l'autorité de certification. Doit correspondre au mot de passe du certificat de l'Agent.	Oui
`--hostname`	Nom d'hôte ou adresse IP du serveur ERA Server auquel se connecter.	Oui
`--port`	Port du serveur (`2222` par défaut) ou port du proxy (`1236` par défaut)	Oui

Paramètres facultatifs

Attribut	Description
`--product-guid`	GUID du produit (s'il n'est pas défini, il sera généré).
`--cert-content`	Contenu codé en Base64 du certificat de clé publique codée PKCS12 et clé privée utilisée pour configurer des canaux de communication sécurisés entre le serveur et les Agents. Utilisez uniquement l'une des options `--cert-path` ou `--cert-content`.
`--cert-auth-content`	: contenu codé en Base64 du certificat de clé privé de l'autorité de certification codée DER utilisé pour vérifier les homologues distants (proxy ou serveur). Utilisez uniquement l'une des options `--cert-auth-path` ou `--cert-auth-content`.
`--webconsole-hostname`	Nom d'hôte ou adresse IP utilisés par la console Web pour se connecter au serveur (si cet attribut n'est pas défini, la valeur est copiée depuis 'hostname').
`--webconsole-port`	Port utilisé par la console Web pour se connecter au serveur (`2223`, par défaut).
`--webconsole-user`	Nom d'utilisateur utilisé par la console Web pour se connecter au serveur (`Administrator`, par défaut).
`--webconsole-password`	Mot de passe utilisé par la console Web pour se connecter au serveur.
`--cert-auth-password`	Mot de passe de l'autorité de certification.

Connexion et certificats

- **Les informations de connexion à ERA Server** doivent être fournies : `--hostname`, `--port` (le port n'est pas nécessaire si l'enregistrement de service a été fourni ; la valeur par défaut est `2222`)
- Fournissez ces informations de connexion pour l'**installation assistée du serveur** : --webconsole-port, --webconsole-user, --webconsole-password
- Fournissez les informations de certificat pour l'**installation hors connexion** : `--cert-path`, `--cert-password`

Paramètres de type de mot de passe

Les paramètres de type de mot de passe peuvent être fournis en tant que variables d'environnement, fichiers, lecture à partir de stdn ou texte brut :
`--password=env:SECRET_PASSWORD`, où SECRET_PASSWORD correspond à une variable d'environnement avec le mot de passe
`--password=file:/opt/secret`, où la première ligne de file/opt/secret contient le mot de passe
`--password=stdin` donne l'instruction au programme d'installation de lire le mot de passe à partir de l'entrée standard
`--password="pass:PASSWORD"` est égal à `--password="PASSWORD"` et est obligatoire si le mot de passe est `"stdin"`(standard input) ou une chaîne commençant par `"env:"`, `"file:"` ou `"pass:"`

Journal du programme d'installation

Le journal du programme d'installation peut s'avérer utile pour résoudre des problèmes éventuels. Il figure à l'emplacement suivant :
/var/log/eset/RemoteAdministrator/EraAgentInstaller.log

Pour déterminer si l'installation a été effectuée correctement, vérifiez l'exécution du service en exécutant la commande suivante :

```
sudo service eraagent status
```

3.2.5.1 Conditions préalables requises pour l'Agent - Linux

Pour installer le composant ERA Agent sur Linux, les conditions préalables requises suivantes doivent être remplies :

- ERA Server et ERA Web Console doivent être installés.
- Un certificat pour l'Agent doit exister.
- Un fichier de clé publique de l'autorité de certification du serveur doit exister.
- L'ordinateur serveur doit être accessible depuis le réseau.
- Le fichier d'installation de l'Agent doit être défini comme exécutable (exécutez chmod +x sur le fichier pour définir ce paramètre).
- La version minimale d'openssl prise en charge est **openssl-1.0.1e-30**.

3.2.6 Installation d'ERA Web Console - Linux

Avant d'installer le composant ERA Web Console, vérifiez que toutes les conditions préalables requises sont réunies. Pour installer ERA Web Console, procédez comme suit :

1. Exécutez les commandes suivantes pour copier le fichier era.war dans le dossier :

   ```
   sudo cp era.war /var/lib/tomcat7/webapps/
   ```

   Vous pouvez également extraire le contenu du fichier era.war dans */var/lib/tomcat7/webapps/era/*

2. Exécutez la commande suivante pour redémarrer le service Tomcat et déployer le fichier .war :

   ```
   sudo service tomcat7 restart
   ```

3. Ouvrez le lien suivant dans votre navigateur sur localhost (un écran de connexion doit s'afficher) :

   http://localhost:8080/era

Testez la connexion à ERA Web Console après l'installation. Ouvrez le lien suivant dans votre navigateur sur localhost (un écran de connexion doit s'afficher) :

`http://localhost:8080/era` ou, si vous accédez à distance au serveur : `http://ADRESSE_IP_OU_NOM_HÔTE:8080/era`

3.2.6.1 Conditions préalables requises pour ERA Web Console - Linux

Pour installer le composant ERA Web Console sur Linux, les conditions suivantes doivent être remplies :

- Java - utilisez toujours la dernière version officielle de Java (ERA Web Console requiert Java version 7 au minimum, mais il est vivement recommandé d'utiliser la dernière version).
- Apache Tomcat (version 6 et ultérieure)
- Le fichier de la console Web (*era.war*) est enregistré sur votre disque dur local.

Pour installer le ou les packages **Java** et/ou **Apache Tomcat**, utilisez les commandes de terminal correspondant à la distribution Linux :

Package	Distributions Debian et Ubuntu	Distributions CentOS, Red-Hat et Fedora
Java	`sudo apt-get install openjdk-7-jdk`	`yum install java-1.8.0-openjdk`
Apache Tomcat	`sudo apt-get install tomcat7`	`yum install tomcat7`

3.2.7 Installation du proxy - Linux

1. Vérifiez que toutes les conditions préalables requises sont remplies.
2. Exécutez un script d'installation pour installer le serveur proxy. Vous trouverez ci-dessous un exemple de script d'installation.

Paramètres de connexion

Une cible doit être spécifiée avec les éléments suivants :

- Nom d'hôte
- Adresse IPv4
- Adresse IPv6
- Enregistrement de ressource DNS : l'ordinateur Linux doit se trouver dans le domaine (voir le chapitre Enregistrement de ressource DNS).

Le port doit être spécifié : utilisez le port 2222 pour le serveur et le proxy.

Exemple de script d'installation

(Les nouvelles lignes sont séparées par une barre « \ » pour copier la commande intégrale dans le terminal.)

```
./Proxy-Linux-x86_64.sh \
--db-hostname=10.1.179.28 \
--db-name=era_6_db_proxy \
--db-admin-username=sa \
--db-admin-password=admin.1 \
--db-user-username=tester \
--db-user-password=Admin.1 \
--db-port=1433 \
--db-type="MS SQL Server" \
--db-driver=SQL \
--skip-license \
--hostname=10.1.179.30 \
--port=2222 \
--cert-path=/home/adminko/Desktop/proxy.pfx \
--cert-auth-path=/home/adminko/Desktop/CA-server.der \
--cert-password=root \
--server-root-password=jjf#jDjr
```

Vous pouvez modifier les attributs suivants :

Attribut	Description	Obligatoire
`--db-hostname`	Nom de l'ordinateur ou adresse IP du serveur de base de données (`localhost` par défaut)	Oui

Attribut	Description	Obligatoire
`--db-name`	Nom de la base de données à utiliser (la valeur par défaut est `era_db` ou `era_proxy_db`)	Oui
`--db-admin-username`	Nom d'utilisateur de l'administrateur de base de données (utilisé par l'installation pour créer et modifier la base de données ; `root` par défaut)	Oui
`--db-admin-password`	Mot de passe de l'administrateur de base de données.	Oui
`--db-user-username`	Nom d'utilisateur de l'utilisateur de la base de données ERA Server (utilisé par ERA Server pour la connexion à la base de données). Il ne doit pas comporter plus de 16 caractères.	Oui
`--db-user-password`	Mot de passe de l'utilisateur de la base de données ERA Server.	Oui
`--db-port`	Port du serveur de base de données (`3306` par défaut).	Oui
`--db-type`	Type de base de données utilisé (les valeurs possibles sont : `MySQL Server`, `MS SQL Server` ; la valeur par défaut est `MySQL Server`)	Oui
`--db-driver`	Pilote ODBC utilisé pour la connexion à la base de données (`MySQL ODBC 5.3 ANSI Driver`, par exemple ; la valeur par défaut est `MySQL`)	Oui
`--skip-license`	L'installation ne demande pas à l'utilisateur de confirmer le contrat de licence.	-
`--hostname`	Nom d'hôte ou adresse IP du serveur (`localhost` par défaut)	Oui
`--port`	Port du serveur (`2222` par défaut) ou port du proxy (`1236` par défaut)	Oui
`--proxy-port`	Port qui est utilisé par le proxy (la valeur par défaut est `2222`)	-
`--product-guid`	GUID du produit (s'il n'est pas défini, il sera généré).	-
`--cert-path`	Chemin d'accès au fichier de certificat du proxy	Oui*
`--cert-content`	Contenu codé en Base64 du certificat de clé publique codée PKCS12 et clé privée utilisée pour configurer des canaux de communication sécurisés entre le serveur et les Agents	Oui*
`--cert-auth-path`	Chemin d'accès au fichier d'autorité de certification du serveur.	Oui**
`--cert-auth-content`	Contenu codé en Base64 du certificat de clé privé de l'autorité de certification codée DER utilisé pour vérifier les homologues distants (proxy ou serveur)	Oui**
`--cert-password`	Mot de passe de l'autorité de certification. Doit correspondre au mot de passe du certificat de l'Agent (peut être vide si le mot de passe n'a pas été utilisé dans le certificat homologue)	Oui
`--cert-auth-password`	Mot de passe de l'autorité de certification.	
`--keep-database`	La base de données ne sera pas supprimée lors de la désinstallation	-

* Utilisez uniquement l'une des options `--cert-path` ou `--cert-content`.
** Utilisez uniquement l'une des options `--cert-auth-path` ou `--cert-auth-content`.

Pour vérifier l'installation, utilisez la commande suivante pour vous assurer que le service est en cours d'exécution :

```
sudo service eraproxy status
```

3.2.7.1 Conditions préalables requises pour le proxy - Linux

Pour installer le composant Proxy sur Linux, les conditions préalables requises suivantes doivent être remplies :

- **ERA Server** et **ERA Web Console** sont installés (sur un ordinateur serveur).
- Un pilote ODBC destiné à la connexion au serveur de base de données (MySQL / MS SQL) est installé sur l'ordinateur.
- Un serveur de base de données est déjà installé et configuré.
- Le certificat de proxy est créé et téléchargé sur le lecteur local.
- L'autorité de certification est préparée sur le lecteur local.
- Vous disposez d'une licence valide.
- ERA Agent doit être installé sur un ordinateur local pour prendre entièrement en charge toutes les fonctionnalités du programme.
- Le fichier d'installation du proxy est défini en tant qu'exécutable.
- La version minimale d'openssl prise en charge est **openssl-1.0.1e-30**.

3.2.8 Installation et conditions préalables requises pour RD Sensor - Linux

Pour installer le composant RD Sensor sur Linux, procédez comme suit :

1. Vérifiez que les conditions préalables requises suivantes sont remplies :
   - Le réseau peut faire l'objet d'une recherche (les ports sont ouverts, le pare-feu ne bloque pas les communications entrantes, etc.).
   - L'ordinateur serveur est accessible.
   - ERA Agent doit être installé sur l'ordinateur local pour prendre entièrement en charge toutes les fonctionnalités du programme.
   - Le terminal est ouvert.
   - Le fichier d'installation de RD Sensor est défini en tant qu'exécutable.

   ```
   chmod +x RDSensor-Linux-x86_64.sh
   ```
2. Utilisez la commande suivante pour exécuter le fichier d'installation en tant que sudo :

   ```
   sudo ./RDSensor-Linux-x86_64.sh
   ```
3. Lisez le Contrat de licence de l'utilisateur final. Pour passer à la page suivante du CLUF, utilisez la barre Espace. Vous êtes invité à indiquer si vous acceptez les termes de la licence. Si vous les acceptez, appuyez sur la touche Y ; sinon appuyez sur la touche N.
4. ESET Rogue Detection Sensor démarre une fois l'installation terminée.
5. Pour déterminer si l'installation a été effectuée correctement, vérifiez l'exécution du service en exécutant la commande suivante :

   ```
   sudo service rdsensor status
   ```
6. Le fichier journal de Rogue Detection Sensor figure à cet emplacement :

   /var/log/eset/RemoteAdministrator/RogueDetectionSensor/trace.log

3.2.9 Installation du Connecteur de périphérique mobile - Linux

Vous pouvez installer le Connecteur de périphérique mobile sur un autre ordinateur que celui sur lequel s'exécute ERA, par exemple lorsque vous souhaitez que le Connecteur de périphérique mobile soit accessible depuis Internet pour que les périphériques mobiles de l'utilisateur puissent être gérés à tout moment.

L'installation du composant ERA Server sur Linux est effectuée à l'aide d'une commande dans le terminal. Vérifiez que toutes les conditions préalables requises sont remplies. Vous pouvez préparer un script d'installation et l'exécuter ensuite à l'aide de *sudo*.

Il existe de nombreux paramètres d'installation facultatifs. Certains d'entre eux sont toutefois obligatoires :

Le certificat homologue ERA est requis pour l'installation. Deux méthodes permettent de l'obtenir :

- **Installation assistée du serveur** : vous devez indiquer les informations d'identification de l'administrateur de la console Web ERA (le programme d'installation télécharge automatiquement les certificats requis).
- **Installation hors connexion** : vous avez également besoin d'un certificat homologue (le certificat de l'Agent exporté depuis ESET Remote Administrator). Vous pouvez également utiliser un certificat personnalisé.

Des paramètres de commandes d'installation doivent être fournis :

Certificat HTTPS :

```
--https-cert-path=
--https-cert-password=
```

Certificat homologue :
Pour une **installation assistée du serveur**, incluez au moins :

```
--webconsole-password=
```

Pour une **installation hors connexion**, incluez :

```
--cert-path=
--cert-password=
```

(le mot de passe n'est pas nécessaire pour le certificat de l'Agent par défaut créé pendant l'installation initiale d'ERA Server)

Connexion à ERA Server (nom ou adresse IP) :

```
--hostname=
```

Pour une base de données MySQL, incluez :

```
--db-type="MySQL Server"
--db-driver=
--db-admin-username=
--db-admin-password=
--db-user-password=
```

Pour une base de données MSSQL, incluez :

```
--db-type="Microsoft SQL Server"
--db-driver=
--db-admin-username=
--db-admin-password=
--db-user-password=
```

Si une base de données MySQL/MSSQL existe déjà, incluez :

```
--db-use-existing-db=
```

ou

```
--db-drop-existing-db=
```

Exemple de script d'installation
(Les nouvelles lignes sont séparées par une barre « \ » pour copier la commande intégrale dans le terminal.)

```
sudo ./MDMCore-Linux-x86_64-0.0.0.0.sh \
--https-cert-path="./httpscert.pfx" \
--https-cert-password="123456789" \
--port=2222 \
--db-type="MySQL" \
--db-driver="MySQL" \
--db-admin-username="root" \
--db-admin-password=123456789 \
--db-user-password=123456789 \
--db-hostname="127.0.0.1" \
--db-use-existing-db \
--webconsole-password=123456789 \
--hostname=username.LOCAL \
--mdm-hostname=username.LOCAL
```

Pour obtenir la liste des paramètres disponibles (imprimer le message d'aide), utilisez :

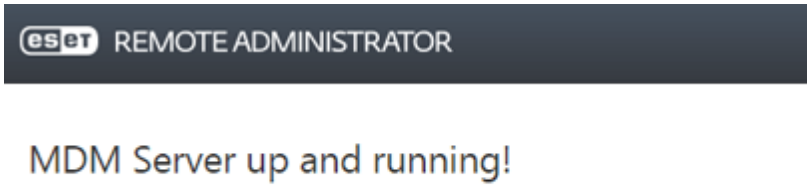
```
--help
```

Journal du programme d'installation

Le journal du programme d'installation peut s'avérer utile pour résoudre des problèmes éventuels. Il figure à l'emplacement suivant :

/var/log/eset/mdminstaller.log

Une fois l'installation terminée, vérifiez si le Connecteur de périphérique mobile fonctionne correctement en ouvrant https://*votre-nom_hôte-mdm*:*port-inscription* (*https://eramdm:9980*, par exemple) dans votre navigateur Web. Si l'installation a été effectuée correctement, le message suivant s'affiche :



Vous pouvez également utiliser cette URL pour vérifier la disponibilité du serveur Connecteur de périphérique mobile depuis Internet (en cas de configuration adéquate) en la visitant à partir d'un périphérique mobile. Si vous ne parvenez pas à accéder à la page, vérifiez votre pare-feu et la configuration de votre infrastructure réseau.

3.2.9.1 Conditions préalables requises pour le Connecteur de périphérique mobile - Linux

Pour installer le Connecteur de périphérique mobile sous Linux, les conditions préalables requises suivantes doivent être remplies :

- Un serveur de base de données est déjà installé et configuré avec un compte racine (il n'est pas nécessaire de créer un compte d'utilisateur avant l'installation ; le programme d'installation peut le créer).
- Un pilote ODBC destiné à la connexion au serveur de base de données (MySQL / MS SQL) est installé sur l'ordinateur.
  `apt-get install unixodbc libmyodbc` (distributions Debian, Ubuntu)
  `yum install mysql-connector-odbc` (distributions CentOS, Red-Hat, Fedora)

REMARQUE : vous devez utiliser le package **unixODBC_23** (et non le package unixODBC par défaut) pour qu'ERA Server se connecte à la base de données MySQL sans aucun problème. Cela est particulièrement vrai pour SUSE Linux.

- Le fichier d'installation du serveur est défini en tant qu'exécutable.

```
chmod +x MDMCore-Linux-x86_64.sh
```

- Après l'installation, vérifiez que le service MDMCore est en cours d'exécution.

```
service mdmcore status
```

- La version minimale d'openSSL prise en charge est **openssl-1.0.1e-30**.

REMARQUE : ERA Server stocke des blobs de données volumineux dans la base de données. Pour qu'ERA s'exécute correctement, il est donc nécessaire de configurer MySQL pour accepter des paquets de grande taille. Pour plus d'informations sur cette configuration, reportez-vous au FAQ.

IMPORTANT : Vous devez posséder un **certificat SSL** au format .pfx pour sécuriser les communications sur HTTPS. Il est recommandé d'utiliser un certificat fourni par une autorité de certification. Les certificats signés automatiquement ne sont pas recommandés, car les périphériques mobiles ne permettent pas tous de les accepter. Les certificats signés par l'autorité de certification ne posent pas de problèmes, car ils sont approuvés et ne nécessitent pas d'être acceptés par l'utilisateur.

IMPORTANT :pour une Installation hors connexion, vous avez également besoin d'un certificat homologue (le **certificat de l'Agent** exporté depuis ESET Remote Administrator). Vous pouvez également utiliser un certificat personnalisé avec ERA.

3.2.10 Installation du proxy HTTP Apache - Linux

Sélectionnez la procédure d'installation du proxy HTTP Apache en fonction de la distribution Linux utilisée sur le serveur :

1. Informations d'installation Linux génériques
2. Ubuntu Server 14.10 et installation d'autres distributions Linux basées sur Debian

Aussi dans cette section :

- Transfert pour les communications ESET uniquement
- Chaînage du proxy (ensemble du trafic)

Informations d'installation Linux génériques pour le proxy HTTP Apache

1. Installez Apache HTTP Server (version 2.4.10 ou ultérieure).
2. Vérifiez que les modules suivants sont chargés :

access_compat, auth_basic, authn_core, authn_file, authz_core, authz_groupfile, authz_host, proxy, proxy_http, proxy_connect, cache, cache_disk

3. Ajoutez la configuration de mise en cache :

```
CacheEnable disk http://
CacheDirLevels 4
CacheDirLength 2
CacheDefaultExpire 3600
CacheMaxFileSize 200000000
CacheMaxExpire 604800
CacheQuickHandler Off
CacheRoot /var/cache/apache2/mod_cache_disk
```

4. Si le répertoire */var/cache/apache2/mod_cache_disk* n'existe pas, créez-le et attribuez-lui des privilèges Apache (r,w,x).
5. Ajoutez une configuration de proxy :

```
ProxyRequests On
ProxyVia On
<Proxy *>
Order deny,allow
Deny from all
Allow from all
</Proxy>
```

6. Activez le proxy de mise en cache et la configuration ajoutés (si la configuration figure dans le fichier de configuration Apache principal, vous pouvez ignorer cette étape).
7. Si nécessaire, modifiez l'écoute sur le port de votre choix (le port 3128 est défini par défaut).
8. Authentification de base facultative :
   - Ajoutez une configuration d'authentification à la directive du proxy :

```
AuthType Basic
AuthName "Password Required"
AuthUserFile /etc/apache2/password.file
AuthGroupFile /etc/apache2/group.file
Require group usergroup
```

   - Créez un fichier de mot de passe à l'aide de la commande `htpasswd.exe -c`.
   - Créez manuellement un fichier appelé group.file avec `usergroup:username`.
9. Redémarrez Apache HTTP Server.

Ubuntu Server 14.10 et installation d'autres distributions Linux basées sur Debian du proxy HTTP Apache

1. Installez la version la plus récente d'Apache HTTP Server à partir du référentiel apt :

```
sudo apt-get install apache2
```

2. Exécutez la commande suivante pour charger les modules Apache requis :

```
sudo a2enmod access_compat auth_basic authn_core authn_file authz_core authz_groupfile
authz_host proxy proxy_http proxy_connect cache cache_disk
```

3. Modifiez le fichier de configuration de mise en cache Apache :

```
sudo vim /etc/apache2/conf-available/caching.conf
```

et copiez/collez la configuration suivante :

```
CacheEnable disk http://
CacheDirLevels 4
CacheDirLength 2
CacheDefaultExpire 3600
CacheMaxFileSize 200000000
CacheMaxExpire 604800
CacheQuickHandler Off
CacheRoot /var/cache/apache2/mod_cache_disk
```

4. Cette étape n'est pas obligatoire. Toutefois, si le répertoire de mise en cache est absent, exécutez les commandes suivantes :

```
sudo mkdir /var/cache/apache2/mod_cache_disk
sudo chown www-data /var/cache/apache2/mod_cache_disk
sudo chgrp www-data /var/cache/apache2/mod_cache_disk
```

5. Modifiez le fichier de configuration du proxy Apache :

```
sudo vim /etc/apache2/conf-available/proxy.conf
```

et copiez/collez la configuration suivante :

```
ProxyRequests On
ProxyVia On
<Proxy *>
Order deny,allow
Deny from all
Allow from all
</Proxy>
```

6. Activez les fichiers de configuration que vous avez modifiés lors des précédentes étapes :

```
sudo a2enconf caching.conf proxy.conf
```

7. Basculez le port d'écoute du serveur HTTP Apache sur le port 3128. Modifiez le fichier */etc/apache2/ports.conf* et remplacez `Listen 80` par `Listen 3128`.

8. Authentification de base facultative :

```
sudo vim /etc/apache2/conf-available/proxy.conf
```

   - Copiez/collez la configuration de l'authentification avant `</Proxy>` :

```
AuthType Basic
AuthName "Password Required"
AuthUserFile /etc/apache2/password.file
AuthGroupFile /etc/apache2/group.file
Require group usergroup
```

   - Installez `apache2-utils` et créez un fichier de mot de passe (nom d'utilisateur : `user`, groupe : `usergroup`):

```
sudo apt-get install apache2-utils
sudo htpasswd -c /etc/apache2/password.file user
```

   - Créez un fichier avec des groupes :

```
sudo vim /etc/apache2/group.file
```

     et copiez/collez la ligne suivante :

```
usergroup:user
```

9. Redémarrez Apache HTTP Server à l'aide de la commande suivante :

```
sudo service apache2 restart
```

Transfert pour les communications ESET uniquement

Remplacez les éléments suivants de la configuration du proxy :

```
<Proxy *>
Order deny,allow
Deny from all
Allow from all
</Proxy>
```

par :

```
<Proxy *>
Deny from all
</Proxy>
<ProxyMatch ^([h,H][t,T][t,T][p,P][s,S]?://)?([^@/]*@)?([a-zA-Z0-9-]{0,63}\.)?[a-zA-Z0-9-]{0,63}\.
[e,E][s,S][e,E][t,T]\.[c,C][o,O][m,M](:[0-9]+)?(/.*)?$>
Allow from all
</ProxyMatch>
<ProxyMatch ^([h,H][t,T][t,T][p,P][s,S]?://)?([^@/]*@)?([a-zA-Z0-9-]{0,63}\.)?[a-zA-Z0-9-]{0,63}\.
[e,E][s,S][e,E][t,T]\.[e,E][u,U](:[0-9]+)?(/.*)?$>
Allow from all
</ProxyMatch>
<ProxyMatch ^([h,H][t,T][t,T][p,P][s,S]?://)?([^@/]*@)?(ds1-uk-rules-1.mailshell.net|ds1-uk-rules-2.
mailshell.net|ds1-uk-rules-3.mailshell.net|fh-uk11.mailshell.net|edf-pcs.cloudapp.net|edf-pcs2.cloudapp.
edfpcs.trafficmanager.net)(:[0-9]+)?(/.*)?$>
Allow from all
</ProxyMatch>
<ProxyMatch ^([h,H][t,T][t,T][p,P][s,S]?://)?([^@/]*@)?(87.106.247.14|209.157.66.250|209.157.66.253|
212.227.134.125|212.227.134.126|212.227.134.128|212.227.134.130|212.227.134.131|212.227.134.132|
212.227.134.133|212.227.134.158)(:[0-9]+)?(/.*)?$>
Allow from all
</ProxyMatch>
```

Chaînage du proxy (ensemble du trafic)

Ajoutez les éléments suivants à la configuration du proxy (le mot de passe fonctionne uniquement avec le proxy enfant) :

```
ProxyRemote * http://IP_ADDRESS:3128
```

3.2.11 Installation du proxy HTTP Squid sur Ubuntu Server 14.10

Vous pouvez utiliser le proxy Squid au lieu d'Apache sur Ubuntu Server. Pour installer et configurer Squid sur Ubuntu Server 14.10 (et des distributions Linux basées sur Debian similaires), procédez comme suit :

1. Installez le package Squid3 :

   ```
   sudo apt-get install squid3
   ```

2. Modifiez le fichier de configuration Squid */etc/squid3/squid.conf* et remplacez

   ```
   #cache_dir ufs /var/spool/squid3 100 16 256
   ```

   par :

   ```
   cache_dir ufs /var/spool/squid3 5000 16 256 max-size=200000000
   ```

   REMARQUE : 5000 correspond à la taille du cache en Mo.

3. Arrêtez le service squid3.

   ```
   sudo service squid3 stop
   sudo squid3 -z
   ```

4. Modifiez à nouveau le fichier de configuration Squid et ajoutez `http_access allow all` avant `http_access deny all` pour permettre à tous les clients d'accéder au proxy.

5. Redémarrez le service squid3 :

   ```
   sudo service squid3 restart
   ```

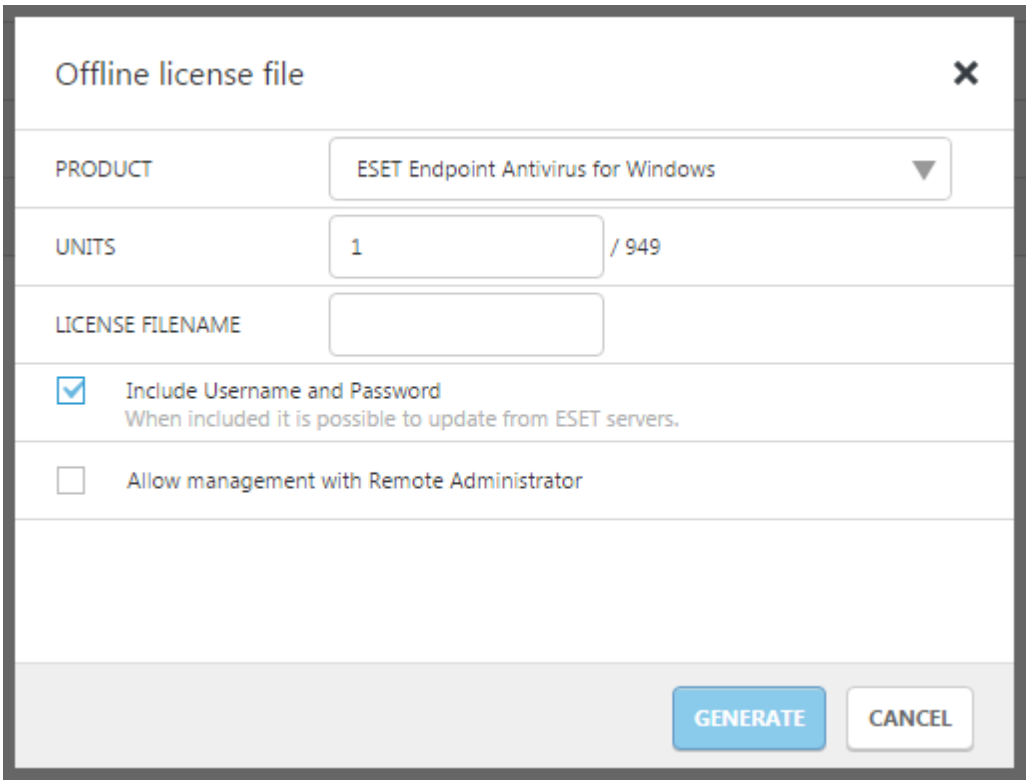
3.2.12 Outil Miroir

L'outil Miroir est nécessaire pour les mises à jour de la base de données de virus hors connexion. Si vos ordinateurs clients ne disposent pas d'une connexion Internet et nécessitent des mises à jour de la base de données de virus, vous pouvez utiliser l'outil Miroir pour télécharger les fichiers de mise à jour depuis les serveurs de mise à jour ESET et les stocker localement.

REMARQUE : l'outil Miroir télécharge uniquement les définitions de la base de données de virus, mais ne télécharge pas les mises à jour des composants du programme (PCU). Pour effectuer la mise à jour d'un produit de sécurité ESET sur des ordinateurs clients hors connexion, il est conseillé de mettre le produit à niveau à l'aide de la tâche d'installer un logiciel sur un client dans ERA. Vous pouvez également mettre les produits à niveau individuellement.

Conditions préalables requises :

- Le dossier cible doit être disponible en partage, Samba/Windows ou un service HTTP/FTP, selon la manière dont vous souhaitez accéder aux mises à jour.
- Vous devez disposer d'un fichier de licence hors connexion incluant le nom d'utilisateur et le mot de passe. Durant la génération d'un fichier de licence, veillez à sélectionner la case à cocher en regard du champ Inclure le nom d'utilisateur et le mot de passe. Vous devez aussi indiquer un nom de fichier de licence.



- L'outil Miroir nécessite que Visual C++ Redistributables for Visual Studio 2012 soit installé sur le système.
- L'installation ne comporte aucune étape, l'outil est composé de deux fichiers :

Windows :
`MirrorTool.exe` et `updater.dll`

Linux :
`MirrorTool` et `updater.so`

Utilisation :

- Pour afficher l'aide de l'outil Miroir, exécutez `MirrorTool --help` afin de voir toutes les commandes disponibles pour l'outil :

```
C:\Users\administrator.FRANTO\Desktop\1.0.136.0\Win32>MirrorTool.exe --help
Mirror Tool, Copyright (c) ESET, spol. s r.o. 1992-2015. All rights reserved.
Allowed options:
  --mirrorType arg                      [required]
                                        Type of mirror. Possible values (case
                                        insensitive): regular, pre-release,
                                        delayed.
  --intermediateUpdateDirectory arg     [required]
                                        Files will be downloaded to this directory
                                        to create mirror in output directory.
  --offlineLicenseFilename arg          [required]
                                        Offline license file.
  --updateServer arg                    [optional]
                                        Update server. (e.g.:http://update.eset.com
                                        /eset_upd/ep6/) Mirror will be created in
                                        output directory, only specified path in
                                        server will be mirrored.
  --outputDirectory arg                 [required]
                                        Directory where mirror will be created.
  --proxyHost arg                       [optional]
                                        Http proxy address (fqdn or IP).
  --proxyPort arg                       [optional]
                                        Http proxy port.
  --proxyUsername arg                   [optional]
                                        Http proxy username.
  --proxyPassword arg                   [optional]
                                        Http proxy password.
  --excludedProducts arg                [optional]
                                        Disable creating mirror for specified
                                        products. Possible values:ep4 ep5 ep6 era6.
  --help                                [optional]
                                        Display this help and exit
```

- Le paramètre `--updateServer` est facultatif. Si vous l'utilisez, vous devez spécifier l'URL complète du serveur de mise à jour.
- Le paramètre `--offlineLicenseFilename` est obligatoire. Vous devez indiquer un chemin d'accès à votre fichier de licence hors connexion (comme mentionné plus haut).
- Pour créer un miroir, exécutez `MirrorTool` avec au moins les paramètres minimums requis. Voici un exemple :

Windows :

```
MirrorTool.exe --mirrorType regular --intermediateUpdateDirectory c:\temp\mirrorTemp --
offlineLicenseFilename c:\temp\offline.lf --outputDirectory c:\temp\mirror
```

Linux :

```
sudo ./MirrorTool --mirrorType regular --intermediateUpdateDirectory /tmp/mirrorTool/mirrorTemp
--offlineLicenseFilename /tmp/mirrorTool/offline.lf --outputDirectory /tmp/mirrorTool/mirror
```

Paramètre de l'outil miroir et de mise à jour :

- Pour automatiser la distribution des mises à jour de la base de données de virus, vous pouvez créer une planification pour l'exécution de l'outil Miroir. Pour ce faire, ouvrez la console Web et accédez à **Tâches client** > **Système d'exploitation** > **Exécuter une commande**. Sélectionnez **Ligne de commande à exécuter** (avec un chemin d'accès à `MirrorTool.exe`) et un déclencheur raisonnable (par exemple, une expression CRON pour toutes les heures 0 0 * * * ? *). Vous pouvez également utiliser le Planificateur de tâches Windows ou CRON dans Linux.
- Pour configurer les mises à jour sur un ordinateur client, créez une stratégie et configurer le **serveur de mise à jour** afin qu'il pointe sur l'adresse miroir ou un dossier partagé.

3.2.13 Cluster de basculement - Linux

Le présent guide traite de l'installation et de la configuration de ESET Remote Administrator sur un cluster Red Hat à haute disponibilité.

- Prise en charge des clusters Linux
- Conditions préalables requises
- Portée
- Étapes d'installation

Prise en charge des clusters Linux

Les composants ESET Remote Administrator Server ou ERA Proxy peuvent être installés sur un cluster **Red Hat Linux 6** ou version ultérieure. Un cluster de basculement est uniquement pris en charge en mode actif/passif avec le gestionnaire de cluster **rgmanager**.

Conditions préalables requises

- Un cluster actif/passif doit être installé et configuré. Un seul nœud peut être actif à la fois. Les autres nœuds doivent être en veille. L'équilibrage de charge n'est pas pris en charge.
- Système de stockage partagé : iSCSI SAN, NFS et d'autres solutions sont prises en charge (toute technologie ou tout protocole qui permet un accès en mode bloc ou fichier au système de stockage partagé et qui fait apparaître les périphériques partagés comme des périphériques connectés localement au système d'exploitation). Le système de stockage partagé doit être accessible à partir de chaque nœud actif du cluster. De plus, le système de fichiers partagé doit être correctement initialisé (à l'aide du système de fichiers EXT3 ou EXT4, par exemple).
- Les modules complémentaires haute disponibilité suivants sont requis pour l'administration système :
  - rgmanager
  - Conga
- **rgmanager** est la pile de cluster Red Hat à haute disponibilité standard. Il s'agit d'un composant obligatoire.
- L'interface utilisateur graphique **Conga** est facultative. Le cluster de basculement peut être géré sans l'aide de celle-ci. Pour des performances optimales, il est toutefois recommandé de l'installer. Ce guide suppose qu'elle est installée.

- **Fencing** doit être correctement configuré pour empêcher tout endommagement des données. L'administrateur du cluster doit configurer l'isolation si ce n'est pas déjà fait.

Si aucun cluster n'est déjà en cours d'exécution, vous pouvez utiliser le guide suivant pour configurer un cluster de basculement à haute disponibilité (actif/passif) sur Red Hat : Red Hat Enterprise Linux 6 Cluster Administration (en anglais).

Portée

Les composants ESET Remote Administrator qui peuvent être installés sur un cluster **Red Hat Linux** à haute disponibilité sont les suivants :

- ERA Server avec ERA Agent
- ERA Proxy avec ERA Agent

REMARQUE : ERA Agent doit être installé. Si ce n'est pas le cas, le service de cluster ERA ne s'exécute pas.

REMARQUE : l'installation sur un cluster de la base de données ERA ou de la console Web ERA n'est pas prise en charge.

L'exemple d'installation ci-après est destiné à un cluster à deux nœuds. Il peut toutefois servir de référence pour l'installation de ESET Remote Administrator sur un cluster à plusieurs nœuds. Dans cet exemple, les nœuds de cluster sont appelés nœud1 et nœud2.

Étapes d'installation

1. Installez ERA Server ou ERA Proxy, puis ERA Agent sur nœud1. Pendant l'installation d'ERA Agent, la commande `--hostname=` vous permet de spécifier `localhost` (n'utilisez pas l'adresse IP ou le nom d'hôte actuel de ce nœud spécifique). Vous pouvez également spécifier le nom d'hôte ou l'adresse IP externe de l'interface du cluster.

- Notez que le nom d'hôte du certificat serveur ou proxy doit contenir l'adresse IP externe (ou le nom d'hôte) de l'interface du cluster (et non l'adresse IP locale ou le nom d'hôte du nœud).
- Pendant l'installation d'ERA Agent, lorsque vous utilisez la commande `--hostname=`, vous avez les possibilités suivantes :
  - Vous pouvez spécifier le nom d'hôte ou l'adresse IP externe de l'interface du cluster.
  - Vous pouvez également spécifier localhost (et non l'adresse IP ou le nom d'hôte actuel de ce nœud spécifique). Dans ce cas, le nom d'hôte du certificat ERA Server ou ERA Proxy doit contenir en plus localhost.

2. Arrêtez et désactivez les services Linux ERA Agent et ERA Server (ou ERA Proxy) à l'aide des commandes suivantes :

```
chkconfig eraagent off
chkconfig eraserver off
service eraagent stop
service eraserver stop
```

3. Montez le système de stockage partagé sur nœud1. Dans cet exemple, le système de stockage partagé est monté dans */usr/share/erag2cluster*.

4. Dans **/usr/share/erag2cluster**, créez les répertoires suivants :

   /usr/share/erag2cluster/etc/opt
   /usr/share/erag2cluster/opt
   /usr/share/erag2cluster/var/log
   /usr/share/erag2cluster/var/opt

5. Déplacez de manière récursive les répertoires suivants vers les destinations indiquées ci-après (source > destination).

Déplacer le dossier :	Déplacer vers :
/etc/opt/eset	*/usr/share/erag2cluster/etc/opt/*
/opt/eset	*/usr/share/erag2cluster/opt/*
/var/log/eset	*/usr/share/erag2cluster/var/log/*

Déplacer le dossier :	Déplacer vers :
/var/opt/eset	*/usr/share/erag2cluster/var/opt/*

6. Créez des liens symboliques :

```
ln -s /usr/share/erag2cluster/etc/opt/eset /etc/opt/eset
ln -s /usr/share/erag2cluster/opt/eset /opt/eset
ln -s /usr/share/erag2cluster/var/log/eset /var/log/eset
ln -s /usr/share/erag2cluster/var/opt/eset /var/opt/eset
```

7. Démontez le système de stockage partagé de nœud1, puis montez-le sur nœud2 dans le même répertoire dans lequel vous l'avez monté sur nœud1 (*/usr/share/erag2cluster*).

8. Sur nœud2, créez les liens symboliques suivants :

```
ln -s /usr/share/erag2cluster/etc/opt/eset /etc/opt/eset
ln -s /usr/share/erag2cluster/opt/eset /opt/eset
ln -s /usr/share/erag2cluster/var/log/eset /var/log/eset
ln -s /usr/share/erag2cluster/var/opt/eset /var/opt/eset
```

9. Copiez le script `eracluster_server` (`eracluster_proxy`) dans */usr/share/cluster*.

   Les scripts `eracluster_server` (`eracluster_proxy`) se trouvent dans le répertoire d'installation d'ERA Server ou ERA Proxy.

Les étapes suivantes sont effectuées dans l'interface utilisateur graphique d'administration de cluster Conga :

10. Créez un groupe de services (EraService, par exemple).

Le service de cluster ESET Remote Administrator requiert les trois ressources suivantes : adresse IP, système de fichiers et script.

11. Créez les ressources de service nécessaires.

    Ajoutez les ressources d'adresse IP, de système de fichiers et de script.
    La ressource de système de fichiers doit pointer vers le système de stockage partagé.
    Le point de montage de la ressource de système de fichiers doit être défini sur */usr/share/erag2cluster*.
    Le paramètre « Full Path to Script File (chemin d'accès complet au fichier de script) » de la ressource de script doit être défini sur */usr/share/cluster/eracluster_server* (ou */usr/share/cluster/eracluster_proxy*).

12. Ajoutez les ressources ci-dessus au groupe EraService.

3.2.14 Comment désinstaller ou réinstaller un composant - Linux

Si vous souhaitez effectuer une réinstallation ou une mise à niveau vers une version plus récente, réexécutez le script d'installation.

Pour désinstaller un composant (dans le cas présent, ERA Server), exécutez le programme d'installation avec le paramètre **--uninstall**, comme indiqué ci-dessous :

```
sudo ./Server-Linux-x86_64.sh --uninstall --keep-database
```

Si vous souhaitez désinstaller un autre composant, utilisez le nom de package adéquat dans la commande. Par exemple, ERA Agent :

```
sudo ./Agent-Linux-x86_64.sh --uninstall
```

IMPORTANT : les fichiers de configuration et de base de données sont supprimés lors de la désinstallation. Pour conserver les fichiers de base de données, créez un vidage SQL de la base de données ou utilisez le paramètre `--keep-database`.

Une fois l'installation terminée, vérifiez que

- le service `eraserverService.sh` est supprimé ;
- le dossier `/etc/opt/eset/RemoteAdministrator/Server/` est supprimé.

REMARQUE : Il est recommandé de créer une sauvegarde de la base de données avant d'effectuer la désinstallation au cas où vous auriez besoin de restaurer vos données.

3.3 Base de données

ESET Remote Administrator utilise une base de données pour stocker les données clientes. Les sections suivantes décrivent l'installation, la sauvegarde, la mise à niveau et la migration de la base de données ERA Server/ERA Proxy :

- Passez en revue la compatibilité et la configuration système requise pour la base de données ERA Server.
- Si vous ne disposez pas d'une base de données configurée pour être utilisée avec ERA Server, vous pouvez utiliser **Microsoft SQL Server Express** qui est inclus dans le programme d'installation.
- Si vous utilisez Microsoft Small Business Server (SBS) ou Essentials, il est recommandé de vérifier que toutes les conditions requises sont réunies et que vous utilisez un système d'exploitation pris en charge. Lorsque toutes les conditions requises sont réunies, suivez les instructions d'installation de Windows SBS / Essentials pour installer ERA sur ces systèmes d'exploitation.
- Si Microsoft SQL Server est installé sur votre système, passez en revue les conditions requises pour vous assurer que Microsoft SQL Server est pris en charge par ESET Remote Administrator. Si votre version de Microsoft SQL Server n'est pas prise en charge, effectuez une mise à niveau vers une version compatible de SQL Server.

3.3.1 Sauvegarde du serveur de base de données

Toutes les informations et tous les paramètres d'ESET Remote Administrator sont stockés dans la base de données. Il est recommandé de sauvegarder régulièrement la base de données pour éviter toute perte de données. Reportez-vous à la section suivante correspondant à votre base de données :

- MySQL
- SQL Server

Une sauvegarde peut être également utilisée ultérieurement lors de migration d'ESET Remote Administrator vers un nouveau serveur.

Si vous souhaitez restaurer la sauvegarde de la base de données, suivez les instructions suivantes :

- MySQL
- SQL Server

3.3.2 Mise à niveau du serveur de base de données

Pour mettre à niveau une instance Microsoft SQL Server existante vers une nouvelle version afin de l'utiliser avec la base de données ERA Proxy ou ERA Server, suivez les instructions suivantes :

1. **Arrêtez** tous les services ERA Server ou ERA Proxy en cours d'exécution qui se connectent au serveur de base de données que vous allez mettre à niveau. Arrêtez également les applications qui peuvent se connecter à votre instance Microsoft SQL Server.
2. Sauvegardez toutes les bases de données pertinentes avant de continuer.
3. Effectuez la mise à niveau du serveur de base de données en suivant les instructions de l'éditeur de la base de données.
4. **Démarrez** tous les services ERA Server et/ou ERA Proxy, puis consultez les journaux de suivi de ces derniers pour vérifier que la connexion à la base de données fonctionne correctement.

Pour plus d'informations spécifiques à votre base de données, consultez les pages Web suivantes :

- Mise à niveau de SQL Server : https://msdn.microsoft.com/fr-fr/library/bb677622.aspx (Vous pouvez cliquer sur **Autres versions** pour obtenir des instructions de mise à niveau vers une version spécifique de SQL Server.)
- Mise à niveau de MySQL Server (vers la version 5.5) : http://dev.mysql.com/doc/refman/5.5/en/upgrading.html

3.3.3 Migration de la base de données ERA

Pour obtenir des instructions afin de migrer la base de données ERA Server ou ERA Proxy entre différentes instances SQL Server (ces instructions s'appliquent également lors de la migration vers une version différente de SQL Server ou vers une instance SQL Server hébergée sur un autre ordinateur), cliquez sur le lien adéquat suivant :

- Processus de migration de SQL Server
- Processus de migration de MySQL Server

3.3.3.1 Processus de migration de SQL Server

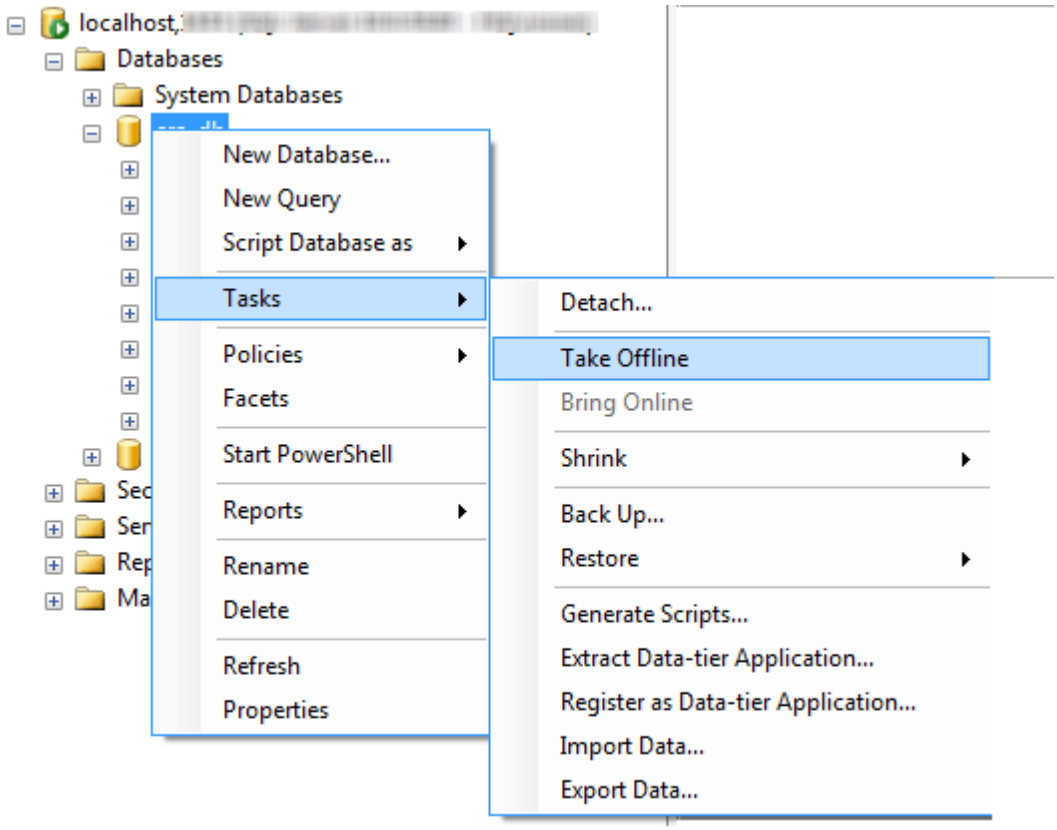
Ce processus de migration est identique pour **Microsoft SQL Server** et **Microsoft SQL Server Express**.

Pour plus d'informations, consultez l'article suivant de la base de connaissances Microsoft : https://msdn.microsoft.com/en-us/library/ms189624.aspx.

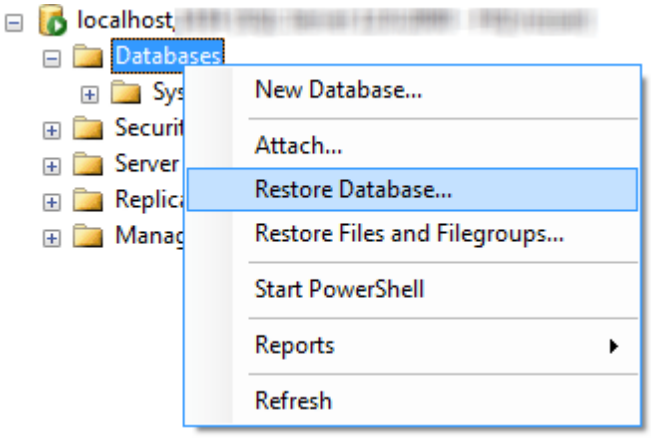
- **Conditions préalables requises :**
  - Les instances SQL Server source et cible doivent être installées. Elles peuvent être hébergées sur des ordinateurs différents.
  - La version de l'instance SQL Serveur cible doit être la même que celle de l'instance source. **Une mise à niveau vers une version antérieure n'est pas prise en charge.**
  - **SQL Server Management Studio** doit être installé. Si les instances SQL Server se trouvent sur des ordinateurs distincts, SQL Server Management Studio doit être installé sur les deux ordinateurs.

- **Migration :**

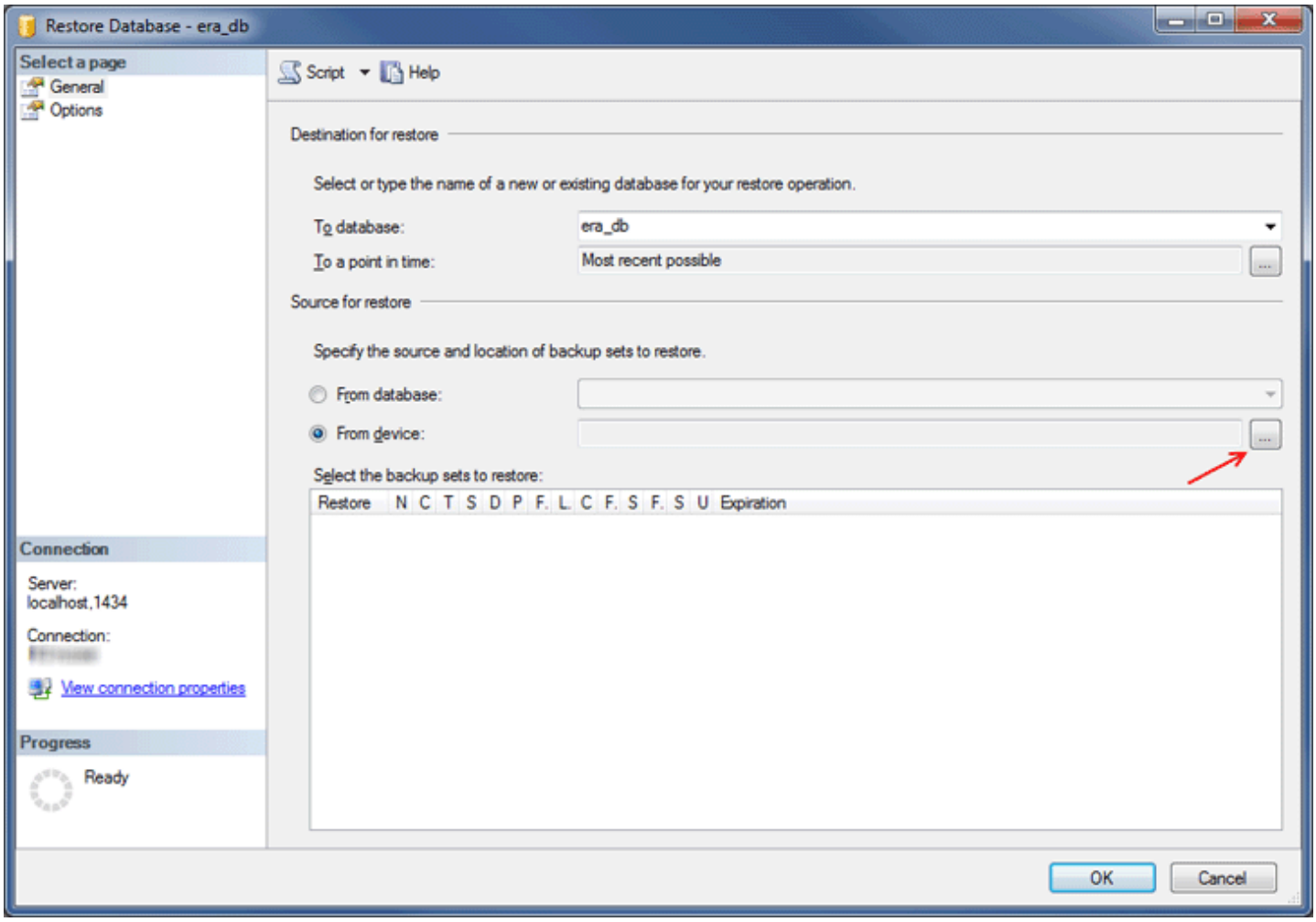
1. **Arrêtez** le service ERA Server ou ERA Proxy.
2. Connectez-vous à l'instance SQL Server source par le biais de SQL Server Management Studio.
3. **Effectuez** une sauvegarde complète de la base de données à migrer. Il est recommandé de spécifier un nouveau nom de jeu de sauvegarde. Sinon, si le jeu de sauvegarde a déjà été utilisé, la nouvelle sauvegarde lui sera ajoutée, ce qui générera un fichier de sauvegarde inutilement volumineux.
4. Mettez la base de données source hors ligne en sélectionnant **Tâches** > **Mettre hors ligne**.



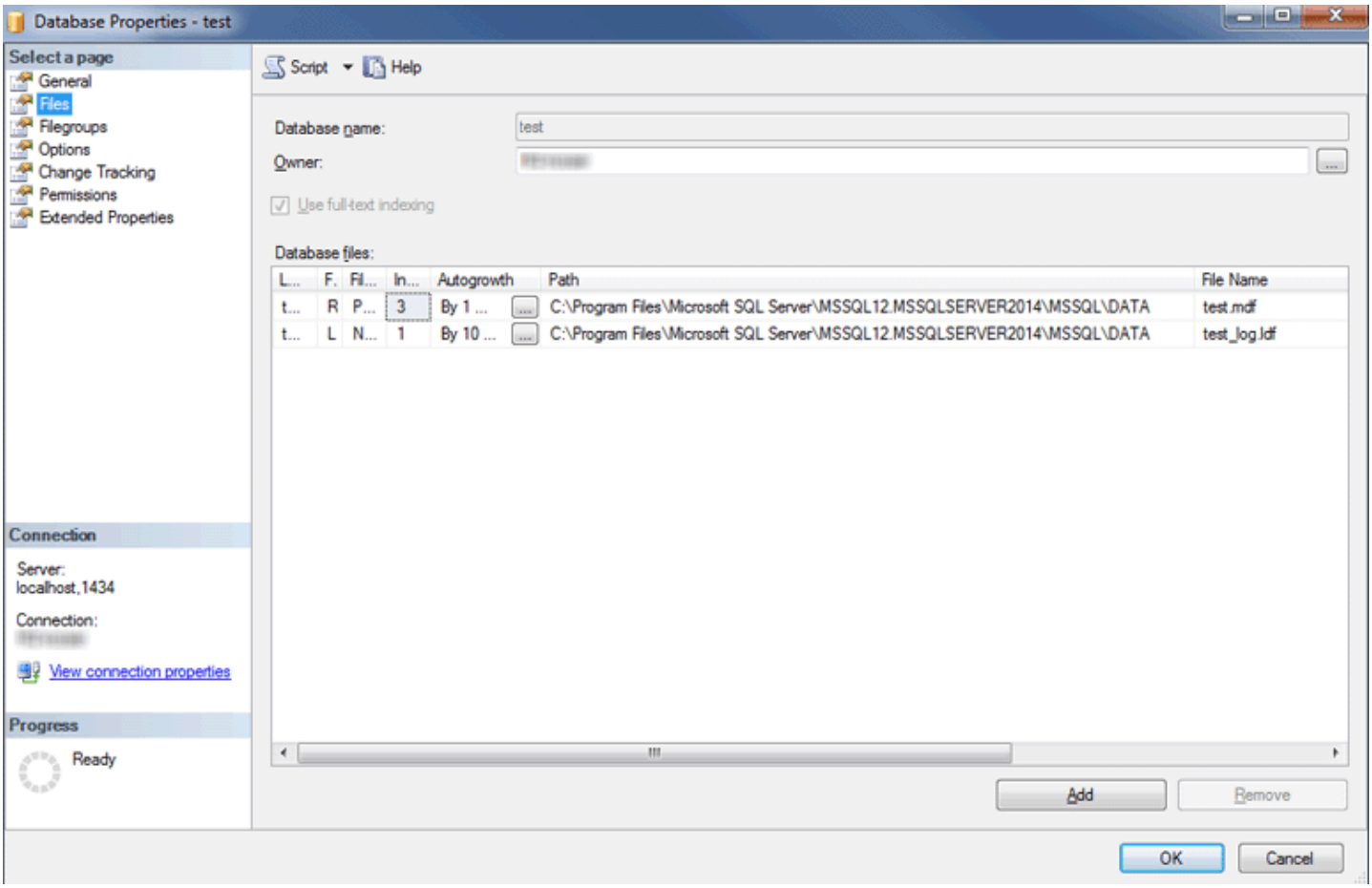
5. **Copiez** le fichier de sauvegarde (.bak) créé à l'étape 3 à un emplacement accessible à partir de l'instance SQL Server cible. Il est possible que vous deviez modifier les droits d'accès du fichier de sauvegarde de base de données.
6. **Remettez** la base de données source en ligne, mais **ne démarrez pas encore ERA Server.**
7. Connectez-vous à l'instance SQL Server cible à l'aide de SQL Server Management Studio.
8. Restaurez votre base de données sur l'instance SQL Server cible.



9. Saisissez le nom de la nouvelle base de données dans le champ **Base de données de destination**. Si vous préférez, vous pouvez utiliser le nom de l'ancienne base de données.
10. Sous Spécifiez la source et l'emplacement des jeux de sauvegarde à restaurer, sélectionnez À partir du périphérique, puis cliquez sur … .

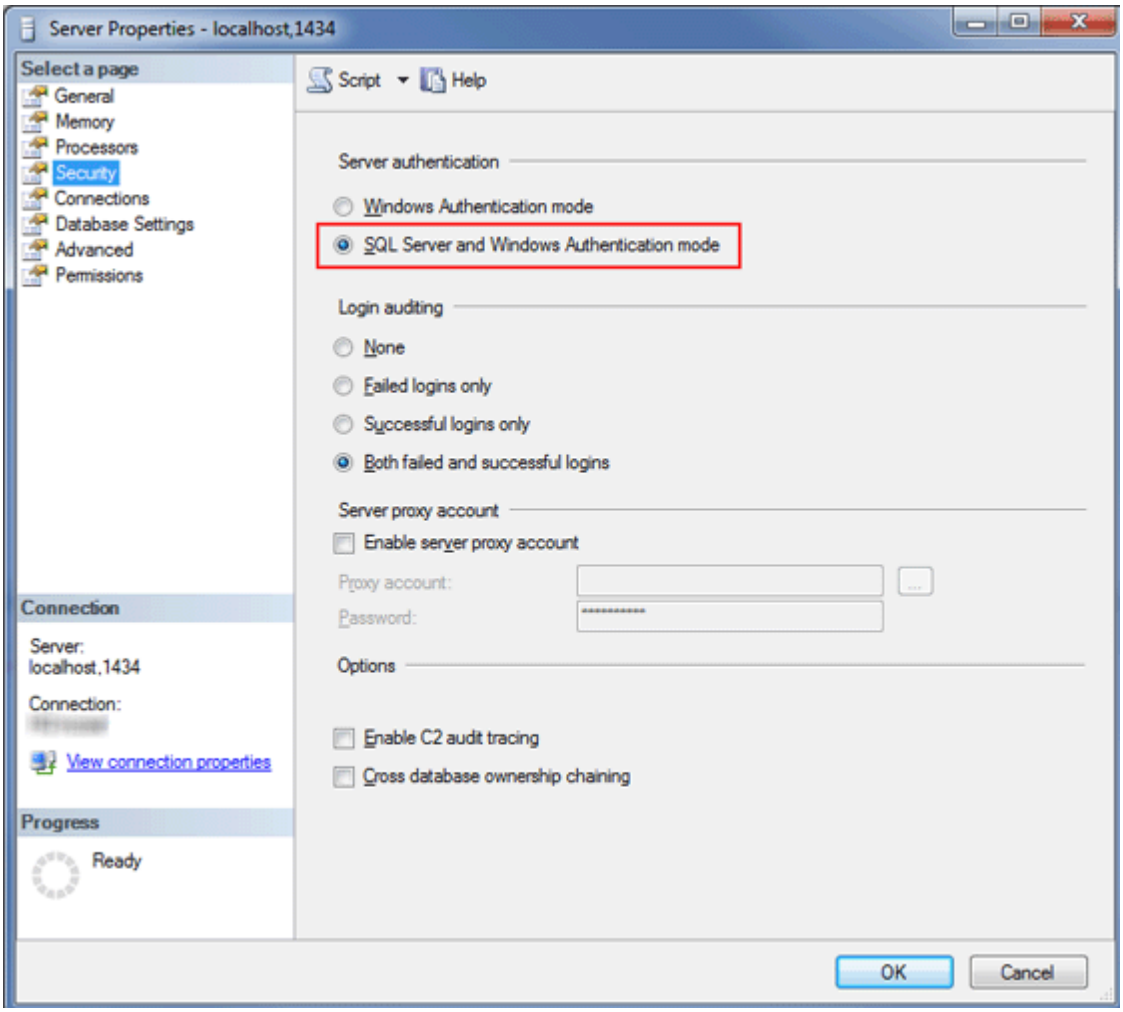


11. Cliquez sur **Ajouter**, accédez à votre fichier de sauvegarde, puis ouvrez-le.
12. Sélectionnez la sauvegarde la plus récente à restaurer (le jeu de sauvegarde peut contenir plusieurs sauvegardes).
13. Cliquez sur la page **Options** de l'assistant de restauration. Vous pouvez éventuellement sélectionner **Remplacer la base de données existante** et vérifier que les emplacements de restauration de la base de données (`.mdf`) et du journal (`.ldf`) sont corrects. Si vous conservez les valeurs par défaut, les chemins de l'instance SQL Server source seront utilisés. Vérifiez que ces valeurs sont correctes.
    - Si vous ne savez pas où les fichiers de base de données sont stockés sur l'instance SQL Server cible, cliquez avec le bouton droit sur une base de données existante, sélectionnez **Propriétés**, puis cliquez sur l'onglet **Fichiers**. Le répertoire dans lequel est stockée la base de données est indiqué dans la colonne **Chemin d'accès** du tableau ci-dessous.

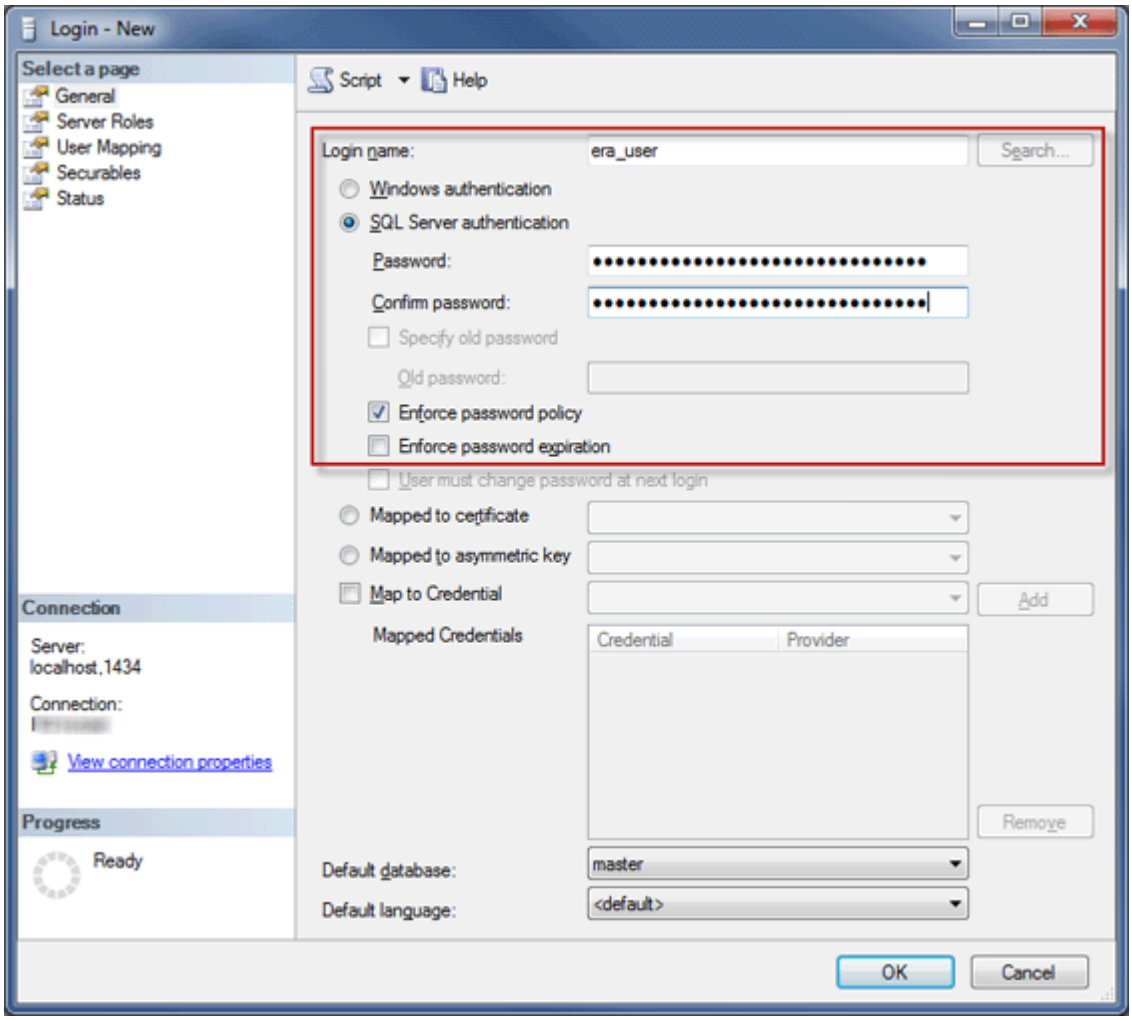


14. Dans la fenêtre de l'assistant de restauration, cliquez sur **OK**.

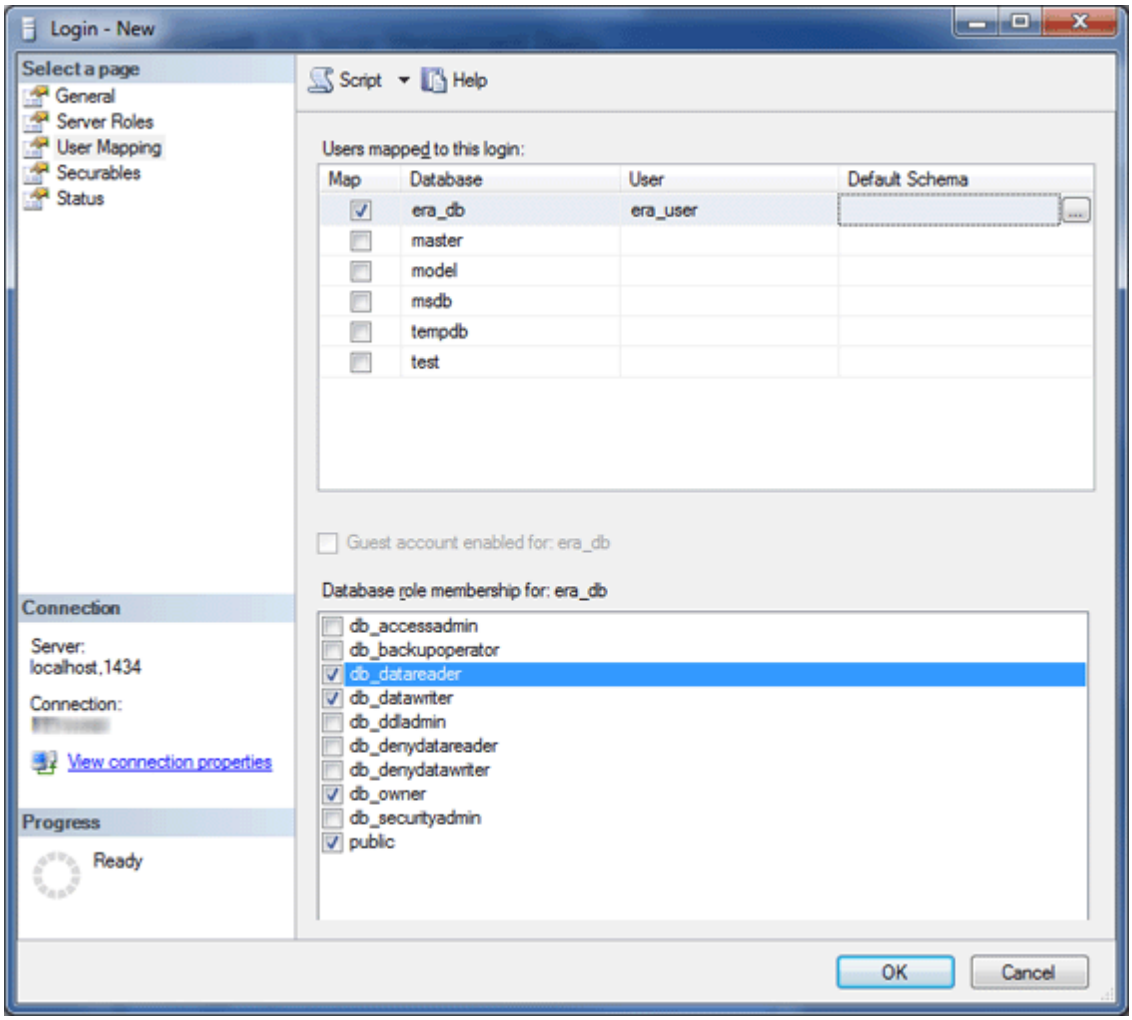
15. Vérifiez que l'**authentification SQL Server est activée** pour la nouvelle base de données. Cliquez avec le bouton droit sur le serveur, puis cliquez sur **Propriétés**. Accédez à **Sécurité**, puis vérifiez que le mode d'authentification SQL Server et Windows est sélectionné.



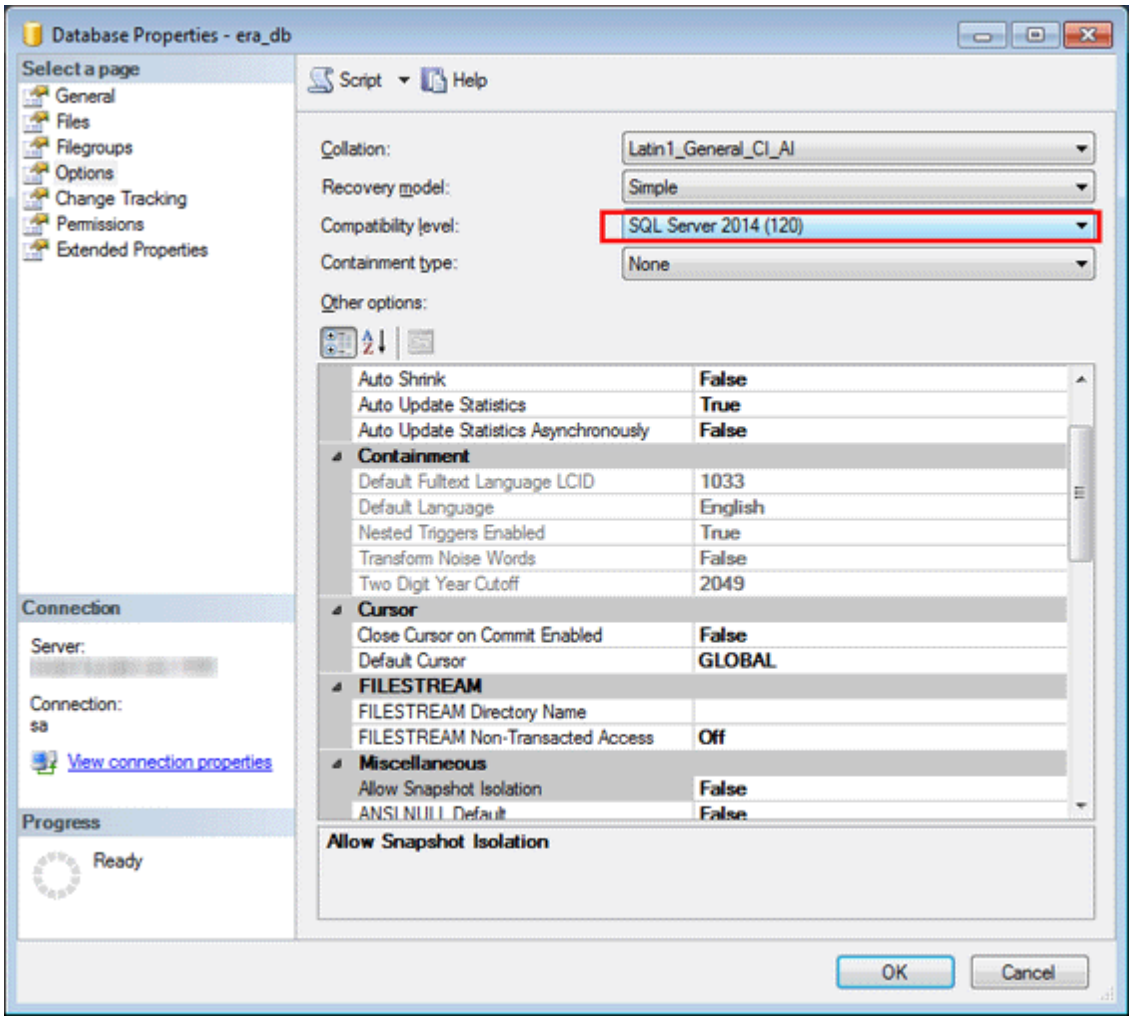
16. **Créez des informations d'identification SQL Server** (pour ERA Server/Proxy) dans l'instance SQL Server cible avec l'**authentification SQL Server** et mappez-les sur un utilisateur de la base de données restaurée.
    - N'appliquez pas l'expiration des mots de passe.
    - Caractères recommandés pour les noms d'utilisateur :
        - Lettres ASCII en minuscules, chiffres et trait de soulignement « _ »
    - Caractères recommandés pour les mots de passe :
        - Caractères ASCII uniquement, notamment des lettres ASCII en majuscules et minuscules, des chiffres, des espaces et des caractères spéciaux
    - N'utilisez pas de caractères non-ASCII tels que les accolades et le caractère @
    - Si vous ne suivez pas les recommandations ci-dessus relatives aux caractères, il est possible que vous rencontriez des problèmes de connexion de base de données ou que vous deviez échapper les caractères spéciaux lors des étapes de modification de la chaîne de connexion à la base de données qui suivent. Les règles d'échappement de caractères ne sont pas incluses dans ce document.



17. Mappez les informations d'identification sur un utilisateur de la base de données cible. Dans l'onglet des mappages des utilisateurs, vérifiez que l'utilisateur de la base de données dispose des rôles suivants : **db_datareader**, **db_datawriter**, **db_owner**.



18. Pour activer les dernières fonctionnalités du serveur de base de données, remplacez le **niveau de compatibilité** de la base de données restaurée par le plus récent. Cliquez avec le bouton droit sur la nouvelle base de données, puis ouvrez ses **propriétés**.



REMARQUE : SQL Server Management Studio n'est pas en mesure de définir les niveaux de compatibilité ultérieurs à la version en cours d'utilisation. Par exemple, SQL Server Management Studio 2008 ne peut pas définir le niveau de compatibilité de SQL Server 2014.

19. **Recherchez le fichier** `startupconfiguration.ini` sur l'ordinateur sur lequel ERA Server/Proxy est installé.

   - Pour Windows Vista et versions ultérieures :
     % PROGRAMDATA %\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini
   - Pour les versions antérieures de Windows :
     % ALLUSERSPROFILE %\ Application Data\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini
   - Pour Linux :
     /etc/opt/eset/RemoteAdministrator/Server/StartupConfiguration.ini

20. **Modifiez** la chaîne de connexion à la base de données dans ERA Server/Proxy startupconfiguration.ini

   - Définissez l'adresse et le port du nouveau serveur de base de données.
   - Définissez les nouveaux nom d'utilisateur et mot de passe ERA dans la chaîne de connexion.
     - Le résultat final doit ressembler à celui-ci :

```
DatabaseType=MSSQLOdbc
DatabaseConnectionString=Driver=SQL Server;Server=localhost,1433;Uid=era_user1;Pwd={SecretPassword123
```

21. **Démarrez** ERA Server/Proxy et vérifiez que le service ERA Server/Proxy s'exécute correctement.

3.3.3.2 Processus de migration de MySQL Server

- **Conditions préalables requises :**
  - Les instances SQL Server source et cible doivent être installées. Elles peuvent être hébergées sur des ordinateurs différents.
  - Les outils MySQL doivent être disponibles sur au moins un des ordinateurs (client mysql et mysqldump).
- **Liens utiles :**

http://dev.mysql.com/doc/refman/5.6/en/copying-databases.html

http://dev.mysql.com/doc/refman/5.6/en/mysqldump.html

http://dev.mysql.com/doc/refman/5.6/en/mysql.html

- Dans les commandes, instructions SQL ou fichiers de configuration suivants, remplacez toujours :
  - **SRCHOST** par l'adresse du serveur de base de données source ;
  - **SRCROOTLOGIN** par la connexion de l'utilisateur racine MySQL Server source ;
  - **SRCERADBNAME** par le nom de la base de données ERA source à sauvegarder ;
  - **BACKUPFILE** par le chemin d'accès au fichier dans lequel la sauvegarde sera stockée ;
  - **TARGETHOST** par l'adresse du serveur de base de données cible ;
  - **TARGETROOTLOGIN** par la connexion de l'utilisateur racine MySQL Server cible ;
  - **TARGETERADBNAME** par le nom de la base de données ERA cible (après migration) ;
  - **TARGETERALOGIN** par le nom d'utilisateur de l'utilisateur de la nouvelle base de données ERA sur l'instance MySQL Server cible ;
  - **TARGETERAPASSWD** par le mot de passe de l'utilisateur de la nouvelle base de données ERA sur l'instance MySQL cible.

Il n'est pas nécessaire d'exécuter les instructions SQL ci-dessous via la ligne de commande. Si vous disposez d'un outil d'interface utilisateur graphique, vous pouvez utiliser une application que vous maîtrisez.

1. **Arrêtez** les services ERA Server/Proxy.
2. **Effectuez** une sauvegarde complète de la base de données ERA source (celle que vous prévoyez de migrer) :
   ```
   mysqldump --host SRCHOST --disable-keys --extended-insert --routines -u SRCROOTLOGIN -p SRCERADBNAME > BA
   ```
3. **Préparez** une base de données vide sur l'instance MySQL Server cible :
   ```
   mysql --host TARGETHOST -u TARGETROOTLOGIN -p "--execute=CREATE DATABASE TARGETERADBNAME /*!40100 DEFAUL
   ```

REMARQUE : sur les systèmes Linux, utilisez des apostrophes « ' » plutôt que des guillemets doubles « " ».

4. **Restaurez** la base de données dans la base de données vide précédemment préparée sur l'instance MySQL Server cible :
   ```
   mysql --host TARGETHOST -u TARGETROOTLOGIN -p TARGETERADBNAME < BACKUPFILE
   ```
5. **Créez** un utilisateur de base de données ERA sur l'instance MySQL Server cible :
   ```
   mysql --host TARGETHOST -u TARGETROOTLOGIN -p "--execute=CREATE USER TARGETERALOGIN@'%' IDENTIFIED BY 'TA
   ```

Caractères recommandés pour **TARGETERALOGIN :**

- Lettres ASCII en minuscules, chiffres et trait de soulignement « _ »

Caractères recommandés pour **TARGETERAPASSWD :**

- Caractères ASCII uniquement, notamment des lettres ASCII en majuscules et minuscules, des chiffres, des espaces et des caractères spéciaux
- N'utilisez pas de caractères non-ASCII tels que les accolades et le caractère @

Si vous ne suivez pas les recommandations ci-dessus relatives aux caractères, il est possible que vous rencontriez des problèmes de connexion de base de données ou que vous deviez échapper les caractères spéciaux lors des étapes de modification de la chaîne de connexion à la base de données qui suivent. Les règles d'échappement de caractères ne sont pas incluses dans ce document.

6. **Accordez** des droits d'accès adéquats à l'utilisateur de la base de données ERA sur l'instance MySQL Server cible :

```
mysql --host TARGETHOST -u TARGETROOTLOGIN -p "--execute=GRANT ALL ON TARGETERADBNAME.* TO TARGETERALOGI
```

REMARQUE : sur les systèmes Linux, utilisez des apostrophes « ' » plutôt que des guillemets doubles « " ».

7. **Recherchez le fichier** `startupconfiguration.ini` sur l'ordinateur sur lequel ERA Server/Proxy est installé.
   - Pour Windows Vista et versions ultérieures :

     % PROGRAMDATA %\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration \startupconfiguration.ini
   - Pour les versions antérieures de Windows :

     % ALLUSERSPROFILE %\ Application Data\ESET\RemoteAdministrator\Server\EraServerApplicationData \Configuration\startupconfiguration.ini
   - Pour Linux :

     /etc/opt/eset/RemoteAdministrator/Server/StartupConfiguration.ini
8. **Modifiez** la chaîne de connexion à la base de données dans ERA Server/Proxy `startupconfiguration.ini`
   - Définissez l'adresse et le port du nouveau serveur de base de données.
   - Définissez le nom d'utilisateur et le mot de passe.
   - Le résultat final doit ressembler à celui-ci :

```
DatabaseType=MySqlOdbc
DatabaseConnectionString=Driver=MySQL ODBC 5.3 Unicode Driver;Server=TARGETHOST;Port=3306;User=TARGETERA
```

9. **Démarrez** ERA Server/Proxy et vérifiez que le service ERA Server/Proxy s'exécute correctement.

3.4 Image ISO

Une image ISO est l'un des formats dans lesquels vous pouvez télécharger (catégorie des programmes d'installation tout en un) les programmes d'installation d'ESET Remote Administrator. Elle contient les éléments suivants :

- Package du programme d'installation ERA
- Programmes d'installation distincts pour chaque composant

L'image ISO s'avère utile lorsque vous souhaitez conserver tous les programmes d'installation d'ESET Remote Administrator à un même emplacement. Elle évite également d'avoir à télécharger les programmes d'installation à partir du site Web ESET chaque fois que vous devez exécuter une installation. Elle permet enfin d'installer ESET Remote Administrator sur une machine virtuelle.

3.5 Enregistrement du service DNS

Pour configurer un enregistrement de ressource DNS :

1. Sur le serveur DNS (serveur DNS sur le contrôleur de domaine), accédez à **Panneau de configuration** > **Outils d'administration**.
2. Sélectionnez la valeur DNS.
3. Dans le Gestionnaire DNS, sélectionnez *_tcp* dans l'arborescence, puis créez un enregistrement **Emplacement du service (SRV)**.
4. Saisissez le nom du service dans le champ **Service** conformément aux règles standard DNS, puis tapez un trait de soulignement (**_**) devant le nom du service (utilisez votre propre nom, comme **_era**).
5. Dans le champ **Protocole**, saisissez le protocole tcp au format suivant : *_tcp*.
6. Saisissez le port 2222 dans le champ **Numéro de port**.
7. Saisissez le nom de domaine complet (FQDN) d'ERA Server dans le champ **Hôte offrant ce service**.
8. Sauvegardez l'enregistrement en cliquant sur [**OK**], puis sur [**Terminé**]. L'enregistrement s'affiche alors dans la liste.

Pour vérifier l'enregistrement DNS :

1. Connectez-vous à un ordinateur de votre domaine, puis ouvrez une ligne de commandes (*cmd.exe*).
2. Saisissez *nslookup* dans la ligne de commandes, puis appuyez sur **Entrée**.
3. Saisissez *set querytype=srv*, puis appuyez sur **Entrée**.
4. Saisissez *_era._tcp.domain.name*, puis appuyez sur **Entrée**. L'emplacement du service est affiché correctement.

REMARQUE : cette procédure est identique pour Windows et Linux.

REMARQUE : veillez à remplacer la valeur Hôte offrant ce service par le nom de domaine complet du nouveau serveur lors de l'installation d'ESET Remote Administrator Server sur un autre ordinateur.

4. Outil de migration

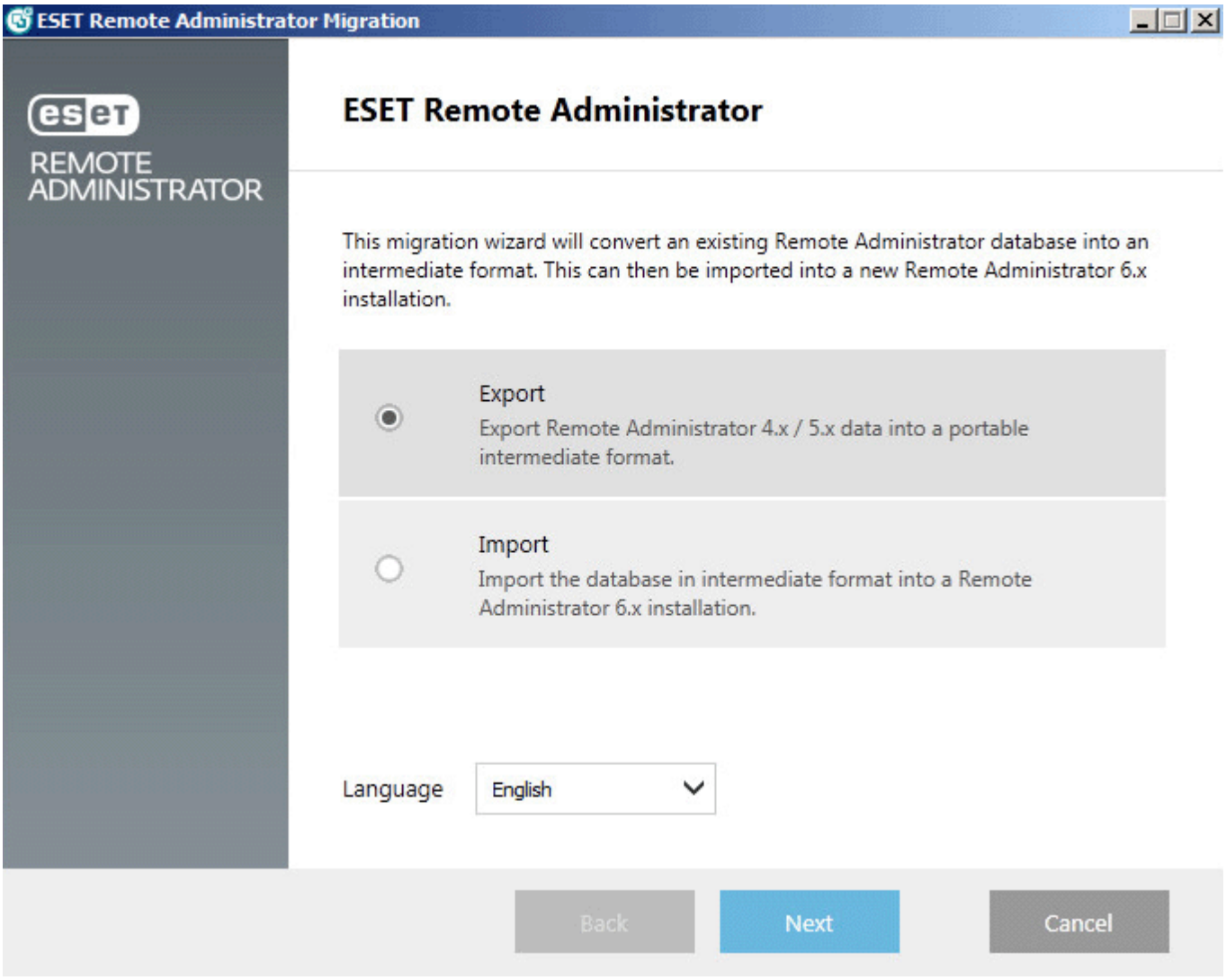
Vous pouvez utiliser l'outil de migration pour effectuer une mise à jour/migration depuis une génération précédente de ESET Remote Administrator vers ESET Remote Administrator 6. L'outil de migration est une application autonome sous la forme d'un assistant qui permet la migration directe des données d'ERA 4.x/5.x dans une base de données intermédiaire, permettant l'importation des données dans ERA 6.x.

IMPORTANT : la version de l'outil de migration doit correspondre à la version d'ESET Remote Administrator vers laquelle vous allez migrer. Pour savoir quelle version de l'outil de migration utiliser, consultez cet article de la base de connaissances.

- Téléchargez la version appropriée de l'outil de migration ESET Remote Administrator. Pour le télécharger, vous avez besoin du nom d'utilisateur et du mot de passe émis par ESET.
- Exécutez l'outil de migration localement sur votre ancien serveur ERA 4.x / 5.x. Il n'est pas possible d'exécuter l'outil de migration depuis une machine distante.
- La configuration de votre ancien serveur ERA n'est pas migré.
- Les groupes paramétriques ne sont pas migrés.
- Vous pouvez migrer les stratégies avec l'outil de migration 6.2.x et les versions ultérieures. Il existe toutefois quelques spécificités pour la migration des stratégies :
  - Seules les stratégies du serveur ERA supérieur sont migrées.
  - Seules les définitions des stratégies sont migrées, les relations des stratégies ne sont pas migrées.
  - Il faudra attribuer manuellement les stratégies migrées aux groupes appropriés après la migration.
  - La hiérarchie des stratégies est omise. Dans le cas où il y a un indicateur **ignorer** dans votre ancien ERA, il sera converti en **forcer** pour le même paramètre dans la stratégie ERA 6.
  - Si l'ancien ERA contient des paramètres relatifs à plusieurs produits dans une seule stratégie, une stratégie individuelle sera créée dans ERA 6 pour chaque produit.

REMARQUE : après la migration, il est conseillé de vérifier tous les éléments (ordinateurs, groupes statiques, stratégies, etc.) pour vérifier qu'ils sont en place et que le résultat de la migration correspond aux attentes. Si vous constatez des divergences, une intervention sera nécessaire, par exemple la création manuelle de stratégies.

REMARQUE : Si une erreur se produit pendant le processus de migration, elle est consignée dans le fichier `migration.log` situé dans le même dossier que l'outil de migration. Si vous avez un accès en lecture seule à ce dossier, une fenêtre de connexion s'ouvrira. La même chose se produit s'il n'y a pas suffisamment d'espace disque. Cela signifie que le fichier journal n'est pas créé et que les résultats ne sont visibles que dans la fenêtre du journal.



REMARQUE : pour résoudre un problème lié aux fichiers `MSVCP100.dll` ou `MSVCR100.dll` manquants, installez la dernière version de Microsoft Visual C++ 2010 Redistributable Package. Vous pouvez utiliser le lien suivant Microsoft Visual C++ 2010 Redistributable Package (x86).

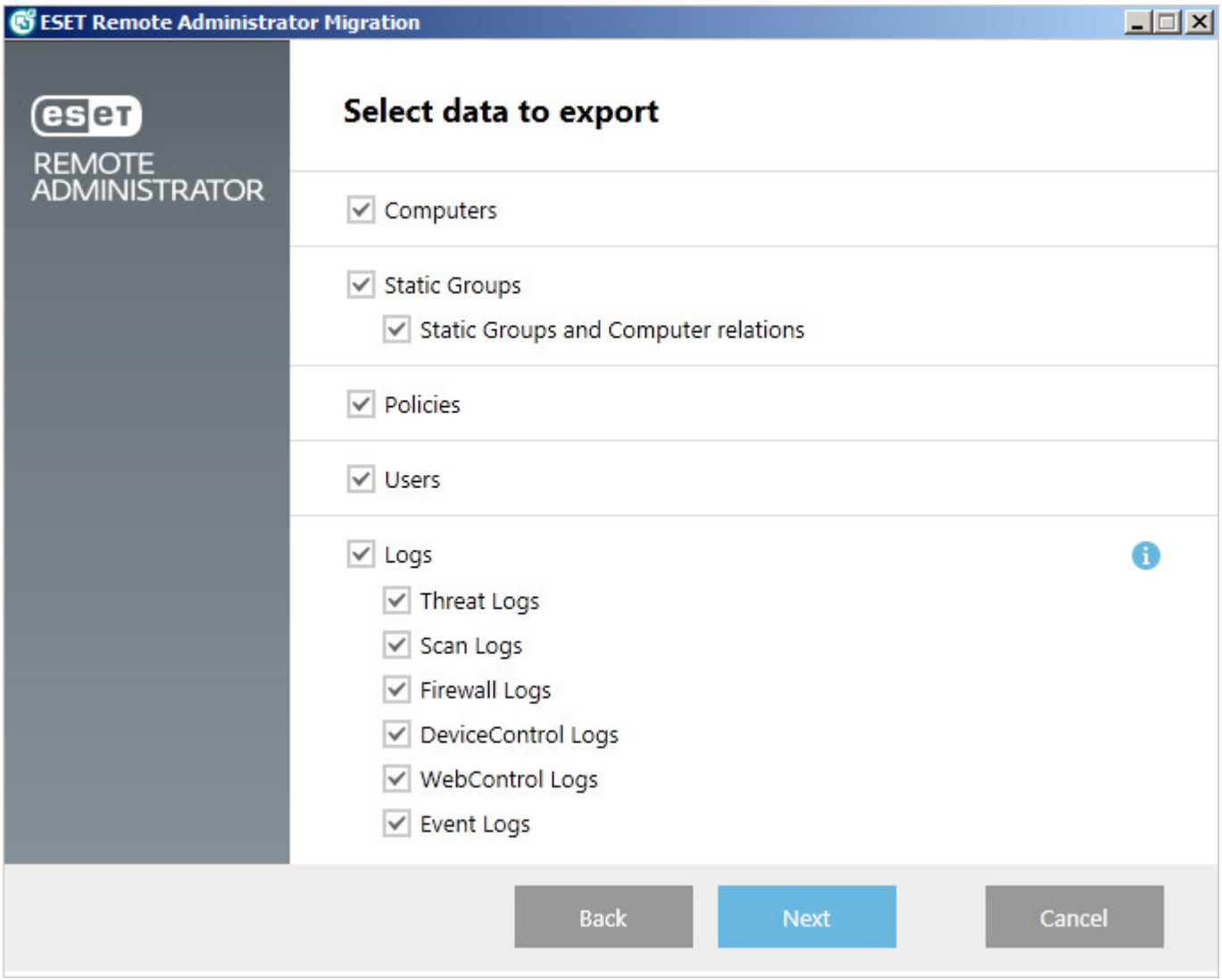
Voici des scénarios de migration pour vous guider pendant le processus de migration :

- Scénario de migration 1 : migration vers ERA 6.x s'exécutant sur un autre ordinateur qu'ERA 4.x / 5.x.
- Scénario de migration 2 : migration vers ESET Remote Administrator 6.x s'exécutant le même ordinateur qu'ERA 4.x / 5.x.
- Scénario de migration 3 : migration vers ERA 6.x où les points de terminaison se connectent à l'ancienne version d'ERA 4.x / 5.x jusqu'à ce qu'ERA Agent soit déployé par ERA 6.x.

4.1 Scénario de migration 1

Ce scénario traite de la migration vers ERA 6 s'exécutant sur un autre ordinateur qu'ERA 4.x / 5.x.

1. La première étape du processus de migration consiste à installer et exécuter ERA 6.x sur un autre ordinateur.
2. Démarrez l'outil de migration ESET Remote Administrator sur l'ordinateur ERA 4.x / 5.x, puis sélectionnez **Exporter** pour enregistrer les données de l'ancienne version d'ERA dans un fichier de base de données intermédiaire.
3. L'assistant de migration peut uniquement transférer des données spécifiques. Sélectionnez les données que vous souhaitez transférer, puis cliquez sur Suivant.



En raison de la nouvelle conception et des nouvelles fonctions des groupes dynamiques d'ERA 6.x, il n'est pas possible de transférer les tâches, stratégies et groupes paramétriques à partir des anciennes versions. Une fois que vous avez sélectionné un dossier dans lequel enregistrer la base de données temporaire, l'assistant affiche l'état de l'archive de la base de données ERA 4.x / 5.x.

Toutes les données sont exportées vers une **base de données intermédiaire**.

4. Lorsque l'exportation des données est terminée, deux options s'offrent à vous :
   - La première option consiste à **terminer** l'exportation, à **copier**le fichier de base de données temporaire sur un serveur exécutant ESET Remote Administrator 6.x et à importer les données à l'aide de l'outil de migration ERA sur ce serveur.
   - La deuxième option consiste à cliquer sur le bouton **Importer maintenant** pour importer directement les données dans ESET Remote Administrator 6x via le réseau. Indiquez les informations de connexion et d'ouverture de session du nouveau serveur ERA Server.

REMARQUE : les groupes statiques synchronisés à partir d'Active Directory sont ignorés et ne sont pas exportés.

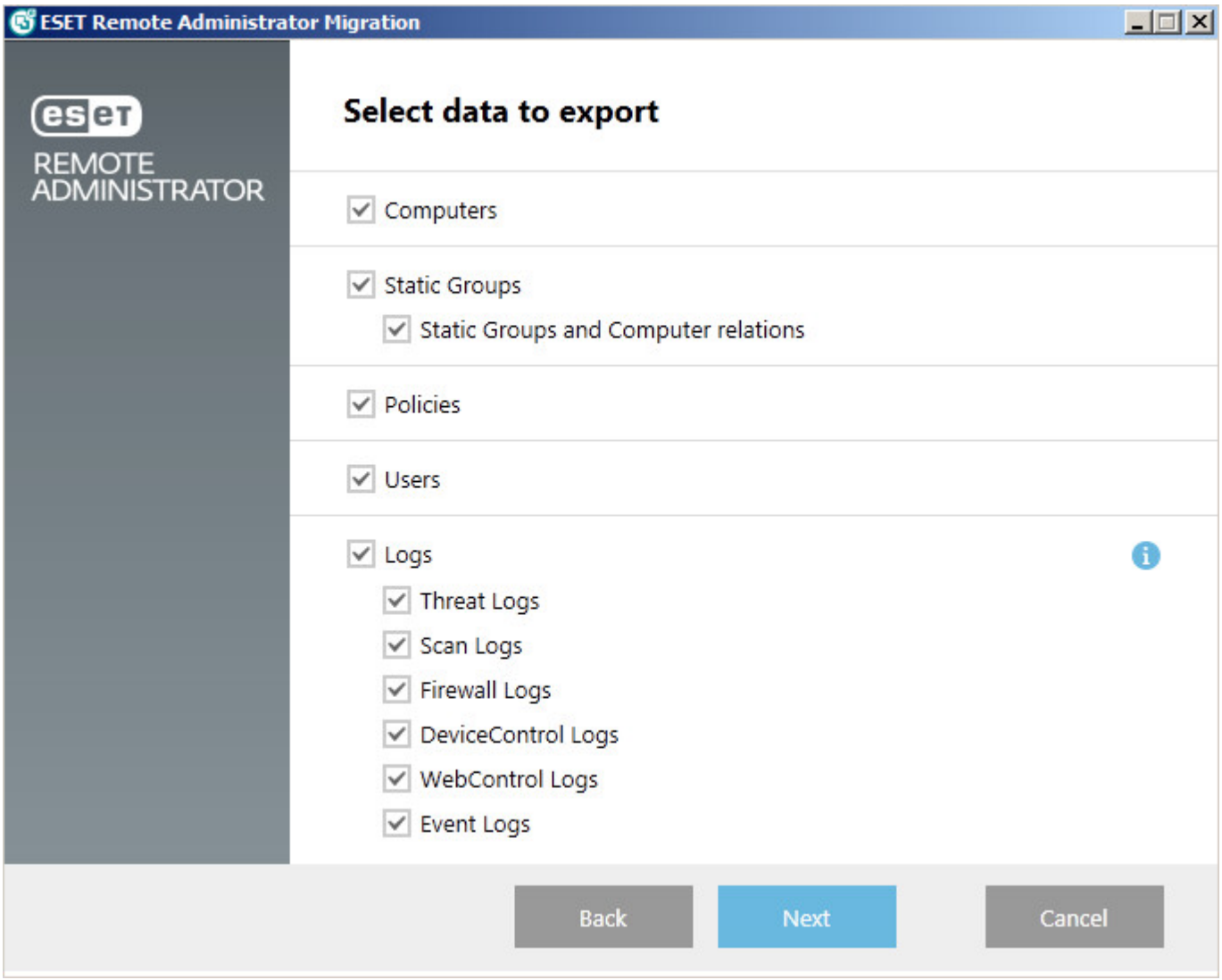
- Si les paramètres du serveur ne permettent pas l'importation de données spécifiques, l'outil de migration ESET Remote Administrator vous offre la possibilité de modifier les paramètres d'ERA 6.x pour des composants en particulier.
- Chaque composant est alors importé. Un **journal d'importation (migration)** est disponible pour chaque composant. Lorsque l'importation est terminée, l'outil de migration affiche les résultats du processus d'importation.
- Si vous avez migré des utilisateurs, les mots de passe de ces derniers sont réinitialisés et remplacés des mots de passe générés de manière aléatoire. Ces mots de passe peuvent être exportés au format `.csv`.
- L'assistant de l'outil de migration génère également un script qui peut être utilisé pour préconfigurer les ERA Agents sur les ordinateurs clients. Ce script se présente sous la forme d'un fichier `.bat` exécutable qui peut être distribué aux ordinateurs clients.
- Il est recommandé d'examiner les paramètres et les données migrés pour s'assurer que l'importation a été correctement effectuée. Une fois l'examen terminé, vous pouvez utiliser ce script pour déployer ERA Agent sur un petit groupe d'ordinateurs afin de vérifier qu'ils se connectent correctement au serveur.
- Une fois la connexion établie pour le groupe de test, vous pouvez déployer l'Agent sur les ordinateurs restants (manuellement ou à la l'aide d'une tâche de synchronisation d'Active Directory).

REMARQUE : si une des étapes de migration échoue, vous devez restaurer les modifications apportées à ERA 6.x, configurer les ordinateurs pour qu'ils se connectent à ERA 4.x / 5.x, récupérer les données de sauvegarde d'ERA 4.x / 5.x et contacter le service client ESET.

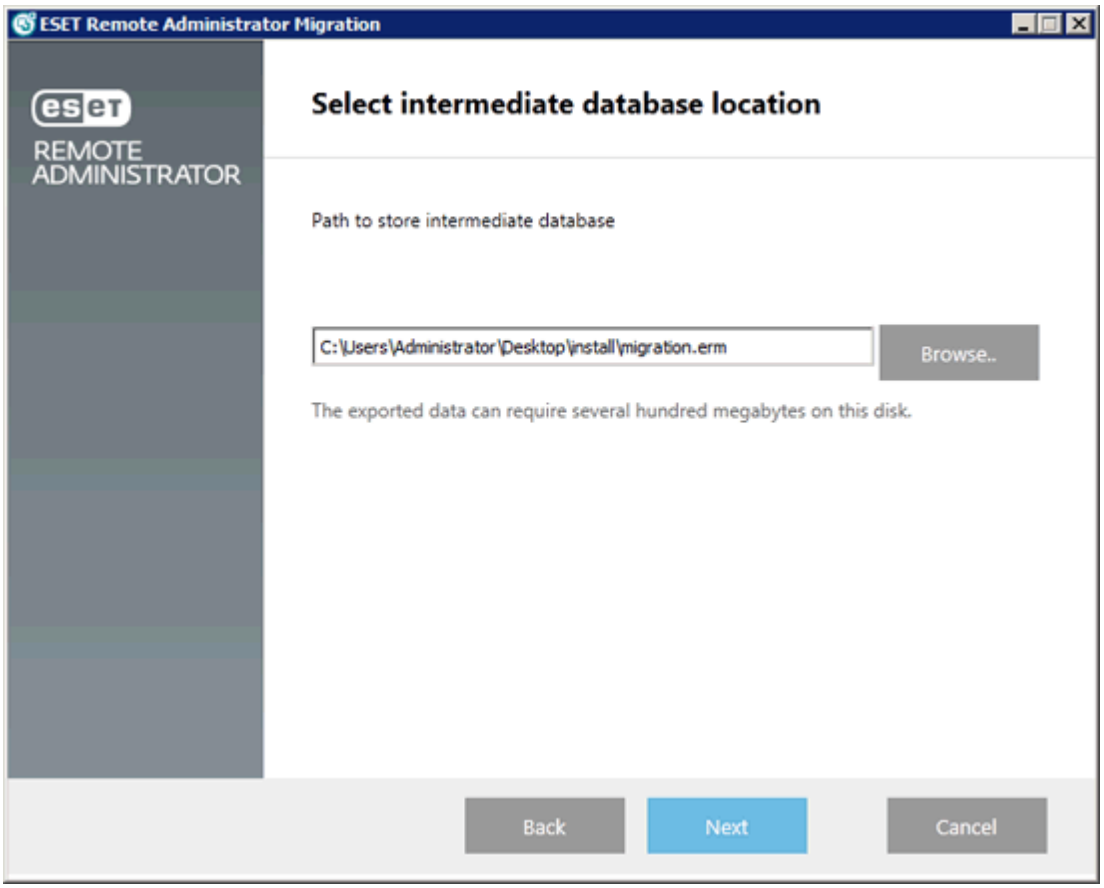
4.2 Scénario de migration 2

Ce scénario traite de la migration vers ESET Remote Administrator 6.x s'exécutant un même ordinateur qu'ERA 4.x / 5.x. Toutes les données d'ERA doivent être sauvegardées (à l'aide de l'outil de maintenance ESET) et les services ERA arrêtés dans le système d'exploitation avant de migrer toute donnée.

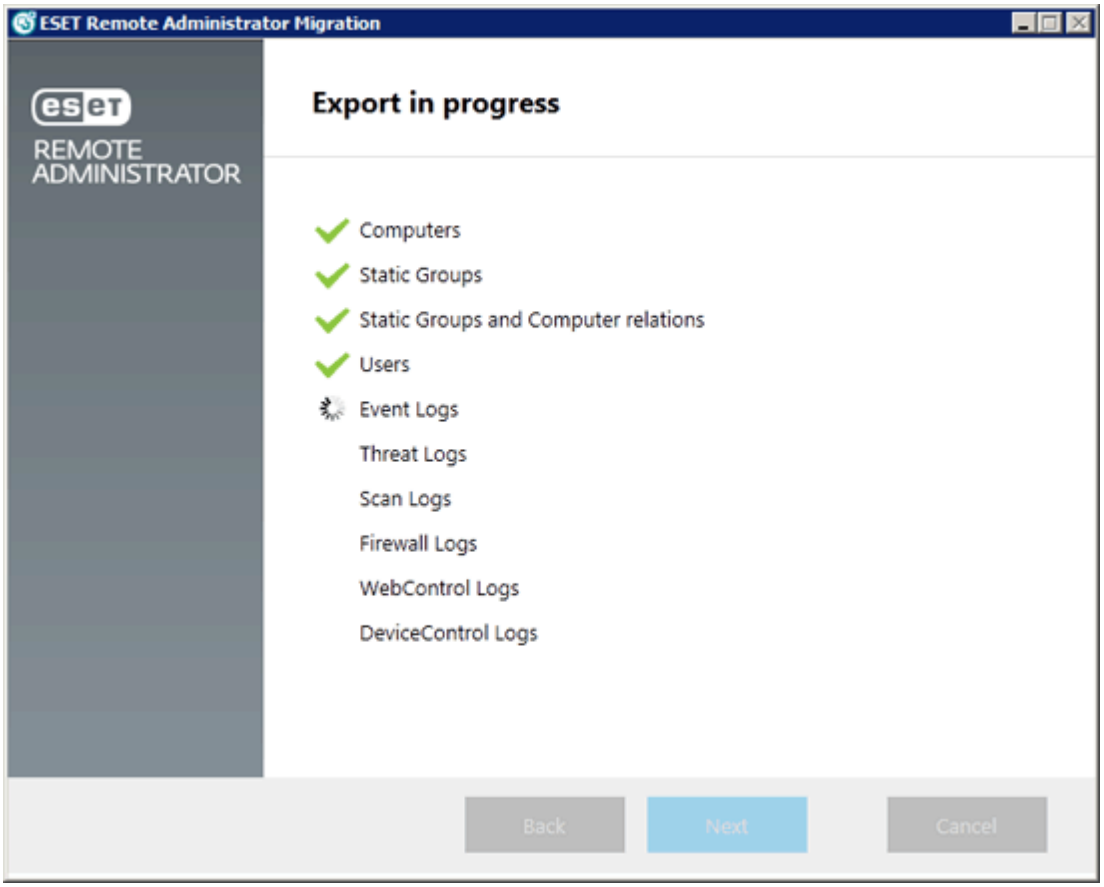
1. Une fois l'outil de migration ESET Remote Administrator exécuté sur l'ordinateur ERA 4.x / 5.x, l'administrateur doit sélectionner l'option **Exporter** pour enregistrer les données d'ERA 4.x / 5.x dans un fichier de base de données intermédiaire. L'assistant de migration peut uniquement transférer des données spécifiques :



REMARQUE : en raison de la nouvelle conception et des nouvelles fonctions des groupes dynamiques d'ERA 6.x, il n'est pas possible de transférer les tâches, stratégies et groupes paramétriques à partir d'ERA 4.x / 5.x.



2. Une fois que vous avez sélectionné un dossier dans lequel enregistrer la base de données temporaire, l'assistant affiche l'état de l'archive de la base de données ERA 4.x / 5.x.



3. Toutes les données sont exportées vers une **base de données intermédiaire**.

- Après l'**exportation** des données, et avant le **déploiement** d'ERA 6.x, ERA 4.x / 5.x doit être **désinstallé**.

- Lorsque ERA 6.x est installé, la base de données exportée peut être importée à l'aide de l'outil de migration. L'administrateur est invité à sélectionner le fichier enregistré.
- Si les paramètres du serveur ne permettent pas l'importation de données spécifiques, l'outil de migration ESET Remote Administrator vous offre la possibilité de modifier les paramètres d'ERA 6.x pour des composants en particulier.
- Chaque composant est alors importé. Un **journal d'importation (migration)** est disponible pour chaque composant. Lorsque l'importation est terminée, l'outil de migration affiche les résultats du processus d'importation.
- Si vous avez migré des utilisateurs, les mots de passe de ces derniers sont réinitialisés et remplacés des mots de passe générés de manière aléatoire. Ces mots de passe peuvent être exportés au format `.csv` .
- L'assistant de l'outil de migration génère également un script qui peut être utilisé pour préconfigurer les ERA Agents sur les ordinateurs clients. Ce script se présente sous la forme d'un fichier `.bat` exécutable qui peut être distribué aux ordinateurs clients.
- Il est recommandé d'examiner les paramètres et les données migrés pour s'assurer que l'importation a été correctement effectuée. Une fois l'examen terminé, vous pouvez utiliser ce script pour déployer ERA Agent sur un petit groupe d'ordinateurs afin de vérifier qu'ils se connectent correctement au serveur.
- Une fois la connexion établie pour le groupe de test, vous pouvez déployer l'Agent sur les ordinateurs restants (manuellement ou à la l'aide d'une tâche de synchronisation d'Active Directory).

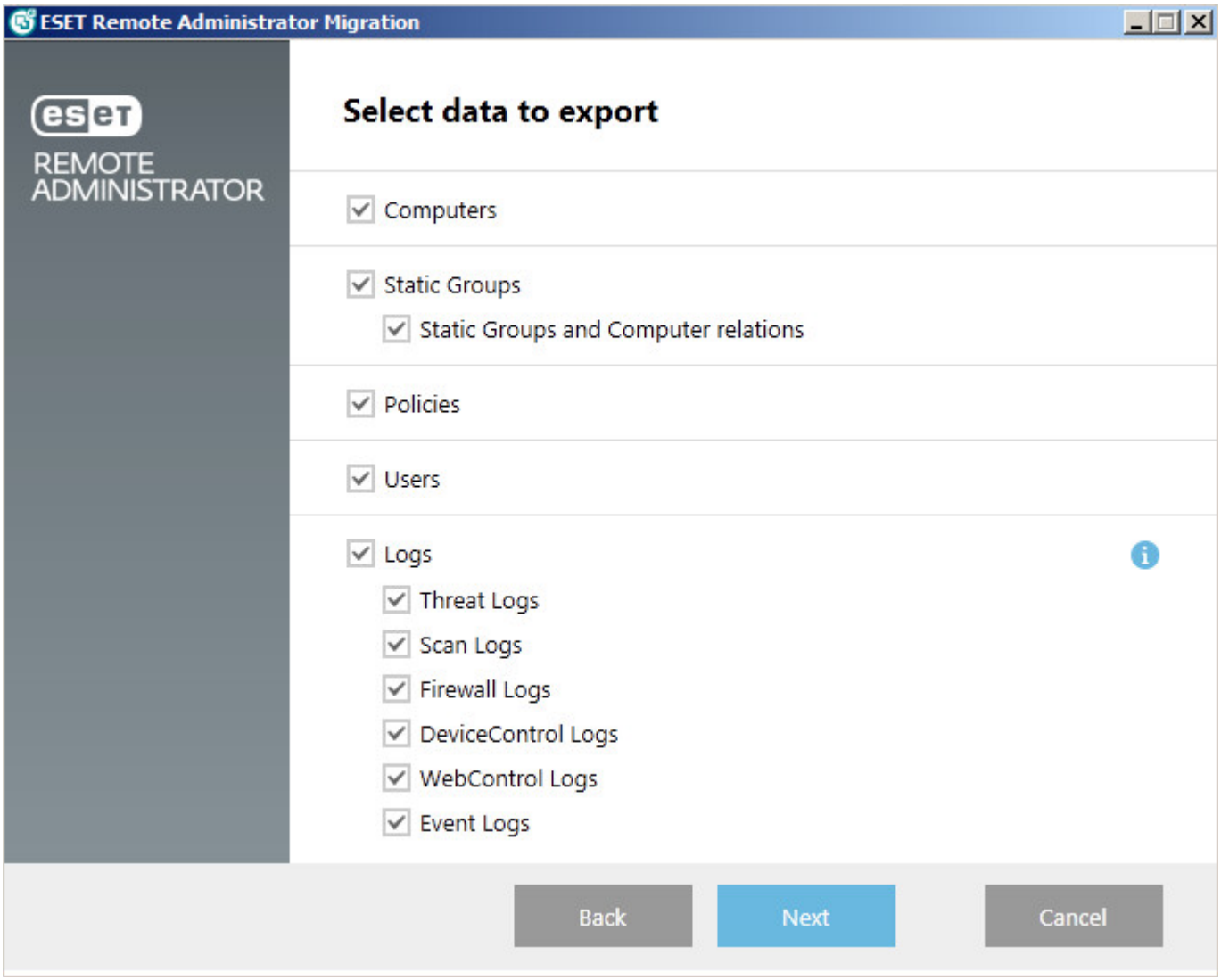
REMARQUE : si une des étapes de migration échoue, vous devez restaurer les modifications apportées à ERA 6.x, configurer les ordinateurs pour qu'ils se connectent à ERA 4.x / 5.x, récupérer les données de sauvegarde d'ERA 4.x / 5.x et contacter le service client ESET.

4.3 Scénario de migration 3

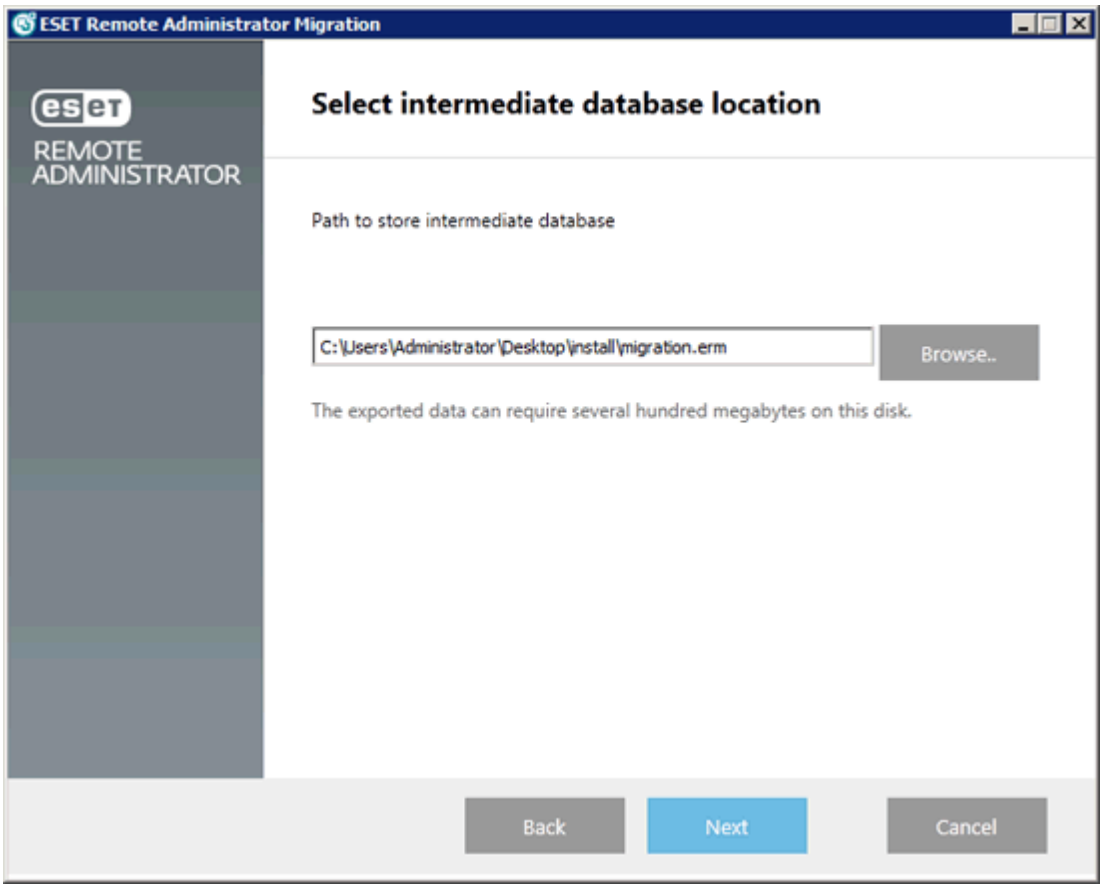
Ce scénario traite de la migration vers ERA 6.x où les points de terminaison se connectent à l'ancienne version d'ERA 4.x / 5.x jusqu'à ce qu'ERA Agent soit déployé par ERA 6.x.

REMARQUE : ce scénario est destiné uniquement à des utilisateurs très expérimentés. Il est déconseillé d'effectuer ce type de migration, à moins qu'il n'y ait pas d'autres alternatives.

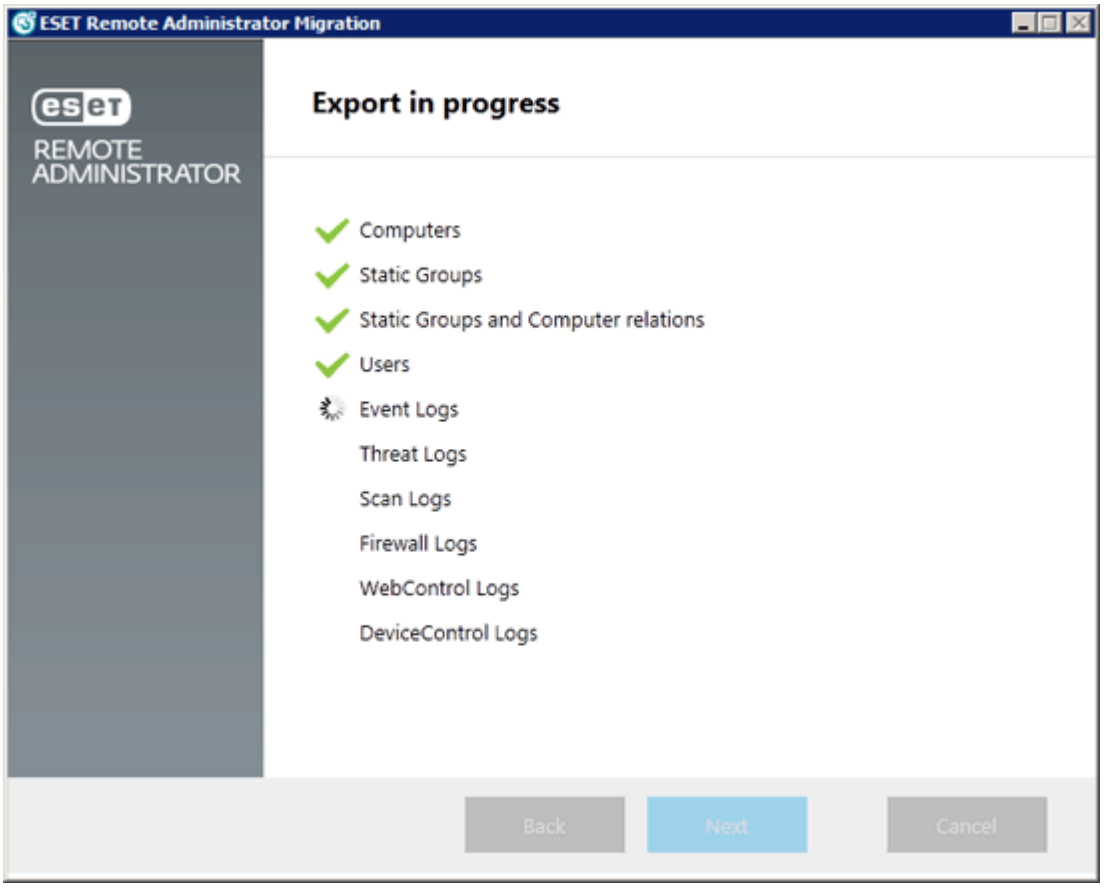
1. Une fois l'outil de migration ESET Remote Administrator exécuté sur l'ordinateur ERA 4.x / 5.x, l'administrateur doit sélectionner l'option **Exporter** pour enregistrer les données d'ERA 4.x / 5.x dans un fichier de base de données intermédiaire. L'assistant de migration peut uniquement transférer des données spécifiques :



REMARQUE : en raison de la nouvelle conception et des nouvelles fonctions des groupes dynamiques d'ERA 6.x, il n'est pas possible de transférer les tâches, stratégies et groupes paramétriques à partir d'ERA 4.x / 5.x.



2. Une fois que vous avez sélectionné un dossier dans lequel enregistrer la base de données temporaire, l'assistant affiche l'état de l'archive de la base de données ERA 4.x / 5.x.



3. Toutes les données sont exportées vers une **base de données intermédiaire**.

4. Si ERA 6 sera installé sur le même ordinateur qu'ERA 4.x / 5.x, vous pouvez modifier les anciens ports d'ERA et renommer le service serveur (`sc config ERA_SERVER DisplayName= "ESET Remote Administrator g1"`).

5. ESET Remote Administrator 4.x / 5.x doit être redémarré après l'exportation des données.
6. Installez ESET Remote Administrator 6, puis importez la base de données intermédiaire à l'aide de l'outil de migration.
    - Si les paramètres du serveur ne permettent pas l'importation de données spécifiques, l'outil de migration ESET Remote Administrator vous offre la possibilité de modifier les paramètres d'ERA 6.x pour des composants en particulier.
    - Chaque composant est alors importé. Un **journal d'importation (migration)** est disponible pour chaque composant. Lorsque l'importation est terminée, l'outil de migration affiche les résultats du processus d'importation.
    - Si vous avez migré des utilisateurs, les mots de passe de ces derniers sont réinitialisés et remplacés des mots de passe générés de manière aléatoire. Ces mots de passe peuvent être exportés au format `.csv` .
    - L'assistant de l'outil de migration génère également un script qui peut être utilisé pour préconfigurer les ERA Agents sur les ordinateurs clients. Ce script se présente sous la forme d'un fichier `.bat` exécutable qui peut être distribué aux ordinateurs clients.
    - Il est recommandé d'examiner les paramètres et les données migrés pour s'assurer que l'importation a été correctement effectuée. Une fois l'examen terminé, vous pouvez utiliser ce script pour déployer ERA Agent sur un petit groupe d'ordinateurs afin de vérifier qu'ils se connectent correctement au serveur.
    - Une fois la connexion établie pour le groupe de test, vous pouvez déployer l'Agent sur les ordinateurs restants (manuellement ou à la l'aide d'une tâche de synchronisation d'Active Directory).

REMARQUE : si une des étapes de migration échoue, vous devez restaurer les modifications apportées à ERA 6.x, configurer les ordinateurs pour qu'ils se connectent à ERA 4.x / 5.x, récupérer les données de sauvegarde d'ERA 4.x / 5.x et contacter le service client ESET.

La conséquence de ce type de migration est qu'aucun journal n'est exporté entre le processus de sauvegarde de la base de données ERA 4.x / 5.x et le déploiement de l'Agent sur un ordinateur client. Ces données seront toutefois toujours présentes sur votre ancienne copie d'ERA 4.x / 5.x.

5. Procédures de mise à niveau

Cette section décrit comment mettre à niveau des composants de l'infrastructure d'ESET Remote Administrator, comment réinstaller ERA Server et quelques autres scénarios de mise à niveau.

Pour connaître la version de chaque composant ERA que vous exécutez, il suffit de savoir quelle est votre version d'ESET Remote Administrator Server. Accédez à la page À propos dans la console Web ERA, puis reportez-vous à cet article de la base de connaissance qui répertorie toutes les versions des composants ERA par ERA Server.

Pour obtenir un autre guide de mise à niveau d'ESET Remote Administrator vers la dernière version (6.x), consultez l'article de la base de connaissances.

REMARQUE : si vous envisagez de migrer d'ERA Server vers un nouveau serveur, vous devez exporter ou sauvegarder le certificat ERA Server et l'autorité de certification. Dans le cas contraire, aucun composant ERA n'est en mesure de communiquer avec votre nouveau ERA Server.

5.1 Mise à niveau des composants

L'utilisation de la tâche Mise à niveau des composants, disponible dans la console Web ERA, est la méthode recommandée pour mettre à niveau votre infrastructure ERA. L'exemple ci-dessous illustre la configuration de la tâche **Mettre à jour les composants d'ESET Remote Administrator** pour effectuer une mise à niveau d'ERA version 6.1.21.0 ou 6.1.28.0 vers ERA version 6.1.33.0.

Lors de l'exécution de cette tâche, il est vivement recommandé de sélectionner le **groupe Tous** comme cible pour être sûr que l'ensemble de l'infrastructure ERA est mise à niveau.

Liste des composants mis à niveau :

- ERA Server
- ERA Agent : la tâche met à jour les instances ERA Agent installées sur tous les ordinateurs du réseau sélectionnés comme cibles pour la tâche.
- ERA Proxy
- Console Web ERA : s'applique uniquement lorsque ce composant a été installé à l'aide du programme d'installation ERA tout en un ou de l'appliance virtuelle ERA et de n'importe quelle distribution Linux (à condition que le dossier d'installation figure dans `/var/lib/tomcat8/webapps/`, `/var/lib/tomcat7/webapps/`, `/var/lib/tomcat6/webapps/`, `/var/lib/tomcat/webapps/`)
- ERA MDM version 6.1.28.0

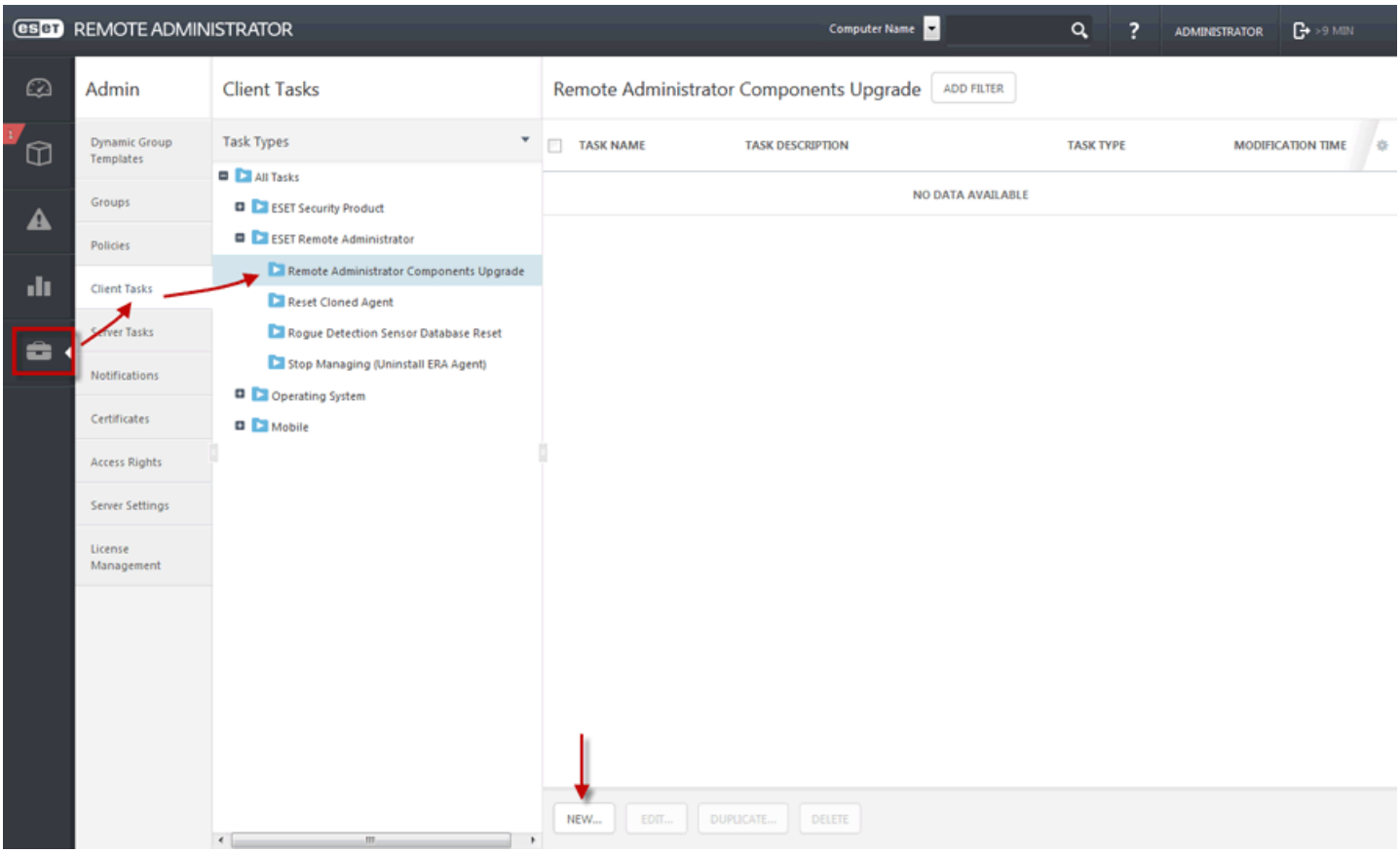
Les composants suivants doivent être manuellement mis à niveau :

- ERA Rogue Detection Sensor
- ERA MDM version 6.1.21.0

AVERTISSEMENT : si la mise à niveau des composants échoue sur un ordinateur qui exécute ERA Server ou la console Web, il est possible que vous ne puissiez pas vous connecter à distance à la console Web. Il est vivement conseillé de configurer un accès physique à l'ordinateur serveur avant d'effectuer cette mise à niveau. Si un accès physique à l'ordinateur est impossible, vérifiez que vous pouvez vous y connecter avec des privilèges administratifs à l'aide du Bureau à distance. Il est recommandé de sauvegarder les bases de données d'ERA Server et du Connecteur de périphérique mobile avant d'effectuer cette opération. Pour sauvegarder l'appliance virtuelle, créez un instantané.

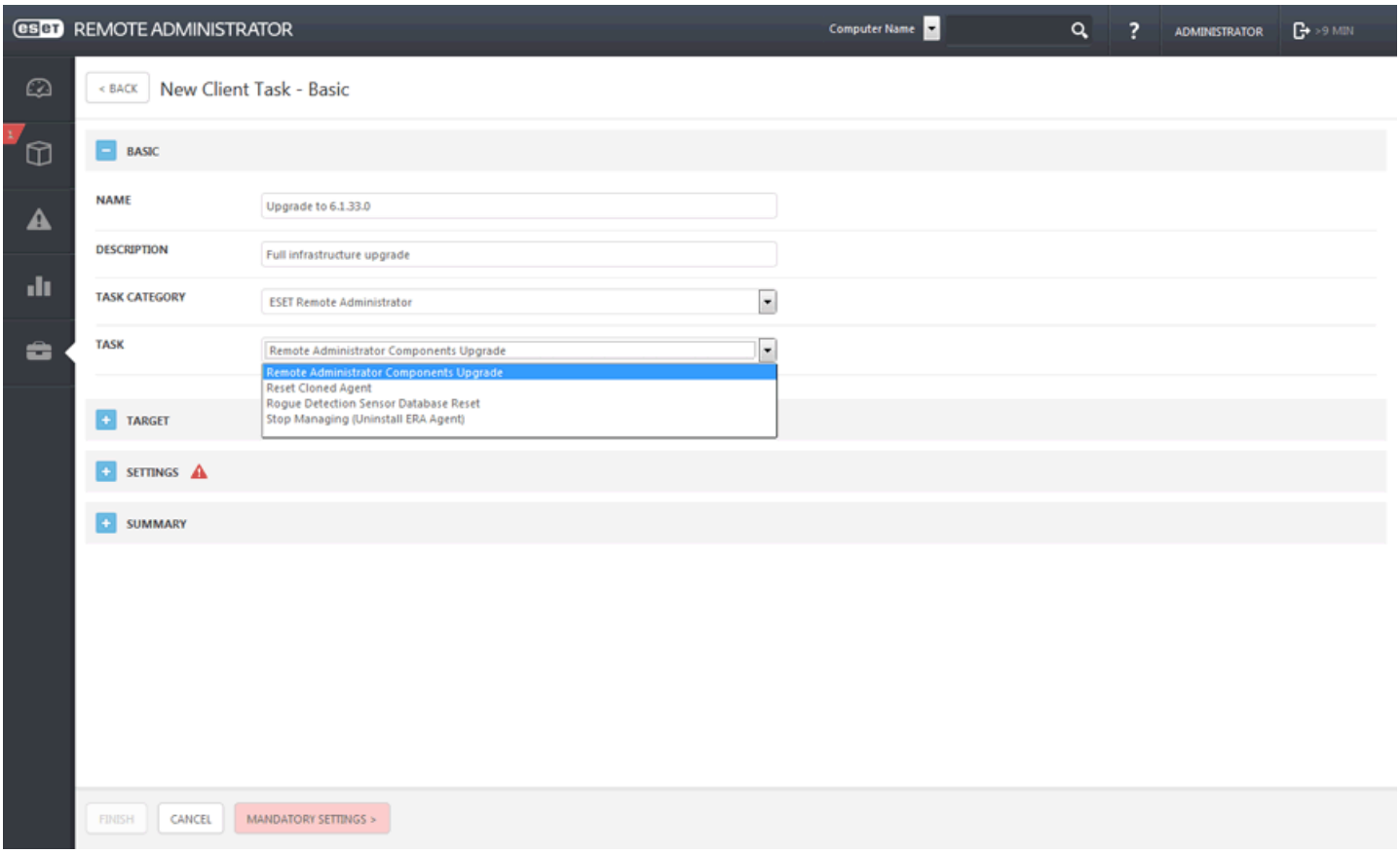
IMPORTANT : si l'instance d'ERA Server est installée sur un cluster de basculement, vous devez mettre à niveau manuellement le composant ERA Server sur chaque nœud du cluster. Une fois ERA Server mis à niveau, vous pouvez exécuter la tâche Mise à niveau des composants pour mettre à niveau le reste de l'infrastructure (les ERA Agents sur les ordinateurs clients, par exemple). Si ERA Agent est installé sur des clients Linux qui s'exécutent avec systemd dans votre infrastructure (les distributions avec des scripts init SysV ou upstart ne sont pas affectées), exécutez ce script avant d'exécuter la tâche Mise à niveau des composants.

1. Cliquez sur **Admin** > **Tâches client**, puis accédez à **Toutes les tâches** > **ESET Remote Administrator** > **Mettre à jour les composants d'ESET Remote Administrator**.
2. Cliquez sur **Nouveau...** pour commencer à configurer la nouvelle tâche.



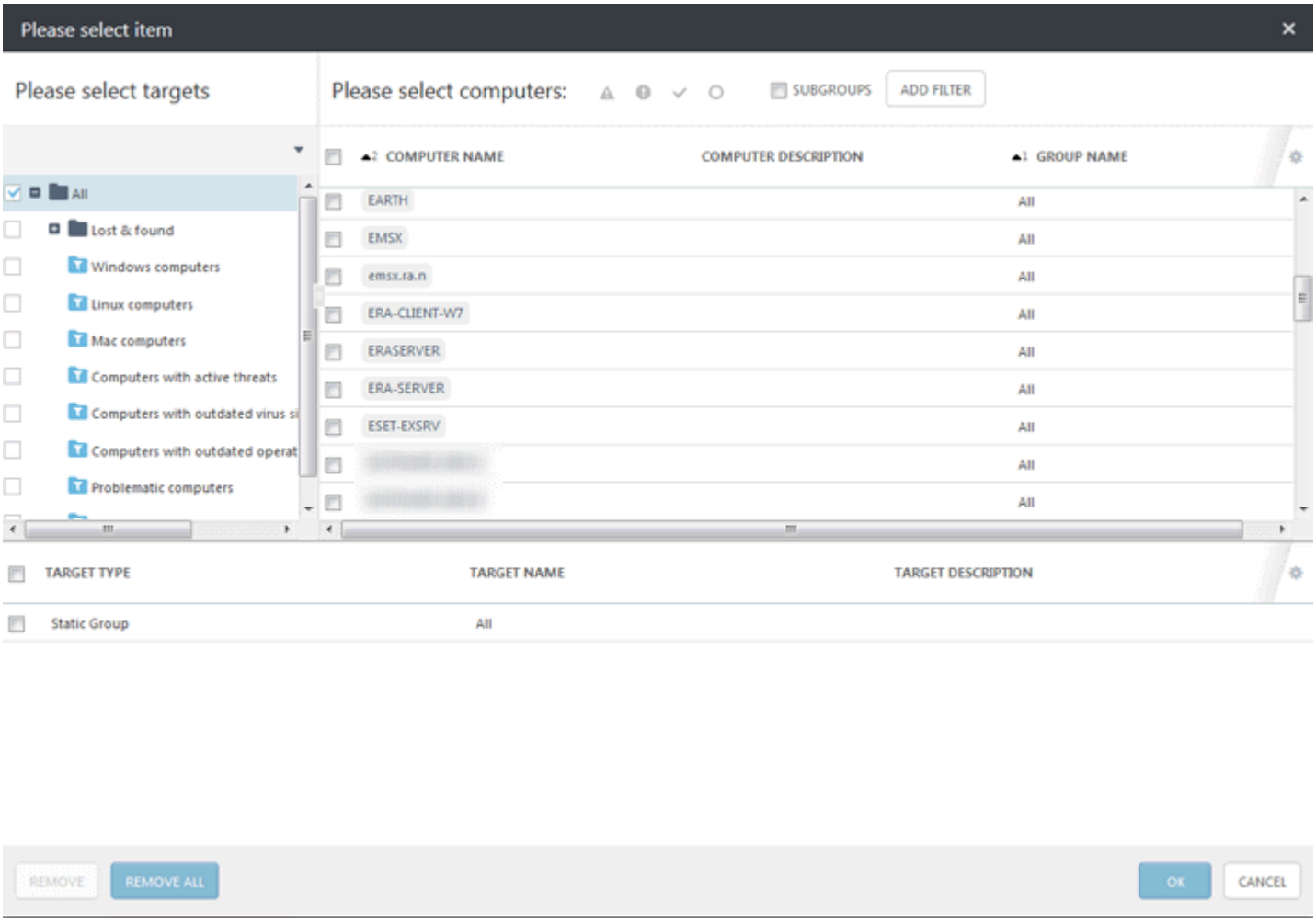
General

3. Entrez le **nom** et éventuellement une **description** de la tâche.
4. Dans le menu déroulant, sélectionnez **Mettre à jour les composants d'ESET Remote Administrator**.


REMOTE ADMINISTRATOR
Computer Name
ADMINISTRATOR
>9 MIN
< BACK
New Client Task - Basic
BASIC
NAME
Upgrade to 6.1.33.0
DESCRIPTION
Full infrastructure upgrade
TASK CATEGORY
ESET Remote Administrator
TASK
Remote Administrator Components Upgrade
Remote Administrator Components Upgrade
Reset Cloned Agent
Rogue Detection Sensor Database Reset
Stop Managing (Uninstall ERA Agent)
TARGET
SETTINGS
SUMMARY
FINISH
CANCEL
MANDATORY SETTINGS >

Cible

5. Cochez les cases en regard de toutes les cibles (ordinateurs individuels ou groupes) qui recevront cette tâche. Cliquez sur **Ajouter des cibles** pour afficher tous les groupes statiques et dynamiques et leurs membres. Sélectionnez **Groupe statique** > **Tous** pour exécuter la mise à jour sur l'infrastructure complète.

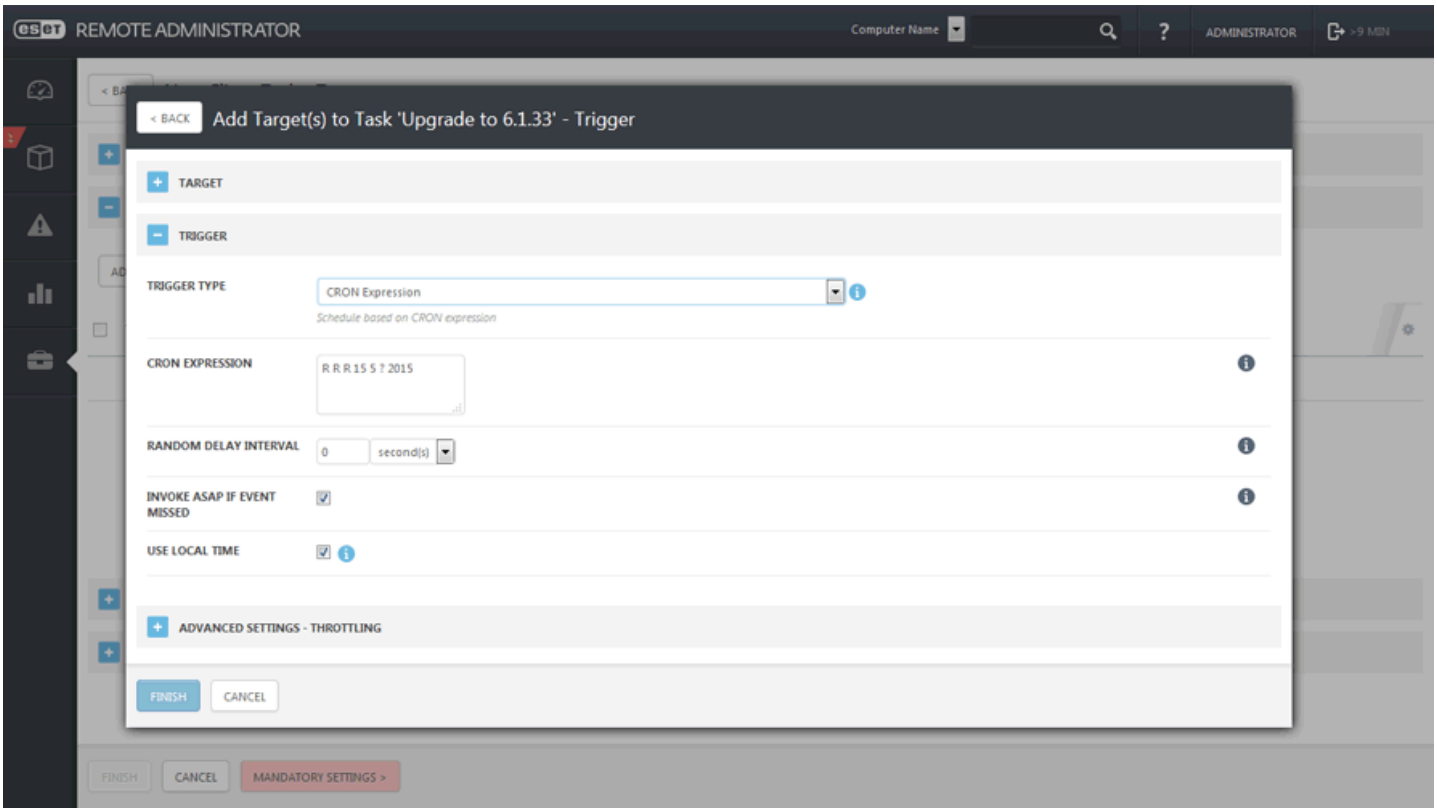


Déclencheur

6. Dans le menu déroulant **Type de déclencheur**, sélectionnez Expression CRON. Dans le champ de texte, tapez une expression CRON pour la date de déclenchement de la tâche. Par exemple, **R R R 15 ? 2015** permet d'exécuter une fois la tâche de manière aléatoire le 15 mai 2015.

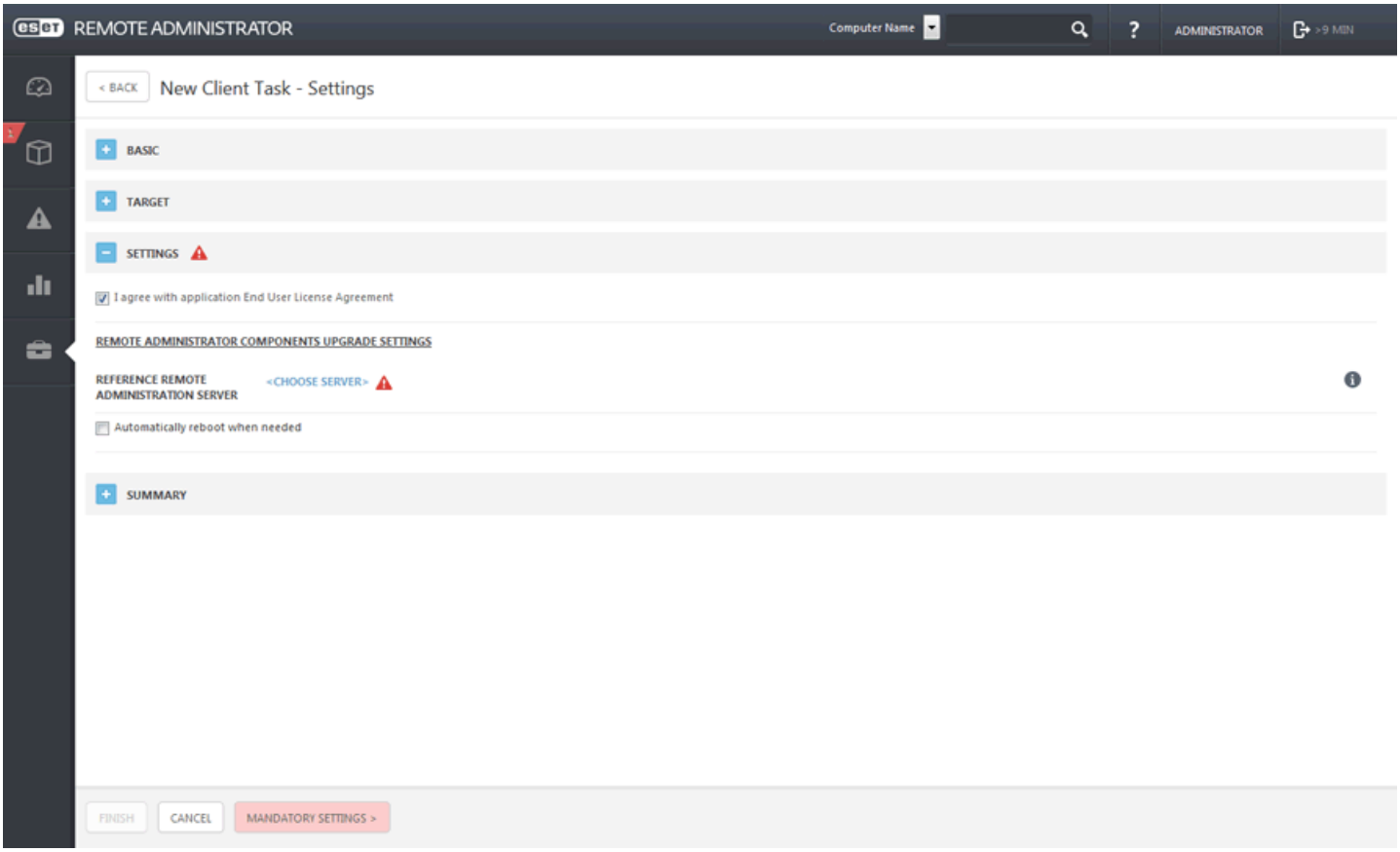
   Appeler dès que possible en cas d'événement manqué : utilisez cette option avec prudence. Si vous utilisez plusieurs clients virtualisés, tous les clients risquent d'être mis à niveau simultanément, ce qui peut entraîner des charges élevées sur l'infrastructure virtuelle.

7. Il est recommandé de sélectionner **Utiliser l'heure locale**. Cette option fait référence à l'heure locale des clients et non à celle du serveur. Lorsque vous avez terminé, cliquez sur **Terminer**.

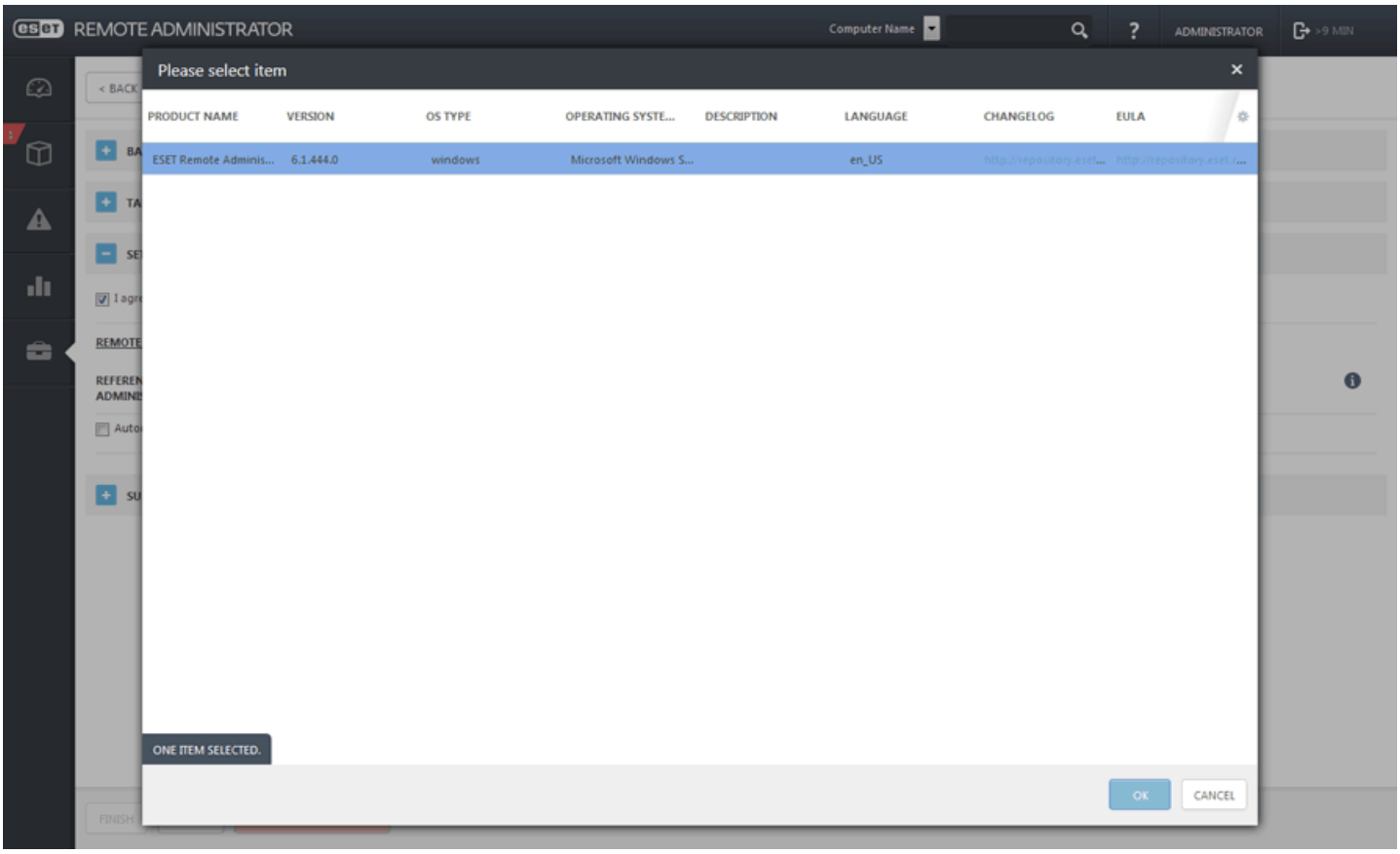


Paramètres

8. Cochez la case en regard de l'option **J'accepte les termes du Contrat de Licence Utilisateur Final de l'application** si vous les acceptez. Pour plus d'informations, reportez-vous à Gestion de licences ou CLUF.

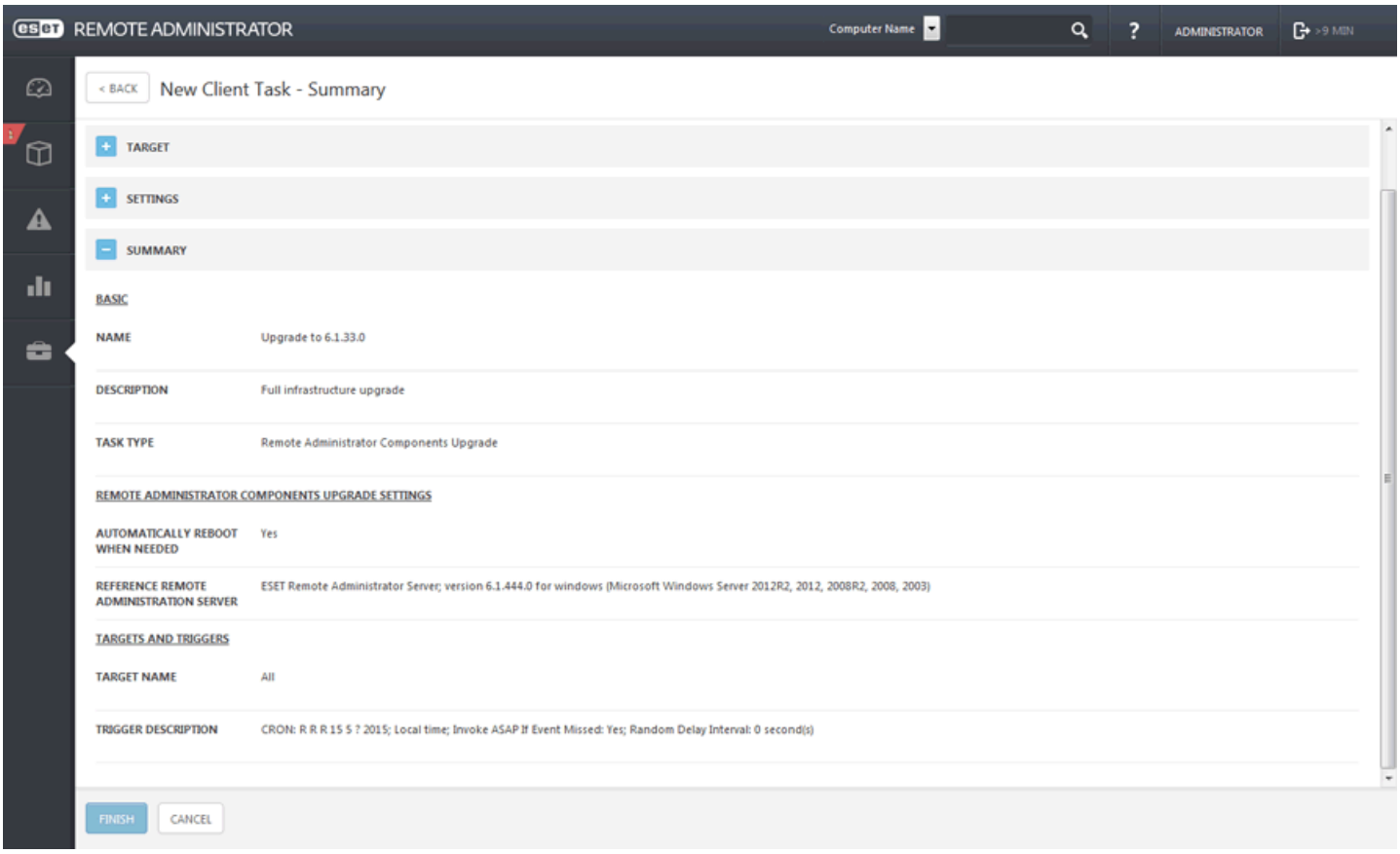


9. Cliquez sur **<Choisir un serveur>**, sélectionnez un produit (ESET Remote Administrator Server version 6.1.444.0 pour Windows ou version 6.1.530.0 pour Linux), puis cliquez sur **OK**.



Résumé

10. Passez en revue le résumé des paramètres configurés, puis cliquez sur **Terminer**. La tâche est créée et sera envoyée aux clients.



Dépannage :

- Vérifiez que vous pouvez accéder au référentiel ESET de l'ordinateur mis à niveau (vérifiez si vous pouvez télécharger *http://repository.eset.com/v1/info.meta*).
- Une nouvelle exécution de la tâche Mettre à jour les composants d'ESET Remote Administrator ne fonctionnera pas si un composant a déjà été mis à niveau vers une nouvelle version.
- S'il n'existe pas de motif clair pour expliquer l'échec, effectuez une mise à niveau manuelle des composants.

Sur les ordinateurs Linux qui utilisent systemd en tant que gestionnaire de service, cette tâche peut ne pas se terminer correctement. Les autres distributions Linux avec les scripts init SysV ou upstart ne sont pas affectées.

Distribuez et exécutez le script ci-après sur tous les ordinateurs exécutant ERA Agent sur Linux avec systemd avant d'appliquer la tâche Mettre à jour les composants d'ESET Remote Administrator.

Exécuter le script en tant que racine :

```
#!/bin/sh -e
systemd_service=eraagent.service
systemd_service_path="/etc/systemd/system/$systemd_service"
if ! grep "^KillMode=" "$systemd_service_path" > /dev/null
then
echo "Applying 'KillMode' change to '$systemd_service_path'"
sed -i 's/\[Service\]/[Service]\nKillMode=process/' "$systemd_service_path"
else
echo "'KillMode' already set. No changes applied."
exit 0
fi
systemctl daemon-reload
if systemctl is□active $systemd_service > /dev/null
then
echo "Restarting instance of '$systemd_service'"
systemctl restart $systemd_service
fi
```

5.2 scénario 2

Effectuer une installation basée sur les composants des produits d'entreprise ESET version 6 et les déployer depuis ESET Remote Administrator.

REMARQUE : ESET Endpoint Security prend en charge une installation basée sur les composants, contrairement à ESET Endpoint Antivirus. Vous pouvez sélectionner les composants à installer à l'aide de la propriété ADDLOCAL. Vous pouvez procéder de deux manières différentes dans ESET Remote Administrator :

1. **À l'aide des tâches Installer un logiciel** : sélectionnez un package du référentiel ou ajoutez le chemin d'accès au `fichier` msi :

   Par exemple :
   fichier://\\Win2012-server\share\ees_nt64_enu.msi (il est nécessaire de définir des autorisations correctes - pas d'authentification)

   ajouter ADDLOCAL=<list> aux PARAMÈTRES D'INSTALLATION

   ADDLOCAL = Internet et messagerie, Filtrage des protocoles, Protection de l'accès Web, Protection du client de messagerie, Antispam, Filtrage Internet, Miroir de mise à jour, Protection des documents, Contrôle de périphérique
   (tous les composants sans NAP ni pare-feu)

2. **À l'aide des tâches Exécuter une commande**

   Par exemple :
   ```
   msiexec.exe /i \\Win2012-server\share\ees_nt64_enu.msi /qn
   ADDLOCAL=WebAndEmail,ProtocolFiltering,WebAccessProtection,EmailClientProtection,Antispam,WebControl,
   C:/install.log
   ```

6. Premières étapes

Une fois ESET Remote Administrator correctement installé, vous pouvez passer à l'étape de configuration.

Tout d'abord, ouvrez la console Web ERA dans votre navigateur Web et connectez-vous.

Découverte de la console Web ERA

Avant de commencer la configuration initiale, il est recommandé de découvrir la console Web ERA, car il s'agit de l'interface à utiliser pour gérer les solutions de sécurité ESET.

Nos tâches de post-installation vous guident tout au long des étapes recommandées pour faciliter l'exécution de la configuration.

Création d'un compte d'utilisateur

Au moment de l'installation, vous avez créé le compte d'administrateur par défaut. Il est recommandé d'enregistrer le compte Administrateur et de créer un compte pour gérer les clients et configurer leurs autorisations.

Ajout des ordinateurs clients, des serveurs et des périphériques mobiles du réseau à ERA

Au cours de l'installation, vous pouvez choisir de rechercher les ordinateurs (clients) sur votre réseau. Tous les clients détectés sont répertoriés dans la section Ordinateurs lorsque vous démarrez ESET Remote Administrator. Si les clients ne sont pas affichés dans la section Ordinateurs, exécutez une tâche Synchronisation des groupes statiques pour rechercher les ordinateurs et les afficher dans des groupes.

Déploiement de l'Agent

Une fois les ordinateurs détectés, déployez l'Agent sur ceux-ci. L'Agent permet les communications entre ESET Remote Administrator et les clients.

Installation d'un produit ESET (activation comprise)

Pour protéger les clients et le réseau, utilisez la tâche Installer un logiciel pour installer les produits ESET.

Création/modification de groupes

Il est recommandé de trier les clients en groupes statiques ou dynamiques selon divers critères. Vous pouvez ainsi gérer plus facilement les clients et avoir une vue d'ensemble du réseau.

Création d'une stratégie

Les stratégies vous permettent de transmettre des configurations spécifiques aux produits ESET s'exécutant sur les ordinateurs clients. Vous pouvez ainsi appliquer la configuration sans avoir à configurer manuellement le produit ESET de chaque client. Une fois que vous avez créé une stratégie avec une configuration personnalisée, vous pouvez l'attribuer à un groupe (statique ou dynamique) en vue d'appliquer vos paramètres personnalisés à tous les ordinateurs de ce groupe.

Attribution d'une stratégie à un groupe

Comme précédemment expliqué, une stratégie doit être attribuée à un groupe pour être appliquée. Les ordinateurs appartenant au groupe se verront appliquer la stratégie. La stratégie est appliquée à chaque connexion d'un Agent à ERA Server.

Configuration de notifications et création de rapports

Pour une meilleure vue d'ensemble de l'état des ordinateurs clients dans votre environnement, il est recommandé d'utiliser des notifications et des rapports. Par exemple, si vous souhaitez être averti d'un événement qui s'est produit ou afficher ou télécharger un rapport.

6.1 Ouverture d'ERA Web Console

Il existe plusieurs méthodes pour ouvrir ERA Web Console :

- Sur le serveur local (l'ordinateur hébergeant la console Web), saisissez cette URL dans le navigateur Web : *https://localhost/era/*

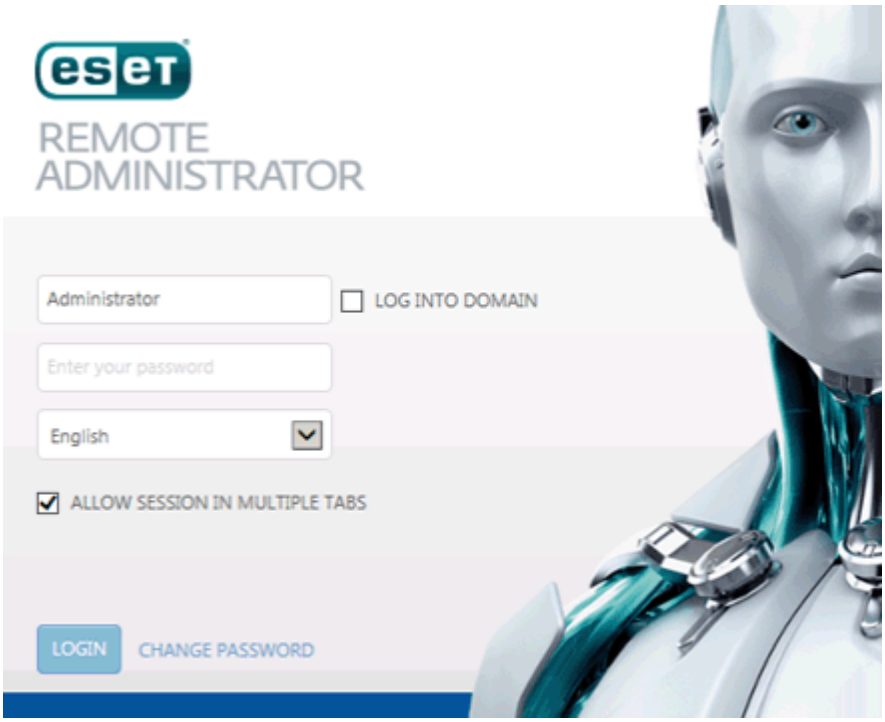
- À partir de n'importe quel emplacement ayant un accès Internet au serveur Web, saisissez l'URL dans le format suivant :
  https://yourservername/era/
  Remplacez « nomvotreserveur » par le nom ou l'adresse IP du serveur Web.

- Pour vous connecter à l'appliance virtuelle ERA, utilisez l'URL suivante :
  https://[IP address]:8443/
  Remplacez [adresse IP] par celle de votre machine virtuelle ERA. Si vous ne vous souvenez pas de l'adresse IP, reportez-vous à l'étape 9 des instructions pour le déploiement de l'appliance virtuelle.

- Sur le serveur local (l'ordinateur hébergeant la console Web), cliquez sur Démarrer > **Tous les programmes** > **ESET** > **ESET Remote Administrator** > **ESET Remote Administrator Webconsole**. Un écran de connexion s'affiche dans votre navigateur Web par défaut. Cela ne s'applique pas à l'appliance virtuelle ERA.

REMARQUE : comme la console Web utilise un protocole sécurisé (HTTPS), un message relatif à un certificat de sécurité ou à une connexion non approuvée peut s'afficher dans le navigateur Web (les termes exacts du message dépendent du navigateur utilisé). Ce message s'affiche, car le navigateur demande la vérification de l'identité du site auquel vous accédez. Cliquez sur **Poursuivre sur ce site Web** (Internet Explorer) ou **Je comprends les risques**, sur **Ajouter une exception...**, puis sur **Confirmer l'exception de sécurité** (Firefox) pour accéder à ERA Web Console. Cela s'applique uniquement lorsque vous accédez à l'URL de la console Web ESET Remote Administrator.

Lorsque le serveur Web (qui exécute la console Web ERA) est fonctionnel, l'écran suivant s'affiche.



S'il s'agit de votre première connexion, indiquez les informations d'identification saisies lors du processus d'installation. Pour plus d'informations sur cet écran, reportez-vous à la section Écran de connexion à la console Web.

REMARQUE : si l'écran de connexion ne s'affiche pas ou s'il semble se charger sans cesse, redémarrez le service *ESET Remote Administrator Server*. Une fois le service *ESET Remote Administrator Server* fonctionnel et en cours d'exécution, redémarrez le service *Apache Tomcat*. Une fois cette opération terminée, l'écran de connexion de la console Web se charge correctement.

7. Outil de diagnostic

L'outil de diagnostic fait partie de tous les composants ERA. Il sert à collecter et à compresser les journaux qui sont utilisés par les développeurs pour résoudre les problèmes liés aux composants du produit. Exécutez l'outil de diagnostic, sélectionnez un dossier racine où enregistrer les journaux, puis choisissez les actions à exécuter (voir la section **Actions** ci-dessous).

Emplacement de l'**outil de diagnostic** :

Windows

Dossier *C:\Program Files\ESET\RemoteAdministrator\<product>* , fichier appelé **Diagnostic.exe**.

Linux

Chemin d'accès sur le serveur : */opt/eset/RemoteAdministrator/<product>/*, exécutable **Diagnostic<produit>** (en un seul mot, par exemple **DiagnosticServer**, **DiagnosticAgent**)

Actions

- **Journaux de vidage** : un dossier de journaux est créé où tous les journaux sont enregistrés.
- **Processus de vidage** : un dossier est créé. Un fichier d'image mémoire de processus est généralement créé en cas de détection de problème. Lorsqu'un problème grave est détecté, un fichier d'image mémoire est créé par le système. Pour le vérifier manuellement, accédez au dossier %temp% (sous Windows) ou au dossier /tmp/ (sous Linux) et insérez un fichier dmp.

REMARQUE : le service (Agent, Proxy, Server, RD Sensor, FileServer) doit être en cours d'exécution.

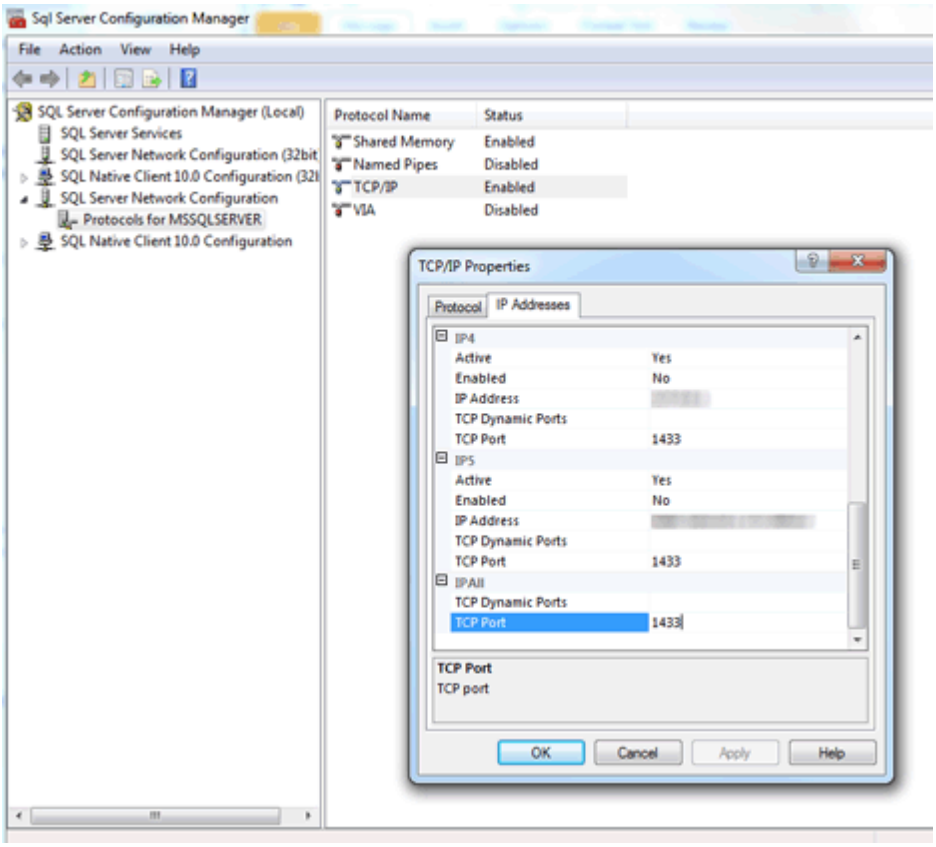
- **Informations générales sur l'application** : le dossier GeneralApplicationInformation est créé avec le fichier GeneralApplicationInformation.txt. Ce fichier contient des informations textuelles comprenant le nom et la version du produit actuellement installé.
- **Configuration des actions** : un dossier de configuration est créé dans lequel le fichier storage.lua est enregistré.

8. FAQ

Q : Pourquoi Java est-il installé sur un serveur ? Cette installation ne présente-t-elle pas un risque de sécurité ?
R : ERA Web Console requiert Java pour fonctionner. Java est une norme du secteur pour les consoles Web. Bien qu'ERA Web Console requière Java version 7 au minimum, il est vivement recommandé d'utiliser la dernière version officielle de Java.

Q : Le message d'erreur suivant est sans cesse consigné dans le journal trace.log d'ESET Rogue Detector : *2015-02-25 18:55:04 Information: CPCAPDeviceSniffer [Thread 764]: CPCAPDeviceSniffer on rpcap://\Device\NPF_{2BDB8A61-FFDA-42FC-A883-CDAF6D129C6B} throwed error: Device open failed with error:Error opening adapter: The system cannot find the device specified. (20)*
R : Ce message indique un problème lié à WinPcap. Arrêtez le service ESET Rogue Detector Sensor, réinstallez la dernière version de WinPcap (version 4.1.0 ou ultérieure) et redémarrez le service ESET Rogue Detector Sensor.

Q : Comment puis-je déterminer le port utilisé par SQL Server ?
R : Plusieurs méthodes vous permettent de déterminer le port utilisé par SQL Server. Le Gestionnaire de configuration SQL Server offre les résultats les plus précis. Pour savoir où rechercher cette information dans le Gestionnaire de configuration SQL Server, reportez-vous à la figure suivante :



Q : Après l'installation de SQL Serveur Express 2008 (compris dans le module ERA) sur Windows Server 2012, SQL Serveur Express 2008 ne semble pas effectuer d'écoute sur un port standard.
R : SQL Serveur Express 2008 effectue probablement l'écoute sur un port autre que le port par défaut (1433).

Q : Comment configurer MySQL pour accepter des paquets de grande taille ?
R : Recherchez le fichier de configuration MySQL (**my.ini** pour Windows et **my.cnf** pour Linux ; l'emplacement exact du fichier .ini peut être différent selon le système d'exploitation), ouvrez-le et recherchez la section `[mysqld]`. Ajouter la nouvelle ligne `max_allowed_packet=33M` (la valeur doit être égale ou supérieure à 33M).

Q : Si j'effectue l'installation de SQL Server, comment dois-je créer une base de données pour ERA ?
R : Il n'est pas nécessaire de créer une base de données. Celle-ci est créée par le programme d'installation **Server.msi** , et non par le programme d'installation d'ERA. Le programme d'installation d'ERA est fourni pour vous simplifier la tâche. Il installe SQL Server, tandis que le programme d'installation server.msi crée la base de données.

Q : Si j'indique les détails et les informations d'identification de la connexion SQL Server, le programme d'installation d'ERA peut-il créer une base de données dans une installation SQL Server existante ? Ce serait pratique si le programme d'installation prenait en charge différentes versions de SQL Server (versions 2008, 2014, etc.)
R : La base de données est créée par **Server.msi**. Le programme d'installation crée donc effectivement une base de données ERA sur chaque instance SQL Server installée. De plus, les versions de SQL Server prises en charge sont effectivement les versions 2008, 2012 et 2014.

Q : Pourquoi la version SQL Server 2008 R2 est-elle utilisée dans le programme d'installation d'ERA ?
R : La version SQL Server 2008 R2 est utilisée, car Microsoft assure la compatibilité de ce type de base de données sur Windows XP et les versions antérieures.

Q : Que dois-je faire lorsque le **code d'erreur : -2068052081** s'affiche au cours de l'installation ?
R : Redémarrez l'ordinateur, puis réexécutez la configuration. Si le problème persiste, désinstallez SQL Server Native Client, puis réexécutez le programme d'installation. Si cela ne permet pas de résoudre le problème, désinstallez tous les produits Microsoft SQL Server, redémarrez l'ordinateur, puis réexécutez le programme d'installation.

Q : Que dois-je faire lorsque le **code d'erreur : -2067922943** s'affiche au cours de l'installation de MSSQL ?
R : Vérifiez que le système répond à la configuration requise de la base de données pour ERA.

Q : En cas d'installation sur une instance SQL Server existante, SQL Server doit-il utiliser le mode intégré **Authentification Windows**par défaut ?
R : Non, car le mode Authentification Windows peut être désactivé sur SQL Server. De plus, le seul moyen de se connecter consiste à utiliser l'authentification SQL Server (saisie d'un nom d'utilisateur et d'un mot de passe). Vous devez utiliser l'authentification SQL Server ou le mode mixte. Lors de l'installation manuelle de SQL Server, il est recommandé de créer un mot de passe racine pour SQL Server (l'utilisateur racine est appelé « sa », ce qui signifie security admin) et de le stocker à un endroit sûr en vue d'une utilisation ultérieure. Le mot de passe racine peut être nécessaire lors de la mise à niveau d'ERA Server.

Q : Je dois installer **Microsoft .NET Framework 3.5** comme le programme d'installation d'ERA me le signale (http://www.microsoft.com/en-us/download/details.aspx?id=21),, mais cette installation ne peut pas être effectuée sur une nouvelle installation de Windows Server 2012 R2 avec SP1.
R : Ce programme d'installation ne peut pas être utilisé avec Windows Server 2012 en raison de la stratégie de sécurité de cette application. Microsoft .NET Framework doit être installé par le biais de **l'Assistant Ajout de rôles et de fonctionnalités.**.

Q : Microsoft .NET Framework 4.5 était déjà installé sur mon système. J'ai du ajouter .NET Framework 3.5 par le biais de l'Assistant Ajout de rôles et de fonctionnalités. Pourquoi n'est-il pas possible d'utiliser .NET 4.5 avec ESET Remote Administrator ?
R : Cela n'est pas possible, car .NET Framework 4.5 n'est pas rétrocompatible avec .NET Framework 3.5 qui est une condition préalable requise du programme d'installation SQL Server.

Q : Il est très difficile de déterminer si l'installation de SQL Server est en cours d'exécution. Comment puis-je savoir ce qui se passe si l'installation dure plus de 10 minutes ?
R : Dans de rares cas, l'installation de SQL Server peut prendre jusqu'à une heure. La durée de l'installation dépend des performances système.

Q : Comment puis-je **réinitialiser le mot de passe de l'administrateur** pour la console Web (saisi pendant la configuration) ?
R : Il est possible de réinitialiser le mot de passe en exécutant le programme d'installation du serveur et en choisissant **Réparer**. Il est possible que vous ayez besoin du mot de passe de la base de données ERA si vous n'avez pas utilisé l'authentification Windows lors de la création de la base de données.

REMARQUE : vous devez faire attention, car certaines des opérations de réparation peuvent éventuellement entraîner la suppression des données stockées.

Q : Lorsque j'importe un fichier contenant la liste des ordinateurs à ajouter à ERA, quel format de fichier dois-je utiliser ?
R : Vous devez utiliser un fichier comportant les lignes suivantes :
Tous\Groupe1\GroupeN\Ordinateur1
Tous\Groupe1\GroupeM\OrdinateurX
Tous est le nom requis pour le groupe racine.

Q : Pouvez-vous utiliser IIS au lieu d'Apache ? Ou un autre serveur HTTP ?
R : IIS est un serveur HTTP. La console Web a besoin d'un conteneur de servlets Java (tel que Tomcat) pour fonctionner, le serveur HTTP ne suffit pas. Il existe des solutions pour transformer IIS en conteneur de servlets Java mais, en général, ce n'est pas conseillé : *http://stackoverflow.com/questions/2256084/running-a-java-web-application-in-iis*
REMARQUE : vous êtes Ne pas utiliser Apache HTTP Server ; nous utilisons Apache Tomcat, qui est un autre produit.

Q : ERA possède-t-il une interface de ligne de commande ?
R : Oui, nous avons le ServerAPI ESET Remote Administrator.

Q : Pouvez-vous installer ERA sur un contrôleur de domaine ?
L'application ERA Server peut être installée sur un contrôleur de domaine, mais il peut exister des restrictions à l'installation de MS SQL sur le Contrôleur de domaine Windows.

Q : Y'a-t-il moyen d'utiliser l'assistant pour l'installation sur un contrôleur de domaine ?
Vous pouvez utiliser l'assistant, mais vous devez désélectionner l'installation de SQL dans la fenêtre de sélection des composants.

Q : L'installation d'ERA Server va-t-elle détecter si SQL est déjà installé sur le système ? Que se passe-t-il alors ? Qu'en est-il de MySQL ?
ERA vérifiera si SQL est exécuté sur un système si vous utilisez un assistant d'installation et que vous avez sélectionné l'installation de SQL Express. Si SQL est exécuté sur un système, l'assistant affichera une notification pour désinstaller l'instance SQL existante et relancer l'installation, ou pour installer ERA sans SQL Express.
http://help.eset.com/era/6/en-US/index.html?database_requirements.htm

Q : Pourquoi exigez-vous l'installation de Java pour utiliser le serveur de gestion ? 99 % des fournisseurs de solutions de sécurité et des cadres de sécurité recommandent de désinstaller Java des ordinateurs, notamment des serveurs. Java est sans nul doute la source d'une multitude de vulnérabilités et d'exploits.
Java est nécessaire pour la prise en charge d'un serveur Web multi-plateformes. C'est aussi une norme du secteur : les principales consoles Web utilisent Java et Web Server (Tomcat) pour leurs opérations (McAfee, Symantec …). Il est possible d'installer un serveur Web sur une machine dédiée s'il existe des risques de sécurité.

Q : Mappage des composants ERA selon la version d'ERA
Voir l'article de la base de connaissances http://kb.eset.com/esetkb/index?page=content&id=SOLN3690

Q : Comment effectuer une mise à jour basée sur les composants de ESET Remote Administrator 6.1.21 vers la version 6.1.28 ?
R : Système d'exploitation Windows : http://kb.eset.com/esetkb/index?page=content&id=SOLN3669 ou http://kb.eset.com/esetkb/index?page=content&id=SOLN3668
Système d'exploitation Linux : http://kb.eset.com/esetkb/index?page=content&id=SOLN3670

Q : Comment effectuer la mise à jour d'un système sans connexion Internet ?
R : En utilisant un proxy HTTP installé sur un ordinateur pouvant se connecter aux serveurs de mise à jour ESET (où les fichiers de mise à jour sont en mémoire cache), et en pointant les points de terminaison vers ce proxy HTTP sur un réseau local. Si votre serveur ne dispose pas d'une connexion Internet, vous pouvez activer la fonction de miroir du produit Endpoint sur un ordinateur, utiliser une clé USB pour transférer le fichier des mises à jour sur cet ordinateur, puis configurer tous les autres ordinateurs hors connexion pour qu'ils l'utilisent comme serveur de mise à jour.

Q : Comment réinstaller ERA Server et le connecter à un serveur SQL existant si le serveur SQL a été configuré automatiquement par l'installation initiale d'ERA ?
R : Si vous installez la nouvelle instance d'ERA Server à l'aide du même compte d'utilisateur (par exemple, un compte d'administrateur de domaine) que celui utilisé pour l'installation du serveur ERA initial, vous pouvez utiliser **MS SQL Server via l'authentification Windows**.

Q : L'installation d'ERA Server échoue sur CentOS 7, que faire ?
R : Si l'erreur « Erreur : DbCheckConnection: locale::facet::_S_create_c_locale name not valid » s'affiche, le problème provient sans doute des paramètres régionaux/de l'environnement. L'exécution de la commande « export LC_ALL="en_US.UTF-8" » avant le script du programme d'installation du serveur devrait résoudre le problème.

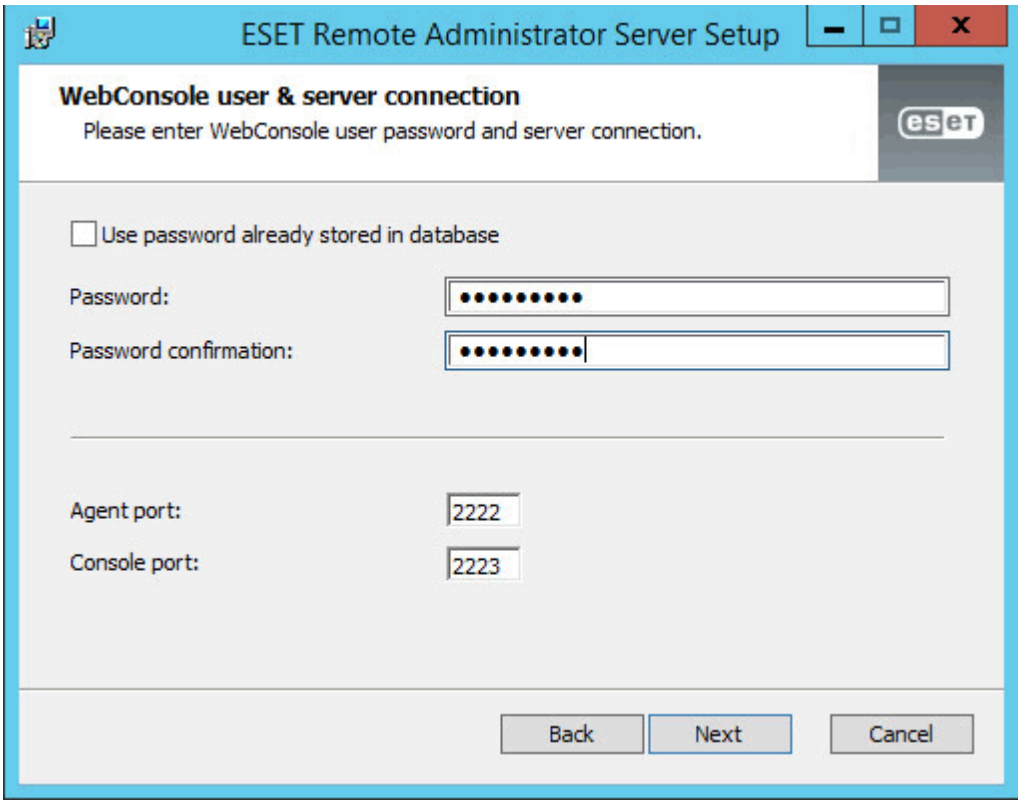
Q : Comment régler les problèmes de synchronisation d'Active Directory sur Linux ?
R : Vérifiez que votre nom de domaine est bien en majuscules « **VER MAJ** » (administrateur@TEST.LOCAL et non administrateur@test.local). Vous pouvez modifier ce paramètre à l'aide du programme d'installation tout en un d'ESET Remote Administrator en sélectionnant le paramètre Réparer.

Q : Existe-t-il un moyen d'utiliser mes propres ressources réseau (comme le partage SMB) au lieu du référentiel ?
R : Vous pouvez choisir de fournir l'URL directe de l'emplacement du package. Si vous utilisez un système de partage de fichier, utilisez le format suivant : fichier:// suivi du chemin d'accès réseau complet vers le fichier, par exemple fichier://\\eraserver\install\ees_nt64_ENU.msi

Mot de passe oublié : dans l'idéal, le compte administrateur ne doit être utilisé que pour créer des comptes pour des administrateurs. Une fois les comptes administrateur créés, le mot de passe de l'administrateur doit être enregistré et le compte administrateur ne doit pas être utilisé. Cette pratique permet d'utiliser le compte administrateur pour réinitialiser les mots de passe/informations de compte des administrateurs en cas de besoin.

Procédure pour **réinitialiser le mot de passe** d'un compte d'administrateur ERA intégré :

1. Ouvrez **Programmes et fonctionnalités** (exécutez appwiz.cpl), recherchez ESET Remote Administrator Server, puis cliquez avec le bouton droit dessus.
2. Sélectionnez **Modifier** dans le menu contextuel.
3. Choisissez **Réparer**.
4. Indiquez les informations de connexion à la base de données.
5. Sélectionnez **Utiliser la base de données existante et appliquez une mise à niveau**.
6. Veillez à désélectionner l'option **Utiliser le mot de passe stocké dans la base de données** et saisissez un nouveau mot de passe.
7. Vous pouvez à présent vous connecter à la console Web ERA avec votre nouveau mot de passe.



REMARQUE : il est vivement conseillé de créer d'autres comptes avec des droits d'accès spécifiques basés sur les compétences souhaitées.

Q : Comment modifier les ports d'ERA Server et de la console Web ERA ?
R : Il convient de modifier le port dans la configuration de votre serveur Web pour permettre à ce dernier de se connecter au nouveau port.
Pour ce faire, procédez comme suit :

1. Arrêtez le serveur Web
2. Modifiez le port dans la configuration de votre serveur Web
   a. Ouvrez le fichier *webapps/era/WEB-INF/classes/sk/eset/era/g2webconsole/server/modules/config/EraWebServerConfig.properties*
   b. Définissez le numéro du nouveau port, par exemple server_port=44591
3. Redémarrez le serveur Web

Q : Comment migrer ERA Server sur un nouveau système ?
R : Installez une nouvelle instance d'ERA Server sur le nouveau système et connectez-la à votre ancienne base de données. Pour plus d'informations sur l'utilisation de l'outil de migration, voir http://help.eset.com/test/era/6/en-US/migration_tool.htm et http://kb.eset.com/esetkb/index?page=content&id=SOLN3607

Q : Puis-je passer d'ERA V5/V4 à la version V6 directement à l'aide du programme d'installation tout en un ?
R : La mise à niveau directe n'est pas prise en charge, l'utilisateur doit employer l'outil de migration conformément aux instructions décrites ici : http://help.eset.com/era/6/en-US/index.html?migration_tool.htm