AUTHORIZED DOCUMENTATION

Guide d'installation

January 5, 2009

Novell®
ZENworks® Endpoint Security Management

3.5

www.novell.com

Mentions légales

Novell, Inc. n'accorde aucune garantie, explicite ou implicite, quant au contenu et à l'utilisation de cette documentation, y compris toute garantie de bonne qualité marchande ou d'aptitude à un usage particulier. Novell se réserve en outre le droit de réviser cette publication à tout moment et sans préavis de ces modifications à quiconque.

Par ailleurs, Novell exclut toute garantie relative à tout logiciel, notamment toute garantie, expresse ou implicite, que le logiciel présenterait des qualités spécifiques ou qu'il conviendrait à un usage particulier. Novell se réserve en outre le droit de modifier à tout moment tout ou partie des logiciels Novell, sans préavis de ces modifications à quiconque.

Tous les produits ou informations techniques fournis dans le cadre de ce contrat peuvent être soumis à des contrôles d'exportation aux États-Unis et à la législation commerciale d'autres pays. Vous vous engagez à respecter toutes les réglementations de contrôle des exportations et à vous procurer les licences et classifications nécessaires pour exporter, réexporter ou importer des produits livrables. Vous acceptez de ne pas procéder à des exportations ou à des réexportations vers des entités figurant sur les listes noires d'exportation en vigueur aux États-Unis ou vers des pays terroristes ou soumis à un embargo par la législation américaine en matière d'exportations. Vous acceptez de ne pas utiliser les produits livrables pour le développement prohibé d'armes nucléaires, de missiles ou chimiques et biologiques. Reportez-vous à la page Web des services de commerce international de Novell (http://www.novell.com/info/exports/) pour plus d'informations sur l'exportation des logiciels Novell. Novell décline toute responsabilité dans le cas où vous n'obtiendriez pas les autorisations d'exportation nécessaires.

Novell, Inc. dispose de droits de propriété intellectuelle sur la technologie intégrée dans le produit décrit dans ce document. En particulier et sans limitation, ces droits de propriété intellectuelle peuvent inclure un ou plusieurs brevets américains mentionnés sur le site Web Novell relatif aux mentions légales (http://www.novell.com/company/legal/patents/) (en anglais) et un ou plusieurs brevets supplémentaires ou en cours d'homologation aux États-Unis et dans d'autres pays.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
États-Unis
www.novell.com

Documentation en ligne : pour accéder à la documentation en ligne la plus récente de ce produit et des autres produits Novell ou pour obtenir des mises à jour, reportez-vous au site Novell de documentation (http://www.novell.com/documentation).

Marques de Novell

Pour connaître les marques commerciales de Novell, reportez-vous à la liste des marques commerciales et des marques de service de Novell (http://www.novell.com/company/legal/trademarks/tmlist.html).

Éléments tiers

Toutes les marques commerciales de fabricants tiers appartiennent à leur propriétaire respectif.

Tables des matières

À propos de ce guide

Ce *guide d'installation de Novell® ZENworks® Endpoint Security Management* fournit des instructions complètes pour l'installation des composants ZENworks Endpoint Security Management et aide les administrateurs à les garder opérationnels.

Il est organisé de la manière suivante :

Public

Ce guide est destiné aux administrateurs de ZENworks Endpoint Security Management.

Commentaires

Nous souhaiterions connaître vos commentaires et suggestions sur ce guide et les autres documentations fournies avec ce produit. Utilisez la fonction Commentaires au bas de chaque page de la documentation en ligne ou accédez au site Novell de commentaires sur la documentation (http://www.novell.com/documentation/feedback.html) pour entrer vos commentaires.

Documentation complémentaire

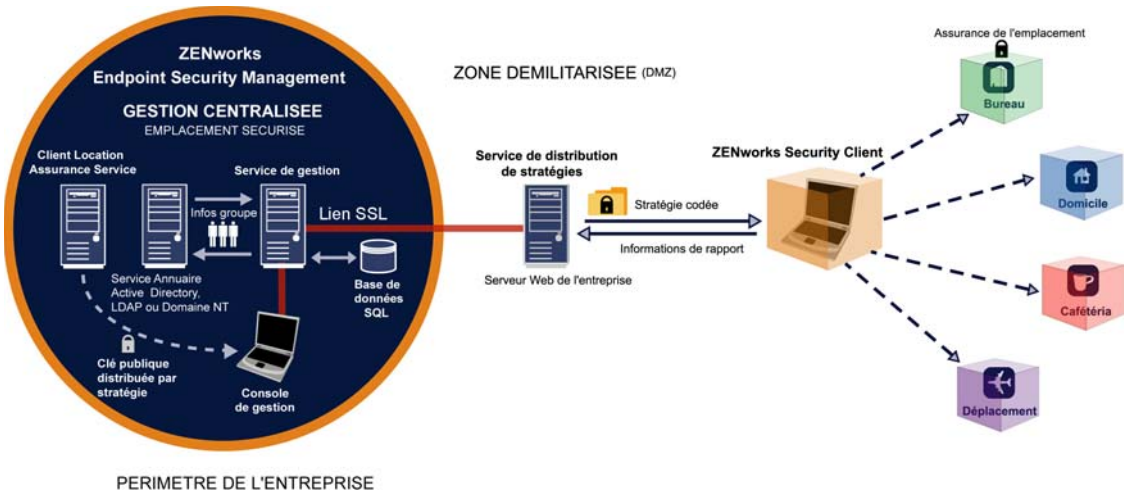
D'autres manuels (aux formats PDF et HTML) viennent compléter la documentation relative à ZENworks Endpoint Security Management. Ils facilitent l'apprentissage et la mise en oeuvre de ce produit : Pour d'autres documents, reportez-vous au site Web de documentation de ZENworks Endpoint Security Management 3.5 (http://www.novell.com/documentation/zesm35).

ZENworks Endpoint Security Management Présentation

1

Novell® ZENworks® Endpoint Security Management comprend cinq composants fonctionnels de haut niveau : un service de distribution de stratégies (Policy Distribution Service), un service de gestion (Management Service), une console de gestion (Management Console), un service d'assurance de l'emplacement des clients (Client Location Assurance Service) et le client Endpoint Security Client. La figure ci-dessous illustre ces composants dans l'architecture :

Figure 1-1 *Architecture de ZENworks Endpoint Security Management*



Endpoint Security Client est responsable de l'application des stratégies de sécurité distribuées au niveau du système de noeuds d'extrémité. Lorsque Endpoint Security Client est installé sur tous les PC de l'entreprise, ces noeuds d'extrémité peuvent sortir du périmètre de la société tout en conservant leur niveau de sécurité ; les noeuds d'extrémité à l'intérieur du périmètre sont, quant à eux, soumis à des contrôles de sécurité supplémentaires au sein du pare-feu du périmètre.

Chaque composant de gestion centralisée est installé séparément (à l'exception d'une installation monoserveur.) Reportez-vous à la rubrique Chapitre 3, « Installation monoserveur », page 17 pour plus d'informations.

Les composants suivants sont installés sur des serveurs sécurisés dans le périmètre de l'entreprise :

- **Service de distribution de stratégies:** chargé de la distribution des stratégies de sécurité auprès de Endpoint Security Client et de la récupération des données de rapport auprès de Endpoint Security Client. Ce service peut être déployé dans la zone démilitarisée (Demilitarized Zone - DMZ), à l'extérieur du pare-feu de l'entreprise, afin de garantir la mise à jour régulière des stratégies pour les noeuds d'extrémité mobiles.
- **Service de gestion:** chargé de l'assignation des stratégies utilisateur et de l'authentification des composants, de la récupération des données de rapport, de la création et de la diffusion de rapports ZENworks Endpoint Security Management, ainsi que de la création et du stockage des stratégies de sécurité.

- **Console de gestion:** interface utilisateur visible qui peut être exécutée directement sur le serveur qui héberge le service de gestion ou sur un poste de travail résidant à l'intérieur du pare-feu de l'entreprise et connecté au serveur du service de gestion. Elle est utilisée pour configurer le service de gestion et pour créer et gérer les stratégies de sécurité pour les utilisateurs et les groupes. Elle permet de créer, de copier, d'éditer, de diffuser et de supprimer des stratégies
- **Service CLAS:** fournit une garantie cryptographique que les périphériques sur lesquels Endpoint Security Client est installé se trouvent bel et bien à un emplacement défini, comme l'indiquent d'autres paramètres d'environnement réseau existants.

1.1 Configuration système requise

Configuration requise pour le système serveur	Configuration système requise pour le noeud d'extrémité (client)
Systèmes d'exploitation :	**Systèmes d'exploitation :**
Microsoft&thrdmrk; Windows&thrdmrk; 2000 Server SP4 Microsoft Windows 2000 Advanced Server SP4 Windows 2003 Server	Windows XP SP1 Windows XP SP2 Windows 2000 SP4 Windows Vista SP1 (32 bits) Windows Server 2008 (32 bits)
Processeur :	**Processeur :**
Pentium&thrdmrk; 4 HT 3 GHz (ou plus rapide) RAM de 756 Mo minimum (1 Go+ recommandé)	Pentium 3, 600 MHz (ou plus rapide) RAM de 128 Mo minimum (256 Mo ou plus recommandé)
Espace disque :	**Espace disque :**
500 Mo : sans la base de données Microsoft SQL locale 5 Go : avec la base de données MS SQL locale (SCSI recommandé)	5 Mo requis, 5 Mo supplémentaires recommandés pour les données de rapport
Configuration logicielle requise :	**Configuration logicielle requise :**
RDBMS pris en charge (SQL Server Standard, SQL Server Enterprise, Microsoft SQL Server 2000 SP4 ou SQL 2005) Microsoft Internet Information Services (configuré pour SSL) Services Annuaire pris en charge (eDirectory™ ou Active Directory&thrdmrk;) .NET Framework 3.5 (pour serveurs et console de gestion uniquement)	Windows 3.1 Installer Toutes les mises à jour Windows doivent être installées
Console de gestion en mode autonome :	
RDBMS pris en charge (SQL Server Standard, SQL Server Enterprise, Microsoft SQL Server 2000 SP4, SQL 2005, SQL Express).	

Les services de gestion, de distribution de stratégies et CLAS exigent l'activation d'un compte local de ASP.NET 2.0. Si ce dernier est désactivé, les services ne fonctionnent pas correctement.

1.2 À propos des manuels ZENworks Endpoint Security Management

Les manuels de ZENworks Endpoint Security Management offrent trois niveaux d'orientation pour les utilisateurs du produit.

- *Guide d'installation de ESM :* ce guide fournit des instructions complètes pour l'installation des composants ZENworks Endpoint Security Management et aide les administrateurs à les garder opérationnels. Il s'agit du guide que vous êtes en train de lire.
- *Guide d'administration de ZENworks Endpoint Security Management* : ce guide est destiné aux administrateurs de ZENworks Endpoint Security Management amenés à gérer les services, à créer des stratégies de sécurité pour l'entreprise, à générer et à analyser des données de rapport et à assister les utilisateurs en cas de problème. Ce manuel fournit des instructions pour mener à bien ces différentes tâches.
- *Guide de l'utilisateur de ZENworks Endpoint Security Client 3.5* : ce guide explique à l'utilisateur le fonctionnement de Endpoint Security Client. Il peut être envoyé à tous les employés de l'entreprise pour leur apprendre à utiliser Endpoint Security Client.

Installation de ZENworks Endpoint Security Management

2

Les sections suivantes contiennent des informations supplémentaires concernant l'installation de Novell® ZENworks® Endpoint Security Management :

2.1 Informations de préinstallation

Le logiciel d'installation ZENworks Endpoint Security Management doit être protégé physiquement pour empêcher toute falsification ou toute utilisation non autorisée. De même, les administrateurs doivent examiner les directives de préinstallation et d'installation pour garantir que le système ZENworks Endpoint Security Management peut fonctionner sans interruption et éliminer toute vulnérabilité liée à une protection matérielle inadéquate.

L'administrateur qui installe ce logiciel DOIT être l'administrateur principal des serveurs et du domaine. Si vous utilisez des certificats SSL d'entreprise, vous devez également employer le même nom d'utilisateur pour créer le certificat de sécurité racine SSL.

2.2 Paquetages d'installation

Lorsque vous installez le logiciel à partir du DVD, un programme d'installation principal se lance ; celui-ci utilise une interface utilisateur simple pour guider l'administrateur ZENworks Endpoint Security Management pendant la procédure d'installation. Chargez le DVD d'installation dans chaque machine pour accéder au programme d'installation principal et installer les composants requis.

2.2.1 À propos du programme d'installation principal

Au démarrage, le programme d'installation principal affiche deux options de menu :*Produits* et *Documentation*.

Le lien *Produits* ouvre le menu d'installation. Les options de menu de cet écran lancent le programme d'installation correspondant à chaque composant. Dans le cas de Endpoint Security Client 3.5 ou Endpoint Security Client 4.0, une option supplémentaire est disponible pour lancer l'installation en mode Administrateur ; ce mode permet à l'administrateur ZENworks Endpoint Security Management de créer un paquetage MSI pour faciliter la distribution (reportez-vous à la rubrique Chapitre 9.2, « Installation MSI », page 61).

Pour obtenir des informations sur le fonctionnement complet des composants de ZENworks Endpoint Security Management, reportez-vous au *Guide d'administration de ZENworks Endpoint Security Management*, disponible via le lien *Documentation*.

2.3 Options d'installation

Les composants principaux de ZENworks Endpoint Security Management peuvent être installés en mode monoserveur ou multiserveur. Les installations monoserveurs sont idéales pour les petits déploiements n'exigeant pas des mises à jour régulières des stratégies. Les installations multiserveurs sont utilisées pour les déploiements de grande envergure nécessitant des mises à jour régulières des stratégies. Consultez les services professionnels de Novell pour déterminer le type d'installation qui vous convient.

Endpoint Security Client peut fonctionner (si nécessaire) sans connexion au service de distribution de stratégies. De même, une console de gestion exécutée en mode autonome peut être installée à des fins d'évaluation. L'installation requise pour ce mode de fonctionnement non géré est décrite au Chapitre 11, « Installation de ZENworks Endpoint Security Management en mode non géré », page 77.

2.4 Ordre d'installation

ZENworks Endpoint Security Management doit être installé dans l'ordre suivant :

1. Installation monoserveur ou multiserveur
   - Service de distribution de stratégies
   - Service de gestion
2. Console de gestion
3. Service CLAS
4. Endpoint Security Client 3.5 ou Endpoint Security Client 4.0

2.5 Avant d'installer ZENworks Endpoint Security Management

L'administrateur ZENworks Endpoint Security Management doit prendre en compte quelques questions avant de commencer l'installation :

Comment les utilisateurs recevront-ils leurs stratégies de sécurité ZENworks Endpoint Security Management ?

Les options de distribution des stratégies dépendent du fait de savoir si les utilisateurs doivent pouvoir recevoir une mise à jour des stratégies où qu'ils se trouvent, y compris à l'extérieur du réseau central, ou s'ils doivent les recevoir uniquement lorsqu'ils se trouvent au sein d'un réseau sécurisé (ou qu'ils y sont connectés via VPN). Pour les entreprises qui prévoient de mettre fréquemment à jour leurs stratégies de sécurité ZENworks Endpoint Security Management, il est recommandé d'utiliser une installation multiserveur qui place le service de distribution de stratégies sur un serveur Web en dehors de la zone démilitarisée.

De quels types de déploiements de serveur disposez-vous ?

Si votre entreprise ne dispose que de quelques serveurs, une installation monoserveur peut être nécessaire. Si la disponibilité de serveurs n'est pas un problème, il convient alors de prendre en compte la taille de déploiement de votre client et le nombre d'utilisateurs opérant en dehors du pare-feu.

Quel est votre déploiement SQL Server disponible ?

ZENworks Endpoint Security Management crée trois bases de données SQL lors de l'installation. Si votre déploiement est de petite envergure, une seule base de données SQL ou une base de données côté serveur peut être installée sur les serveurs du service de gestion et du service de distribution de stratégies. Pour les déploiements de plus grande envergure, un serveur de base de données SQL distinct doit être utilisé pour recevoir les données des services de distribution de stratégies et de gestion. Seuls les types de RDBMS suivants sont autorisés :

- SQL Server Standard
- SQL Server Enterprise
- Microsoft SQL Server 2000 SP4

Dans le cas d'une instance nommée, les serveurs doivent être configurés comme suit :

Provider=sqloledb

Data Source=NomServeur\NomInstance (ce type de définition est obligatoire pour l'installation de ZENworks Endpoint Security Management)

Initial Catalog=NomBaseDeDonnées

User Id=NomUtilisateur

Password=MotdePasse

Définissez SQL en mode mixte.

Le nom d'utilisateur et le mot de passe utilisés lors de l'installation ne peuvent pas être ceux d'un utilisateur du domaine, mais ceux d'un utilisateur SQL disposant de droits SysAdmin.

Allez-vous utiliser des certificats existants pour établir la communication SSL ou des certificats Novell auto-signés ?

Pour les configurations de récupération après sinistre et de reprise, vous devez utiliser des certificats SSL provenant d'une autorité de certification d'entreprise ou autre (VeriSign, GeoTrust, Thawte, etc.) pour des déploiements complets de ESM. Si vous utilisez vos propres certificats, le certificat du service Web et l'autorité de certification racine seront créés sur la machine désignée par le service de distribution de stratégies, puis distribués vers les machines appropriées. Pour créer une autorité de certification d'entreprise, consultez la procédure détaillée de configuration d'une autorité de certification, disponible sur le site Web de Microsoft.

Pour des déploiements d'évaluation ou de petite envergure (inférieurs à 100 utilisateurs), ZENworks Endpoint Security Management possède des certificats auto-signés qui peuvent être utilisés. Des certificats SSL Novell sont installés sur les serveurs dans le cas d'une installation standard.

Comment allez-vous déployer vos clients Endpoint Security Client ?

Le logiciel Endpoint Security Client peut être déployé individuellement sur chaque noeud d'extrémité ou via une distribution de données du serveur (push) MSI. Des instructions sur la création d'un paquetage MSI sont fournies au Chapitre 9.2, « Installation MSI », page 61.

Voulez-vous des stratégies basées sur la machine ou sur les utilisateurs ?

Les stratégies peuvent être distribuées vers une seule machine, à laquelle chaque utilisateur qui se logue reçoit la même stratégie, ou peuvent être définies pour des utilisateurs ou des groupes spécifiques.

Chaque installation doit satisfaire à des exigences préalables. Il est recommandé de compléter la liste de contrôle des exigences préalables avant de lancer l'installation d'un composant. Veuillez prendre connaissance de ces listes aux pages suivantes :

- Chapitre 3, « Installation monoserveur », page 17
- Chapitre 5, « Installation du service de distribution de stratégies », page 23
- Chapitre 6, « Installation du service de gestion », page 31
- Chapitre 7, « Installation de la console de gestion », page 43
- Chapitre 8, « Installation du service CLAS (Client Location Assurance Service) », page 55
- Chapitre 9, « Installation de Endpoint Security Client 3.5 », page 59

Installation monoserveur

3

L'installation monoserveur (SSI) ZENworks Endpoint Security Management permet la coexistence du service de distribution de stratégies et du service de gestion sur le même serveur, ce qui n'est pas possible sans cette option d'installation. Pour des raisons de sécurité, le serveur doit être déployé à l'intérieur du pare-feu, nécessitant ainsi que les utilisateurs reçoivent les mises à jour des stratégies uniquement lorsqu'ils se trouvent au sein de l'infrastructure de l'entreprise ou qu'ils y sont connectés via un VPN.

Le déploiement de l'installation monoserveur sur un contrôleur de domaine primaire n'est pas pris en charge pour des raisons à la fois de sécurité et de fonctionnalité.

Remarque : Il est recommandé de configurer (durcir) le serveur SSI de manière à désactiver les applications, services, comptes et autres options qui ne sont pas nécessaires à la finalité prévue du serveur. La procédure à suivre pour ce faire varie selon les spécificités de l'environnement local et ne peut donc pas être décrite au préalable. Les administrateurs sont invités à consulter la section appropriée de la page Web de sécurité Microsoft Technet (http://www.microsoft.com/technet/security/default.mspx). D'autres recommandations concernant le contrôle d'accès sont fournies dans le *Guide d'administration de ZENworks Endpoint Security Management*.

Afin de limiter l'accès aux seules machines approuvées, le répertoire virtuel et IIS peuvent être configurés pour utiliser des listes de contrôle d'accès (ACL). Reportez-vous aux articles ci-dessous :

- Accorder et refuser l'accès aux ordinateurs (http://www.microsoft.com/technet/prodtechnol/windows2000serv/default.mspx)
- Restreindre l'accès au site par l'adresse IP ou le nom de domaine (http://support.microsoft.com/default.aspx?scid=kb%3BEN-US%3BQ324066)
- FAQ IIS : restrictions de l'adresse IP 2000 et du nom de domaine (http://www.iisfaq.com/default.aspx?View=A136&P=109)
- Utilisation du filtrage de paquets IIS (http://www.15seconds.com/issue/011227.htm)

Pour des raisons de sécurité, il est vivement recommandé de supprimer les dossiers par défaut suivants de toute installation IIS :

- `IISHelp`
- `IISAdmin`
- `Scripts`
- `Printers`

Nous vous recommandons également d'utiliser IIS Lockdown Tool 2.1, disponible sur microsoft.com (http://www.microsoft.com/technet/security/tools/locktool.mspx).

La version 2.1 de cet outil repose sur des modèles fournis pour les principaux produits Microsoft basés dépendant de IIS. Sélectionnez le modèle qui correspond le mieux au rôle de ce serveur. En cas de doute, le modèle de serveur Dynamic Web est recommandé.

Assurez-vous que les exigences suivantes sont satisfaites avant de commencer l'installation :

- ❑ Assurez l'accès à un service Annuaire pris en charge (eDirectory, Active Directory ou NT Domains). NT Domains est uniquement pris en charge lorsque Singer Server Service est installé sur un serveur Microsoft Windows 2000 Advanced Server (SP4).
- ❑ Si vous effectuez le déploiement à l'aide d'un service eDirectory, assurez-vous que Novell Client™ est installé sur le serveur et peut s'authentifier correctement auprès de eDirectory. Créez un mot de passe de compte qui ne changera jamais pour l'authentification à la console de gestion (reportez-vous à la Section 7.2.1, « Ajout de services eDirectory », page 47).
- ❑ Pour la résolution de nom de serveur entre Endpoint Security Client et le monoserveur, vérifiez que les ordinateurs cibles (où est installé Endpoint Security Client) peuvent exécuter une commande ping sur le nom de serveur SSI. En cas d'échec, vous devez résoudre ce problème avant de poursuivre l'installation. (Changez le nom de serveur SSI en nom de domaine complet/NETBIOS, changez AD pour utiliser le nom de domaine complet/NETBIOS, changez les configurations DNS en modifiant le fichier hôte local sur les ordinateurs cibles de manière à inclure les informations correctes du service de gestion, etc.)
- ❑ Activez ou installez Microsoft Internet Information Services (IIS) et configurez-les de manière à accepter les certificats SSL (Secure Socket Layer).

  Important : Ne cochez pas la case *Requérir un canal sécurisé (SSL)* sur la page Communications sécurisées (dans l'utilitaire Microsoft Gestion de l'ordinateur, développez *Services et applications* > *Gestionnaire des services ISS* > *Sites Web* > cliquez avec le bouton droit de la souris sur *Site Web par défaut* > cliquez sur *Propriétés* > cliquez sur l'onglet *Sécurité de répertoire* > cliquez sur le bouton *Éditer* dans la zone de groupe Communications sécurisées). L'activation de cette option interrompt la communication entre le serveur ZENworks Endpoint Security Management et le client ZENworks Endpoint Security sur le noeud d'extrémité.

- ❑ Si vous utilisez vos propres certificats SSL, assurez-vous que le certificat de service Web et l'autorité de certification racine sont chargés sur la machine et que le nom de serveur validé aux étapes précédentes (NETBIOS ou nom de domaine complet) correspond à la valeur *Délivré à* du certificat configuré dans IIS.
- ❑ Si vous utilisez vos propres certificats ou avez déjà installé le certificat auto-signé Novell, vous pouvez également valider SSL en essayant l'URL suivante à partir d'une machine sur laquelle Endpoint Security Client est installé : `https://NOM_SERVEUR_SSI/AuthenticationServer/UserService.asmx (où NOM_SERVEUR_SSI est le nom du serveur).` Cette opération devrait renvoyer des données valides (une page html) et non des alertes de certificat. Toute alerte de certificat doit être résolue avant l'installation, à moins que vous ne choisissiez d'utiliser des certificats Novell auto-signés.
- ❑ Assurez l'accès à un RDBMS pris en charge (Microsoft SQL Server 2000 SP4, SQL Server Standard, SQL Server Enterprise). Définissez la base de données en mode mixte.

3.1 Procédure d'installation

Cliquez sur *Installation monoserveur* dans le menu du programme d'installation principal. Cette installation combine les installations pour le service de distribution de stratégies et le service de gestion Pour plus d'informations, reportez-vous à Chapitre 5, « Installation du service de distribution de stratégies », page 23 et à Chapitre 6, « Installation du service de gestion », page 31.

Comme pour les installations individuelles, l'installation *standard* installe les paramètres par défaut des services et les certificats SSL Novell auto-signés. *L'installation personnalisée* permet à l'administrateur de déterminer les chemins d'accès des répertoires et permet d'utiliser une autorité de certification d'entreprise.

3.2 Démarrage du service

Le service combiné de distribution et de gestion se lance immédiatement après l'installation, sans qu'il soit nécessaire de redémarrer le serveur. La console de gestion permet de gérer les services de distribution et de gestion à l'aide de l'outil de configuration. Pour plus d'informations, reportez-vous au *Guide d'administration de ZENworks Endpoint Security Management*.

Une fois l'installation terminée, la console de gestion et le service CLAS peuvent être installés sur ce serveur. Si vous souhaitez installer la console de gestion sur une machine distincte, copiez le dossier des fichiers d'installation de ZENworks Endpoint Security Management sur la machine de la console de gestion désignée pour terminer l'installation.

Passez au Chapitre 5, « Installation du service de distribution de stratégies », page 23.

Installation multiserveur

4

Une installation multiserveur est recommandée pour les déploiements de grande envergure ou lorsque le service de distribution de stratégies doit être placé à l'extérieur du pare-feu de l'entreprise afin que les utilisateurs reçoivent des mises à jour régulières des stratégies lorsqu'ils se situent en dehors du périmètre. Une installation multiserveur doit être effectuée sur au moins deux serveurs distincts. Si vous tentez d'installer séparément le service de distribution de stratégies et le service de gestion sur le même serveur, l'installation échoue. Pour plus d'informations, reportez-vous au Chapitre 3, « Installation monoserveur », page 17 pour une installation monoserveur.

Une installation multiserveur doit commencer par l'installation du service de distribution de stratégies sur un serveur sécurisé, que ce soit à l'extérieur ou à l'intérieur du pare-feu de l'entreprise. Pour plus d'informations, reportez-vous à Chapitre 5, « Installation du service de distribution de stratégies », page 23.

Une fois le service de distribution de stratégies installé, l'installation du service de gestion devrait suivre. Pour plus d'informations, reportez-vous à Chapitre 6, « Installation du service de gestion », page 31.

Il est recommandé d'installer également la console de gestion sur ce serveur. Pour plus d'informations, reportez-vous à Chapitre 7, « Installation de la console de gestion », page 43.

Passez à Chapitre 5, « Installation du service de distribution de stratégies », page 23.

Installation du service de distribution de stratégies

5

Le serveur hébergeant le service de distribution de stratégies ZENworks® Endpoint Security Management doit toujours être accessible aux utilisateurs, qu'ils se trouvent au sein du réseau ou à l'extérieur, dans la zone démilitarisée. Assurez-vous que les logiciels requis sont installés sur le serveur avant l'installation (reportez-vous à la section « Configuration système requise » page 10). Après avoir sélectionné le serveur, notez son nom, tant le nom NETBIOS que le nom de domaine complet.

Le déploiement du service de distribution de stratégies sur un contrôleur de domaine primaire n'est pas pris en charge pour des raisons de sécurité et de fonctionnalité.

Remarque : Il est recommandé de configurer (durcir) le serveur SSI de manière à désactiver les applications, services, comptes et autres options qui ne sont pas nécessaires à la finalité prévue du serveur. La procédure à suivre pour ce faire varie selon les spécificités de l'environnement local et ne peut donc pas être décrite au préalable. Les administrateurs sont invités à consulter la section appropriée de la page Web de sécurité Microsoft Technet (http://www.microsoft.com/technet/security/default.mspx). D'autres recommandations concernant le contrôle d'accès sont fournies dans le *Guide d'administration de ZENworks Endpoint Security Management*.

Afin de limiter l'accès aux seules machines approuvées, le répertoire virtuel et IIS peuvent être configurés pour utiliser des listes de contrôle d'accès (ACL). Reportez-vous aux articles ci-dessous :

- Accorder et refuser l'accès aux ordinateurs (http://www.microsoft.com/technet/prodtechnol/windows2000serv/default.mspx)
- Restreindre l'accès au site par l'adresse IP ou le nom de domaine (http://support.microsoft.com/default.aspx?scid=kb%3BEN-US%3BQ324066)
- FAQ IIS : restrictions de l'adresse IP 2000 et du nom de domaine (http://www.iisfaq.com/default.aspx?View=A136&P=109)
- Utilisation du filtrage de paquets IIS (http://www.15seconds.com/issue/011227.htm)

Pour des raisons de sécurité, il est vivement recommandé de supprimer les dossiers par défaut suivants de toute installation IIS :

- `IISHelp`
- `IISAdmin`
- `Scripts`
- `Printers`

Nous vous recommandons également d'utiliser IIS Lockdown Tool 2.1, disponible sur microsoft.com (http://www.microsoft.com/technet/security/tools/locktool.mspx).

La version 2.1 de cet outil repose sur des modèles fournis pour les principaux produits Microsoft basés dépendant de IIS. Sélectionnez le modèle qui correspond le mieux au rôle de ce serveur. En cas de doute, le modèle de serveur Dynamic Web est recommandé.

Assurez-vous que les exigences suivantes sont satisfaites avant de commencer l'installation :

- Vérifiez la résolution de nom de serveur entre le service de gestion et le service de distribution de stratégies : vérifiez que l'ordinateur cible sur lequel le service de gestion est installé peut exécuter une commande ping sur le nom de serveur du service de distribution (NETBIOS si le service de distribution est configuré à l'intérieur du pare-feu du réseau, nom de domaine complet s'il est installé à l'extérieur, dans la zone démilitarisée).
- Si la résolution aboutit, il s'agit du nom de serveur à spécifier pendant l'installation. En cas d'échec, vous devez résoudre ce problème avant de poursuivre l'installation.
- Pour la résolution de nom de serveur entre Endpoint Security Client et le service de distribution, vérifiez que les clients du noeud d'extrémité (où est installé Endpoint Security Client) peuvent exécuter une commande ping sur le nom de serveur du service de distribution utilisé ci-dessus. En cas d'échec, vous devez résoudre ce problème avant de poursuivre l'installation.
- Activez ou installez Microsoft Internet Information Services (IIS), assurez-vous qu'ASP.NET est activé et configurez-le pour qu'il accepte les certificats SSL (Secure Socket Layer).

  Important : Ne cochez pas la case *Requérir un canal sécurisé (SSL)* sur la page Communications sécurisées (dans l'utilitaire Microsoft Gestion de l'ordinateur, développez *Services et applications* > *Gestionnaire des services ISS* > *Sites Web* > cliquez avec le bouton droit de la souris sur *Site Web par défaut* > cliquez sur *Propriétés* > cliquez sur l'onglet *Sécurité de répertoire* > cliquez sur le bouton *Éditer* dans la zone de groupe Communications sécurisées). L'activation de cette option interrompt la communication entre le serveur ZENworks Endpoint Security Management et le client ZENworks Endpoint Security sur le noeud d'extrémité.

- Si vous utilisez vos propres certificats SSL, assurez-vous que le certificat de service Web est chargé sur la machine et que le nom de serveur validé aux étapes précédentes (NETBIOS ou nom de domaine complet) correspond à la valeur *Délivré à* du certificat configuré dans IIS.
- Si vous utilisez vos propres certificats SSL, validez le SSL du serveur du service de gestion vers le serveur du service de distribution : ouvrez un navigateur Web sur le service de gestion et entrez l'URL suivante : `https://NOMDS` (où *NOMDS* correspond au nom du serveur du service de distribution). Cette opération devrait renvoyer des données valides et non des alertes de certificat (des données valides peuvent être du type « Page en construction »). Toute alerte de certificat doit être résolue avant l'installation, à moins que vous ne choisissiez d'utiliser des certificats Novell auto-signés.
- Assurez l'accès à un RDBMS pris en charge (Microsoft SQL Server 2000 SP4, SQL Server Standard, SQL Server Enterprise, SQL Server 2005). Définissez la base de données en mode mixte. Cette base de données doit être hébergée sur le serveur du service de gestion ou sur un serveur partagé sécurisé derrière le pare-feu de l'entreprise.

5.1 Procédure d'installation

Cliquez sur *Installation du service de distribution de stratégies* dans le menu Interface d'installation. L'installation du service de distribution de stratégies démarre.

Au lancement, le programme d'installation vérifie que tous les logiciels requis sont présents sur le serveur. Si un logiciel est absent, il est automatiquement installé avant l'affichage de l'écran de bienvenue du programme d'installation (vous devrez éventuellement accepter les accords de licence des logiciels supplémentaires). Si Microsoft Data Access Components (MDAC) 2.8 doit être

installé, le serveur doit redémarrer après cette installation, avant que l'installation de ZENworks Endpoint Security Management puisse continuer. Si vous utilisez Windows Server 2003, ASP.NET 2.0 est configuré pour être exécuté par le programme d'installation.

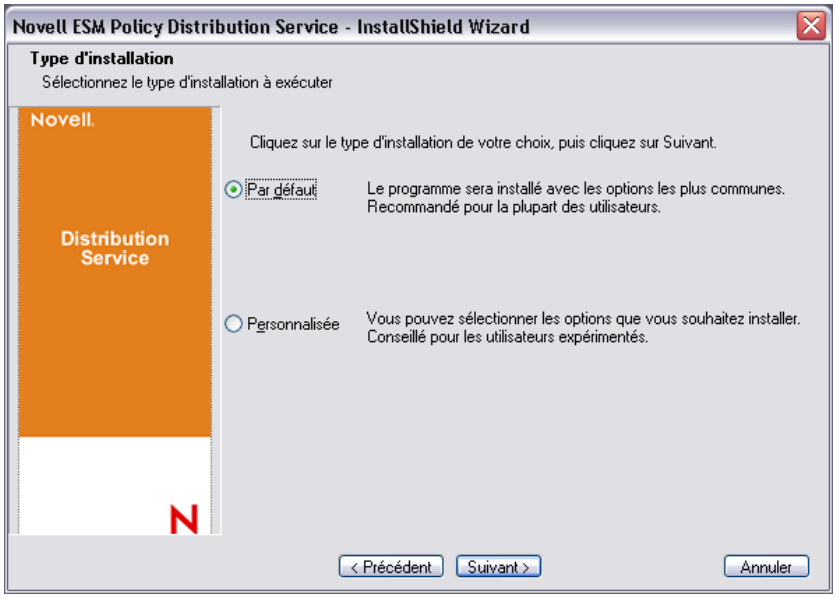
Une fois que l'installation du service de distribution de stratégies commence, procédez comme suit :

Remarque : La procédure qui suit décrit ce que vous, administrateur, devez faire pour mener à bien l'installation. Des processus internes s'affichent tout au long de l'installation et ne sont pas documentés ici, à moins qu'une action ou information spécifique soit nécessaire pour que l'installation réussisse.

---

1. Cliquez sur *Suivant* dans l'écran de bienvenue pour continuer.
2. Acceptez l'accord de licence, puis cliquez sur *Suivant*.
3. Sélectionnez une installation *Standard* ou *Personnalisée*.

Figure 5-1 *Sélectionnez une installation Standard ou personnalisée*



Les deux options sont présentées ci-dessous :

- Section 5.1.1, « Installation standard », page 25
- Section 5.1.2, « Installation personnalisée », page 27

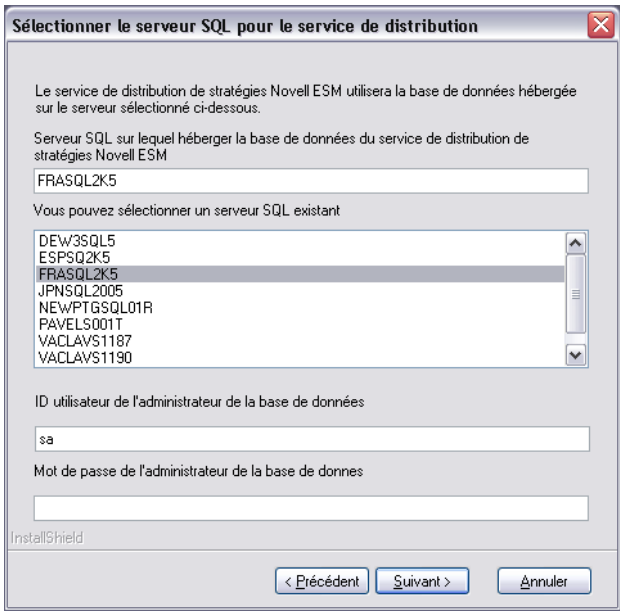
5.1.1 Installation standard

Une installation standard place les fichiers du logiciel du service de distribution de stratégies dans le répertoire par défaut : `\Program Files\Novell\Service de distribution de stratégies ESM`. Le nom de base de données SQL assigné est STDSDB. Les trois fichiers de base de données SQL (données, index et journal) sont placés dans :`\Program Files\Microsoft SQL Server\mssql\Data`.

1. Des certificats SSL Novell sont créés pour l'installation. Si vous souhaitez utiliser vos propres certificats SSL, choisissez une installation personnalisée. Ces certificats doivent être distribués à tous les utilisateurs.

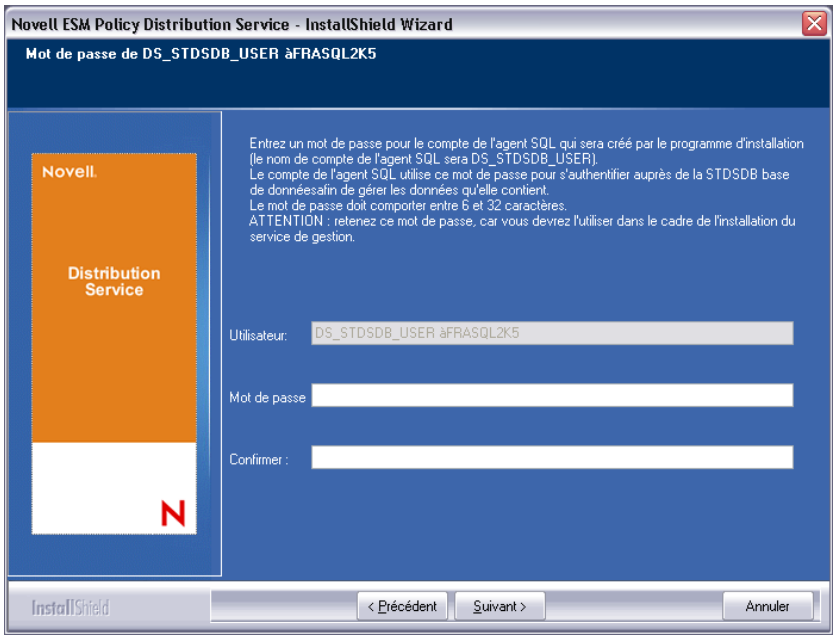
2 Le programme d'installation détecte les bases de données SQL disponibles sur la machine et sur le réseau. Sélectionnez une base de données SQL sécurisée pour le service de distribution de stratégies et entrez le nom et le mot de passe de l'administrateur de la base de données (si aucun mot de passe n'est spécifié, le programme d'installation vous avertit du risque potentiel pour la sécurité). Le nom d'utilisateur et le mot de passe ne peuvent pas être ceux d'un utilisateur du domaine, mais ceux d'un utilisateur SQL possédant des droits SysAdmin.

Figure 5-2 *Sélection du serveur SQL*



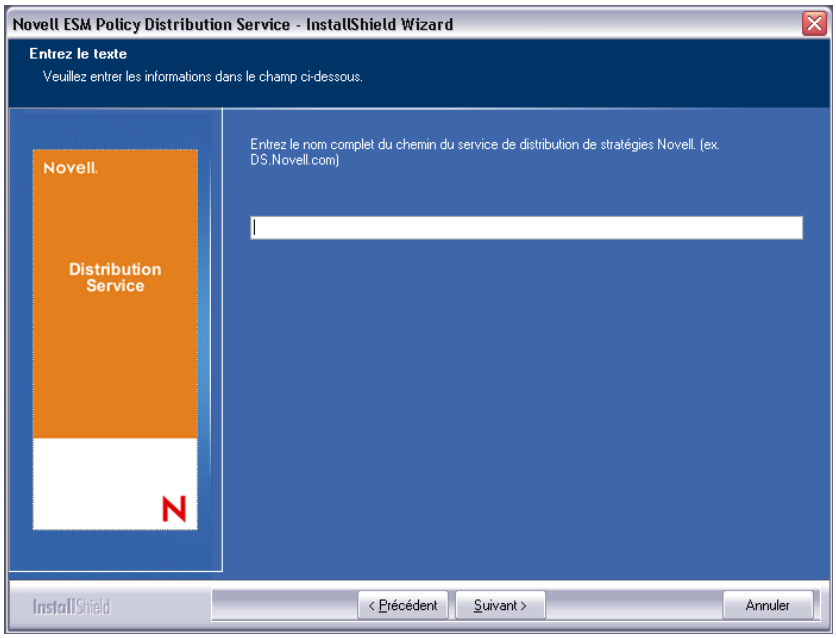
3 Spécifiez le mot de passe de l'agent de service de distribution de stratégies. Il s'agit du nom d'utilisateur et du mot de passe que le service utilise pour se loguer à sa base de données SQL.

Figure 5-3 *Mot de passe SQL du service de distribution*



4 Spécifiez le nom de domaine du service de distribution de stratégies. Ce nom doit être le nom de domaine complet si le serveur est installé à l'extérieur du pare-feu de l'entreprise. Dans le cas contraire, seul le nom NETBIOS du serveur est requis.

Figure 5-4 *Saisie du nom de domaine du service de distribution de stratégies*



5 Dans l'écran Copier les fichiers, cliquez sur *Suivant* pour démarrer l'installation.

6 Un dossier `Fichiers d'installation de ESM` est créé dans le répertoire d'installation. Ce dossier contient un fichier `ID d'installation` et le fichier `ESM-DS.cer` (certificat SSL Novell auto-signé) requis par le service de gestion. Copiez ce fichier directement sur la machine désignée comme hôte du service de gestion, soit via un partage réseau soit en enregistrant le fichier sur un disque ou une clé USB et en le chargeant manuellement dans le répertoire d'installation du serveur.

7 Le service de distribution de stratégies est maintenant installé ; cliquez sur *Terminer* pour fermer le programme d'installation et lancer le moniteur de performances.

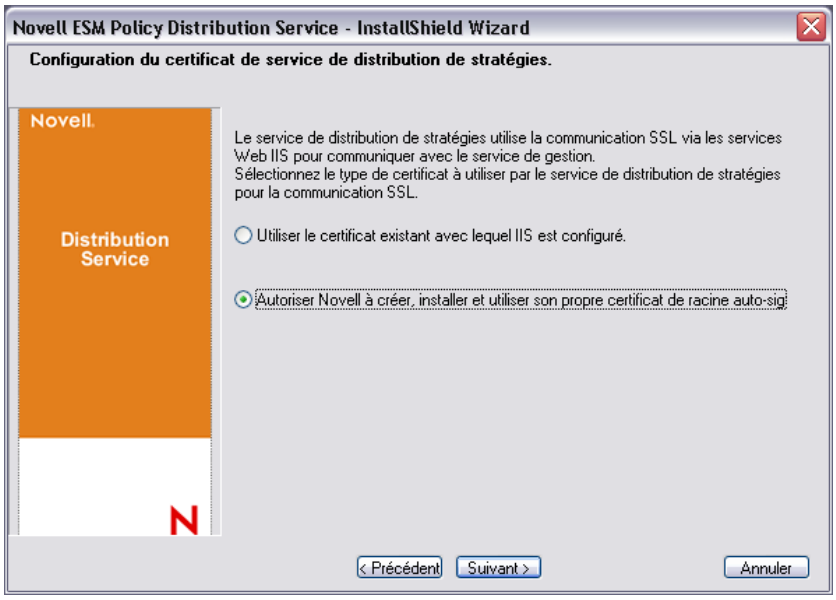
5.1.2 Installation personnalisée

Une installation personnalisée affiche les valeurs par défaut utilisées dans l'installation standard et permet à l'administrateur de spécifier ou de localiser un autre répertoire pour l'enregistrement des fichiers du logiciel.

L'administrateur peut choisir d'installer un certificat SSL Novell auto-signé ou d'utiliser un de ses propres certificats.

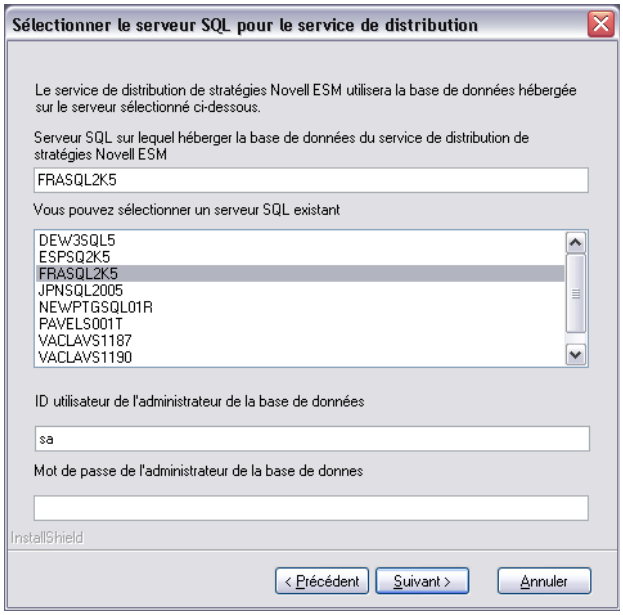
1 Un certificat SSL est requis pour sécuriser la communication entre le service de distribution de stratégies et le service de gestion, ainsi qu'entre le service de distribution et tous les clients de sécurité de Novell. Si vous avez déjà une autorité de certification, cliquez sur *Utiliser le certificat existant pour lequel IIS est configuré*. Si vous avez besoin d'un certificat, cliquez sur *Autoriser Novell à créer, installer et utiliser son propre certificat de racine auto-signé*. Le programme d'installation crée les certificats et l'autorité de signature. Quel que soit le type de certificat, ces certificats doivent être distribués à tous les utilisateurs.

Figure 5-5 *Configuration de la racine approuvée*



2 Le programme d'installation détecte les bases de données SQL disponibles sur la machine et sur le réseau. Sélectionnez la base de données SQL sécurisée pour le service de distribution de stratégies et entrez le nom et le mot de passe de l'administrateur de la base de données (si aucun mot de passe n'est spécifié, le programme d'installation vous avertit du risque potentiel pour la sécurité). Le nom d'utilisateur et le mot de passe ne peuvent pas être ceux d'un utilisateur du domaine, mais ceux d'un utilisateur SQL possédant des droits SysAdmin.

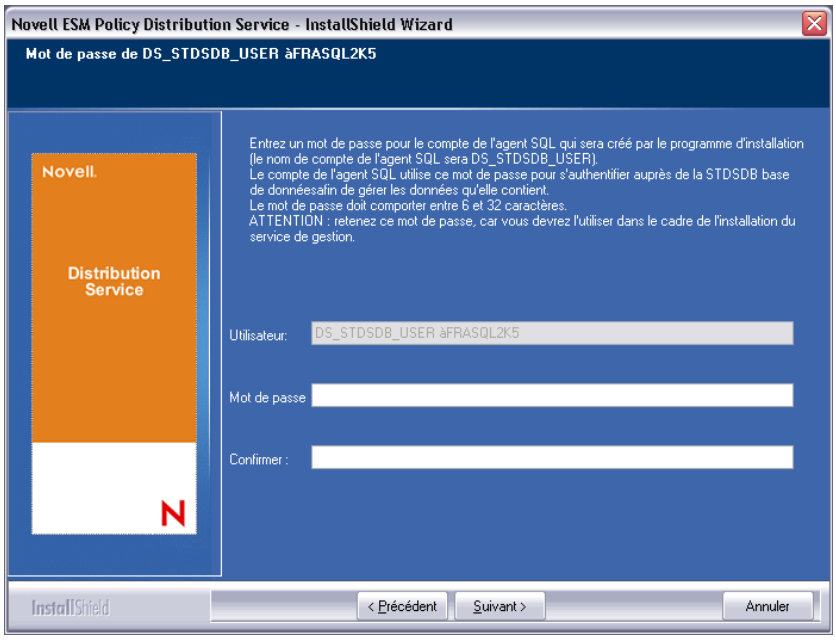
Figure 5-6 *Sélection du serveur SQL*



3 Spécifiez le nom de la base de données (le nom utilisé par défaut est STDSDB).

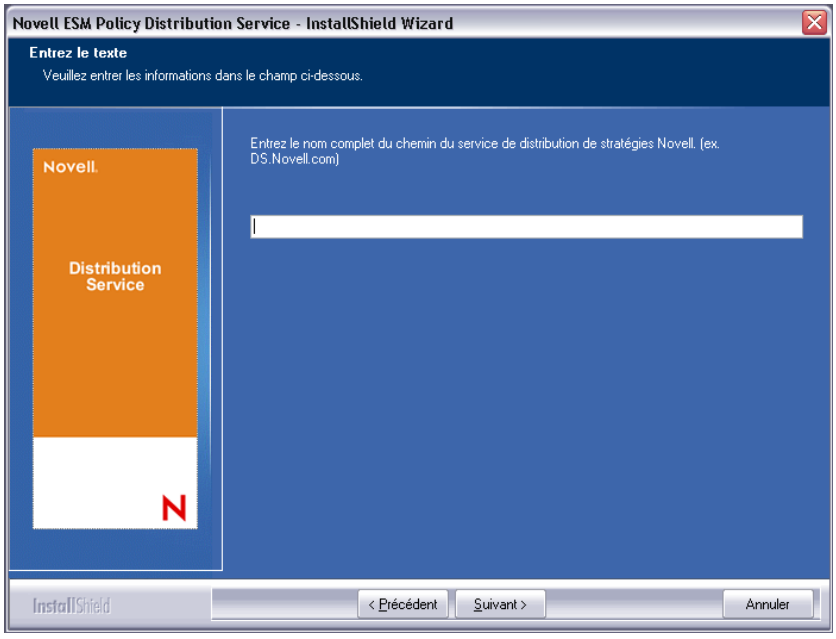
4 Spécifiez le mot de passe de l'agent de service de distribution de stratégies. Il s'agit du nom d'utilisateur et du mot de passe que le service utilise pour se loguer à sa base de données SQL.

Figure 5-7 *Mot de passe SQL du service de distribution*



5 Spécifiez le nom de domaine du service de distribution de stratégies. Ce nom doit être le nom de domaine complet si le serveur est installé à l'extérieur du pare-feu de l'entreprise. Dans le cas contraire, seul le nom NETBIOS du serveur est requis.

Figure 5-8 *Saisie du nom de domaine du service de distribution de stratégies*



6 Dans l'écran Copier les fichiers, cliquez sur *Suivant* pour démarrer l'installation.

7 Sélectionnez les chemins d'accès des fichiers journaux, de données et d'index.

8 Un dossier `Fichiers d'installation de ESM` est créé dans le répertoire d'installation. Ce dossier contient un fichier `ID d'installation` et le fichier `ESM-DS.cer` (certificat SSL Novell auto-signé, le cas échéant) requis par le service de gestion. Utilisez le bouton Parcourir pour indiquer l'endroit où ce fichier doit être enregistré sur le serveur (par défaut : le répertoire d'installation).

Figure 5-9 *Enregistrement des fichiers d'installation*

9 Si vous avez choisi d'utiliser un certificat SSL d'entreprise, placez une copie de ce fichier dans le dossier `Fichiers d'installation de ESM`.

10 Copiez l'ensemble du dossier `Fichiers d'installation de ESM` directement sur la machine désignée comme hôte du service de gestion, via un partage réseau ou en enregistrant le fichier sur un disque ou une clé USB et en le chargeant manuellement dans le répertoire d'installation du serveur.

11 Le service de distribution de stratégies est maintenant installé ; cliquez sur *Terminer* pour fermer le programme d'installation et lancer le moniteur de performances.

5.2 Démarrage du service

Le service de distribution de stratégies se lance immédiatement après l'installation, sans qu'il soit nécessaire de redémarrer le serveur. La console de gestion permet d'ajuster le moment de téléchargement du service de distribution à l'aide de l'outil de configuration. Pour plus d'informations, reportez-vous au *Guide d'administration de ZENworks Endpoint Security Management*.

Passez au Chapitre 6, « Installation du service de gestion », page 31.

Installation du service de gestion

6

Le service de gestion doit être installé sur un serveur sécurisé derrière le pare-feu et ne peut pas partager le même serveur que le service de distribution de stratégies (à l'exception d'une installation monoserveur, reportez-vous au Chapitre 3, « Installation monoserveur », page 17). Pour des raisons de sécurité, le service de gestion ne peut pas être installé en dehors du pare-feu du réseau. Après avoir sélectionné le serveur, notez son nom, tant le nom NETBIOS que le nom de domaine complet. Le déploiement du service de gestion sur un contrôleur de domaine primaire n'est pas pris en charge pour des raisons de sécurité et de fonctionnalité.

Remarque : Il est recommandé de configurer (durcir) le serveur SSI de manière à désactiver les applications, services, comptes et autres options qui ne sont pas nécessaires à la finalité prévue du serveur. La procédure à suivre pour ce faire varie selon les spécificités de l'environnement local et ne peut donc pas être décrite au préalable. Les administrateurs sont invités à consulter la section appropriée de la page Web de sécurité Microsoft Technet (http://www.microsoft.com/technet/security/default.mspx). D'autres recommandations concernant le contrôle d'accès sont fournies dans le *Guide d'administration de ZENworks Endpoint Security Management*.

Afin de limiter l'accès aux seules machines approuvées, le répertoire virtuel et IIS peuvent être configurés pour utiliser des listes de contrôle d'accès (ACL). Reportez-vous aux articles ci-dessous :

- Accorder et refuser l'accès aux ordinateurs (http://www.microsoft.com/technet/prodtechnol/windows2000serv/default.mspx)
- Restreindre l'accès au site par l'adresse IP ou le nom de domaine (http://support.microsoft.com/default.aspx?scid=kb%3BEN-US%3BQ324066)
- FAQ IIS : restrictions de l'adresse IP 2000 et du nom de domaine (http://www.iisfaq.com/default.aspx?View=A136&P=109)
- Utilisation du filtrage de paquets IIS (http://www.15seconds.com/issue/011227.htm)

Pour des raisons de sécurité, il est vivement recommandé de supprimer les dossiers par défaut suivants de toute installation IIS :

- `IISHelp`
- `IISAdmin`
- `Scripts`
- `Printers`

Nous vous recommandons également d'utiliser IIS Lockdown Tool 2.1, disponible sur microsoft.com (http://www.microsoft.com/technet/security/tools/locktool.mspx).

La version 2.1 de cet outil repose sur des modèles fournis pour les principaux produits Microsoft basés dépendant de IIS. Sélectionnez le modèle qui correspond le mieux au rôle de ce serveur. En cas de doute, le modèle de serveur Dynamic Web est recommandé.

Assurez-vous que les exigences suivantes sont satisfaites avant de commencer l'installation :

- ❑ Assurez l'accès à un service Annuaire pris en charge (eDirectory, Active Directory ou NT Domains*). * = Uniquement pris en charge lorsque le service de gestion est installé sur un serveur Microsoft Windows 2000 Advanced Server (SP4).

- ❑ Si vous effectuez le déploiement à l'aide d'un service eDirectory™, assurez-vous que le client Novell™ est installé sur le serveur et peut s'authentifier correctement auprès de eDirectory. Créez un mot de passe de compte qui ne changera jamais pour l'authentification à la console de gestion (reportez-vous à la Section 7.2.1, « Ajout de services eDirectory », page 47).
- ❑ Pour la résolution de nom de serveur entre Endpoint Security Client et le service de gestion, vérifiez que les ordinateurs cibles (où est installé Endpoint Security Client) peuvent exécuter une commande ping sur le nom de serveur du service de gestion. Si cela fonctionne, il s'agit de la valeur entrée lors de l'installation. En cas d'échec, vous devez résoudre ce problème avant de poursuivre l'installation.
- ❑ Activez ou installez Microsoft Internet Information Services (IIS), assurez-vous qu'ASP.NET est activé et configurez-le pour qu'il accepte les certificats SSL (Secure Socket Layer).

  Important : Ne cochez pas la case *Requérir un canal sécurisé (SSL)* sur la page Communications sécurisées (dans l'utilitaire Microsoft Gestion de l'ordinateur, développez *Services et applications* > *Gestionnaire des services ISS* > *Sites Web* > cliquez avec le bouton droit de la souris sur *Site Web par défaut* > cliquez sur *Propriétés* > cliquez sur l'onglet *Sécurité de répertoire* > cliquez sur le bouton *Éditer* dans la zone de groupe Communications sécurisées). L'activation de cette option interrompt la communication entre le serveur ZENworks Endpoint Security Management et le client ZENworks Endpoint Security sur le noeud d'extrémité.

- ❑ Si vous utilisez vos propres certificats SSL, assurez-vous que l'autorité de certification racine est chargée sur la machine et que le nom de serveur validé aux étapes précédentes (NETBIOS ou nom de domaine complet) correspond à la valeur *Délivré à* du certificat configuré dans IIS.
- ❑ Si vous utilisez vos propres certificats ou avez déjà installé le certificat auto-signé Novell, vous pouvez également valider SSL en essayant l'URL suivante à partir d'une machine sur laquelle Endpoint Security Client est installé : `https://NOM_SERVEUR_SERVICE DE GESTION/AuthenticationServer/UserService.asmx` (où *NOM_SERVEUR_SERVICE DE GESTION* est le nom du serveur). Cette opération devrait renvoyer des données valides (une page html) et non des alertes de certificat. Toute alerte de certificat doit être résolue avant l'installation.
- ❑ Assurez l'accès à un RDBMS pris en charge (Microsoft SQL Server 2000 SP4, SQL Server Standard, SQL Server Enterprise, SQL 2005). Définissez la base de données en mode mixte.
- ❑ Copiez dans le répertoire d'installation de ce serveur le répertoire `Fichiers d'installation de ESM` qui contient l'ID d'installation et le certificat SSL racine du service de distribution de stratégies.

6.1 Procédure d'installation

Cliquez sur *Installation du service de gestion* dans le menu Interface d'installation. L'installation du service de gestion démarre.

Au lancement, le programme d'installation vérifie que tous les logiciels requis sont présents sur le serveur. Si un logiciel est absent, il est automatiquement installé avant l'affichage de l'écran de bienvenue du programme d'installation (vous devrez éventuellement accepter les accords de licence des logiciels supplémentaires). Si Microsoft Data Access Components (MDAC) 2.8 doit être installé, le serveur doit redémarrer après cette installation, avant que l'installation de ZENworks Endpoint Security Management puisse continuer. Si vous utilisez Windows Server 2003, ASP.NET 2.0 doit être configuré pour être exécuté par le programme d'installation.

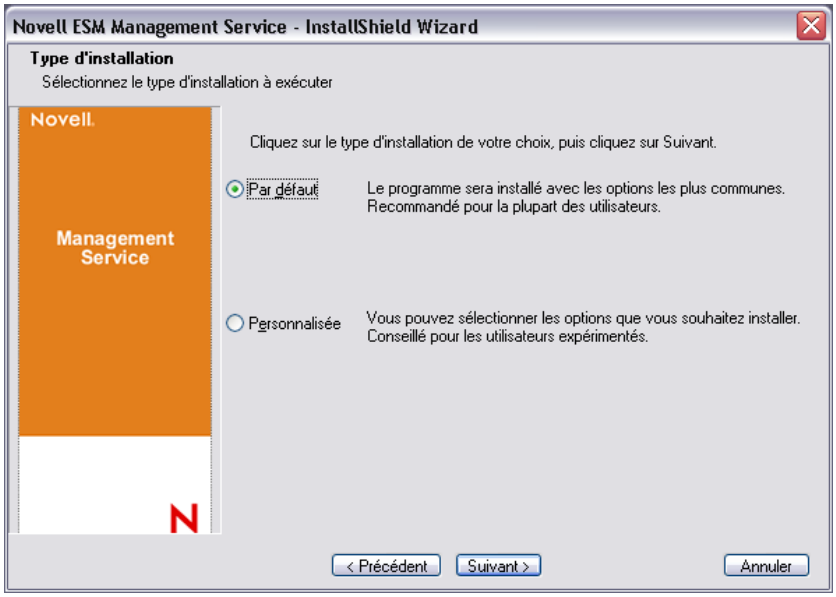
Une fois que l'installation du service de gestion commence, procédez comme suit :

Remarque : La procédure qui suit décrit ce que vous, administrateur, devez faire pour mener à bien l'installation. Des processus internes s'affichent tout au long de l'installation et ne sont pas documentés ici, à moins qu'une action ou information spécifique soit nécessaire pour que l'installation réussisse.

---

1. Cliquez sur *Suivant* dans l'écran de bienvenue pour continuer.
2. Acceptez l'accord de licence, puis cliquez sur *Suivant*.
3. Sélectionnez une installation *Standard* ou *Personnalisée*.

Figure 6-1 *Installation standard ou personnalisée*



Les deux options sont présentées ci-dessous :

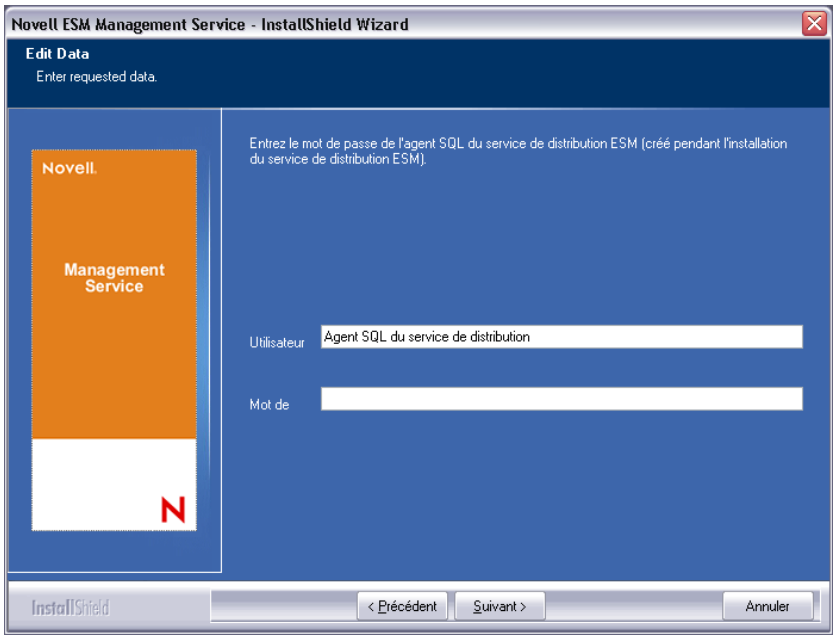
- Section 6.1.1, « Installation standard », page 33
- Section 6.1.2, « Installation personnalisée », page 37

6.1.1 Installation standard

Une installation standard place les fichiers du logiciel du service de gestion dans le répertoire par défaut :`\Program Files\Novell\Service de gestion ESM`. Le nom de base de données SQL assigné est STMSDB. Les trois fichiers de base de données SQL (données, index et journal) sont placés dans :`\Program Files\Microsoft SQL Server\mssql\Data`.

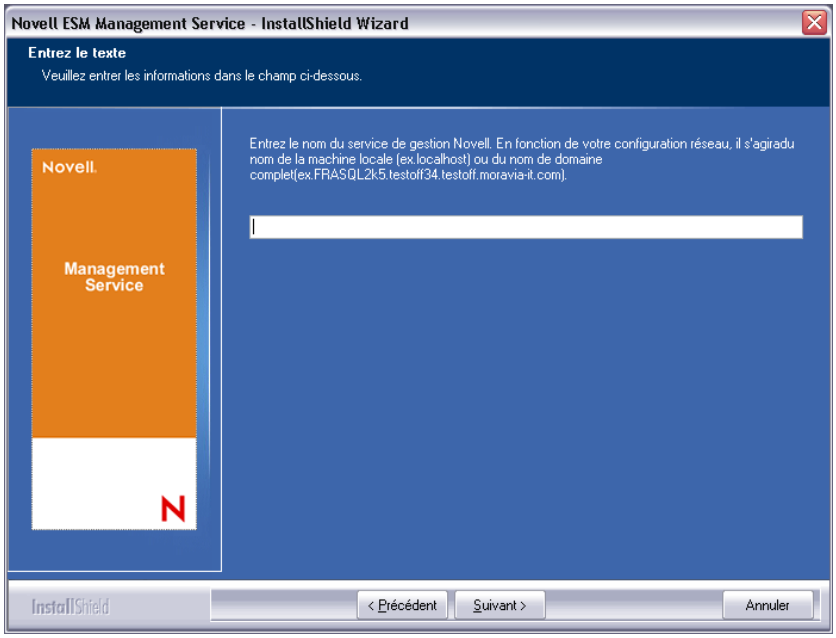
1. Spécifiez le mot de passe de l'agent du service de distribution de stratégies créé pendant l'installation du service de distribution de stratégies.

Figure 6-2 *Saisie du mot de passe SQL*



2 Spécifiez le nom du serveur qui héberge le service de gestion.

Figure 6-3 *Saisie du nom de serveur du service de gestion*

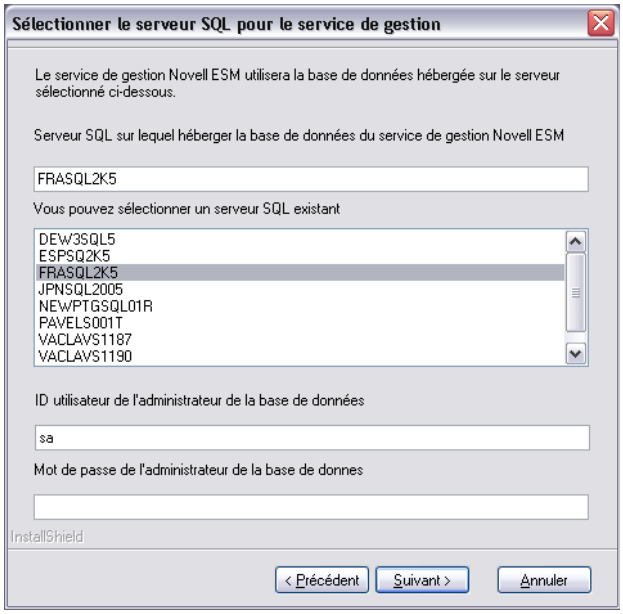


3 Des certificats SSL Novell sont créés pour l'installation. Si vous souhaitez utiliser vos propres certificats SSL, effectuez une installation personnalisée. Ces certificats doivent être distribués à tous les utilisateurs.

4 Le programme d'installation détecte les bases de données SQL disponibles sur la machine et sur le réseau. Sélectionnez la base de données SQL pour le service de gestion et spécifiez le nom d'utilisateur et le mot de passe de l'administrateur de la base de données (si aucun mot de passe

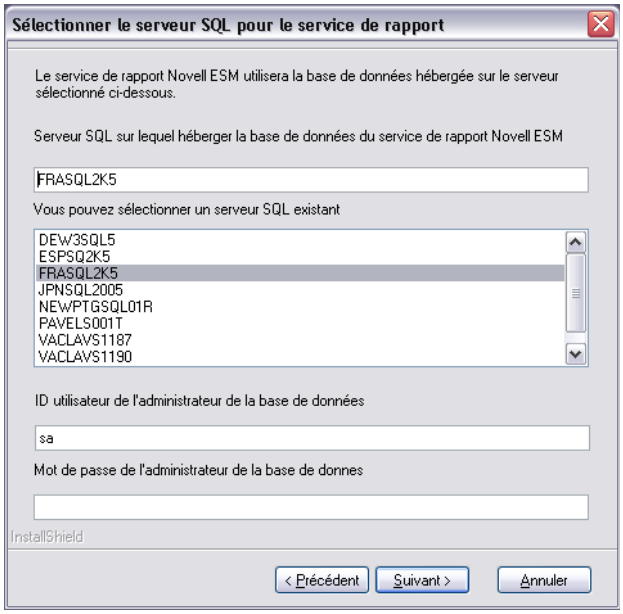
n'est spécifié, le programme d'installation vous avertit du risque potentiel pour la sécurité). Le nom d'utilisateur et le mot de passe ne peuvent pas être ceux d'un utilisateur du domaine, mais ceux d'un utilisateur SQL possédant des droits SysAdmin.

Figure 6-4 *Sélection de la base de données SQL du service de gestion*



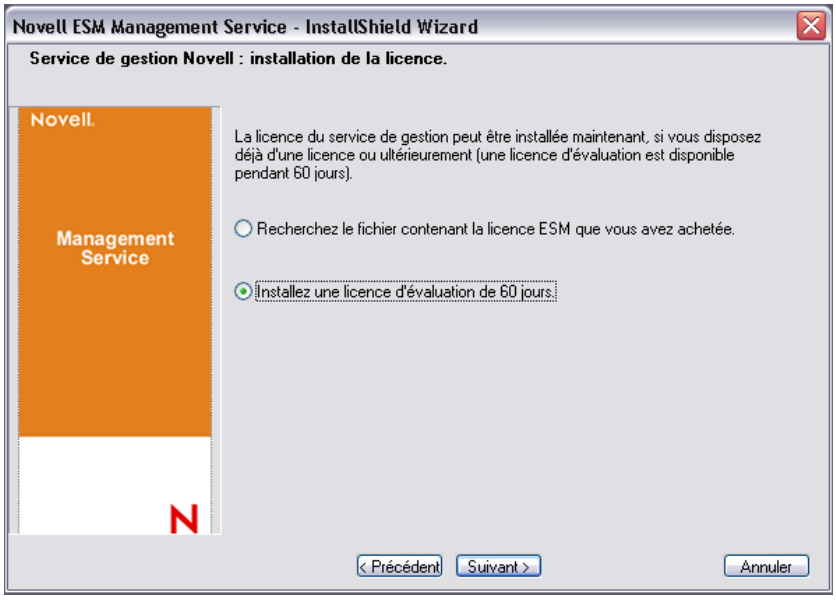
5 Sélectionnez la base de données SQL du service de rapport et spécifiez le mot de passe de l'administrateur de la base de données. Si vous prévoyez de capturer et de stocker un nombre important de rapports, il est recommandé d'affecter son propre serveur SQL à la base de données du service de rapport.

Figure 6-5 *Sélection de la base de données du service de rapport*



6 Si ZENworks Endpoint Security Management a déjà été acheté, un fichier de licence distinct est fourni. Copiez le fichier de licence sur ce serveur et localisez-le (pour des détails, reportez-vous à la page d'instructions fournie avec votre fichier de licence). Si vous n'avez pas encore acheté de licence ZENworks Endpoint Security Management, sélectionnez *Licence d'évaluation de 60 jours* pour continuer.

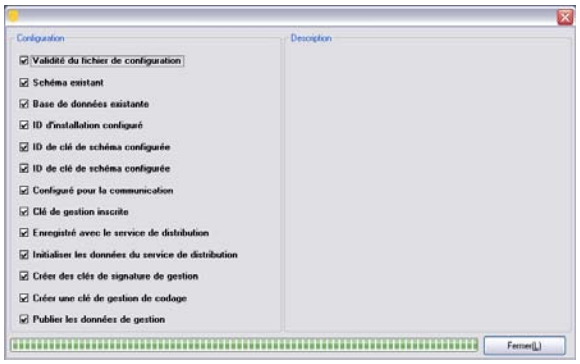
Figure 6-6 *Localisation du fichier de licence Novell*



7 Dans l'écran Copier les fichiers, cliquez sur *Suivant* pour démarrer l'installation.

8 Le service de gestion exécute une vérification de la communication avec les bases de données SQL et le service de distribution de stratégies. Si la communication échoue, le programme d'installation vous avertit du problème. Toutes les cases doivent être cochées pour que l'installation réussisse.

Figure 6-7 *Vérification de la communication*



9 Passez l'Étape 10 et l'Étape 11 et si vous effectuez l'installation avec eDirectory comme service Annuaire.

10 Si cette installation a lieu sur un serveur membre d'un domaine utilisant un service Annuaire Active Directory ou NT Domains, le programme d'installation détecte automatiquement les données suivantes et les ajoute à l'installation via une connexion sécurisée en lecture seule :

- Nom de domaine racine ou nom de la machine
- Nom de l'administrateur du domaine ou compte de la ressource disposant des autorisations de lecture appropriées

11 Entrez le mot de passe de l'administrateur dans l'espace prévu à cet effet et cliquez sur *Test pour vérifier que la connexion peut être établie*. Si le test réussit, cliquez sur *Enregistrer*. Si le test échoue ou si le domaine correct n'est pas détecté, il doit être ajouté manuellement via la console de gestion (reportez-vous à la Section 7.2.1, « Ajout de services eDirectory », page 47).

Remarque : Le mot de passe entré doit être configuré de sorte à ne jamais expirer, de même que ce compte ne doit jamais être désactivé.

---

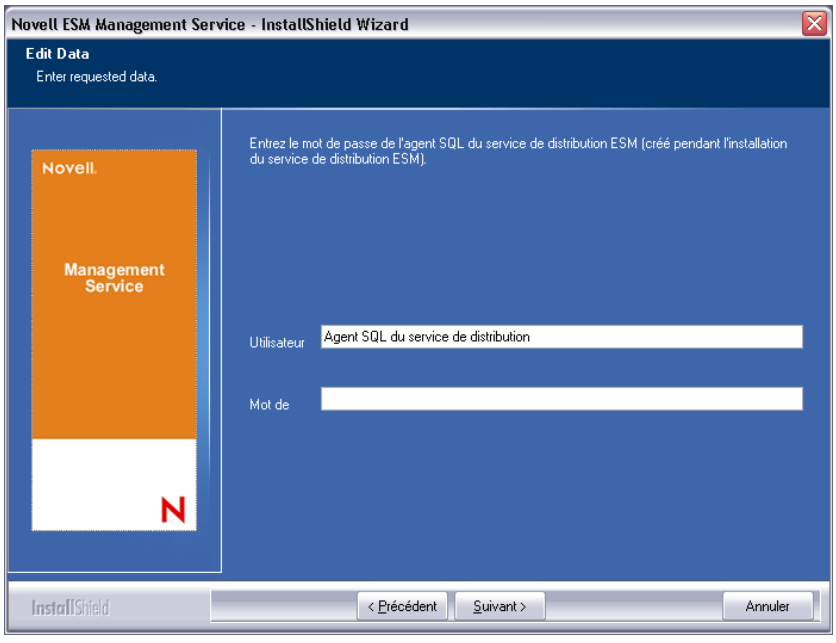
12 Le service de gestion est maintenant installé. Cliquez sur *Terminé* pour mettre fin aux vérifications de communication, puis sur *Terminer* pour fermer le programme d'installation.

6.1.2 Installation personnalisée

Une installation personnalisée affiche les valeurs par défaut utilisées dans l'installation standard et permet à l'administrateur d'entrer ou de localiser un autre emplacement.

1 Spécifiez le mot de passe de l'agent du service de distribution de stratégies créé pendant l'installation du service de distribution de stratégies.

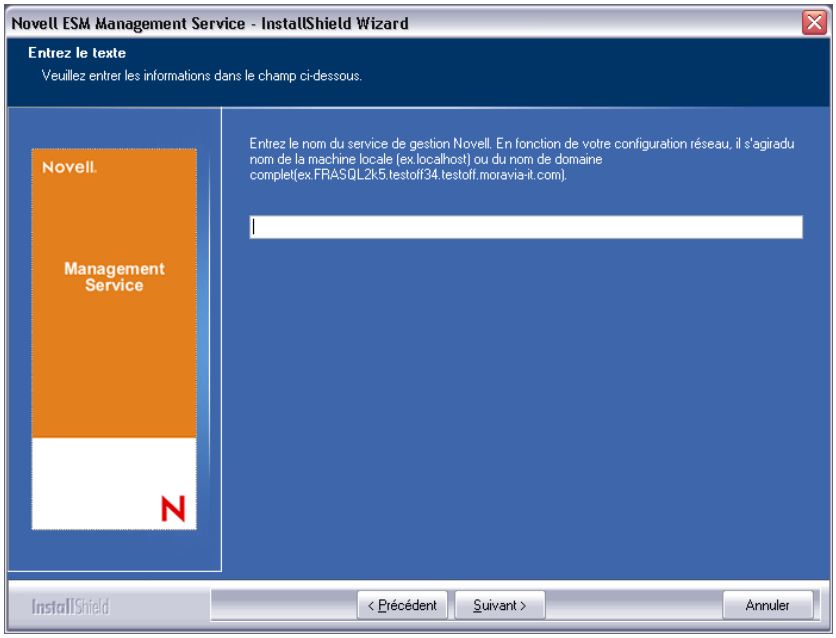
Figure 6-8 *Saisie du mot de passe SQL*



2 Sélectionnez le type de certificat SSL utilisé pour l'installation du service de distribution de stratégies. Si vous avez utilisé votre autorité de certification (d'entreprise), cliquez sur *Le service de distribution Novell a utilisé un certificat ayant déjà servi à la configuration de IIS*. Si le programme d'installation du service de distribution a créé un certificat Novell, cliquez sur *Le service de distribution Novell a installé un certificat de racine auto-signé Novell*.

3 Spécifiez le nom du serveur qui héberge le service de gestion.

Figure 6-9 *Saisie du nom de serveur du service de gestion*

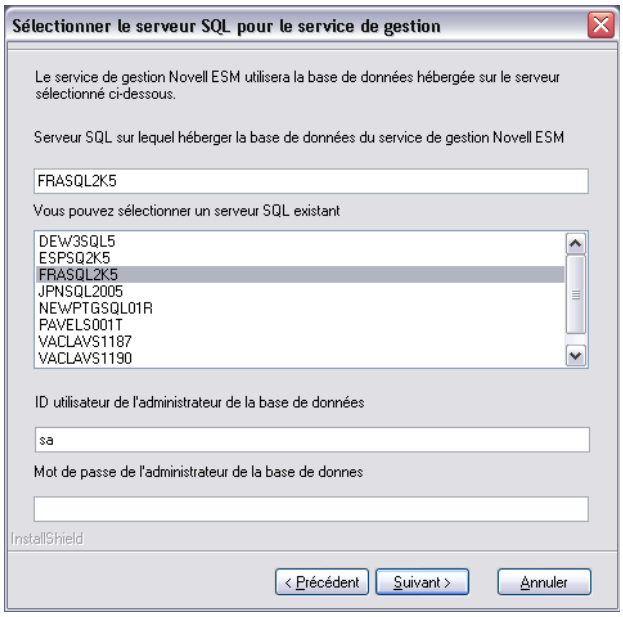


4 Un certificat SSL est requis pour sécuriser la communication entre le service de gestion et tous les clients Endpoint Security Client. Si vous avez déjà une autorité de certification, cliquez sur *Utiliser le certificat existant pour lequel IIS est configuré*. Si vous avez besoin d'un certificat, cliquez sur *Autoriser Novell à créer, installer et utiliser son propre certificat de racine auto-signé*. Le programme d'installation crée les certificats et l'autorité de signature. Quel que soit le type de certificat, ces certificats doivent être distribués à tous les utilisateurs.

5 Lorsque vous sélectionnez des certificats Novell, indiquez l'emplacement dans lequel le certificat peut être enregistré afin de faciliter sa distribution (par défaut, le répertoire d'installation).

6 Le programme d'installation détecte les bases de données SQL disponibles sur la machine et sur le réseau. Sélectionnez la base de données SQL pour le service de gestion et spécifiez le nom d'utilisateur et le mot de passe de l'administrateur de la base de données (si aucun mot de passe n'est spécifié, le programme d'installation vous avertit du risque potentiel pour la sécurité). Le nom d'utilisateur et le mot de passe ne peuvent pas être ceux d'un utilisateur du domaine, mais ceux d'un utilisateur SQL possédant des droits SysAdmin.

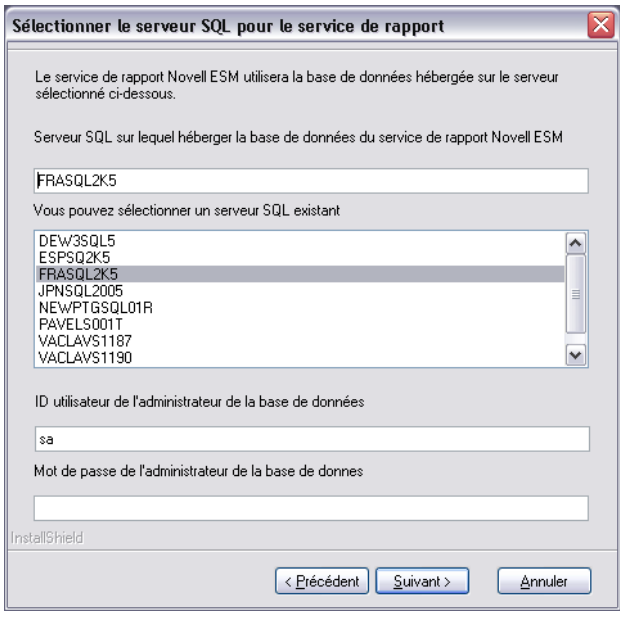
Figure 6-10 *Sélection de la base de données SQL du service de gestion*



7 Spécifiez le nom de la base de données (le nom utilisé par défaut est STMSDB).

8 Sélectionnez la base de données SQL du service de rapport et spécifiez le mot de passe de l'administrateur de la base de données.

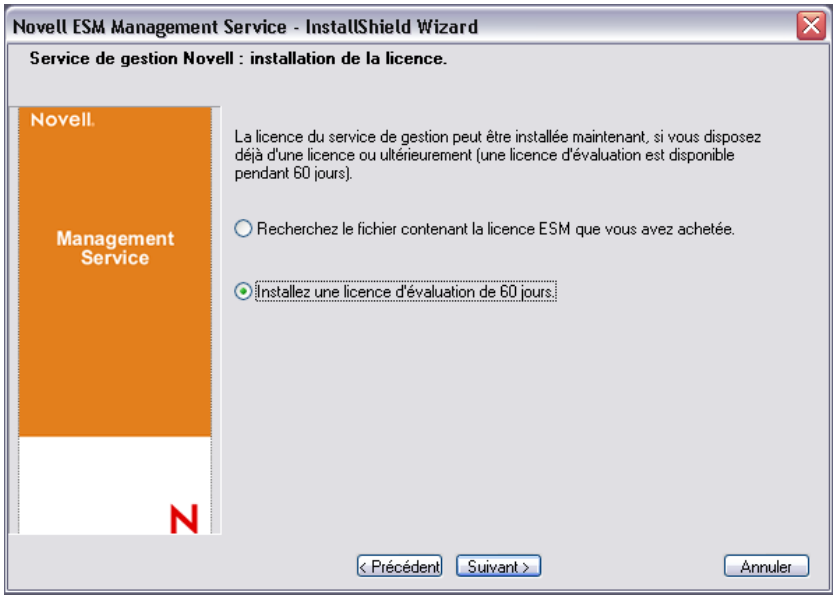
Figure 6-11 *Sélection de la base de données du service de rapport*



9 Spécifiez le nom de la base de données (le nom utilisé par défaut est STRSDB).

10 Si ZENworks Endpoint Security Management a déjà été acheté, un fichier de licence distinct est fourni. Copiez le fichier de licence sur ce serveur et localisez-le (pour des détails, reportez-vous à la page d'instructions fournie avec votre fichier de licence). Si vous n'avez pas encore acheté de licence ZENworks Endpoint Security Management, sélectionnez *Licence d'évaluation de 60 jours* pour continuer.

Figure 6-12 *Localisation du fichier de licence Novell*



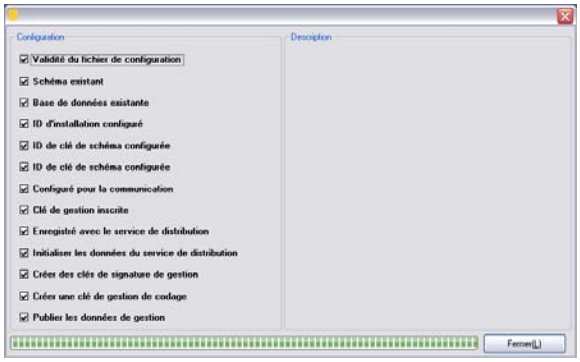
11 Dans l'écran Copier les fichiers, cliquez sur *Suivant* pour démarrer l'installation.

12 Sélectionnez les chemins d'accès des fichiers journaux, de données et d'index de la base de données du service de gestion.

13 Sélectionnez les chemins d'accès des fichiers journaux, de données et d'index de la base de données du service de rapport.

14 Le service de gestion exécute une vérification de la communication avec les bases de données SQL et le service de distribution de stratégies. Si la communication échoue, le programme d'installation vous avertit du problème. Toutes les cases doivent être cochées pour que l'installation réussisse.

Figure 6-13 *Vérification de la communication*



15 Passez l'Étape 16 et l'Étape 17 et si vous effectuez l'installation avec eDirectory comme service Annuaire.

16 Si cette installation a lieu sur un serveur membre d'un domaine utilisant un service Annuaire Active Directory ou NT Domains, le programme d'installation détecte automatiquement les données suivantes et les ajoute à l'installation via une connexion sécurisée en lecture seule :

- Nom de domaine racine ou nom de la machine
- Nom de l'administrateur du domaine ou compte de la ressource disposant des autorisations de lecture appropriées

17 Entrez le mot de passe de l'administrateur dans l'espace prévu à cet effet et cliquez sur *Test pour vérifier que la connexion peut être établie*. Si le test réussit, cliquez sur *Enregistrer*. Si le test échoue ou si le domaine correct n'est pas détecté, il doit être ajouté manuellement via la console de gestion (reportez-vous à la Section 7.2.1, « Ajout de services eDirectory », page 47).

Remarque : Le mot de passe spécifié doit être configuré de sorte à ne jamais expirer, de même que ce compte ne doit jamais être désactivé.

---

18 Le service de gestion est maintenant installé. Cliquez sur *Terminé* pour mettre fin aux vérifications de communication, puis sur *Terminer* pour fermer le programme d'installation.

6.2 Démarrage du service

Le service de gestion se lance immédiatement après l'installation, sans qu'il soit nécessaire de redémarrer le serveur. La console de gestion permet de gérer les données sur le service de gestion (reportez-vous au *Guide d'administration de ZENworks Endpoint Security Management*).

Novell recommande d'installer la console de gestion sur ce serveur. Si vous installez la console de gestion sur une autre machine, copiez le répertoire `Fichiers d'installation de ESM`, via un partage réseau ou en enregistrant le fichier sur un disque ou une clé USB, sur la machine qui hébergera la console.

Passez au Chapitre 7, « Installation de la console de gestion », page 43.

Installation de la console de gestion

7

La console de gestion peut être installée sur le serveur du service de gestion ou sur un ordinateur sécurisé disposant d'une communication directe avec le serveur du service de gestion. Plusieurs installations de console de gestion peuvent être configurées pour communiquer avec un seul service de gestion, mais il est vivement recommandé que l'accès à la console de gestion soit restreint à certains utilisateurs.

Pour des raisons de sécurité, il est recommandé d'installer la console de gestion directement sur le serveur du service de gestion.

Si vous l'installez sur un autre poste de travail, assurez-vous que les exigences suivantes sont satisfaites avant de commencer l'installation :

- ❑ Veillez à ce que le périphérique sur lequel vous installez la console de gestion réponde aux exigences suivantes :
  - Windows XP SP1, Windows XP SP2 ou Windows 2000 SP4.
  - Un processeur à 1,0 GHz est recommandé, avec un minimum de 256 Mo de RAM et 100 Mo d'espace disque disponible.
- ❑ Copiez sur l'ordinateur le dossier `Fichiers d'installation de ESM`, qui contient les certificats SSL racines des services de distribution de stratégies et de gestion, ainsi que le fichier `STInstParam.id`.
- ❑ Si vous effectuez l'installation de la console de gestion sur le serveur du service de gestion, assurez-vous que la version de Microsoft Internet Explorer est 5.5 ou supérieure.

7.1 Procédure d'installation

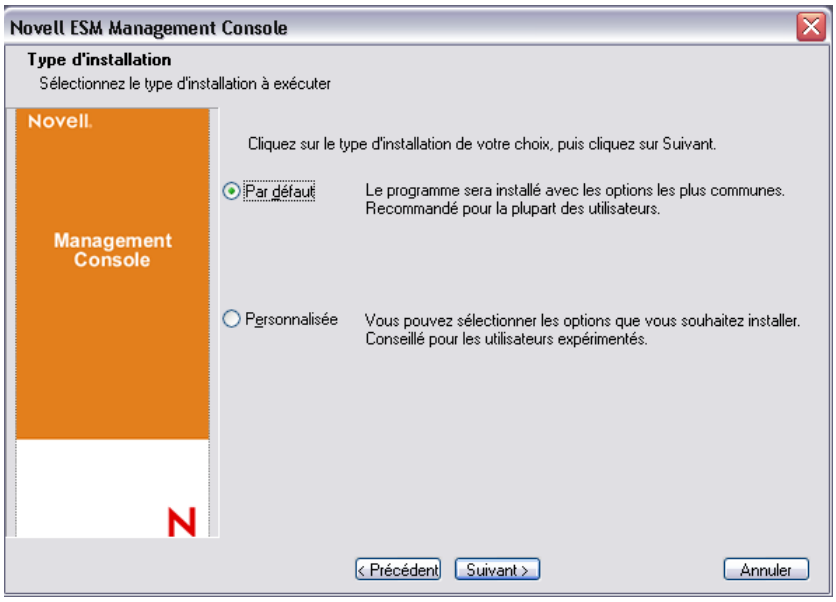
Cliquez sur *Installation de la console de gestion* dans le menu Interface d'installation.

Au démarrage, le programme d'installation vérifie que .NET Framework 3.5 et WSE 2.0 SP2, tous deux nécessaires, sont présents sur la machine. Si l'un de ces programmes ou les deux sont absents, ils sont installés automatiquement avant l'affichage de l'écran de bienvenue du programme d'installation (vous devez accepter l'accord de licence de .NET 3.5).

Pour installer la console de gestion :

1. Cliquez sur *Suivant* pour continuer.
2. Acceptez l'accord de licence, puis cliquez sur *Suivant*.
3. Sélectionnez une installation *Standard* ou *Personnalisée*.

Figure 7-1 *Installation standard ou personnalisée*



Les deux options sont présentées ci-dessous :

- Section 7.1.1, « Installation standard », page 44
- Section 7.1.2, « Installation personnalisée », page 44

7.1.1 Installation standard

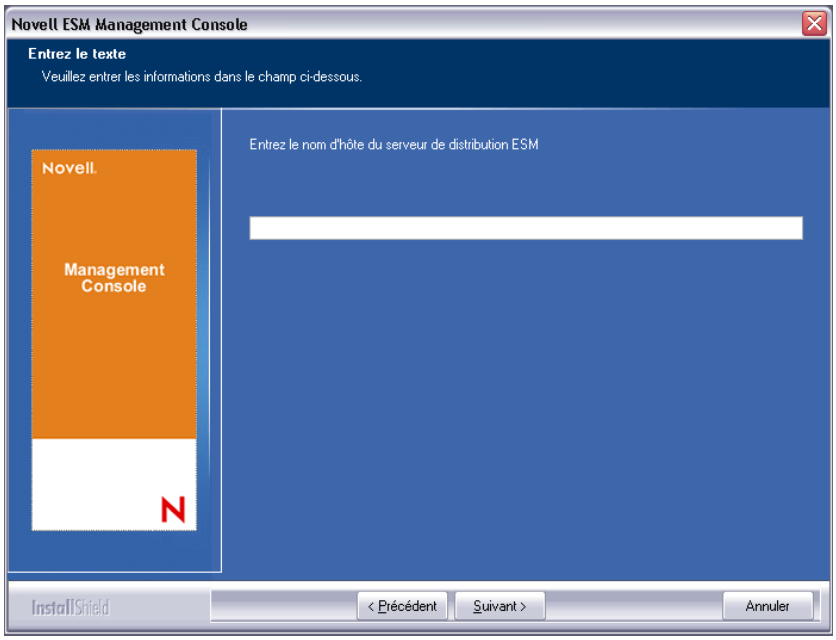
Une installation standard utilise toutes les données de serveur et SSL par défaut contenues dans le fichier `STInstParam.id` et crée le répertoire par défaut : `\Program Files\Novell\Console de gestion ESM`. Vous ne devez sélectionner aucune autre option pour l'installation de la console de gestion, à condition que le répertoire `Fichiers d'installation de ESM` se trouve sur la machine.

7.1.2 Installation personnalisée

Une installation personnalisée affiche les valeurs `STInstParam.id` par défaut utilisées dans l'installation standard et permet à l'administrateur de modifier ces informations.

1 Spécifiez le nom d'hôte du service de distribution de stratégies (ce doit être un nom de domaine pleinement qualifié si le serveur de distribution est déployé en dehors du pare-feu d'entreprise).

Figure 7-2 *Saisie du nom d'hôte du service de distribution*

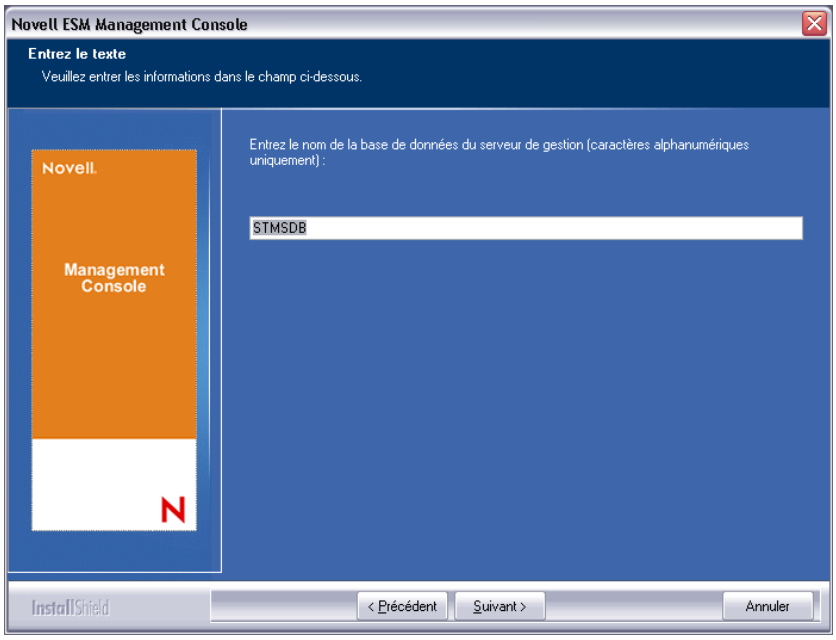


2 Spécifiez le nom d'hôte du service de gestion.

3 Spécifiez le nom d'hôte de la base de données SQL du service de gestion.

4 Spécifiez le nom de la base de données SQL du service de gestion.

Figure 7-3 *Saisie du nom de la base de données SQL du service de gestion*



5 Spécifiez le nom d'utilisateur et le mot de passe SA SQL identifiés lors de l'installation du service de gestion.

6 Sélectionnez le type de certificat SSL installé sur les services de distribution de stratégies et de gestion.

Figure 7-4 *Sélection des certificats des serveurs*

7 Sélectionnez le répertoire dans lequel la console de gestion est installée. L'emplacement par défaut est `\Program Files\Novell\Console de gestion ESM`.

Après avoir installé ZENworks Endpoint Security Management, vous devez créer et configurer un service Annuaire avant de pouvoir gérer les périphériques de votre système.

L'assistant de création de configuration du service Annuaire permet de créer une configuration de service Annuaire qui définit la portée de vos installations Endpoint Security Client. La nouvelle configuration utilise votre service Annuaire existant pour définir la limite logique à appliquer à vos installations du client basées sur les utilisateurs ou sur l'ordinateur.

L'assistant vous guide pour sélectionner le service Annuaire et les contextes qui hébergeront les comptes actuels et futurs du client.

L'assistant vous permet également de synchroniser les entrées d'annuaire présentes dans la nouvelle configuration. Cette synchronisation s'effectue en arrière-plan, vous permettant ainsi de commencer à utiliser la nouvelle configuration sans plus tarder.

Dès que vous avez installé ZENworks Endpoint Security Management, l'assistant de création de configuration du service Annuaire s'affiche automatiquement. Pour plus d'informations sur la création et la configuration du service Annuaire, reportez-vous à la section « Configuration du service Annuaire » dans le *Guide d'administration de ZENworks Endpoint Security Management*.

7.2 Démarrage de la console

Pour ouvrir la fenêtre de login de la console de gestion, cliquez sur *Démarrer > Tous les programmes > Novell > Console de gestion ESM > Console de gestion*.

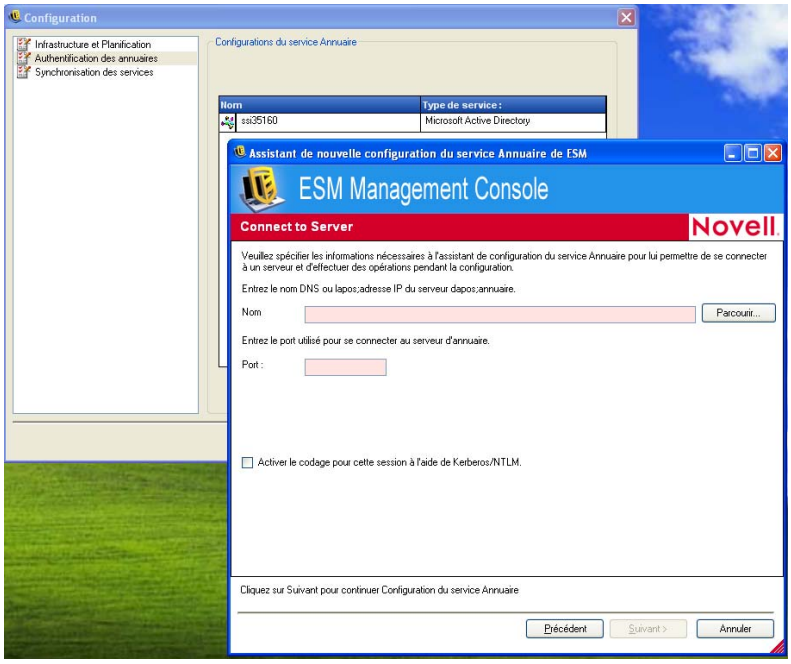
Loguez-vous à la console de gestion en entrant le nom et le mot de passe de l'administrateur. Avant de pouvoir entrer le nom d'utilisateur et le mot de passe, vous devez être connecté au domaine du service Annuaire (reportez-vous à la Section 7.2.1, « Ajout de services eDirectory », page 47). Le nom d'utilisateur doit être un utilisateur du domaine du service de gestion.

Figure 7-5 *Login à la console de gestion ZENworks Endpoint Security Management*

7.2.1 Ajout de services eDirectory

1 Cliquez sur le bouton *Options* dans l'écran de login pour afficher la fenêtre de configuration.

Figure 7-6 *Authentification des annuaires*



2 Entrez un nom convivial pour le service Annuaire et sélectionnez eDirectory dans la liste déroulante *Type de services*.

3 Dans le champ *Nom de domaine/hôte*, spécifiez l'adresse IP du serveur eDirectory et le nom de l'arborescence dans l'arborescence *Domaine*.

4 Cochez la case *Disponible pour l'authentification de l'utilisateur* pour afficher le domaine dans le menu déroulant de login.

5 Désélectionnez la case *Authentification sécurisée* dans les options *Connexion au service*.

6 Spécifiez le nom de compte au format LDAP. Par exemple : "cn=admin,o=acmeserver", cn étant l'utilisateur et o l'objet où est stocké le compte utilisateur.

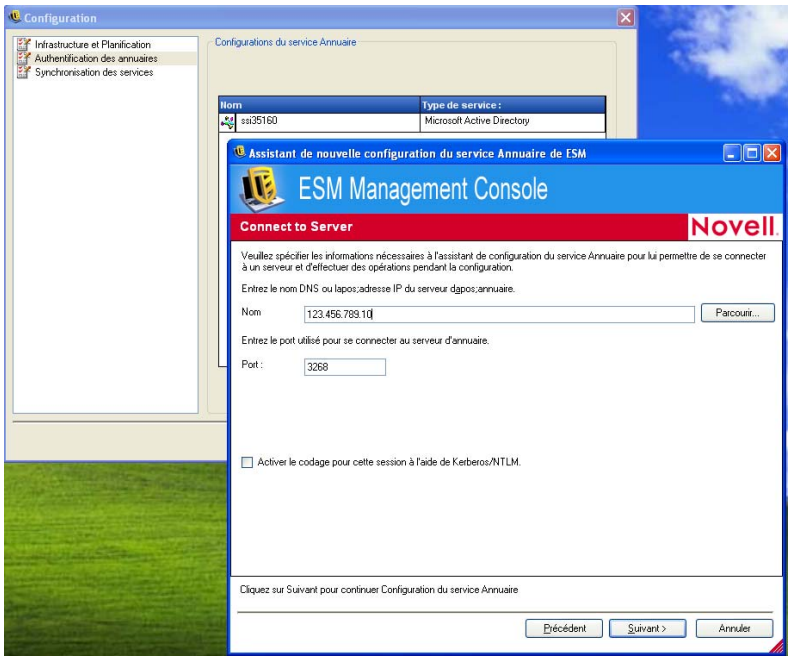
7 Spécifiez le mot de passe du compte.

Remarque : Le mot de passe doit être configuré de sorte à ne jamais expirer, de même que ce compte ne doit jamais être désactivé.

---

8 Cliquez sur *Test* pour vérifier la communication sur ce service Annuaire. En cas d'échec de communication, l'utilisateur en est informé. Toute information inexacte est corrigée, si possible, par l'interface pendant le test.

Figure 7-7 *Écran d'annuaire complété*



9 Cliquez sur *Enregistrer* pour ajouter ce service Annuaire à la base de données, puis cliquez sur *Nouveau* pour ajouter un autre service Annuaire à la base de données.

10 Cliquez sur *OK* ou sur *Annuler* pour quitter la fenêtre de configuration et revenir à l'écran de login.

Reportez-vous au *Guide d'administration de ZENworks Endpoint Security Management* pour obtenir des informations sur la configuration de l'écoute d'autres services Annuaire, dont les services Active Directory et NT Domains pris en charge.

7.2.2 Configuration des paramètres d'autorisation de la console de gestion

Autorisations se trouve dans le menu *Outils* de la console de gestion et n'est accessible que par l'administrateur principal du service de gestion et par tout autre administrateur à qui celui-ci a accordé des autorisations. Il n'est pas disponible si la console de gestion est exécutée en mode autonome. Pour des détails, reportez-vous à la rubrique Chapitre 11, « Installation de ZENworks Endpoint Security Management en mode non géré », page 77).

Les paramètres des autorisations définissent quel utilisateur ou groupe d'utilisateurs est autorisé à accéder à la console de gestion, à publier des stratégies et à modifier les paramètres des autorisations.

Pendant l'installation du serveur de gestion, un nom de compte de ressource ou d'administrateur est entré dans l'écran de configuration. Une fois le test réussi et les informations utilisateur enregistrées, les autorisations sont automatiquement accordées à cet utilisateur.

Une fois la console de gestion installée, tous les groupes d'utilisateurs du domaine reçoivent des autorisations complètes. L'utilisateur de la ressource doit supprimer l'accès de tous les groupes et utilisateurs, à l'exception de ceux devant disposer d'un accès. L'utilisateur de la ressource peut définir d'autres autorisations pour les utilisateurs désignés. Les autorisations accordées génèrent les résultats suivants :

- **Accès à la console de gestion :** l'utilisateur peut consulter des stratégies et des composants et éditer des stratégies existantes. Les utilisateurs ayant uniquement obtenu ce privilège ne seront pas autorisés à ajouter ou supprimer des stratégies ; les options relatives à la publication et aux autorisations ne sont pas disponibles.
- **Publier des stratégies :** l'utilisateur ne peut publier des stratégies que pour des utilisateurs et groupes assignés.
- **Modifier des autorisations :** l'utilisateur peut accéder aux autorisations d'autres utilisateurs ayant déjà été définis et les modifier ou encore en octroyer à de nouveaux utilisateurs.
- **Créer des stratégies :** l'utilisateur peut créer de nouvelles stratégies dans la console de gestion.
- **Supprimer des stratégies :** l'utilisateur peut supprimer n'importe quelle stratégie dans la console de gestion.

Remarque : Pour des raisons de sécurité, seul l'utilisateur de la ressource ou très peu d'administrateurs se voient accorder les autorisations de modification des autorisations et de suppression des stratégies.

Les sections suivantes contiennent davantage d'informations :

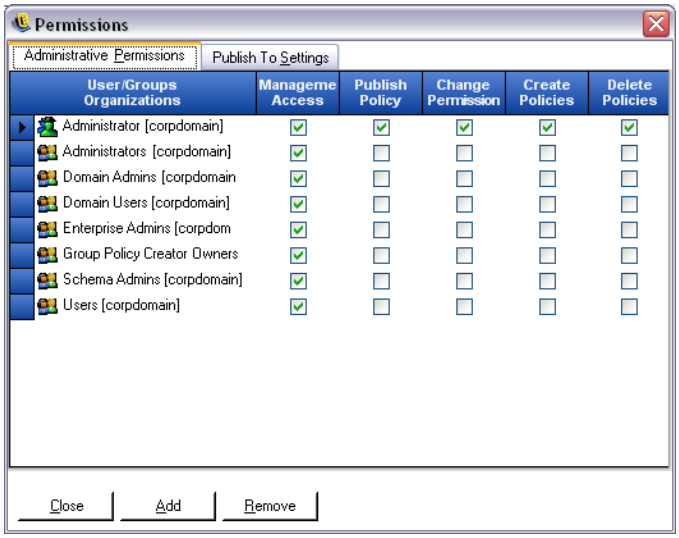
- « Configuration des autorisations administratives » page 49
- « Configuration de paramètres de publication » page 51

Configuration des autorisations administratives

1 Cliquez sur *Outils* > *Autorisations*.

Les groupes associés au domaine s'affichent.

Figure 7-8 *Fenêtre des paramètres d'autorisations de la console de gestion*



Remarque : Par défaut, tous les groupes se voient octroyer des autorisations complètes dans la console de gestion. Les administrateurs doivent immédiatement désélectionner toutes les tâches stratégiques des groupes non autorisés. L'accès à la console peut être supprimé en désactivant l'autorisation correspondante.

---

2 (Facultatif) Pour ajouter des utilisateurs et groupes à cette liste :

2a Cliquez sur le bouton *Ajouter* au bas de l'écran pour afficher la table organisationnelle.

Figure 7-9 *Table organisationnelle des paramètres d'autorisations*

2b Sélectionnez les utilisateurs et groupes appropriés dans la liste. Utilisez les touches Ctrl ou Maj pour sélectionner plusieurs utilisateurs.

2c Lorsque tous les utilisateurs et groupes ont été sélectionnés, cliquez sur le bouton *OK* pour ajouter les utilisateurs et groupes dans le tableau de l'écran des autorisations.

3 Assignez des autorisations aux utilisateurs et groupes disponibles.

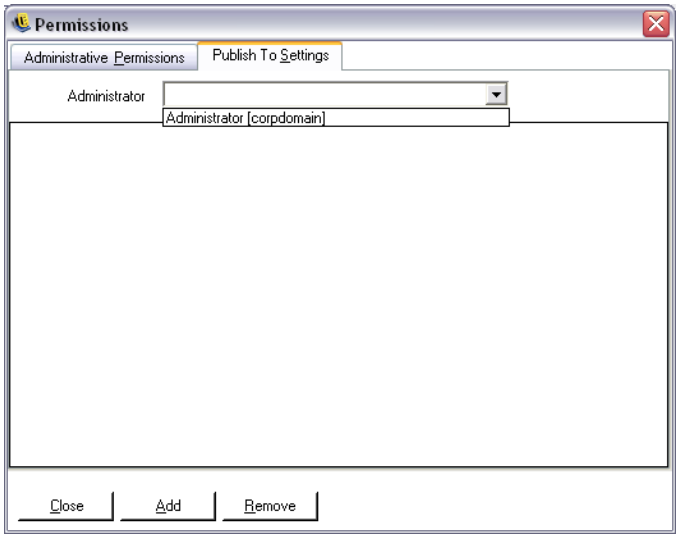
Pour supprimer un utilisateur ou groupe sélectionné, sélectionnez son nom, puis cliquez sur *Supprimer*.

Configuration de paramètres de publication

Les utilisateurs ou groupes pour lesquels l'option *Publier des stratégies* est cochée doivent se voir assigner des utilisateurs ou des groupes pour qui publier. Pour définir les paramètres de publication :

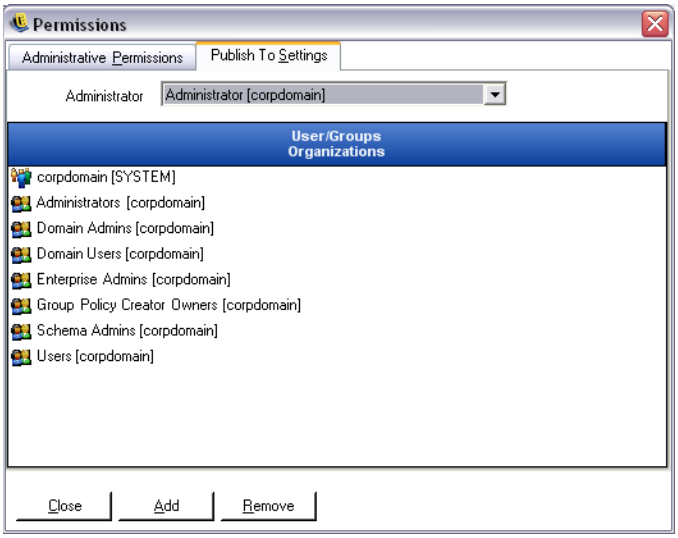
1. Cliquez sur l'onglet *Paramètres de publication.*.
2. Dans la liste déroulante, sélectionnez les utilisateurs et groupes ayant reçu l'autorisation de publication.

Figure 7-10 *Paramètres de publication*



3. Pour assigner des utilisateurs et groupes à cet utilisateur ou groupe :
   - **3a** Cliquez sur le bouton *Ajouter* au bas de l'écran pour afficher la table organisationnelle.
   - **3b** Sélectionnez les utilisateurs et groupes appropriés dans la liste. Utilisez les touches Ctrl et Maj pour sélectionner plusieurs utilisateurs.
   - **3c** Une fois tous les utilisateurs/groupes sélectionnés, cliquez sur le bouton *OK*.

Figure 7-11 *Liste de publication*



Pour supprimer un utilisateur ou groupe sélectionné, sélectionnez son nom dans la liste, puis cliquez sur *Supprimer*.

Les paramètres d'autorisations étant immédiatement mis en œuvre, l'administrateur doit simplement cliquer sur *Fermer* et accepter les changements pour retourner à l'éditeur.

Lors de l'ajout d'un nouveau service Annuaire, le compte de ressource se voit accorder des paramètres d'autorisations complètes, comme décrit ci-dessus.

7.2.3 Publication d'une stratégie

Pour publier une stratégie de sécurité avec les paramètres par défaut :

1. Cliquez sur *Créer une nouvelle stratégie*.
2. Nommez la stratégie, puis cliquez sur *Créer*.
3. Enregistrez la stratégie et cliquez sur l'onglet *Publier*.
4. Puisque les utilisateurs de Endpoint Security Client doivent s'enregistrer pour apparaître dans l'arborescence, double-cliquez sur le sommet de l'arborescence, à gauche, pour renseigner le champ de publication avec tous les groupes et utilisateurs actuels.
5. Cliquez sur *Publier* pour envoyer la stratégie au service de distribution de stratégies.

La stratégie générée de cette manière a les caractéristiques suivantes :

- Un seul emplacement (Inconnu) est créé.
- Les unités de CD/DVD-ROM sont autorisées.
- Les périphériques de stockage amovibles sont autorisés.
- Tous les ports de communication (y compris Wi-Fi) sont autorisés.
- Le paramètre de pare-feu Tous - Adaptatif (tout le trafic sortant sur les ports de la réseautique est autorisé ; le trafic entrant non sollicité est refusé) est inclus.

Pour obtenir des informations sur la création d'une stratégie de sécurité plus robuste, consultez le *Guide d'administration de ZENworks Endpoint Security Management*.

Passez au Chapitre 8, « Installation du service CLAS (Client Location Assurance Service) », page 55.

7.3 Installation du lecteur USB

Le paquetage d'installation comprend un lecteur USB Novell, qui aide l'administrateur à créer des listes de périphériques USB autorisés.

Pour installer le lecteur :

1. Cliquez sur *Installer* pour lancer l'installation
2. Dans l'écran de bienvenue, cliquez sur *Suivant* pour continuer.
3. Acceptez l'accord de licence, puis cliquez sur *Suivant*.
4. Dans l'écran des informations sur le client, entrez le nom d'utilisateur et l'organisation appropriés, puis spécifiez si tous les utilisateurs de cet ordinateur ou uniquement l'utilisateur spécifié plus haut est autorisé à accéder au logiciel.
5. Cliquez sur *Installer*.
6. Cliquez sur *Terminer*.

Pour plus d'informations sur l'utilisation du lecteur USB, reportez-vous au *Guide d'administration de ZENworks Endpoint Security Management*.

Installation du service CLAS (Client Location Assurance Service)

8

Ce serveur devrait être accessible uniquement lorsque l'utilisateur entre dans un environnement réseau contrôlé, pour garantir qu'il se trouve bien dans l'environnement identifié par ZENworks® Security Client. Des instructions sur les configurations appropriées de reprise après échec et de redondance sont fournies ci-dessous. Au besoin, le service CLAS peut être déployé sur le même serveur que celui qui héberge l'installation monoserveur ou l'installation du service de gestion multiserveur.

Installez le service CLAS sur un serveur que les noeuds d'extrémité ne pourront détecter que lorsqu'ils se trouvent dans l'environnement réseau qui exige une vérification cryptographique.

Le déploiement du service CLAS sur un contrôleur de domaine primaire n'est pas pris en charge pour des raisons à la fois de sécurité et de fonctionnalité.

Remarque : Il est recommandé de configurer (durcir) le serveur SSI de manière à désactiver les applications, services, comptes et autres options qui ne sont pas nécessaires à la finalité prévue du serveur. La procédure à suivre pour ce faire varie selon les spécificités de l'environnement local et ne peut donc pas être décrite au préalable. Les administrateurs sont invités à consulter la section appropriée de la page Web de sécurité Microsoft Technet (http://www.microsoft.com/technet/security/default.mspx). D'autres recommandations concernant le contrôle d'accès sont fournies dans le *Guide d'administration de ZENworks Endpoint Security Management*.

Afin de limiter l'accès aux seules machines approuvées, le répertoire virtuel et IIS peuvent être configurés pour utiliser des listes de contrôle d'accès (ACL). Reportez-vous aux articles ci-dessous :

- Accorder et refuser l'accès aux ordinateurs (http://www.microsoft.com/technet/prodtechnol/windows2000serv/default.mspx)
- Restreindre l'accès au site par l'adresse IP ou le nom de domaine (http://support.microsoft.com/default.aspx?scid=kb%3BEN-US%3BQ324066)
- FAQ IIS : restrictions de l'adresse IP 2000 et du nom de domaine (http://www.iisfaq.com/default.aspx?View=A136&P=109)
- Utilisation du filtrage de paquets IIS (http://www.15seconds.com/issue/011227.htm)

Pour des raisons de sécurité, il est vivement recommandé de supprimer les dossiers par défaut suivants de toute installation IIS :

- `IISHelp`
- `IISAdmin`
- `Scripts`
- `Printers`

Nous vous recommandons également d'utiliser IIS Lockdown Tool 2.1, disponible sur microsoft.com (http://www.microsoft.com/technet/security/tools/locktool.mspx).

La version 2.1 de cet outil repose sur des modèles fournis pour les principaux produits Microsoft basés dépendant de IIS. Sélectionnez le modèle qui correspond le mieux au rôle de ce serveur. En cas de doute, le modèle de serveur Dynamic Web est recommandé.

Assurez-vous que les exigences suivantes sont satisfaites avant de commencer l'installation :

- ❑ Vérifiez la résolution de nom de serveur entre le service de gestion et le service de distribution de stratégies : vérifiez que l'ordinateur cible sur lequel le service de gestion est installé peut exécuter une commande ping sur le nom de serveur du service de distribution (NETBIOS si le service de distribution est configuré à l'intérieur du pare-feu du réseau, nom de domaine complet s'il est installé à l'extérieur, dans la zone démilitarisée).
- ❑ Activez ou installez Microsoft Internet Information Services (IIS) et assurez-vous qu'ASP.NET est activé.

  Important : Ne cochez pas la case *Requérir un canal sécurisé (SSL)* sur la page Communications sécurisées (dans l'utilitaire Microsoft Gestion de l'ordinateur, développez *Services et applications* > *Gestionnaire des services ISS* > *Sites Web* > cliquez avec le bouton droit de la souris sur *Site Web par défaut* > cliquez sur *Propriétés* > cliquez sur l'onglet *Sécurité de répertoire* > cliquez sur le bouton *Éditer* dans la zone de groupe Communications sécurisées). L'activation de cette option interrompt la communication entre le serveur ZENworks Endpoint Security Management et le client ZENworks Endpoint Security sur le noeud d'extrémité.

Cliquez sur *Installation du service CLAS* dans le menu Interface d'installation. L'installation du service CLAS démarre.

Au lancement, le programme d'installation vérifie que tous les logiciels requis sont présents sur le serveur. Si un logiciel est absent, il est automatiquement installé avant l'affichage de l'écran de bienvenue du programme d'installation (vous devrez éventuellement accepter les accords de licence des logiciels supplémentaires). Si MDAC (Microsoft Data Access Components) 2.8 n'est pas installé, le serveur doit redémarrer après cette installation, avant que l'installation de ZENworks Endpoint Security Management puisse continuer. Si vous utilisez Windows Server 2003, ASP.NET 2.0 est configuré pour être exécuté par le programme d'installation.

8.1 Procédure d'installation

Pour installer le service CLAS et générer une clé de licence :

1. Cliquez sur *Suivant* dans l'écran de bienvenue pour continuer.
2. Acceptez l'accord de licence, puis cliquez sur *Suivant*.
3. Le programme d'installation copie les fichiers dans le répertoire par défaut :`\Program Files\Novell\ESM CLAS.`
4. L'installation du service CLAS génère deux clés : la clé privée et la clé publique. Le fichier de clé publique peut être stocké sur le Bureau ou dans un autre répertoire. Si vous souhaitez stocker le fichier de clé publique dans un autre répertoire, cliquez sur *Oui* et localisez le dossier souhaité. Cliquez sur *Non* pour accepter l'option par défaut. Le fichier de clé publique sera stocké avec le fichier de clé privée.
5. Cliquez sur *Terminer* pour fermer le programme d'installation.

La clé publique doit être accessible par le service de gestion.

8.2 Installations de CLAS avec reprise après échec

Plusieurs itérations du service CLAS peuvent être installées sur les serveurs de l'entreprise, pour assurer la vérification cryptographique d'autres emplacements ou pour garantir qu'en cas d'arrêt du serveur CLAS primaire, l'emplacement puisse toujours être vérifié.

Dans le second scénario, la clé privée est localisée sur la base d'une URL au lieu d'une adresse IP. Un bloc de serveurs peut dès lors être configuré pour partager la même URL. Le service CLAS peut être soit installé sur un seul serveur, puis l'image du serveur peut être copiée sur chacun des autres serveurs, soit installé sur chaque serveur séparément et les clés privées et publiques peuvent être recopiées sur les autres serveurs. TOUS les serveurs d'un bloc URL doivent avoir des clés privées et publiques identiques.

8.3 Transfert de la clé publique au service de gestion

Une fois l'installation terminée, la clé publique générée pour un transfert à Endpoint Security Client via la stratégie de sécurité est située dans le répertoire `\Program Files\Novell\Novell ESM CLAS` du serveur. La clé publique est identifiée par son nom de fichier, `publickey` que vous pouvez modifier si vous le souhaitez.

Ce fichier doit être copié et transféré au service de gestion (à n'importe quel emplacement au sein de ce service), ce qui permettra à la console de gestion d'accéder à la clé et de pouvoir la distribuer à tous les clients Endpoint Security Client par le biais d'une stratégie de sécurité. Le fichier de `clé publique` peut être chargé sur un ordinateur exécutant la console de gestion ZENworks Endpoint Security Management.

Passez au Chapitre 9, « Installation de Endpoint Security Client 3.5 », page 59.

Installation de Endpoint Security Client 3.5

9

Utilisez la version 3.5 de Novell ZENworks Endpoint Security Client pour les clients Windows XP (SP1 et SP2) et Windows 2000 SP4. Cliquez sur le programme d'installation approprié de *ZENworks Security Client* dans le menu Interface d'installation. L'installation de Endpoint Security Client démarre. Les pages suivantes décrivent à la fois l'installation de base et l'installation MSI.

- L'installation de base installe Endpoint Security Client 3.5 uniquement sur la machine actuelle.
- L'installation MSI lance le programme d'installation en mode Administratif (`/a`) et crée un paquetage MSI pour le logiciel. Ce paquetage peut ensuite être distribué à l'initiative du serveur ou rendu disponible de toute autre manière à un emplacement spécifique du réseau, avec les entrées utilisateur requises préconfigurées. Cela permet aux utilisateurs individuels d'installer le logiciel avec les valeurs de serveur prédéfinies.

9.1 Installation de base de Endpoint Security Client 3.5

Cette procédure installe Endpoint Security Client 3.5 uniquement sur la machine actuelle.

Vérifiez que tous les correctifs de sécurité Microsoft et les logiciels antivirus sont installés et à jour.

Installez les certificats racines SSL du service de gestion sur la machine locale (`ESM-MS.cer` ou le certificat d'entreprise).

Remarque : Nous vous recommandons de fermer tous les logiciels antivirus/anti-espions susceptibles d'interagir avec des fonctions de registre valides pendant l'installation de Endpoint Security Client 3.5.

---

1. Cliquez sur *Suivant* dans l'écran de bienvenue pour continuer.
2. Acceptez l'accord de licence, puis cliquez sur *Suivant*.
3. Entrez un mot de passe d'installation. Cela empêche l'utilisateur de désinstaller Endpoint Security Client 3.5 via l'outil *Ajout/suppression de programmes* (recommandé).

Figure 9-1 *Mot de passe de désinstallation*

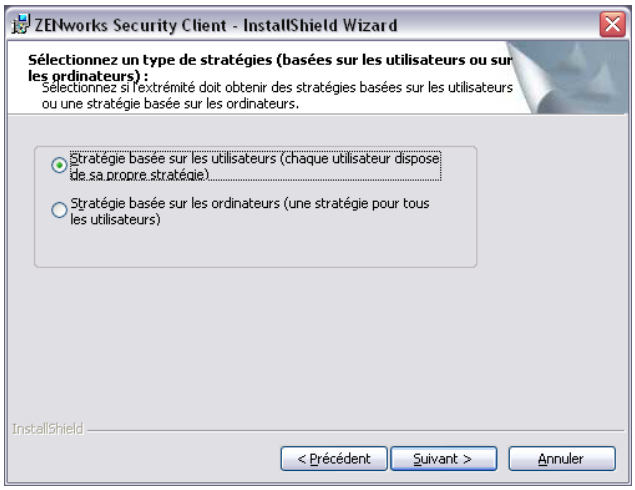
4 Sélectionnez la façon dont les stratégies seront reçues (à partir du service de distribution pour les clients gérés ou récupérées localement pour les configurations non gérées - [voir Chapitre 11, « Installation de ZENworks Endpoint Security Management en mode non géré », page 77 pour des détails sur les clients non gérés]).

Figure 9-2 *Paramètres de gestion*

5 Spécifiez les informations relatives au service de gestion.

6 Spécifiez si les stratégies doivent être reçues pour les utilisateurs ou pour la machine (stratégies basées sur la machine).

Figure 9-3 *Stratégies basées sur les utilisateurs ou sur la machine*



7 Cliquez sur *Installer*.

Une fois le logiciel installé, l'utilisateur est invité à redémarrer sa machine.

Remarque : Vous pouvez éventuellement copier le certificat du service de gestion dans un dossier situé au même emplacement que `setup.exe` avant de lancer l'installation. Le certificat est alors installé automatiquement sur la machine (p. ex., pour tous les utilisateurs). Le même résultat peut être obtenu avec le fichier license.`dat` émis par Novell.

9.2 Installation MSI

Cette procédure crée un paquetage MSI pour le client Endpoint Security Client 3.5. Ce paquetage est utilisé par un administrateur système pour publier l'installation vers un groupe d'utilisateurs via une stratégie Active Directory ou par toute autre méthode de distribution de logiciels.

Pour créer le paquetage MSI :

Si vous utilisez une installation à partir du CD ou du programme d'installation principal ISO et si vous ne prévoyez pas d'utiliser des variables de ligne de commande (reportez-vous à la Section 9.2.1, « Variables de ligne de commande », page 64) :

1 Introduisez le CD et attendez que le programme d'installation principal se lance.
2 Cliquez sur *Installation d'un produit*.
3 Cliquez sur *Client de sécurité*.
4 Cliquez sur *Créer un paquetage MSI pour ZSC*.

Si vous utilisez simplement le fichier `setup.exe`pour effectuer l'installation (l'exécutable se trouve sur le CD sous `D:\ESM32\ZSC)`, commencez comme suit :

1 Cliquez avec le bouton droit sur `setup.exe`.
2 Cliquez sur *Créer un raccourci*.
3 Cliquez avec le bouton droit de la souris sur l'élément, puis cliquez sur *Propriétés*.

4 A la fin du champ Cible, après les guillemets, cliquez une fois sur la barre d'espacement, puis tapez `/a`.

   Exemple :`"C:\Documents and Settings\euser\Desktop\CL-Release-3.2.455\setup.exe" /a`

   Plusieurs variables de ligne de commande sont disponibles pour l'installation MSI, reportez-vous à la Section 9.2.1, « Variables de ligne de commande », page 64 pour plus de détails.

5 Cliquez sur *OK*.

6 Double-cliquez sur le raccourci pour lancer le programme d'installation MSI.

Lorsque l'installation commence :

1 Cliquez sur *Suivant* dans l'écran de bienvenue pour continuer.

2 Acceptez l'accord de licence, puis cliquez sur *Suivant*.

3 Spécifiez si un mot de passe de désinstallation est requis (recommandé) et entrez le mot de passe.

4 Sélectionnez la façon dont les stratégies seront reçues (à partir du service de distribution pour les clients gérés ou récupérées localement pour les configurations non gérées). Si vous avez choisi des clients gérés :

   - Spécifiez les informations relatives au service de gestion (nom de domaine complet ou NETBIOS selon les éléments qui ont été entrés lors de l'installation du service de gestion).
   - Spécifiez si les stratégies seront basées sur les utilisateurs ou sur la machine.

5 (Facultatif) Spécifiez une adresse électronique dans le champ prévu à cet effet pour recevoir une notification en cas d'échec de l'installation.

6 Spécifiez l'emplacement réseau dans lequel l'image MSI est créée ou localisez cet emplacement en cliquant sur le bouton *Changer*.

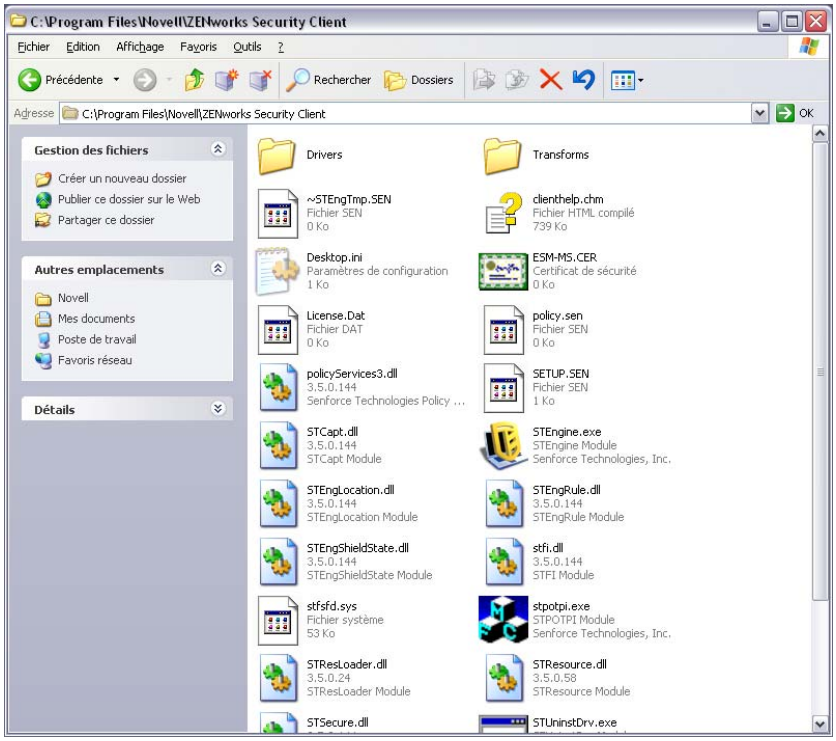
Figure 9-4 *Sélection de l'emplacement réseau de l'image MSI*

7 Cliquez sur *Installer* pour créer l'image MSI.

8 Localisez l'image MSI créée et ouvrez le dossier "`\program files\Novell\ZENworks Security Client\`"

9 Copiez le certificat SSL du service de gestion (`ESM-MS.cer` ou le certificat d'entreprise) et la clé de licence Novell dans ce dossier, en remplaçant les fichiers par défaut de 0 Ko qui s'y trouvent déjà. Le certificat SSL ESM-MS est disponible dans le dossier `Fichiers d'installation de ZENworks Endpoint Security Management`. La clé de licence est envoyée séparément par courrier électronique (si vous utilisez une copie d'évaluation de 30 jours, aucune clé de licence n'est requise à ce stade).

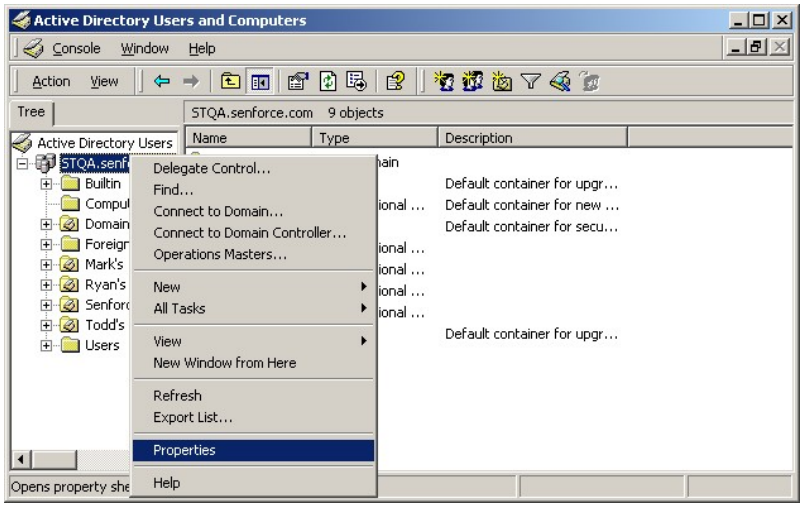
Figure 9-5 *Remplacement des fichiers par défaut dans le paquetage MSI*



Pour configurer la distribution du paquetage MSI aux groupes d'utilisateurs comme Stratégie de groupe :

1 Ouvrez *Outils d'administration - Utilisateurs et ordinateurs Active Directory* et ouvrez propriétés dans *Domaine racine* ou *Unité organisationnelle*.

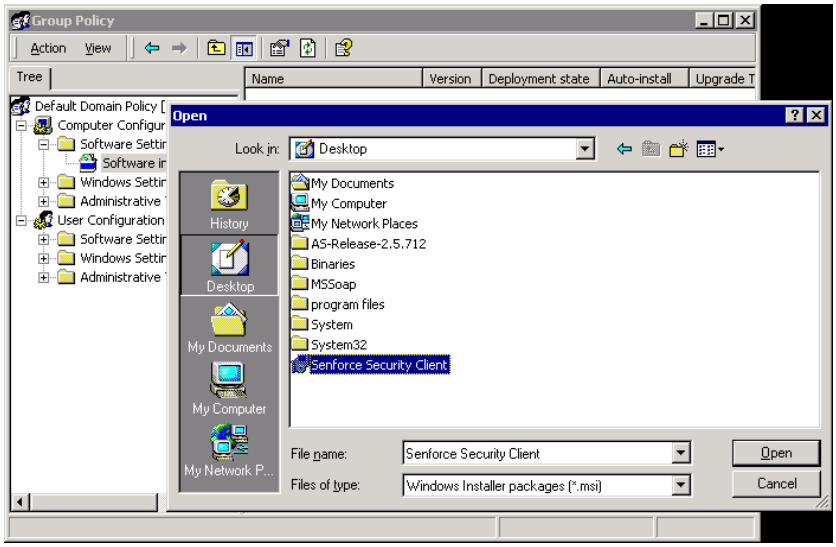
Figure 9-6 *Ouverture des propriétés dans le domaine racine ou dans l'unité organisationnelle*



2 Cliquez sur l'onglet *Stratégie de groupe*, puis sur *Éditer*.

3 Ajoutez le paquetage MSI à Configuration de l'ordinateur.

Figure 9-7 *Sélection du paquetage MSI à ajouter*



9.2.1 Variables de ligne de commande

Des variables de ligne de commande sont disponibles pour une installation MSI. Ces variables doivent être définies dans le raccourci de l'exécutable configuré pour fonctionner en mode administrateur. Pour utiliser une variable, entrez la ligne de commande suivante dans le raccourci MSI :

`"...\setup.exe" /a /V"variables"`. Entrez entre guillemets l'une des commandes ci-dessous. Si vous spécifiez plusieurs variables, séparez-les par un espace simple.

Exemple : `setup.exe /a /V"STDRV=stateful STBGL=1"` crée un paquetage MSI dans lequel Endpoint Security Client 3.5 démarre avec l'état Tous - Avec état avec liste blanche stricte.

Remarque : Le démarrage avec état peut entraîner certains problèmes d'interopérabilité (retards d'adresse DHCP, problèmes d'interopérabilité du réseau Novell, etc.).

Les variables de ligne de commande suivantes sont disponibles :

Tableau 9-1 *Variables de ligne de commande*

Variable de ligne de commande	Description	Remarques
STDRV=stateful	Pilote NDIS avec l'état Tous - Avec état au démarrage.	Remplace l'état par défaut du pilote NDIS Tous - Ouvert par Tous - Avec état et autorise ainsi tout le trafic réseau au démarrage, jusqu'à ce que le client Endpoint Security Client 3.5 ait déterminé son emplacement.
/qn	Installation silencieuse.	Permet de suspendre le processus d'installation MSI standard. Endpoint Security Client 3.5 s'active au prochain redémarrage de l'utilisateur.
STRBR=ReallySuppress	Pas de redémarrage après l'installation.	L'application de la sécurité et l'auto-défense du client ne sont pas entièrement fonctionnelles tant que l'ordinateur n'a pas redémarré.
STBGL=1	Mise en œuvre stricte de la liste blanche dans le contrôle des applications.	Une stratégie qui identifie l'application sur la liste blanche distribuée avec cette stratégie DOIT être créée.
STUPGRADE=1	Mise à niveau de Endpoint Security Client 3.5	À utiliser lors de la mise à niveau de Endpoint Security Client.
STUNINSTALL=1	Désinstallation de Endpoint Security Client 3.5	À utiliser lors de la désinstallation de Endpoint Security Client 3.5.
STUIP=”mot de passe”	Désinstallation avec mot de passe	À utiliser lorsqu'un mot de passe de désinstallation est actif.
STNMS=”Nom du service de gestion”	Changement du nom du service de gestion.	Change le nom du service de gestion de Endpoint Security Client 3.5.
POLICYTYPE=1	Remplacement des stratégies Endpoint Security Client 3.5 par des stratégies basées sur la machine.	Permet de changer les stratégies Endpoint Security Client installées par MSI afin d'accepter des stratégies basées sur la machine plutôt que sur les utilisateurs.
POLICYTYPE=2	Remplacement des stratégies Endpoint Security Client 3.5 par des stratégies basées sur les utilisateurs.	Permet de changer les stratégies Endpoint Security Client installées par MSI afin d'accepter des stratégies basées sur les utilisateurs plutôt que sur la machine.
STVA=”Nom de l'adaptateur”	Ajout d'un adaptateur virtuel.	Permet d'activer le contrôle de stratégies sur un adaptateur virtuel

Variable de ligne de commande	Description	Remarques
/L*v c:\log.txt	Activation de la consignation.	Permet d'activer la consignation lors de l'installation. Sinon, cette opération doit être effectuée via les outils de diagnostic de Endpoint Security Client (reportez-vous au manuel de l'administrateur).

9.2.2 Distribution d'une stratégie avec le paquetage MSI

La stratégie par défaut incluse lors de l'installation MSI peut être remplacée par une stratégie configurée pour l'entreprise. Pour distribuer une stratégie spécifique avec l'image MSI :

1. Créez une stratégie à distribuer à tous les utilisateurs via la console de gestion (reportez-vous au *Guide d'administration de ZENworks Endpoint Security Management* pour obtenir des détails sur la création de stratégies).
2. Exportez la stratégie, enregistrez-la sous `policy.sen`.

   Remarque : Toutes les stratégies distribuées de cette manière (non gérée) doivent être nommées `policy.sen` pour être acceptées par Endpoint Security Client 3.5. Les stratégies dont le nom n'est pas `policy.sen` ne sont pas implémentées par Endpoint Security Client 3.5.
3. Ouvrez le dossier vers lequel vous avez exporté la stratégie et copiez les fichiers `policy.sen` et `setup.sen`.
4. Localisez l'image MSI créée et ouvrez le dossier `"\program files\Novell\ZENworks Security Client\"`
5. Collez les fichiers `policy.sen` et `setup.sen` dans ce dossier. Ils remplaceront ainsi les fichiers `policy.sen` et `setup.sen` par défaut.

9.2.3 Installation de Endpoint Security Client 3.5 par l'utilisateur à partir d'un paquetage MSI

Lorsque l'utilisateur se réauthentifie auprès du domaine (par un redémarrage de sa machine), le paquetage d'installation MSI s'exécute avant qu'il se logue. Une fois l'installation effectuée, la machine redémarre et l'utilisateur est autorisé à se loguer à la machine. Endpoint Security Client 3.5 est installé et exécuté sur la machine.

9.3 Exécution de Endpoint Security Client 3.5

Endpoint Security Client 3.5 s'exécute automatiquement au démarrage du système. Pour plus d'informations sur Endpoint Security Client 3.5, reportez-vous au *Guide de l'utilisateur de ZENworks Endpoint Security Client 3.5*.

Le guide de l'utilisateur peut être distribué à tous les utilisateurs pour les aider à mieux comprendre le fonctionnement de leur nouveau logiciel de sécurisation des noeuds d'extrémité.

Installation de ZENworks Endpoint Security Client 4.0

10

Novell® ZENworks® Endpoint Security Client 4.0 est une version client prenant en charge Microsoft Windows Vista avec Support Pack 1 s'exécutant en mode 32 bits et Windows Server 2008 s'exécutant également en mode 32 bits. Endpoint Security Client 4.0 utilise le serveur et la console de gestion de ZENworks Endpoint Security Management 3.5. Windows XP peut désormais être géré avec le client 3.5 et Windows Vista avec le client 4.0.

Les pages suivantes décrivent à la fois l'installation de base et l'installation MSI.

L'installation de base installe Endpoint Security Client 4.0 uniquement sur la machine actuelle.

L'installation MSI lance le programme d'installation en mode Administratif (`/a`) et crée un paquetage MSI pour le logiciel. Ce paquetage peut ensuite être distribué ou mis à disposition à un emplacement spécifique du réseau, avec les entrées utilisateur requises préconfigurées. Cela permet aux utilisateurs individuels d'installer le logiciel avec les valeurs de serveur prédéfinies.

10.1 Installation de base de Endpoint Security Client 4.0

Cette procédure installe ZENworks Endpoint Security Client 4.0 uniquement sur la machine actuelle.

Conditions préalables :

- Vérifiez que tous les correctifs de sécurité Microsoft et les logiciels antivirus sont installés et à jour. Le logiciel Endpoint Security Client 4.0 peut être installé sous Windows Vista en exécutant le Support Pack 1 et sous Windows Server 2008, les deux s'exécutant en mode 32 bits.
- Novell recommande de fermer tous les logiciels antivirus/anti-espions susceptibles d'interagir avec des fonctions de registre valides pendant l'installation de Endpoint Security Client 4.0.
- Le client Endpoint Security Client géré requiert une connexion sécurisée SSL avec le composant de service ZENworks Endpoint Security Management. Si vous avez sélectionné « Certificats auto-signés » pendant l'installation du service de gestion ou l'installation monoserveur, le certificat du noeud d'extrémité exécutant le client de sécurité doit être installé dans le contexte approprié (de préférence, celui de l'ordinateur local).

  Pour effectuer cette opération automatiquement, placez le fichier `ESM-MS.cer` dans le dossier avec le fichier `Setup.exe` du programme d'installation de Endpoint Security Client. Accessoirement, vous pouvez copier l'ensemble du dossier `Fichiers d'installation`

`de ESM` de l'installation du service de gestion (ou de l'installation monoserveur) dans le dossier avec le programme d'installation Endpoint Security Client `Setup.exe`. (Vérifiez que le fichier `ESM-MS.cert` se trouve dans le dossier `Fichiers d'installation de ESM` et que le dossier porte bien le nom `Fichiers d'installation de ESM`). Le certificat est alors installé automatiquement sur la machine (p. ex., pour tous les utilisateurs). Le même résultat peut être obtenu avec le fichier license.`dat` émis par Novell.

Sélectionnez le répertoire d'installation approprié de *ZENworks Security Client* dans le menu Interface d'installation.

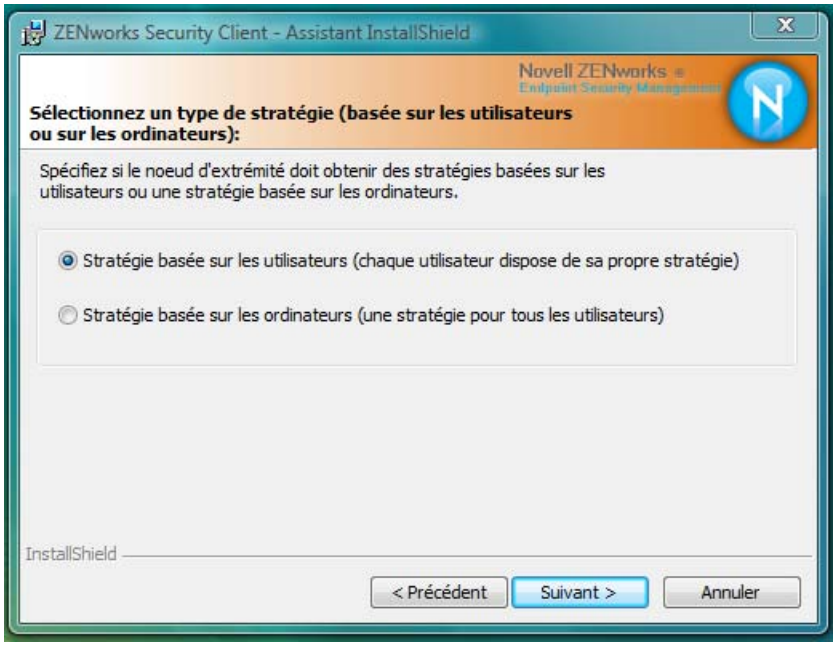
1. Double-cliquez sur `Setup.exe` pour lancer le processus d'installation.
2. Sélectionnez la langue d'installation, puis cliquez sur *OK*.

   Les langues disponibles sont les suivantes :

   - Chinois simplifié
   - Chinois traditionnel
   - Anglais (par défaut)
   - Français
   - Allemand
   - Italien
   - Japonais
   - Portugais
   - Espagnol traditionnel
3. Avant de pouvoir installer Endpoint Security Client 4.0, votre ordinateur doit disposer de Microsoft Web Services Enhancements (WSE) 2.0 avec Service Pack 3 et Microsoft Visual C++ 2008. Si le processus d'installation ne détecte pas ces composants, cet écran s'affiche. Cliquez sur *Installer* pour installer ces composants requis.
4. Si ce n'est déjà fait, désactivez les logiciels antivirus et anti-espion avant de cliquer sur *Suivant* dans l'écran de bienvenue.
5. Acceptez l'accord de licence, puis cliquez sur *Suivant*.

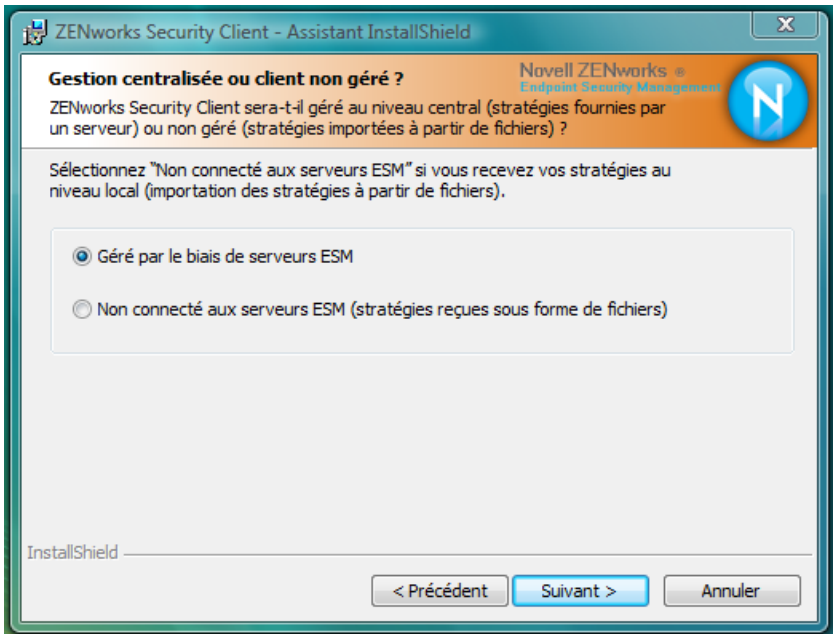
6 Sélectionnez *Exiger un mot de passe de désinstallation*. Cela empêche l'utilisateur de désinstaller Endpoint Security Client 4.0 (recommandé).

7 Ajoutez un mot de passe de désinstallation, confirmez-le, puis cliquez sur *Suivant*.



8 Sélectionnez un type de stratégie (une stratégie basée sur les utilisateurs dans laquelle chaque utilisateur dispose de sa propre stratégie ou une stratégie basée sur l'ordinateur dans laquelle une stratégie s'applique à tous les utilisateurs). Cliquez sur *Suivant*.

Remarque : sélectionnez Stratégie basée sur les utilisateurs si votre réseau utilise eDirectory comme service Annuaire. eDirectory ne prend pas en charge les stratégies basées sur l'ordinateur.



9 Sélectionnez le mode de réception des stratégies (à partir des serveurs ESM pour les clients gérés ou récupérées localement pour les configurations non gérées, en mode autonome). Cliquez sur *Suivant*.

Pour plus d'informations sur une installation non gérée, reportez-vous à la rubrique Chapitre 11, « Installation de ZENworks Endpoint Security Management en mode non géré », page 77.

10 (Facultatif) Si vous avez sélectionné *Géré par le biais de serveurs ESM*à l'Étape 9, tapez le nom du serveur prenant en charge le service de gestion.

Le nom de serveur entré doit correspondre au nom « Délivré à » fourni dans le certificat de racine approuvée utilisé sur le serveur où vous avez installé le service de gestion ZENworks Endpoint Security ou le monoserveur. Il s'agit du nom NETBIOS ou du nom de domaine complet du serveur exécutant le composant de service ZENworks Endpoint Security Management. Une fois entré, cliquez sur *Suivant*.

11 Cliquez sur *Installer* pour lancer l'installation.

12 Une fois le logiciel installé, redémarrez la machine lorsque vous y êtes invité.

Pour obtenir une liste des fonctions qui ne sont pas disponibles pour la version 4.0 du client pour Vista, reportez-vous à la section Section 10.4, « Fonctionnalités non prises en charge dans la version 4.0 de Endpoint Security Client », page 75.

10.2 Installation MSI

Cette procédure crée un paquetage MSI pour le client Endpoint Security Client 4.0. Ce paquetage est utilisé par un administrateur système pour publier l'installation vers un groupe d'utilisateurs via une stratégie Active Directory ou par toute autre méthode de distribution de logiciels.

10.2.1 Utilisation du programme d'installation principal

Si vous effectuez une installation à partir du CD ou du programme d'installation principal ISO et si vous ne prévoyez pas d'exécuter des variables de ligne de commande :

1. Introduisez le CD et attendez que le programme d'installation principal se lance.
2. Cliquez sur *Installation d'un produit*.
3. Cliquez sur *Client de sécurité*.
4. Cliquez sur *Créer un paquetage MSI pour ZSC*.
5. Passez à la section Section 10.2.3, « Finalisation de l'installation », page 72.

10.2.2 Utilisation du fichier Setup.exe

Si vous n'utilisez que le fichier `setup.exe` pour effectuer l'installation :

1. Cliquez avec le bouton droit sur `setup.exe`.

   Le fichier exécutable se trouve sur le CD à l'emplacement `D:\ESM32\ZSC`.
2. Cliquez sur *Créer un raccourci*.
3. Cliquez avec le bouton droit de la souris sur l'élément, puis cliquez sur *Propriétés*.
4. À la fin du champ *Cible*, après les guillemets, appuyez sur la barre d'espacement pour insérer un espace, puis tapez `/a`.

   Exemple :`"C:\Documents and Settings\euser\Desktop\CL-Release-3.2.455\setup.exe" /a`

   Plusieurs variables de ligne de commande sont disponibles pour l'installation MSI. Reportez-vous à la section Section 9.2.1, « Variables de ligne de commande », page 64 pour plus d'informations.
5. Cliquez sur *OK*.
6. Double-cliquez sur le raccourci pour lancer le programme d'installation MSI.
7. Passez à la section Section 10.2.3, « Finalisation de l'installation », page 72.

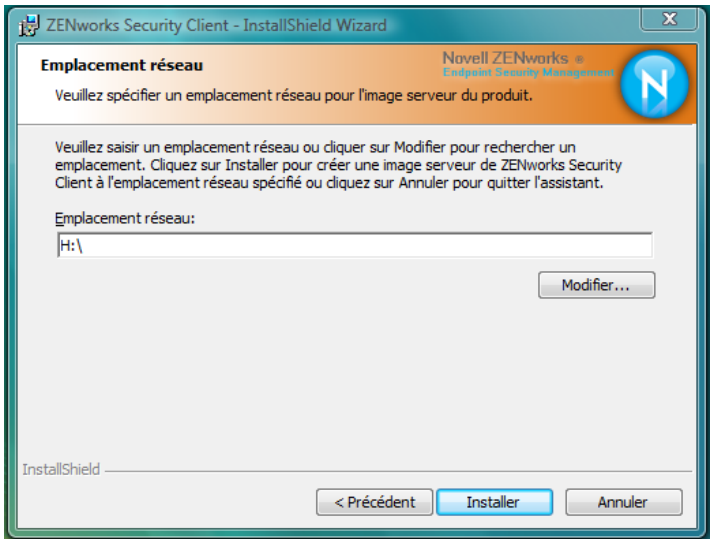
10.2.3 Finalisation de l'installation

Effectuez la procédure de la section Utilisation du programme d'installation principal ou Utilisation du fichier Setup.exe, puis suivez les étapes suivantes pour terminer l'installation du client.

1. Cliquez sur *Suivant* dans l'écran de bienvenue pour continuer.
2. Sélectionnez *Exiger un mot de passe de désinstallation* (recommandé), puis entrez le mot de passe. Cliquez sur *Suivant*.

   Remarque : si vous désinstallez le client Endpoint Security Management à l'aide d'un paquetage MSI, vous devez spécifier le mot de passe de désinstallation via les propriétés MSI (voir section Tableau 10-1 page 73).
3. Sélectionnez un type de stratégie (une stratégie basée sur les utilisateurs dans laquelle chaque utilisateur dispose de sa propre stratégie ou une stratégie basée sur l'ordinateur dans laquelle une stratégie s'applique à tous les utilisateurs). Cliquez sur *Suivant*.

   Remarque : sélectionnez Stratégie basée sur les utilisateurs si votre réseau utilise eDirectory comme service Annuaire. eDirectory ne prend pas en charge les stratégies basées sur l'ordinateur.
4. Sélectionnez le mode de réception des stratégies (à partir des serveurs ESM pour les clients gérés ou récupérées localement pour les configurations non gérées, en mode autonome).
5. (Facultatif) Si vous avez sélectionné*Géré par le biais de serveurs ESM* à l'Étape 4 :
   - Le nom de serveur entré doit correspondre au nom « Délivré à » fourni dans le certificat de racine approuvée utilisé sur le serveur où vous avez installé le service de gestion ZENworks Endpoint Security ou le monoserveur. Il s'agit du nom NETBIOS ou du nom de domaine complet du serveur exécutant le composant de service ZENworks Endpoint Security Management.
6. (Facultatif) Spécifiez une adresse électronique dans le champ prévu à cet effet pour recevoir une notification en cas d'échec de l'installation.
7. Spécifiez l'emplacement réseau où vous souhaitez créer l'image MSI ou localisez et sélectionnez cet emplacement en cliquant sur le bouton *Changer*.



8 Cliquez sur *Installer* pour créer l'image MSI. Cliquez sur *Terminer* pour fermer le programme d'installation.

9 Recherchez l'emplacement où vous avez créé l'image MSI et ouvrez le dossier `\Program Files\Novell ZENworks\Endpoint Security Client\`.

10 Copiez le certificat SSL du service de gestion (`ESM-MS.cer` ou le certificat d'entreprise) et la clé de licence Novell dans ce dossier, en remplaçant les fichiers par défaut de 0 Ko qui s'y trouvent déjà.

Le certificat SSL ESM-MS est disponible dans le dossier `Fichiers d'installation de ZENworks Endpoint Security Management`. La clé de licence est envoyée séparément par courrier électronique. Si vous utilisez une copie d'évaluation de 60 jours, aucune clé de licence n'est requise à ce stade.

10.2.4 Variables de ligne de commande

Des variables de ligne de commande sont disponibles pour une installation MSI. Ces variables doivent être définies dans le raccourci du fichier exécutable configuré pour fonctionner en mode administrateur. Pour utiliser une variable, entrez la ligne de commande suivante dans le raccourci MSI :

`"...\setup.exe" /a /V"variables"`. Entrez entre guillemets l'une des commandes ci-dessous. Si vous spécifiez plusieurs variables, séparez-les par un espace simple.

Les variables de ligne de commande suivantes sont disponibles :

Tableau 10-1 *Variables de ligne de commande*

Variable de ligne de commande	Description	Remarques
/qn	Installation silencieuse.	Met fin au processus d'installation MSI standard. Endpoint Security Client s'active au prochain redémarrage de l'utilisateur.
SESMSG=1	Indique à l'utilisateur final que le codage des fichiers des dossiers « Safe Harbor » ne peut pas être supprimé automatiquement si une stratégie de codage est déployée.	La valeur par défaut est 0 (messages non affichés) pour permettre une désinstallation « silencieuse ».
STRBR=ReallySuppress	Pas de redémarrage après l'installation.	L'application de la sécurité et l'auto-défense du client ne sont pas entièrement fonctionnelles tant que l'ordinateur n'a pas redémarré.
STUPGRADE=1	Mise à niveau de Endpoint Security Client 4.0.	Met à niveau Endpoint Security Client 4.0.
STUNINSTALL=1	Désinstallation de Endpoint Security Client 4.0.	Désinstalle Endpoint Security Client 4.0.
STUIP="mot de passe"	Désinstallation avec mot de passe	À utiliser lorsqu'un mot de passe de désinstallation est actif.

Variable de ligne de commande	Description	Remarques
STNMS=”Nom du service de gestion”	Changement du nom du service de gestion.	Change le nom du service de gestion de Endpoint Security Client 4.0.
POLICYTYPE=1	Remplacement des stratégies Endpoint Security Client 4.0 par des stratégies basées sur la machine.	Modifie les stratégies Endpoint Security Client installées par MSI afin d'accepter des stratégies basées sur la machine plutôt que sur les utilisateurs.
POLICYTYPE=2	Remplacement des stratégies Endpoint Security Client 4.0 par des stratégies basées sur les utilisateurs.	Modifie les stratégies des clients ZENworks Security Client 4.0 pour Vista installés par MSI afin d'accepter des stratégies basées sur les utilisateurs plutôt que sur la machine.
STVA=”Nom de l'adaptateur”	Ajout d'un adaptateur virtuel.	Active le contrôle de stratégies sur un adaptateur virtuel
/L*v c:\log.txt	Activation de la consignation.	Active la consignation lors de l'installation. Si vous n'utilisez pas cette variable, la consignation doit être effectuée par le biais des outils de diagnostic Endpoint Security Client.

10.2.5 Distribution d'une stratégie avec le paquetage MSI

La stratégie par défaut incluse lors de l'installation MSI peut être remplacée par une stratégie configurée pour l'entreprise. Pour distribuer une stratégie spécifique avec l'image MSI :

1. Créez une stratégie à distribuer à tous les utilisateurs via la console de gestion (reportez-vous au *Guide d'administration de ZENworks Endpoint Security Management* pour obtenir des détails sur la création de stratégies).
2. Exportez la stratégie, puis renommez-la `policy.sen`.

   Toutes les stratégies distribuées de cette manière (non gérée) doivent être nommées `policy.sen` pour être acceptées par Endpoint Security Client 4.0. Les stratégies dont le nom n'est pas `policy.sen` ne sont pas implémentées par Endpoint Security Client 4.0.
3. Ouvrez le dossier vers lequel vous avez exporté la stratégie et copiez les fichiers `policy.sen` et `setup.sen`.
4. Localisez l'image MSI créée et ouvrez le dossier `\Program Files\Novell ZENworks\Endpoint Security Client\`
5. Collez les fichiers `policy.sen` et `setup.sen` dans ce dossier. Ils remplaceront ainsi les fichiers `policy.sen` et `setup.sen` par défaut.

10.3 Exécution de Endpoint Security Client 4.0

Endpoint Security Client 4.0 s'exécute automatiquement au démarrage du système. Pour plus d'informations sur Endpoint Security Client 4.0, reportez-vous au *Guide de l'utilisateur de ZENworks Endpoint Security Client 4.0*.

Le guide de l'utilisateur peut être distribué à tous les utilisateurs pour les aider à mieux comprendre le fonctionnement de leur nouveau logiciel de sécurisation des noeuds d'extrémité.

10.4 Fonctionnalités non prises en charge dans la version 4.0 de Endpoint Security Client

Les fonctionnalités suivantes ne sont pas prises en charge ou pas totalement avec Endpoint Security Client 4.0 :

- l'auto-défense du client ;
- la prise en charge du modem ;
- l'écriture de scripts ;
- le changement manuel des pare-feux au sein d'un emplacement ;
- l'affichage de plusieurs pare-feux au sein d'un même emplacement ; (seul le pare-feu par défaut est disponible).
- les règles d'intégrité ;
- le blocage d'applications ;
- les informations affichées dans l'info-bulle de l'icône de la zone de notification ont été modifiées (désormais, seules les informations associées à la stratégie et à l'emplacement sont fournies) ;
- la connectivité USB ;
- la gestion de clés Wi-Fi ;
- les connexions filaires ne sont pas davantage privilégiées que les connexions sans fil ;
- les mises à jour de Endpoint Security Client (par stratégie) ;
- le timeout de l'authentification VPN ;
- la fonction de lecture automatique (Autoplay) pour le contrôle des périphériques de stockage ;
- les entrées de répertoire téléphonique dans l'environnement réseau.

Installation de ZENworks Endpoint Security Management en mode non géré

11

Une entreprise peut exécuter le client ZENworks® Security Client et la console de gestion de en mode non géré (sans connexion au service de distribution de stratégies ou au service de gestion). Cette possibilité est offerte sous la forme d'une option d'installation et est principalement conçue pour les évaluations simples. Cette option est également idéale pour les entreprises qui n'ont pas ou peu d'espace serveur, ou qui n'ont que des besoins de sécurité de base. Toutefois, les mises à jour rapides de stratégies et les rapports de conformité ne sont pas disponibles dans cette configuration.

11.1 Installation d'un client Endpoint Security Client non géré

Pour installer Endpoint Security Client en mode non géré, suivez les instructions de la section Chapitre 9, « Installation de Endpoint Security Client 3.5 », page 59 et cliquez sur l'option *Non connecté aux serveurs ZENworks Endpoint Security Management (stratégies reçues sous forme de fichiers)*. L'installation ignore les questions relatives aux noms des serveurs et installe Endpoint Security Client sur cette machine (un paquetage MSI peut également être créé pour un client Endpoint Security Client non géré).

Figure 11-1 *Sélection de l'option « Non connecté aux serveurs ZENworks Security Management »*

11.2 Console de gestion exécutée en mode autonome

Cette configuration permet l'installation d'une console de gestion ZENworks Endpoint Security Management et la création de stratégies sans se connecter à un service de gestion extérieur ni distribuer de stratégies via le service de distribution de stratégies. Cliquez sur *Installation d'une*

console de gestion exécutée en mode autonome dans le menu du programme d'installation principal et suivez les instructions du Chapitre 7, « Installation de la console de gestion », page 43 pour l'installation.

Au début de l'installation, une base de données SQL est installée en premier (s'il en existe une sur la machine, le programme d'installation configurera les bases de données appropriées). Une fois que le base de données est installée, l'installation s'arrête. La machine doit être redémarrée pour activer la base de données SQL. Après le redémarrage, activez de nouveau l'installation pour continuer.

Les plupart des fonctionnalités de stratégie peuvent être déployées, à l'exception des rapports. Tous les fichiers de stratégie exportés doivent être distribués vers un répertoire `\Program Files\Novell\ZENworks Security Client\` de Endpoint Security Client.

11.3 Distribution de stratégies non gérées

Pour distribuer des stratégies non gérées :

1. Localisez et copiez le fichier `setup.sen` de la console de gestion dans un dossier distinct.

   Le fichier `setup.sen` est généré lors de l'installation de la console de gestion et placé dans le répertoire `\Program Files\Novell\Console de gestion ESM`.
2. Créez une stratégie dans la console de gestion (pour plus d'informations, reportez-vous au *Guide d'administration de ZENworks Endpoint Security Management*).
3. Utilisez la commande *Exporter* pour exporter la stratégie vers le même dossier contenant le fichier `setup.sen`. Pour être acceptées par Endpoint Security Client, toutes les stratégies distribuées doivent porter le nom `policy.sen`.
4. Distribuez les fichiers `policy.sen` et `et setup.sen`. Ces fichiers doivent être copiés dans le répertoire `\Program Files\Novell\ZENworks Security Client\` pour tous les clients non gérés.

   Le fichier `setup.sen` ne doit être copié qu'une seule fois vers les périphériques non gérées, avec la première stratégie. Par la suite, seules les nouvelles stratégies doivent être distribuées.

Si un client Endpoint Security Client non géré est installé sur la même machine que la console de gestion exécutée en mode autonome, le fichier `setup.sen` doit également être copié dans le répertoire `\Program Files\Novell\ZENworks Security Client\`. Si le client Endpoint Security Client non géré est installé sur la machine après l'éditeur autonome, le fichier doit être transféré manuellement comme décrit ci-dessus.

Le bouton *Publier* publie immédiatement la stratégie pour le client Endpoint Security Client non géré sur cette machine. Pour fournir des stratégies à plusieurs utilisateurs non gérés, utilisez la fonction d'exportation décrite plus haut.

Mises à jour de la documentation

A

Cette section contient des informations sur les changements de contenu de la documentation apportés au *Guide d'installation de Novell ZENworks Endpoint Security Management* après la publication initiale pour la version 3.5. Les changements sont listés en fonction de leur date de publication.

La documentation est fournie sur le Web dans deux formats : HTML et PDF. Tous deux sont mis à jour avec les modifications listées dans cette section.

Pour savoir si votre copie de la documentation PDF est la plus récente, reportez-vous à la date de publication de ce document sur sa page de garde.

La documentation a été mise à jour aux dates suivantes :

A.1 Le 5 janvier 2009.

Les sections suivantes ont fait l'objet de mises à jour :

Emplacement	Mise à jour
Toutes les sections	Le nom du client a été modifié dans l'ensemble du guide. Son nom officiel est désormais Novell ZENworks Endpoint Security Client. Dans les chapitres respectifs, les clients sont appelés Endpoint Security Client 3.5 (pour Windows XP) et Endpoint Security Client 4.0 (pour Windows Vista).
Section 1.1, « Configuration système requise », page 10	Informations ajoutées sur la configuration requise pour le nouveau client Vista et la console de gestion en mode autonome.
Chapitre 9, « Installation de Endpoint Security Client 3.5 », page 59	Informations ajoutées et changement de nom indiquant que Endpoint Security Client 3.5 doit être utilisé avec Windows XP.
Chapitre 10, « Installation de ZENworks Endpoint Security Client 4.0 », page 67	Chapitre ajouté concernant Endpoint Security Client 4.0 (à exécuter avec Windows Vista).