LANDesk® System Manager 8.7

Guide d'installation et de deploiement

LANDesk®

v8.5

Sommaire

Présentation

Ce guide décrit le processus d'installation et de déploiement de LANDesk® System Manager, un produit qui réduit le coût total de propriété (TOC) en facilitant la gestion d'un ordinateur et la résolution des problèmes courants.

Cette présentation traite des sujets suivants :

- Fonctionnalités incluses dans cette version
- Notions de base du produit (y compris les termes)
- Stratégies d'installation et de déploiement
- Présentation de l'installation et du déploiement

Fonctionnalités incluses dans cette version

Incité par le développement de l'industrie informatique, les systèmes informatiques deviennent plus complexes et plus difficile à gérer. Le temps passé à maintenir et réparer un ordinateur durant sa période d'utilisation peut augmenter le coût total de propriété (TCO) bien au-delà du prix d'achat initial. LANDesk® System Manager peut aider à réduire le coût total de propriété (TCO) en facilitant la gestion d'un ordinateur et la résolution des problèmes courants.

- **Afficher l'inventaire du système:** System Manager fournit des informations complètes sur la configuration logicielle ou matérielle de l'ordinateur.
- **Surveiller la santé d'un ordinateur:** System Manager rapporte lorsque l'ordinateur passe à un état de santé Avertissement ou Critique en fonction de la température, tension, mémoire disponible et espace disque.
- **Recevoir des alertes pour les événements système:** System Manager peut utiliser plusieurs méthodes d'alerte pour vous prévenir en cas de problème.
- **Surveiller en temps réel ou la performance historique:** System Manager permet de surveiller la performance de divers objets système tels que les lecteurs, processeurs, mémoires et services. Vous pouvez définir des actions d'alerte pour engendrer une notification lorsqu'un compteur spécifié franchit un seuil supérieur ou inférieur un nombre prédéterminé de fois.
- **Surveiller les services et les processus actuels:** System Manager permet d'afficher les services actuels et leurs états ou de définir des actions d'alerte pour vous notifier des changements de l'état du service.
- **Mettre hors tension, mettre sous tension et redémarrer à distance les ordinateurs:** System Manager initialise la gestion d'alimentation à distance à partir d'une console administrateur pour tous les systèmes sur lesquels elle est prise en charge.
- **Vue de la tâche planifiée:** Affichez ou replanifiez tous les déploiements d'agent, les découvertes,
- **Prise en charge améliorée de système d'exploitation:** Gérez tous les périphériques de votre environnement hétérogène via une console unique. Prend en charge Windows 2000, 2003 et XP Professional, Red Hat Linux, SUSE Linux, HP-UX et AIX. Voir la section Phase 1 : Exigences système pour plus d'informations.

- **Prise en charge d'Intel* AMT et d'Intelligent Platform Management Interface (IPMI):** System Manager prend en charge les composants de gestion basés sur matériel qui permettent de gérer à distance les périphériques en réseau dans n'importe quel état système via la communication hors bande (OOB). Tant que le périphérique est connecté à un réseau d'entreprise et qu'il utilise une alimentation en veille, vous pouvez accéder à l'inventaire, afficher les informations de diagnostic à distance et redémarrer à distance le système.
- **Prise en charge du serveur Blade:** Prise en charge des serveurs Blade et des modules de gestion de châssis (CMM) Blade, y compris les fonctions de gestion et d'inventaire.
- **Outil de scripts:** Vous pouvez planifier et exécuter des tâches personnalisées sur les périphériques
- **Planificateur de tâche:** Un schéma de base de données unique doté d'une intégrité et d'une évolutivité améliorées des données permet d'accéder à de nombreuses informations sur les périphériques gérés (y compris une intégration complète avec Management Suite). Le planificateur de tâche fait partie de ce schéma unique. Vous pouvez désormais afficher toutes les tâches (, découverte, configuration d'agent, dans une fenêtre commune. A partir de cette fenêtre, vous pouvez replanifier, modifier ou rendre récurrente la planification.
- **Administration basée sur les rôles:** Configurez l'accès utilisateurs aux outils et périphériques de réseau selon le rôle administratif de l'utilisateur dans l'organisation. Grâce à l'administration basée sur les rôles, vous attribuez une portée pour spécifier les périphériques qu'un utilisateur peut voir et gérer, et des droits pour indiquer les tâches qu'il peut effectuer.
- **Découverte de périphériques non gérés:** Découvrez les périphériques gérés sur le réseau via diverses méthodes. Le produit identifie les serveurs exécutant Windows ou Linux, les serveurs et les châssis de lame, les serveurs dotés de IPMI, les serveurs dotés d'AMT d'Intel, ainsi que d'autres périphériques réseau. Planifiez une découverte de périphériques afin d'être constamment averti des nouveaux périphériques. Vous pouvez également générer des rapports sur les périphériques non gérés sur le réseau.
- **Sécurité améliorée:** Un modèle de sécurité basé sur un certificat permet aux périphériques de communiquer uniquement avec les consoles et serveurs principaux autorisés.
- **Distribution de logiciel:** Automatisez le processus d'installation de logiciels ou de distribution de fichiers aux périphériques.
- **Rapports:** Des rapports de service prédéfinis sont disponibles pour la planification et l'analyse stratégique
- **Prise en charge des tâches planifiées:** Offrez plusieurs connexions permettant au service Planificateur de s'authentifier lorsque des tâches sont exécutées sur des périphériques sans agents. Cette fonction est particulièrement utile pour gérer des périphériques sur plusieurs domaines Windows.

Notions de base du produit

System Manager gère des périphériques qui exécutent plusieurs systèmes d'exploitation différents, y compris les serveurs Windows 2000 Pro SP4, Windows XP Pro SP1, Windows* 2000/2003, les serveurs Red Hat Enterprise Linux v3, les serveurs SUSE Linux 9, les serveurs HP-UX et AIX et fournit une interface commune pour la gestion des périphériques de ces systèmes d'exploitation de réseau. Il peut coexister également avec d'autres produits LANDesk, tels que LANDesk® Management Suite et LANDesk® Server Manager.

Termes du produit

- **Serveur principal:** Centre d'un domaine de gestion. Tous les fichiers et services clés du produits sont situés sur le serveur principal. Un domaine de gestion possède un seul serveur principal. Un serveur principal peut être un nouveau serveur ou un serveur redéfini.
- **Console:** La console basée sur un navigateur qui est l'interface principale du produit.
- Base de données principale :Le produit crée une base de données MSDE sur le serveur principal pour stocker les données de gestion.
- **Périphériques gérés:** Périphériques du réseau sur lesquels les agents de produit sont installés. "Périphériques" inclut les ordinateurs de bureau, les serveurs, les ordinateurs portables, les châssis Blade, etc. Un serveur principal peut gérer des milliers de périphériques.
- **Public:** Eléments (comme par exemple des groupes, des paquets de distribution ou des tâches) qui peuvent être visualisés par tous les utilisateurs. Lorsqu'un utilisateur modifie un élément Public, la modification reste publique. Les groupes publics sont créés par un utilisateur doté des droits Administrateur.
- **Privé ou Utilisateur:** Eléments créés par l'utilisateur connecté. Ils ne sont pas visibles aux autres utilisateurs. Les éléments Utilisateur ou Privé s'affichent dans les arborescences **Mes méthodes de distribution**, **Mes paquets** et **Mes tâches**. Les utilisateurs dotés des droits Administrateur peuvent visualiser les groupes privés ainsi que les tâches et les paquets utilisateurs.
- **Courant:** Un élément pouvant être visualisé par les autres utilisateurs. Lorsqu'un utilisateur prend possession d'un élément courant (en le modifiant), ce dernier se divise en deux éléments : l'élément Courant reste en place et un élément Utilisateur est enregistré dans le dossier Utilisateurs. L'instance Utilisateur de l'élément n'est plus visible aux autres utilisateurs. Un utilisateur peut marquer toute tâche qu'il peut visualiser comme étant Courante, ce qui lui permet de la partager avec d'autres utilisateurs. Après qu'un utilisateur efface l'option Courante des propriétés de l'élément, la tâche est visible uniquement dans le groupe Tâches d'utilisateur.

Comment ce produit s'ajuste-t-il à mon réseau ?

Ce produit utilise l'infrastructure de votre réseau existant pour établir des connexions avec les périphériques qu'il gère. La tâche de gestion des périphériques existants est fortement simplifiée, que vous gériez un petit réseau ou un environnement de grande entreprise.

Utilisation de System Manager avec Management Suite ou Server Manager

Si vous disposez de System Manager et souhaitez l'utiliser avec Management Suite ou Server Manager, utilisez l'outil d'activation du serveur principal pour fournir un nom d'utilisateur et un mot de passe valides pour le produit avec lequel vous voulez utiliser System Manager. Une installation System Manager / Management Suite fonctionne avec trois consoles : les consoles Windows 32 et Web Management Suite et la console Web System Manager. La console Server Manager inclut trois éléments de navigation (Alerte, Surveillance et Journaux) qui contiennent des fonctions qui ne sont pas offertes par les deux consoles Management Suite.

Si vous déployez Management Suite, l'installation Management Suite supprime l'agent System Manager des périphériques gérés et vice-versa. Lorsque vous exécutez Management Suite avec System Manager, la fonction de configuration Management Suite inclut des options de surveillance.

Installation de System Manager avec Management Suite ou Server Manager déjà installé

Si Management Suite ou Server Manager est déjà installé sur le serveur principal et si vous voulez ajouter System Manager, utilisez la même installation que pour l'installation d'origine de Management Suite ou Server Manager.

1. Ouvrez autorun.exe.
2. Cliquez sur **Installer maintenant**.
3. Sélectionnez une langue et cliquez sur **OK**.
4. L'écran de bienvenue s'affiche. Cliquez sur **Suivant**.
5. Sélectionnez sur **Modifier** (si nécessaire), puis sur **Suivant**.
6. Cliquez sur LANDesk® Server Manager, puis sur **Suivant**.
7. Suivez les instructions de l'assistant.

Exigences système du serveur principal

Lorsque vous considérez le serveur que vous allez configurer comme serveur principal, passez en revue les exigences système ci-dessous et confirmez que le serveur satisfait ou dépasse les exigences répertoriées dans Phase 1 : Exigences système. Le programme de vérification d'exigences le fait automatiquement.

Un serveur principal dédié est fortement recommandé
En raison du trafic qui passe au travers du serveur principal pour la gestion du domaine, il est fortement recommandé que chaque serveur principal soit dédié à l'hébergement du produit.

Si vous installez d'autres produits sur le même serveur, vous pouvez rencontrer des problèmes de ressources à court et long termes.

N'installez pas les composants du serveur principal sur un contrôleur principal de domaine, un contrôleur secondaire de domaine ou un contrôleur de domaine Active Directory.

Stratégies d'installation et de déploiement

Lorsque vous installez à l'aide de la fonction d'exécution automatique (Autorun) à partir du support du produit, le programme d'installation vérifie automatiquement que le serveur principal satisfait ces exigences avant de poursuivre. L'installation et le déploiement d'une application au niveau du système vers un réseau hétérogène requièrent une méthodologie délibérée et une planification importante *avant* l'exécution du programme d'installation. Ce guide inclut des stratégies pour la configuration du produit. Avant de le déployer, vous devez brièvement caractériser vos besoins de gestion.

Déploiement des considérations de stratégie

Le déploiement est le processus d'expansion des possibilités de gestion vers les serveurs à inclure dans le domaine. Dans ce guide, le déploiement est présenté en "phases".

La stratégie de déploiement graduel offre une approche structurée pour activer la gestion sur les périphériques. Cette approche est basée sur deux principes simples :

- Déployez en premier les composants du produit ayant un impact minimal sur le réseau existant. Passez ensuite aux composants ayant un impact maximal.
- Procédez au déploiement du produit via des phases bien planifiées, plutôt que de déployer tous les services en une opération, ce qui peut compliquer tout dépannage requis.

Ce guide est organisé de manière séquentielle pour vous aider à déployer le produit. Commencez par le premier chapitre, "Phase 1 : Conception du domaine de gestion, plus loin dans ce guide. Vous pouvez ensuite continuer en passant par chaque phase.

Présentation de l'installation et du déploiement

Ce guide groupe les tâches d'installation et de déploiement suivant les phases suivantes. Pour chaque phase, une section correspondante de ce guide vous décrit cette partie de l'installation. Le chapitre vous aide à rapidement utiliser le produit en configurant les services, exécutant la console, découvrant des périphériques, plaçant les périphériques dans la liste Mes périphériques et configurant les actions de périphériques gérés. Il est conçu pour être succinct, en présumant que vous consulterez le reste du livre pour obtenir plus d'informations. Certaines procédures de ce guide sont également présentées dans le chapitre Mise en route.

Récapitulatif de la phase 1

Durant la phase 1 de l'installation, vous concevez le domaine de gestion en réalisant les tâches ci-dessous :

- Rassemblement des informations du réseau
- Confirmation que le réseau correspond aux exigences système

Pour plus de détails, reportez-vous à la section "Phase 1 : Conception du domaine de gestion, plus loin dans ce guide.

Récapitulatif de la phase 2

Durant la phase 2, vous installez le produit en réalisant les tâches ci-dessous :

- Installation du serveur principal

Pour plus de détails, reportez-vous à la section "Phase2 : Installation du serveur principal et de la console", plus loin dans ce guide.

Récapitulatif de la phase 3

Durant la phase 3 de l'installation, vous découvrez des périphériques sur le réseau et déployez les agents du produit. Vous pouvez pousser les agents de la console ou les tirer du partage de serveur.

Pour plus de détails, reportez-vous à la section "Phase3 : Déploiement des agents vers les périphériques", plus loin dans ce guide.

Mise en route

Présentation

Bienvenue dans LANDesk® System Manager, une application de gestion de périphériques autonome qui permet de mieux utiliser votre temps en gérant rapidement et efficacement vos périphériques, permettant ainsi à votre organisation d'économiser du temps et de l'argent. System Manager gère vos périphériques de manière centralisée, les regroupe selon les actions à suivre (cycles d'alimentation, évaluations de vulnérabilités, configuration des alertes), résout à distance une variétés de problèmes, protège votre réseau et maintient vos périphériques à jour avec les derniers correctifs.

Ce guide vous aide à rapidement utiliser System Manager en configurant les services, exécutant la console, découvrant des périphériques, plaçant les périphériques dans la liste Mes périphériques et configurant les actions de périphériques gérés.

System Manager est une application Web que vous pouvez accéder via le navigateur pour gérer vos serveurs depuis un poste de travail distant. Il se comporte comme la majorité des applications Web que vous utilisez, mais il contient également plusieurs commandes avancées Windows qui permettent d'améliorer votre expérience. Par exemple, déplacez le curseur de la souris sur une commande, vous pouvez soit cliquer deux fois sur la commande soit la cliquer avec le bouton droit de la souris (comme dans une application Windows). Dans la liste Mes périphériques, vous pouvez par exemple cliquer deux fois sur un nom de périphérique pour accéder à ses informations spécifiques ou cliquer avec le bouton droit de la souris pour afficher les actions disponibles

Les étapes ci-dessous décrivent l'activation de System Manager, la découverte des périphériques sur le réseau, la sélection des périphériques à placer dans la liste Mes périphériques, le déploiement des agents et le ciblage de ces périphériques pour diverses tâches.

Exécution du programme d'installation

Durant l'installation, veuillez sélectionner LANDesk® System Manager dans la page d'exécution automatique. Vous trouverez des instructions d'installation dans les et Phase 2 du Guide d'installation et de déploiement.

Une fois System Manager installé, vous pouvez commencer à l'utiliser. Les sections ci-dessous décrivent comment effectuer plusieurs tâches obligatoires : exécution de l'utilitaire d'activation du serveur principal, configuration des services, découverte d'ordinateurs, spécification des périphériques à activement gérer en les déplaçant vers la liste Mes périphériques, regroupement des périphériques, ajout d'utilisateurs et déploiement d'agents. Une fois ces tâches terminées, vous êtes prêt à découvrir comment l'ensemble des fonctions robustes de System Manager va vous permettre de gérer vos périphériques.

Activation du serveur principal

Vous ne pouvez exécuter le programme qu'après avoir activé le serveur principal.

L'utilitaire d'activation du serveur principal permet d'effectuer les opérations suivantes :

- activer un nouveau serveur principal System Manager pour la première fois
- mettre à jour un serveur principal System Manager existant

Chaque serveur principal doit utiliser un certificat d'autorisation unique.

Cet utilitaire s'exécute automatiquement lorsque l'ordinateur redémarre.

Avec votre serveur principal connecté à l'Internet, procédez comme suit :

1. Cliquez sur **Démarrer | Programmes | Activation** du serveur principal. Le nom d'utilisateur et le mot de passe sont fournis.
2. Cliquez sur **Activer**.

Le serveur principal communique avec le serveur de mise sous licence du logiciel via HTTP. Si vous utilisez un serveur proxy, cliquez sur l'onglet Proxy de l'utilitaire et entrez les informations correspondantes. Si votre serveur principal utilise une connexion Internet, la communication avec le serveur de licences est automatique et n'exige aucune intervention de votre part. Si le serveur principal n'est pas connecté, cliquez sur Fermer au redémarrage puis envoyez le fichier d'autorisation à l'adresse licensing@landesk.com.

Périodiquement, le serveur principal génère des informations de vérification de nombre de nœuds dans le fichier "\Program Files\LANDesk\Authorization Files\LANDesk.usage". Ce fichier est régulièrement envoyé au serveur de mise sous licence de LANDesk Software. Il s'agit d'un fichier au format XML codé et signé numériquement. Toute modification manuelle de ce fichier annule le contenu et le rapport d'utilisation suivant pour le serveur de mise sous licence du logiciel.

- Utilitaire Activation du serveur principal ne démarre pas automatiquement une connexion Internet à distance, mais si vous lancez manuellement celle-ci, puis exécutez l'utilitaire d'activation, il peut utiliser la connexion à distance pour rapporter les données d'utilisation.

- Vous pouvez également activer le serveur principal par courrier électronique. Envoyez le fichier doté de l'extension .TXT situé dans le dossier Program Files\LANDesk\Authorization to licensing@landesk.com. L'assistance clientèle de LANDesk répondra au message électronique en envoyant un fichier et des instructions pour copier le fichier dans le serveur principal afin de terminer la procédure d'activation.

Ajout d'utilisateurs

Les utilisateurs de System Manager sont des utilisateurs qui peuvent se connecter à la console et réaliser des tâches spécifiques pour des périphériques donnés sur le réseau. L'administration basée sur les rôles permet de gérer les utilisateurs. L'administration basée sur les rôles permet d'attribuer à des utilisateurs du produit des rôles administratifs spéciaux selon leurs droits et leur portée. Les droits déterminent les outils et fonctions du produit qu'un utilisateur peut voir et employer. La portée détermine la plage de périphériques qu'un utilisateur peut voir et gérer. Vous pouvez créer une variété d'utilisateurs et personnaliser leurs droits et étendue selon vos exigences. Par exemple, vous pouvez créer un utilisateur qui a pour rôle de s'occuper du bureau des réclamations en lui attribuant les droits nécessaires à ces fonctions. Pour plus de détails, reportez-vous au chapitre Administration basée sur les rôles duSystem Manager Guide d'utilisation.

Lorsque vous installez le produit, deux comptes d'utilisateur sont automatiquement créés (voir ci-dessous). Si souhaité, vous pouvez ajouter manuellement plus d'utilisateurs. Les utilisateurs ne sont pas actuellement créés dans la console. Ils s'affichent dans le groupe Utilisateurs (cliquez sur Utilisateurs dans le volet de navigation de gauche) une fois qu'ils ont été ajoutés au groupe LANDesk Management Suite dans l'environnement d'utilisateurs Windows NT sur le serveur principal. Le groupe Utilisateurs affiche tous les utilisateurs résidant actuellement dans le groupe LANDesk Management Suite sur le serveur principal.

Le groupe Utilisateurs contient deux utilisateurs par défaut. L'un des deux est l'Administrateur par défaut. Il s'agit de l'utilisateur administratif qui est connecté au serveur lors de l'installation du logiciel.

L'autre utilisateur est l'Utilisateur modèle par défaut.Cet utilisateur contient un modèle de propriétés d'utilisateur (droits et portée) qui est employé pour configurer de nouveaux utilisateurs lors de leur ajout au groupe Management Suite. En d'autres termes, lorsque vous ajoutez un utilisateur à ce groupe dans l'environnement Windows NT, l'utilisateur hérite des droits et de la portée actuellement définis dans les propriétés d'utilisateur modèle par défaut. Si l'utilisateur modèle par défaut dispose de tous les droits sélectionnés et que la portée Toutes les machines par défaut est sélectionnée, tout nouvel utilisateur placé dans le groupe LANDesk Management Suite sera ajouté au groupe Utilisateurs avec des droits sur tous les outils du produit et un accès à tous les périphériques.

Vous pouvez modifier les paramètres de propriétés de l'utilisateur modèle par défaut en le sélectionnant et en cliquant sur Modifier. Par exemple, si vous souhaitez ajouter un nombre important d'utilisateurs en une opération, mais ne voulez pas leur octroyer un accès à tous les outils ou périphériques, modifiez d'abord les paramètres de l'utilisateur modèle par défaut, puis ajoutez les utilisateurs au groupe LANDesk Management Suite (voir la procédure ci-dessous). L'utilisateur modèle par défaut ne peut pas être supprimé.

Lorsque vous ajoutez un utilisateur au groupe LANDesk Management Suite sous Windows NT, il est automatiquement lu dans le groupe Utilisateurs de la fenêtre Utilisateurs, en héritant des

mêmes droits et portées que l'utilisateur modèle par défaut actuel. Le nom, la portée et les droits de l'utilisateur sont affichés. De plus, de nouveaux sous-groupes d'utilisateur, nommés suivant l'ID de connexion unique de l'utilisateur, sont créés dans les groupes Périphériques utilisateur, Requêtes utilisateur, Rapports d'utilisateur et Scripts utilisateur (notez que SEUL un administrateur peut visualiser les groupes Utilisateur).

Inversement, si vous supprimez un utilisateur du groupe LANDesk Management Suite, l'utilisateur ne s'affiche plus dans la liste Utilisateurs. Le compte de l'utilisateur existe toujours sur le serveur principal et peut à nouveau être ajouté à tout moment au groupe LANDesk Management Suite. En outre, les sous-groupes de l'utilisateur sous les groupes Périphériques utilisateur, Requêtes utilisateur, Rapports d'utilisateur et Scripts utilisateur sont conservés afin que vous puissiez restaurer l'utilisateur sans perte de données et que vous puissiez également copier des données vers d'autres utilisateurs.

Pour actualiser la fenêtre Utilisateurs dans la console System Manager, appuyez sur F5. Pour apprendre comment ajouter un groupe d'utilisateurs ou de domaines dans le groupe LANDesk Management Suite ou comment créer un nouveau compte d'utilisateur, reportez-vous à la section "Ajout d'utilisateurs de produit" du chapitre Administration basée sur les rôles du System Manager *Guide d'utilisation*.

Pour ajouter un groupe de domaine ou d'utilisateur au groupe LANDesk Management Suite

1. Naviguez vers l'utilitaire **Outils d'administration | Gestion de l'ordinateur | Utilisateurs et groupes locaux | Groupes** du serveur.
2. Cliquez avec le bouton droit de la souris sur le groupe **LANDesk Management Suite**, puis cliquez sur **Ajouter au groupe**.
3. Cliquez sur **Ajouter**, puis entrez ou sélectionnez un utilisateur (ou des utilisateurs) dans la liste.
4. Cliquez sur **Ajouter**, puis sur **OK**.

Remarque : Vous pouvez également ajouter un utilisateur au groupe LANDesk Management Suite en cliquant avec le bouton droit de la souris sur le compte d'utilisateur dans la liste **Utilisateurs**, en cliquant sur **Propriétés | Membre de**, puis en cliquant sur **Ajouter** pour sélectionner le groupe et ajouter l'utilisateur.

Si le compte d'utilisateur n'existe pas déjà dans le serveur, vous devez d'abord le créer sur le serveur

Pour créer un compte d'utilisateur

1. Naviguez vers l'utilitaire **Outils d'administration | Gestion de l'ordinateur | Utilisateurs et groupes locaux | Utilisateurs** du serveur.
2. Cliquez avec le bouton droit de la souris sur **Utilisateurs**, puis cliquez sur **Nouvel utilisateur**.
3. Dans la boîte de dialogue **Nouvel utilisateur**, entrez un nom et un mot de passe.
4. Spécifiez les paramètres du mot de passe.
5. Cliquez sur **Créer**. La boîte de dialogue **Nouvel utilisateur** reste ouverte afin que vous puissiez créer d'autres utilisateurs.
6. Cliquez sur **Fermer** pour fermer la boîte de dialogue.

Ajoutez l'utilisateur au groupe LANDesk Management Suite afin qu'il apparaisse dans le groupe Utilisateurs dans la console.

Configuration de services et de références d'authentification

Avant de pouvoir gérer des périphériques sur le réseau, vous devez fournir les références d'authentification nécessaires à System Manager. Utilisez l'utilitaire Configuration de services sur le serveur principal (SVCCFG.EXE) pour spécifier le système d'exploitation requis, AMT d'Intel*, et les références d'authentification IPMI BMC. Vous pouvez également spécifier des paramètres supplémentaires, tels que les paramètres par défaut d'inventaire, les paramètres de file d'attente PXE et les paramètres de la base de données LANDesk.

Utiliser l'utilitaire Configuration de services pour configurer :

- Le nom de base de données, le nom d'utilisateur et le mot de passe. (Veuillez définir une heure d'installation.)
- Références d'authentification pour la planification de tâches sur les périphériques gérés. (Vous pouvez entrer plusieurs ensembles de références d'administrateur.)
- Références d'authentification pour la configuration de BMC IPMI. (Vous pouvez entrer un seul ensemble de références BMC.)
- Références pour la configuration des périphériques dotés d'AMT d'Intel. (Vous pouvez entrer un seul ensemble de références AMT d'Intel.)
- L'intervalle d'analyse de logiciel serveur, la maintenance, les jours de conservation d'analyses d'inventaire et la durée de l'historique de connexion.
- Le traitement des doublons d'ID de périphérique .
- Configuration du Planificateur, y compris les tâches planifiées et les intervalles entre évaluations de requête.
- Configuration d'une tâche personnalisée, y compris le délai d'exécution distante.

1. **Dans le serveur principal, cliquez surDémarrer | Programmes | LANDesk | Configuration des services LANDesk.**
2. **Cliquez sur l'ongletPlanificateur.**
3. Cliquez sur le bouton **Modifier la connexion**.
4. Entrez les références qui seront utilisées par le service sur les périphériques gérés, généralement un compte administrateur de domaine.
5. Cliquez sur **Ajouter**. Si les périphériques gérés n'ont pas tous les mêmes comptes de nom d'utilisateur administrateur activés, ajoutez des références supplémentaires selon les besoins.
6. Cliquez sur **Appliquer**.
7. Si votre environnement dispose d'un serveur doté de IPMI, cliquez sur l'onglet Mot de passe BMC. Renseignez les zones de texte Mot de passe et Confirmer le mot de passe, puis cliquez sur OK. (Tous les serveur IPMI gérés doivent partager le même nom d'utilisateur et mot de passe BMC.)
8. Si vous avez des périphériques dotés d'Intel AMT, cliquez sur l'onglet Configuration d'Intel AMT. Entrez le nom d'utilisateur d'Intel AMT actuellement configuré dans la zone de texte Nom d'utilisateur, puis entrez le mot de passe actuellement configuré dans la zone de texte Mot de passe. Retapez le mot de passe dans la zone Confirmer le mot de passe, puis cliquez sur OK.
9. Veuillez configurer tout autre paramètre comme souhaité, tel que les intervalles d'analyse de logiciel.
10. Pour enregistrer les modifications, cliquez sur **OK**.

Pour obtenir des informations supplémentaires sur chaque onglet de Configuration de services, cliquez sur **Aide**.

Exécution de la console

System Manager inclut une gamme complète d'outils qui permettent de visualiser, de configurer, de gérer et de protéger les périphériques du réseau. La console est la fonction centrale qui vous permet d'utiliser ces outils.

Le volet supérieur de la console affiche le serveur auquel vous êtes connecté et le nom d'utilisateur utilisé pour la connexion. La liste Mes périphériques est située dans la fenêtre principale de la console et correspond au point de départ de la plupart des fonctions. Le volet de gauche affiche les outils disponibles. Le volet de droite de la console affiche des boîtes de dialogue et des écrans qui vous permettent de réaliser des tâches de gestion.

L'avantage offert par la console est que vous pouvez exécuter toutes ses fonctions à partir d'un emplacement distant, tel que votre poste de travail ; vous n'avez donc plus à visiter la pièce contenant le serveur ou à vous déplacer vers chaque périphérique géré pour réaliser une maintenance de routine ou résoudre des problèmes.

Utilisez une des trois méthodes suivantes pour lancer la console :

- Dans le serveur principal, cliquez sur **Démarrer | Programmes | LANDesk | System Manager**.
- Dans un navigateur du poste distant, entrez l'URL http://serveur_principal/LDSM.

Découverte des périphériques

Utilisez l'onglet **Configurations de découverte** pour créer de nouvelles configurations de découverte, modifier et supprimer des configurations existantes et planifier une configuration pour la découverte. Chaque configuration de découverte comporte un nom descriptif, des plages d'adresses IP à analyser et le type de découverte.

Une fois la configuration créée, utilisez la boîte de dialogue **Planifier une découverte** pour définir la date et l'heure d'exécution.

1. Dans le volet de navigation de gauche, cliquez sur **Découverte de périphérique**.
2. Dans l'onglet **Configurations de découverte**, cliquez sur le bouton **Nouveau**.
3. Renseignez les champs décrits ci-dessous. Une fois terminé, cliquez sur le bouton **Ajouter**, puis sur **OK**.

Le texte ci-dessous décrit les zones de la boîte de dialogue **Configuration de découverte**.

- **Nom de configuration:** Entrez un nom pour cette configuration. Donnez à la configuration un nom significatif facile à mémoriser. La configuration peut comporter jusqu'à 255 caractères et ne devrait pas contenir les caractères suivants : **"**, **+**, **#**, **&** ou **%**. Le nom de configuration ne s'affiche pas si ces caractères sont utilisés.

- **Analyse de réseau standard:** Recherche des périphériques en envoyant des paquets ICMP aux adresses IP dans la plage spécifiée. Il s'agit de la recherche la plus poussée mais également la plus lente. Par défaut, cette option utilise NetBIOS pour regrouper des informations sur le périphérique.

  L'analyse réseau dispose de l'option **Empreintes IP** qui permet à la fonction de découverte de périphériques d'identifier le type de SE à travers les réponses de paquets TCP. L'option Empreinte IP ralentit quelque peut le processus de découverte.

  L'analyse réseau dispose aussi de l'option **Utiliser SNMP** qui permet à l'analyse d'utiliser SNMP. Cliquez sur **Configurer** pour entrer les informations relatives à votre configuration SNMP.
- **Découverte LANDesk CBA:** Recherche sur les périphériques l'agent de gestion standard (auparavant appelé agent à base commune (CBA) dans Management Suite). L'agent de gestion standard permet au serveur principal de découvrir et de communiquer avec les clients du réseau. Cette option découvre les périphériques dotés des agents de produit. Les routeurs bloquent l'agent de gestion standard et le trafic PDS2. Pour lancer une découverte CBA standard sur plusieurs sous-réseaux, le routeur doit être configuré de manière à permettre une diffusion dirigée sur plusieurs sous-réseaux.

  La découverte CBA dispose de l'option **Découverte LANDesk PDS2** par laquelle la découverte de périphériques recherche LANDesk Ping Discovery Service (PDS2) sur les périphériques. Les produits LANDesk Software tels que LANDesk® System Manager, Server Manager, et LANDesk Client Manager utilisent l'agent PDS2. Sélectionnez cette option si des périphériques du réseau possèdent ces produits. La découverte CBA n'est pas prise en charge pour les ordinateurs Linux, mais si vous choisissez PDS2, les ordinateurs Linux dotés d'un agent peuvent être découverts.
- **IPMI:** Recherche les serveurs dotés de IPMI. IPMI est une spécification développée par Intel,***** H-P,* NEC,* et Dell* pour définir l'interface système et de message des matériels gérables. PMI contient des fonctions de surveillance et de récupération qui permettent d'accéder à ces fonctions que le périphérique soit sous tension ou pas, ou indépendamment de l'état du système d'exploitation. N'oubliez pas que si le contrôleur de gestion de la carte de base (BMC) n'est pas configuré, il ne répond pas aux pings ASF que le produit utilise pour découvrir IPMI. Cela signifie que vous devrez le découvrir comme un ordinateur normal. Lorsque vous poussez le client, ServerConfig analyse le système et détecte qu'il correspond à IPMI et configure le BMC.
- **Châssis de serveur:** Recherche des modules de gestion de châssis (CMM) de serveur Blade. Les serveurs Blade dans le châssis de serveur sont détectés comme étant normaux.
- **Intel* AMT:** Recherche les périphériques qui prennent en charge Intel Active Management Technology.
- **IP de début:** Entrez l'adresse IP de début de la plage d'adresses à analyser.
- **IP de fin:** Entrez l'adresse IP de fin de la plage d'adresses à analyser.
- **Masque de sous-réseau:** Entrez le masque de sous-réseau de la plage d'adresses IP à analyser.
- **Ajouter:** Ajoute les plages d'adresses IP dans la file d'attente de travail au bas de la boîte de dialogue.
- **Effacer:** Efface les champs de la plage d'adresses IP.
- **Modifier:** Sélectionnez une plage d'adresses IP dans la file d'attente de travail puis cliquez sur **Modifier**. La plage s'inscrit dans les zones de texte au-dessus de la file d'attente de travail où vous pouvez la modifier et l'ajouter à la file d'attente.

- **Supprimer:** Supprime la plage d'adresses IP sélectionnée de la file d'attente de travail.
- **Tout supprimer:** Supprime toutes les plages d'adresses IP sélectionnées de la file d'attente de travail.

Maintenant que la tâche de découverte a été configurée, il vous suffit de planifier la tâche pour découvrir les périphériques connectés à votre réseau.

Planification et exécution d'une tâche de découverte

Utilisez le bouton Planifier dans l'onglet Découvrir les périphériques pour afficher la boîte de dialogue Planifier une découverte. Utilisez cette boîte de dialogue pour planifier l'exécution d'une découverte. L'exécution de la tâche de découverte peut être immédiate, ultérieure, récurrente ou unique.

Une fois une découverte planifiée, passez à l'onglet Tâches de découverte pour afficher l'état de la découverte. La planification d'une tâche de découverte récurrente vous aide à découvrir automatiquement les nouveaux périphériques qui apparaissent sur le réseau.

La boîte de dialogue Planifier une découverte comporte les options suivantes.

- **Laisser non planifié:** La tâche reste non planifiée, mais la conserve dans la liste Configurations de découverte pour une utilisation ultérieure.
- **Démarrer maintenant:** Exécute la tâche dès que possible. Le démarrage de la tâche peut prendre une minute.
- **Démarrer à une heure prévue:** Démarre la tâche à l'heure spécifiée. Si vous sélectionnez cette option, vous devez entrer les informations suivantes :
    - **Heure:** L'heure de démarrage de la tâche.
    - **Date:** La date de démarrage de la tâche. En fonction de vos paramètres régionaux, le format de la date peut être jour-mois-année ou mois-jour-année.
    - **Répéter chaque:** Si vous souhaitez répéter la tâche, sélectionnez parmi les options Quotidien, Hebdomadaire ou Mensuel. Si vous sélectionnez Mensuel et si la date n'existe pas dans tous les mois (par exemple, 31), la tâche s'exécute uniquement les mois contenant cette date.

Pour planifier une tâche de découverte

1. Dans le volet de navigation de gauche, cliquez sur **Périphériques découverts**.
2. Dans l'onglet Configurations de découverte, sélectionnez la configuration de votre choix et cliquez sur **Planifier**. Configurez la planification de la découverte et cliquez sur **Enregistrer**.
3. Surveillez la progression de la découverte dans l'onglet Tâches de découverte. Cliquez sur **Actualiser** pour mettre à jour l'état.
4. Une fois la découverte terminée, cliquez sur Non gérés pour afficher tous les périphériques découverts dans le volet supérieur Périphériques découverts (le volet n'est pas automatiquement actualisé).

Affichage des périphériques découverts

Les périphériques découverts sont catégorisés par type de périphérique dans le volet Périphériques découverts. Le dossier Ordinateurs s'affiche par défaut. Cliquez sur les dossiers

situés dans le volet de gauche pour afficher les périphériques dans des catégories différentes. Cliquez sur Non géré pour afficher tous les périphériques renvoyés par la découverte.

- Les châssis de serveurs Blade s'affichent dans le dossier **Châssis**.
- Les périphériques d'entreprise standard s'affichent dans le dossier **Ordinateurs**.
- Les routeurs et les autres périphériques s'affichent dans le dossier **Infrastructure**.
- Les périphériques dotés d'AMT d'Intel s'affichent dans le dossier **AMT d'Intel**.
- Les serveurs dotés de IPMI s'affichent dans le dossier **IPMI**.
- Les périphériques non catégorisés s'affichent dans le dossier **Autre**.
- Les imprimantes s'affichent dans le dossier **Imprimantes**.

Remarque: Certains serveurs Linux utilisent le nom générique "Unix" comme nom du système d'exploitation (ou s'affichent parfois dans le dossier Autre). Lorsque l'agent de gestion standard est déployé, ces serveurs mettent à jour leur entrée Nom du système d'exploitation dans la liste Mes périphériques et affichent un inventaire complet. Pour afficher les serveurs découverts

1. Dans le volet de gauche de la page Découverte de périphérique, cliquez sur Ordinateurs ou sur un autre type de périphérique à afficher. Les résultats s'affichent dans le volet de droite.
2. Pour filtrer les résultats, cliquez sur l'icône **Filtre**, entrez au moins une partie de ce que vous recherchez, et cliquez sur Rechercher.

Attribution de noms

Durant une découverte d'analyse réseau, certains serveurs renvoient un nom de nœud (ou nom d'hôte) vierge. Ceci se produit plus fréquemment avec des serveurs exécutant Linux. Vous devez attribuer un nom au périphérique avant d'utiliser l'option Gérer pour le déplacer vers la liste Mes périphériques.

1. Dans la page Découverte de périphérique, cliquez sur le périphérique sans nom. (Vous devez cliquer la zone vierge dans la colonne de noms de nœuds.)
2. Cliquer sur Attribuer un nom dans la barre d'outils.
3. Entrez un nom et cliquez sur **OK**.

Lorsque vous installez un agent de produit sur un périphérique, il analyse automatiquement le nom d'hôte et met à jour la base de données principale avec les informations correctes.

Déplacement des périphériques vers la liste Mes périphériques

Une fois découverts, vous devez manuellement cibler les périphériques à gérer et les déplacer vers la liste Mes périphériques. Le déplacement du périphérique n'installe pas des logiciels sur le périphérique. Ce dernier devient uniquement disponible pour l'interrogation, le regroupement et le triage dans la liste Mes périphériques. Vous "ciblez" une action spécifique sur des périphériques spécifiques, un genre de "panier" comme en possèdent de nombreuses applications Web.

1. Dans la vue Périphériques découverts, sélectionnez le périphérique à placer dans la liste Mes périphériques. Pour sélectionner plusieurs périphériques, appuyez sur **MAJ+cliquer** ou **CTRL+cliquer**.

2. Cliquez sur le bouton **Cible**. S'il n'est pas visible, cliquez sur **<<** sur la barre d'outils. Le bouton est situé à l'extrême droite. Ou, cliquez avec le bouton droit de la souris sur les serveurs sélectionnés et cliquez sur **Cible**.
3. Dans le volet inférieur, cliquez sur l'onglet **Gérer**.
4. Vous pouvez déplacer les périphériques vers la base de données de gestion ou déplacer les périphériques ciblés.
5. Cliquer sur **Déplacer**.

Un clic sur le bouton Déplacer déplace les périphériques vers la liste Mes périphériques et place les informations sur le périphérique dans la base de données. Une fois les informations dans la base de données, vous pouvez exécuter des requêtes et des rapports limités sur celle-ci (tels que par nom de périphérique, adresse IP ou système d'exploitation).

Regroupement des périphériques pour des actions

Pour effectuer plus rapidement des actions sur vos périphériques, il est recommandé de les organiser en groupes, tels que par emplacement géographique ou fonction. Par exemple, vous pouvez souhaiter afficher les vitesses de processeur de tous les périphériques d'un répertoire spécifique.

1. Dans la liste Mes périphériques, cliquez sur Groupes privés ou Groupes publics, puis cliquez sur Ajouter un groupe.
2. Entrez un nom pour le groupe dans la zone Nom de groupe.
3. Cliquez sur le type de groupe que vous souhaitez créer.
    - **Statique:** Périphériques ajoutés au groupe. Ils restent dans le groupe jusqu'à ce qu'ils soient supprimés ou que vous ne les gériez plus.
    - **Dynamique:** Périphériques qui correspondent à un ou plusieurs critères définis par une requête. Par exemple, un groupe peut contenir tous les serveurs qui sont actuellement dans un état d'avertissement. Ils restent dans le groupe tant qu'ils correspondent aux critères définis pour le groupe. Les périphériques sont ajoutés automatiquement aux groupes dynamiques lorsqu'ils satisfont les critères de requête du groupe.
4. Une fois terminé, cliquez sur **OK**.
5. Pour ajouter des périphériques au groupe statique, cliquez sur les périphériques dans le volet de droite de la liste Mes périphériques, cliquez sur Déplacer/Copier, sélectionnez le groupe, puis cliquez sur **OK**.

Configuration des périphériques pour la gestion

La découverte des périphériques ne les place pas automatiquement dans un groupe de gestion. Avant de pouvoir entièrement gérer des périphériques avec la console et recevoir des alertes de santé, vous devez y installer des agents de gestion. Vous pouvez choisir d'installer la configuration d'agent par défaut (qui installe tous les agents de gestion) ou de personnaliser votre propre configuration d'agent à installer sur vos périphériques. (Pour recevoir des alertes de santé, la configuration d'agent doit inclure l'agent de surveillance.)

Vous pouvez installer des agents de gestion par une des méthodes suivantes :

- Ciblez les périphériques de la liste Mes périphériques, puis planifiez une tâche de configuration d'agent pour installer à distance des agents sur les périphériques. (étapes ci-dessous)

- Mappez le partage LDlogon du serveur principal (//serveur_principal/ldlogon) et exécutez SERVERCONFIG.EXE. (les étapes sont indiquées à la section "Tirage des agents" dans le chapitre Installation et configuration d'un agent de périphérique du System Manager Guide d'utilisation)
- Créez d'un paquet d'installation de périphérique auto-extractible. Pour installer les agents, exécutez ce paquet localement sur le périphérique. Pour ce faire, vous devez être connecté avec des droits administratifs. (les étapes sont indiquées à la section "Installation d'un agent par un paquet d'installation" dans le chapitre Installation et configuration d'un agent de périphérique du System Manager Guide d'utilisation)

Pour pousser l'agent :

1. Ciblez les périphériques dans la liste Mes périphériques (comme expliqué ci-dessus dans la section Déplacement des périphériques vers la liste Mes périphériques)
2. Dans le volet de navigation de gauche, cliquez sur Configuration d'agent, cliquez avec le bouton droit de la souris sur la configuration que vous souhaitez pousser, et cliquez sur Planifier une tâche.
3. Dans le volet de gauche, cliquez sur Cibler les périphériques, et cliquez sur Ajouter la liste cible.
4. Cliquez sur Planifier une tâche, cliquez sur Démarrer maintenant pour démarrer immédiatement la tâche ou cliquez sur Démarrer ultérieurement et réglez la date et l'heure de démarrage de la tâche, puis cliquez sur Enregistrer.

Vous pouvez afficher l'état de la tâche dans l'onglet Tâches de configuration.

Installation des agents de serveur Linux

Vous pouvez déployer et installer à distance des RPM et des agents Linux sur des serveurs Linux. Pour ce faire, votre serveur Linux doit être correctement configuré. Pour configurer correctement un serveur Linux, suivez les instructions données dans la section "Installation des agents de serveur" dans le chapitre Installation et configuration d'un agent de périphérique du *System Manager Guide d'utilisation.*

Configuration des alertes

Lorsqu'un problème ou un autre événement se produit sur un périphérique (par exemple, si le périphérique ne dispose plus de suffisamment d'espace disque), System Manager peut envoyer une alerte. Vous pouvez personnaliser ces alertes en choisissant le niveau de sécurité ou le seuil de déclenchement de l'alerte. Les alertes sont envoyées à la console et peuvent être configurées pour effectuer certaines tâches. Vous pouvez configurer des alertes pour de nombreux événements ou problèmes possibles. Le logiciel contient un ensemble de règles d'alertes par défaut qui s'installe sur un périphérique géré lorsque le composant de surveillance est installé. Cet ensemble de règles d'alertes envoie des informations sur l'état de santé au console. Cet ensemble de règles par défaut inclut des alertes telles que :

- Disque ajouté ou supprimé
- Espace disque
- Utilisation de la mémoire
- Température, ventilateurs et tensions

- Surveillance de la performance
- Événement IPMI (sur le matériel applicable)

Pour en savoir plus sur les alertes, reportez-vous au chapitre Configuration des alertes dans le System Manager Guide d'utilisation.

Configuration des alertes

Lorsqu'un problème ou un autre événement se produit sur un périphérique (par exemple, si le périphérique ne dispose plus de suffisamment d'espace disque), System Manager peut envoyer une alerte. Vous pouvez personnaliser ces alertes en choisissant le niveau de sécurité ou le seuil de déclenchement de l'alerte. Les alertes sont envoyées à la console et peuvent être configurées pour effectuer certaines tâches. Vous pouvez configurer des alertes pour de nombreux événements ou problèmes possibles. Le logiciel contient un ensemble de règles d'alertes par défaut qui s'installe sur un périphérique géré lorsque le composant de surveillance est installé. Cet ensemble de règles d'alertes envoie des informations sur l'état de santé au console. Cet ensemble de règles par défaut inclut des alertes telles que :

- Disque ajouté ou supprimé
- Espace disque
- Utilisation de la mémoire
- Température, ventilateurs et tensions
- Surveillance de la performance

Pour en savoir plus sur les alertes, reportez-vous au chapitre Configuration des alertes dans le System Manager *Guide d'utilisation*.

Et ensuite ?

Server Manager est maintenant opérationnel. Vous n'avez utilisé qu'une partie des fonctions de Server Manager (telles que la découverte de périphériques et la configuration d'agents). Les guides complémentaires (le *Guide de déploiment et d'installation* et le *Guide d'utilisation*) contiennent des informations plus détaillées sur toutes les fonctions du logiciel. Vous y trouverez notamment les fonctions suivantes :

Mises à jour de logiciel: Établissez une sécurité permanente au niveau des correctifs sur l'ensemble des périphériques gérés de votre réseau. Vous pouvez automatiser les processus répétitifs de gestion des informations actuelles de vulnérabilité, d'estimation des vulnérabilités des divers systèmes d'exploitation exécutés sur les périphériques gérés, de téléchargement des fichiers exécutables appropriés de correctif, de correction de vulnérabilités via le déploiement et l'installation des correctifs nécessaires sur les périphériques affectés et de vérification du succès d'une installation de correctif.

Alerte: Assurez-vous d'être prévenu si un de vos périphériques atteint un seuil particulier. Comme elle se rapporte à la fonction de surveillance, l'alerte vous prévient de plusieurs façons. Par exemple, vous pouvez configurer une alerte si vous souhaitez être prévenu lorsque le niveau de stockage sur vos périphériques atteint les 95% (l'agent peut envoyer un message électronique ou numérique, redémarrer ou fermer un périphérique, ou ajouter des informations dans le fichier journal d'alertes).

Requêtes: Gérez votre réseau en recherchant et organisant les périphériques de la base de données principale selon des critères spécifiques établis par l'utilisateur ou le système. Vous pouvez rechercher dans la liste des périphériques gérés les critères qui correspondent à ceux que vous avez spécifiés (tels que tout ce qui appartient au bureau d'administration ou tout ce qui dispose de 256K de mémoire vive) et les regrouper selon leur plan d'exécution. Ces groupes peuvent être statiques (leurs membres ne peuvent être modifiés que manuellement) ou dynamiques (leurs membres changent lorsque les périphériques correspondent ou non à des critères spécifiques).

Distribution de logiciel: Crée des tâches pour distribuer des paquets logiciels (un ou plusieurs fichiers MSI, un fichier exécutable, un fichier de traitement par lot, des fichiers RPM (Linux) ou un paquet créé à l'aide du Générateur de paquet de LANDesk) aux périphériques cibles.

Surveillance: Surveillez l'intégrité d'un périphérique par l'intermédiaire d'un des types de surveillance pris en charge (surveillance ASIC directe, IPMI en-bande, IPMI hors-bande, CIM, etc.) La surveillance permet de suivre de nombreuses données sur vos périphériques, tels que les niveaux d'utilisation, les événements de SE, les processus et les services, la performance, et les détecteurs de matériel (ventilateurs, tensions, températures, etc.) L'Alerte est une fonction apparentée qui utilise l'agent de surveillance pour lancer des actions d'alerte.

Rapports: Générez toute une gamme de rapports spécialisés contenant des informations importantes sur les périphériques gérés de votre réseau.Server Manager utilise un utilitaire d'analyse d'inventaire pour ajouter des périphériques (et regrouper des données logicielles et matérielles sur ces périphériques) dans la base de données principale. Vous pouvez afficher et imprimer ces données d'inventaire depuis une vue d'inventaire de périphérique. Vous pouvez également définir des requêtes et regrouper des périphériques. Les Rapports utilisent ces données d'inventaire analysé en les regroupant et les organisant en rapports utiles ; ceci est particulièrement utile pour la création de rapports réglementaires.

Découverte de périphériques non gérés: Recherchez les périphériques qui ne sont pas gérés par la console. La Découverte est la première étape à effectuer si vous souhaitez préparer rapidement les nouveaux ordinateurs à la gestion. Vous pouvez configurer une tâche de découverte pour rechercher les nouveaux ordinateurs tous les mois.

Contrôle de la conformité des logiciels: Effectuez un suivi de conformité des licences. L'agent de contrôle de conformité des logiciels obtient des données (telles que le nombre total de minutes d'utilisation, le nombre de démarrages et la date du dernier démarrage de toutes les applications installées sur un périphérique) et stocke ces données dans le registre du périphérique. vous pouvez utiliser ces données pour surveiller les tendances d'utilisation et de refus du logiciel. L'agent contrôle passivement l'utilisation de produit sur les périphériques, en employant une bande passante de réseau minimale. L'agent continue à contrôler l'utilisation pour les périphériques mobiles déconnectés du réseau.

Déploiement de système d'exploitation: Déployez des images de SE vers les périphériques de votre réseau en utilisant l'outil de déploiement basé sur PXE. Ceci permet de créer une image des périphériques dotés d'un disque dur vierge ou d'un système d'exploitation inutilisable. Les représentants PXE de petits clients éliminent le besoin d'un serveur PXE dédié sur chaque sous-réseau. Le déploiement de système d'exploitation simplifie l'approvisionnement de nouveaux périphériques sans requérir l'interaction supplémentaire d'un technicien ou de l'utilisateur final une fois que le processus démarre.

Phase 1 : Conception du domaine de gestion

Dans la phase 1, vous rassemblerez des informations sur l'infrastructure du réseau et prendrez des décisions afin de vous aider à personnaliser le domaine de gestion.

Cette phase traite des sujets suivants :

Rassemblement des informations de réseau

Identification et collecte d'informations critiques sur le réseau et relatives à System Manager. Vous devez spécifiquement :

- Déterminer des configurations de périphérique
- Sélectionner le serveur principal

Sélection du serveur principal

Le serveur principal est le centre d'un domaine de gestion. Tous les fichiers et services clés sont situés sur le serveur principal. Physiquement, il peut être un nouveau serveur ou un serveur redéfini.

Utilisez un navigateur sur un poste de travail distant pour exécuter la console d'administrateur, à partir de laquelle vous dirigez des activités de gestion telles que la gestion d'alertes, l'interrogation de la base de données principale ou la création de scripts personnalisés.

Assurez-vous que le serveur que vous sélectionnez comme serveur principal satisfait les exigences système. Reportez-vous à la section Exigences système, plus loin dans cette phase.

Planification du positionnement des fichiers du programme

Durant l'installation, vous pouvez spécifier l'emplacement de l'installation des fichiers du programme. Sauf en cas de raisons spécifiques, acceptez les répertoires de destination par défaut. Si vous modifiez le répertoire de destination, le chemin du répertoire de destination ne peut pas contenir de caractères à deux octets.

Le répertoire de destination par défaut des fichiers du serveur principal est le suivant :

```
C:\Program Files\LANDesk\ManagementSuite
```

La base de données principale

System Manager installe une base de données MSDE sur le serveur principal. Chaque base de données MSDE présente une limite de taille de base de données de 2 Go. Le nombre de serveurs pris en charge par cette base de données dépend de la taille du fichier d'analyse d'inventaire du réseau.

Vous observerez vraisemblablement des problèmes de performances de la base de données MSDE lorsqu'elle exécute simultanément plus de cinq tâches. Par exemple, lorsque cinq administrateurs System Manager accèdent à la base de donnée exactement au même moment.

Sécurité du client / serveur principal

Ce produit utilise un système d'authentification basé sur les certificats. Durant l'installation du serveur principal, le programme d'installation crée un certificat pour celui-ci. Les clients recherchent ce certificat lors de la communication avec le serveur principal et ne communiquent pas avec un serveur principal pour lequel ils ne possèdent pas de certificat.

Les périphériques communiqueront uniquement avec les serveurs principaux pour lesquels le périphérique possède un fichier de certificat approuvé correspondant. Chaque serveur principal dispose de ses propres clés privées et certificat et, par défaut, les agents de client que vous déployez à partir de chaque serveur principal communiqueront uniquement avec le serveur principal à partir duquel le logiciel est déployé.

Planification d'une portée

L'administration basée sur les rôles est une puissante fonction de la gestion de sécurité. Accédez aux outils de l'administration basée sur les rôles de la console en cliquant sur Utilisateurs dans le volet de gauche. Vous devez être connecté avec des droits administratifs.

L'administration basée sur les rôles fournit des possibilités avancées de gestion du périphérique en permettant d'ajouter des utilisateurs au système et en leur attribuant des droits et des portées. Les droits déterminent les outils et fonctions qu'un utilisateur peut visualiser et employer (voir la section "Présentation des droits" du Guide d'utilisation Server Manager). La portée détermine la plage de périphériques qu'un utilisateur peut visualiser et gérer (voir la section "Création de portées" du Guide d'utilisation Server Manager).

Vous pouvez créer des rôles sur la base des responsabilités des utilisateurs, les tâches de gestion qu'ils doivent effectuer et les périphériques que vous souhaitez qu'ils puissent visualiser, accéder et gérer. L'accès aux périphériques peut être restreint à un emplacement géographique tel qu'un pays, une région, un département, une ville ou même un groupe ou type de serveur spécifique.

Pour mettre en œuvre ce type d'administration basée sur les rôles à travers le réseau, il suffit de configurer les utilisateurs actuels, ou de créer et d'ajouter de nouveaux utilisateurs du produit, puis de leur attribuer les droits nécessaires (sur les fonctions du produit) et une portée (sur les périphériques gérés).

Le serveur principal utilise les portées pour limiter les périphériques que les utilisateurs de console peuvent voir. Plusieurs portées peuvent être attribuées à un utilisateur, et chaque portée peut être utilisée par plusieurs utilisateurs. Vous pouvez baser les portées sur une des méthodes suivantes :

- (Option par défaut) **Portée Toutes les machines:** Les utilisateurs peuvent visualiser tous les périphériques.
- **Basé sur une requête:** Les utilisateurs peuvent voir les périphériques qui satisfont les critères sélectionnés d'une requête spécifique qui leur est attribuée par l'administrateur.
- **Basé sur un groupe:** Les utilisateurs peuvent visualiser tous les périphériques qui satisfont les critères du groupe.

Pour plus d'informations sur les portées, reportez-vous au Server Manager*Guide d'utilisation*.

Exigences système

Vérifiez que les exigences système ci-dessous sont respectées avant d'installer le produit. Le programme de vérification d'exigences le vérifie pour vous.

Serveur principal et serveurs de bases de données

Assurez-vous que le serveur principal et les serveurs de base de données respectent les exigences introduites dans la présentation.

- Windows 2000 Server ou Advanced Server avec SP 4, ou Windows Server 2003 édition Standard ou Enterprise x86 SP1 ou Windows 2003 R2
- Microsoft Data Access Components (MDAC) 2.8 ou ultérieur
- Microsoft .NET Framework 1.1
- Internet Information Services (IIS)
- Prise en charge IIS pour la création de scripts ASP.NET v1.1
- Internet Explorer 6.0 SP1 ou ultérieur
- Système de fichiers Microsoft NT (NTFS)
- Le serveur Windows que vous utilisez comme serveur principal doit être installé en tant que serveur autonome et non en tant que contrôleur principal de domaine (PDC), contrôleur secondaire de domaine (BDC) ou contrôleur de domaine Active Directory.
- SNMP doit être installé et SNMP et les services de trappe SNMP doivent être lancés
- 200 Mo d'espace disponible sur le lecteur système et 900 Mo d'espace disponible sur au moins un lecteur
- Privilèges d'administrateur
- La version du client LANDesk est correcte ou il n'est pas installé

Exigences du serveur principal
Le fichier de page Windows doit avoir une taille minimum de 12 + *N* (où *N* est le nombre de mégaoctets de mémoire RAM sur le serveur principal). Dans le cas contraire, les applications du produit peuvent générer des erreurs de mémoire.

Si vous planifiez d'installer les produits Management Suite et Server Manager sur un même serveur principal, il est recommandé que la mémoire de l'ordinateur principal ait 1gigaoctet à sa disposition.

Tous les services du produit doivent être hébergés sur un serveur

Pour les domaines de gestion plus petits, vous pouvez installer le serveur principal et la base de donnée principale sur un serveur. Pour ces réseaux, vous pouvez souhaiter envisager d'utiliser la base de données Microsoft MSDE par défaut, dont la gestion est généralement plus simple. Il s'agit de la seule option de base de données pour System Manager.

Considérations relatives aux limitations

Avant d'installer le serveur principal et la base de données, le serveur doit satisfaire au minimum les exigences système suivantes :

- Processeur Pentium 4
- 4 Go d'espace disque disponible sur les lecteurs d'une vitesse de 10 000 tr/mn ou plus rapides
- 768 Mo de mémoire RAM au minimum

Ordinateurs serveur gérés

Ce produit prend en charge les systèmes d'exploitation de serveur suivants (tous les systèmes d'exploitation ne sont pas pris en charge de la même manière) :

- Microsoft Windows 2000 Server (avec SP4)
- Microsoft Windows 2000 Advanced Server (avec SP4)
- Microsoft Windows 2000 Professional (avec SP4)
- Microsoft Windows 2003 Server R2
- Microsoft Windows 2003 Server R2 Standard Edition x86
- Microsoft Windows 2003 Server R2 Standard x64 Edition
- Microsoft Windows 2003 Server R2 Enterprise Edition x86
- Microsoft Windows 2003 Server R2 Enterprise x64 Edition
- Microsoft Windows XP Professional (avec SP2)
- Microsoft Windows XP Professional x64 (avec SP2)
- Windows Small Business Server 2000 (avec SP4)
- Windows Small Business Server 2003 (avec SP1)
- Red Hat Enterprise Linux v3 (ES) 32 bits - U6
- Red Hat Enterprise Linux v3 (ES) EM64t - U6
- Red Hat Enterprise Linux v3 WS 32 bits - U6
- Red Hat Enterprise Linux v3 WS EM64t - U6
- Red Hat Enterprise Linux v3 (AS) 32 bits - U6
- Red Hat Enterprise Linux v3 (AS) EM64t - U6
- Red Hat Enterprise Linux v4 (ES) 32 bits – U3
- Red Hat Enterprise Linux v4 (ES) EM64t – U3
- Red Hat Enterprise Linux v4 (AS) 32 bits – U3
- Red Hat Enterprise Linux v4 (AS) EM64t – U3
- Red Hat Enterprise Linux v4 WS 32 bits – U3
- Red Hat Enterprise Linux v4 WS EM64t – U3
- SUSE* Linux Server 9 ES 32 bits SP2

- SUSE Linux Server 9 EM64t SP2
- SUSE Linux Server 10 ES 32-bit
- SUSE Linux Server 10 EM64t
- SUSE Linux Professional 9.3
- SUSE Linux Professional 9.3 EM64t
- HP-UX 11.1
- Unix AIX

Ordinateurs serveur gérés Linux

La liste ci-dessous répertorie les exigences de pare-feu et RPM requises pour activer les périphériques Linux pour la gestion.

Pare-feu

Pour initialement installer l'agent de gestion et configurer un serveur Linux afin qu'il communique avec le serveur principal (en utilisant la méthode "push"), les connexions SSH doivent être autorisées à passer au travers du pare-feu local du serveur Linux:

22 - TCP uniquement

Pour que les agents puissent communiquer avec les serveurs principaux (pour des analyses d'inventaire, distributions de logiciel, mises à jour de vulnérabilité, etc.), le pare-feu local du serveur Linux doit être configuré pour autoriser la communication sur les ports suivants :

9593 - TCP uniquement

9594 - TCP uniquement

9595 - TCP et UDP

Pour communiquer avec l'agent de gestion, le pare-feu local du serveur Linux doit être configuré pour autoriser la communication sur les ports suivants :

6780 - TCP uniquement

RPM requis (version # ou ultérieure)

Il est recommandé de stocker tous les RPM dans le répertoire ...\ManagementSuite\ldlogon\RPMS. Vous pouvez passer à ce répertoire via http://nom_serveur_principal/RPMS.

REDHAT_ENTERPRISE

python

Version RPM : 2.2.3-5 (RH3)

2.3.4-14 (RH4)

Version Binaire : 2.2.3

pygtk2

Version RPM : 1.99.16-8 (RH3)

2.4.0-1 (RH4)

Version Binaire :

sudo

Version RPM : 1.6.7p5-1

Version Binaire : 1.6.7.p5

bash Version RPM : 2.05b-29 (RH3)

3.0-19.2 (RH4)

Version Binaire : 2.05b.0(1)-version

xinetd Version RPM : 2.3.12-2.3E (RH3)

2.3.13-4 (RH4)

Version Binaire : 2.3.12

mozilla Version RPM : 1.7.3-18.EL4 (RH4)

Version Binaire : 1.5

openssl Version RPM : 0.9.7a-22.1 (RH3)

0.9.7a-43.1 (RH4)

Version Binaire : 0.9.7a

sysstat Version RPM : 4.0.7-4

Version Binaire : 4.0.7

lm_sensors

Version RPM : 2.6 (cette version peut ne pas être suffisante pour afficher les détecteurs sur les nouveaux ordinateurs ASIC. Pour obtenir plus d'informations, consultez la documentation de lm_sensors ou le site Web (http://www2.lm-sensors.nu/~lm78).)

SUSE LINUX

(SUSE 64)

bash

Version RPM : 2.05b-305.6

mozilla

Version RPM : 1.6-74.14

net-snmp

Version RPM : 5.1-80.9

openssl

Version RPM : 0.9.7d-15.13

python-gtk

Version RPM : 2.0.0-215.1 [remarque : modification du nom du paquet]

python

Version RPM : 2.3.3-88.1

sudo

Version RPM : 1.6.7p5-117.1

sysstat

Version RPM : 5.0.1-35.1

xinetd

Version RPM : 2.3.13-39.3

lm_sensors

Version RPM : S/O (remarque : incorporé dans le noyau pour la version 2.6)

Utilisation du port du produit

Introduction

Lorsque vous utilisez ce produit dans un environnement qui inclut des pare-feux (ou routeur qui filtre le trafic), vous pouvez avoir besoin de régler les configurations du routeur ou du pare-feu pour permettre à ce produit de fonctionner. Cette section décrit les ports utilisés par les divers

composants du produit. Les informations incluses ici se concentrent sur les informations nécessaires pour configurer les routeurs et pare-feux et ignorent les ports qui sont uniquement utilisés localement (dans des sous-réseaux individuels).

Informations récapitulatives sur les règles de pare-feu

Ces informations s'appliquent à la configuration des règles de pare-feu. Si vous n'êtes pas familier avec ce sujet, cette section fournit des informations récapitulatives générales relatives aux concepts principaux.

Règles de pare-feu

"Ouverture d'un port" n'est pas un terme exacte. Vous ne pouvez pas simplement aller à un pare-feu et "ouvrir un port". L'ouverture d'un port est une expression abrégée pour la configuration d'une règle de pare-feu. Les règles de pare-feu décrivent quel trafic est autorisé ou pas à travers le pare-feu. Les règles de pare-feu ne filtrent pas le trafic uniquement en fonction du numéro de port. Les règles peuvent être basées sur les protocoles, les numéros de port source et de destination, la direction (entrant/sortant), les adresses IP source et de destination, etc.

Une règle de pare-feu typique ressemble à la règle suivante : "autoriser le trafic entrant sur le port TCP 9535". Pour l'utilisation de ce produit, cette règle est nécessaire pour prendre en charge le contrôle distant. La règle est basée sur trois éléments :

1. Le protocole (TCP ou UDP)
2. Le numéro de port
3. La direction (entrante ou sortante)

Ces trois éléments sont requis pour configurer les règles de pare-feu.

Ports de destination et source, ports dynamiques

Il y a toujours deux ports impliqués dans la communication TCP ou UDP. Tout paquet TCP ou UDP passe d'un port source à un port de destination. Les règles de pare-feu sont basées sur le port source, le port de destination ou les deux. Les ports répertoriés dans des documents tels que celui-ci sont toujours des ports de destination.

Les ports bien connus tels que le port 5007 (utilisé par le service d'inventaire) font référence uniquement à un seul côté de la communication. L'autre côté de la communication utilise un port dynamique. Les ports dynamiques sont automatiquement attribués par le système d'exploitation entre 1024 et 5000.

Pare-feux et trafic UPD

Pour autoriser le trafic TCP à travers un pare-feu, une règle unique est suffisante (par exemple, pour autoriser les connexions TCP entrantes au port 5007). Une fois la connexion TCP établie, les données peuvent être transmises dans les deux sens via la connexion.

Le trafic UDP est différent car il n'utilise pas de connexion. Par exemple, par défaut, le serveur principal effectue un sondage "ping" des périphériques au port UDP 38293 avant de lancer une

tâche. Une règle de pare-feu qui autorise les paquets UDP sortants au port 38293 autorise les paquets du serveur principal sur un périphérique en dehors du pare-feu, mais n'autorise pas les paquets de réponse du périphérique.

Une règle qui autorise les paquets sortants et entrants au port 38293 ne fonctionne pas non plus car un seul côté de la communication écoute sur le port bien connu. L'autre côté utilise un port dynamique. Dans la mesure où les paquets sortants du serveur principal passent d'un port dynamique au port 38293, les paquets de réponse du périphérique passent du port 38293 au même port dynamique, et non pas au port 38293. Pour autoriser la communication dans les deux sens, vous devez disposer d'une règle qui autorise les paquets UPD avec un port source ou un port de destination égal au port 38293. Une règle de ce type est généralement acceptable sur l'intranet mais pas sur un pare-feu externe (car elle autoriserait des paquets entrants sur tout les ports UDP).

Pour cette raison, le trafic UDP n'est en général pas considéré comme étant "facile à utiliser avec les pare-feux". Pour revenir à l'exemple, il existe une alternative au port UDP 38293 : le port TCP 9595. Lors de la gestion de périphériques à travers un pare-feu, il est préférable de configurer le produit pour utiliser le port TCP.

Ports utilisés

Port	Direction	Protocole	Service
31770	console vers périphérique, périphérique vers serveur principal	TCP	communication entre la console et le périphérique
6787	console vers périphérique	TCP	communication entre la console et le périphérique
9595	console vers périphérique	UDP	découverte
9595	console vers périphérique	TCP	configuration d'agent
623	console vers périphérique	UDP	découverte ASF, IPMI
9535	console vers périphérique	TCP	contrôle distant

Ce produit doit découvrir des nœuds dotés de l'agent de gestion avant de pouvoir les gérer. Le port UDP 9595 est utilisé pour la découverte. Vous pouvez également ajouter manuellement des périphériques individuels à la console, mais le périphérique doit tout de même répondre à un

"ping" sur le port UDP 9595. La communication entre la console et le périphérique utilise les ports TCP 31770 et 6787. Le trafic sur ce dernier port est basé sur HTTP. Le port UDP 623 est utilisé pour la découverte ASF (alert standard forum). En outre, il utilise le port TCP 9535 pour le contrôle distant. La découverte IPMI est liée à la découverte ASF et utilise le même port (udp/623).

Phase 2: Installation du serveur principal

Cette phase se concentre sur l'installation du serveur principal.

Cette phase traite des sujets suivants :

- Installation du serveur principal
- Activation du serveur principal
- Déploiement vers des périphériques Windows
- Déploiement vers des périphériques Linux

L'installation des composants présentés dans cette phase dure 30 à 60 minutes.

Installation du serveur principal

Pour installer le serveur principal

Avant de démarrer l'installation, il est recommandé de fermer toutes les autres applications et d'enregistrer tous les fichiers ouverts. Sur le serveur Windows 2000/2003 sélectionné pour agir comme serveur principal :

1. Insérez le support du produit dans le lecteur ou exécutez le fichier AUTORUN.EXE à partir de l'image d'installation. L'écran d'exécution automatique (Autorun) s'affiche.
2. Cliquez sur **Vérifier les conditions requises et installer**.
3. Le programme de vérification des exigences système vérifie que le serveur satisfait les exigences système minimales. Assurez-vous de respecter toutes les exigences. Si tel n'est pas le cas, cliquez sur **Echec** sur le lien des exigences échouées pour obtenir des liens ou des informations relatives à l'installation des exigences non satisfaites.
4. Cliquez sur **Installer maintenant** pour exécuter le programme d'installation.
5. Sélectionnez la langue à installer par le programme d'installation. Cliquez sur **OK**.
6. Un écran de bienvenu s'affiche. Cliquez sur **Suivant** pour continuer.
7. Dans l'écran Contrat de licence, cliquez sur **J'accepte les termes du contrat de licence** pour continuer. Cliquez sur **Suivant**.
8. Acceptez le dossier de destination par défaut ou spécifiez un dossier de destination personnalisé, puis cliquez sur **Suivant**. Le chemin du dossier de destination ne peut pas contenir des caractères à deux octets. Si vous modifiez ce dossiez, souvenez-vous de remplacer votre chemin par tout chemin présenté dans la documentation du produit.
9. Entrez un mot de passe de base de données MSDE. Mémorisez ce mot de passe ou prenez-en note. Cliquez sur **Suivant** pour continuer.
10. Entrez le nom d'une organisation et d'un certificat pour le certificat de sécurité du serveur principal. Ces informations aident à nommer le certificat et à le décrire. Cliquez sur **Suivant**.
11. Sur la page Prêt à installer, cliquez sur **Installer**. L'installation du produit démarre.
12. La boîte de dialogue **Assistant d'installation terminé** s'affiche à la fin de l'installation.
13. Cliquez sur **Terminer**.

14. Le programme d'installation vous invite à redémarrer le serveur. Vous devez cliquer sur **Oui** pour terminer l'installation. Vous remarquerez qu'après avoir redémarré et vous être connecté, le programme d'installation s'exécute pendant encore quelques minutes avant d'achever l'installation. Le programme d'installation ne vous invite pas à fournir des informations supplémentaires durant le premier redémarrage.

Lors de l'installation d'une base de données principale MSDE sur un serveur Windows 2003, Windows peut interrompre l'installation et demander si vous acceptez d'ouvrir SETUP.EXE. Si cette invite apparaît, cliquez sur Ouvrir ou le produit ne sera pas installé correctement.
Si vous voulez installer Intel Platform Extensions pour LANDesk Software, suivez les instructions de l'Assistant qui s'ouvre après l'installation de Server Manager.

Activation du serveur principal

Vous devez activer le serveur principal avant de pouvoir utiliser les produits System Manager sur ce serveur. Vous pouvez activer le serveur principal automatiquement via Internet ou manuellement par courrier électronique. Vous pouvez être amené à réactiver un serveur principal si vous modifiez de manière significative sa configuration matérielle.

Le composant d'activation sur le serveur principal génèrera régulièrement des données concernant :

- le nombre exact des périphériques que vous utilisez ;
- la configuration matérielle chiffrée non personnelle ;
- les programmes spécifiques LANDesk Software que vous utilisez (collectivement, les "données de nombre de nœuds").

Aucune autre donnée n'est collectée ou générée par l'activation. Le code clé de matériel est généré sur le serveur principal à l'aide des facteurs de configuration matérielle non personnelle, tels que la taille du disque dur, la vitesse de traitement de l'ordinateur, etc. Le code clé de matériel est envoyé à LANDesk dans un format codé et la clé privée de codage réside uniquement sur le serveur principal. Le code clé de matériel est alors utilisé par LANDesk Software pour créer une partie du certificat d'autorisation.

Une fois le serveur principal installé, l'utilitaire d'activation du serveur principal (**Démarrer | Programmes | LANDesk | Activation du serveur principal**) s'exécute au premier redémarrage et active le serveur principal avec le nom d'utilisateur et le mot de passe fournit par l'OEM.

Vous pouvez passer de System Manager à Server Manager ou Management Suite grâce à l'utilitaire d'activation du serveur principal. Voir Utilisation de System Manager avec Management Suite ou Server Manager.

Une fois le serveur principal activé, vous pouvez utiliser la boîte de dialogue **Préférences | Licence** de la console pour afficher les informations sur l'attribution des licences. La licence OEM d'Intel vous permet d'exécuter un agent de produit sur toutes les cartes mère ou serveurs Intel.

Utilitaire d'activation du serveur principal

Utilisez l'utilitaire d'activation du serveur principal pour activer un nouveau serveur pour la première fois. Lancez l'utilitaire en cliquant sur **Démarrer | Programmes | LANDesk | Activation**

du serveur principal. Si votre serveur principal n'est pas doté d'une connexion Internet, reportez-vous à la section "Activation manuelle d'un serveur principal ou vérification des données de nombre de serveurs", plus loin dans cette section.

Chaque serveur principal doit utiliser un certificat d'autorisation unique.

Le serveur principal vérifie régulièrement les licences en générant le fichier "\Program Files\LANDesk\Authorization Files\LANDesk.usage". Ce fichier est régulièrement envoyé au serveur de mise sous licence de LANDesk Software. Il s'agit d'un fichier au format XML codé et signé numériquement. Toute modification manuelle de ce fichier annule le contenu et le rapport d'utilisation suivant pour le serveur de mise sous licence de LANDesk Software.

Le serveur principal communique avec le serveur de mise sous licence de LANDesk Software via HTTP. Si vous utilisez un serveur proxy, cliquez sur l'onglet **Proxy** de l'utilitaire et entrez les informations correspondantes. Si votre serveur principal utilise une connexion Internet, la communication avec le serveur de licences est automatique et n'exige aucune intervention de votre part.

Notez que l'utilitaire Activation du serveur principal ne démarre pas automatiquement une connexion Internet à distance, mais si vous lancez manuellement celle-ci, puis exécutez l'utilitaire d'activation, il peut utiliser la connexion à distance pour rapporter les données d'utilisation.

Si votre serveur principal n'utilise pas de connexion Internet, vous pouvez vérifier et envoyer le nombre de serveurs manuellement, comme décrit plus loin dans cette section.

Activation du serveur principal

Pour activer un serveur

1. Cliquez sur **Démarrer | Programmes | LANDesk | Activation du serveur principal**.
2. Cliquez sur **Activer ce serveur principal** à l'aide de votre nom de contact et mot de passe LANDesk.

Le nom de contact et le mot de passe sont founis automatiquement.

Activation d'un serveur principal ou vérification des données de nombre de serveurs manuellement

Si le serveur principal n'utilise pas de connexion Internet, l'utilitaire Activation du serveur principal ne peut pas envoyer les données de nombre de serveurs. Un message vous invite donc à envoyer manuellement les données de vérification de nombre de serveurs et d'activation par courrier électronique. L'activation par courrier électronique est simple et rapide. Lorsque le message d'activation manuelle s'affiche sur le serveur principal, ou si vous vous servez de l'utilitaire d'activation du serveur principal, suivez les étapes ci-après.

Pour activer un serveur principal ou vérifier des données de nombre de serveurs manuellement

1. Lorsque le serveur principal vous invite à vérifier manuellement les données de nombre de serveurs, il crée un fichier de données nommé activate.txt dans le dossier "\Program Files\LANDesk\Authorization Files". Attachez ce fichier à un message électronique et envoyez-le à licensing@landesk.com. L'objet et le texte du message n'ont pas d'importance.
2. LANDesk Software traite le message joint et répond à l'adresse électronique depuis laquelle vous avez envoyé le message. Le message de LANDesk Software fournit des instructions et un nouveau fichier d'autorisation.
3. Enregistrez le fichier d'autorisation joint dans le dossier "\Program Files\LANDesk\Authorization Files". Le serveur principal traite immédiatement le fichier et met à jour son état d'activation.

Si l'activation manuelle échoue ou si le serveur principal ne peut pas traiter le fichier d'activation joint, le fichier d'autorisation que vous avez copié est renommé avec l'extension .rejected et l'utilitaire crée un événement plus détaillé dans le journal d'application de l'observateur d'événements de Windows.

Connexion à la console

Une fois que le programme d'installation est terminé, que le serveur principal a redémarré et qu'il est activé, démarrez la console en ouvrant un navigateur et en tapant l'adresse du serveur selon le format suivant : http://nom_serveur/ldsm. (Dans le serveur principal, cliquez sur Démarrer | Programmes | LANDesk | System Manager) Au démarrage de la console, la fenêtre de connexion apparaît. Vous pouvez être invité à saisir les références d'authentification du compte ayant installé LDSM afin de vous connecter. Seul les membres du groupe LANDesk Management Suite sur le serveur principal peuvent se connecter. Par défaut, le programme d'installation a ajouté au groupe LANDesk Management Suite l'utilisateur sous lequel vous étiez connecté lors de l'installation du serveur principal. Si vous souhaitez que d'autres utilisateurs puissent accéder à la console, ajoutez-les à ce groupe.

La console peut mettre 90 secondes avant de s'afficher lorsque vous l'ouvrez pour la première fois dans un navigateur. Ce délai se produit car le serveur doit réaliser une compilation unique de certains codes. Le prochain lancement de la console sera beaucoup plus rapide.

Déploiement vers des périphériques Windows

Ce produit prend en charge une méthode de configuration en mode Push planifiée qui permet de déployer des agents à distance.

Pour activer une configuration en mode Push de serveurs Windows 2000/2003 qui n'exécutent pas déjà l'agent de gestion standard, vous devez fournir les références de connexion appropriées comme suit :

1. Dans le serveur principal, cliquez sur **Démarrer | Programmes | LANDesk |** LANDesk**Configuration des services**, puis cliquez sur l'onglet **Planificateur**.

2. Cliquez sur **Modifier la connexion**.
3. Dans les champs **Nom d'utilisateur et Mot de passe**, spécifiez un compte d'administrateur de domaine (utilisez le format domaine\nom_utilisateur).
4. Arrêtez et redémarrez le service Planificateur.
5. Dans la console Web, ciblez les périphériques souhaités, puis cliquez sur **Configuration d'agent > Tâches planifiées** pour déployer les configurations.

Vous pouvez spécifier l'administrateur de domaine lors de la configuration de membres Windows 2000/2003 qui appartiennent au même domaine que le serveur principal. Pour configurer des serveurs Windows 2000/2003 dans d'autres domaines, vous devez définir des relations d'approbation. Gardez à l'esprit que le compte identifié à l'étape 3 ci-dessus est celui sous lequel le service Planificateur sera exécuté sur le serveur principal. Assurez-vous que le compte dispose du droit **Ouvrir la session en tant que service**.

Si la configuration en mode Push échoue et affiche le message "Impossible de trouver l'agent", essayez la procédure ci-dessous pour identifier le problème. Cette procédure réplique les actions du Planificateur lors d'une configuration en mode Push.

1. Recherchez le nom d'utilisateur sous lequel le service Planificateur est exécuté.
2. Sur le serveur principal, connectez-vous avec le nom d'utilisateur trouvé à l'étape 1.
3. Mappez un lecteur sur \\nom_serveur\C$. (Cette étape est celle qui échouera probablement. Elle peut échouer pour deux raisons. Très certainement, vous ne disposez pas de droits administratifs sur le serveur. Si ce nom d'utilisateur ne dispose pas de droits administratifs, il est possible que le partage administratif du serveur (C$) soit désactivé.)
4. Créez un répertoire \\nom_serveur\C$\$ldtemp$ et copiez un fichier vers celui-ci.
5. Utilisez le Gestionnaire de services Windows et essayez de démarrer et d'arrêter des services sur le serveur.

S'il s'agit d'un périphérique doté de IPMI, vous devez fournir le mot de passe BMC. Utilisez l'onglet **Mot de passe** de **Configuration des services** pour créer un mot de passe pour le contrôleur de gestion de la carte de base (BMC) IPMI.

1. Dans l'onglet **Mot de passe BMC**, renseignez la zone de texte **Mot de passe**, retapez le mot de passe dans la zone de texte **Confirmer le mot de passe**, puis cliquez sur **OK**.

Le mot de passe ne peut pas contenir plus de 15 caractères qui doivent correspondre à des chiffres compris entre 0 et 9 ou à des lettres majuscules/minuscule de a-z.

Si le périphérique est doté de la technologie Intel* AMT, vous devez fournir le mot de passe Intel AMT. Utilisez l'onglet **Configuration Intel AMT** de **Configuration des services** pour créer ou modifier le mot de passe sur les périphériques dotés d'Intel* Active Management Technology.

Pour configurer un mot de passe Intel AMT

1. Dans l'onglet **Configuration Intel AMT**, entrez le mot de passe et le nom d'utilisateur actuels. Ces derniers doivent correspondre au nom d'utilisateur et au mot de passe configurés dans l'écran Configuration d'Intel AMT (accessible dans les paramètres BIOS de l'ordinateur).
2. Pour modifier le nom d'utilisateur et le mot de passe, renseignez la section **Nouveau mot de passe d'Intel AMT**.
3. Cliquez sur **OK**. Cette modification est appliquée lorsque la configuration du client est exécutée.

Remarque: Le nouveau mot de passe doit correspondre à un mot de passe fort. C'est-à-dire que le mot de passe doit :

- Avoir au moins sept caractères
- Contenir des lettres, des chiffres et des symboles
- Disposer d'au moins un symbole entre la deuxième et sixième position.
- Etre différent de manière significative des mots de passe précédents
- Ne pas contenir des noms ou des noms d'utilisateur
- Ne pas être un nom ou mot courant

Déploiement vers des périphériques Linux

Vous pouvez déployer et installer à distance des RPM et des agents Linux sur des serveurs Linux. Pour ce faire, votre serveur Linux doit être correctement configuré. Pour installer un agent sur un serveur Linux, vous devez disposer des privilèges racine.

L'installation par défaut de Linux (Red Hat 3 et 4, et SUSE) inclut les RPM requis par l'agent de gestion standard de Linux. Si vous sélectionnez l'agent de surveillance dans Configuration d'agent, vous devez disposer d'un RPM supplémentaire, sysstat.

Pour une configuration initiale de l'agent Linux, le serveur principal utilise une connexion SSH pour cibler les serveurs Linux. Vous devez disposer d'une connexion SSH fonctionnelle avec une authentification par nom d'utilisateur et mot de passe. Ce produit ne prend pas en charge l'authentification par clé publique/clé privée. Tout pare-feu entre le serveur principal et les serveurs Linux doit autoriser le port SSH. Il est recommandé de tester votre connexion SSH depuis le serveur principal via une application SSH d'un tierce parti.

Le paquet d'installation de l'agent Linux est composé d'un script shell, de tarballs d'agent, d'une configuration d'agent .INI et de certificats d'authentification d'agent. Ces fichiers sont stockés dans le partage LDLogon du serveur principal. Le script Shell extrait des fichiers des tarballs, installe des RPM et configure le serveur pour charger des agents et exécuter périodiquement le scanner d'inventaire suivant l'intervalle spécifié dans la configuration d'agent. Les fichiers sont placés dans le dossier /usr/landesk.

Vous devez également configurer le service Planificateur sur le serveur principal pour utiliser les références d'authentification SSH (nom d'utilisateur/mot de passe) sur votre serveur Linux. Le service Planificateur utilise ces références pour installer les agents sur vos serveurs. Utilisez l'utilitaire Configuration des services pour entrer les références SSH qui seront utilisées par le service Planificateur en tant qu'autres références. Le système devrait vous inviter à redémarrer le service Planificateur. Si tel n'est pas le cas, cliquez sur Arrêter puis sur Démarrer dans l'onglet **Planificateur** pour redémarrer le service. Vos modifications sont alors activées.

Une fois vos serveurs Linux configurés et vos références d'authentification Linux ajoutées au serveur principal, vous devez ajouter des serveurs dans la vue **Mes périphériques** afin de pouvoir déployer vos agents Linux. Avant de pouvoir déployer un serveur, vous devez l'ajouter dans la liste **Mes périphériques**. Pour l'ajouter, découvrez votre serveur Linux en utilisant la fonction Découvrir des périphériques.

Pour découvrir vos serveurs Linux

1. Dans Découverte de périphériques, créez une tâche de découverte pour chaque serveur Linux. Utilisez une analyse de réseau standard et entrez l'adresse IP du serveur Linux pour la plage d'adresses IP de début et de fin. Si vous disposez de beaucoup de serveurs Linux, entrez une plage d'adresses IP. Une fois votre plage d'adresses IP de découverte ajoutée, cliquez sur OK.
2. Planifiez la tâche de découverte que vous venez de créer en la sélectionnant puis en cliquant sur **Planifier**. Une fois la tâche terminée, assurez-vous que la découverte de périphériques non gérés a trouvé les serveurs Linux à gérer.
3. Dans Découverte de périphériques, sélectionnez les serveurs à gérer, cliquez sur **Cible** pour ajouter les périphériques sélectionnés dans la liste Cible. Cliquez sur l'onglet **Gérer** situé dans la partie inférieure de la fenêtre. Cliquez sur **Déplacer les périphériques sélectionnés** et cliquez sur **Déplacer**. Les serveurs sont ajoutés dans la liste **Mes périphériques**, à partir de laquelle vous pouvez les cibler pour le déploiement.

Pour créer une configuration d'agent Linux

1. Dans Configuration d'agent, cliquez sur **Nouveau**.
2. Entrez un nom de configuration, cliquez sur HP-UX ou sur Linux Server Edition, puis cliquez sur **OK**.
3. Sélectionnez la configuration que vous venez de créer et cliquez sur **Modifier**.
4. Sélectionnez les agents que vous souhaitez utiliser.
5. Dans l'onglet Inventaire, sélectionnez les options et les intervalles de fréquence d'analyse souhaités. Le script d'installation ajoutera une tâche qui exécute le scanner à l'intervalle sélectionné.
6. Cliquez sur **Enregistrer les modifications**.

Pour déployer votre configuration d'agent, sélectionnez-la dans Configuration d'agent et cliquez sur **Planifier une tâche**. Configurez la tâche et surveillez sa progression dans Tâches de configuration.

Remarque: Vous ne recevrez pas d'informations relatives à la santé d'un ordinateur Linux avant que le scanner d'inventaire termine sa première analyse après l'installation. **Pour tirer une configuration d'agent Linux**

1. Créez un répertoire temporaire sur votre ordinateur Linux (par exemple, /tmp/ldcfg), et copiez ce qui suit dans le répertoire :
    1. Tous les fichiers du répertoire LDLOGON\unix\linux.
    2. Copiez dans le répertoire temporaire le script Shell nommé en fonction de la configuration (<nom de la configuration>.sh).
    3. Copiez dans le répertoire temporaire le fichier *.0 nommé en fonction de la configuration. L'astérisque (*) représente huit caractères (0-9, a-f).
    4. Copiez dans le répertoire temporaire tous les fichiers répertoriés dans le fichier <nom de la configuration>.ini. Pour identifier ces fichiers, cherchez "FICHIERxx" dans le fichier .INI, où xx représente un nombre. La majorité des fichiers trouvés ont été copiés dans le client à l'étape 1, mais vous trouverez des fichiers .XML qui restent à copier. Ne modifiez pas les noms de fichier, excepté les fichiers suivants :
        - alertrules\<tout texte>.ruleset.xml doit être renommé internal.ruleset.xml
        - monitorrules\<tout texte>.ruleset.monitor.xml doit être renommé masterconfig.ruleset.monitor.xml

2. S'il s'agit d'un ordinateur IPMI/BMC (avec la fonction Surveillance incluse dans l'installation), entrez le paramètre suivant dans la ligne de commande :

export BMCPW="(mot de passe bmc)"

3. En tant que racine, exécutez le script Shell pour la configuration. Par exemple, si vous nommez le script "pull," utilisez le chemin complet ci-dessous :

/tmp/ldcfg/pull.sh

4. Supprimez le répertoire temporaire et tout son contenu.

Remarque: Si vous poussez ou tirez un agent vers un ordinateur Linux, puis exécutez

./linuxuninstall.sh -f ALL

pour le nettoyer et ensuite poussez ou tirez à nouveau, le fichier contenant le GUID est le fichier présent sur l'ordinateur à la fin de l'opération.

L'option -f supprime tous les répertoires du produit. Pour plus d'informations à ce sujet, veuillez consulter la documentation sur la désinstallation de Linux.

Phase 3: Déploiement graduel

La phase 3 traite du déploiement graduel: Le *déploiement* est le processus d'expansion des possibilités de gestion vers les périphériques à inclure dans le domaine de gestion.

Vous déployez ce produit en chargeant des agents et services de produit sur les périphériques. Ceci vous permet de gérer ces derniers à partir d'un emplacement central unique.

La phase 3 traite des sujets suivants :

Stratégie du déploiement graduel

Le déploiement graduel est basé sur trois principes :

1. Déployez en premier les composants les moins utilisés ou ayant un impact minimal sur les périphériques de votre réseau. Passez ensuite aux périphériques les plus utilisés ou ayant un impact maximal.
2. Vérifiez que la fonctionnalité de chaque périphérique géré est stable avant de déployer plus d'agents.
3. Procédez au déploiement de ce produit via des phases bien planifiées, plutôt que de déployer des agents vers tous les types de périphériques en une opération, ce qui peut compliquer tout dépannage requis.

Si vous avez terminé les deux premières phases, vous êtes prêt à démarrer cette phase finale du déploiement du produit vers les périphériques.

Liste de contrôle relative à la configuration de périphériques

Pour configurer des périphériques, déployez à distance des agents via la console Web ou installer-les à partir du périphérique géré. Pour réaliser une configuration par poussage, vous devez configurer les services des ordinateurs IPMI ou Intel* AMT. Vous pouvez utiliser l'applet Configuration des services pour configurer les services suivants pour tous les serveurs principaux et les bases de données. Pour lancer l'applet Configuration des service sur le serveur principal, cliquez sur **Démarrer | Programmes | LANDesk | Configuration des services LANDesk**. Utilisez les onglets Mot de passe BMC ou Configuration Intel AMT.

- **Configuration par poussage:** Utilisez une configuration d'agent pour définir une configuration de périphérique. Fournissez les références nécessaires pour les ordinateurs Intel AMT ou IPMI via Configuration des services (voir "Configuration des services" dans le *Guide d'utilisation*. Ciblez les périphériques souhaités, puis planifiez une tâche pour pousser la configuration vers les périphériques. Reportez-vous à la section "Configuration des agents" dans le *Guide d'utilisation*.
- **Configuration manuelle:** Dans le périphérique géré, mappez un lecteur au partage LDLogon du serveur principal et exécutez le fichier SERVERCONFIG.EXE (le programme de configuration du serveur). Les composants déployés vers le périphérique doivent être sélectionnés de manière interactive.

Evidemment, la configuration manuelle n'est pas pratique dans un environnement de grande taille lors de la configuration et de l'installation sur des périphériques. Dans la plupart des cas, les agents seront poussés vers les périphériques gérés. Veuillez noter que l'installation du produit n'installe pas automatiquement les agents sur le serveur principal. Vous devez également installer les agents sur le serveur principal, puis le redémarrer manuellement.

Quelle que soit la manière dont vous configurez les périphériques, assurez-vous d'utiliser Configuration d'agent dans la console pour créer la configuration de périphérique à déployer.

Les systèmes Windows XP Professional SP2 ou 2003 SP1 requièrent une configuration manuelle du pare-feu pour que tout le produit fonctionne. Spécifiez les paramètres suivants pour ces périphériques : **Serveurs gérés :**

Partage de fichiers et d'imprimantes - TCP 139, 445 ; UDP 137,138 (le poussage d'agent ne fonctionne pas sans cette option)

Distribution de logiciel - TCP 9594, 9595 (le poussage de l'agent ne fonctionne pas sans cette option)

ICMP - avancé - "Autoriser la requête d'écho entrante" (le périphérique ne peut pas être découvert si cette option n'est pas activée.)

Serveur principal :

Inventaire - 5007

Pour spécifier ces paramètres, cliquez sur **Démarrer | Panneau de configuration | Sécurité**, sur le périphérique géré. Ce produit est livré avec une configuration d'agent par défaut qui inclut : l'agent de gestion standard, l'agent de mise à jour de logiciel et l'agent de surveillance.

Vous pouvez créer de nouvelles configurations qui incluent uniquement les composants que vous souhaitez installer, ou (pour la version OEM uniquement) vous pouvez ajouter Intel Active System Console à la configuration d'agent par défaut. Notez que le processus de déploiement des agents n'est pas cumulatif ; tout déploiement désinstalle tous les agents existants. Pour déployer un nouvel agent vers une configuration, vous devez l'inclure avec tous les agents précédents que vous souhaitez incorporer dans la configuration. **Pour créer une configuration de périphérique**

1. Dans le volet de navigation de gauche, cliquez sur **Configuration d'agent**.
2. Cliquez sur **Nouveau**.
3. Entrez un nom pour la nouvelle configuration dans la zone Nom de configuration.

Entrez un nom qui décrit la configuration que vous créez, tel que DBServer ou Executive Office Server. Il peut s'agir d'un nom de configuration existant ou d'un nouveau nom.

4. Sélectionnez **Linux Server Edition**, **Microsoft Windows Server Edition** ou HP-UX.
5. Pour gérer les serveurs dotés d'IPMI sans installer les agents du produit, cochez l'option **IPMI BMC-uniquement** si la configuration est pour des serveurs compatibles IPMI, puis cliquez sur **OK**.
6. Sélectionnez la configuration que vous venez de créer et cliquez sur **Modifier**.

Certaines options des onglets peuvent être grisées car elles ne s'appliquent pas à la configuration sélectionnée. Par exemple, si vous avez sélectionné une configuration Windows IPMI BMC-uniquement, aucune option n'est configurable.

7. Dans l'onglet **Agent**, sélectionnez les agents à déployer.
    - **Tous:** Installe tous les agents sur le périphérique sélectionné.
    - **Mise à jour de logiciel:** Installe l'agent de mise à jour de logiciel. Une fois cet agent installé, vous pouvez configurer la méthode d'exécution du scanner pour détecter les mises à jour disponibles.
    - **Surveillance:** Installe l'agent de surveillance sur le périphérique sélectionné. L'agent de surveillance autorise plusieurs types de surveillance, y compris la surveillance directe ASIC, IPMI en band, IPMI hors bande, Intel Active System Console, Intel AMT et CIM.
8. La **Configuration** s'affiche uniquement à titre d'information
9. Sélectionnez une option de redémarrage.

Le redémarrage manuel signifie que les périphériques ne sont pas redémarrés même si les agents sélectionnés requièrent un redémarrage. Vous devez manuellement redémarrer le périphérique. Si le périphérique requiert un redémarrage, les agents installés ne fonctionneront pas correctement tant que le périphérique n'aura pas été redémarré. Le redémarrage des périphériques, si nécessaire, redémarre les périphériques uniquement si l'agent sélectionné requiert un redémarrage.

Remarque : Seuls les périphériques qui mettent à jour des agents 8.5 existants nécessitent un redémarrage.

10. Dans l'onglet **Inventaire**, réglez les paramètres de configuration du scanner d'inventaire. Ces paramètres sont décrits ci-dessous.

- **Mise à jour automatique:** Les périphériques distants lisent la liste de logiciels à partir du serveur principal durant les analyses de logiciels. Si cette option est définie, chaque périphérique doit posséder un lecteur mappé sur le répertoire LDLOGON sur le serveur principal afin qu'il puisse accéder à la liste de logiciels. Les modifications apportées à la liste de logiciels sont immédiatement disponibles aux périphériques.
- **Mise à jour manuelle:** a liste de logiciels utilisée pour exclure des titres durant les analyses de logiciels est chargée sur chaque périphérique distant. A chaque modification de la liste de logiciels à partir de la console, vous devez la renvoyer manuellement aux périphériques distants.
- **Paramètres du scanner d'inventaire:** La durée d'exécution de l'inventaire. Vous pouvez sélectionner la fréquence et vous pouvez spécifier qu'il est toujours exécuté au démarrage.

Si vous sélectionnez l'option **Entre les heures de** du scanner d'inventaire, vous pouvez spécifier une plage d'heures d'exécution du scanner. Si un périphérique se connecte pendant la plage

horaire spécifiée, l'analyse d'inventaire s'exécute automatiquement. Si le périphérique est déjà connecté, l'analyse d'inventaire s'exécute automatiquement à l'heure de démarrage spécifiée. Cette option est utile si vous souhaitez échelonner les analyses d'inventaire sur les périphériques pour éviter l'envoi simultané de toutes les analyses.

- **Toujours exécuter au démarrage:** Le scanner d'inventaire est exécuté chaque fois que le périphérique est démarré.

11. Dans l'onglet **Ensembles de règles**, sélectionnez tout ensemble de règle de surveillance et/ou d'alerte que vous souhaitez inclure dans la configuration. Les ensembles de règles sont stockés dans le dossier ldlongon/alertrules. Il est possible de créer de nouveaux ensembles de règles dans Surveillance ou Alerte. Pour que les nouveaux ensembles de règles créés s'affichent dans les listes déroulantes, vous devez générer le fichier XML pour l'ensemble de règles personnalisé.
12. Cliquez sur **Enregistrer les modifications** pour enregistrer la configuration d'agent.

Pour plus d'informations sur le déploiement vers des périphériques, reportez-vous à la section "Présentation de l'architecture de configuration d'agent" à la fin de ce chapitre.

Déploiement vers des périphériques Windows

Ce produit prend en charge une méthode de configuration en mode Push planifiée qui permet de déployer des agents à distance.

Pour activer une configuration en mode Push de serveurs Windows 2000/2003 qui n'exécutent pas déjà l'agent de gestion standard, vous devez fournir les références de connexion appropriées comme suit :

1. Dans le serveur principal, cliquez sur **Démarrer | Programmes |** LANDesk | **Configuration des services LANDesk**, puis cliquez sur l'onglet **Planificateur**.
2. Cliquez sur **Modifier la connexion**.
3. Dans les champs **Nom d'utilisateur et Mot de passe**, spécifiez un compte d'administrateur de domaine (utilisez le format domaine\nom_utilisateur).
4. Arrêtez et redémarrez le service Planificateur.
5. Dans la console Web, ciblez les périphériques souhaités, puis cliquez sur **Configuration d'agent > Tâches planifiées** pour déployer les configurations.

Vous pouvez spécifier l'administrateur de domaine lors de la configuration de membres Windows 2000/2003 qui appartiennent au même domaine que le serveur principal. Pour configurer des serveurs Windows 2000/2003 dans d'autres domaines, vous devez définir des relations d'approbation. Gardez à l'esprit que le compte identifié à l'étape 3 ci-dessus est celui sous lequel le service Planificateur sera exécuté sur le serveur principal. Assurez-vous que le compte dispose du droit **Ouvrir la session en tant que service**.

Si la configuration en mode Push échoue et affiche le message "Impossible de trouver l'agent", essayez la procédure ci-dessous pour identifier le problème. Cette procédure réplique les actions du Planificateur lors d'une configuration en mode Push.

1. Recherchez le nom d'utilisateur sous lequel le service Planificateur est exécuté.
2. Sur le serveur principal, connectez-vous avec le nom d'utilisateur trouvé à l'étape 1.

3. Mappez un lecteur sur \\nom_serveur\C$. (Cette étape est celle qui échouera probablement. Elle peut échouer pour deux raisons. Très certainement, vous ne disposez pas de droits administratifs sur le serveur. Si ce nom d'utilisateur ne dispose pas de droits administratifs, il est possible que le partage administratif du serveur (C$) soit désactivé.)
4. Créez un répertoire \\nom_serveur\C$\$ldtemp$ et copiez un fichier vers celui-ci.
5. Utilisez le Gestionnaire de services Windows et essayez de démarrer et d'arrêter des services sur le serveur.

S'il s'agit d'un périphérique doté de IPMI, vous devez fournir le mot de passe BMC. Utilisez l'onglet **Mot de passe** dans Configuration des services pour créer un mot de passe pour le contrôleur de gestion de la carte de base (BMC) IPMI.

1. Dans l'onglet **Mot de passe BMC**, renseignez la zone de texte **Mot de passe**, retapez le mot de passe dans la zone de texte **Confirmer le mot de passe**, puis cliquez sur **OK**.

Le mot de passe ne peut pas contenir plus de 15 caractères qui doivent correspondre à des chiffres compris entre 0 et 9 ou à des lettres majuscules/minuscule de a-z.

Si le périphérique est doté de la technologie Intel* AMT, vous devez fournir le mot de passe Intel AMT. Utilisez l'onglet **Configuration Intel AMT** dans Configuration des services pour créer ou modifier le mot de passe sur les périphériques dotés d'Intel* Active Management Technology.

Pour configurer un mot de passe Intel AMT

1. Dans l'onglet **Configuration Intel AMT**, entrez le mot de passe et le nom d'utilisateur actuels. Ces derniers doivent correspondre au nom d'utilisateur et au mot de passe configurés dans l'écran **Configuration Intel AMT** (accessible dans les paramètres BIOS de l'ordinateur).
2. Pour modifier le nom d'utilisateur et le mot de passe, renseignez la section **Nouveau mot de passe d'Intel AMT**.
3. Cliquez sur **OK**. Cette modification est appliquée lorsque la configuration du client est exécutée.

Remarque: Le nouveau mot de passe doit correspondre à un mot de passe sûr. C'est-à-dire que le mot de passe doit:

- Avoir au moins sept caractères
- Contenir des lettres, des chiffres et des symboles
- Disposer d'au moins un symbole entre la deuxième et sixième position.
- Etre différent de manière significative des mots de passe précédents
- Ne pas contenir des noms ou des noms d'utilisateur
- Ne pas être un nom ou mot courant

Vérification du succès du déploiement de l'agent

Pour vérifier que vous avez déployé avec succès l'agent de gestion vers les périphériques, vérifiez que vous pouvez réaliser les tâches suivantes à partir de la console. Si vous nécessitez des informations supplémentaires pour la réalisation de ces tâches, reportez-vous aux chapitres correspondant aux fonctions respectives dans le *System ManagerGuide d'utilisation*.

Inventaire

- Dans la liste **Mes périphériques**, cliquez deux fois sur un périphérique, puis affichez la liste des agents installés.
- Exécutez une requête d'inventaire.
- Sélectionnez un périphérique, puis cliquez sur **Inventaire** pour afficher les données de ce périphérique.
- Modifiez le fichier WIN.INI d'un périphérique Windows, analysez à nouveau le périphérique, puis vérifiez que les modifications ont été enregistrées dans le fichier CHANGES.LOG.

Déploiement de périphériques à partir de la ligne de commande

Vous pouvez contrôler quels composants sont installés sur les périphériques en utilisant des paramètres de ligne de commande avec SERVERCONFIG.EXE.

Vous pouvez démarrer le programme SERVERCONFIG.EXE en mode autonome. Il est situé dans le répertoire (lecteur système)\Program Files\LANDesk\ManagementSuite\LDLogon sur le serveur principal. SERVERCONFIG.EXE est également disponible dans le partage \\nom_serveur_principal\LDLogon, qui peut être lu à partir de tout serveur Windows 2000/2003.

Présentation de l'architecture de configuration d'agent

Présentation de SERVERCONFIG.EXE

SERVERCONFIG.EXE est l'utilitaire de configuration de périphérique du produit. Il configure en trois étapes les serveurs Windows pour la gestion :

1. SERVERCONFIG détermine si l'ordinateur a été précédemment configuré par un autre produit LANDesk. Si c'est le cas, le fichier SERVERCONFIG supprime les fichiers plus anciens et inverse toutes les autres modifications.
2. Le fichier SERVERCONFIG recherche un fichier masqué nommé CCDRIVER.TXT afin de décider si le serveur doit être (re)configuré. (Le processus de décision du fichier SERVERCONFIG est traité ci-dessous.) Si le périphérique n'a pas à être (re)configuré, le fichier SERVERCONFIG se ferme.
3. Si le périphérique doit être (re)configuré, le fichier SERVERCONFIG charge le fichier d'initialisation approprié (SERVERCONFIG.INI) et exécute les instructions qu'il contient.

Si vous exécutez le fichier SERVERCONFIG.EXE une deuxième fois et sélectionnez des agents différents de ceux utilisés lors de la première exécution, les agents de la première exécution seront supprimés. Vous devez sélectionnez chaque agent dont vous avez besoin lors de chaque exécution de SERVERCONFIG.EXE, même si vous avez déjà installé des agents.

Les paramètres de ligne de commande suivants sont disponibles pour le fichier SERVERCONFIG.EXE :

Paramètre	Description
/I=	Composants à inclure (guillemets inclus) : "Agent à base commune" "Scanner d'inventaire" "Alerte" "Scanner de vulnérabilité" "Surveillance de serveur" "Active System Console" Vous pouvez les combiner sur la même ligne de commande. Par exemple, Exemple : SERVERCONFIG.EXE /I="Pilote miroir" /I="Scanner de vulnérabilité"
/IP	Configure en utilisant IP
/L ou /Log=	Chemin vers les fichiers journaux CFG_YES et CFG_NO qui consignent les périphériques configurés ou non
/LOGON	Exécute les commandes dotées du préfixe [LOGON]
/N ou /NOUI	N'affiche pas l'interface utilisateur
/NOREBOOT	Ne redémarre pas le périphérique une fois terminé
/P	Demande la permission de l'utilisateur pour exécuter
/REBOOT	Force un redémarrage après l'exécution
/TCPIP	Identique à IP (voir ci-dessus)
/X=	Composants à exclure Exemple : SERVERCONFIG.EXE /X=SD
/CONFIG=	/CONFIG]= Spécifie un fichier de configuration de périphérique serveur à utiliser à la place du fichier SERVERCONFIG.INI par défaut. Par exemple, si vous avez créé un fichier de configuration nommé NTTEST.INI, utilisez cette syntaxe : SERVERCONFIG.EXE /CONFIG=TEST.INI

	Les fichiers .INI personnalisés doivent être dans le même répertoire que le fichier SERVERCONFIG.EXE. Notez également que le paramètre /config utilise le nom de fichier sans le préfixe 95.
/? ou /H	Affiche le menu d'aide

Déploiement de l'agent de gestion standard

L'agent de gestion standard est un agent obligatoire et est le protocole sous-jacent du produit.

Déploiement du scanner de vulnérabilités

L'agent Scanner de vulnérabilités exécute des opérations d'analyse et de réparation Le bouton **Planifier des tâches de sécurité** crée une tâche qui lance le programme vulscan.exe sans paramètre. Une fois lancé sans paramètre, vulscan détermine l'emplacement du serveur principal en accédant à la clé de registre "hklm\software\intel\landesk\LDWM", avec une valeur "CoreServer". Il demande alors la dernière liste des informations sur les vulnérabilités à rechercher, exécute une analyse et soumet les résultats au serveur principal. Les résultats sont placés dans la liste Mises à jour détectées. Les mises à jour détectées doivent être téléchargées vers le serveur principal. Les mises à jour peuvent être corrigées à l'aide du processus de correction. Si le processus ce correction installe avec succès un ou plusieurs correctifs, il exécute une nouvelle analyse et soumet les résultats obtenus au serveur principal. Ce processus est approprié pour les mises à jour LANDesk et OEM.

Déploiement du scanner d'inventaire

Vous pouvez utiliser le scanner d'inventaire pour ajouter des périphériques à la base de données principale et pour collecter les données relatives aux logiciels et matériels des périphériques. Le scanner d'inventaire s'exécute automatiquement lors de la configuration initiale du périphérique. Le scanner collecte les données de matériels et de logiciels et les saisit dans la base de données principale. Ensuite, l'analyse de matériels est exécutée à chaque démarrage du périphérique, mais l'analyse de logiciels est uniquement exécutée suivant un intervalle que vous spécifiez.

Déploiement de l'agent de surveillance

L'agent de surveillance autorise plusieurs types de surveillance, y compris la surveillance directe ASIC, IPMI en band, IPMI hors bande, Intel AMT et CIM.

Déploiement de Active System Console

Installe l'agent qui permet d'accéder à Active System Console à partir de System Manager à l'aide d'une interface ou de menus. Cet agent est installé uniquement sur les périphériques dotés de cartes Intel ; il n'est pas installé lorsque vous l'incluez dans un déploiement vers une carte non-Intel.

Désinstallation du serveur principal

De la même manière qu'il existe une stratégie spécifique à suivre pour déployer les différents composants, il existe une stratégie correspondante pour la désinstallation des composants.

Les sections suivantes décrivent comment désinstaller correctement chaque composant. Vous devez désinstaller les composants dans l'ordre indiqué :

1. Désinstaller les agents de produit des périphériques.
2. Désinstaller le serveur principal.

Désinstallation des agents de produit des périphériques.

La première étape de désinstallation du logiciel du réseau consiste à désinstaller ses agents des périphériques.

Pour désinstaller des agents des serveurs

1. Connectez-vous au serveur avec des droits administratifs.
2. Mappez un lecteur sur le dossier partagé de ManagementSuite du serveur principal.
3. Ouvrez une invite de commande, modifiez la lettre de lecteur du dossier ManagementSuite, puis entrez :

uninstallwinclient.exe

4. La désinstallation s'exécute en mode silencieux, supprimant tous les agents.

Vous pouvez également cliquer sur Démarrage,Exécuter et entrer *nom du serveur principal*\LANDesk\ManagementSuite\uninstallwinclient.exe.**Pour supprimer complètement l'agent Linux d'un serveur Linux**

1. Dans le dossier partagé ManagementSuite, trouvez le fichier linuxuninstall.tar.gz et copiez-le dans la zone Linux.
2. Exécutez ce fichier en utilisant les options x, z et f. La ligne de commande devrait s'afficher de la manière suivante :

tar xzf linuxuninstall.tar.gz

3. Une fois l'exécution du fichier terminée, exécutez ./linuxuninstall.sh à partir de la ligne de commande.

Pour obtenir de l'aide sur ce fichier, exécutez-le en conjonction avec l'option -h. Remarque : notez que si vous poussez ou tirez un agent vers un ordinateur Linux, puis exécutez

./linuxuninstall.sh -f ALL

pour le nettoyer et ensuite poussez ou tirez à nouveau, vous créez des doublons (pour l'ordinateur du même nom et de la même adresse IP) dans la base de données car le GUID de l'ordinateur est supprimé.

L'option -f supprime tous les répertoires du produit. Pour plus d'informations à ce sujet, veuillez consulter la documentation sur la désinstallation de Linux.

Après la désinstallation, il ne reste plus que le fichier /etc/ldiscnux.conf. Sa présence permet d'éviter que la base de données s'encombre de périphériques en double. Si vous ne replacez pas ce périphérique dans la base de données, vous pouvez le supprimer en toute sécurité.
Le fichier UninstallWinClient.exe se trouve dans le dossier partagé de ManagementSuite. Seuls les administrateurs ont accès à ce partage. Ce programme désinstalle les agents des périphériques sur lesquels il est exécuté. Il s'agit d'une application Windows qui s'exécute en mode silencieux sans afficher une interface. Deux instances du serveur supprimé peuvent être présentes dans la base données. Une de ces instance contient uniquement des données historiques, alors que l'autre instance contient des données vers l'avant.

Remarque: Par défaut, Uninstallwinclient.exe redémarre le périphérique après la désinstallation des agents. Pour éviter un redémarrage, vous pouvez ajouter à la ligne de commande l'option /noreboot.

Désinstallation du serveur principal

L'étape finale de la désinstallation du produit du réseau consiste à désinstaller le logiciel sur le serveur principal. Avant de procéder, assurez-vous d'avoir désinstallé les agents de produit des serveurs.

Pour désinstaller le serveur principal

1. Accédez au serveur principal.
2. Cliquez sur **Démarrer** | **Paramètres** | **Panneau de configuration**, puis cliquez deux fois sur **Ajout/Suppression de programmes**.
3. Si le logiciel est installé, cliquez sur Intel Platform Extensions pour LANDesk Software puis surAjout/Suppression.
4. Pour désinstaller le logiciel, cliquez sur logiciel LANDesk.
5. Cliquez sur **Ajouter/Supprimer**.

Désinstallation de la base de données principale
Vous devez désinstaller manuellement la base de données principale.

Désinstallation de la base de données principale

Par défaut, la base de données principale n'est pas désinstallée lors de la désinstallation de LANDesk® System Manager. Important : ne désinstallez pas la base de données principale si vous penser réinstaller LANDesk® System Manager ultérieurement sur l'ordinateur.

Pour désinstaller la base de données principale

1. Accédez au serveur principal.
2. Cliquez sur **Démarrer** | **Paramètres** | **Panneau de configuration**, puis cliquez deux fois sur **Ajout/Suppression de programmes**.
3. Pour désinstaller la base de données principale, cliquez sur Microsoft SQL Server Desktop Engine (LDMSDATA).
4. Cliquez sur **Ajouter/Supprimer**.

Fichiers de base de données
Lors de la désinstallation de Microsoft SQL Server Desktop Engine, les fichiers de base de données utilisés par LANDesk® System Manager ne sont pas supprimés. Les fichiers de base de données prennent de la place sur votre ordinateur mais peuvent y rester sans aucun risque. Pour les supprimer manuellement, il vous suffit de supprimer le contenu du dossier \ProgramFiles\Microsoft SQL Server\MSSQL$LDMSDATA\Data.

Assistance

Vous pouvez accéder aux services d'assistance en ligne de LANDesk Software sur le Web (disponible en anglais uniquement). Les services contiennent les informations les plus récentes sur les produits LANDesk Software. Vous pouvez également y trouver des notes sur l'installation, des conseils de dépannage, des mises à jour logicielles et des informations d'assistance clientèle. Visitez le site Web ci-dessous, puis accédez à la page du produit :

http://www.landesk.com/support/index.php

Vous pouvez également télécharger les versions les plus récentes des notes de version et de la documentation, qui peuvent inclure des informations qui n'étaient pas disponibles au moment de la distribution du produit. Si vous avez reçu System Manager d'un fabricant OEM, veuillez contacter son assistance clientèle.

Si vous ne pouvez pas résoudre votre problème en utilisant ce guide ou en consultant le site Web d'assistance LANDesk Software, LANDesk Software propose une gamme de services d'assistance payante, de consultation et de partenariat. Pour plus d'informations, consultez la page d'assistance clientèle à l'adresse suivante :

http://www.landesk.com/wheretobuy/

Avant de nous appeler dans le cas de problèmes liés à l'assistance clientèle, ayez les informations ci-dessous à portée de main :

- Votre nom, le nom de votre société et la version du produit que vous utilisez.
- Le système d'exploitation de réseau que vous utilisez (nom et version).
- Tous les correctifs ou Service Packs que vous avez installés.
- Etapes détaillées permettant de reproduire le problème.
- Etapes déjà effectuées pour tenter de résoudre le problème.
- Toutes les informations propres à votre système qui peuvent aider l'ingénieur de l'assistance clientèle à comprendre le problème, telles que le type d'application de base de données utilisé, la marque de la carte vidéo que vous avez installée ou la marque et le modèle de l'ordinateur utilisé.