LANDesk® System Manager 8.7

Guide d'utilisation

Rien dans ce document ne constitue une garantie ou une licence, qu'elle soit expresse ou implicite. LANDesk rejette toute responsabilité concernant de telles garanties et licences, y compris mais sans s'y limiter : garantie de qualité marchande, garantie d'aptitude à une fonction définie, infraction à tout droit de propriété intellectuelle ou autre de partie tierce ou de LANDesk, indemnité et autres. Les produits LANDesk ne sont pas destinés à une utilisation dans des applications médicales thérapeutiques salvatrices ou essentielles au maintien de la vie. Le lecteur est averti que des parties tierces peuvent posséder des droits de propriété intellectuelle concernant ce document et les technologies traitées dans celui-ci, et est avisé de consulter un expert juridique qualifié, sans obligation de LANDesk.

LANDesk se réserve le droit de modifier à tout moment ce document ou les spécifications et descriptions de produit associées, sans avertissement préalable. LANDesk n'offre aucune garantie concernant l'utilisation de ce document et n'assume aucune responsabilité pour toute erreur pouvant apparaître dans celui-ci. En outre, LANDesk n'offre aucun engagement concernant la mise à jour des informations contenues dans ce document.

Sommaire

Présentation

Présentation de LANDesk® System Manager

Bienvenue dans LANDesk® System Manager8.70, une application de gestion autonome qui assure la disponibilité de vos serveurs, y compris ceux qui exécutent Windows, Linux, HP-UX et AIX. Ce logiciel peut également être installé et utilisé simultanément avec LANDeskManagement Suite, en utilisant la même base de données principale que Management Suite pour faciliter la création de rapports informatiques.

Conçu pour faire appel le moins possible aux ressources, ce produit dispose de plusieurs agents et services " à la demande " qui sont uniquement exécutés selon vos besoins, libérant donc des cycles de processeur et de la mémoire pour d'autres tâches. LANDesk réalise que la disponibilité des périphériques est essentielle à votre entreprise, pour cette raison ce produit fait preuve d'une stabilité sans égal, permettant une exécution 7 jours sur 7, 24 heures sur 24. Il vous permet de contrôler les logiciels exécutés sur vos périphériques. Vous pouvez installer l'agent intégral, sélectionner des composants spécifiques ou placer les périphériques dans votre liste de périphériques sans installer d'agents.

Pour afficher correctement les boîtes de dialogue et les fenêtres, il est nécessaire d'ajouter le site Web de System Manager à la liste des sites autorisés du programme de blocage de menus contextuels du navigateur.

Nouveautés de la version 8.70

Les fonctions suivantes ont été ajoutées ou mises à niveau à partir de la version précédente de System Manager :

Gestion de périphérique sans agent : Gérez les périphériques dans la vue **Mes périphériques** sans y installer un agent de gestion, lorsqu'ils sont activés avec une technologie de gestion hors bande telle que Intel* AMT, IPMI ou DRAC.

Groupes personnalisés dans Tâches planifiées : Vous pouvez grouper les tâches dans des groupes personnalisés pour les exécuter.

Mode Débutant : Ce mode vous permet d'afficher les étiquettes des boutons des barres d'outils pour permettre aux nouveaux utilisateurs d'identifier plus aisément les fonctions des boutons. Vous pouvez tout aussi bien décider de ne pas afficher les étiquettes (les astuces s'afficheront toujours au passage de la souris).

Configuration du matériel : Ce nouvel outil permet de configurer des options pour les périphériques dotés de la technologie Intel* AMT. Vous pouvez générer des ID pour l'approvisionnement des périphériques Intel AMT, afficher les ID générées et modifier les options de configuration associées à l'approvisionnement des périphériques Intel AMT. Vous pouvez

également définir les stratégies de disjoncteur (Circuit Breaker) qui détectent et bloquent les activités réseau suspicieuses sur les périphériques.

Support amélioré pour Active Management Technology : Ce produit prend maintenant en charge Intel* Active Management Technology 2 (en plus de la version 1). La version 2 de AMT prend également en charge la gestion sans agent et la découverte automatique des périphériques Intel* AMT 2.

Fonctions du produit

System Manager permet de choisir le niveau de reportage de gestion, depuis la collecte d'informations simple jusqu'à l'analyse de performance étendue et le contrôle de configuration et de sécurité.System Manager inclut les fonctions suivantes :

Console Web facile à utiliser : Exécutez le produit à tout moment et n'importe où en utilisant une console Web qui fournie des données importantes via une interface facile à utiliser. Vous pouvez l'exécuter depuis votre poste de travail principal ou depuis un poste situé dans la pièce contenant le serveur sans aucune installation. Recherchez simplement l'URL du produit, http://*serveur_principal*/LDSM. Vous "ciblez" des périphériques spécifiques pour des actions telles que la distribution de logiciel en les sélectionnant et les plaçant dans la liste **Périphériques ciblés**, opération semblable au "panier d'achat" de nombreuses applications Web.

Prise en charge de système d'exploitation plus étendue : Gérez vos divers environnements de serveur à partir d'une seule console intégrée. En plus de la gestion des serveurs Windows 2000 et 2003, System Manager prend en charge plusieurs environnements Linux et Unix :

- 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 - U2
- Red Hat Enterprise Linux v4 (ES) EM64t - U2
- Red Hat Enterprise Linux v4 (AS) 32 bits - U2
- Red Hat Enterprise Linux v4 (AS) EM64t - U2
- Red Hat Enterprise Linux v4 WS 32 bits - U2
- Red Hat Enterprise Linux v4 WS EM64t - U2
- SUSE* Linux Server 9 ES 32 bits SP2
- SUSE Linux Server 9 EM64t SP2
- SUSE Linux Professional 9.3
- SUSE Linux Professional 9.3 EM64t
- HP-UX 11.1
- Unix AIX

Vue de la tâche planifiée : Affichez toutes les tâches de déploiement d'agent, de découverte, de mise à jour de logiciel et de script personnalisé qui sont planifiées ou complétées depuis un emplacement. Vous pouvez replanifier la tâche, la modifier ou la rendre récurrente.

Prise en charge d'Intel* AMT : Prise en charge des versions 1 et 2 de Intel* Active Management Technology. Intel AMT permet de gérer à distance les périphériques en réseau dans n'importe quel état système via la communication hors bande (OOB), même lorsque le système ne répond pas ou que le périphérique est désactivé. La connexion du périphérique à un réseau d'entreprise et la disposition d'une alimentation en veille sont les seules exigences du côté du périphérique.

Prise en charge d'interface IPMI : Le produit fournit une prise en charge des serveurs dotés de Intelligent Platform Management Interface (IPMI) (versions 1.5 ou 2.0), autorisant la récupération distante hors bande des serveurs hors service et l'affichage des données de gestion autonomes même lorsque le système d'exploitation ou le processeur n'est pas exécuté.

Outil de scripts : Vous pouvez exécuter des tâches personnalisées sur des périphériques en créant des scripts de planificateur local.

Surveillance de la performance : Vous pouvez surveiller en temps réel la performance de vos serveurs Blade ou d'entreprise gérés en utilisant plusieurs attributs. Vous pouvez même suivre ces attributs et afficher les données historiques de performance rapportées pendant plusieurs jours. Vous pouvez surveiller des périphériques sur lesquels l'agent de surveillance est installé, et vous pouvez également surveiller des serveurs dotés de IPMI hors bande sans agent.

Prise en charge du serveur Blade : Les serveurs Blade et les châssis Blade IBM sont pris en charge, y compris les fonctions de découverte, de détection de châssis, d'inventaire, et de gestion de correctifs. Les outils du produit permettent de grouper les serveurs Blade par fonction, châssis, rangement modulaire et autres critères pour une collecte de données plus efficace.

Rapports : Vous pouvez exécuter des rapports sur n'importe quel périphérique de la base de données qui affichent des statiques d'utilisation, l'allocation des ressources et de nombreuses autres mesures. Ce produit inclut plusieurs rapports enregistrés (pré-formulés). Ces rapports s'exécutent rapidement en accédant directement à la base de données pour collecter des informations et représenter les données sous la forme de diagrammes en deux ou trois dimensions ou de graphes à barres. Vous pouvez créer des rapports supplémentaires en créant des requêtes personnalisées.

Contrôle de santé / Alertes : La surveillance de la santé globale d'un périphérique est facile. Vvous pouvez définir des seuils pour des mesures telles que l'espace disque ou l'utilisation du processeur, et configurer la méthode d'alerte lorsqu'un seuil est dépassé. Vous pouvez afficher les problèmes de santé du périphérique sélectionné et initialiser les actions pour les résoudre avant que des utilisateurs ne se rendent compte de des problèmes de performance ou éprouvent des moments d'inactivité.

Mises à jour de logiciel : Vous pouvez recevoir des mises à jour de logiciel pour System Manager et pour le matériel Intel*. Vous pouvez déployer manuellement les mises à jour sélectionnées en utilisant les fonctions de distribution de logiciel.

Administration basée sur les rôles : Ajoutez des utilisateurs et configurez leur accès aux outils et aux autres périphériques en fonction de leur rôle administratif. 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, telles que la création de rapports uniquement.

Inventaire : L'outil d'analyse d'inventaire permet au produit de compiler de nombreuses informations sur les matériels et les logiciels dans la base de données principale. Vous pouvez alors afficher, imprimer et exporter ces données.

Découverte de périphériques : Permet de déterminer ce qui est présent dans votre réseau. La découverte de périphériques permet de rassembler des informations de base sur tous les périphériques dans votre environnement, améliorant le contrôle et accélérant le déploiement des agents vers les périphériques ciblés.

Prise en charge d'Active System Console : Prise en charge d'Active System Console, qui fournit un aperçu rapide de l'état de santé du système lorsque vous installez un agent Active System Console sur un périphérique. Vous pouvez déterminer rapidement si les éléments matériels sélectionnés fonctionnent correctement et s'il existe des problèmes potentiels qui doivent être examinés. Vous pouvez également afficher des mesures détaillées de la performance système et afficher une liste des composants, y compris les matériels, logiciels, fichiers journaux et informations sur Intel* AMT et IPMI (si inclus dans le périphérique).

Tableau de bord exécutif : Un groupe d'outils (graphiques, diagrammes, cadrans et compteurs informatifs) qui permettent aux cadres de surveiller la santé ou l'état de leur entreprise.

Aide : Ce produit inclut un Guide de mise en route, ainsi que des rubriques d'aide contextuelles.

Termes du produit

- **Serveur principal :** Centre d'un domaine de gestion. Tous les fichiers et services clés du produit 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 du produit sont installés. "Périphériques" incluent les ordinateurs de bureau, des serveurs, des ordinateurs portables ou mobiles, des châssis Blade, etc. Un serveur principal peut gérer des milliers de périphériques.
- **Public :** Eléments (tels que groupes, paquets de distribution, ou tâches) qui sont visibles à 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 sont 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 visible aux 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 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 visible comme étant Courante lui permettant ainsi 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.

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 ou passer à Management Suite ou System Manager

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**.
2. Entrez le nom d'utilisateur et le mot de passe uniques fournis lors de l'achat de vos licences.
3. 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.

- 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.
- 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 du System 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 sur **Démarrer | Programmes | LANDesk | Configuration des services LANDesk**.
2. Cliquez sur l'onglet **Planificateur**.
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).

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.

Mise sous licence

La procédure de mise sous licence permet à votre organisation de rester conforme à ses contrats de nœud sous licence en exécutant une procédure d'autorisation continue. Elle permet également d'utiliser plusieurs serveurs principaux sous un compte d'utilisateur défini. La procédure de mise sous licence utilise une base de données d'arrière plan pour créer et gérer des comptes utilisateur. Il s'agit d'une procédure de requête et réponse simple, du serveur principal vers la base de données d'arrière plan, qui permet au serveur principal de renouveler son activité pour une autre période.

Lorsque vous exécutez le produit (ou tout produit additionnel) après une installation, vous pouvez activer une licence d'évaluation pour une période d'essai ou vous pouvez entrer un nom d'utilisateur et un mot de passe pour activer une licence achetée obtenue auprès du service des ventes de LANDesk. Les mêmes nom d'utilisateur et mot de passe sont utilisés pour activer tous les serveurs principaux du compte existant.

La procédure d'activation est essentiellement la même pour l'évaluation et l'achat des produits. Lorsque le périphérique utilise une connexion Internet, la procédure est un échange d'informations simple. Lorsque le périphérique n'est pas connecté, vous devez suivre la procédure manuelle d'envoi d'un fichier électronique à LANDesk suivi de l'enregistrement du fichier renvoyé dans le serveur principal. La procédure d'activation fonctionne de la manière suivante :

1. L'utilisateur exécute l'utilitaire Activer le serveur principal
2. Un fichier contenant des informations d'utilisation et de serveur est créé. Il est signé par la clé privée du serveur principal et encodé par la clé publique de LANDesk.
3. Si une connexion Internet est disponible, le serveur principal et les serveurs LANDesk communiquent entre eux et le serveur principal charge un fichier d'activation. La base de données en arrière plan traite les informations et renvoie les informations d'activation qui sont directement écrites dans la base de données.
4. Si aucune connexion Internet n'est disponible, vous pouvez envoyer le fichier situé dans le répertoire \Program Files\LANDesk\Authorization Files à licensing@landesk.com.

Ajout de licences

Les fonctions disponibles via la console dépendent de la clé de licence. Vous pouvez ajouter une nouvelle clé de licence pour accéder à d'autres fonctions ou pour mettre à jour le nombre d'utilisateurs. Durant l'installation, une licence d'évaluation de 45 jours est créée. Lorsque vous ajoutez une licence valide via la console, cette licence temporaire est supprimée.

Pour ajouter une clé de licence

1. Dans le volet de navigation de gauche, cliquez sur **Préférences**.
2. Cliquez sur l'onglet **Licence**.
3. Dans la partie inférieure de l'écran, cliquez sur le lien http:/www.landesk.com/contactus/.

Si le lien ci-dessus ne fonctionne pas, il est possible que le niveau de sécurité du navigateur ne soit pas réglé sur Moyen. Vous devriez modifier le niveau de sécurité Internet par défaut et le

régler sur Moyen dans Internet Explorer (**Outils > Options Internet > Sécurité > Internet > Niveau par défaut**).

La console

Démarrage de la console

Pour démarrer la console

1. Dans le serveur principal, cliquez sur **Démarrer | Programmes | LANDesk | LANDesk System Manager**.

   ou

   Sur un poste distant, ouvrez un navigateur et saisissez l'adresse de la console. Utilisez le format http://*nom_serveur_principal*/ldsm.

2. Entrez un nom d'utilisateur et un mot de passe valides.

   Si vous vous connectez à un serveur principal distant, suivez les règles Windows normales de connexion (par exemple, si l'utilisateur est local par rapport à ce serveur principal, entrez uniquement le nom d'utilisateur ; s'il s'agit d'un utilisateur de domaine, entrez le nom de domaine\nom d'utilisateur).
3. Cliquez sur **OK**.

Si les boutons et la liste de périphériques ne s'affichent pas lorsque vous démarrez la console, veuillez, si besoin, activer le serveur principal.

Boîte de dialogue de connexion System Manager

Utilisez cette boîte de dialogue pour démarrer la console et vous connecter à un serveur principal.

- **Nom d'utilisateur :** Identifie un utilisateur. Il peut s'agir d'un utilisateur administrateur ou d'un autre type d'utilisateur du produit doté de droits d'accès restreints (pour plus d'informations, reportez-vous à la section Administration basée sur les rôles). L'utilisateur doit être un membre du groupe LANDesk Management Suite sur le serveur principal. Si vous vous connectez à un serveur principal distant, entrez les nom d'utilisateur et domaine.
- **Mot de passe :** Mot de passe de l'utilisateur.

Utilisation de la console

Vous pouvez utiliser les outils pour visualiser, configurer, gérer et protéger les périphériques du réseau — tout cela à partir d'une console unique. Vous pouvez mettre à jour des paramètres de logiciel ou de configuration, diagnostiquer des problèmes matériels et logiciels, ainsi qu'utiliser l'administration basée sur les rôles pour contrôler l'accès des utilisateurs aux fonctions et périphériques. De plus, si vous utilisez également d'autres produits LANDesk, vous pouvez vous y connecter directement depuis la console.

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 permettent de gérer des périphériques et des utilisateurs, d'afficher des rapports, d'exécuter des découvertes, de créer et modifier des requêtes, etc. Vous pouvez redimensionner les volets et les colonnes de la liste **Mes périphériques**. Lorsqu'aucun agent n'est installé sur un périphérique, seules les colonnes des noms et des adresses IP contiennent des informations. Dans certains cas, des informations sur le système d'exploitation s'affichent.

System Manager fournit des fonctions d'application similaires aux applications Windows avec les avantages et l'accessibilité d'un navigateur Web.

- Cliquez avec le bouton droit sur un périphérique dans la liste **Mes périphériques** pour afficher les options disponibles de ce périphérique, telles que les options Envoyer un Ping et Cibler.
- Pour sélectionner plusieurs entrées consécutives dans une liste, cliquez sur le premier élément de la liste, appuyez et maintenez la touche **Maj.** enfoncée, puis cliquez sur le dernier élément de la liste.
- Pour sélectionner plusieurs entrées non consécutives dans une liste, appuyez et maintenez la touche **Ctrl** enfoncée, puis cliquez sur chaque élément voulu.

Pour afficher correctement les boîtes de dialogue et les fenêtres, il est nécessaire d'ajouter le site Web de System Manager à la liste des sites autorisés du programme de blocage de menus contextuels du navigateur.

Administration basée sur les rôles
En tant qu'utilisateur, les périphériques que vous pouvez visualiser et gérer dans la liste **Mes périphériques**, ainsi que les outils de gestion que vous pouvez utiliser, sont déterminés par les droits d'accès et la portée de périphériques qui vous sont attribués par l'administrateur. Pour plus d'informations, reportez-vous à la section "Utilisation de l'administration basée sur les rôles".

Cette section fournie des informations sur :

- Liste Mes périphériques
- Icônes de périphérique
- Utilisation des menus contextuels
- Utilisation des outils
- Affichage des propriétés de périphérique

Liste Mes périphériques

La liste **Mes périphériques** contient les groupes et sous-groupes suivants. De plus, en fonction des droits d'accès et de la portée du périphérique, vous pouvez créer vos propres groupes pour faciliter la gestion des périphériques.

Tous les périphériques

La liste **Tous les périphériques** affiche les périphériques de l'utilisateur actuellement connecté, selon la limite de sa portée, dans une liste non hiérarchique (sans sous-groupes). Lorsqu'il est connecté à un serveur principal donné, l'administrateur peut visualiser chaque périphérique géré par ce serveur principal. Par contre, les utilisateurs du produit sont limités et peuvent uniquement visualiser les périphériques qui résident dans leur portée attribuée (une portée est définie par une requête de base de données ou un emplacement de répertoire).

Les périphériques qui exécutent des agents du produit (agent de gestion standard et Inventaire) apparaissent automatiquement dans la liste **Tous les périphériques** lorsqu'ils sont analysés dans la base de données principale par le scanner d'inventaire. Généralement, cette analyse a lieu pour la première fois lors de la configuration initiale du périphérique. Une fois un périphérique analysé dans la base de données principale, il est considéré comme périphérique géré — il peut maintenant être géré par ce serveur principal. Pour plus d'informations sur la configuration de périphériques, reportez-vous à la section "Configuration des agents de client".

Le groupe **Tous les périphériques** étant automatiquement renseigné via une analyse d'inventaire, vous pouvez avoir à ne jamais découvrir manuellement les périphériques. Toutefois, pour découvrir des périphériques qui ne sont pas déjà dans la base de données principale (ou pour déplacer des périphériques non gérés vers le groupe des serveurs), vous pouvez utiliser l'outil de découverte de périphériques pour rechercher des périphériques dans le réseau. Pour plus d'informations, reportez-vous à la section "Utilisation de la découverte".

Le groupe **Tous les périphériques** fournit les informations suivantes pour chaque périphérique. Pour ouvrir la liste, cliquez deux fois sur **Tous les périphériques**.

- **Nom :** Le nom d'hôte du périphérique, tel que le nom d'ordinateur Windows*.
- **Adresse IP :** L'adresse IP du périphérique.
- **Santé :** L'état de santé et de la disponibilité du périphérique. L'état peut être Normal, Avertissement ou Critique.
- **Agent :** L'agent actuel exécuté sur le périphérique.
- **Type de périphérique :** Affiche le type de matériel sur l'ordinateur (Intel AMT, IPMI, ASIC ou IPMI avancé).
- **Système d'exploitation :** Le type de système d'exploitation exécuté par le périphérique.
- **Actif depuis :** La date et l'heure depuis lesquelles l'ordinateur a fonctionné sans interruption (dans le fuseau horaire de la base de données).

Lorsque vous sélectionnez un périphérique, les propriétés du périphérique s'affichent dans le volet **Propriétés** sous la liste des périphériques. Le volet **Propriétés** affiche de nombreux attributs de périphérique importants :

- **ID :** Le numéro d'identification du périphérique. Ce numéro est déterminé par l'ordre d'ajout du périphérique dans la liste **Tous les périphériques**.
- **Adresse IP :** L'adresse IP du périphérique.
- **Fabricant :** Le fabricant du périphérique.
- **Modèle :** Le modèle du périphérique.
- **Vitesse du processeur :** La vitesse du processeur du périphérique.
- **Type de processeur :** Le type de processeur du périphérique.

Depuis la console, vous pouvez afficher un inventaire détaillé et cibler le périphérique pour une action, telle que l'exécution d'un rapport.

Cliquez deux fois sur un périphérique dans la liste **Tous les périphériques** pour passer à la Console d'informations du serveur, qui contient des informations récapitulatives du périphérique, des options de configuration de contrôle distant et des informations sur l'ensemble des règles d'alerte.

Groupes publics

La liste **Groupes public** affiche les groupes de périphériques créés par un utilisateur doté des droits Administrateur. Ils sont visibles aux autres utilisateurs.

Cette liste affiche également les groupes de châssis Blade qui sont automatiquement créés lorsqu'un module de gestion de châssis (CMM) est ajouté à la liste des périphériques gérés. Le groupe répertorie le CMM et chaque serveur Blade associé que vous gérez. Vous ne pouvez pas modifier un groupe de châssis de la même manière qu'un groupe que vous avez créé.

Les groupes peuvent être statiques ou dynamiques. Les groupes dynamiques contiennent des périphériques qui satisfont des critères de filtre prédéfinis, tels que la vitesse de processeur, le système d'exploitation du périphérique ou un attribut personnalisé tel que le type de périphérique. Les groupes statiques incluent une liste définie de périphériques, d'autres groupes statiques ou de groupes dynamiques.

Groupes privés

La liste **Groupes privés** affiche des groupes de périphériques créés par l'utilisateur actuellement connecté. Les groupes privés ne sont pas visibles par les autres utilisateurs et ne peuvent donc pas être utilisés par d'autres utilisateurs.

Icônes de périphérique

Les icônes de périphérique s'affichent dans la liste **Tous les périphériques**et indiquent l'état de santé actuel de chaque périphérique. Pour mettre à jour l'état de santé des périphériques un à la fois lorsque vous les sélectionnez parmi les périphériques de la liste **Mes périphériques**, cliquez sur le bouton **Actualiser** de la barre d'outils.

Le tableau suivant répertorie les icônes de périphérique et d'état et leur signification :

Icône	Description
	Périphérique à l'état Normal
	Périphérique à l'état Avertissement

Icône	Description
	Périphérique à l'état Critique
	Périphérique à l'état Inconnu

Utilisation des menus contextuels

Les menus contextuels sont disponibles pour tous les éléments de la console, y compris les groupes, périphériques, requêtes, tâches planifiées, scripts, rapports, etc. Les menus contextuels fournissent un accès rapide aux tâches courantes d'un élément et à des informations critiques.

Pour afficher le menu contextuel d'un élément, cliquez avec le bouton droit de la souris sur l'élément. Par exemple, lorsque vous cliquez avec le bouton droit de la souris sur un périphérique géré dans la liste **Mes périphériques**, son menu contextuel affiche généralement les options suivantes :

- **Supprimer du groupe :** Supprime l'élément d'un groupe défini par l'utilisateur.
- **Cible :** Déplace le périphérique sélectionné vers la liste Périphériques ciblés. **Remarque :** Si les périphériques ciblés ne s'affichent pas dans la liste **Cible**, cliquez sur **Actualiser** dans l'onglet **Périphériques ciblés**.
- **Envoyer un Ping au périphérique :** S'assure que le périphérique est réveillé.
- **Périphérique Tracert :** Envoie une commande de suivi de l'itinéraire pour afficher l'envoi et la réception d'un paquet réseau ainsi que le nombre de sauts requis pour que le paquet atteigne sa destination.

Cette aide ne présente pas le menu contextuel de tous les éléments de la console, mais il est recommandé de cliquer avec le bouton droit de la souris sur tout élément pour afficher les options disponibles.

Utilisation des outils

Les outils sont disponibles via le volet de gauche. Utilisez les touches fléchées situées dans la partie supérieure du volet pour afficher tous les outils.

Un administrateur affiche tous les outils dans le volet de navigation de gauche. Les autres utilisateurs visualisent uniquement les outils (fonctions) autorisés par leurs droits attribués. Par exemple, si un utilisateur ne dispose pas du droit Rapports, l'outil Rapports n'apparaît pas dans le volet de navigation de gauche.

La section suivante présente la liste complète des outils :

- **Mises à jour de logiciel :** Télécharger les paquets de mise à jour applicables.
- **Scripts :** Créer et gérer des scripts.
- **Tâches planifiées :** Afficher toutes les tâches (provenant de Configuration d'agent, Vulnérabilités, Découverte de périphérique, ou Scripts) dans le Planificateur.

- **Surveillance :** Surveiller en temps réel la performance de vos périphériques gérés en utilisant plusieurs attributs.
- **Alerte :** Configurer des alertes en réglant les seuils et les réponses utilisées par le produit lorsqu'un seuil est dépassé.
- **Configuration d'agent :** Définir une configuration d'agent IPMI (Contrôleur de gestion de la carte de base, BMC), Linux ou Windows.
- **Découverte de périphériques :** Rechercher sur le réseau des périphériques non analysés dans la base de données principale.
- **Journaux :** Affiche le journal d'alertes qui permet de visualiser les alertes marquées sur les périphériques gérés.
- **Rapports :** Gérer des rapports de service prédéfinis.
- **Requêtes :** Créer et modifier des requêtes pour la base de données afin d'isoler des périphériques spécifiques qui satisfont les critères.
- **Utilisateurs :** Contrôler l'accès des utilisateurs aux périphériques et outils selon leurs droits et leur portée.
- **Préférences :** Créer des attributs d'inventaire personnalisés et afficher des informations sur la mise sous licence.
- **Configuration du matériel :** Ouvre une fenêtre distincte qui affiche les options de configuration des périphériques Intel* AMT.

Lorsque vous cliquez sur un nom d'outil, la fenêtre de l'outil s'ouvre dans le volet de droite.

Affichage des propriétés de périphérique

Dans la vue **Mes périphériques**, vous pouvez rapidement visualiser des informations sur un périphérique en cliquant sur celui-ci dans la liste et en sélectionnant **Propriétés** dans le volet du bas.

Des informations plus détaillées sur le périphérique sont disponibles dans ses données d'inventaire. Vous pouvez afficher des données d'inventaire dans la vue **Mes périphériques** en cliquant sur le périphérique et en sélectionnant l'onglet **Afficher l'inventaire** dans le volet du bas pour ouvrir la fenêtre **Inventaire** intégrale.

Ciblage de périphériques

La liste **Périphériques ciblés** vous aide à compléter des tâches sur des périphériques sélectionnés, telles que le déploiement des agents ou la recherche de mises à jours de logiciel sur un groupe sélectionné de périphériques.

Le nombre recommandé de périphériques à ajouter à la liste est 250 ou moins. Les périphériques doivent rester dans la liste jusqu'à expiration de la session de console (après 20 minutes d'inactivité).

Ajoutez des périphériques dans la liste **Périphériques ciblés** en les sélectionnant dans une liste de périphérique. Si vous ne trouvez pas le périphérique voulu, utilisez le bouton **Rechercher** de la barre d'outils. Recherchez un périphérique donné ou recherchez-en plusieurs en utilisant des caractères génériques % ou *. Cliquez sur le bouton **Cible** de la barre d'outils pour ajouter le périphérique à la liste **Périphériques ciblés**. Si le bouton n'est pas visible, cliquez sur le bouton **<<**.

Si plusieurs périphériques sont trouvés, sélectionnez celui que vous souhaitez ajouter à la liste, puis cliquez sur **Cible**. Si la liste de périphériques renvoyés s'étend sur plusieurs pages, vous devez cliquer sur **Cible** pour chaque page. Vous ne pouvez pas sélectionner des périphériques sur plusieurs pages et cliquer une seule fois sur les boutons pour toutes les pages. Vous pouvez cliquer sur la flèche vers le bas située sous la barre d'outils à l'extrême droite pour définir le nombre de périphériques à afficher par page. Vous pouvez afficher jusqu'à 500 périphériques par page. Pour modifier le nombre de périphérique affichés dans une liste, reportez-vous Configuration de la page sous **Préférences**.

Avec un ou plusieurs périphériques dans la liste **Périphériques ciblés**, vous pouvez compléter une tâche telle que le déploiement d'une configuration d'agent sur chaque périphérique ciblé ou le déplacement des périphériques non gérés dans la liste **Mes périphériques**.

Pour cibler les périphériques

1. Dans la liste **Mes périphériques** ou dans la vue **Périphériques découverts**, sélectionnez le périphérique à cibler pour une action. Vous pouvez sélectionner plusieurs périphériques en utilisant les méthodes standard de sélection multiple (SHIFT+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.

Dans le volet inférieur, les périphériques sélectionnés sont répertoriés dans l'onglet **Périphériques ciblés**. Une fois qu''ils sont répertoriés dans cet onglet, vous pouvez ouvrir un outil (tel que Déploiement d'agent) et planifier une tâche qui peut être appliquée aux périphériques cibles. Si vous avez ciblé des périphériques non gérés, vous pouvez cliquer sur l'onglet **Gérer** et les déplacer dans la liste **Mes périphériques**.

Filtrage de la liste d'affichage

La liste **Mes périphériques** dispose d'une icône de filtrage qui permet de déterminer quels périphériques sont affichés dans la liste. Vous pouvez filtrer par un seul critère (par nom de périphérique ou adresse IP), ou vous pouvez combiner les critères pour vous concentrer sur un sous-ensemble d'ordinateurs.

Pour filtrer la liste d'affichage

1. Dans la liste **Mespériphériques**, cliquez deux fois sur **Tous les périphériques** ou naviguez vers un groupe.
2. Cliquez sur **Filtrer**  dans la barre d'outils.
3. Dans la liste déroulante, sélectionnez **Nom de périphérique** ou **Adresse IP**.
4. Définissez les paramètres du critère spécifié en renseignant la zone de texte. Dans la zone **Recherche**, les caractères étendus suivants ne sont pas pris en charge : < , > , " , ' , !.

   Si vous filtrez par nom de périphérique, entrez le nom d'hôte ou la plage de noms d'ordinateurs. Vous pouvez utiliser des caractères génériques pour trouver certains noms d'ordinateurs (comme *srv).

5. Cliquez sur **Rechercher**.

Utilisation de groupes

Pour faciliter la gestion, vous pouvez organiser les périphériques en groupes. Vous pouvez créer des groupes afin d'organiser les périphériques selon leur fonction, emplacement géographique, service, attributs de périphérique ou toute autre catégorie correspondant à vos besoins. Par exemple, vous pouvez créer un groupe de serveurs Web pour tous les serveurs configurés en tant que serveur Web ou créer un groupe qui inclut tous les périphériques exécutant un système d'exploitation spécifique. Cliquez avec le bouton droit de la souris sur un groupe pour l'ouvrir, le supprimer ou cibler tous les périphériques qu'il contient pour des actions telles que les ensembles de règles d'alerte et le déploiement d'agent.

La vue principale **Mes périphériques** contient les groupes suivants :

- **Tous les périphériques :** Répertorie tous les périphériques pouvant être visualisés par l'utilisateur actuellement connecté, selon la limite de sa portée, dans une liste non hiérarchique (sans sous-groupes). Pour un administrateur, le groupe **Tous les périphériques** répertorie tous les périphériques ayant été analysés ou déplacés vers la base de données principale. Les périphériques configurés avec l'agent de gestion standard apparaissent automatiquement dans le groupe/dossier **Tous les périphériques** où ils peuvent être analysés dans la base de données principale à l'aide du scanner d'inventaire. Les utilisateurs, y compris les administrateurs, ne peuvent pas créer de groupes dans **Tous les périphériques**.
- **Groupes publics :** Répertorie tous les groupes/périphériques qu'un administrateur a ajoutés à partir du groupe **Tous les périphériques**, ainsi que les groupes de châssis Blade. Un administrateur (utilisateur doté du droit d'administrateur) voit tous les périphériques dans ce groupe, alors que les autres utilisateurs voient uniquement ceux autorisés par leur portée. Seuls les administrateurs peuvent créer des groupes sous **Groupes publics**.
- **Groupes privés :** Répertorie les groupes/périphériques pour l'utilisateur actuellement connecté, en fonction de sa portée. Un utilisateur peut créer des sous-groupes de périphériques uniquement sous **Groupes privés**. Les utilisateurs peuvent ajouter des périphériques dans leur groupe **Groupes privés**, ou dans ses sous-groupes, en les déplaçant ou les copiant depuis les groupes **Groupes publics** et **Tous les périphériques**. Tous les utilisateurs peuvent créer des groupes sous **Groupes privés**.

Pour plus d'informations sur les périphériques pouvant être affichés et gérés dans la vue des périphériques et sur les outils de gestion à votre disposition, reportez-vous à la section "Administration basée sur les rôles".

Types de groupe

Vous pouvez créer et gérer deux types de groupes :

- **Groupes statiques**. Un *groupe statique* est composé de périphériques que vous avez manuellement ajoutés à ce groupe. Les groupes statiques peuvent uniquement être modifiés en ajoutant ou en supprimant des périphériques.

- **Groupes dynamiques**. Un *groupe dynamique* est composé d'ordinateurs qui satisfont la définition de la requête ou du filtre. Chaque fois que le groupe est développé, la requête est résolue et les résultats s'affichent. Par exemple, un groupe dynamique peut contenir tous les périphériques qui sont actuellement dans un état d'avertissement. Les ordinateurs sont ajoutés ou supprimés de ce groupe en fonction de leur état.

Pour créer un groupe statique

1. Dans la vue de périphérique de la console, cliquez deux fois sur le groupe parent (tel que **Groupes privés**), puis cliquez sur **Ajouter un groupe**.
2. Entrez un nom pour le nouveau groupe.
3. Sélectionnez **Statique**, puis sur **OK**.

Une fois le groupe statique créé, vous pouvez déplacer ou copier les périphériques dans le groupe en les sélectionnant dans une liste et en cliquant sur le bouton **Déplacer/Copier** de la barre d'outils. Vous pouvez copier des périphériques à partir de la liste **Tous les périphériques** et les placer dans un groupe ou les déplacer/copier depuis d'autres groupes.

Pour créer un groupe dynamique

1. Dans la vue de périphérique de la console, cliquez deux fois sur le groupe parent (tel que **Groupes privés**), puis cliquez sur **Ajouter un groupe**.
2. Entrez un nom pour le nouveau groupe.
3. Sélectionnez **Dynamique**, puis sur **OK**.

Une fois le groupe dynamique créé, vous devez spécifier un filtre pour ce groupe afin de déterminer quels ordinateurs s'y affichent. Vous pouvez spécifier un nouveau filtre ou baser le filtre sur une requête existante.

Pour créer un nouveau filtre

1. Sélectionnez le groupe dynamique créé (les **Propriétés du groupe** s'affichent dans le volet du bas).
2. Dans **Propriétés du groupe**, sélectionnez **Créer un nouveau filtre** et cliquez sur **Nouveau filtre**.
3. Sélectionnez le critère du filtre que vous souhaitez utiliser, puis cliquez sur **OK**.

Pour créer un filtre basé sur une requête existante

1. Sélectionnez le groupe dynamique créé (les **Propriétés du groupe** s'affichent dans le volet du bas).
2. Dans **Propriétés du groupe**, sélectionnez **Créer un filtre en fonction d'une requête existante**.
3. Sélectionnez la requête existante que vous souhaitez utiliser pour filtrer le groupe et cliquez sur **Nouveau filtre**.
4. Sélectionnez tout critère supplémentaire de filtre que vous souhaitez utiliser, puis cliquez sur **OK**.

Si vous basez un filtre sur une requête existante et et que vous, ou un autre utilisateur, la modifiez plus tard, le filtre basé sur cette requête ne sera pas dynamiquement modifié pour correspondre à la requête modifiée.

Utilisation de l'onglet Actions

Utilisez l'onglet **Actions** pour exécuter des opérations sur les périphériques ciblés et sélectionnés. Vous pouvez supprimer des périphériques de la liste des ordinateurs gérés, mettre sous tension, mettre hors tension, redémarrer des périphériques et surveiller les connexions aux périphériques gérés.

Supprimer des périphériques

Cette option permet de supprimer les périphériques ciblés ou sélectionnés de la liste d'ordinateurs gérés. La fonction de suppression peut supprimer un ou plusieurs périphériques de n'importe quel groupe (un groupe par défaut ou un groupe créé par un utilisateur) dans System Manager. Une fois qu'un périphérique a été supprimé d'un groupe, il est complètement supprimé de toutes les listes des périphériques gérés/répertoriés, y compris le groupe par défaut **Tous les périphériques**.

Si vous supprimez un nombre important de périphériques, l'opération peut expirer. Si l'opération expire, tentez de diviser l'opération en plusieurs opérations plus petites.

Options d'alimentation

Les **options d'alimentation** permettent de mettre hors tension, redémarrer, et dans le cas des ordinateurs IPMI gérés, mettre sous tension les périphériques distants. Dans le cas des serveurs non-IPMI, l'agent LANDesk doit être déployé sur le périphérique pour que ce dernier puisse exécuter les fonctions de redémarrage et de mise hors tension. Avec les ordinateurs IPMI, vous devez disposer des références d'authentification correctes pour exécuter les fonctions de mise sous/hors tension et de redémarrage. Si l'agent LANDesk est déployé sur un boîtier IPMI, vous pouvez alors exécuter les fonctions de mise hors tension et de redémarrage sans les références IMPI. Utilisez l'utilitaire Configuration des services pour définir le mot de passe IPMI BMC à utiliser pour gérer les serveurs IPMI.

Pour utiliser les options d'alimentation

1. Dans la liste **Mes périphériques**, cliquez sur un périphérique ou ciblez une liste de périphériques.
2. Dans le volet inférieur, cliquez sur l'onglet **Actions**.
3. Cliquez sur **Options d'alimentation**.
4. Indiquez si vous souhaitez effectuer l'action sur les périphériques de la liste Périphériques ciblés ou uniquement sur les périphériques sélectionnés.
5. Choisissez parmi les options suivantes :
    - Redémarrage

- Mise hors tension
- Mise sous tension (fonctionne sur les périphériques dotés d'IPMI et de Wake on LAN)

6. Cliquez sur la **fenêtre Afficher la redirection de la console** pour lancer un conteneur ultra-mince via un lanceur (il est plus facile de recompiler le lanceur pour EM64T que d'exécuter la commande TTY).

   Lors de la mise sous tension ou du redémarrage d'un serveur IPMI géré, vous pouvez ouvrir une fenêtre de redirection de la console qui affiche les informations de démarrage du serveur. Ceci peut être utile si vous voulez vous assurer que le serveur redémarre. Vous pouvez également utiliser la fenêtre de la console pour suspendre le processus de redémarrage et modifier les paramètres du BIOS sur le serveur géré.

   Pour afficher la fenêtre de redirection de la console, le serveur doit avoir activé l'option de redirection de la console via un port en série dans la configuration du BIOS. Les données de la console sont envoyées au port en série. Si le serveur et la console de l'administrateur sont connectés par un câble en série, la redirection de la console s'effectue par ce câble. Sinon, System Manager initialise une connexion SOL (Serial over LAN) pour rediriger les données du port en série vers la connexion LAN. La connexion SOL reste ouverte tant que la fenêtre de la console est ouverte. Fermez la fenêtre ue fois que toutes les données ont été affichées dans la console.

   Lorsque la fenêtre de la console s'ouvre, une deuxième fenêtre de message s'affiche. Vous pouvez fermer la fenêtre de message. Des caractères aléatoires peuvent s'afficher dans la fenêtre après l'ouverture de la fenêtre de redirection de la console, mais avant l'affichage de la séquence de redémarrage. Ces caractères s'affichent car le BMC du serveur envoie des messages de pulsation qui sont transmis à la console de l'administrateur via la connexion. Les caractères ne s'affichent pas lorsque la console affiche l'écran de démarrage, mais ils peuvent réapparaître une fois le processus de démarrage terminé.

Moniteur de périphérique

Utilisez Moniteur de périphérique pour vérifier la connectivité des périphériques sélectionnés. Si un périphérique perd sa connectivité de réseau, il ne peut pas envoyer une alerte au serveur principal. Le moniteur de périphérique s'assure que les périphériques peuvent toujours communiquer sur le réseau.

1. Dans la liste **Tous les périphériques**, cliquez sur un périphérique ou ciblez une liste de périphériques.
2. Dans le volet du bas, cliquez sur l'onglet **Actions**, puis cliquez sur **Moniteur de périphérique**.
3. Pour afficher une liste des périphériques actuellement surveillés, cliquez sur **Afficher les périphériques surveillés**.
4. Entrez un nombre pour définir les minutes entre les balayages de commande Ping et le nombre de fois que le produit tentera de communiquer avec un périphérique.
5. Indiquez si vous souhaitez effectuer l'action sur les périphériques dans la Liste des périphériques ciblés ou sur tous les périphériques du groupe **Tous les périphériques**.
6. Pour arrêter de surveiller tous les périphériques, sélectionnez **Ne jamais envoyer une commande Ping aux périphériques**.

7. Cliquez sur **Appliquer**.

Seul le dernier groupe des périphériques ciblés est surveillé. Par exemple, si vous sélectionnez le périphérique A et le périphérique B, et appliquez sur ces périphériques la surveillance de périphérique, le serveur principal enverra une commande Ping uniquement aux périphériques A et B. Si vous sélectionnez ensuite un périphérique C et D, puis appliquez sur ces derniers la surveillance de périphérique, seuls les périphériques C et D seront surveillés. Les périphériques A et B ne sont plus surveillés.

Colonnes personnalisées

Utilisez l'option **Colonnes personnalisées** pour modifier les champs et les noms des colonnes. Un nom correspond au nom de la colonne et un champ contient le ou les attributs qui apparaissent dans la colonne (si un attribut est présent). Aucune des modifications de colonne que vous effectuez ne sera visible par d'autres utilisateurs. Les modifications de personnalisation des colonnes s'afficheront dans la vue **Mes périphériques**.

Ce produit inclut une configuration de colonne par défaut avec sept colonnes. Vous ne pouvez pas modifier la configuration par défaut, mais vous pouvez définir une configuration de colonne personnalisée que vous pouvez utiliser comme configuration par défaut.

Il n'est pas recommandé de créer des colonnes avec plusieurs noms de champ. Par exemple, si vous créez un champ Computer.Software.Package.Name et si le périphérique dispose de plusieurs paquets, System Manager ne répertoriera qu'un seul nom de paquet par ligne, même si les différents noms de paquet sont sur le même périphérique. La liste **Tous les périphériques** contiendra donc plusieurs entrées pour un périphérique unique.

Pour créer une configuration de colonne personnalisée

1. Dans le volet de navigation de gauche, cliquez sur **Préférences**.
2. Cliquez sur l'onglet **Colonnes personnalisées**.
3. Cliquez sur **Nouveau**.
4. Entrez un nom pour la configuration de colonne.
5. Dans la case du haut, cliquez sur chaque intitulé de colonne que vous voulez, puis cliquez sur **Ajouter**.

   La case affiche une liste qui représente toutes les données d'inventaire actuellement dans la base de données. Explorez cette liste pour sélectionner un attribut à afficher dans la liste des résultats de requête. Souvenez-vous de sélectionner des attributs qui vous aident à identifier les clients renvoyés dans la requête. Si vous ne pouvez pas trouver des attributs à afficher, vous pouvez les ajouter dans la boîte de dialogue Attributs personnalisés. Toutefois, ces attributs doivent être attribués à des ordinateurs avant qu'ils ne puissent s'afficher dans la boîte de dialogue de requête.

   Remarque : Si vous sélectionnez dans la base de données un attribut doté de la relation 1:*, vous obtenez des doublons pour le périphérique. Lorsque vous sélectionnez des attributs dotés de la relation 1:1 (un seul attribut possible, tel que la balise Computer.System.Asset), vous n'obtiendrez pas de doublons.

6. Pour modifier l'ordre des colonnes, sélectionnez un intitulé de colonne et cliquez sur **Monter** ou **Descendre**.
7. Pour supprimer une colonne, sélectionnez-la dans la case du bas et cliquez sur **Supprimer**.
8. Pour modifier l'intitulé existant d'une colonne, sélectionnez l'intitulé dans la case du bas, cliquez sur **Modifier**, effectuez vos modifications et appuyez sur **Entrée**. Les caractères étendus suivants ne sont pas pris en charge : < , > , ' , " , !.
9. Cliquez sur **OK** pour enregistrer la configuration de colonne.
10. Pour utiliser la configuration de colonne personnalisée lorsque vous affichez la liste **Tous les périphériques**, sélectionnez-la et cliquez sur **Définir comme configuration actuelle de colonne** dans la barre d'outils.

Pour modifier une configuration de colonne personnalisée

1. Dans le volet de navigation de gauche, cliquez sur **Préférences**.
2. Cliquez sur l'onglet **Colonnes personnalisées**.
3. Sélectionnez une configuration de colonne personnalisée et cliquez sur **Modifier**.
4. Dans la case du haut, sélectionnez un intitulé de colonne et cliquez sur **Ajouter** pour ajouter la colonne (reportez-vous aux remarques sous l'étape 5 ci-dessus).
5. Pour supprimer une colonne, sélectionnez-la dans la case du bas et cliquez sur **Supprimer**.
6. Pour modifier l'intitulé existant d'une colonne, sélectionnez l'intitulé dans la case du bas, cliquez sur **Modifier**, effectuez vos modifications et appuyez sur **Entrée**. Les caractères étendus suivants ne sont pas pris en charge : < , > , ' , " , !.
7. Pour modifier l'ordre des colonnes, sélectionnez un intitulé de colonne et cliquez sur **Monter** ou **Descendre**.
8. Cliquez sur **OK** pour enregistrer vos modifications.

Attributs personnalisés

Les attributs sont des caractéristiques ou des propriétés qui appartiennent à un périphérique. Plus un périphérique dispose d'attributs dans la base de données, plus il est facile de l'identifier de manière unique. Vous pouvez créer des attributs personnalisés uniquement si LANDesk® Server Manager est doté du droit Administrateur. Si des attributs personnalisés ont été créés et ajoutés à la base de données principale, vous pouvez attribuer des valeurs pour ces attributs à un périphérique géré. Si aucun attribut personnalisé n'a été ajouté à la base de données principale, l'option **Assigner des attributs** ne s'affiche pas dans l'onglet **Actions**.

Pour attribuer des attributs personnalisés à des périphériques

1. Dans la liste **Tous les périphériques**, sélectionnez un ou plusieurs périphériques.
2. Dans le volet inférieur, cliquez sur l'onglet **Actions**.
3. Dans le volet de gauche, sélectionnez **Assigner des attributs**.
4. Chaque nom d'attribut contient une liste déroulante de valeurs. Sélectionnez une valeur dans la liste déroulante du nom d'attribut et répétez selon les besoins. Cliquez sur **Périphériques sélectionnés**.
5. Cliquez sur **Assigner**, puis cliquez sur **OK**.

Vous pouvez également assigner des attributs personnalisés à plusieurs périphériques que vous avez ciblés. Si la liste Cible contient des périphériques, cliquez sur **Périphériques ciblés** à l'étape 4 ci-dessus.

Configuration de la page

Utilisez **Configuration de la page** pour configurer les préférences d'affichage des pages listant des périphériques ou affichant des graphiques.

1. Dans le volet de navigation de gauche, cliquez sur **Préférences**.
2. Cliquez sur l'onglet **Configuration de la page**.
3. Dans la liste déroulante **Type de graphe**, sélectionnez le type de graphe à afficher dans **Rapports**.
4. Dans la zone **Eléments/page**, entrez le nombre maximal d'éléments à afficher dans chaque page utilisant un système de pagination. La valeur doit être inférieure ou égale à 500 éléments.

Mode Débutant

Vous pouvez afficher du texte avec les boutons des barres d'outils pour permettre aux nouveaux utilisateurs d'identifier leurs fonctions. Si cette option n'est pas sélectionnée, seules les icônes s'affichent sur les barres d'outils. Les icônes afficheront un texte descriptif au passage de la souris.

1. Pour afficher du texte avec les boutons des barres d'outils, cochez la case **Afficher le texte sur les barres d'outils**.
2. Cliquez sur **Mettre à jour**.

Affichage de la console d'informations de serveur

Utilisez la console d'informations de serveur pour afficher des informations récapitulatives de niveau supérieur sur un périphérique, afficher des informations système telles que des informations sur le processeur ou le ventilateur, surveiller l'état de santé et les seuils de composants clé d'un périphérique, gérer des vulnérabilités et mettre sous tension, mettre hors tension ou redémarrer un périphérique. La console d'informations de serveur contient les sections suivantes répertoriées dans le volet de navigation de gauche.

- Informations système
- Mises à jour de logiciel
- Surveillance
- Ensembles de règles
- Options d'alimentation
- Configuration du matériel

Pour afficher la console d'informations de serveur d'un périphérique, vous devez auparavant déployer l'agent de gestion standard sur ce périphérique (voir Configuration des agents). En outre, le périphérique doit être redémarré après l'installation de l'agent pour que la console d'informations de serveur fonctionne correctement. Ce redémarrage est requis si vous installez l'agent sur le serveur principal ou sur des périphériques gérés.

Pour afficher la console d'informations de serveur

1. Dans la vue **Mes périphériques**, cliquez deux fois sur le nom de périphérique.

   La console s'ouvre dans une nouvelle fenêtre de navigateur et affiche par défaut la page **Récapitulatif de santé**.

2. Cliquez sur les boutons du volet de navigation de gauche pour afficher les informations du serveur et utiliser les outils disponibles.

Informations système

Informations système contient un récapitulatif des données relatives à la santé d'un périphérique ainsi que des informations sur les matériels et logiciels, les journaux système et d'autres données telles que les informations d'inventaire et de réseau.

Récapitulatif de santé

La page **Récapitulatif de santé** fournit un aperçu rapide de la santé de ce périphérique. Vous pouvez déterminer rapidement si les éléments matériels sélectionnés fonctionnent correctement et s'il existe des problèmes potentiels qui doivent être examinés.

Lorsque des éléments de santé passent à un état critique ou d'avertissement, le bouton correspondant contient une icône jaune (avertissement) ou rouge (critique) qui indique la présence d'un problème. Cliquez sur le bouton pour afficher une description de l'événement ayant provoqué une alerte critique ou d'avertissement.

Récapitulatif du système

Utilisez l'écran **Récapitulatif du système** pour afficher des informations importantes sur le périphérique sélectionné. Selon les types de matériel et logiciel configurés sur le périphérique, les informations suivantes s'affichent.

- **Santé :** La santé globale du périphérique, telle que définie par les conditions et les paramètres que vous avez configurés.
- **Type :** Le type de périphérique, tel que impression, application ou base de données.
- **Fabricant :** Le fabricant du périphérique.
- **Modèle :** Le modèle du périphérique.
- **Version du BIOS :** La version du BIOS du périphérique.
- **Système d'exploitation :** Le système d'exploitation du périphérique.
- **Version du SE :** Le numéro de version du système d'exploitation.
- **UC :** Le fabricant, modèle et la vitesse du processeur du périphérique.

- **Scanner de vulnérabilités :** La version du scanner de vulnérabilités.
- **Contrôle distant :** La version de l'agent de contrôle distant.
- **Distribution de logiciel :** La version de l'agent de distribution de logiciel.
- **Scanner d'inventaire :** La version du scanner d'inventaire.
- **Type IPMI, version IPMI :** Le type et le numéro de version de l'interface IPMI que le périphérique utilise.
- **Version SDR :** La version du SDR (Sensor Data Record) dans le BMC du périphérique.
- **Version BMC :** La version du contrôleur de gestion de la carte de base (BMC) du périphérique.
- **Noyau :** Pour les périphériques Linux, le numéro de version du noyau installé.
- **Surveillance :** Le numéro de version de l'agent de surveillance sur le périphérique.
- **Utilisation de l'UC :** Le pourcentage du processeur actuellement utilisé.
- **Mémoire physique utilisée* :** Le pourcentage de mémoire physique totale utilisée sur le périphérique.
- **Mémoire virtuelle utilisée* :** Le pourcentage de mémoire virtuelle totale utilisée sur le périphérique.
- **Dernière réinitialisation* :** La date et l'heure du dernier redémarrage du périphérique (dans le fuseau horaire de la base de données).
- **Lecteur :** Les lecteurs du périphérique avec la taille totale du lecteur et le pourcentage d'espace utilisé.

Ces informations sont tirées du registre dans Windows ou des fichiers de configuration dans Linux.

*Ces informations s'affichent lorsqu'un agent a été installé sur le périphérique.

Matériels

Utilisez la page **Matériel** pour afficher des détails sur la configuration matérielle du périphérique. Les éléments de la liste **Matériel** sont groupés dans les catégories suivantes. Notez que toutes les catégories ne s'affichent pas pour tous les périphériques. Par exemple, si le périphérique ne dispose pas de détecteurs thermiques et d'un ventilateur, la catégorie **Refroidissement** n'apparaît pas dans la liste.

- **UC :** processeurs et mémoire cache
- **Stockage :** lecteurs logiques, lecteurs physiques, supports amovibles et cartes réseau de stockage
- **Mémoire :** informations sur l'utilisation et modules de mémoire
- **Châssis :** le châssis du serveur ; indique si le boîtier est ouvert ou fermé
- **Périphériques d'entrée :** clavier, souris et autres périphériques
- **Carte mère :** carte mère, logements d'extension et BIOS
- **Refroidissement :** ventilateurs et détecteurs thermiques
- **Alimentation :** sources d'alimentation et tension

Configuration des seuils d'alerte pour les éléments matériels

Certains éléments de la liste **Matériel** représentent les données des détecteurs du périphérique, telles que les détecteurs thermiques. Si un périphérique géré contient des composants munis de détecteurs pris en charge, vous pouvez modifier les seuils de valeur des détecteurs qui

déclencheront une alerte. Par exemple, un détecteur thermique de processeur peut avoir défini des seuils de température supérieurs et inférieurs qui déclenchent des alertes d'avertissement et de limite critique. Les seuils sont en général basés sur les paramètres recommandés par le fabricant mais vous pouvez modifier les paramètres inférieurs et supérieurs dans la boîte de dialogue **Seuils**.

1. Dans la console d'informations du serveur, cliquez sur **Informations système**.
2. Ouvrez le dossier **Matériel** et explorez-le pour trouver l'élément matériel que vous voulez (tel que **Refroidissement | Températures**).
3. Dans la liste des détecteurs, cliquez deux fois sur le détecteur dont vous allez configurer les seuils.
4. Renseignez les zones de texte des seuils inférieurs et/ou supérieurs ou faites glisser les barres de défilements à droite ou à gauche pour modifier les valeurs.
5. Cliquez sur **Mettre à jour** pour enregistrer vos modifications.
6. Pour restaurer les valeurs d'origine des seuils, cliquez sur **Restaurer les valeurs par défaut**.

Journaux

Cette page affiche les journaux système locaux, le journal d'événements du système (System Events Log, SEL) pour les périphériques dotés d'IPMI et un journal d'alerte.

Il n'existe pas de boutons pour effacer les journaux locaux, tels que les journaux d'applications, de sécurité et système depuis la console, mais vous pouvez afficher et effacer les fichiers journaux via l'outil Gestion de l'ordinateur de Windows.

Si le BIOS de ce périphérique peut effacer le journal SMBIOS, cliquez sur le bouton **Effacer le journal** pour supprimer toutes les entrées du fichier journal. Ce bouton n'est pas disponible si cette action n'est pas prise en charge par le BIOS.

Logiciels

La page **Logiciel** affiche les informations récapitulatives sur les processus, les services et les paquets sur ce périphérique ainsi qu'une liste des variables d'environnement actuelles.

- **Processus :** affiche les processus en cours d'exécution ; sélectionnez un processus et cliquez sur **Arrêter le processus** pour l'interrompre
- **Services :** affiche les services disponibles sur le périphérique ainsi que leur état ; sélectionnez un service et cliquez sur **Arrêter**, **Démarrer** ou **Redémarrer** pour effectuer des modifications
- **Paquets :** répertorie les paquets installés avec les numéros de version et le nom du fournisseur
- **Environnement :** répertorie les variables d'environnement actuellement définies sur le périphérique

Autre

La page **Autre** affiche les informations d'inventaire et un récapitulatif du matériel et des connexions réseau

- **Informations sur les biens :** affichez et modifiez les informations de gestion des biens, telles que l'emplacement et le numéro de balise du bien ; vous pouvez également afficher le numéro de série, le fabricant et le type de châssis
- **Informations de réseau :** affichez la liste des matériels réseau installés, les statistiques de l'activité du réseau, un récapitulatif de la configuration (contenant l'adresse IP, l'adresse de la passerelle par défaut et les informations de serveur DNS, WINS et DHCP) et la liste des connexions réseau actuelles (lecteurs mappés)

Mises à jour de logiciel

Utilisez la page **Mises à jour de logiciel** pour rechercher les vulnérabilités détectées sur le périphérique sélectionné.

Pour déterminer la présence de vulnérabilités détectées

1. Dans la vue **Mes périphériques**, cliquez deux fois sur le périphérique que vous souhaitez configurer. La console d'informations du serveur s'ouvre dans une nouvelle fenêtre de navigation.

2. Dans le volet de navigation de gauche, cliquez sur **Mises à jour de logiciels**.

Descriptions des colonnes

- **ID :** Identifie la vulnérabilité par un code alphanumérique unique défini par le fournisseur.
- **Gravité :** Indique le niveau de gravité de la vulnérabilité. Les niveaux de gravité incluent : Service Pack, Critique, Elevée, Moyenne, Faible, Sans objet et Inconnue.
- **Titre :** Décrit la nature ou cible de la vulnérabilité dans une brève chaîne de texte.
- **Langue :** Indique la langue du système d'exploitation affecté par la vulnérabilité.
- **Date de publication :** Indique la date à laquelle la vulnérabilité a été publiée par le fournisseur.
- **Installation silencieuse :** Indique si le correctif associé à la vulnérabilité s'installe en mode silencieux (sans interaction de l'utilisateur). Certaines vulnérabilités peuvent avoir plus d'un correctif. Si un des correctifs d'une vulnérabilité ne s'installe pas en mode silencieux, l'attribut **Installation silencieuse** de la vulnérabilité spécifie **Non**.
- **Peut être réparé :** Indique si la vulnérabilité peut être réparée par installation et déploiement d'un fichier de correctif. Les valeurs possibles sont : Oui, Non et Quelques (pour une vulnérabilité qui inclut plusieurs règles de détection et toutes les vulnérabilités détectées ne peuvent pas être réparées).

Surveillance

Utilisez **Surveillance** pour afficher les graphes et les compteurs de performance et pour régler les seuils des composants de périphérique. Pour plus d'informations sur cette fonction, reportez-vous à la section Surveillance de périphérique.

Pour sélectionner un compteur de performance à surveiller

1. Dans la vue **Mes périphériques**, cliquez deux fois sur le périphérique que vous souhaitez configurer. La console d'informations du serveur s'ouvre dans une nouvelle fenêtre de navigation.

2. Dans le volet de navigation de gauche, cliquez sur **Surveillance**.
3. Cliquez sur l'onglet **Configuration des compteurs de performance**.
4. Dans la colonne **Objets**, sélectionnez l'objet à surveiller.
5. Dans la colonne **Instances**, sélectionnez l'instance de l'objet à surveiller, si applicable.
6. Dans la colonne **Compteurs**, sélectionnez le compteur spécifique à surveiller.
7. Spécifiez la fréquence d'interrogation et combien de jours l'historique du compteur doit être conservé.
8. Dans la zone de texte **Alerter une fois le compteur hors limites**, spécifiez le nombre de fois que le compteur est autorisé à dépasser les seuils avant qu'une alerte ne soit générée.
9. Spécifiez les seuils supérieurs et inférieurs.
10. Cliquez sur **Appliquer**.

Pour afficher un graphe de performance pour un compteur surveillé.

1. Cliquez sur l'onglet **Compteurs de performance active**.
2. Sélectionnez un compteur dans la liste.
3. Dans la liste **Compteurs**, sélectionnez le compteur pour lequel afficher un graphe de performance.
4. Sélectionnez **Afficher les données en temps réel** pour afficher un graphe des performances actuelles ou sélectionnez **Afficher les données historiques** pour afficher un graphe qui affiche des performances pour la période spécifiée (Garder un historique) lors de la sélection du compteur.

Dans le graphe de performance, l'axe horizontal représente le temps écoulé. L'axe vertical représente les unités mesurées, telles que octets par seconde (lors de la surveillance de transferts de fichier, par exemple), pourcentage (lors de la surveillance du pourcentage du processeur utilisé) ou octets disponibles (lors de la surveillance de l'espace du disque dur).

Ensembles de règles

Utilisez la page **Ensembles de règles** pour afficher une liste des configurations des ensembles de règles d'alerte et de surveillance attribuées au périphérique sélectionné et pour afficher les détails de chaque alerte.

Pour afficher des ensembles de règles d'alerte

1. Dans la vue **Mes périphériques**, cliquez deux fois sur le périphérique que vous souhaitez configurer. La console s'ouvre dans une nouvelle fenêtre de navigation.
2. Dans le volet de navigation de gauche, cliquez sur **Ensembles de règles**.
3. Cliquez sur l'onglet **Ensembles de règles d'alerte**.

Le texte suivant décrit les détails fournis sur chaque alerte. Pour plus d'informations sur la modification de ces détails, reportez-vous à la section Utilisation des alertes.

- **Lorsque l'état atteint :** Lorsque l'état de l'alerte atteint l'état affiché, une alerte est générée.
- **Affecte la santé :** Si l'état d'alerte atteint le seuil spécifié, l'état affecte l'état de santé globale du périphérique. Vous pouvez sélectionner une alerte affectant la santé dans la boîte de dialogue Ensembles de règles d'alerte.
- **Nom de l'ensemble de règles :** Le nom de l'ensemble de règles d'alerte, comme défini dans la boîte de dialogue Ensembles de règles d'alerte.
- **Type d'alerte :** Le type d'alerte à générer, tel que message électronique, trappe SNMP ou exécution d'un programme.
- **Configuration d'action :** L'action qui se produit lorsqu'une alerte est générée, comme définie dans la boîte de dialogue Ensembles de règles des actions.
- **Gestionnaire d'alertes :** Le gestionnaire associé à l'alerte, tel qu'un gestionnaire de messagerie.
- **Instance :** Indique la source spécifique de l'alerte.

Pour afficher des ensembles de règles de surveillance

1. Dans la vue **Mes périphériques**, cliquez deux fois sur le périphérique que vous souhaitez configurer. La console d'informations du serveur s'ouvre dans une nouvelle fenêtre de navigateur.
2. Dans le volet de navigation de gauche, cliquez sur **Ensembles de règles**.
3. Cliquez sur l'onglet **Ensembles de règles de surveillance**.

Le texte suivant décrit les détails fournis sur chaque ensemble de règles de surveillance. Pour plus d'informations sur la modification de ces détails, reportez-vous à la section Présentation de la surveillance.

- **Nom :** Le nom de la configuration d'ensemble de règles, tel que spécifié dans la page Surveillance.
- **Nom de l'ensemble de règles :** Spécifie si l'ensemble de règles est un ensemble de règles par défaut ou non.
- **Activé :** L'exécution de ensemble de règles sur le périphérique a été activée ou pas.
- **Seuil d'avertissement :** Le seuil auquel, si franchi, le périphérique envoie un message d'avertissement au serveur principal.
- **Seuil Critique :** Le seuil auquel, si franchi, le périphérique envoie un message d'avertissement critique au serveur principal.
- **Vérifier chaque :** La fréquence à laquelle l'élément est surveillé.

Options d'alimentation

Les **options d'alimentation** permettent de mettre hors tension, redémarrer, et dans le cas des périphériques IPMI gérés et Intel AMT, mettre sous tension les périphériques distants. Dans le cas des serveurs non-IPMI, l'agent LANDesk doit être déployé sur le serveur pour que ce dernier puisse exécuter les fonctions de redémarrage et de mise hors tension.

Avec les périphériques IPMI et Intel AMT, vous devez avoir configurer les références d'authentification correctes pour exécuter les fonctions de mise sous/hors tension et de redémarrage. Si les périphériques IPMI ou Intel AMT disposent de l'agent LANDesk, vous pouvez alors exécuter les fonctions de mise hors tension et de redémarrage sans les références IMPI ou Intel AMT. Pour configurer les références d'authentification BMC pour les périphériques IPMI, ou

les références d'authentification de périphérique Intel AMT, utilisez l'utilitaire Configuration des services (reportez-vous à la section Configuration de services et de références d'authentification).

Pour utiliser des options d'alimentation sur le périphérique sélectionné

1. Dans la vue **Mes périphériques**, cliquez deux fois sur le périphérique que vous souhaitez configurer. La console s'ouvre dans une nouvelle fenêtre de navigateur.
2. Dans le volet de navigation de gauche, cliquez sur **Options d'alimentation**.
3. Choisissez parmi les options suivantes :

   -  Redémarrage
   -  Mise hors tension
   -  Mise sous tension

Configuration du matériel

L'outil **Configuration du matériel** vous permet de configurer des options pour les périphériques dotés de IPMI ou d'Intel* AMT. Cet outil et toute option associée s'affichent uniquement sur les périphériques dotés du matériel correspondant (par exemple, les options IPMI s'affichent uniquement si le périphérique est reconnu en tant que périphérique IPMI).

Vous pouvez générer des ID pour l'approvisionnement des périphériques Intel AMT, afficher les ID générées et modifier les options de configuration associées à l'approvisionnement des périphériques Intel AMT. Vous pouvez également définir les stratégies de disjoncteur (Circuit Breaker) qui détectent et bloquent les activités réseau suspicieuses sur les périphériques et vous pouvez activer la surveillance Agent Presence pour vous assurer que des agents de gestion sont constamment exécutés sur vos périphériques. Pour plus d'informations, reportez-vous à la section Prise en charge d'Intel AMT.

Pour les périphériques IPMI, vous pouvez personnaliser les options de configuration telles que l'horloge de surveillance, les options d'alimentation et les paramètres d'utilisateur BMC. Vous pouvez également configurer l'utilisation d'un canal LAN ou Serial over LAN pour maintenir une communication hors bande avec un périphérique IPMI. (Pour plus d'informations, reportez-vous à la section Configuration IPMI BMC.)

Pour les périphériques dotés d'un contrôleur Dell* DRAC (Remote Access Controller), vous pouvez afficher les journaux Dell DRAC et modifier les noms d'utilisateur pour accéder à OpenManage Server Administrator. (Pour plus d'informations, reportez-vous à la section Gestion des périphériques Dell DRAC.)

Gestion des périphériques Intel* AMT

Une fois qu'un périphérique configuré avec Intel* AMT est découvert et ajouté à la base de données principale, il peut être géré de manière limitée même si le périphérique ne dispose pas d'un agent LANDesk. (Voir la section Découverte des périphériques Intel* AMT pour plus

d'informations sur la découverte des périphériques et leur déplacement vers la base de données principale.)

Le tableau suivant répertorie les options de gestion disponibles lorsqu'un périphérique dispose uniquement d'Intel AMT par rapport à Intel AMT et un agent de gestion System Manager.

	Intel AMT uniquement	**Intel AMT et un agent**	**Agent uniquement**
Inventaire	récapitulatif	X	X
Journal d'événement	X	X	X
Gestionnaire de démarrage distant	X	X	
Désactivation du réseau de système d'exploitation		X	
Activation du réseau de système d'exploitation		X	
Forçage de vulscan au redémarrage		X	
Historique d'inventaire		X	X
Contrôle distant		X	X
Discussion		X	X
Transfert de fichiers		X	X
Exécution distante		X	X
Réveille		X	X
Arrêt		X	X

	Intel AMT uniquement	Intel AMT et un agent	Agent uniquement
Redémarrage		X	X
Analyse d'inventaire		X	X
Tâches planifiées et stratégies	limité	X	X
Options de groupe		X	X
Exécution du rapport d'inventaire		X	X
Système d'alerte Intel AMT		X	X

Pour afficher le récapitulatif d'inventaire d'Intel AMT d'un périphérique

1. Cliquez deux fois sur le périphérique dans la liste **Tous les périphériques**.
2. Dans la console d'informations du serveur, cliquez sur **Options d'Intel AMT**.
3. Cliquez sur **Récapitulatif d'inventaire**.

Le récapitulatif affiche l'identificateur unique global (GUID) du périphérique, le produit et le fabricant, le numéro de série et le BIOS, le processeur et les récapitulatifs de la mémoire et le numéro de version d'Intel AMT. Si des informations sont manquantes, actualisez les données en appuyant sur **Mettre à jour l'inventaire**.

Accès à des périphériques approvisionnés au mode Enterprise

Lorsque vous approvisionnez un périphérique Intel AMT au mode Enterprise, le serveur principal installe un certificat sur le périphérique pour garantir une communication sécurisée. Si le périphérique doit être géré par un autre serveur principal, il doit être désapprovisionné puis réapprovisionné par le nouveau serveur principal. Sinon, l'accès Intel AMT du périphérique ne répond pas car le nouveau serveur principal ne possède pas un certificat correspondant. De même, tout autre ordinateur tentant d'accéder à la fonction Intel AMT du périphérique échoue car il ne dispose pas d'un certificat correspondant. (Pour plus d'informations sur les modes d'approvisionnement, reportez-vous à la section Prise en charge d'Intel* AMT.)

Journal d'événement d'Intel AMT

System Manager permet d'afficher le journal d'événements généré par les périphériques Intel AMT. Les paramètres déterminent quels événements sont capturés dans ce journal. Vous

pouvez afficher la date et l'heure de l'événement, sa source (colonne Entité), une description, et la sévérité telle que définie par les paramètres Intel AMT (Critique ou Non critique). Vous pouvez également exporter les données journal dans un fichier formaté CSV (valeur séparée par des virgules).

Pour afficher le journal d'événement d'Intel AMT

1. Cliquez deux fois sur le périphérique dans la liste **Tous les périphériques**.
2. Dans la console d'informations du serveur, cliquez sur **Informations système**.
3. Développez les **Journaux** et cliquez sur **Journal Intel AMT**.
4. Pour exporter le journal dans un fichier formaté CSV, cliquez sur le bouton **Exporter** de la barre d'outils et spécifiez un emplacement dans lequel le fichier est enregistré.
5. Pour effacer toutes les données du journal, cliquez sur le bouton **Purger le journal** sur la barre d'outils.
6. Pour mettre à jour les entrées du journal, cliquez sur le bouton **Rafraîchir le journal** sur la barre d'outils.

Options d'alimentation d'Intel AMT

System Manager contient des options pour mettre sous tension et hors tension les périphériques Intel AMT. Ces options peuvent être utilisées même lorsque le système d'exploitation d'un périphérique ne fonctionne pas, tant que le périphérique est connecté au réseau et qu'il fonctionne sur une alimentation en veille.

Lorsque System Manager initialise des commandes d'option d'alimentation, il n'est pas possible dans certains cas de vérifier que les commandes sont prises en charge sur le matériel recevant la commande Certains périphériques avec Intel AMT peuvent ne pas prendre en charge toutes les fonctions d'option d'alimentation (par exemple, un périphérique peut prendre en charge le redémarrage IDE-R à partir d'un CD pas à partir d'une disquette). Consultez la documentation du fabricant du matériel si cette option d'alimentation ne fonctionne pas correctement avec un périphérique particulier. Si les options d'alimentation en fonctionnent pas comme prévu, vérifiez si Intel a créé des mises à jour du BIOS ou Firmware pour le périphérique.

Vous pouvez simplement mettre le périphérique sous tension ou non, ou vous pouvez redémarrer et spécifier la méthode de redémarrage du périphérique. Ces options sont décrites dans le tableau ci-dessous.

Mise hors tension	Interrompt l'alimentation du périphérique
Mise sous tension	Met le périphérique sous tension
Redémarrage	Cycle à nouveau l'alimentation hors et sous tension sur le périphérique
Démarrage normal	Démarre le périphérique en utilisant la séquence de démarrage définie par défaut sur le

	périphérique
Démarrage via un disque dur local	Force un démarrage via le disque dur du périphérique quel que soit le mode de démarrage par défaut sur le périphérique
Démarrage via un lecteur CD/DVD local	Force un démarrage via le lecteur de CD ou DVD du périphérique quel que soit le mode de démarrage par défaut sur le périphérique
Démarrage PXE	Lorsque le périphérique doté de PXE est redémarré, il recherche un serveur PXE sur le réseau ; si ce dernier est trouvé, une session de démarrage PXE est initialisée sur le périphérique
Démarrage IDE-R	Redémarre le périphérique en utilisant l'option de redirection IDE sélectionnée (voir ci-dessous)
Entrer la configuration du BIOS	Lorsqu'un périphérique est démarré, il permet à l'utilisateur d'accéder à la configuration du BIOS
Affichage de la fenêtre de redirection de la console	Lorsque le périphérique est démarré, il utilise le mode SOL (Serial over LAN) pour afficher une fenêtre de redirection de console
Redirection IDE : Redémarrage via disquette	Lorsque le périphérique est démarré, il est amorcé via un lecteur de disquette ou une image qui est spécifiée (les fichiers image de disquette doivent utiliser l'extension .img ; voir la remarque ci-dessous)
Redirection IDE : Redémarrage via un CD/DVD	Lorsque le périphérique est démarré, il est amorcé via un lecteur de CD ou une image qui est spécifiée (les fichiers image de CD doivent utiliser l'extension .iso ; voir la remarque ci-dessous)
Redirection IDE : Redémarrage via un fichier image spécifié	Lorsque le périphérique est démarré, il est amorcé via un fichier image qui est spécifié (voir la remarque ci-dessous)

Pour utiliser les options d'alimentation Intel AMT

1. Cliquez deux fois sur le périphérique dans la liste **Tous les périphériques**.
2. Dans la console d'informations du serveur, cliquez sur **Options d'alimentation**.
3. Sélectionnez une commande d'alimentation. Si vous sélectionnez **Redémarrer**, sélectionnez une option de démarrage.
4. Cliquez sur **Envoyer** pour initialiser la commande.

Remarques sur l'utilisation des options de redirection IDE

Pour utiliser les options de redirection IDE, un démarrage via disquette ou via un fichier image de disquette et un démarrage via CD/DVD ou via un fichier image CD/DVD doivent être spécifiés. Les fichiers image de disquette doivent utiliser le format .img et les fichiers image de CD doivent utiliser le format .iso. Certains BIOS peuvent requérir qu'une image de CD soit présente sur le disque dur.

En général, Intel AMT se rappelle des derniers paramètres IDE-R, mais System Manager efface les paramètres après 45 secondes. Par conséquent, les démarrages ultérieurs ne redémarreront pas la fonction IDE-R. La session IDE-R sur un périphérique Intel AMT dure 6 heures ou jusqu'à ce que la console System Manager soit arrêtée. Toute opération IDE-R en cours après 6 heures sera interrompue.

Forçage d'une analyse de vulnérabilité et désactivation de l'accès réseau sur les ordinateurs Intel AMT

Lorsqu'un périphérique configuré avec Intel AMT est doté de l'agent LANDesk, l'agent inclut des fonctions qui aide à résoudre les problèmes causés par des logiciels malfaisants et d'autres problèmes qui vous empêchent d'accéder au périphérique.

Le service amtmon.exe est installé avec l'agent LANDesk. Lorsque ce service est exécuté sur un périphérique, vous pouvez forcer l'analyse de vulnérabilité lors du prochain redémarrage afin d'essayer d'identifier les logiciels malfaisants du périphérique. Si la communication avec le périphérique échoue, vous pouvez désactiver la connexion au réseau du périphérique même si le système d'exploitation ne fonctionne pas, comme lorsqu'un logiciel malfaisant désactive le système d'exploitation en utilisant tous les cycles du processeur. En désactivant la connexion au réseau, vous pouvez empêcher le périphérique d'envoyer des paquets non voulus dans le réseau.

Lorsque l'agent LANDesk est installé sur un périphérique Intel AMT, les options suivantes sont disponibles dans la page **Options Intel AMT** :

- **Connexion réseau du système d'exploitation :** cliquez sur **Désactiver** pour désactiver la pile de réseau de système d'exploitation et interrompre l'accès au réseau ; cliquez sur **Activer** pour activer l'accès au réseau de système d'exploitation si ce dernier a été désactivé.
- **Effectuer une analyse de vulnérabilité après le redémarrage :** force l'exécution du scanner de vulnérabilité la prochaine fois que le périphérique redémarre.

Lorsqu'un périphérique ne répond pas si un logiciel malfaisant y est exécuté, il est recommandé de d'abord exécuter une analyse de vulnérabilité lors du prochain redémarrage pour essayer

d'identifier le problème. Si le problème persiste et si l'ordinateur infecte/attaque le réseau, ou si vous ne pouvez pas accéder au périphérique, vous pouvez désactiver la carte NIC de système d'exploitation.

Pour forcer une analyse de vulnérabilité après un redémarrage

1. Cliquez deux fois sur le périphérique dans la liste **Tous les périphériques**.
2. Dans la fenêtre de la console du périphérique, cliquez sur **Options d'Intel AMT**.
3. Cliquez sur **Options de configuration**, puis cliquez sur **Analyser**. Un message s'affiche sur le périphérique et indique qu'une analyse sera exécutée la prochaine fois qu'il redémarre.
4. Pour arrêter ou redémarrer le périphérique, utilisez les fonctions du gestionnaire de démarrage distant d'Intel AMT ci-dessus.

Pour désactiver ou activer la connexion réseau sur un périphérique sans réaction

1. Cliquez deux fois sur le périphérique dans la liste **Tous les périphériques**.
2. Dans la fenêtre de la console du périphérique, cliquez sur **Options d'Intel AMT**.
3. Pour désactiver la carte réseau du périphérique afin d'interrompre la communication avec les autres périphériques du réseau, cliquez sur **Désactiver**. Lorsque la connexion au réseau est désactivée, un message s'affiche sur le périphérique pour indiquer que la carte réseau a été désactivée.
4. Si le périphérique est sûr et peut à nouveau se connecter au réseau, cliquez sur **Activer**. Lorsque la connexion est restaurée, un message s'affiche sur le périphérique pour indiquer que la carte réseau est à nouveau activée.

Ouverture de l'écran de configuration d'Intel AMT

System Manager inclut un lien qui permet d'ouvrir l'écran de configuration d'Intel AMT. Il s'agit d'une interface fournie par Intel qui permet d'afficher l'état du périphérique, les informations de matériel, le journal d'événements Intel AMT, les paramètres de redémarrage distant et les paramètres de réseau. Elle permet également d'ajouter et de modifier des comptes d'utilisateur Intel AMT pour le périphérique. La fenêtre qui affiche cet écran est distincte de la console System Manager, et toute question à propos de l'utilisation de cette interface devrait être envoyée au support technique du fabricant du périphérique.

Pour ouvrir l'écran de configuration d'Intel AMT

1. Cliquez deux fois sur le périphérique dans la liste **Tous les périphériques**.
2. Dans la fenêtre de la console du périphérique, cliquez sur **Options d'Intel AMT**.
3. Cliquez sur **Console Intel AMT**, puis cliquez sur **Lancer la console Web d'Intel AMT**.

Administration basée sur les rôles

Présentation de l'administration basée sur les rôles

Utilisez l'administration basée sur les rôles pour configurer l'accès utilisateur aux outils du produit et aux autres périphériques en fonction de leur rôle administratif dans le système 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.

Les administrateurs (utilisateurs dotés du droit Administrateur) peuvent accéder aux outils de l'administration basée sur les rôles en cliquant sur **Utilisateurs** dans le volet de navigation de gauche.

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 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 service ou bureau unique. Ou bien, l'accès peut être limité à une plate-forme donnée, un type de processeur ou tout autre attribut de matériel ou de logiciel de périphérique. Grâce à l'administration basée sur les rôle, vous pouvez décider du nombre de rôles différents à créer, des utilisateurs pouvant agir dans ces rôles et de l'étendue de leur portée de périphériques.

Exemples de rôles administratifs

Le tableau ci-dessous répertorie certains des rôles administratifs possibles que vous pouvez souhaiter mettre en œuvre, les tâches courantes que l'utilisateur peut effectuer et les droits requis par cet utilisateur pour accomplir ce rôle.

Rôle	Tâches	Droits requis
Administrateur	Configuration des serveurs principaux, gestion d'utilisateurs, intégration d'autres produits d'entreprise, etc. (Bien sûr, les administrateurs dotés de droits complets peuvent effectuer toute tâche de gestion.)	(tous les droits implicites)
Gestionnaire de parc	Découverte de périphériques, configuration de périphériques, exécution du scanner d'inventaire, activation du suivi d'historique d'inventaire, etc.	Découverte de périphériques, distribution de logiciel et gestion de

Rôle	Tâches	Droits requis
		requêtes publiques
Gestionnaire de rapports	Exécution de rapports prédéfinis, impression de rapports, etc.	Rapports (requis pour tous les rapports)

Ce sont uniquement des exemples de rôle. L'administration basée sur les rôles est suffisamment souple pour vous permettre de créer autant de rôles personnalisés que vous le souhaitez. Vous pouvez attribuer les mêmes droits à différents utilisateurs mais restreindre leur accès à un ensemble limité de périphériques à l'aide d'une portée étroite. Même un administrateur peut être restreint par une portée, en faisant essentiellement de celui-ci un administrateur sur une région géographique ou un type de périphérique géré spécifique. La manière dont vous tirez parti de l'administration basée sur les rôles dépend des ressources de réseau et de personnel, ainsi que de vos besoins particuliers.

Pour mettre en œuvre l'administration basée sur les rôles, il suffit de désigner des utilisateurs Windows locaux actuels ou d'en créer et d'en ajouter de nouveaux, comme utilisateurs du produit, d'ajouter les utilisateurs au groupe d'utilisateurs Management Suite, puis de leur attribuer les droits nécessaires (sur les fonctions du produit) et une portée (sur les périphériques gérés). Suivez les procédures ci-dessous :

Présentation des droits

Les droits offrent accès à des outils et fonctions spécifiques. Les utilisateurs doivent disposer du ou des droits nécessaires pour réaliser les tâches correspondantes. Par exemple, afin de contrôler à distance des périphériques dans leur portée, un utilisateur doit posséder le droit de contrôle distant. Si plusieurs produits de gestion LANDesk sont installés, vous pouvez assigner des droits aux utilisateurs à partir de n'importe quelle console.

Lorsqu'un droit n'est pas octroyé à un utilisateur, il ne voit pas les outils associés à ce droit dans la console du produit. Par exemple, si un utilisateur ne reçoit pas le droit de rapports, l'élément de rapport ne s'affiche pas dans le volet de navigation de gauche. Le tableau ci-dessous spécifie les droits requis pour qu'un utilisateur affiche l'outil.

Outil	Les droits requis pour l'affichage dans le volet de navigation de gauche
Mes périphériques	Console Web de base
Configuration d'agent	Administrateur
Alerte	Alerte et surveillance
Découverte de périphériques	Découverte de périphériques

Outil	Les droits requis pour l'affichage dans le volet de navigation de gauche
Surveillance	Alerte et surveillance
Requêtes	Console Web de base, Gestion de requêtes publiques, Rapports
Rapports	Rapports, Gestion des correctifs
Tâches planifiées	Découverte de périphérique
Scripts	Gestion des correctifs
Utilisateurs	Administrateur
Mises à jour de logiciel	Gestion des correctifs
Préférences	Console Web de base
Configuration du matériel	Administrateur

Pour en savoir plus sur chaque droit du produit et la manière dont les droits peuvent être utilisés pour créer des rôles administratifs, reportez-vous aux descriptions ci-dessous.

La portée contrôle l'accès aux périphériques
Lors de l'utilisation des fonctions autorisées par ces droits, les utilisateurs seront toujours limités par leur portée (les périphériques qu'ils peuvent voir et manipuler).

Administrateur

L'administrateur fournit un accès complet à tous les outils du produit (toutefois, l'utilisation de ces outils est limitée aux périphériques inclus dans la portée de l'administrateur).

Il s'agit du droit par défaut pour tout utilisateur nouvellement ajouté, à moins que vous ne modifiez les paramètres de l'utilisateur modèle par défaut.

Le droit Administrateur permet aux utilisateurs d'effectuer les opérations suivantes :

- Afficher et accéder à l'outil **Utilisateurs** dans le volet de navigation de gauche.
- Afficher l'attribution de licences de produits dans l'option **Préférences** du volet de navigation de gauche.

- Exécuter toutes les tâches du produit autorisées par les autres droits répertoriés ci-dessous.

Il est déconseillé de supprimer l'Administrateur. Si vous êtes le dernier administrateur à vous connecter à une console LDSM, que vous entrez dans Windows Computer Management et que vous supprimez l'Administrateur dans le groupe Management Suite, vous rencontrerez des problèmes lorsque vous entrez de nouveau dans la console. Vous resterez connecté en tant qu'Administrateur pendant environ 20 minutes (délai d'attente de session par défaut) mais lorsque vous démarrerez une action ou que vous actualiserez le navigateur de la console (touche F5) dans lequel vous êtes connecté en tant qu'Administrateur, tous les droits appartenant uniquement à l'Administrateur ne seront plus disponibles. Vous ne devez en aucun cas supprimer le dernier Administrateur.

Remarque sur les droits et les outils
Le droit d'administrateur est exclusivement associé à l'outil **Utilisateurs**. Si un utilisateur ne dispose pas du droit d'administrateur, cet outil ne s'affichera pas dans la console.

Tous les outils présents dans la console du produit sont associés à un droit (comme indiqué ci-dessous).

Découverte de périphériques

Le droit Découverte de périphériques permet aux utilisateurs d'effectuer ce qui suit :

- Trouver sur le réseau des périphériques n'ayant pas soumis d'analyse d'inventaire à la base de données principale du produit de plusieurs manières, telles qu'une analyse de réseau, la découverte de l'agent de gestion standard et la découverte IPMI
- Planifier des découvertes périodiques
- Déplacer des périphériques de la liste Découverts à la liste Gérés

Gestion de requêtes publiques

Le droit Gestion de requêtes publiques permet aux utilisateurs d'effectuer ce qui suit :

- Créer des requêtes disponibles à tous les utilisateurs
- Créer ou supprimer des requêtes publiques
- Modifier les requêtes publiques existantes

Rapports

Le droit de rapports permet aux utilisateurs d'effectuer ce qui suit :

- Affichage et utilisation de l'outil **Rapports** dans le volet de navigation de gauche.
- Exécution de rapports prédéfinis

Gestion des correctifs

Le droit Gestion des correctifs est spécifique à la fonction d'analyse de vulnérabilités. Pour plus d'informations, reportez-vous à la section "Utilisation des outils de la console".

Console Web de base

Le droit Console Web de base permet aux utilisateurs d'utiliser les fonctions associées au droit. Les fonctions sont répertoriées ci-dessous, y compris toutes les exceptions de la fonction.

- **Mes périphériques** (le droit n'autorise pas la mise à jour des groupes publics ou la suppression des périphériques sous l'onglet **Actions**)
- Modifier les préférences (mais pas les attributs personnalisés)

Alerte et surveillance

Le droit Alerte et surveillance permet aux utilisateurs d'effectuer ce qui suit :

- Surveillance de la performance de plusieurs composants de systèmes d'exploitation et de systèmes, tels que des lecteurs, processeurs, mémoires, processus, octets/sec transférés par le serveur Web du système, etc.
- Suivi de l'intégrité exacte de tous les périphériques gérés
- Personnalisation des alertes à envoyer par niveau de gravité (Critique, Avertissement, Informationnel, OK, Inconnu) ou seuil (par exemple, si le pourcentage de disque dur utilisé dépasse 90% de la capacité du disque dur)
- Sélection d'une action à suivre si une alerte dépasse un seuil (en ajoutant des informations au fichier journal, envoyant un avertissement par courrier électronique, exécutant un programme sur le serveur principal ou un périphérique individuel ou envoyant une trappe SNMP à une console de gestion SNMP sur le réseau)

Ajout des utilisateurs du produit

Les utilisateurs du produit sont des utilisateurs qui peuvent se connecter à la console du produit et réaliser des tâches spécifiques pour des périphériques donnés sur le réseau.

Les utilisateurs du produit ne sont pas créés dans la console. Ils s'affichent dans l'onglet **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 qui résident actuellement dans le groupe LANDesk Management Suite sur le serveur principal.

Le groupe **Utilisateurs** contient deux utilisateurs par défaut :

- **Utilisateur Modèle par défaut :** Cet utilisateur est en fait un modèle de propriétés d'utilisateur (droits et portée) qui est employé pour configurer de nouveaux utilisateurs lors de leur ajout au groupe LANDesk Management Suite. En d'autres termes, lorsque vous ajoutez un utilisateur à ce groupe dans l'environnement Windows, l'utilisateur hérite des droits et de la portée actuellement définis dans les propriétés d'utilisateur Modèle par défaut. Si tous les droits de l'utilisateur Modèle par défaut et la portée Toutes les machines par défaut sont sélectionnés, 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.

  Pour modifier les paramètres de propriétés de l'utilisateur modèle par défaut, sélectionnez-le avec le bouton droit de la souris puis cliquez sur **Modifier les droits**. Par exemple, si vous souhaitez ajouter un nombre important d'utilisateurs en une opération sans 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.

- **Administrateur par défaut :** Utilisateur administratif connecté au serveur lors de l'installation du serveur principal de ce produit.

Lorsque vous ajoutez un utilisateur au groupe LANDesk Management Suite sous Windows, il est automatiquement lu dans le groupe **Tous les utilisateurs** de la fenêtre **Utilisateurs**, et hérite des mêmes droits et portée que l'utilisateur Modèle par défaut actuel. Le nom, la portée et les droits de l'utilisateur sont affichés.

Si vous supprimez un utilisateur du groupe LANDesk Management Suite dans l'environnement d'utilisateurs Windows, l'utilisateur n'est plus actif et peut être supprimé du groupe **Utilisateurs**. Le compte de l'utilisateur existe toujours sur le serveur 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 perdre de données et que vous puissiez également copier des données vers d'autres utilisateurs.

Pour actualiser la liste **Utilisateurs** afin d'afficher les utilisateurs dernièrement ajoutés, cliquez sur **Utilisateurs** puis sur le bouton **Actualiser** de votre navigateur.

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

Vous pouvez maintenant attribuer des droits et une portée aux utilisateurs du produit.

Création de portées

Une portée définit les périphériques qui peuvent être visualisés et gérés par un utilisateur de produit. Si plusieurs produits de gestion LANDesk sont installés, les portées peuvent être attribuées aux utilisateurs depuis n'importe quelle console et sont efficaces dans toutes les consoles.

Une portée peut avoir la taille de votre choix, regroupant tous les périphériques gérés et analysés dans une base de données principale, juste un périphérique unique ou aucun périphérique. Cette souplesse, combinée avec un accès modulaire aux outils, est ce qui permet de faire de l'administration basée sur les rôles une fonction de gestion si flexible.

Portées par défaut

L'administration basée sur les rôles inclut deux portées par défaut. Ces deux portées prédéfinies peuvent être utiles lors de la configuration des propriétés de l'utilisateur modèle par défaut.

- **(Option par défaut) Portée Aucune machine :** Exclut tous les périphériques dans la base de données.
- **(Option par défaut) Portée Toutes les machines :** Inclut tous les périphériques dans la base de données.

Vous ne pouvez pas modifier ou supprimer les portées par défaut.

Portées personnalisées

Vous pouvez créer les types de portées personnalisées suivants et les attribuer aux utilisateurs :

- **Portée basée sur une requête :** Contrôle l'accès aux seuls périphériques qui répondent à une recherche de requête personnalisée. Pour définir une portée, vous pouvez sélectionner une requête existante ou en créer de nouvelles à partir de la boîte de dialogue **Requête** . Pour plus d'informations sur la création de requêtes, reportez-vous à la section "Création de requêtes de base de données".
- **Portée basée sur un groupe :** Contrôle l'accès uniquement aux périphériques situés dans le groupe sélectionné. Pour définir une portée, vous pouvez sélectionner des groupes à partir de la boîte de dialogue **Propriétés de la portée de groupe**.

Vous pouvez attribuer plusieurs portées à vos utilisateurs. Lorsque plusieurs portées sont attribuées à un utilisateur, la portée effective cumulative (par exemple, la plage complète de périphériques qui peuvent être accédés et gérés à la suite de la combinaison de portées attribuées) correspond à un composite simple.

Vous pouvez personnaliser une portée effective d'utilisateur en ajoutant et supprimant des portées à tout moment. Tous les types de portées peuvent être utilisés simultanément.

Pour créer une portée

1. Dans le volet de navigation de gauche, cliquez sur **Utilisateurs**.
2. Dans l'onglet **Portée**, cliquez sur **Nouvelle portée de requête** ou le bouton **Nouvelle portée de groupe** de la barre d'outils.
3. Entrez un nom pour la nouvelle portée.
4. Si vous avez sélectionné une portée basée sur une requête, sélectionnez une requête existante, ou cliquez sur **Définir** pour créer une nouvelle requête. Cliquez sur **OK**.
5. Si vous avez sélectionné une portée basée sur un groupe, sélectionnez un groupe, puis cliquez sur **OK**.
6. Cliquez sur **OK** pour enregistrer la portée et fermer la boîte de dialogue.

Attribution de droits et d'une portée aux utilisateurs

- Boîte de dialogue Droits/Portée d'utilisateur
- Boîte de dialogue Paramètres du contrôle distant

Une fois que vous avez ajouté des utilisateurs de produit, avez assimilé les droits et la manière dont ils contrôlent l'accès aux outils et fonctions, et créé des portées de périphériques pour autoriser ou restreindre l'accès aux périphériques gérés, l'étape suivante de l'établissement de l'administration basée sur les rôles consiste à attribuer les droits appropriés et une portée à chaque utilisateur.

Vous pouvez à tout moment modifier les droits d'un utilisateur et sa portée.

Si vous modifiez les droits ou la portée d'un utilisateur, ces modifications ne sont prises en charge que la prochaine fois que l'utilisateur se connecte à la console.

Pour attribuer des droits et une portée à un utilisateur

1. Dans le volet de navigation de gauche, cliquez sur **Utilisateurs**.
2. Développez la liste des utilisateurs pour afficher tous les utilisateurs actuellement membres du groupe LANDesk Management Suite dans l'environnement Windows NT du serveur principal.

   Cette liste affiche les noms d'utilisateur et les droits attribués (une coche indique que le droit est activé).

3. Cliquez avec le bouton droit sur un utilisateur, puis cliquez sur **Modifier**.
4. Dans la boîte de dialogue **Droits/Portée d'utilisateur**, activez ou désactivez les droits suivant les besoins.
5. Cliquez sur l'onglet **Portée** et sélectionnez une portée dans la liste **Portées attribuées.**
6. Cliquez sur **Appliquer**.

Les nouveaux droits s'affichent en regard du nom de l'utilisateur dans la liste et prendront effet la prochaine fois que l'utilisateur se connectera au serveur principal.

Pour supprimer une portée

1. Dans le volet de navigation de gauche, cliquez sur **Utilisateurs**.
2. Dans l'onglet **Portée**, sélectionnez la portée à supprimer, puis cliquez sur **Supprimer**. Cliquez sur **OK**.

Faites attention lorsque vous supprimez des portées. Les utilisateurs attribués à ces portées auront accès à des droits précédemment interdits par la portée.

Boîte de dialogue Droits/Portées de l'utilisateur

Utilisez cette boîte de dialogue pour afficher et modifier les droits attribués et la portée d'un utilisateur. Ouvrez la boîte de dialogue en sélectionnant un utilisateur et en cliquant sur **Modifier**.

Onglet Droits : Répertorie les droits attribués à l'utilisateur.

- **Administrateur**
- **Découverte de périphériques**
- **Gestion de requêtes publiques**
- **Rapports**
- **Gestion de correctifs**
- **Console Web de base**
- **Alerte et surveillance**

Onglet Portée : Répertorie les portées assignées à l'utilisateur.

- **Portées assignées :** Indique les portées actuelles de l'utilisateur.

- **Ajouter :** Ouvre la boîte de dialogue **Ajouter la portée** qui permet de sélectionner une portée à ajouter à l'utilisateur.
- **Supprimer :** Supprime la portée sélectionnée.
- **Annuler :** Ferme la boîte de dialogue sans enregistrer les modifications.

Découverte de périphériques

Utilisation de la découverte de périphérique

La découverte de périphérique recherche sur le réseau les périphériques qui ne sont pas dotés d'agents du serveur principal de découverte et qui n'ont pas soumis une analyse d'inventaire à la même base de données principale. La découverte de périphérique dispose de plusieurs méthodes pour découvrir des périphériques sur le réseau.

- **Analyse de réseau :** Recherche des ordinateurs via une scrutation ping ICMP. Il s'agit de la recherche la plus poussée mais elle peut prendre plus de temps (si Empreinte IP est utilisé). Vous pouvez limiter la recherche à des plages d'adresses IP et de sous-réseau spécifiées. Par défaut, cette option utilise NetBIOS pour rassembler des informations sur le périphérique. Vous pouvez également sélectionner la fonction d'empreinte IP qui permet de fournir le type de SE (dans la plupart des cas). L'option d'analyse du réseau offre également une option **Utiliser SNMP** qui permet d'utiliser SNMP pour les périphériques SNMP tels que certaines imprimantes.
- **Découverte CBA :** Recherche l'agent de gestion standard (anciennement agent à base commune (CBA) dans Management Suite) sur les ordinateurs. Cette option découvre les ordinateurs gérés par Server Manager, System Manager, etc. Sélectionnez l'option PDS2 pour découvrir les périphériques utilisant l'ancien agent PDS2 LANDesk. 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 Intelligent Platform Management Interface, qui permet d'accéder au Baseboard Management Controller (BMC) que le serveur soit sous tension ou pas ou indépendamment de l'état du système d'exploitation.
- **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 des périphériques dotés de Intel Active Management Technology (version 1), qui permet d'accéder à de nombreuses fonctions que le serveur soit sous tension ou pas, ou indépendamment de l'état du système d'exploitation.

La découverte de périphérique tente de découvrir des informations élémentaires sur chaque périphérique. Toutes les informations ci-dessous ne sont pas disponibles pour chaque périphérique.

- **Nom du nœud :** Nom du périphérique découvert, si disponible.
- **Adresse IP :** Adresse IP découverte.
- **Masque de sous-réseau :** Masque de sous-réseau découvert.
- **Catégorie :** Le groupe de découverte de périphérique auquel le périphérique appartient.
- **Nom du SE :** Description du système d'exploitation découvert, si disponible.

Lorsque la fonction de découverte de périphérique trouve un périphérique pour la première fois, elle inspecte la base de données principale pour déterminer si l'adresse IP et le nom de ce périphérique sont déjà dans la base de données dans la liste **Mes périphériques**. Un

périphérique dans la liste **Non gérés** sera redécouvert et génèrera potentiellement plus de données. En cas de correspondance, la découverte de périphérique ignore le périphérique. En cas d'absence de correspondance, elle ajoute le périphérique au tableau des périphériques **Non gérés**. Les périphériques de ce tableau n'utilisent pas de licence System Manager. Un périphérique est considéré être géré une fois qu'il envoie une analyse d'inventaire à la base de données principale. Une fois qu'un périphérique est placé dans le groupe **Tous les périphériques**, il ne s'affiche plus dans la liste **Périphériques découverts**.

Les périphériques IPMI doivent disposer d'un BMC (Contrôleur de gestion de la carte de base) qui est configuré pour être découvert comme périphérique IMPI et pour utiliser des fonctions IPMI complètes. Si le contrôleur BMC n'est pas configuré, le périphérique peut être découvert comme un ordinateur. Vous pouvez alors ajouter le périphérique à la liste des périphériques gérés et exécuter la fonction Configuration du matériel pour configurer le mot de passe BMC. Les fonctions IPMI du périphérique seront alors reconnues par ce produit. Notez que l'adresse IP du BMC n'est pas nécessairement identique à celle du SE. Par conséquent, elle ne pourra peut être pas effectuer un poussage d'agent direct vers l'adresse IP du BMC. Une redécouverte des IP standard peut être exigée pour qu'un agent standard soit poussé vers l'IP du BMC. L'IP du BMC devrait pouvoir accepter un poussage d'agent IP.

Pour que les périphériques dotés de Intel* AMT (version 1) soient découverts et reconnus comme étant des périphériques Intel AMT, ils doivent être configurés avec un nom d'utilisateur et mot de passe Intel AMT. Une fois le périphérique découvert, vous pouvez exécuter la fonction Configuration du matériel pour configurer les paramètres Intel AMT et approvisionner le périphérique en utilisant le mode Small Business ou le mode sécurisé Enterprise.

Pour automatiser la découverte de périphériques, vous pouvez planifier des découvertes afin qu'elles s'exécutent périodiquement. Par exemple, vous pouvez diviser le réseau en sous-réseaux et planifier une scrutation ping pour un sous-réseau différent chaque nuit. Pour toutes les découvertes, le serveur principal exécute la recherche.

Pour découvrir et gérer des périphériques sur le réseau, exécutez les tâches suivantes :

- Créer des configurations de découverte
- Planifier et exécuter une découverte
- Afficher les périphériques découverts
- Déplacer les périphériques découverts vers la liste **Mes périphériques**

Utilisation de la découverte de périphériques non gérés avec les périphériques dotés de pare-feux

Sachez que la découverte de périphériques non gérés ne peut généralement pas détecter des périphériques qui utilisent un pare-feu, comme le fait le Pare-feu Windows, à moins que vous ne configuriez manuellement le pare-feu. Vous devez ouvrir les ports suivants. Pour modifier ces paramètres, accédez au Pare-feu Windows via le Panneau de configuration de Windows.

Serveurs gérés :

- Partage de fichiers et d'imprimantes : TCP 139, 445 ; UDP 137, 138 (le mode Push ne fonctionne pas sans cette option)
- Distribution de logiciel : TCP 9595 (le mode Push ne fonctionne pas sans cette option)

- ICMP - Avancé : "Autoriser la requête d'écho entrante" (Ne peut pas être découvert si cette option n'est pas activée)

Serveur principal :

- Inventaire : 5007
- Contrôle distant : 9535

Création de configurations de découverte

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 **Empruntes 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 d'empruntes IP ralentit légèrement le processus d'identification.

  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. Pour plus d'informations, reportez-vous à la section Configuration des analyses 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 ciblée 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. Pour une présentation de IPMI, reportez-vous à la section Prise en charge IPMI.
- **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.

Pour modifier ou supprimer une configuration

- Dans l'onglet **Configurations de découverte**, sélectionnez la configuration de votre choix et cliquez sur **Modifier** ou **Supprimer**.

Configuration d'analyses SNMP

Les découvertes d'analyse réseau peuvent utiliser SNMP. Selon la configuration SNMP de votre réseau, vous devrez peut-être entrer des informations SNMP complémentaires dans la configuration de découverte. Cliquer sur **Configurer** à côté de l'option **SNMP** affiche la boîte de dialogue **Configuration SNMP** qui propose les options suivantes :

- **Tentatives :** Nombre de fois que la découverte de périphérique tente une connexion SNMP.
- **Attente de réponse en secondes :** Durée pendant laquelle la découverte de périphérique attend un réponse SNMP.
- **Port :** Le port auquel la découverte de périphérique doit envoyer les requêtes SNMP.
- **Nom de la communité :** Le nom de la communauté SNMP que la découverte de périphérique doit utiliser.
- **Configurer SNMP V3 :** La découverte de périphérique prend également en charge SNMP V3. Cliquez sur ce bouton pour configurer les options SNMP V3 dans la boîte de dialogue **Configuration SNMP V3**.

La boîte de dialogue **Configuration SNMP V3** propose les options suivantes :

- **Nom d'utilisateur :** Le nom d'utilisateur que la découverte de périphérique doit utiliser pour s'authentifier auprès du service SNMP distant.
- **Mot de passe :** Le mot de passe pour le service SNMP distant.
- **Type d'authentification :** Le type d'authentification que SNMP utilise. Il peut s'agir de **MD5**, **SHA** ou de **Aucun**.
- **Type de confidentialité :** La méthode de codage que le service SNMP utilise. Il peut s'agir de **DES**, **AES128** ou de **Aucun**.
- **Mot de passe de confidentialité :** Le mot de passe à utiliser avec le type de confidentialité spécifié. Non disponible si vous avez sélectionné le type de confidentialité **Aucun**.

Planification et exécution d'une découverte

Utilisez le bouton **Planifier** dans l'onglet **Configuration de découverte** pour afficher la boîte de dialogue **Tâche planifiée**. Utilisez cette boîte de dialogue pour planifier l'exécution des configurations de découverte. L'exécution de la configuration de découverte peut être immédiate, ultérieure, récurrente, ou unique.

Les tâches de découverte peuvent être replanifiées ou supprimées depuis l'onglet **Tâches de découverte**. Une fois une découverte planifiée, passez à l'onglet **Tâches de découverte** pour afficher l'état de la découverte. Vous pouvez également accéder à l'état de la tâche de découverte à partir de l'outil **Tâches planifiées**. Une fois une tâche de découverte terminée, les nouveaux périphériques qui ne sont pas déjà présents dans la base de données seront ajoutés aux catégories de périphériques découverts.

La boîte de dialogue **Tâche planifiée** comporte les options suivantes.

- **Afficher dans les tâches courantes :** Permet aux autres utilisateurs d'afficher la tâche. Lorsqu'un autre utilisateur modifie ou exécute la tâche, l'utilisateur devient le propriétaire d'une instance de la tâche.
- **Propriétaire :** Le propriétaire de la tâche.
- **Laisser non planifié :** (valeur par défaut) Conserve la tâche dans la liste des tâches pour une planification 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 :
    - **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.
    - **Heure :** L'heure de démarrage de la tâche.
    - **Répéter chaque :** Pour que la tâche soit récurrente, sélectionnez une fréquence (tous les jours, toutes les semaines ou tous les mois). Si vous sélectionnez Mois 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 découverte

1. Dans le volet de navigation de gauche, cliquez sur **Découverte de périphérique**.
2. Dans l'onglet **Configurations de découverte**, sélectionnez la configuration de votre choix et cliquez sur **Planifier**. Configurez la planification de découverte. Une fois terminé, cliquez sur **Enregistrer**.
3. Surveillez la progression de la découverte dans l'onglet **Tâches de découverte**.
4. Une fois la découverte terminée, tous les résultats s'affichent dans le volet supérieur **Périphériques découverts**. Si vous cliquez deux fois sur la tâche de découverte, la quantité et le pourcentage de périphérique sont à zéro car ces valeurs sont liées aux périphériques ciblés, et les tâches de découverte ne possèdent aucune cible.

L'onglet **Tâches de découverte** affiche l'état de la tâche de découverte. L'état inclut ce qui suit :

- Le nom de la configuration de découverte.
- L'état de la tâche, qui peut correspondre à Traitement en cours, Tout terminé, Rien de terminé ou Échec.
- La dernière exécution de la tâche.
- Le type d'exécution.

Pour supprimer ou replanifier une découverte

Si vous souhaitez supprimer une tâche de la liste, qu'elle ait été exécutée ou pas, sélectionnez la tâche et cliquez sur **Supprimer**. Si une tâche n'ayant pas encore été exécutée ou récurrente est supprimée, il est impossible de l'exécuter ultérieurement.

Pour également planifier la réexécution d'une tâche de découverte de la liste ou la planifier pour un autre moment, cliquez sur la tâche puis sur **Modifier** et sélectionnez **Planifier** puis réinitialisez la planification. Pour réexécuter immédiatement la tâche, sélectionnez-la puis cliquez sur **Démarrer maintenant**.

Pour afficher un état de tâche de découverte

1. Dans le volet de navigation de gauche, cliquez sur **Périphériques découverts**.
2. Cliquez sur l'onglet **Tâches de découverte** ou cliquez sur **Actualiser** sur la barre d'outils du panneau.

Affichage des périphériques découverts

Affichez tous les périphériques découverts dans le volet supérieur **Découverte de périphérique**. Ce volet affiche les résultats de toutes les découvertes exécutées. Lorsque vous lancez une nouvelle découverte, tous les périphériques trouvés sont ajoutés dans cette liste.

Lorsque la fonction de découverte de périphérique trouve un périphérique, elle essaie d'identifier le type du périphérique afin de pouvoir l'ajouter à une des catégories suivantes :

- **Châssis :** Contient des modules de gestion de châssis (CMM) de serveur Blade.
- **Ordinateurs :** Contient des ordinateurs. Les systèmes Linux peuvent être indiqués comme étant des systèmes Unix dans la colonne **Nom du SE**.
- **Infrastructure :** Contient des routeurs et d'autres matériels de réseau.
- **Intel AMT :** Contient des périphériques qui prennent en charge Intel* Active Management Technology.
- **IPMI :** Contient des périphérique dotés de IPMI.
- **Autre :** Contient des périphériques non identifiés.
- **Imprimantes :** Contient des imprimantes.

Ces catégories vous aident à organiser la liste **Découverte de périphérique** afin de pouvoir trouver plus facilement les périphériques souhaités. Vous pouvez trier les listes de périphériques par intitulé de colonne lorsque vous cliquez sur un intitulé. La fonction Découverte de périphérique peut ne pas catégoriser les périphériques correctement à chaque fois. Pour déplacer aisément des périphériques identifiés de manière incorrecte vers le groupe approprié, cliquez avec le bouton droit sur le périphérique à déplacer, cliquez sur **Déplacer**, sélectionnez la catégorie correcte puis cliquez sur **OK.**

Parfois, le serveur principal est répertorié deux fois. Ceci se produit lorsque vous trouvez le même ordinateur par des mécanismes de découverte différents (par exemple, CBA, IPMI, CMM, PDS1 et PDS2) et les informations de l'ordinateur sont ajoutées à la base de données pour ce mécanisme.

Une fois que des agents sont déployés vers un périphérique découvert et que le périphérique envoie une analyse d'inventaire sur le serveur principal, le périphérique découvert est supprimé de la liste des périphériques découverts.

Filtrage de la liste de périphériques

Trouvez les périphériques qui correspondent aux critères de recherche que vous spécifiez à l'aide du champ **Filtrer par** de la barre d'outils. Vous pouvez filtrer par Nom de nœud, Adresse IP, Masque de sous-réseau, Catégorie ou Nom de SE. Lorsque vous utilisez un filtre, les périphériques sont triés alphabétiquement par l'attribut utilisé pour filtrer.

Pour filtrer la liste de périphériques

1. Dans le volet de navigation de gauche, cliquez sur **Découverte de périphérique**.
2. Dans l'arborescence **Non gérés**, cliquez sur le groupe à filtrer.
3. Dans **Filtrer par**, cliquez sur l'attribut que vous souhaitez utiliser pour filtrer. (Si **Filtrer par** ne s'affiche pas, cliquez sur **>>** pour le développer.)
4. Dans la zone de texte en regard de l'attribut, entrez le texte à utiliser pour filtrer.
5. Cliquez sur **Rechercher**.

Ajout de catégories

Vous pouvez créer des catégories de périphériques pour grouper les périphériques non gérés. Si vous déplacez un périphérique vers une autre catégorie, il s'affiche à nouveau dans ce groupe si la découverte de périphériques le détecte plus tard. En déplaçant les périphériques qui ne seront pas gérés par la console dans d'autres groupes, vous pouvez plus facilement visualiser les nouveaux périphériques dans le groupe **Ordinateurs**.

Si vous supprimez un groupe qui contient des périphériques, la découverte de périphériques déplace ces derniers vers le groupe **Autre**.

Pour ajouter une catégorie de périphérique

1. Dans la vue **Découverte de périphériques**, cliquez sur **Ajouter une catégorie**.
2. Entrez un nom de groupe dans la zone **Nom de catégorie**, puis cliquez sur **OK**.
3. Pour supprimer une catégorie que vous avez ajoutée, sélectionnez-la, cliquez sur **Supprimer la catégorie**, puis cliquez sur **OK** pour confirmer la suppression.

Déplacement des périphériques découverts vers la liste Mes périphériques

Une fois les périphériques découverts, vous pouvez les placer dans la liste **Mes périphériques**. Durant le déplacement des périphériques, leurs informations sont ajoutées à la base de données. Une fois les informations placées dans la base de données, vous pouvez déployer la configuration d'agent, exécuter des requêtes, créer des rapports et effectuer plusieurs autres tâches de gestion.

Pour les périphériques pouvant être gérés hors bande (ceux dotés des fonctions IPMI, Intel AMT, ou DRAC), vous avez la possibilité de gérer les périphériques sans déployer un agent. Dans ce cas, les informations du périphérique sont enregistrées dans la base de données et le BMC du périphérique est configuré pour utiliser les fonctions de gestion autorisées par le matériel de gestion hors bande du périphérique.

Pour déplacer les périphériques découverts vers la liste Mes périphériques

1. Dans la vue **Découverte de périphérique**, sélectionnez le périphérique à placer dans la liste **Mes périphériques**. Vous pouvez sélectionner plusieurs périphériques en utilisant MAJ+cliquer ou CTRL+cliquer.

2. Cliquez sur le bouton **Cible**. Les périphériques sélectionnés sont alors répertoriés dans l'onglet **Liste de cibles**.
3. Cliquez sur l'onglet **Gérer**.
4. Sélectionnez **Déplacer les périphériques ciblés**.
5. Si les périphériques peuvent être gérés hors bande et si vous ne souhaitez pas y déployer un agent de gestion, sélectionnez **Gérer les périphériques activés hors bande sans agent**.
6. Cliquer sur **Déplacer**.

Les périphériques sont supprimés de la liste des périphériques non gérés et s'affichent dans la liste **Mes périphériques**.

Si vous sélectionnez l'option de gestion hors bande, vous pouvez afficher l'état du déplacement en cliquant sur l'onglet **Statut du déplacement** situé dans le volet inférieur. Toutes les erreurs de configuration sont notées ici. Avant de déplacer un périphérique doté de IPM vers la liste **Mes périphériques**, vous devez fournir les références d'authentification BMC appropriées dans l'utilitaire Configurations des services pour que le serveur principal s'authentifie sans problème au périphérique.

Lorsque vous déplacez un module de gestion de châssis (CMM) vers la liste **Mes périphériques**, il s'affiche dans la liste **Tous les périphériques** et en tant que groupe dans la liste **Groupes publics**. Les détails du groupe affichent le CMM et une liste des baies disponibles dans le châssis avec les noms des serveurs Blade dans les baies. Les serveurs Blade sont également détectés et gérés comme des serveurs individuels.

Découverte des périphériques Intel* AMT

System Manager permet de découvrir les périphériques configurés avec la version 1 d'Intel* Active Management Technology (Intel* AMT). Les périphériques peuvent être découverts comme étant des périphériques Intel AMT uniquement si vous avez accédé à l'écran de configuration d'Intel AMT sur le périphérique et remplacé le mot de passe par défaut du fabricant par un mot de passe sécurisé. (Consultez la documentation du fabricant pour obtenir plus d'informations pour accéder à l'écran de configuration d'Intel AMT.) Si vous ne complétez pas ces étapes, les périphériques sont découverts mais ils ne sont pas identifiés comme étant des périphériques Intel AMT et les informations de récapitulatif d'inventaire affichées peuvent ne pas correspondre.

Les périphériques dotés de la version 2 d'Intel AMT ne sont pas découverts par l'intermédiaire de ce processus. Une fois les ID d'approvisionnement entrées dans l'écran de configuration d'Intel AMT avec l'adresse IP du serveur principal, le périphérique est automatiquement découvert. Pour plus d'informations sur l'utilisation de la version 2, reportez-vous à la section Configuration des périphériques Intel AMT.

Pour découvrir les périphériques Intel AMT

1. Dans le volet de navigation de gauche, cliquez sur **Découverte de périphérique**.
2. Cliquez sur **Nouveau** pour créer une nouvelle configuration et donnez-lui un nom. Ou cliquez sur une configuration existante et cliquez sur **Modifier** pour la modifier.
3. Cochez l'option **Découvrir les périphériques Intel AMT**.

4. Entrez des adresses IP de début et de fin pour analyser une plage d'adresses et entrez un masque de sous-réseau.
5. Cliquez sur **Ajouter**, puis cliquez sur **OK**.
6. Sélectionnez la configuration et cliquez sur **Planifier**. Réglez les options de planification, ou cliquez sur **Démarrer maintenant**, puis cliquez sur **Enregistrer**.
7. Pour afficher la progression de l'analyse, cliquez sur l'onglet **Tâches de découverte**.

Les périphériques dotés d'AMT s'affichent dans un dossier appelé **Intel AMT**. A partir de ce dossier, vous pouvez sélectionner le périphérique et le déplacer vers la liste de périphériques gérés.

Pour ajouter le périphérique à la base de données principale afin de le gérer, le nom d'utilisateur et le mot de passe du périphérique doivent correspondre au nom d'utilisateur et mot de passe enregistrés dans l'utilitaire Configuration des services, ce qui permet à System Manager de s'authentifer au périphérique. Lorsque vous enregistrez la configuration du mot de passe dans l'utilitaire Configuration des services, les informations sont stockées dans la base de données principale afin que System Manager puisse s'authentifier aux périphériques Intel AMT.

Si vous disposez de périphériques AMT qui utilisent des références d'authentification différentes, vous devrez vous assurez que les références de chaque périphérique correspondent à celles de l'utilitaire Configuration des services avant de les gérer.

Lorsqu'un périphérique Intel AMT est découvert et placé dans la liste **Mes périphériques**, il est automatiquement approvisionné selon le mode sélectionné dans l'utilitaire Configuration des services. Le mode Small Business offre une gestion de base sans des services d'infrastructure de réseau et n'est pas sécurisé, alors que le mode Enterprise est approprié pour des grandes sociétés et offre une sécurité basée sur les services de réseau, tels que DHCP, DNS et le service d'autorité de certification TLS.

Si votre serveur principal utilise un serveur de proxy, celui-ci doit prendre en charge Digest Access Authentication pour pouvoir découvrir les périphériques Intel AMT.

Pour configurer le mot de passe d'Intel AMT

1. Cliquez sur **Démarrer | Programmes | LANDesk | Configuration des services**. Cliquez sur l'onglet **Configuration Intel AMT**.
2. Entrez le nom d'utilisateur et le mot de passe 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) afin de gérer les périphériques Intel AMT.
3. Pour modifier le nom d'utilisateur et le mot de passe, renseignez la section **Nouveau mot de passe d'Intel AMT**.
4. Sélectionnez le mode (**Small Business** ou **Enterprise**) à utiliser pour approvisionner les périphériques lorsque vous les ajoutez à la base de données principale pour les gérer.
5. Cliquez sur **OK**. Cette modification est appliquée lorsque la configuration du client est exécutée.

Pour déplacer les périphériques Intel AMT découverts dans la liste des périphériques gérés

1. Cliquez sur un ou plusieurs noms de périphérique dans la liste des périphériques non gérés.
2. Cliquez sur le bouton **Cibler** de la barre d'outils.
3. Cliquez sur le bouton **Gérer** dans le volet inférieur, sélectionnez **Déplacer les périphériques ciblés**, puis cliquez sur **Déplacer**.

   Si tous les périphériques que vous voulez gérer s'affichent dans la liste, sélectionnez-les, cliquez sur le bouton **Gérer** du volet inférieur, sélectionnez **Déplacer les périphériques sélectionnés**, puis cliquez sur **Déplacer**.

Le périphérique est supprimé de la liste des périphériques non gérés et apparaît dans la liste **Tous les périphériques**. Notez que lorsque vous déplacez les périphériques dans la liste **Mes périphériques**, l'approvisionnement Intel AMT s'exécute via un processus distinct en arrière-plan. Durant ce processus, vous pouvez continuer vos autres tâches de gestion ou de découverte.

Pour plus d'informations sur la gestion des périphériques Intel AMT, reportez-vous aux sections Gestion des périphériques Intel* AMT et Prise en charge d'Intel* AMT.

Installation et configuration d'un agent de périphérique

Présentation de l'installation et de la configuration d'un agent

Pour entièrement gérer les périphériques avec la console, vous devez installer des agents de gestion sur ces périphériques. Vous pouvez installer la configuration d'agent par défaut (qui installe tous les agents du produit) ou en installer une personnalisée sur vos périphériques. Veuillez noter que l'installation de System Manager n'installe pas automatiquement les agents sur le serveur principal. Ceux-ci doivent être installés par vous-même puis le serveur principal doit être redémarré manuellement. Pour recevoir des alertes de santé, la configuration d'agent doit inclure l'agent de surveillance.

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

- Déploiement d'agents. 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.
- Installation d'agents avec un paquet d'installation. Créez 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.
- Tirage de l'agent. Assignez une unité au partage ldlogon du serveur principal (//*nom_serveur*/ldlogon) et exécutez SERVERCONFIG.EXE.
- Manuellement sur un périphérique doté d'un lecteur USB portable (voir Installation d'agents avec un paquet d'installation)

Le chapitre Découverte de périphérique du *Guide d'utilisation* est une autre source d'informations sur l'installation et la configuration d'un agent.

Remarque : Vous pouvez définir une configuration de périphérique comme configuration par défaut en sélectionnant la configuration dans la page **Configuration d'agent** et en cliquant sur **Définir comme valeur par défaut**. Une configuration BMC IPMI uniquement ne peut pas être définie comme configuration par défaut. Les configurations par défaut ne peuvent pas être supprimées.

Pour les systèmes Windows, les paramètres de port suivants requierent une configuration manuelle du pare-feu pour que tout le produit fonctionne. Pour modifier ces paramètres, accédez au Pare-feu Windows via le Panneau de configuration de Windows.

Serveurs gérés :

- Partage de fichiers et d'imprimantes : TCP 139, 445 ; UDP 137, 138 (le mode Push ne fonctionne pas sans cette option)
- Distribution de logiciel : TCP 9595 (le mode Push ne fonctionne pas sans cette option)

- Options avancées : ICMP - "Autoriser la requête d'écho entrante" (Ne peut pas être découvert si cette option n'est pas activée.)

Serveur principal :

- Inventaire : 5007
- Contrôle distant : 9535

Pour ce faire, cliquez sur **Démarrer** | **Panneau de configuration** | **Sécurité**.

Mise à jour des agents existants

Vous pouvez pousser des configurations d'agent vers vos périphériques, même si les agents de gestion standard ou Contrôle distant ne sont pas encore présents. Pour plus d'informations sur la configuration des références d'authentification, voir Configuration des services et des références d'authentification dans le *Guide d'utilisation*.

Une fois un paquet d'agents installé, l'installation supprime l'installation précédente et installe la nouvelle. Vous pouvez désinstaller un agent en créant un nouveau paquet d'agents qui n'inclut pas l'agent que vous souhaitez supprimer.

Désinstallation des agents

Si vous devez désinstaller les agents des serveurs, suivez la procédure suivante :

Avertissement : Par défaut, Uninstallwinclient.exe redémarre le périphérique après la désinstallation des agents à moins que vous n'utilisiez l'option **/noreboot** à la ligne de commande. Pour terminer l'installation, il est nécessaire de redémarrer. Si un redémarrage est initialisé, le serveur redémarre sans avertissement et toutes les autres applications sont obligées de s'arrêter. L'option /noreboot permet au serveur de continuer sans avoir à redémarrer.

Pour désinstaller les agents d'un serveur

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

   ```
   uninstallwinclient.exe /noreboot
   ```

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

Vous pouvez également sélectionner **Démarrer** > **Exécuter** >***nom du serveur principal*\ldmain\uninstallwinclient.exe /noreboot**.

Pour désinstaller les agents d'un serveur Linux

1. Copiez le fichier linuxuninstall.tar.gz dans un répertoire temporaire du périphérique Linux. Celui-ci se trouve dans le dossier partagé de ManagementSuite du serveur principal.

   Samba n'étant probablement pas installé/configuré sur le périphérique Linux, il n'est pas possible de le copier directement ; il peut être déplacé du serveur principal ou copié dans le dossier ldlogon ou sur un support amovible.
2. A partir d'une invite Shell (sur l'ordinateur Linux), décompressez ce fichier à l'aide de la commande tar et des options x, z et f.

   ```
   tar -xzf linuxuninstall.tar.gz
   ```
3. Une fois le fichier décompressé, ouvrez une invite Shell et exécutez le script linuxuninstall à partir du répertoire actuel :

   ```
   ./linuxuninstall.sh
   ```

Configuration d'agents

Pour entièrement gérer les périphériques avec la console, vous devez installer des agents de gestion sur ces périphériques. Veuillez noter que l'installation de System Manager n'installe pas automatiquement les agents sur le serveur principal. Ceux-ci doivent être installés par vous-même puis le serveur principal doit être redémarré manuellement. Que vous utilisiez une des configurations d'agent par défaut ou créiez une configuration d'agent dans la console, vous pouvez utiliser une des trois méthodes suivantes pour l'installer sur vos périphériques Windows ou Linux :

- Créez une configuration d'agent, ciblez des périphériques dans la liste **Mes périphériques**, puis planifiez une tâche de configuration d'agent pour installer à distance des agents sur les périphériques.
- Création d'un paquet d'installation auto-extractible. Pour installer les agents, exécutez ce paquet localement sur le périphérique. Pour ce faire, vous devez être connecté avec des droits administratifs. Pour plus d'informations, reportez-vous à la section "Installation des agents avec un paquet d'installation".
- À partir d'un périphérique Windows, assignez le partage ldlogon du serveur principal (*mon_serveur*\ldlogon) et exécutez SERVERCONFIG.EXE.

Pour créer une configuration d'agent

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 la configuration**.

   Entrez un nom qui décrit la configuration que vous utilisez. Il peut s'agir d'un nom de configuration existant ou d'un nouveau nom.

4. Sélectionnez une plate-forme pour la configuration.

5. Sélectionnez le type d'installation pour la configuration (sélectionnée par l'utilisateur ou PIMI BMC-uniquement) Sélectionnez **IPMI BMC-uniquement** sous **Configuration** pour configurer le contrôleur de gestion de la carte de base (BMC) sur les périphériques dotés de IPMI (voir la note sous l'étape 9 ci-dessous).

   Une configuration uniquement IPMI BMC configure le contrôleur BMC pour les accès hors bande, effectue une analyse complète d'inventaire et se supprime elle-même. Une configuration BMC IPM-uniquement ne peut pas être définie comme configuration par défaut. Notez que lorsque vous créez une configuration uniquement IPMI BMC, la majorité des options de modification décrites dans les étapes suivantes ne sont pas disponibles.

6. Sélectionnez la configuration que vous venez de créer puis cliquez sur **Modifier**.

   Certaines options des onglets sont grisées car vous ne pouvez pas les définir pour la configuration sélectionnée.
7. Dans l'onglet **Agent**, sélectionnez les agents à déployer.

   - **Tous :** Installe tous les agents sur le périphérique sélectionné.
   - **Agent de gestion standard :** Forme la base de la communication entre les périphériques et le serveur principal. Cet agent est obligatoire (excepté pour les configurations BMC-uniquement). La plupart des processus de cet agent sont sur demande.
   - **Mises à jour de logiciel :** Installe le scanner des mises à jour de logiciel. Une fois cet agent installé, vous pouvez configurer la méthode d'exécution du scanner. Il ne s'agit pas d'un agent sur demande.
   - **Surveillance :** Installe l'agent de surveillance sur le serveur sélectionné. L'agent de surveillance autorise plusieurs types de surveillance, y compris la surveillance directe ASIC, IPMI en band, IPMI hors bande et CIM. Il ne s'agit pas d'un agent sur demande.
   - **Active System Console :** Installe l'agent qui permet à Active System Console d'être accessible via l'interface ou les menus de System Manager. Cet agent n'est pris en charge que sur les périphériques dotés de cartes mères Intel.

8. Sélectionnez le type dans les zones de type de système **Configuration**. Si vous avez déjà sélectionné le type, cette zone sera grisée.

9. Sélectionnez une option de **Redémarrage**.

   Le redémarrage manuel signifie que les périphériques ne sont pas redémarrés après l'installation. Un redémarrage de périphériques n'est pas requis après la configuration d'un agent. Vous devez redémarrer le périphérique manuellement.

   Le cas échéant, le redémarrage relance les mises à jour d'agent lorsque les fichiers mis à jour sont verrouillés.

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 lors des 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 :** La 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. Vous pouvez exécuter le scanner manuellement à partir du serveur géré ; vous pouvez le lancer via Démarrer | Programmes | LANDesk Management | Analyse d'inventaire. Dans Linux, ne vous connectez pas en tant que racine et exécutez les options suivantes à partir de la ligne de commande : `/usr/LANDesk/ldms/ldiscan -ntt`

    - **Toujours exécuter au démarrage :**Exécute le scanner d'inventaire au démarrage du périphérique. Si vous créez une configuration HP-UX, ce bouton est grisé car le scanner HP-UX est prêt à fonctionner comme une tâche, celle-ci pouvant être quotidienne, hebdomadaire ou mensuelle. Cette opération ne peut pas être modifiée.
    - **Heure de début :** Spécifiez 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.
    - **Répéter chaque :** Entrez un chiffre qui représente l'incrément (tel que 1, 2 ou 3) et la mesure (Minutes, Heures ou Jours).
    - **Restrictions :** Limite les heures et jours d'exécution du scanner d'inventaire. Cliquez sur **Heure du jour**, **Jour de la semaine** ou **Jour du mois**, puis entrez les paramètres inclusifs. Par exemple, entrez 10 pour **Jour du mois** et 1h00 et 3h00 pour **Heure du jour** afin d'autoriser l'exécution du scanner d'inventaire le 10ème jour de chaque mois entre 1h00 et 3h00 du matin.

11. Dans l'onglet **Mises à jour de logiciel**, réglez les jours et les heures d'exécution du scanner des mises à jour de logiciel. Le scanner s'exécute automatiquement sans requérir une tâche planifiée.
    - **Toujours exécuter au démarrage :** Exécute le scanner des mises à jour de logiciel au démarrage du périphérique.
    - **Heure de début :** Spécifiez une plage d'heures d'exécution du scanner. Si un périphérique se connecte pendant la plage horaire spécifiée, l'analyse des mises à jour de logiciel s'exécute automatiquement. Si le périphérique est déjà connecté, l'analyse des mises à jour de logiciel s'exécute automatiquement à l'heure de démarrage spécifiée. Cette option est utile si vous souhaitez échelonner les analyses sur les périphériques pour éviter l'envoi simultané de toutes les analyses.
    - **Répéter chaque :** Entrez un chiffre qui représente l'incrément (tel que 1, 2 ou 3) et la mesure (Minutes, Heures ou Jours).

- **Restrictions :** Limite les heures et jours d'exécution du scanner des mises à jour de logiciel. Cliquez sur **Heure du jour**, **Jour de la semaine** ou **Jour du mois**, puis entrez les paramètres inclusifs. Par exemple, entrez 10 pour **Jour du mois** et 1h00 et 3h00 pour **Heure du jour** afin d'autoriser l'exécution du scanner d'inventaire le 10ème jour de chaque mois entre 1h00 et 3h00 du matin.

12. 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.
13. Cliquez sur **Enregistrer les modifications** pour enregistrer les informations dans la base de données. Cliquez sur **Enregistrer comme fichier** pour enregistrer la configuration sous la forme de paquet distribuable.

Remarque : Vous pouvez définir une configuration d'agent comme configuration par défaut en sélectionnant la configuration dans la page **Configuration d'agent** et en cliquant sur **Définir comme valeur par défaut**. Les configurations par défaut ne peuvent pas être supprimées.

Pour planifier une tâche de configuration d'agent

1. Dans le volet de navigation de gauche, cliquez sur **Configuration d'agent**.
2. Cliquez sur la configuration d'agent, puis cliquez sur **Planifier une tâche**.
3. Modifiez la liste des périphériques ciblés et la planification des tâches.
4. Cliquez sur **Enregistrer**.

Lorsque vous cliquez sur **Planifier une tâche**, une tâche est créée (elle ne dispose d'aucun périphérique ciblé et elle n'est pas planifiée). Si vous annulez cette tâche de configuration d'agent sans l'enregistrer, n'oubliez pas qu'elle a tout de même été créée et qu'elle apparaît dans la liste **Tâche** avec l'état Non planifié. Vous pouvez la supprimer de la liste **Mes tâches**.

Une fois la tâche de configuration d'agent terminée, vous devrez redémarrer le périphérique pour afficher les détails sur le périphérique dans la console (voir Affichage de la console d'informations de serveur). Ce redémarrage est requis si vous installez l'agent sur le serveur principal ou sur des périphériques gérés. La procédure de configuration d'agent vous permet de déterminer quand le redémarrage doit être effectué afin de ne pas interférer avec l'utilisation du serveur.

Déploiement des agents vers des périphériques gérés

Une fois que vous avez découvert des périphériques, vous pouvez déployer des agents vers eux. Vous ne pouvez déployer des agents que vers des périphériques de système d'exploitation Windows et Linux et HP-UX. Vous devez disposer des droits Administrateur pour déployer des agents vers des périphériques Windows, ainsi que le privilège racine pour configurer les périphériques Linux et HP-UX.

Plusieurs méthodes permettent de déployer des agents vers des périphériques non gérés :

- Déploiements par poussage à l'aide de tâches de découverte et d'un compte administratif de domaine que vous avez configuré pour le Planificateur, qui traite les tâches de découverte. Le compte administratif de domaine donne aux services planificateur les droits nécessaires pour installer les agents de serveur. Méthode appropriée pour les serveurs de la famille Windows NT.
- Déploiements en mode push par l'agent de gestion standard. Si les serveurs disposent de l'agent de gestion standard, utilisé par de nombreux produits de LANDesk Software, vous pouvez déployer vers ceux-ci sans avoir besoin d'un compte administratif de domaine.

Lorsque vous déployez vers des périphériques découverts, utilisez l'option **Filtrer par** de l'arborescence **Non gérés**. Vous pouvez filtrer suivant l'adresse IP pour isoler les périphériques.

Pour les systèmes Windows, les paramètres de port suivants requierent une configuration manuelle du pare-feu pour que tout le produit fonctionne. Pour modifier ces paramètres, accédez au Pare-feu Windows via le Panneau de configuration de Windows.

Serveurs gérés :

- Partage de fichiers et d'imprimantes : TCP 139, 445 ; UDP 137, 138 (le mode Push ne fonctionne pas sans cette option)
- Distribution de logiciel : TCP 9595 (le mode Push ne fonctionne pas sans cette option)
- ICMP - Avancé : "Autoriser la requête d'écho entrante" (Ne peut pas être découvert si cette option n'est pas activée.)

Serveur principal :

- Inventaire : 5007
- Contrôle distant : 9535

Configuration des références d'authentification de périphérique

Les périphériques non gérés dotés de l'agent de gestion standard ne requièrent pas de références d'authentification pour le déploiement d'agents. Pour installer des agents sur des serveurs Windows ne disposant pas de l'agent de gestion standard, vous devez spécifier les références d'authentification que le service Planificateur installé sur le périphérique de la console utilisera pour obtenir les droits requis.

Pour installer des agents de périphérique sur des périphériques non gérés, le service Planificateur doit pouvoir se connecter aux périphériques avec un compte administratif. Le compte par défaut utilisé par le service Planificateur est LocalSystem. Les références d'authentification LocalSystem fonctionnent en général sur les périphériques qui ne sont pas présents dans un domaine.

Si les périphériques sont situés dans un domaine, vous devez spécifier un compte d'administrateur de domaine. Si vous configurez des périphériques non gérés dans plusieurs domaines, vous devez les configurer un domaine à la fois, car le service Planificateur s'authentifie avec un ensemble de références, et chaque domaine requiert un compte administratif de domaine différent.

Le serveur principal inclut l'utilitaire Configuration des services, que vous pouvez utiliser pour personnaliser des options d'inventaire. Cet utilitaire peut uniquement être exécuté sur le serveur principal.

Pour configurer les références de connexion au service Planificateur

1. Lancez l'utilitaire Configuration des services sur le serveur principal en cliquant sur **Démarrer | Programmes | LANDesk | Configuration des services**.
2. Cliquez sur l'onglet **Planificateur**.
3. Cliquez sur le bouton **Modifier la connexion**.
4. Entrez les références qui seront utilisées par le service sur les clients, généralement un compte administrateur de domaine.

Installation des agents

Une fois une configuration d'agent créée dans la console, vous devez l'installer sur les périphériques. Veuillez noter que l'installation de System Manager n'installe pas automatiquement les agents sur le serveur principal. Ceux-ci doivent être installés par vous-même puis le serveur principal doit être redémarré manuellement.

Les paquets de l'agent de client correspondent à un fichier exécutable auto-extractible unique. Par défaut, ils sont stockés dans le dossier \Program Files\LANDesk\ManagementSuite\ldlogon du serveur principal. Le fichier exécutable installe les agents de client en transparence, sans aucune interaction de l'utilisateur. Il n'est pas nécessaire que le périphérique ciblé dispose d'un navigateur pour réussir à installer l'agent.

Installation des agents

Vous pouvez mettre à jour les agents en créant une nouvelle configuration de client et en la distribuant à partir de la console, ou installer directement les agents sur des périphériques non gérés.

Une fois un paquet d'agents de périphérique installé, l'installation d'autres paquets d'agents de client supprime tous les agents et installe uniquement les agents spécifiquement sélectionnés. Vous pouvez désinstaller un agent en créant un nouveau paquet d'agents de client qui n'inclut pas l'agent que vous souhaitez supprimer.

Désinstallation des agents

Si vous devez désinstaller certains agents des périphériques, reportez-vous à la section "Présentation de l'installation et de la configuration d'un agent".

Installation d'agents avec un paquet d'installation

Vous pouvez installer des agents par l'intermédiaire d'un paquet d'agent de périphérique auto-extractible. Cette méthode permet de copier le fichier sur un CD ou un lecteur USB et d'installer

manuellement les agents. Pour créer ces paquets, cliquez sur **Enregistrer comme fichier** en bas de la boîte de dialogue **Configuration**.

1. Cliquez sur **Configuration d'agent**, puis cliquez deux fois sur un nom de configuration.
2. Dans la boîte de dialogue **Configuration d'agent**, cliquez sur **Enregistrer comme fichier**, puis cliquez sur **Fermer**.

Lorsque vous cliquez sur **Enregistrer comme fichier**, un paquet exécutable auto-extractible, dont le nom de fichier correspond au nom de configuration spécifié, est créé. Le paquet peut ne pas être disponible dans le dossier Program Files\LANDesk\ManagementSuite\ldlogon\ConfigPackages du serveur principal avant quelques minutes.

Le fichier exécutable installe les agents, sans aucune interaction de l'utilisateur. Vous devez vous connecter avec des privilèges administratifs.

Si les utilisateurs ne peuvent pas se connecter avec des privilèges administratifs pour installer le paquet, vous pouvez déployer les paquets via une messagerie, un téléchargement Web, un script de connexion ou à partir d'un partage.

Tirage des agents

Cette section contient des détails sur le déploiement d'agents 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 SERVERCONFIG.EXE. Vous pouvez démarrer le programme SERVERCONFIG.EXE en mode autonome. Il est situé dans le partage *http:**serveur_principal**LDLogon*, qui peut être lu à partir de tout serveur Windows.

SERVERCONFIG.EXE utilise SERVERCONFIG.INI pour configurer des périphériques.

Présentation de SERVERCONFIG.EXE

SERVERCONFIG.EXE configure les serveurs Windows NT à l'aide des étapes suivantes :

1. SERVERCONFIG détermine si l'ordinateur a été précédemment configuré avec un agent de gestion. Si tel est le cas, SERVERCONFIG supprime tous les composants et réinstalle les composants sélectionnés.
2. SERVERCONFIG charge le fichier d'initialisation approprié (SERVERCONFIG.INI) et exécute les instructions qu'il contient.

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 (CBA)"

Paramètre	Description
	"Scanner d'inventaire" "Alerte" "Scanner de vulnérabilités" "Moniteur de serveur" Vous pouvez les combiner sur la même ligne de commande. Par exemple : `SERVERCONFIG.EXE /I="Alerte" /I="Scanner de vulnérabilités"`
/L ou /Log=	Chemin vers les fichiers journaux CFG_YES et CFG_NO qui consignent les serveurs 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 serveur une fois terminé (par défaut)
/REBOOT	Force un redémarrage après l'exécution
/X=	Composants à exclure. Par exemple : `SERVERCONFIG.EXE /X=SD`
/CONFIG= /[CONFIG]=	Spécifie un fichier de configuration de 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 se trouver dans le même répertoire que le fichier SERVERCONFIG.EXE. Notez également que le paramètre /config utilise le nom de fichier sans le préfixe NT.
/? ou /H	Affiche le menu d'aide

Création d'une configuration d'agent

Utilisez **Configuration d'agent** pour créer et mettre à jour des configurations d'agent de serveur (indiquant quels agents sont installés ou gérés). Vous pouvez créer différentes configurations pour les besoins spécifiques à un groupe. Par exemple, vous pouvez créer une configuration pour les serveurs Web et une autre pour les serveurs d'applications.

Pour pousser une configuration vers un serveur, vous devez effectuer les opérations suivantes :

- **Créer la configuration d'agent**: Installer des configurations spécifiques pour les serveurs.
- **Planifier la configuration d'agent :** Pousser la configuration vers des serveurs ou, depuis le serveur, exécuter SERVERCONFIG.EXE à partir du partage LDLogon du serveur principal.

Pour créer une configuration d'agent

1. Dans la console, cliquez sur **Configuration d'agent**
2. Cliquez sur le bouton **Nouveau** de la barre d'outils.
3. Entrez un **Nom de configuration** et sélectionnez le système d'exploitation, puis cliquez sur **OK**.
4. Cliquez sur le nom de la nouvelle configuration, puis cliquez sur **Modifier**.
5. Sélectionnez les agents que vous souhaitez déployer.
6. Utilisez les onglets dans la partie supérieure de la boîte de dialogue pour passer aux options relatives aux composants sélectionnés. Personnalisez les options sélectionnées selon les besoins.
7. Cliquez sur **Enregistrer les modifications**, puis fermez la boîte de dialogue.
8. Si vous souhaitez que la configuration soit celle par défaut, cliquez sur **Définir comme configuration par défaut**.

Tirer une configuration d'agent Linux

Pour tirer une configuration d'agent Linux

1. Créez un répertoire temporaire sur votre périphérique 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, recherchez "FILE*xx"* dans le fichier .INI, *xx* représentant un chiffre. 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\<*texte*>.ruleset.monitor.xml doit être renommé masterconfig.ruleset.monitor.xml

2. Si le périphérique est doté de IPMI et d'un 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 utilisé ci-dessous :

   ```
   /tmp/ldcfg/pull.sh
   ```

4. Supprimez le répertoire temporaire et tout ce qu'il contient.

Remarque : Si vous poussez ou tirez un agent vers un périphérique Linux, que vous exécutez

```
./linuxuninstall.sh -f ALL
```

pour le nettoyer puis ensuite que vous poussez ou tirez à nouveau, alors le fichier avec le GUID est le seul fichier présent sur le périphérique une fois cette opération terminée.

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.

Création de paquets de configuration d'agent autonomes

En général, l'utilitaire de configuration d'agent, SERVERCONFIG.EXE, configure les agents sur les périphériques gérés. Si vous le souhaitez, la fenêtre **Configuration d'agent** peut créer un fichier exécutable unique auto-extractible qui installe une configuration d'agent sur le serveur sur lequel il est exécuté. Ceci peut s'avérer utile si vous voulez installer des agents depuis un CD ou depuis un lecteur USB portable.

Poussage d'une configuration d'agent vers des périphériques

Pour pousser une configuration d'agent

1. Dans la console, sélectionnez les périphériques vers lesquels déployer les agents, puis cliquez sur **Cible**.
2. Dans le volet de navigation de gauche, cliquez sur **Configuration d'agent**.
3. Cliquez avec le bouton droit de la souris sur la configuration d'agent que vous souhaitez pousser, puis cliquez sur **Planifier une tâche.**
4. Cliquez sur **Périphériques cible** dans boîte de dialogue **Propriétés de la planification de tâches**, puis cliquez sur **Ajouter la liste cible**.
5. Cliquez sur **Planifier une tâche**.
6. Spécifiez l'heure de déploiement de l'agent, puis cliquez sur **Enregistrer**.

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 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 via **Configuration d'agent**, vous avez besoin d'un RPM supplémentaire, sysstat. Pour obtenir une liste complète des RPM requis par le produit, consultez le *Guide de déploiement System Manager*.

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.

Déploiement des agents Linux

Une fois vos serveurs Linux configurés et vos références d'authentification Linux ajoutées au serveur principal, vous devez ajouter des serveurs dans la liste **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 **Découverte de 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 le processus de découverte a trouvé les serveurs Linux à gérer.
3. Dans **Découverte de périphérique**, sélectionnez les serveurs à gérer et cliquez sur **Cible** pour ajouter les périphériques sélectionnés à la Liste de cibles. 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**, sélectionnez le type d'installation (serveur ou bureau), 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. 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.
7. Cliquez sur **Enregistrer les modifications**.

Pour déployer votre configuration d'agent, sélectionnez-la dans **Configurations 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 périphérique 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 périphérique Linux (par exemple, /tmp/ldcfg) et copiez ce qui suit dans le répertoire temporaire :
    - Tous les fichiers du répertoire LDLOGON\unix\linux.
    - Le script Shell nommé en fonction de la configuration (<*nom de la configuration*>.sh).
    - Le fichier *.0 nommé en fonction de la configuration. L'astérisque (*) représente huit caractères (0-9, a-f).
    - Tous les fichiers répertoriés dans le fichier <*nom de la configuration*>.ini. Pour identifier ces fichiers, recherchez "FILE*xx"* dans le fichier .INI, *xx* représentant un chiffre. 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*>.rruleset.monitor.xml doit être renommé masterconfig.ruleset.monitor.xml

2. Si le périphérique est doté de IPMI et d'un 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 en utilisant le chemin complet ci-dessous :

   ```
   /tmp/ldcfg/lsminstall.sh
   ```

4. Supprimez le répertoire temporaire et tout ce qu'il contient.

Remarque : N'oubliez pas que si vous poussez ou tirez un agent vers un périphérique Linux, puis exécutez

```
./linuxuninstall.sh -f ALL
```

pour le nettoyer et ensuite poussez ou tirez à nouveau, le fichier avec le GUID est le seul fichier présent sur le périphérique une fois cette opération terminée.

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.

Paramètres de ligne de commande du scanner d'inventaire

Le scanner d'inventaire, ldiscan dispose de plusieurs paramètres de ligne de commande qui spécifient sa méthode d'exécution. Reportez-vous à la section "ldiscan -h" ou "man ldiscan" pour obtenir une description détaillée de chacun de ces paramètres. Chaque option doit être précédée par "-" ou "/".

Paramètre	Description
-d=Dir	Démarre l'analyse de logiciels dans le répertoire Dir au lieu de la racine. Par défaut, l'analyse démarre dans le répertoire root.
-f	Force une analyse de logiciels. Si vous ne spécifiez pas -f, le scanner effectue des analyses de logiciels selon l'intervalle quotidien (chaque jour par défaut) spécifié dans la console sous **Configuration | Services | Inventaire | Paramètres du scanner**.
-f-	Désactive l'analyse de logiciels.
-i=Nom_Conf	Spécifie le nom du fichier de configuration. Le nom par défaut est etc/ldappl.conf.

Paramètre	Description
-ntt=addresse:port	Nom d'hôte ou adresse IP du serveur principal. Le port est facultatif.
-o=Fichier	Ecrit les informations d'inventaire vers le fichier de sortie spécifié.
-s=Serveur	Indique le serveur principal. Cette commande est facultative et existe uniquement pour des besoins de compatibilité en amont.
-stdout	Ecrit les données d'inventaire vers la sortie standard.
-v	Active les messages d'état durant l'analyse.
-h ou -?	Affiche l'écran d'aide.

Exemples

Pour sortir des données vers un fichier texte, entrez :

```
ldiscan -o=data.out -v
```

Pour envoyer des données au serveur principal, entrez :

```
ldiscan -ntt=ServerIPName -v
```

Fichiers du scanner d'inventaire Linux

Fichier	Description
ldiscan	Fichier exécutable exécuté avec des paramètres de ligne de commande pour indiquer l'action à prendre. Tous les utilisateurs qui exécuteront le scanner doivent posséder des droits suffisants pour exécuter le fichier. Il existe une version différente de ce fichier pour chaque plate-forme prise en charge ci-dessus.
/etc/ldiscan.conf	Fichier résidant toujours dans /etc et contenant les informations suivantes : • ID unique attribué par l'inventaire • Dernière analyse de matériels • Dernière analyse de logiciels

Fichier	Description
	Tous les utilisateurs qui exécutent le scanner doivent posséder des attributs de lecture/écriture sur ce fichier. L'ID unique dans /etc/ldiscan.conf est un numéro unique attribué à un ordinateur lors de la première exécution du scanner d'inventaire. Ce numéro est utilisé pour identifier l'ordinateur. S'il change éventuellement, le serveur principal le traite comme un ordinateur différent, ce qui peut résulter en un doublon d'entrée dans la base de données. **Avertissement :** Ne modifiez pas le numéro d'ID unique et ne supprimez pas le fichier ldiscan.conf après sa création..
/etc/ldappl.conf	Fichier dans lequel vous personnalisez la liste des fichiers exécutables rapportés par le scanner d'inventaire lors de l'exécution d'une analyse de logiciels. Le fichier inclut certains exemples et vous devrez ajouter des entrées pour les paquets logiciels que vous utilisez. Les critères de recherche sont basés sur le nom et la taille des fichiers. Bien que ce fichier réside généralement dans /etc, le scanner peut utiliser un fichier alternatif à l'aide du paramètre de ligne de commande -i=.
ldiscan.8	Page man pour ldiscan.

Intégration de la console

Une fois un ordinateur Linux analysé dans la base de données principale, vous pouvez :

- Rechercher tout attribut renvoyé par le scanner d'inventaire Linux à la base de données principale.
- Utiliser les fonctions de rapport pour générer des rapports qui comportent des informations rassemblées par le scanner Linux. Par exemple, Linux apparaît comme un type de système d'exploitation dans le rapport Récapitulatif de systèmes d'exploitation.
- Afficher les informations d'inventaire des ordinateurs Linux.

Les requêtes sur le "Temps de fonctionnement du système" sont triées par ordre alphabétique, renvoyant des résultats inattendus
Si vous souhaitez effectuer une requête pour déterminer le nombre d'ordinateurs ayant fonctionné pendant une période supérieure à un nombre donné de jours (par exemple, 10 jours), exécutez une requête sur "Démarrage du système" plutôt que sur "Temps de fonctionnement du système". Les requêtes sur "Temps de fonctionnement du système" peuvent renvoyer des résultats inattendus, car le temps de fonctionnement du système est simplement une chaîne du format "x jours, y heures, z minutes et j secondes". Le tri est effectué alphabétiquement et non selon les intervalles de temps.

Le chemin des fichiers de configuration référencés dans le fichier ldappl.conf n'apparaît pas dans la console
Les entrées ConfFile dans le fichier ldappl.conf doivent inclure un chemin.

Surveillance de périphérique

Présentation de la surveillance

System Manager fournit plusieurs méthodes de surveillance de l'état de santé d'un périphérique. Les fonctions de surveillance regroupent des données de sources variées pour vous aider à suivre les données de vos périphériques, telles que :

- Niveaux d'utilisation
- Evénements de système d'exploitation
- Procédures et services
- Performance historique
- Détecteurs de matériel (ventilateurs, tensions, températures, etc.)

Ce chapitre contient des informations sur les différentes fonctions qui surveillent les périphériques gérés :

- Installation d'un agent de surveillance sur des périphériques et création d'ensembles de règles de surveillance qui peuvent être déployés vers des périphériques.
- Configuration des compteurs de performance sur des périphériques et surveillance des données de performance.
- Surveillance des modifications de configuration avec des alertes lorsque des modifications se produisent.
- Sondage Ping régulier des périphériques pour surveiller leur connectivité, à l'aide de la fonction **Moniteur de périphérique**.

L'envoi d'alertes est une fonction associée qui utilise l'agent de surveillance pour initialiser des actions d'alerte, telles que l'envoi de messages électronique et de messages par téléavertisseur, le redémarrage et l'arrêt d'un périphérique ou l'ajout d'informations au journal d'alerte. Vous pouvez générer des alertes depuis n'importe quel événement de périphérique pouvant être surveillé. Pour plus d'informations, reportez-vous à la section "Utilisation des alertes".

Remarques

- Les communications avec l'agent de surveillance sont effectuées via HTTP sur TCP/IP sous la forme de requêtes GET, POST ou XML. Les réponses aux requêtes sont au format de documents de tableau HTML ou XML.
- Pour exécuter et stocker une requête sur l'état de santé des périphériques (Computer.Health.State), n'oubliez pas que l'état est représenté par un nombre dans la base de données. Les nombres correspondent aux états suivants : 4=Critique, 3=Avertissement, 2=Normal, 1=Informationnel, nul ou 0=inconnu.
- La surveillance de matériel dépend des possibilités du matériel installé sur un périphérique, ainsi que sur la configuration correcte du matériel. Par exemple, si un disque dur avec des fonctions de surveillance S.M.A.R.T. est installé sur un périphérique, mais si la détection S.M.A.R.T n'est pas activée dans les paramètres BIOS du périphérique, ou si le BIOS du périphérique ne prend pas en charge les lecteurs S.M.A.R.T., la surveillance des données ne sera pas disponible.

- Si un ordinateur n'envoie plus de rapport, vous pouvez utiliser le fichier restartmon.exe se trouvant dans le dossier LDCLIENT pour redémarrer le collecteur et tous les fournisseurs de surveillance. Cet utilitaire ne fonctionne que sur les ordinateurs sur lesquels il a été installé et qui ont cessé d'envoyer des rapports. Utilisez cet utilitaire pour redémarrer le collecteur et les fournisseurs sans redémarrer le périphérique.

Déploiement de l'agent de surveillance vers les périphériques

System Manager fournit un récapitulatif immédiat de la santé du périphérique lorsque l'agent de surveillance est installé sur le périphérique. L'agent de surveillance est un des six agents pouvant être installés sur les périphériques gérés. Il vérifie périodiquement la configuration et le matériel du périphérique et reflète toute modification dans l'état de santé du périphérique. L'état est représenté par des icônes d'état dans la liste **Mes périphériques** et les détails sont affichés dans les entrées du fichier journal (dans le récapitulatif **Informations système** du périphérique) et dans des graphes (dans la page de récapitulatif **Surveillance** du périphérique).

Par exemple, un périphérique surveillé pour lequel le disque dur se remplit peut afficher une icône d'état d'avertissement lorsque le disque est rempli à 90 % et passe à une icône d'état critique lorsque le disque est rempli à 95 %. Vous pouvez également recevoir des alertes pour les mêmes états de lecteur de disque si le périphérique utilise un ensemble de règles d'alerte qui inclut des règles pour une alerte d'espace de disque.

Vous pouvez déployer l'ensemble de règles de surveillance par défaut vers les périphériques. Ou, si vous le préférez, vous pouvez créer un ensemble de règles personnalisé qui inclut uniquement les éléments de santé qui vous concernent.

Création d'un ensemble de règles de surveillance

Vous pouvez choisir les situations à surveiller sur un périphérique en créant un ensemble de règles de surveillance, qui définit ce que l'agent de surveillance vérifie sur le périphérique. Vous pouvez déployer un ensemble de règles vers un périphérique ou vers un groupe ciblé de périphériques. Par exemple, vous pouvez définir un ensemble de règles pour les serveurs dédiés au stockage et utiliser un autre ensemble de règles pour les serveurs Web.

L'ensemble de règles de surveillance par défaut inclut 16 éléments. Lorsque vous créez un ensemble de règles vous pouvez activer ou désactiver ces éléments, spécifier la fréquence de leur vérification, et, pour certains éléments, configurer des seuils. Vous pouvez également sélectionner les services qui sont exécutés sur les périphériques que vous surveillez.

Le processus général de création et de déploiement d'un ensemble de règles d'alerte est le suivant :

1. Sélectionnez les périphériques vers lesquels déployer l'ensemble de règles et cliquez sur **Cibler** pour les ajouter à la liste **Périphériques ciblés**.
2. Créez ou modifiez un ensemble de règles de surveillance. Notez que vous devez cocher la case pour activer la surveillance pour chaque événement que vous souhaitez surveiller dans l'ensemble de règles. Ils ne sont pas tous surveillés par défaut. Certains événements, tels que les services, requièrent également que vous sélectionniez chaque service à surveiller. (Voir les étapes ci-dessous.)

3. Déployer l'ensemble de règles sur les périphériques ciblés. Vous pouvez cibler des périphériques supplémentaires avant de déployer l'ensemble de règles si nécessaire. (Voir les étapes ci-dessous.)

Pour créer un ensemble de règles de surveillance

1. Dans le volet de navigation de gauche, cliquez sur **Surveillance**.
2. Cliquez sur l'icône **Nouveau**, entrez un nom et une description de la configuration, puis cliquez sur **OK**.
3. Sélectionnez la configuration dans la colonne de gauche.
4. Dans la liste des éléments, cliquez sur un élément à modifier et cliquez sur **Modifier**.
5. Pour désactiver la surveillance d'un élément, désélectionnez la case à cocher et cliquez sur **Mettre à jour**.
6. Pour modifier la fréquence à laquelle l'élément est surveillé, sélectionnez **Secondes** ou **Minutes** et spécifiez un nombre dans la zone de texte.
7. Si applicable, réglez les pourcentages des seuils des états Avertissement et Critique.
8. Pour la surveillance de **Services**, sélectionnez le système d'exploitation dans la liste déroulante. Sélectionnez un ou plusieurs services à surveiller (utiliser CTRL + cliquer pour sélectionner plusieurs services) et cliquez sur **>>** pour ajouter des services à la liste de droite.
9. Pour chaque élément que vous modifiez, cliquez sur **Mettre à jour** pour appliquer vos modifications à la configuration. Si vous modifiez un élément et que vous changiez d'avis après, cliquez sur **Retourner à l'état précédent** pour restaurer les paramètres d'origine.

Lorsque vous modifiez les services dans une configuration de surveillance à partir du serveur principal, la liste **Services disponibles** affiche les services connus de la base de données d'inventaire. Aucun service ne s'affiche dans la liste **Services disponibles** tant qu'un agent LANDesk n'a pas été déployé vers un ou plusieurs périphériques et qu'une analyse d'inventaire n'a pas été renvoyée au serveur principal. Par exemple, pour sélectionner des services Linux dans la liste, vous devez auparavant avoir déployé un agent vers un périphérique Linux.

Pour déployer un ensemble de règles de surveillance

1. Dans le volet de navigation de gauche, cliquez sur **Mes périphériques**, puis cliquez sur le groupe **Tous les périphériques**.
2. Sélectionnez les périphériques vers lesquels déployer l'ensemble de règles, puis cliquez sur **Cibler** pour placer les périphériques dans la liste **Périphériques ciblés**.
3. Dans le volet de navigation de gauche, cliquez sur **Surveillance**, puis cliquez sur l'onglet **Déployer l'ensemble de règles**.
4. Dans la case **Ensemble de règles de surveillance**, sélectionnez l'ensemble de règles à déployer.
5. Cliquez sur le lien pour afficher la liste **Périphériques ciblés**. Pour supprimer un périphérique de cette liste, cliquez avec le bouton droit de la souris sur un périphérique, puis cliquez sur **Supprimer**. (Pour ajouter des périphériques, vous devez les ajouter à la liste ciblée comme décrit dans l'étape 2)
6. Cliquez sur **Déployer** pour déployer l'ensemble de règles sélectionné vers les périphériques ciblés.

En tant que partie du processus de déploiement, la page XML est créée et répertorie les ensembles de règles déployés et les périphériques vers lesquels les ensembles de règles ont été

déployés. Ce rapport est enregistré sur le serveur principal dans le répertoire LDLOGON, et est nommé avec un numéro séquentiel attribué par la base de données. Si vous souhaitez afficher cette page XML séparément du déploiement d'un ensemble de règles, cliquez sur le bouton **Générer XML**, puis cliquez sur le lien pour afficher le fichier XML. Lorsque vous générez un ensemble de règles en tant que XML, celui-ci s'affiche dans la liste des ensembles disponibles dans les paramètres **Configuration d'agent**.

Désactivation du service ModemView

Le service ModemView correspond au service/pilote qui surveille les appels de modem (entrant et sortant) et génère une alerte lorsqu'il en détecte. Ce service utilise environ 10 Mo de mémoire car il utilise MFC. Vous pouvez souhaiter le désactiver, particulièrement si votre périphérique n'utilise pas un modem.

Pour désactiver le service ModemView

1. Sur le périphérique (directement ou par contrôle distant) cliquez sur **Démarrer** > **Panneau de configuration** > **Outils d'administration** > **Services**.
2. Cliquez deux fois sur **LANDesk Message Handler Service**.
3. Sous **Type de démarrage**, sélectionnez **Manuel**, et cliquez sur **OK**.

Vous pouvez également cliquez sur **Arrêt** sous **Etat du service**.

Configuration des compteurs de performance

System Manager permet de sélectionner les éléments de performance (compteurs) à surveiller sur un périphérique géré. Vous pouvez surveiller plusieurs types d'éléments, y compris des composants matériels, tels que des lecteurs, processeurs et mémoires, ou vous pouvez surveiller des composants de système d'exploitation, tels que des processus ou bien vous pouvez surveiller des composants d'application, tels que les octets par seconde transférés par le serveur Web du système. Lorsque vous sélectionnez un compteur de performance, vous spécifiez également la fréquence d'interrogation de l'élément, ainsi que les seuils de performance et le nombre de violations autorisées avant qu'une alerte ne soit générée.

Une fois qu'un compteur de performance est sélectionné, vous pouvez surveiller la performance sur la page **Surveiller** en affichant un graphe en temps réel ou les données historiques. Pour plus d'informations, reportez-vous à la section "Performance de surveillance".

Pour sélectionner un compteur de performance à surveiller

1. Dans la vue **Mes périphériques**, cliquez deux fois sur le périphérique que vous souhaitez configurer. La console d'informations du serveur s'ouvre dans une autre fenêtre de navigateur.
2. Dans le volet de navigation de gauche, cliquez sur **Surveillance**.
3. Cliquez sur l'onglet **Configuration des compteurs de performance**.
4. Dans la colonne **Objets**, sélectionnez l'objet à surveiller.
5. Dans la colonne **Instances**, sélectionnez l'instance de l'objet à surveiller, si applicable.

6. Dans la colonne **Compteurs**, sélectionnez celui que vous souhaiter surveiller.

   Si le compteur que vous recherchez ne se trouve pas dans la liste, cliquez sur **Recharger les compteurs** pour actualiser la liste avec les nouveaux objets, instances ou compteurs.

7. Spécifiez la fréquence d'interrogation (**Vérifier toutes les** *n* **secondes**) et le nombre de jours de conservation de l'historique du compteur.
8. Dans la zone de texte **Alerter une fois le compteur hors limites**, spécifiez le nombre de fois que le compteur est autorisé à dépasser les seuils avant qu'une alerte ne soit générée.
9. Spécifiez les seuils supérieurs et inférieurs.
10. Cliquez sur **Appliquer**.

Remarques

- La taille des fichiers journaux de performance peut augmenter rapidement ; l'interrogation d'un compteur unique selon un intervalle de deux secondes ajoute 2,5 Mo d'informations au journal de performance par jour.
- Une alerte d'avertissement est généré lorsqu'un compteur de performance tombe en dessous d'un seuil inférieur sur un périphérique Windows ou Linux. Lorsqu'un compteur de performance dépasse un seuil supérieur sur un périphérique Linux, une alerte d'avertissement est générée. Lorsqu'un compteur de performance dépasse un seuil supérieur sur un périphérique Windows, une alerte critique est générée.
- Lors de la configuration des seuils, n'oubliez pas que les alertes seront générées que le seuil supérieur ou inférieur soit franchi. Dans le cas d'un manque d'espace disque, vous pouvez ne souhaiter recevoir une alerte que si l'espace du périphérique est insuffisant. Dans ce cas, il est recommandé de régler le seuil supérieur sur une valeur suffisamment élevée qui ne génèrera pas une alerte si beaucoup d'espace disque devient disponible sur le périphérique.
- La modification du nombre **Alerter une fois le compteur hors limites** permet vous concentrer sur un problème lorsqu'il est persistent ou lorsqu'il s'agit d'un événement isolé. Par exemple, si vous surveillez les octets envoyés par un serveur Web, System Manager peut vous envoyer une alerte lorsque les octets/sec sont constamment élevés. Ou, vous pouvez spécifier un nombre faible, tel que 1 ou 2, pour recevoir une alerte chaque fois que vos connexions FTP anonymes dépassent un certain nombre d'utilisateurs.

Surveillance de la performance

La page **Surveillance** permet de surveiller la performance de plusieurs objets système. Vous pouvez surveiller des composants matériels spécifiques, tels que des lecteurs, processeurs et mémoires, ou vous pouvez surveiller des composants de système d'exploitation, tels que des processus ou octets par seconde transférés par le serveur Web du système. La page **Surveillance** inclut un graphe qui affiche des données historiques ou en temps réel pour les compteurs.

Pour surveiller un compteur de performance vous devez auparavant sélectionner le compteur qui est ajouté à la liste des compteurs surveillés. Vous pouvez également spécifier la fréquence d'interrogation de l'élément et définir des seuils de performance et le nombre de violations autorisées avant qu'une alerte ne soit générée. Pour plus d'informations sur la sélection des compteurs, reportez-vous à la section "Configuration des compteurs de performance".

Pour afficher un graphe de performance pour un compteur surveillé.

1. Dans la vue **Mes périphériques**, cliquez deux fois sur le périphérique que vous souhaitez configurer. La console d'informations du serveur s'ouvre dans une autre fenêtre de navigateur.
2. Dans le volet de navigation de gauche, cliquez sur **Surveillance**.
3. Si nécessaire, cliquez sur l'onglet **Compteurs des performances actifs**.
4. Dans la liste déroulante **Compteurs**, sélectionnez le compteur pour lequel afficher un graphe de performance.
5. Sélectionnez **Afficher les données en temps réel** pour afficher un graphe des performances en temps réel.

   ou

   Sélectionnez **Afficher les données historiques** pour afficher un graphe qui affiche des performances pour la période spécifiée (Garder un historique) lors de la sélection du compteur.

Dans le graphe de performance, l'axe horizontal représente le temps écoulé. L'axe vertical représente les unités mesurées, telles que octets par seconde (lors de la surveillance de transferts de fichier, par exemple), pourcentage (lors de la surveillance du pourcentage du processeur utilisé) ou octets disponibles (lors de la surveillance de l'espace du disque dur). La hauteur de la ligne n'est pas une unité fixe. Elle varie en fonction des extrêmes des données ; pour un compteur, l'axe vertical peut représenter des valeurs comprises entre 1 et 100 alors que pour un compteur différent, il peut représenter des valeurs comprises entre 1 et 500 000. Lorsque la différence entre les données est extrême, des variations insignifiantes peuvent donner l'impression d'une ligne horizontale.

Remarques

- La sélection d'un autre compteur actualise le graphe et réinitialise les unités de mesure.
- Cliquez sur **Actualiser**  pour effacer et réinitialiser le graphe.
- Si vous recevez une alerte générée par un compteur de la liste, cliquez avec le bouton droit de la souris sur un compteur puis sur **Accuser réception** pour effacer l'alerte.

Pour arrêter la surveillance d'un compteur de performance.

1. Dans la vue **Mes périphériques**, cliquez deux fois sur le périphérique que vous souhaitez configurer. La console d'informations du serveur s'ouvre dans une autre fenêtre de navigateur.
2. Dans le volet de navigation de gauche, cliquez sur **Surveillance**.
3. Si nécessaire, cliquez sur l'onglet **Compteurs des performances actifs**.
4. Sous **Compteurs de performance surveillés**, cliquez avec le bouton droit de la souris sur le compteur, puis cliquez sur **Supprimer**.

Surveillance des modifications de configuration

Ce produit peut gnrer des alertes si la configuration du matriel et logiciel d'un priphrique est modifie et si l'agent de surveillance est install sur le priphrique. Ces modifications peuvent affecter la performance et la stabilit du priphrique ou engendrer des problmes dans une installation standard. En surveillant des sections critiques du priphrique, ce produit peut vous aider rduire le cot total de proprit (TCO).

Les modifications de configuration de priphrique qui gnrent des alertes sont :

- **Application installe ou dsinstalle :** Vous pouvez visualiser quels utilisateurs ont install ou supprim des applications. Cette fonction peut s'avrer utile pour suivre des licences ou la productivit d'un employ. Les applications qui sont enregistres dans la zone de Windows Ajout/Suppression de programmes du Panneau de configuration sont surveilles. Les autres applications sont ignores. Le nom d'application qui est utilis dans la fonction Ajout/Suppression de programme de Windows correspond au nom d'application qui s'affiche dans le journal de notification ou la fentre contextuelle d'alerte.
- **Mmoire ajoute ou supprime :** Ce produit dtecte et surveille la quantit et le type de mmoire installe. Si la configuration est modifie, une alerte est gnre.
- **Disques durs ajouts ou supprims :** Ce produit dtecte et surveille le type et la taille des lecteurs installs sur les serveurs. Si la configuration est modifie, une alerte est gnre.
- **Processeur (ou processeurs) ajout(s), supprim(s) ou modifi(s) :** Ce produit dtecte et surveille le nombre, le type et la vitesse du ou des processeurs. Si la configuration est modifie, une alerte est gnre.
- **Carte rseau ajoute ou supprime :** Ce produit dtecte et surveille le nombre et le type de cartes d'interface rseau sur les priphriques et gnre des alertes lorsque la configuration est modifie.

Pour afficher un enregistrement des alertes sur les modifications de la configuration, passez en revue le journal des alertes sur la console d'informations du serveur. Pour plus d'informations, reportez-vous la section "Affichage du journal d'alertes".

Surveillance de la connectivité

Dans la plupart des cas, les périphériques peuvent vous avertir lorsqu'une situation critique se présente, comme par exemple lorsque le disque dur est saturé ou lorsque le ventilateur s'arrête. Toutefois, dans certaines situations, il se peut que le périphérique passe hors ligne avant de pouvoir envoyer une alerte. Par exemple, un commutateur ou un routeur peut perturber le trafic réseau ou le périphérique peut éprouver des pannes d'alimentation.

Dans ces situation, ce produit peut vérifier périodiquement les périphériques afin de déterminer s'ils sont disponibles sur le réseau. Si le périphérique ne répond pas au Ping, son état de santé passe à l'état critique la prochaine fois que vous actualisez la liste **Mes périphériques**.

Vous devez configurer l'utilitaire de surveillance de périphériques pour qu'il envoie un Ping aux périphériques ciblés ou à tous les périphériques du groupe **Tous les périphériques**.

Pour configuration la surveillance de périphérique

1. Dans la liste **Mes périphériques**, sélectionnez les périphériques à surveiller. Vous pouvez les sélectionner dans la liste **Tous les périphériques** ou dans un groupe privé ou public.
2. Cliquez sur **Cibler**.
3. Dans le volet du bas, cliquez sur **Actions**, puis cliquez sur **Moniteur de périphérique**.
4. Pour afficher une liste des périphériques actuellement surveillés, cliquez sur **Afficher les périphériques surveillés**.
5. Entrez un nombre pour définir les minutes entre les balayages de commande Ping et le nombre de fois que le produit tentera de communiquer avec un périphérique.
6. Indiquez si vous souhaitez effectuer l'action sur les périphériques dans la Liste des périphériques ciblés ou sur tous les périphériques du groupe **Tous les périphériques**.
7. Pour arrêter de surveiller tous les périphériques, sélectionnez **Ne jamais envoyer une commande Ping aux périphériques**.
8. Cliquez sur **Appliquer**.

Seul le dernier groupe des périphériques ciblés est surveillé. Par exemple, si vous sélectionnez le périphérique A et le périphérique B, et appliquez sur ces périphériques la surveillance de périphérique, le serveur principal enverra une commande Ping uniquement aux périphériques A et B. Si vous sélectionnez ensuite un périphérique C et D, puis appliquez sur ces derniers la surveillance de périphérique, seuls les périphériques C et D seront surveillés. Les périphériques A et B ne sont plus surveillés.

Configuration d'alertes

Utilisation 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 des actions spécifiques. Utilisez ce chapitre pour comprendre comment les alertes fonctionnent.

Comment afficher les alertes ?

Ce produit peut vous notifier des problèmes ou d'autres événements d'ordinateur en :

- Ajoutant des informations au fichier journal
- Envoyant par courrier électronique un avertissement ou en envoyant un message par téléavertisseur
- Exécutant un programme sur un serveur principal ou sur un périphérique individuel
- Envoyant une trappe SNMP à une console de gestion SNMP sur le réseau
- Redémarrant ou arrêtant un périphérique

N'oubliez pas que certaines alertes attribuées à des groupes d'ordinateurs peuvent simultanément gérer un nombre important de réponses. Vous pouvez, par exemple, configurer l'alerte “Modification de la configuration de l'ordinateur” et l'associer à une action de courrier électronique. Si un correctif de distribution de logiciel est appliqué aux ordinateurs utilisant cette configuration d'alerte, un nombre de messages électroniques provenant du serveur principal égal au nombre d'ordinateurs auxquels ce correctif a été appliqué est généré, "inondant" potentiellement votre serveur de messagerie. Dans ce cas, il est préférable d'écrire cette alerte dans le journal principal au lieu d'envoyer des messages électroniques.

Quels types de problèmes de périphérique créent des alertes ?

Ce produit contient une longue liste des événements qui peuvent générer des alertes. Certains problèmes exigent votre attention immédiate ; d'autres sont des modifications de configuration qui peuvent correspondre ou pas à un problème mais qui fournissent des informations utiles à un administrateur système. (Pour obtenir des informations connexes, reportez-vous à la section "Surveillance des modifications de configuration". Des alertes peuvent uniquement être générées

lorsque les périphériques sont équipés du matériel approprié. Par exemple, les alertes générées par des lectures de capteurs ne s'appliquent qu'aux périphériques équipés des capteurs corrects.

Les types d'événements que vous pouvez potentiellement surveiller incluent les types suivants :

- **Modification du matériel :** Un composant tel qu'un processeur, une mémoire, un lecteur ou une carte a été ajouté ou supprimé.
- **Application ajoutée ou supprimée :** Une application a été installée ou désinstallée d'un périphérique.
- **Événement de service :** Un service été démarré ou arrêté sur le périphérique.
- **Performance :** Un seuil de performance a été franchi, tel qu'une capacité de lecteur, la mémoire disponible, etc.
- **Événement IPMI :** Un événement détectable sur les périphériques IPMI s'est produit, y compris des modifications apportées aux contrôleurs, capteurs, journaux, etc.
- **Utilisation du modem :** Le modem du système a été utilisé ou un modem a été ajouté ou supprimé.
- **Sécurité physique :** Une détection d'intrusion de châssis, des cycles d'alimentation ou une autre modification physique s'est produite.
- **Installation de paquet** : Un paquet a été installé sur l'ordinateur cible.
- **Activité du contrôle distant :** Une activité d'une session de contrôle distant s'est produite, y compris un démarrage, un arrêt ou des échecs.

Une surveillance de matériel qui génère des alertes dépend des possibilités du matériel installé sur un périphérique, ainsi que sur la configuration correcte du matériel. Par exemple, si un disque dur avec des fonctions de surveillance S.M.A.R.T. est installé sur un périphérique, mais si la détection S.M.A.R.T n'est pas activée dans les paramètres BIOS du périphérique, ou si le BIOS du périphérique ne prend pas en charge les lecteurs S.M.A.R.T., aucune alerte ne sera générée via la surveillance de lecteur S.M.A.R.T.

Configuration des niveaux de sécurité pour les événements

Les événements ou problèmes de périphériques peuvent être associés à certains ou tous les niveaux de sécurité indiqués ci-dessous.

- **Informationnel :** Prend en charge les événements ou modifications de configuration que les fabricants peuvent inclure dans leurs systèmes. Ce niveau de gravité n'affecte pas la santé du périphérique.
- **OK :** Indique que l'état est à un niveau acceptable.
- **Avertissement :** Fournit des avertissements avant qu'un problème atteigne un point critique.
- **Critique :** Indique que le problème exige votre attention immédiate.
- **Inconnu :** L'état de l'alerte ne peut pas être déterminé ou l'agent de surveillance n'a pas été installé sur le périphérique.

Selon la nature de l'événement ou le problème du serveur, certains niveaux de sécurité ne s'appliquent pas et ne sont pas inclus. Par exemple, avec l'événement de détection d'intrusion, le châssis du périphérique est ouvert ou fermé. S'il est ouvert, une alerte indiquant la gravité Avertissement peut être créée. D'autres événements, tels que Espace disque et Mémoire virtuelle, incluent trois niveaux de sévérité (OK, Avertissement et Critique).

Vous pouvez sélectionner le seuil ou niveau de sévérité qui déclenche des alertes. Par exemple, vous pouvez sélectionner des actions différentes pour un état d'alerte Avertissement ou Critique. L'état Inconnu ne peut pas être sélectionné pour déclencher une alerte, mais il indique simplement que l'état ne peut pas être déterminé.

Processus pour la configuration d'ensembles de règles d'alerte personnalisés

Vous pouvez configurer un ensemble de règles d'alerte pour déployer un périphérique individuel ou un groupe de périphériques ciblés. Avant de pouvoir envoyer des alertes au serveur principal, chaque périphérique géré doit disposer du composant de surveillance. (Pour plus d'informations, reportez-vous à la section "Configuration des agents".)

Lorsque le composant de surveillance est installé sur un périphérique géré, un ensemble de règles d'alertes par défaut est inclus pour fournir des commentaires sur l'état de la santé à la 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)

Outre l'ensemble de règles par défaut, vous pouvez configurer et déployer des ensembles de règles d'alertes personnalisées. Vous pouvez inclure des actions d'alertes personnalisées pour répondre à un événement particulier. Par exemple, si un ventilateur s'arrête, une alerte est déclenchée et un message électronique est envoyé à votre groupe de maintenance de matériel.

Le processus général de création et de déploiement d'un ensemble de règles d'alerte est le suivant :

1. Sélectionnez les périphériques vers lesquels déployer l'ensemble de règles et cliquez sur **Cibler** pour les ajouter à la liste **Périphériques ciblés**.
2. Créez des ensembles de règles d'action d'alerte à utiliser. Ces ensembles de règles d'action définissent les types d'actions déclenchées par les alertes. (Pour plus d'informations, reportez-vous à la section "Configuration d'actions d'alerte").
3. Créez votre ensemble de règles d'alerte personnalisé Durant cette création, vous pouvez sélectionner les actions que vous avez précédemment définies. (Pour plus d'informations, reportez-vous à la section "Configuration d'un ensemble de règles d'alerte".)
4. Déployer l'ensemble de règles sur les périphériques ciblés. Vous pouvez cibler des périphériques supplémentaires avant de déployer l'ensemble de règles. (Pour plus d'informations, reportez-vous à la section "Déploiement d'ensembles de règles".)

L'exemple suivant est un exemple simple de ce processus.

Exemple : Configuration d'un ensemble de règles d'alerte pour un problème d'espace disque

1. Dans le volet de navigation de gauche, cliquez sur **Mes périphériques**, puis cliquez deux fois sur le groupe **Tous les périphériques**.
2. Sélectionnez les périphériques pour lesquels vous souhaitez définir l'alerte, puis cliquez sur **Cibler** pour placer les périphériques dans la liste **Périphériques ciblés**.
3. Cliquez sur **Alerte**, puis cliquez sur l'onglet **Ensembles de règles des actions**.
4. Dans la liste déroulante **Actions**, sélectionnez l'action à configurer (telle que **Envoyer un message électronique/radiomessage**). Cliquez sur **Nouveau**, renseignez le champ **Nom**, puis cliquez sur **OK**.
5. Retournez à la page **Ensembles de règles des actions**, sélectionnez l'ensemble de règles nommé précédemment, puis cliquez sur **Modifier les actions**. Spécifiez la date suivant les besoins dans les zones de texte. Une fois terminé, cliquez sur **Enregistrer**.
6. Cliquez sur l'onglet **Ensembles de règles d'alerte**.
7. Cliquez sur **Nouveau**, entrez une information du type "Problème d'espace disque" dans le champ **Nom**, entrez une description dans le champ **Description**, puis cliquez sur **OK**.
8. Cliquez sur l'ensemble de règles que vous venez de créer puis cliquez sur **Modifier l'ensemble de règles**.
9. Cliquez sur le bouton **Nouveau**.
10. Dans la liste déroulante **Type d'alerte**, cliquez sur **Espace disque**.
11. Cochez l'état pour lequel vous souhaitez envoyer une alerte : **OK**, **Avertissement** ou **Critique**. (Si vous souhaitez déclencher une action identique pour plusieurs états, sélectionnez-en plusieurs. Si vous souhaitez déclencher une action différente pour chaque état, créez une configuration distincte pour chaque état afin de déclencher des actions différentes pour des niveaux d'état différents.)
12. Dans la liste déroulante **Action**, sélectionnez l'action qui est effectuée si les conditions spécifiées aux étapes 6 et 7 sont satisfaites. Si l'action que vous souhaitez sélectionner n'est pas dans la liste, vous pouvez la créer en utilisant la page **Ensembles de règles des actions**. (Si vous n'avez pas créé un ensemble de règles d'action d'alerte, elle ne sera pas dans la liste.)
13. Dans la liste déroulante **Action d'alerte**, sélectionnez la configuration que vous souhaitez utiliser.
14. Cochez l'option **Affecte la santé du périphérique**, si vous souhaitez que l'alerte s'applique à l'état de santé du serveur lorsqu'il est affiché dans dans la liste **Tous les périphériques**. Si le niveau de gravité de l'alerte est uniquement **Informationnel**, l'alerte n'affectera pas la santé du périphérique.
15. Cliquez sur **Ajouter**.
16. Si vous souhaitez ajouter des alertes supplémentaires à l'ensemble de règles, répétez les étapes 6 à 12.
17. Une fois terminé, cliquez sur **Fermer**.
18. Si vous souhaitez modifier des types d'alerte dans l'ensemble de règles, sélectionnez le type d'alerte et cliquez sur **Modifier**, apportez les modifications, cliquez sur **Mettre à jour**, puis cliquez sur **Fermer**.
19. Une fois l'ensemble de règles d'alerte défini, appliquez-le aux périphériques ciblés : cliquez sur **Déployer l'ensemble de règles**, sélectionnez l'ensemble de règles, puis cliquez sur **Déployer**.

Configuration d'actions d'alerte

Utilisez la page **Ensembles de règles des actions** pour fournir des informations supplémentaires sur le comportement des actions sélectionnées. Lorsqu'un seuil est franchi, une alerte est générée. Vous pouvez associer une action à l'alerte, telle que l'envoi d'un message électronique. Chaque action dispose de ses propres configurations et doit être configurée individuellement.

Pour créer un ensembles de règles des actions

1. Dans le volet de navigation de gauche, cliquez sur **Alerte**, puis cliquez sur l'onglet **Ensembles de règles des actions**.
2. Dans la liste déroulante **Actions**, sélectionnez l'action à configurer. Chaque action dispose de sa propre liste de configurations uniques.
3. Cliquez sur **Nouveau**, renseignez le champ **Nom**, puis cliquez sur **OK**.
4. Retournez à la page **Ensembles de règles des actions**, sélectionnez l'ensemble de règles nommé précédemment, puis cliquez sur **Modifier les actions**.
5. Si vous avez sélectionné **Exécuter le programme sur le serveur principal** ou **Exécuter le programme sur le client**, entrez ou collez le chemin du programme à exécuter avec l'alerte, puis cliquez sur **Enregistrer**. Lorsque vous sélectionnez une des actions **Exécuter un programme**, notez que les programmes peuvent ne pas s'afficher comme prévu sur le bureau. Lorsque le programme est exécuté, il est démarré comme un service dans Windows et ne s'affiche donc pas comme une application normale. Il n'est pas nécessaire que les programmes exécutés de cette manière utilisent une interface utilisateur qui requiert une interaction. Pour déterminer de manière définitive si le programme est exécuté, consultez Windows Task Manager.

   Si vous avez sélectionné **Envoyer un message électronique/radiomessage**, entrez l'adresse électronique complète du destinataire du message dans le champ **Destinataire**, entrez une adresse électronique valide dans le champ **Expéditeur**, entrez un objet dans le champ **Objet**, entrez un message dans le champ **Message**, sélectionnez le jour ou l'heure à laquelle vous souhaitez envoyer le message et entrez l'emplacement d'un serveur SMTP dans le champ **Serveur SMTP**. Cliquez sur la case **Aide** pour obtenir plus d'informations sur l'envoi de messages à plusieurs destinataires et sur l'utilisation des variables dans vos messages. Une fois terminé, cliquez sur **Enregistrer**.

   Si vous avez sélectionné **Envoyer une trappe SNMP**, entrez le nom d'hôte, sélectionnez une version, entrez une chaîne de communauté dans la zone **Chaîne de communauté**, puis cliquez sur **Enregistrer**.

Remarques

- Certaines alertes attribuées à des groupes d'ordinateurs peuvent simultanément gérer un nombre important de réponses. Vous pouvez, par exemple, configurer l'alerte “Modification de la configuration de l'ordinateur” et l'associer à une action de courrier électronique. Si un correctif de distribution de logiciel est appliqué aux ordinateurs utilisant cette configuration d'alerte, un nombre de messages électroniques provenant du serveur principal égal au nombre d'ordinateurs auxquels ce correctif a été appliqué est généré, "inondant" potentiellement votre serveur de messagerie. Dans ce cas, il est préférable d'écrire cette alerte dans le journal principal au lieu d'envoyer des messages électroniques.
- Certaines actions d'alerte n'affectent pas la santé du périphérique. Ces actions incluent Exécuter le programme sur le client, Arrêter/Redémarrer, et toute alerte à l'état Informationnel uniquement. Toutefois, si une de ces actions est combinée avec d'autres actions d'alerte qui affectent la santé des périphériques, toute alerte générée affecte la santé du périphérique et s'affiche dans le fichier journal d'alertes).
- Le champ **Expéditeur** d'un message électronique doit contenir une adresse valide pour que l'alerte SMTP fonctionne.
- Les trappes SNMP identifiées comme étant de la version 1 sont traitées, alors que celles identifiées comme étant de la version 3 sont uniquement transférées.
- Les niveaux de gravité des trappes SNMP sont indiqués dans le champ Type de trappe spécifique. Les valeurs sont 1 = inconnu, 2 = infos, 3 = OK, 4 = avertissement, 5 = critique.

Configuration d'un ensemble de règles d'alerte

Pour créer un nouvel ensemble de règles d'alerte, utilisez la page **Ensembles de règles d'alerte**. Avant de pouvoir configurer des alertes, vous devez configurer des actions. (Pour plus d'informations, reportez-vous à la section "Configuration d'actions d'alerte").

Deux ensembles de règles d'alerte s'affichent par défaut dans la page **Ensembles de règles d'alerte** :

- **Ensemble de règles d'alerte du serveur principal** : cet ensemble de règles assure que les alertes sont envoyées au serveur principal lorsque la fonction **Surveillance de périphérique** est activée (voir Surveillance de la connectivité). Cet ensemble de règles contient un groupe prédéfini de types d'alertes, y compris les types Device Monitor, AMT Circuit Breaker Alert et Serial Over LAN Session. Vous pouvez modifier l'état, l'action, le déclenchement d'alerte et les paramètres de santé des types principaux. Toute autre modification ne sera pas prise en charge.
- **Ensemble de règles par défaut** : cet ensemble de règles est déployé sur tous les périphériques gérés et contient un certain nombre de types d'alerte d'utilisation générale pour la plupart des administrateurs de réseau. Vous pouvez modifier cet ensemble de règles pour ajouter d'autres types d'alerte et modifier les paramètres des types d'alerte par défaut. Chaque fois que vous modifiez cet ensemble de règles, les modifications sont déployées sur tous les périphériques gérés, même si vous ne redéployez pas explicitement l'ensemble de règles.

En plus de ces ensembles de règles, vous pouvez créer des ensembles de règles personnalisés qui s'appliquent aux groupes ciblés des périphériques gérés. Ces ensembles de règles doivent être générés au format XML pour qu'ils puissent s'afficher dans la **Configuration d'agent**.

Lorsque vous créez un ensemble de règles personnalisé pour un périphérique, notez que si un ensemble de règles par défaut à déjà été déployé sur un périphérique, les règles d'alerte peuvent se chevaucher ou être en contradiction. Si vous déployez l'ensemble de règles par défaut lorsque vous configurez le périphérique géré, puis déployez un ensemble de règles personnalisé, les deux ensembles de règles seront exécutés sur le périphérique. Par exemple, si les deux ensembles de règles génèrent des alertes pour le même type d'alerte mais prennent des mesures distinctes, vous pouvez en conséquence avoir des actions d'alerte en double ou imprévisibles. Il est impossible de supprimer l'ensemble de règles par défaut une fois déployé, toutefois vous pouvez le modifier.

Pour créer un ensemble de règles d'alerte

1. Dans le volet de navigation de gauche, cliquez sur **Alerte**, puis cliquez sur l'onglet **Ensembles de règles d'alerte** (si nécessaire).
2. Cliquez sur **Nouveau**, renseignez le champ **Nom**, entrez une description de l'alerte dans le champ
   Description, puis cliquez sur **OK**.
3. Cliquez sur l'ensemble de règles que vous venez de nommer et cliquez sur **Modifier l'ensemble de règles**.
4. Cliquez sur **Nouveau**.
5. Dans la liste déroulante **Type d'alerte**, sélectionnez le composant, l'action ou le type d'événement pour lequel vous souhaitez recevoir des alertes.
6. Cochez chaque état pour lequel vous souhaitez envoyer une alerte : **Informationnel**, **OK**, **Avertissement** ou **Critique**. Par exemple, pour recevoir une alerte si le type sélectionné à l'étape 5 franchit un seuil critique, cochez **Critique**.
7. Dans la liste déroulante **Action**, sélectionnez l'action qui est effectuée si les conditions spécifiées aux étapes 5 et 6 sont satisfaites. Ces actions sont configurées au préalable ; si vous souhaitez utiliser une action qui ne se trouve pas dans la liste, vous pouvez en créer une à l'aide de la page **Ensembles de règles des actions**.

   Remarque : Certaines alertes attribuées à des groupes d'ordinateurs peuvent simultanément gérer un nombre important de réponses. Vous pouvez, par exemple, configurer l'alerte "Modification de la configuration de l'ordinateur" et l'associer à une action de courrier électronique. Si un correctif de distribution de logiciel est appliqué aux ordinateurs utilisant cette configuration d'alerte, un nombre de messages électroniques provenant du serveur principal égal au nombre d'ordinateurs auxquels ce correctif a été appliqué est généré, "inondant" potentiellement votre serveur de messagerie. Dans ce cas, il est préférable d'écrire cette alerte dans le journal principal au lieu d'envoyer des messages électroniques.

8. Sélectionnez une configuration dans la liste déroulante **Action d'alerte**. Il se peut qu'il n'y ait qu'une seule configuration disponible (le contenu de cette liste change en fonction de votre sélection à l'étape 7.)
9. Cochez l'option **Affecte la santé du périphérique**, si vous souhaitez que l'alerte s'applique à l'état de santé du serveur lorsqu'il est affiché dans dans la liste **Tous les périphériques**. Si le niveau de gravité de l'alerte est uniquement **Informationnel**, l'alerte n'affectera pas la santé du périphérique.

10. Cliquez sur **Ajouter**.
11. Répétez les étapes 5 à 10 pour ajouter des alertes supplémentaires à l'ensemble de règles.
12. Une fois terminé, cliquez sur **Fermer**.

Pour modifier un ensemble de règles, sélectionnez-le (étape 3) et cliquez sur **Modifier l'ensemble de règles**, puis passez aux étapes ci-dessous.

Quelques minutes après la création ou la modification d'un ensemble de règles, le service de déploiement d'ensemble de règles tente automatiquement de mettre à jour tous les ordinateurs vers lesquels cet ensemble de règles avait été déployé auparavant. Ou, si vous voulez déployer l'ensemble de règles immédiatement, cliquez sur l'onglet **Déployer l'ensemble de règles** et cliquez sur **Déployer**.

Déploiement d'ensembles de règles

Utilisez la page **Déployer un ensemble de règles** pour déplacer l'ensemble de règle d'alerte sélectionné vers les périphériques ciblés.

Vous devez d'abord installer un agent de gestion sur un périphérique géré avant de lui déployer un ensemble de règles. Quand vous déployez l'agent de gestion standard, l'ensemble de règles par défaut est également déployé. Une fois l'agent configuré, vous pouvez mettre à jour ou déployer de nouveaux ensembles de règles. Tout d'abord, il est recommandé de cibler les périphériques auxquels vous souhaitez envoyer l'ensemble de règles d'alerte.

Pour déployer un ensemble de règles d'alerte

1. Dans le volet de navigation de gauche, cliquez sur **Mes périphériques**, puis cliquez sur le groupe **Tous les périphériques**.
2. Sélectionnez les périphériques vers lesquels déployer l'ensemble de règles d'alerte, puis cliquez sur **Cibler** pour placer les périphériques dans la liste **Périphériques ciblés**.
3. Dans le volet de navigation de gauche, cliquez sur **Alerte**, puis cliquez sur l'onglet **Déployer l'ensemble de règles**.
4. Dans la case **Ensemble de règles d'alerte**, sélectionnez l'ensemble de règles d'alerte à déployer.
5. Cliquez sur le lien pour afficher la liste des périphériques ciblés. Pour supprimer un périphérique de cette liste, sélectionnez-le avec le bouton droit puis cliquez sur **Supprimer**. Pour supprimer tous les périphériques, sélectionnez-en un avec le bouton droit puis cliquez sur **Réinitialiser**. Pour ajouter des périphériques, vous devez les ajouter à la liste des périphériques ciblés (étapes 1 à 2 ci-dessus).
6. Fermez la fenêtre **Liste des périphériques ciblés** et cliquez sur **Déployer** pour leur déployer la configuration sélectionnée.

En tant que partie du processus de déploiement, la page XML est créée et répertorie les ensembles de règles déployés et les périphériques vers lesquels les ensembles de règles ont été déployés. Ce rapport est enregistré sur le serveur principal dans le répertoire \ldlogon\alertrules et est nommé avec un numéro séquentiel attribué par la base de données. Si vous souhaitez afficher cette page XML séparément du déploiement d'un ensemble de règles, cliquez sur le bouton **Générer XML**, puis cliquez sur le lien pour afficher le fichier XML.

Notez qu'un seul ensemble de règles ne peut être appliqué à la fois sur un périphérique géré. Si vous avez déployé un ensemble de règles personnalisé sur un périphérique et que vous lui en déployez un autre, le premier ensemble est écrasé et le deuxième est pris en compte.

Affichage des ensembles de règles d'alerte pour un périphérique

Utilisez la page **Ensembles de règles d'alertes** pour afficher une liste des ensembles de règles d'alertes attribués au périphérique sélectionné et pour afficher les détails de chaque alerte.

Pour afficher des ensembles de règles d'alerte

1. Dans la vue **Mes périphériques**, cliquez deux fois sur le périphérique que vous souhaitez configurer. La console d'informations du serveur s'ouvre dans une autre fenêtre de navigateur.
2. Dans le volet de navigation de gauche, cliquez sur **Ensembles de règles**.
3. Cliquez sur l'onglet **Ensembles de règles d'alerte**.

Les détails suivants sont fournis sur chaque ensemble de règles. Pour plus d'informations sur la modification de ces détails, reportez-vous à la section Utilisation des alertes.

- **Lorsque l'état atteint :** Lorsque l'état de l'alerte atteint l'état affiché, une alerte est générée.
- **Affecte la santé :** Indique si l'état de l'alerte s'applique à l'état de santé du serveur lorsqu'il est affiché dans la liste **Tous les périphériques**.
- **Nom de l'ensemble de règles :** Le nom de l'ensemble de règles d'alerte, comme défini dans la boîte de dialogue Ensembles de règles d'alerte.
- **Type d'alerte :** Une description de la source d'alerte (matériel, logiciel, événement, etc).
- **Configuration d'action :** L'action qui se produit lorsqu'une alerte est générée, comme définie dans la boîte de dialogue Configurations d'action.
- **Gestionnaire d'alertes :** Le type d'alerte à générer, tel que message électronique, trappe SNMP ou exécution d'un programme.
- **Instance :** Indique la source spécifique de l'alerte.

Vous pouvez également cliquer sur le bouton **Journal d'alertes** pour passer au journal d'alerte du périphérique et afficher des détails sur les alertes. (Pour plus d'informations, reportez-vous à la section Affichage du journal d'alertes.)

Affichage du journal d'alertes

Utilisez la page **Journal d'alertes** pour consulter les alertes envoyées au serveur principal (journal d'alertes global) ou aux périphériques gérés. Le fichier journal est organisé par Heure (Heure de Greenwich, GMT), l'alerte la plus récente s'affichant au début du journal.

Le Journal d'alertes contient les colonnes suivantes :

- **Nom de l'alerte :** Le nom associé à l'alerte, comme défini dans la page **Configurations d'alerte**.
- **Heure :** La date et l'heure de création de l'alerte (Heure de Greenwich, GMT).
- **Etat :** L'état de l'alerte, qui peut être :
  - **Inconnu :** L'état ne peut pas être déterminé.
  - **Informationnel :** Prend en charge les événements ou modifications de configuration que les fabricants peuvent inclure dans leurs systèmes.
  - **OK :** Indique que l'état est à un niveau acceptable.
  - **Avertissement :** Fournit des avertissements avant qu'un problème atteigne un point critique.
  - **Critique :** Indique que le problème exige votre attention immédiate.
- **Instance :** Indique la source spécifique de l'alerte.
- **Nom de périphérique :** Le nom du périphérique sur lequel l'alerte a été créée. Il doit s'agir d'un nom de domaine pleinement qualifié. (Journal d'alerte globale uniquement.)
- **Adresse IP :** Le nom de l'adresse IP du périphérique sur lequel l'alerte a été créée. (Journal d'alerte globale uniquement.)

Si le nom de périphérique ne s'affiche pas comme un nom de domaine pleinement qualifié, le produit n'a pas pu résoudre le nom de domaine pleinement qualifié pour le périphérique.

Pour afficher le journal d'alertes globales

1. Dans le volet de navigation de gauche, cliquez sur **Journaux**.
2. Pour organiser les entrées par heure, nom, état ou instance, cliquez sur un en-tête de colonne.
3. Pour une description détaillée, double-cliquez l'alerte dans la colonne **Nom de l'alerte**.
4. Pour afficher les entrées de journal par nom, état ou instance, sélectionnez le filtre souhaité dans la liste déroulante. Par exemple, sélectionnez **Nom de l'alerte** et entrez un nom complet (tel que Performance) ou un nom partiel avec le caractère générique * (tel que Distant*). Pour rechercher par date, sélectionnez **Activer le filtre de date**, entrez les dates initiale et finale puis cliquez sur **Rechercher.**
5. Pour effacer l'état d'intégrité d'une alerte, cliquez sur le chiffre indiqué dans la colonne **Nom de l'alerte**, cliquez sur **Effacer l'alerte**, et cliquez sur **OK**. Pour supprimer une entrée du journal, sélectionnez l'alerte et cliquez sur **Supprimer l'entrée**.
6. Pour supprimer toutes les entrées dans le fichier journal, cliquez sur **Purger le journal**.

Pour afficher le journal d'alertes d'un périphérique spécifique

1. Cliquez deux fois sur le périphérique dans la liste **Mes périphériques**.
2. Dans le volet de navigation de gauche, cliquez sur **Informations système**.
3. Cliquez sur **Journaux**, puis cliquez deux fois sur **Journal d'alertes**.
4. Pour organiser les entrées par heure, nom, état ou instance, cliquez sur un en-tête de colonne.
5. Pour une description détaillée, cliquez sur l'alerte dans la colonne **Nom de l'alerte**.
6. Pour répertorier les entrées du journal par nom, état ou instance, cliquez sur le bouton **Filtre** de la barre d'outils et sélectionnez les critères du filtre. Par exemple, sélectionnez **Nom de l'alerte** et entrez un nom complet (tel que Performance) ou un nom partiel avec le caractère générique * (tel que Distant*). Cliquez sur le bouton Rechercher de la barre d'outils pour afficher les alertes associées aux options de filtre que vous avez choisies.

7. Pour afficher les entrées du journal pour une plage de dates, désélectionnez la case **Afficher les événements pour toutes les dates** et sélectionnez une plage de dates. Cliquez sur **Actualiser** pour afficher les entrées correspondant à cette plage de dates.

Mises à jour de logiciel

System Manager inclut un outil de mises à jour de logiciel qui permet de rechercher les mises à jour des logiciels de gestion, des logiciels du système d'exploitation et des pilotes du périphérique. Vous pouvez télécharger ces types de mises à jour et corriger les périphériques affectés en déployant et installant les mises à jour appropriées (également appelées correctifs).

Ce chapitre traite des sujets suivants :

Présentation des mises à jour de logiciel

L'outil des mises à jour de logiciel vous permet de vous assurer que le logiciel des périphériques gérés du réseau est à jour. Vous pouvez automatiser les processus répétitifs de maintenance des logiciels actuels, du téléchargement des fichiers de mise à jour appropriés et de déploiement et installation des mises à jour nécessaires sur les périphériques affectés.

Ce produit utilise l'administration standard basée sur les rôles pour permettre aux utilisateurs d'accéder à l'outil des mises à jour de logiciel. L'administration basée sur les rôles est le modèle de sécurité et d'accès du produit qui permet aux administrateurs de limiter l'accès aux outils et aux périphériques. Chaque utilisateur reçoit des portées et des droits spécifiques qui déterminent quelles fonctions ils peuvent utiliser et quels périphériques ils peuvent gérer. Un administrateur attribue ces droits aux autres utilisateurs (pour obtenir plus d'informations, reportez-vous à la section Présentation de l'administration basée sur les rôles). Pour utiliser l'outil des mises à jour de logiciel, un utilisateur doit se connecter avec les droits Patch Management, Console Web de base et Rapports.

Plates-formes de serveur prises en charge

Les mises à jour de logiciel prennent en charge la plupart des plates-formes de serveur standard, ce qui permet d'effectuer une analyse pour déterminer la présence de mises à jour et de les déployer vers des serveurs gérés qui exécutent les systèmes d'exploitation suivants :

- Windows 2000 Server SP4
- Windows 2000 Advanced Server SP4
- Windows 2000 Professional SP4

- Windows 2003 Standard Edition SP1
- Windows 2003 Enterprise Edition SP1
- Windows XP Pro SP2
- RedHat Enterprise Linux ES/AS 3
- SUSE Linux Server 9 (Professional, Enterprise et Advanced)

Présentation de la fenêtre Mises à jour de logiciel

Les utilisateurs dotés du droit Patch Management peuvent voir l'outil **Mises à jour de logiciel** dans le volet de navigation de gauche de la console. Lorsque vous cliquez sur **Mises à jour de logiciel**, une barre d'outil et deux volets apparaissent à droite de la fenêtre. Le volet de gauche affiche une vue hiérarchique des groupes de mises à jour de logiciel. Cliquez sur un groupe pour afficher son contenu dans le volet de droite. Le volet de droite affiche des détails sur les définitions de mise à jour de logiciel dans une liste organisée par colonne. Le bouton **Rechercher**, situé dans la partie supérieure du volet, permet de rapidement rechercher les critères spécifiés. Dans la zone **Recherche**, les caractères étendus suivants ne sont pas pris en charge : <, >, ', ", !.

Boutons de la barre d'outils

- **Mettre à jour :** Ouvre la boîte de dialogue **Mise à jour de paramètres de vulnérabilités**, qui permet de spécifier les plates-formes et langues pour lesquelles vous souhaitez actualiser les informations de mise à jour de logiciel. Vous pouvez également placer des mises à jour dans le groupe **Analyser**, télécharger simultanément les correctifs associés, spécifier l'emplacement du téléchargement des correctifs et sélectionner les paramètres de serveur proxy.
- **Planifier le téléchargement :** Ouvre la tâche de téléchargement dans la boîte de dialogue **Tâche planifiée** qui permet de configurer les options des tâches. Lorsque vous cliquez sur **Enregistrer**, la tâche de téléchargement est placée dans la fenêtre **Tâches planifiées** sous l'onglet **Tâches de vulnérabilités**.
- **Planifier des tâches de correctif :** Ouvre la boîte de dialogue **Planifier l'analyse de vulnérabilités** qui permet de nommer et de configurer les options du scanner.
- **Actualiser :** Met à jour la liste du volet de droite avec les dernières informations de mise à jour téléchargées.
- **Purger :** Ouvre la boîte de dialogue **Purger les définitions de sécurité et de correctif** qui permet de spécifier les plates-formes et langues pour lesquelles vous souhaitez supprimer les informations de vulnérabilité de la base de données principale.

Volet de gauche (arborescence)

Le volet de gauche de la fenêtre affiche les groupes suivants :

- **Analyser :** Répertorie toutes les mises à jour recherchées lorsque l'outil des mises à jour de logiciel est exécuté sur les périphériques gérés. En d'autres termes, si une mise à jour est incluse dans ce groupe, elle fera partie de la prochaine opération d'analyse ; autrement elle ne fait pas partie de l'analyse.

  L'état Analyser est considéré comme un des trois états de vulnérabilité, avec les états Ne pas Analyser et Non attribuée. Ainsi, une mise à jour de logiciel ne peut résider que dans l'un de ces trois groupes à tout moment. Une mise à jour est identifiée par uneicône unique pour chaque état : un icône avec un point d'interrogation (?) pour Non attribuée, un icône X rouge pour Ne pas analyser et un icône de vulnérabilité normale pour Analyser. Le déplacement d'une mise à jour d'un groupe à un autre modifie automatiquement son état.

  Pour déplacer des mises à jour de logiciel d'un groupe à un autre, cliquez avec le bouton droit sur la mise à jour et sélectionnez le groupe vers lequel les déplacer.

  En déplaçant les mises à jour de logiciel dans le groupe Analyser, vous pouvez contrôler la nature et la taille spécifiques de la prochaine analyse de mise à jour de logiciel.

  De nouvelles mises à jour de logiciel peuvent aussi être automatiquement ajoutées au groupe Analyser durant une mise à jour en cochant l'option **Placer les nouvelles définitions dans le groupe Analyser** de la boîte de dialogue **Mise à jour de paramètres de vulnérabilités**.

  Avertissement concernant le déplacement de mises à jour de logiciel à partir du groupe Analyser
  Lors du déplacement de mises à jour de logiciel du groupe Analyser vers le groupe Ne pas analyser, les informations présentes dans la base de données principale relatives aux périphériques analysés ayant détecté ces mises à jour de logiciel sont supprimées de la base de données et ne sont plus disponibles dans la boîte de dialogue Propriétés des mises à jour de logiciel ni dans la boîte de dialogue Informations du serveur analysé. Pour restaurer ces informations d'évaluation, vous devez déplacer à nouveau les mises à jour de logiciel vers le groupe Analyser et exécuter une nouvelle analyse.

- **Ne pas analyser :** Répertorie les mises à jour de logiciel non recherchées la prochaine fois que le scanner est exécuté sur les périphériques. Comme mentionné ci-dessus, si une mise à jour est présente dans ce groupe, elle ne peut pas être dans le groupe Analyser ou Non attribuée Vous pouvez déplacer des mises à jour vers ce groupe afin de les supprimer d'une analyse de mise à jour de logiciel.

- **Détecté :** Répertorie toutes les mises à jour de logiciel détectées par l'analyse précédente, pour tous les périphériques cibles inclus dans cette tâche d'analyse. Le contenu de ce groupe est toujours déterminé par la dernière analyse de mise à jour de logiciel, que l'analyse porte sur un périphérique ou sur plusieurs.

  La liste Détectée est composée de toutes les mises à jour de logiciel détectées trouvées par l'analyse la plus récente. Les colonnes Analysé et Détecté sont utiles pour afficher le nombre de périphériques ayant été analysés et le nombre de périphériques sur lesquels la mise à jour de logiciel a été détectée. Pour afficher uniquement les serveurs disposant d'une mise à jour de logiciel détectée, cliquez avec le bouton droit sur la définition puis sélectionnez **Afficher les ordinateurs affectés**. Notez que vous pouvez également afficher les informations sur les mises à jour d'un serveur spécifique dans sa boîte de dialogue Console d'informations du serveur.

  Vous pouvez uniquement déplacer des mises à jour de logiciel du groupe Détectée vers le groupe Non attribuée ou Ne pas analyser.

- **Non attribuée :** Répertorie toutes les mises à jour de logiciel qui n'appartiennent pas aux groupes Analyser ou Ne pas analyser. Le groupe Non attribuée est essentiellement une zone de stockage des mises à jour de logiciel collectées jusqu'à ce que vous décidiez de les analyser ou non.

  Par défaut, les mises à jour de logiciel collectées sont ajoutées au groupe Analyser lors d'une mise à jour.

  Vous pouvez déplacer des mises à jour de logiciel du groupe Non attribuée vers le groupe Analyser ou Ne pas analyser.

- **Afficher par SE :** Répertorie toutes les mises à jour de logiciel téléchargées organisées par sous-groupes de systèmes d'exploitation de périphériques spécifiques. Ces sous-groupes aident à identifier les mises à jour de logiciel par catégorie de système d'exploitation. Vous pouvez utiliser ces sous-groupes de système d'exploitation pour copier un ensemble de mises à jour de logiciel dans le groupe Analyser pour une analyse spécifique à un système d'exploitation.

  Les mises à jour de logiciel peuvent être copiées d'un groupe de systèmes d'exploitation vers le groupe Analyser, Ne pas analyser ou Non attribuée. Les mises à jour de logiciel peuvent résider simultanément dans plusieurs groupes de plates-formes et/ou produits.

- **Afficher par Produit :** Répertorie toutes les mises à jour de logiciel téléchargées organisées par sous-groupes de produits spécifiques. Ces sous-groupes aident à identifier les mises à jour de logiciel par catégorie de produit. Vous pouvez utiliser ces sous-groupes de produits pour copier des mises à jour de logiciel dans le groupe Analyser pour une analyse spécifique à un produit.

Volet de droite (liste)

Le volet de droite de la fenêtre affiche les détails suivants des mises à jour de logiciel et les affiche dans des colonnes pouvant être triées :

- **ID :** Identifie la mise à jour grâce à un code alphanumérique unique défini par le fournisseur.
- **Gravité :** Indique le niveau de gravité de la mise à jour. Les niveaux de gravité incluent : Service Pack, Critique, Elevée, Moyenne, Faible, Sans objet et Inconnue.
- **Titre :** Décrit la nature ou cible de la mise à jour dans une brève chaîne de texte.
- **Langue :** Indique la langue du système d'exploitation affecté par la mise à jour.
- **Date de publication :** Indique la date à laquelle la mise à jour a été publiée par le fournisseur.
- **Installation silencieuse :** Indique si le correctif associé à la mise à jour s'installe en mode silencieux (sans interaction de l'utilisateur). Certaines mises à jour peuvent avoir plusieurs correctifs. Si un des correctifs d'une mise à jour ne s'installe pas en mode silencieux, l'attribut Installation silencieuse de la mise à jour spécifie Non.
- **Peut être réparé :** Indique si la mise à jour peut être réparée par installation et déploiement d'un fichier de correctif. Les valeurs possibles sont : Oui, Non et Quelques (pour une mise à jour qui inclut plusieurs règles de détection et toutes les mises à jour détectées ne peuvent pas être réparées).

Cliquez deux fois sur l'ID de mise à jour pour afficher des informations plus détaillées sur sa boîte de dialogue de propriétés. A partir d'une boîte de propriétés de mise à jour de logiciel, vous pouvez afficher les règles de détection de la mise à jour, télécharger les correctifs associés et cliquer sur la règle pour afficher sa boîte de dialogue détaillée des propriétés.

Configuration des périphériques pour l'analyse des mises à jour de logiciel

Avant que des périphériques gérés puissent être analysés pour déterminer la présence de vulnérabilités et recevoir des déploiements de correctif, l'agent Mises à jour de logiciel doit être installé sur ceux-ci.

La méthode la plus simple de déploiement de l'agent Mises à jour de logiciel vers plusieurs périphériques Windows consiste à créer une configuration d'agent, avec l'agent Mises à jour de logiciel sélectionné (configuration par défaut), puis de planifier la configuration pour les périphériques cible souhaités via **Tâches planifiées**.

Lorsque vous configurez un périphérique pour la prise en charge des mises à jour de logiciel, les fichiers nécessaires pour l'analyse et la correction de mises à jour de logiciel (déploiement et installation de correctifs) sont installés sur le périphérique cible.

Mise à jour des définitions de mise à jour de logiciel

Le réseau est constamment vulnérable aux problèmes de maintenance ordinaires tels que les mises à jour de logiciel et les corrections de bogues. L'outil des mises à jour de logiciel simplifie et accélère le processus de collecte des informations les plus récentes concernant les correctifs connus en permettant de mettre à jour les logiciels via une base de données hébergée par LANDesk. Ce service consolide les mises à jour de logiciel connues auprès de sources d'industrie/fournisseur approuvées.

En établissant et en gérant les informations à jour de correctifs, vous pouvez mieux comprendre la nature et l'étendue des mises à jour de logiciel requises pour chaque système d'exploitation de

serveur que vous prenez en charge. La première étape consiste à obtenir les informations de mise à jour connues les plus récentes.

Vous pouvez configurer et effectuer des mises à jour de logiciel sur le champ ou créer une tâche de mise à jour planifiée à exécuter à une heure définie ou en tant que tâche récurrente.

Pour mettre à jour des informations de mise à jour de logiciel

1. Dans le volet de navigation de gauche, cliquez sur **Mises à jour de logiciels**. (Pour obtenir une description de la boîte de dialogue, reportez-vous à la section Présentation de la fenêtre Mises à jour de logiciel.)
2. Cliquez sur le bouton **Mettre à jour** de la barre d'outils.
3. Sélectionnez le site source de téléchargement dans la liste des serveurs de contenu disponibles.
4. Sélectionnez les plates-formes pour lesquelles mettre à jour les informations de mise à jour de logiciel. Vous pouvez sélectionner une ou plusieurs plates-formes dans la liste. Plus le nombre de plates-formes sélectionnées est élevé, plus longue sera la mise à jour.
5. Sélectionnez les langues pour lesquelles mettre à jour les informations de mise à jour de logiciel pour les plates-formes spécifiées. Vous pouvez sélectionner une ou plusieurs langues dans la liste. Plus le nombre de langues sélectionnées est élevé, plus longue sera la mise à jour.
6. Si vous souhaitez que les nouvelles définitions de mises à jour de logiciel (celles n'existant pas déjà dans la base de données) soient automatiquement placées dans le groupe Non attribuée au lieu de l'emplacement par défaut qui est le groupe Analyser, ne cochez pas la case **Placer les nouvelles définitions dans le groupe Analyser**.
7. Si vous souhaitez télécharger automatiquement les fichiers exécutables du correctif actuel, cochez la case **Télécharger les correctifs pour les définitions sélectionnées ci-dessus**, puis cliquez sur une des options de téléchargement.

    - **Pour les définitions détectées uniquement :** Télécharge uniquement les correctifs associés aux mises à jour de logiciel détectées par la dernière analyse de mises à jour de logiciel (par exemple, les mises à jour qui résident actuellement dans le groupe Détectées).
    - **Pour toutes les définitions référencées :** Télécharge TOUS les correctifs associés aux mises à jour de logiciel qui résident actuellement dans le groupe Analyser. Cela peut prendre un certain temps.

Les correctifs sont téléchargés vers l'emplacement spécifié dans la section Paramètres du correctif de la boîte de dialogue (voir les étapes ci-dessous).

8. Si vous disposez sur le réseau d'un serveur proxy utilisé pour des transmissions Internet externes (requises pour la mise à jour d'informations de mise à jour de logiciel et le téléchargement de correctifs), cliquez sur l'onglet **Paramètres du Proxy** et cochez la case **Utiliser le serveur proxy**. Spécifiez l'adresse du serveur, le numéro de port et les références d'authentification si une connexion est requise pour accéder au serveur proxy.
9. Cliquez sur **Appliquer** à tout moment pour enregistrer vos paramètres.
10. Cliquez sur le bouton **Mettre à jour maintenant** pour exécuter la mise à jour de logiciel. La boîte de dialogue **Mise à jour des définitions de sécurité et de correctifs** affiche l'opération actuelle et son état.
11. Une fois la mise à jour terminée, cliquez sur **Fermer**. Notez que si vous cliquez sur **Annuler** avant la fin de la mise à jour, seules les informations des mises à jour déjà traitées sont téléchargées dans la base de données principale. Pour obtenir le reste des informations, vous devrez à nouveau exécuter la mise à jour.

Remarque : Ne fermez pas la console durant un processus de mise à jour, faute de quoi ce dernier prendra fin. Ceci ne s'applique pas à une tâche de téléchargement planifiée.

Si System Manager et LANDesk® Management Suite sont installés sur le même serveur principal, les deux produits utilisent le même fichier de paramètres pour déterminer les types de vulnérabilités mis à jour. Dans certains cas, des mises à jour de System Manager ne sont configurables qu'à partir de Management Suite lorsque vous exécutez la mise à jour. Par exemple, si vous avez sélectionné Menaces de sécurité comme option de mise à jour dans Management Suite et que vous choisissez de mettre à jour l'outil Mises à jour de logiciel dans System Manager, les mises à jour de logiciel et les menaces de sécurité s'affichent alors dans les éléments mis à jour lorsque vous exécutez la mise à jour dans System Manager.

Pour configurer l'emplacement de téléchargement des correctifs

1. Dans la boîte de dialogue **Mise à jour de paramètres de vulnérabilités**, cliquez sur l'onglet **Paramètres du correctif**.
2. Entrez le chemin UNC de l'emplacement vers lequel copier les fichiers de correctif. L'emplacement par défaut est le répertoire \LDLogon\Patch du serveur principal.
3. Si le chemin UNC saisi est un emplacement autre que le serveur principal, entrez un nom d'utilisateur et un mot de passe valides pour l'authentification auprès de cet emplacement.

   Les partages de fichiers et Web doivent être activés sur le dossier, de même que l'accès anonyme.

4. Entrez l'URL Web via laquelle les serveurs peuvent accéder aux correctifs téléchargés pour le déploiement. L'URL Web doit correspondre au chemin UNC ci-dessus.
5. Vous pouvez cliquer sur le bouton **Tester les paramètres** pour vérifier si une connexion peut être établie avec l'adresse Web spécifiée ci-dessus.
6. Si vous souhaitez restaurer le chemin UNC et l'URL Web sur leur emplacement par défaut, cliquez sur **Réinitialiser les paramètres du correctif**. L'emplacement par défaut est le répertoire \LDLogon\Patch du serveur principal.

Planification des téléchargements des mises à jour de logiciel

Vous pouvez également configurer des mises à jour de logiciel en tant que tâche planifiée devant se produire automatiquement à une heure définie ou en tant que tâche récurrente. Pour ce faire, cliquez sur le bouton **Planifier le téléchargement** de la barre d'outils pour ouvrir la boîte de dialogue **Propriétés de la tâche planifiée** qui permet de nommer la tâche et de configurer ses options. Lorsque vous cliquez sur **Enregistrer**, la tâche s'affiche dans la fenêtre Tâches planifiées.

Toutes les tâches de mises à jour de logiciel planifiées utilisent les paramètres actuels de la boîte de dialogue **Mise à jour des paramètres de vulnérabilités**. Ainsi, si vous souhaitez modifier les paramètres de site source, de plate-forme, de langue, de site de téléchargement de correctifs ou de serveur proxy pour une tâche de mise à jour donnée, vous devez d'abord modifier ces paramètres dans la boîte de dialogue **Mise à jour des paramètres de vulnérabilités** avant d'exécuter la tâche.

Pour configurer une tâche de planification de téléchargement

1. Dans le volet de navigation de gauche, cliquez sur **Mises à jour de logiciels**.
2. Cliquez sur **Planifier le téléchargement**.
3. Dans la page **Planifier une tâche**, configurez la planification.
4. Cliquez sur **Enregistrer**.

Lorsque vous cliquez sur **Planifier un téléchargement**, une tâche est créée (elle ne dispose d'aucun périphérique ciblé et elle n'est pas planifiée). Si vous annulez la procédure des **Tâches planifiées**, n'oubliez pas qu'une tâche a été créée et qu'elle apparaît dans la liste **Mes tâches**.

Affichage des informations sur les mises à jour de logiciel et les règles de détection

Une fois les mises à jour de logiciel actualisées à l'aide des dernières informations du service de sécurité LANDesk, vous pouvez afficher les listes des mises à jour de logiciel dans la console, par plate-forme et produit, et déplacer les mises à jour vers différents groupes d'état. Pour plus d'informations sur les différents groupes dans la fenêtre et sur leur utilisation, reportez-vous à la section Présentation de la fenêtre Mises à jour de logiciel, plus haut dans ce chapitre.

Pour afficher plus de détails sur la mise à jour de logiciel, cliquez deux fois sur une ID des mises à jour de logiciel pour l'ouvrir et afficher sa boîte de dialogue des propriétés. Cette boîte de dialogue permet également d'accéder aux détails de la règle de détection en cliquant deux fois sur un nom de fichier de correctif dans la liste **Règles de détection** pour ouvrir la boîte de dialogue des propriétés du correctif (voir Boîte de dialogue Propriétés du correctif).

Ces informations peuvent vous aider à déterminer les mises à jour significatives pour les plates-formes de serveur prises en charge du réseau, comment les règles de détection d'une mise à jour vérifient la présence d'une vulnérabilité, quels correctifs sont disponibles et comment vous voulez configurer et exécuter une correction pour les périphériques affectés.

Vous pouvez également afficher les informations de définition de mise à jour et de règle de détection spécifiques à des périphériques analysés directement à partir de la console en accédant à la console d'information de serveur depuis **Mes périphériques**, et en cliquant sur **Mises à jour de logiciel** dans le volet de navigation de gauche.

Purge des informations des mises à jour de logiciel

Vous pouvez purger des informations de mise à jour de logiciel de la fenêtre des mises à jour de logiciel (et par la suite de la base de données principale) si vous déterminez qu'elles ne concernent plus votre environnement.

Lorsque vous purgez des informations de mise à jour de logiciel, les informations de la règle de détection associée sont également supprimées de la base de données. Toutefois, les fichiers exécutables du correctif actuel ne sont pas supprimés par ce processus. Les fichiers du correctif doivent être supprimés manuellement du référentiel local, qui est généralement situé sur le serveur principal.

Pour purger des informations des mises à jour de logiciel

1. Cliquez sur le bouton **Purger** de la barre d'outils. (Pour obtenir une description de la boîte de dialogue, reportez-vous à la section Boîte de dialogue Purger les définitions de sécurité et de correctifs.)
2. Sélectionnez les plates-formes pour lesquelles supprimer les informations de mise à jour de logiciel. Vous pouvez sélectionner une ou plusieurs plates-formes dans la liste.

   Si une mise à jour est associée à plusieurs plates-formes, vous devez sélectionner toutes ses plates-formes associées afin de pouvoir supprimer les informations de la mise à jour.

3. Sélectionnez les langues pour lesquelles supprimer les informations de mise à jour (associée à la plate-forme spécifiée ci-dessus).

   Si vous sélectionnez une plate-forme Windows ci-dessus, il est recommandé de spécifier les informations de mise à jour de langue à supprimer. Si vous sélectionnez une plate-forme UNIX ci-dessus, vous devez spécifier l'option Langue neutre afin de supprimer les informations de mise à jour multilingues.

4. Cliquez sur **Supprimer**.

Analyse des périphériques pour des mises à jour de logiciel

L'estimation des mises à jour de logiciel consiste à comparer les versions actuellement installées des fichiers et des clés de registre spécifiques à des systèmes d'exploitation sur un périphérique aux mises à jour de logiciel les plus courantes afin d'identifier les besoins d'actualisation des serveurs. Après avoir vérifié les informations de mise à jour de logiciel connues (mises à jour à partir des sources de l'industrie) et décidé des mises à jour pour lesquelles effectuer une analyse, vous pouvez effectuer une estimation personnalisée sur les périphériques gérés qui disposent de l'agent Mises à jour de logiciel. (Pour plus d'informations sur la configuration de périphériques pour l'analyse et le déploiement de correctifs, reportez-vous à la section "Configuration des périphériques pour l'analyse des mises à jour de logiciel", plus haut dans ce chapitre.)

Lorsque le scanner de mises à jour logiciel est exécuté, il lit toujours le contenu du groupe Analyser et effectue une analyse de ces mises à jour spécifiques. Avant d'effectuer une analyse de mises à jour sur les serveurs, assurez-vous que les mises à jour de logiciel à analyser sont incluses dans ce groupe. Vous pouvez déplacer les mises à jour de logiciel vers et à partir du groupe Analyser pour personnaliser la taille et la nature d'une analyse.

Exécution du scanner des mises à jour de logiciel

Le scanner des mises à jour de logiciel peut être poussé vers des périphériques sous forme de tâche d'analyse planifiée depuis la console.

Pour créer une tâche d'analyse de mise à jour de logiciel

1. Dans le volet de navigation de gauche, cliquez sur **Mises à jour de logiciels**.
2. Assurez-vous que les définitions de mise à jour de logiciel ont été récemment mises à jour.

3. Assurez-vous que le groupe Analyser contient uniquement les mises à jour pour lesquelles effectuer une analyse.
4. Cliquez sur le bouton **Planifier des tâches de correctif** de la barre d'outils. (Pour obtenir une description de la boîte de dialogue, reportez-vous à la section "Boîte de dialogue Planifier l'analyse de vulnérabilités".)
5. Entrez un nom unique pour l'analyse. Si le script de tâche existe déjà, vous pouvez choisir d'écraser le script existant.
6. Spécifiez si vous souhaitez que le scanner des mises à jour de logiciel affiche une boîte de dialogue de progression sur le périphérique cible. Vous pouvez également spécifier si vous voulez que le bouton Annuler s'affiche dans la boîte de dialogue du scanner pour que l'utilisateur final puisse annuler l'analyse si souhaité.
7. Spécifiez la méthode de fermeture de la boîte de dialogue du scanner des mises à jour de logiciel une fois que l'exécution sur les périphériques cibles est terminée. Vous pouvez exiger l'intervention de l'utilisateur final ou vous pouvez configurer la boîte de dialogue pour qu'elle se ferme après une période d'inactivité déterminée.
8. Cliquez sur **OK**.
9. Sélectionnez la tâche dans le volet inférieur (sous **Tâches de vulnérabilité**) et cliquez sur **Modifier**. Configurez les paramètres de ciblage et de planification, puis cliquez sur **Enregistrer**.

Affichage des mises à jour détectées

Si le scanner des mises à jour de logiciel découvre des mises à jour pour des mises à jour de logiciel activées sur des périphériques cibles, ces informations sont transmises au serveur principal et ajoutées à la liste **Détectée**.

Vous pouvez utiliser une des méthodes suivantes pour afficher les mises à jour détectées après l'exécution d'une analyse de mises à jour de logiciel :

Par le groupe Détectée

Sélectionnez le groupe **Détectée** dans la fenêtre des mises à jour de logiciel pour afficher une liste complète de toutes les mises à jour détectées par l'analyse la plus récente.

Par périphérique individuel

Cliquez deux fois sur un nom de périphérique dans **Mes périphériques**, puis cliquez sur **Mises à jour de logiciel** pour afficher les informations détaillées d'estimation des mises à jour de logiciel de ce périphérique.

Téléchargement de correctifs

Pour déployer des correctifs vers des périphériques sur lesquels des mises à jour de logiciel ont été détectées, le fichier exécutable du correctif doit être d'abord être téléchargé vers un dépôt local de correctifs sur le réseau. L'emplacement par défaut des téléchargements de fichiers de correctif est le répertoire /LDLogon du serveur principal. Vous pouvez modifier cet emplacement dans l'onglet **Paramètres du correctif** de la boîte de dialogue **Mise à jour de paramètres de vulnérabilités**.

Paramètres d'emplacement des téléchargements de correctif et de serveur proxy
Les téléchargements de correctifs utilisent toujours les paramètres d'emplacement de téléchargements actuellement présents dans l'onglet **Paramètres du correctif** de la boîte de dialogue **Mise à jour de paramètres de vulnérabilités**. Notez également que, si le réseau utilise un serveur proxy pour un accès Internet, vous devez d'abord configurer les paramètres du serveur proxy dans l'onglet **Paramètres du proxy** de la boîte de dialogue **Mise à jour de paramètres de vulnérabilités** avant de pouvoir télécharger des fichiers de correctif.

Ce produit tente d'abord de télécharger un fichier de correctif à partir de l'URL affichée dans la boîte de dialogue Propriétés de correctif. Si aucune connexion ne peut être établie, ou si le correctif n'est pas disponible pour une raison quelconque, le produit télécharge le correctif à partir du service de sécurité LANDesk, qui est une base de données hébergée par l'entreprise contenant des correctifs provenant de sources de l'industrie approuvées.

Vous pouvez télécharger un correctif à la fois ou un ensemble de correctifs simultanément.

Pour télécharger des correctifs uniques

1. Cliquez deux fois sur un nom de mise à jour de logiciel pour ouvrir sa boîte de dialogue **Propriétés**.
2. Dans la section **Règles de détection**, sélectionnez les fichiers de correctifs de règle de détection à télécharger, puis cliquez sur **Télécharger les correctifs sélectionnés**.
3. L'opération du téléchargement et son état s'affichent dans la boîte de dialogue **Téléchargement de correctifs**. Vous pouvez à tout moment cliquer sur le bouton **Annuler** pour arrêter le processus entier du téléchargement.
4. Une fois le téléchargement terminé, cliquez sur le bouton **Fermer**.

Pour télécharger plusieurs correctifs

Toutes les tâches de mises à jour de logiciel planifiées utiliseront les paramètres actuels de la boîte de dialogue **Mise à jour des paramètres de vulnérabilités**. Ainsi, si vous souhaitez modifier les paramètres de site source, de plate-forme, de langue, de site de téléchargement de correctifs ou de serveur proxy pour une tâche de mise à jour donnée, vous devez d'abord modifier ces paramètres dans la boîte de dialogue **Mise à jour des paramètres de vulnérabilités** avant d'exécuter la tâche.

1. Dans le volet de navigation de gauche, cliquez sur **Mises à jour de logiciels**.
2. Cliquez sur **Planifier le téléchargement**.
3. Dans la page **Planifier une tâche**, configurez la planification.
4. Cliquez sur **Enregistrer**.

Suppression de fichiers de correctif

Pour supprimer des fichiers de correctif, vous devez supprimer manuellement les fichiers du référentiel de correctifs, qui correspond en général au répertoire LDLogon du serveur principal.

Correction des mises à jour de logiciel

Une fois que vous avez mis à jour les définitions des mises à jour de logiciels, placé les mises à jour pour lesquelles effectuer une analyse dans le groupe Analyser, exécuté une analyse sur les périphériques gérés, déterminé les mises à jour de logiciel requérant une intervention et téléchargé les correctifs nécessaires, l'étape suivante consiste à effectuer une correction des mises à jour de logiciel en déployant et en installant les correctifs nécessaires sur les périphériques affectés.

La correction des mises à jour de logiciel est effectuée par mise à jour de logiciel individuelle. En d'autres termes, vous créez une tâche de correction pour une mise à jour de logiciel spécifique qui déploie et installe les correctifs nécessaires.

Notez que la correction, comme l'analyse de mises à jour de logiciel, fonctionne uniquement sur les périphériques ayant été configurés avec l'agent Mises à jour de logiciel. Pour plus d'informations, reportez-vous à la section Configuration des périphériques pour l'analyse des mises à jour de logiciel, plus haut dans ce chapitre.

La correction Linux est prise en charge. Vous pouvez utiliser l'outil Mises à jour de logiciel pour découvrir des vulnérabilités sur les périphériques Linux, puis décider si vous voulez corriger les mises à jour. Si tel est le cas, vous pouvez utiliser un abonnement au fournisseur Red Hat pour télécharger les RPM nécessaires, puis déployer les RPM aux périphériques.

Avertissement : Une fois terminé, de nombreux correctifs redémarreront automatiquement le périphérique.

Pour créer un script de correction personnalisé

1. Dans le volet de navigation de gauche, cliquez sur **Mises à jour de logiciels**.
2. Sélectionnez le groupe **Détectée** pour afficher les mises à jour de logiciel détectées par l'analyse la plus récente. (Il n'est pas obligatoire de sélectionner ce groupe. Si vous souhaitez créer un script de correction personnalisé pour les mises à jour pour lesquelles une analyse n'a pas été effectuée ou qui n'ont pas encore été détectées, cliquez sur tout autre groupe de vulnérabilités pour afficher son contenu et sélectionnez une vulnérabilité spécifique.)
3. Cliquez avec le bouton droit sur la définition, puis sélectionnez **Afficher les périphériques affectés** pour afficher les périphériques affectés par cette mise à jour de logiciel.
4. Cliquez avec le bouton droit sur la définition, puis sélectionnez **Créer une tâche de correction**.
5. (facultatif) Modifiez le nom dans la zone de texte **Nom de la tâche**.
6. Sélectionnez une option, puis cliquez sur **OK**.
    - **Copiez les ordinateurs affectés dans le chariot cible :** Copie les ordinateurs affectés par la mise à jour de logiciel vers le chariot cible pour être corrigés.
    - **Afficher la progression lors de l'exécution :** Active le scanner pour afficher des informations sur les périphériques d'utilisateur final durant son exécution. Cliquez sur cette option si vous souhaitez afficher l'activité du scanner et configurer d'autres options d'affichage et d'interaction dans cette boîte de dialogue. Si vous ne cliquez pas sur cette option, aucune des autres options de cette boîte de dialogue ne peut être configurée et le scanner est exécuté de manière transparente sur les périphériques.

- **Requiert une saisie de la part de l'utilisateur avant la fermeture de la boîte de dialogue d'analyse de vulnérabilités** : Cliquez sur cette option si vous souhaitez que le scanner invite l'utilisateur final à intervenir avant que sa boîte de dialogue d'affichage se ferme sur le périphérique. Si vous sélectionnez cette option, et si l'utilisateur final ne répond pas, la boîte de dialogue principale reste ouverte, ce qui peut entraîner l'expiration d'autres tâches planifiées.
- **Fermer automatiquement la boîte de dialogue après un délai :** Cliquez sur cette option si vous souhaitez que la boîte de dialogue d'affichage du scanner se ferme après une durée spécifiée.

Scripts

Gestion des scripts

Ce produit utilise des scripts pour exécuter des tâches personnalisées sur les périphériques. Le remplissage des boîtes de dialogue de création de script crée un fichier texte ASCII au format INI Windows doté d'une extension .INI. Ces scripts sont stockés sur le serveur principal dans le dossier \Program Files\LANDesk\ManagementSuite\Scripts. Le nom de fichier du script devient le nom du script dans la console. Vous pouvez créer des scripts de planificateur local pour des périphériques Windows dans la fenêtre **Scripts** (cliquez sur **Scripts** dans le volet de navigation de gauche) ou écrir vos propres fichiers de script et les enregistrer dans le dossier Scripts.

La fenêtre **Scripts** divise les scripts en les catégories suivantes :

- **Mes scripts :** Les scripts que vous associez à ce groupe.
- **Tous les autres scripts :** Tous les scripts présents sur le serveur principal.
- **Scripts utilisateur** (visible uniquement aux administrateurs) : Scripts créés par tous les utilisateurs du produit. Ces scripts sont triés par créateur.

Vous pouvez créer des groupes sous l'élément **Mes scripts** afin de classer davantage vos scripts. Pour créer un nouveau script de planificateur local, cliquez sur le bouton **Local**.

Une fois le script créé, vous pouvez cliquer sur **Planifier** dans le menu contextuel du script. Dans la fenêtre **Mes périphériques**, vous pouvez cibler les périphériques sur lesquels la tâche doit être exécutée et vous pouvez planifier l'exécution de cette tâche dans la fenêtre **Tâches planifiées**. Reportez-vous à la section Planification de tâches pour plus d'informations sur la planification des tâches.

Modifications de la propriété de la tâche et du script des utilisateurs des versions précédentes de Management Suite

Dans les versions de Management Suite antérieures à 8.70, tous les scripts étaient globaux et visibles par tous les utilisateurs. Maintenant, les scripts sont uniquement visibles au créateur du script et aux administrateurs.

La fenêtre **Scripts** contient une colonne Etat. La colonne Etat spécifie que l'état est Public si tous les utilisateurs peuvent visualiser le script, ou Privé si seul son auteur et les administrateurs peuvent le visualiser. Pour modifier l'état d'un script, les utilisateurs peuvent cliquer avec le bouton droit sur les scripts qu'ils ont créés et sélectionner Privé ou Public. Les administrateurs peuvent modifier l'état de tout script.

La valeur par défaut est DOS PE. Si vous sélectionnez un autre EP vous ne pourrez pas créer un script de commande. Pour les EP Windows et Linux, vous pouvez uniquement générer un script de déploiement ou de capture.

Si vous choisissez EP Linux, vous ne disposez que des options d'outil de mise en image LANDesk ou Autre. Si vous choisissez EP Windows, vous disposez de LANDesk, Autre et Microsoft* XImage.

Création d'un script du planificateur local

Le planificateur local est un service exécuté sur les périphériques. Il est installé lorsque vous déployez une configuration d'agent comme partie de l'agent de gestion standard. Le planificateur local gère généralement les tâches du produit, telles que l'exécution périodique du scanner d'inventaire. En revanche, les autres tâches planifiées sont gérées par le serveur principal. Le planificateur local permet de planifier vos tâches personnelles qui seront exécutées périodiquement sur les périphériques. Une fois le script du planificateur local créé, déployez-le sur les périphériques gérés de la même manière que les autres scripts.

Le planificateur local affecte un numéro d'identification à chaque tâche. Les scripts du planificateur local utilisent une plage d'ID différente de celle des scripts du planificateur local par défaut employés par le produit. Un seul script de planificateur personnalisé peut être actif sur chaque périphérique. Si vous créez un script et le déployez sur les périphériques, il remplace l'ancien script (n'importe quel script dans la plage d'ID du planificateur local personnalisé) sans affecter les scripts du planificateur local par défaut, tels que la planification d'analyse d'inventaire local.

Lorsque vous sélectionnez les options de planification du script, rappelez-vous des qualités restrictives des options. Si vous sélectionnez par exemple lundi comme jour de la semaine et 17 comme jour du mois, la tâche sera exécutée uniquement un lundi tombant le 17 du mois, ce qui est très rare.

Vous pouvez créer un script pour exécuter le fichier restartmon.exe sur un ordinateur local, immédiatement ou à l'heure que vous désirez. Si un ordinateur n'envoit plus de rapport, vous pouvez utiliser le fichier restartmon.exe se trouvant dans le dossier LDClient pour redémarrer le collecteur et tous les fournisseurs de surveillance. Cet utilitaire ne fonctionne que sur les ordinateurs sur lesquels il a été installé et qui ont cessé d'envoyer des rapports. Utilisez cet utilitaire pour redémarrer le collecteur et les fournisseurs sans redémarrer le périphérique.

1. Dans le volet de navigation de gauche, cliquez sur **Scripts**.
2. Cliquez sur **Local**.
3. Entrez un nom de script.
4. Cliquez sur **Ajouter** pour définir les options de script.
5. Configurez les options du planificateur local comme décrit précédemment. Une fois terminé, cliquez sur **Enregistrer**.
6. Cliquez sur **Enregistrer** pour sauvegarder votre script.
7. Sélectionnez le script dans le groupe **Mes scripts**, puis cliquez sur **Planifier** pour le déployer vers les périphériques.

Présentation des options de bande passante

Lors de la configuration des commandes du planificateur local, vous pouvez spécifier la bande passante minimale du périphérique géré nécessaire à l'exécution de la tâche. Lors du traitement de la tâche, chaque périphérique qui exécute la tâche du planificateur local envoie un trafic réseau ICMP en petite quantité à l'ordinateur spécifié et évalue la performance du transfert. Si l'ordinateur cible n'est pas disponible, la tâche n'est pas exécutée.

Vous pouvez sélectionner les options de bande passante suivantes :

- **RAS :** La tâche s'exécute si la connexion réseau du périphérique à l'ordinateur cible correspond au moins à une vitesse RAS ou de connexion de réseau à distance. En règle générale, la sélection de cette option entraîne l'exécution systématique de la tâche quelle que soit la connexion réseau.
- **WAN :** La tâche s'exécute si la connexion réseau du périphérique à l'ordinateur cible est au moins une vitesse WAN. La vitesse WAN est définie comme une connexion non-RAS plus lente que le seuil LAN.
- **LAN :** La tâche s'exécute lorsque la connexion du périphérique à l'ordinateur cible dépasse le paramètre de vitesse LAN. La vitesse LAN est définie à 262 144 bps par défaut.

Planification de tâches de création de script

La fenêtre **Tâches planifiées** affiche l'état de la tâche planifiée, lorsqu'elle s'exécute et lorsqu'elle se termine. Le service du planificateur communique avec les périphériques de deux manières :

- Via l'agent de gestion standard (qui doit déjà être installé sur les périphériques).
- Via un compte système de niveau de domaine. Le compte que vous choisissez doit disposer de la connexion en tant que privilège de service et vous devez avoir spécifié les références d'authentification dans Configuration des services. Pour plus d'informations sur la configuration du compte Planificateur, reportez-vous à la section "Configuration du service Planificateur".

LANDesk installe plusieurs scripts standard que vous pouvez planifier afin de réaliser des tâches de maintenance de routine telles que l'exécution d'analyses d'inventaire sur des ordinateurs sélectionnés. Cliquez sur **Scripts** dans le volet de navigation de gauche, puis cliquez sur **Tous les autres scripts** pour afficher et planifier ces scripts.

Pour planifier une tâche

1. Dans le volet de navigation de gauche, cliquez sur **Scripts**.
2. Cliquez pour passer au groupe de scripts.
3. Cliquez sur un script, puis cliquez sur **Planifier**.
4. Entrez un nom pour la tâche et cliquez sur **OK**.
5. Dans l'onglet **Tâches de script personnalisé**, cliquez sur **Toutes les tâches**, cliquez sur la tâche nommée à l'étape 3 et cliquez sur **Modifier**.
6. Renseignez les pages de la tâche du script personnalisé. Cliquez sur le bouton Aide pour obtenir plus d'informations sur les pages, ou reportez-vous à l'aide du Planificateur de tâche.

Lorsque vous cliquez sur **Planifier**, une tâche est créée (elle ne dispose d'aucun périphérique ciblé et elle n'est pas planifiée). Si vous annulez cette procédure de planification de tâche, n'oubliez pas qu'une tâche a été créée et qu'elle apparaît dans la liste Tâches.

Utilisation des scripts par défaut

Ce produit est livré avec deux scripts par défaut. Vous pouvez les utiliser pour exécuter certaines tâches typiques. Ces scripts sont disponibles dans l'arborescence **Tous les autres scripts** dans la fenêtre **Scripts** (volet de navigation de gauche | **Scripts**) .

- **Scanner d'inventaire :** Exécute le scanner d'inventaire sur les périphériques sélectionnés. Ce script contient une documentation qui décrit comment écrire un script. Lisez ou imprimez ce fichier pour plus d'informations sur l'utilisation correcte des commandes et paramètres.
- **Restauration des enregistrements de client :** Exécute le scanner d'inventaire sur les périphériques sélectionnés, mais le scanner envoie un rapport au serveur principal depuis lequel le périphérique a été configuré. Si vous devez réinitialiser la base de données, cette tâche vous permet de retourner les périphériques à la base de données de serveur principal appropriée dans un environnement à plusieurs serveurs principaux.

Planification de tâches

L'outil **Tâches planifiées** est utilisé par la configuration d'agent, les mises à jour logicielles, la distribution de logiciel , et la découverte de périphériques. Les tâches sont filtrées dans le volet du bas des pages de fonctions spécifiques pour afficher uniquement les tâches associées. Par exemple, si vous ouvrez l'outil **Découverte de périphériques**, les tâches de découverte s'affichent dans l'onglet **Tâches de découverte** du volet inférieur. Toutes les tâches sont toujours visibles via l'outil **Tâches planifiées**. Ici, vous pouvez planifier l'exécution des configurations pour qu'elle soit immédiate, ultérieure, récurrente ou unique.

Le volet de gauche de la page **Tâches planifiées** affiche les groupes de tâche suivants :

- **Mes tâches :** Les tâches que vous avez planifiées. Seuls vous et les utilisateurs administratifs peuvent visualiser ces tâches.
- **Toutes les tâches :** Vos tâches et les tâches marquées comme étant publiques.
- **Tâches courantes :** Les tâches marquées par l'utilisateur comme étant courantes. Tout individu qui modifie ou planifie une tâche appartenant à ce groupe devient propriétaire de cette tâche. La tâche reste dans le groupe Tâches communes et sera également visible dans le groupe Tâches d'utilisateur de cet utilisateur.
- **Tâches d'utilisateur** (utilisateurs administratifs uniquement) : Tâches créées par des utilisateurs.

Lorsque vous cliquez sur **Mes tâches**, **Tâches courantes** ou **Toutes les tâches**, le volet de droite affiche les informations suivantes :

- **Tâche :** Les noms de tâche.
- **Commencer à :** Spécifie le moment de l'exécution de la tâche. Cliquez sur un nom de tâche, puis cliquez sur **Modifier** pour modifier l'heure de début ou la replanifier.
- **Etat :** L'état global des tâches. Pour plus de détails, affichez la colonne Etat du volet de droite. La colonne du volet de droite affiche l'état de la tâche, qui peut correspondre à Traitement en cours, Tout terminé, Rien de terminé ou Échec.
- **Paquet de distribution :** Le nom du paquet distribué par la tâche. Ce champ s'applique à la distribution de logiciel.
- **Méthode de livraison :** La méthode de livraison utilisée par la tâche. Ce champ s'applique à la distribution de logiciel.
- **Propriétaire :** Le nom de l'individu qui a à l'origine créé le script utilisé par cette tâche.

Lorsque vous cliquez deux fois sur une tâche planifiée, le volet de droite affiche des informations de récapitulatif :

- **Nom :** Le nom de l'état de la tâche.
- **Quantité :** Le nombre de périphériques dans chaque état de tâche.
- **Pourcentage :** Le pourcentage de périphériques dans chaque état de tâche.

Avant de planifier des tâches pour un périphérique, ce dernier doit disposer de l'agent approprié et doit être dans la base de données d'inventaire. Les configurations sont une exception. Elles peuvent cibler un périphérique qui ne dispose pas de l'agent de gestion standard. Les tâches peuvent être replanifiées (modifiées) ou supprimées de l'onglet Tâches. Une fois une tâche planifiée, passez à l'onglet Tâches pour afficher l'état de la tâche.

Pour modifier une tâche, sélectionnez la tâche à modifier et cliquez sur **Modifier**. La tâche s'ouvre et affiche les options de modification applicables à cette tâche.

Groupes de tâches personnalisés

Vous pouvez créer des groupes personnalisés pour les types de tâches **Mes tâches**, **Toutes les tâches**, et **Tâches communes**. Les groupes personnalisés permettent de regrouper les tâches apparentées telles que l'analyse de vulnéralibilités et l'exécution d'un script. Les groupes et les sous-groupes peuvent contenir une vingtaine de catégories.

Pour créer un groupe de tâches personnalisé

1. Dans le volet de navigation de gauche, cliquez sur **Tâches planifiées**.
2. Dans le volet de gauche, cliquez sur le type de tâche pour lequel vous souhaitez créer un groupe.
3. Cliquez sur **Nouveau groupe** sur la barre d'outils.
4. Entrez un nom dans la zone de texte **Nom du groupe** et cliquez sur **OK**

Une fois le groupe personnalisé créé, vous pouvez déplacer ou copier les tâches ou les autres groupes dans le groupe en les sélectionnant dans la liste et en cliquant sur le bouton **Déplacer** de la barre d'outils.

Page Périphériques cible

Utilisez cette page pour ajouter des cibles de périphérique pour la tâche à configurer. Vous pouvez également afficher les périphériques ciblés, les requêtes et les groupes de périphériques de la tâche sur cet onglet. Si plusieurs produits de gestion LANDesk sont installés, les groupes de périphériques créés dans une console de produit peuvent être affichés dans toutes les consoles. Cette page n'est pas nécessaire pour les tâches de découverte de périphériques.

- **Ajouter la liste cible :** Ajoute les périphériques précédemment placés dans la liste cible depuis la liste **Mes périphériques**.
- **Ajouter une requête :** Cible les résultats d'une requête précédemment créée.
- **Supprimer :** Supprime les cibles sélectionnées.

Cette page affiche les groupes de périphériques ciblés, cependant ils ne s'affichent que si LANDesk Management Suite est installé sur le serveur principal. Si vous exécutez Server Manager, System Manager ou la Console Web dans Management Suite, les groupes de périphériques ne sont pas considérés comme des groupes. Toutefois, si vous sélectionnez et ciblez un groupe, les périphériques qu'il contient sont ajoutés dans la liste de périphériques ciblés et s'affichent dans **Périphériques ciblés** au lieu de **Groupes ciblés**.

Page Planifier une tâche

Le Planificateur contient un onglet **Propriétés de la tâche planifiée** qui contient les options suivantes.

- **Laisser non planifié** : (valeur par défaut) Conserve la tâche dans la liste des tâches pour une planification ultérieure.
- **Démarrer maintenant** : Exécute la tâche dès que possible. Le démarrage de la tâche peut prendre une minute, selon les paramètres.
- **Démarrer à une heure prévue** : Démarre la tâche à l'heure spécifiée. Si vous sélectionnez cette option, vous devez entrer les informations suivantes :
  - **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.
  - **Heure** : L'heure de démarrage de la tâche.
  - **Répéter chaque** : Si vous souhaitez répéter la tâche, sélectionnez parmi les options **Toutes les heures**, **Quotidien**, **Hebdomadaire** ou **Mensuel**. Si vous sélectionnez **Mensuel** et que la date n'existe pas dans tous les mois (par exemple, 31), la tâche s'exécute uniquement les mois contenant cette date.
- **Planifier ces périphériques :** La première fois qu'une tâche est exécutée, conservez la valeur par défaut En attente ou en cours d'exécution. Pour les exécutions suivantes, sélectionnez Tous, Périphériques n'ayant pas réussi ou Périphériques n'ayant pas tenté d'exécuter la tâche. Ces options sont expliquées ci-dessous.
  - **Périphériques ayant échoué :** Sélectionnez cette option si vous souhaitez que la tâche soit exécutée uniquement sur tous les périphériques n'ayant pas terminé la tâche la première fois. Cette option exclut les périphériques présentant un état Réussi. Cette tâche sera exécutée sur les périphériques présentant tous les autres états, y compris les états En attente ou Actif. Veuillez considérer utiliser cette option si la tâche doit être exécutée sur autant de périphériques non réussis que possible, mais si elle ne doit se terminer avec succès qu'une seule fois par périphérique.
  - **En attente ou en cours d'exécution :** Choisissez cette option pour exécuter la tâche sur les périphériques qui vont être exécutés ou ceux qui le sont déjà.
  - **Tout :** Sélectionnez cette option si vous souhaitez que la tâche soit exécutée sur tous les périphériques, quel que soit l'état. Veuillez considérer utiliser cette option si vous disposez d'une tâche, en particulier une tâche récurrente, qui doit être exécutée sur autant de périphérique que possible.
  - **Périphériques n'ayant pas tenté d'exécuter la tâche :** Sélectionnez cette option si vous souhaitez que la tâche soit exécutée uniquement sur les périphériques n'ayant pas terminé et n'ayant pas échoué la tâche. Cette option exclut les périphérique présentant l'état Désactivé, Occupé, Echoué ou Annulé. Veuillez considérer utiliser cette option si un beaucoup de périphériques cible n'ayant pas exécuté la tâche avec succès ne sont pas des cibles importantes.

Page Scripts personnalisés

- **Script personnalisé actuellement sélectionné :** Sélectionnez le script à planifier.

Rapports

Présentation des rapports

System Manager inclut un outil d'édition de rapports qui permet de créer divers types de rapports spécialisés qui fournissent des informations critiques sur les périphériques gérés du réseau.

System Manager emploie un utilitaire d'analyse d'inventaire pour ajouter des périphériques (et collecter les données de logiciel et de matériel relatives à ces périphériques) à 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. L'outil des rapports bénéficie davantage de ces données d'inventaire analysées en collectant et organisant ces données sous forme de rapports utiles.

Vous pouvez utiliser les rapports de parc d'inventaire et les rapports de service prédéfinis. Après l'exécution d'un rapport, vous pouvez l'afficher dans la console.

Si Server Manager et Management Suite sont installés ensemble, les rapports exécutés dans Server Manager incluront uniquement des serveurs. Si vous exécutez une requête, vous obtiendrez des serveurs et d'autres périphériques, à moins que votre requête n'ait été configurée pour exclure les autres périphériques.

Si la création de rapports d'un ordinateur spécifique est interrompue, vous pouvez utiliser restartmon.exe dans le dossier LDCLIENT pour relancer le programme de collecte et tous les fournisseurs d'application de surveillance. Cet utilitaire est utilisé pour les ordinateurs sur lequel un programme de création de rapport a été installé puis interrompu. Utilisez cet utilitaire pour relancer le programme de collecte et les fournisseurs sans avoir à redémarrer le périphérique.

Présentation de groupes de rapports et de rapports prédéfinis

Les rapports sont organisés en groupes dans la fenêtre **Rapports** (volet de navigation de gauche **| Rapports**). Les administrateurs peuvent visualiser le contenu de tous les groupes de rapports. System Manager inclut un rôle spécifique, appelé Rapports, qui permet à d'autres utilisateurs d'afficher des rapports sans leur donner accès à d'autres fonctions de gestion (Pour plus d'informations, reportez-vous à la section "Administration basée sur les rôles".) Les utilisateurs dotés du droit Rapports peuvent également afficher et exécuter des rapports, mais uniquement sur les périphériques inclus dans leur portée.

La fenêtre **Rapports** contient les groupes de rapports suivants :

- Matériels
- Logiciels

Affichage de rapports

Vous pouvez excuter tout rapport partir de la fentre **Rapports**.

Dans la fentre **Rapports**, cliquez sur un groupe de rapports, puis cliquez sur le rapport excuter. Les donnes du rapport s'affichent dans la vue **Rapport**.

Fentre Rapports

Les rapports vous permettent d'accder rapidement la reprsentation graphique des actifs sur vos ordinateurs client. Les rapports sont crs partir de donnes stockes dans la base de donnes par le scanner. Vous pouvez afficher ou imprimer des rapports partir de votre navigateur.

Pour afficher un rapport

1. Dans le volet de navigation de gauche, cliquez sur **Rapports**. Les catgories de rapports s'affichent dans le volet de droite. Cliquez sur une en-tte de catgorie pour afficher la liste de rapports. Une icne en regard de chaque rapport identifie le type de rapport.

    Un rapport avec une icne reprsentant un diagramme s'affiche sous la forme d'un diagramme ou d'un graphe barres (deux ou trois dimensions). Dans un diagramme, vous pouvez cliquez sur n'importe quelle section colore pour obtenir un rcapitulatif.

    Un rapport avec une icne reprsentant un document s'affiche sous la forme d'un texte.

2. Cliquez sur le nom du rapport pour l'afficher.
3. Pour obtenir un rcapitulatif des dates d'analyse du logiciel ou matriel, cliquez sur les dates de dbut et de fin pour dterminer la plage de date, puis cliquez sur **Excuter**.

Le rapport Rcapitulatif d'espace disque contient uniquement des donnes pour les priphriques Windows.

Pour imprimer un rapport, cliquez avec le bouton droit de la souris sur la page, puis slectionnez **Imprimer**. Dans la bote de dialogue d'impression, cliquez sur **Imprimer**. Si un rapport s'tend sur plusieurs pages, vous devez cliquer avec le bouton droit de la souris sur chaque page pour l'imprimer.

Pour distribuer un rapport

- Pour envoyer un rapport par courrier lectronique, il est recommand d'imprimer le rapport dans un fichier .PDF, puis de l'attacher au message en tant que pice jointe.

La console affiche les diagrammes de rapport sous la forme de diagramme ou de graphe barres. Pour dfinir le type de diagramme, cliquez sur la liste droulante du diagramme de rapport, puis modifiez le type de diagramme.

Pour visualiser les diagrammes et graphes barre interactifs qui s'affichent dans de nombreux rapports, Macromedia Flash Player* 7 doit tre install.

Requêtes

Utilisation de requêtes

Les requêtes sont des recherches personnalisées des bases de données principales. Ce produit fournit des outils qui permettent de créer des requêtes de base de données pour les périphériques dans votre base de données principale. Vous créez les requêtes de base de données principale dans la vue **Requête** de la console. Les requêtes publiques System Manager sont visibles dans LANDesk® Management Suite et vice-versa, si les deux sont utilisés.

Cette section traite des sujets suivants :

Présentation des requêtes

Les requêtes vous aident à gérer le réseau en vous permettant de rechercher et d'organiser les périphériques de la base de données principale en fonction de critères spécifiques au système ou à l'utilisateur.

Par exemple, vous pouvez créer une requête qui capture uniquement les périphériques dotés d'une vitesse d'horloge de processeur inférieure à 166 MHz, ou d'une quantité de mémoire RAM inférieure à 64 Mo ou d'un disque dur d'une taille inférieure à 2 Go. Créez une ou plusieurs instructions de requête qui représentent ces conditions et associez les instructions à l'aide d'opérateurs logiques standard. Lors de l'exécution d'une requête, vous pouvez imprimer ses résultats et accéder aux périphériques correspondants et les gérer.

Groupes de requêtes

Les requêtes peuvent être associées à des groupes dans la vue **Mes périphériques**. Ce sont les groupes dynamiques. Le contenu d'un groupe dynamique est le résultat de la requête associée à ce groupe dynamique. Par exemple, un groupe comprenant tous les périphériques d'une région géographique peut être associé à une requête de taille de disque dur, de mémoire, etc.

Pour plus d'informations sur l'affichage des requêtes et des groupes de requêtes dans la vue **Tous les périphériques**, et sur ce que vous pouvez en faire, reportez-vous à la section "Regroupement des périphériques pour des actions".

Création de requêtes de base de données

Utilisez la boîte de dialogue **Nouvelle requête** pour générer une requête en sélectionnant des attributs, des opérateurs relationnels et des valeurs d'attribut. Générez une instruction de requête en choisissant un attribut d'inventaire et en l'associant à une valeur acceptable. Reliez

logiquement les instructions de requête afin qu'elles soient évaluées en tant que groupe avant de les associer à d'autres instructions ou groupes.

Pour créer une requête de base de données

1. Dans la vue **Requêtes** de la console, cliquez sur **Nouveau**.
2. Sélectionnez un **composant** dans la liste d'attributs d'inventaire.
3. Sous **Etape 1 : Conditions de recherche**, cliquez sur **Modifier**.
    1. Explorez cette liste pour sélectionner les attributs devant former la condition de recherche. Par exemple, pour repérer tous les clients qui exécutent un type particulier de logiciel, vous pouvez sélectionner Computer.Software.Package.Name.
    2. Une fois les attributs sélectionnés, vous pouvez remarquer qu'une série de champs s'affiche sur le côté droit de la fenêtre. A partir de ces champs, sélectionnez un opérateur et une valeur pour renseigner la condition de recherche. Par exemple, pour repérer tous les clients qui exécutent Internet Explorer 5.0, les attributs seraient "Computer.Software.Package.Name", l'opérateur "=" et la valeur "Internet Explorer 5".
    3. Au bas de la fenêtre, cliquez sur **Ajouter** pour renseigner le champ vide avec la condition de recherche.
    4. Vous pouvez continuer à affiner la requête en créant une autre condition de recherche, puis en l'ajoutant à la première à l'aide d'un opérateur booléen (ET ou OU). Utilisez également les boutons pour ajouter, supprimer, remplacer, grouper ou dissocier les conditions que vous créez.
    5. Une fois terminé, cliquez sur **OK**.
4. Sous **Etape 2 : Attributs à afficher**, cliquez sur **Modifier**.
    1. Explorez cette liste pour sélectionner un attribut à afficher dans la liste des résultats de requête. Souvenez-vous de sélectionner des attributs qui vous aident à identifier les clients renvoyés dans la requête. Si vous ne pouvez pas trouver des attributs à afficher, vous pouvez les ajouter dans la boîte de dialogue Attributs personnalisés. Toutefois, ces attributs doivent être attribués à des ordinateurs avant qu'ils puissent s'afficher dans la boîte de dialogue de requête.

    2. Une fois un attribut sélectionné, cliquez sur **Ajouter** pour le déplacer vers le champ vide au bas de la fenêtre. Si vous souhaitez énumérer la liste des résultats de requête, cliquez sur **Inclure le nombre**.
    3. Si vous souhaitez ajouter d'autres attributs, répétez cette procédure. Utilisez le bouton **Supprimer** pour supprimer des attributs, puis cliquez sur **Monter/Descendre** pour modifier l'ordre des attributs.
    4. Cliquez sur **Cibler les résultats** pour cibler les résultats de la requête pour toute action spécifiée.
    5. Une fois terminé, cliquez sur **OK**.
5. (Facultatif) Sous **Etape 3 : Trier les résultats par attribut**, cliquez sur **Modifier** pour personnaliser l'ordre des résultats de la requête.
6. Si vous souhaitez exécuter la requête d'autres fois, cliquez sur **Enregistrer la requête**, et entrez un nom unique pour la requête. Si vous exécutez la requête avant de l'enregistrer, les paramètres de requête sont perdus et doivent être reconstruits pour exécuter à nouveau la même requête.
7. Sous **Etape 4 : Exécuter la requête**, cliquez sur **Exécuter la requête**.

Les instructions de requête sont exécutées dans l'ordre affiché
Si aucun groupement n'est réalisé, les instructions de requête répertoriées dans cette boîte de

dialogue sont exécutées du bas vers le haut. Veillez à grouper les éléments de requête associés afin qu'ils soient évalués en tant que groupe, faute de quoi les résultats de la requête peuvent être différents de ceux attendus.

Exécution de requêtes

Pour exécuter une requête

1. Dans le volet de navigation de gauche, cliquez sur **Requêtes**.
2. Sélectionnez la requête et cliquez sur **Exécuter**.

   ou

   Pour modifier la requête avant de l'exécuter, cliquez deux fois sur la requête, cliquez sur **Modifier**, modifiez les étapes 1 à 3, puis cliquez sur **Exécuter la requête**.

   Remarque : Si vous avez modifié la requête et si vous souhaitez enregistrer vos modifications, cliquez sur **Enregistrer la requête** pour enregistrer les modifications ou sur **Enregistrer la requête sous** pour donner un nouveau nom à la requête modifiée. Réalisez cette tâche avant d'exécuter la requête. Si vous n'enregistrez pas vos modifications avant d'exécuter la requête, les modifications ne seront pas enregistrées avec la requête.

3. Les résultats (périphériques correspondants) s'affichent dans le volet de droite de la vue **Tous les périphériques**.

Importation et exportation de requêtes

Vous pouvez utiliser les fonctions d'importation et d'exportation pour transférer des requêtes d'une base de données principale vers une autre. Les requêtes exportées sont enregistrées en tant que fichiers .XML.

Pour importer une requête

1. Cliquez avec le bouton droit de la souris sur le groupe de requêtes dans lequel placer la requête importée.
2. Sélectionnez **Importer** dans le menu contextuel.
3. Naviguez vers la requête à importer et sélectionnez-la.
4. Cliquez sur **Ouvrir** pour ajouter la requête au groupe sélectionné dans la vue **Tous les périphériques**.

Pour exporter une requête

1. Cliquez avec le bouton droit de la souris sur la requête à exporter.
2. Sélectionnez **Exporter** dans le menu contextuel.
3. Naviguez vers l'emplacement dans lequel enregistrer la requête (en tant que fichier .XML).
4. Entrez un nom pour la requête.
5. Cliquez sur **Enregistrer** pour exporter la requête.

Présentation des requêtes personnalisées

Les requêtes personnalisées sont utiles lorsque vous souhaitez obtenir des détails d'inventaire sur les matériels et les logiciels installés sur les périphériques. Utilisez une requête personnalisée pour générer une liste d'ordinateurs ayant des inventaires similaires. Les requêtes personnalisées sont également utilisées pour définir des groupes et des portées.

La page **Requêtes personnalisées** (cliquez sur **Requêtes** dans le volet de navigation de gauche) affiche une liste des requêtes que vous avez enregistrées. Pour exécuter une requête enregistrée, sélectionnez la requête, puis sélectionnez **Exécuter**.

Si la liste de requêtes s'étend sur plusieurs pages, utilisez les flèches en haut de la page pour passer d'une page à l'autre. Entrez le nombre d'éléments à afficher par page et cliquez sur **Définir**.

Création de requêtes personnalisées

Les requêtes personnalisées sont utiles lorsque vous souhaitez obtenir des détails d'inventaire sur les matériels et les logiciels installés sur les périphériques. Utilisez une requête personnalisée pour générer une liste de périphériques ayant des inventaires similaires. Par exemple, si vous souhaitez mettre à niveau tous les périphériques afin qu'ils utilisent au moins 750 MHz, vous pouvez rechercher tous les périphériques dans la base de données dont la vitesse de processeur est inférieure à 750 MHz. Les requêtes personnalisées sont également utilisées pour définir des groupes et des portées.

Vous pouvez effectuer une requête sur tous les éléments d'inventaire (appelés "attributs") que le scanner d'inventaire stocke dans la base de données, ainsi que sur tout attribut personnalisé.

Gestion des requêtes

Gérez les requêtes dans la vue **Requêtes**. Utilisez cette vue pour créer, modifier ou supprimer des requêtes :

- Pour exécuter une requête existante, sélectionnez-la et cliquez sur **Exécutez**.
- Pour créer une nouvelle requête, cliquez sur **Nouveau**. Une fois la requête créée et enregistrée, son nom apparaît dans la liste figurant sur cette page.
- Pour modifier une requête dans la liste, cliquez deux fois sur celle-ci. La page **Modifier la requête** s'affiche avec des paramètres de requêtes modifiables.
- Pour modifier la requête la plus récente, cliquez sur **Modifier la requête actuelle**.
- Pour supprimer une requête, sélectionnez la requête et cliquez sur **Supprimer**.

La création d'une requête est un processus à quatre étapes :

1. **Création d'une condition de recherche :** Spécifiez un ensemble d'attributs d'inventaire qui formera la base de la requête.
2. **Sélection d'attributs à afficher :**Affinez davantage ou "filtrez" la requête afin que les résultats affichent les attributs les plus utiles, tels que les adresses IP ou les noms de périphérique d'ordinateur.

3. **Tri des résultats par attribut (facultatif) :** Spécifiez la méthode de tri des résultats. (Cette étape est uniquement applicable si, à l'étape 2, vous avez sélectionné d'afficher plus d'un type d'attribut dans les résultats de requête.)
4. **Exécution de la requête :** Exécutez la requête que vous venez de créer. Vous pouvez également l'enregistrer pour une utilisation ultérieure ou effacer toutes ses informations pour redémarrer de zéro.

Etape 1 : Création d'une condition de recherche (obligatoire)

Une condition de recherche est un ensemble d'attributs d'inventaire et de valeurs associées que vous recherchez. Vous pouvez utiliser une condition de recherche ou en grouper plusieurs afin de former la base d'une requête.

La procédure suivante a lieu sur la page **Modifier la requête**. Dans la vue **Exécution des requêtes**, cliquez sur **Nouveau** ou sélectionnez une requête existante et cliquez sur **Modifier**.

Pour créer une condition de recherche

1. A l'**étape 1**, cliquez sur **Modifier**. Une fenêtre affiche une liste qui représente toutes les données d'inventaire actuellement dans la base de données.
2. Explorez cette liste pour sélectionner les attributs devant former la condition de recherche. Par exemple, pour repérer tous les clients qui exécutent un type particulier de logiciel, vous pouvez sélectionner Computer.Software.Package.Name.
3. Une fois les attributs sélectionnés, vous pouvez remarquer qu'une série de champs s'affiche sur le côté droit de la fenêtre. A partir de ces champs, sélectionnez un opérateur et une valeur pour renseigner la condition de recherche. Par exemple, pour repérer tous les clients qui exécutent Internet Explorer 5.0, les attributs seraient "Computer.Software.Package.Name", l'opérateur "=" et la valeur "Internet Explorer 5".
4. Au bas de la fenêtre, cliquez sur **Ajouter** pour renseigner le champ vide avec la condition de recherche.
5. Vous pouvez continuer à affiner la requête en créant une autre condition de recherche, puis en l'ajoutant à la première à l'aide d'un opérateur booléen (ET ou OU). Utilisez également les boutons pour ajouter, supprimer, remplacer, grouper ou dissocier les conditions que vous créez.
6. Une fois terminé, cliquez sur **OK**.

Pour exécuter et stocker une requête sur l'état de santé des serveurs (Computer.Health.State), n'oubliez pas que l'état est représenté par un nombre dans la base de données. Utilisez le tableau ci-dessous pour créer des conditions de recherche. Par exemple, pour créer une condition de recherche pour des ordinateurs dont l'état de santé est "Inconnu", utilisez l'opérateur "NOT EXIST".

Etat de santé	Opérateur
Inconnu	NOT EXIST
Normal	2

Etat de santé	Opérateur
Avertissement	3
Critique	4

Etape 2 : Sélection d'attributs à afficher (obligatoire)

Pour l'étape 2, sélectionnez les attributs qui seront les plus utiles pour identifier les ordinateurs renvoyés dans les résultats de requête. Par exemple, si vous souhaitez des résultats qui vous aident à repérer physiquement chaque ordinateur correspondant à la condition de recherche définie à l'étape 1, vous pouvez spécifier des attributs tels que le nom d'affichage de chaque ordinateur (Computer.DisplayName) ou l'adresse IP (Computer.Network.TCPIP.Address).

La procédure suivante a lieu sur la page **Modifier la requête**.

Pour sélectionner des attributs à afficher

1. A l'**étape 2**, cliquez sur **Modifier**. Une fenêtre affiche une liste qui représente toutes les données d'inventaire actuellement dans la base de données.
2. Explorez cette liste pour sélectionner un attribut à afficher dans la liste des résultats de requête. Souvenez-vous de sélectionner des attributs qui vous aident à identifier les clients renvoyés dans la requête. Si vous ne pouvez pas trouver des attributs à afficher, vous pouvez les ajouter dans la boîte de dialogue Attributs personnalisés. Toutefois, ces attributs doivent être attribués à des ordinateurs avant qu'ils puissent s'afficher dans la boîte de dialogue de requête.

   Remarque : Si vous utilisez une base de données Oracle, assurez-vous de sélectionner au moins un attribut défini de manière native par le scanner d'inventaire (par exemple, Computer.Display Name, Computer.Device Name, Computer.Device ID, Computer.Login Name, etc.).

3. Une fois un attribut sélectionné, cliquez sur **>>** pour le déplacer vers le champ vide sur le côté droit de la fenêtre. Si vous souhaitez énumérer la liste des résultats de requête, cliquez sur **Inclure le nombre**.
4. Si vous souhaitez ajouter d'autres attributs, répétez cette procédure. Utilisez les boutons fléchés pour ajouter ou supprimer des attributs, puis cliquez sur **Monter/Descendre** pour modifier l'ordre des attributs.
5. Cliquez sur **Cibler les résultats** pour cibler les résultats de la requête pour toute action spécifiée.
6. Une fois terminé, cliquez sur **OK**.

Vous pouvez également ajouter un ou plusieurs intitulés de colonne à la liste des résultats de requête.

Pour modifier des intitulés de colonne (facultatif)

1. A l'**étape 2**, cliquez sur **Modifier**.

2. Dans la case du bas, cliquez sur un intitulé de colonne, puis cliquez sur **Modifier**. Modifiez l'intitulé et appuyez sur **Entrée**. Répétez selon les besoins.
3. Cliquez sur **OK**.

A ce stade, vous pouvez souhaiter enregistrer la requête. La procédure suivante du processus de création de requête est facultative et s'applique uniquement aux résultats de requête qui contiennent deux colonnes ou plus. Pour enregistrer la requête, cliquez sur **Enregistrer la requête** en haut de la page. Une fenêtre s'affiche et vous invite à entrer un nom pour cette requête. Entrez un nom, puis cliquez sur **Enregistrer** dans l'angle supérieur droit de la fenêtre.

Etape 3 : Trier les résultats par attribut (facultatif)

Cette procédure est uniquement requise si vous avez défini plusieurs intitulés de colonne et attributs à l'étape 2 et souhaitez maintenant trier les résultats alphabétiquement ou numériquement dans une de ces colonnes.

Par exemple, supposons que vous avez spécifié deux attributs différents à afficher dans les résultats de requête : l'adresse IP et le type de processeur de chaque ordinateur renvoyé. A l'étape 3, vous pouvez trier alphabétiquement les résultats suivant le type de processeur.

Si vous omettez cette étape, la requête est automatiquement triée suivant le premier attribut sélectionné à l'étape 2.

Pour trier les résultats par attribut

1. A l'**étape 3**, cliquez sur **Modifier**. Une fenêtre s'affiche et présente les attributs sélectionnés à l'**étape 2**.
2. Sélectionnez l'attribut suivant lequel effectuer le tri, puis cliquez sur **>>** pour le déplacer vers la zone de texte vide.
3. Cliquez sur **OK**.

Etape 4 : Exécution de la requête

Une fois la requête créée, vous pouvez l'exécuter, l'enregistrer ou l'effacer pour redémarrer à zéro.

Pour enregistrer la requête pour une utilisation ultérieure, cliquez sur le bouton **Enregistrer** de la barre d'outils. La requête figure maintenant dans la liste qui se trouve à la page **Requêtes personnalisées**. Si la requête est une version modifiée d'une autre, cliquez sur le bouton **Enregistrer sous** de la barre d'outils pour lui donner un nouveau nom.

Par défaut, les requêtes enregistrées sont uniquement visibles à la personne les ayant enregistrées. Si vous cochez la case **Requête publique** avant de l'enregistrer, la requête enregistrée sera visible à tous les utilisateurs. Seuls les administrateurs dotés du droit de gestion de requêtes publiques peuvent créer une requête publique.

Si plusieurs familles de produit sont installées, les requêtes sont partagées entre les produits. Si vous enregistrez une requête dans une console de produit, elle sera également visible dans les autres consoles de produit.

Pour afficher les résultats de cette requête, cliquez sur le bouton **Exécuter** de la barre d'outils.

Pour effacer les paramètres de requête à partir de la page **Modifier la requête**, cliquez sur le bouton **Effacer** de la barre d'outils. Si la requête a déjà été enregistrée, elle est effacée de cette page mais est conservée dans la liste **Requêtes personnalisées**.

Affichage des résultats de requête

Les résultats de la requête correspondent aux critères de recherche que vous avez spécifiés dans la procédure de génération de requête. Si les résultats ne sont pas ceux attendus, revenez à la page **Modifier la requête** et affinez les informations.

Pour obtenir plus d'informations sur l'un des périphériques de la liste des résultats de la requête, cliquez deux fois sur les données de requête ou cliquez avec le bouton droit de la souris et sélectionnez **Affichage d'ordinateurs** dans le menu résultant.

A partir de la page **Résultats de la requête**, vous pouvez cliquer sur le bouton **Enregistrer au format CSV** de la barre d'outils pour exporter les résultats dans un format compatible vers un tableur ou une autre application.

Pour imprimer les résultats de la requête, cliquez sur **Imprimer la vue** dans la page des résultats de la requête.

Affichage des résultats de la requête d'exploration

Les résultats de la requête correspondent aux critères de recherche que vous avez spécifiés dans la procédure de génération de requête. Si les résultats ne sont pas ceux attendus, revenez à la page **Modifier la requête** et affinez les informations.

Pour obtenir plus d'informations sur l'un des périphériques de la liste des résultats de la requête, cliquez deux fois sur les données de requête ou cliquez avec le bouton droit de la souris et sélectionnez **Affichage d'ordinateurs** dans le menu résultant.

Exportation de résultats de requête vers des fichiers CSV

Pour afficher les données de résultats de requête dans un tableur, exportez les données en tant que fichier CSV (Comma Separated Values). Dans la page **Résultats de la requête**, cliquez sur **Enregistrer au format CSV** de la barre d'outils pour enregistrer les informations sous forme d'un fichier CSV. Vous pouvez ensuite utiliser une application telle que Microsoft Excel* pour importer et utiliser le fichier CSV.

Modification des intitulés de colonne de recherche

1. Ouvrez une requête existante ou créez une nouvelle requête.
2. Dans la case du bas, cliquez sur un intitulé de colonne, puis cliquez sur **Modifier**. Modifiez l'intitulé et appuyez sur **Entrée**. Répétez selon les besoins.
3. Cliquez sur **OK**.

Exportation et importation de requêtes

Vous pouvez exporter et importer toute requête créée. Toutes les requêtes sont exportées en tant que fichiers XML. Si vous exportez plus d'une fois le même nom de fichier de requête, le fichier existant est écrasé. Pour éviter cela, vous pouvez souhaiter copier le fichier vers un autre emplacement une fois qu'il est exporté.

Les fonctions d'exportation et d'importation sont utiles dans deux scénarios :

- Si vous devez réinstaller votre base de données, utilisez les fonctions d'exportation/importation pour enregistrer les requêtes existantes afin de les utiliser dans une nouvelle base de données.

  Par exemple, vous pouvez exporter les requêtes, puis les déplacer vers un répertoire non affecté par une réinstallation de base de données. Une fois la base de données réinstallée, vous pouvez déplacer à nouveau les requêtes vers le répertoire de requêtes sur le serveur Web, puis les importer dans la nouvelle base de données.
- Vous pouvez utiliser les fonctions d'exportation/importation pour copier des requêtes vers d'autres bases de données.

  Par exemple, vous pouvez exporter une requête vers un répertoire de requêtes sur le serveur Web, puis les envoyer par courrier électronique ou FTP à une autre personne. Cette personne peut ensuite placer les requêtes dans le répertoire de requêtes sur un autre serveur Web, puis les importer dans une base de données différente. Vous pouvez également mapper un lecteur et directement copier les requêtes dans le répertoire de requêtes sur un autre serveur Web.

Pour exporter une requête

Suivez cette procédure en étant connecté à une base de données contenant une requête à exporter.

1. Dans le volet de navigation de gauche, cliquez sur **Requêtes**.
2. Sur la page **Requêtes personnalisées**, cliquez sur le nom de la requête à exporter. Cliquez sur **Modifier**.
3. Sur la page **Modifier la requête** cliquez sur le bouton **Exporter** de la barre d'outils pour exporter la requête vers le disque.
4. Sur la page **Requête exportée**, cliquez avec le bouton droit de la souris sur la requête pour la télécharger en tant que fichier XML vers un répertoire sélectionné. La requête devient le fichier XML.

Veuillez noter que si vous exportez plus d'une fois le même nom de fichier de requête, le fichier existant est écrasé. Pour éviter cela, vous pouvez souhaiter copier le fichier vers un autre emplacement une fois qu'il est exporté.

Si vous souhaitez éventuellement réimporter la requête dans une base de données, vous devez la déplacer vers le répertoire de requêtes reconnu par le serveur Web (par défaut, c:\inetpub\wwwroot\LANDesk\LDSM\queries).

Pour importer une requête

Suivez cette procédure en étant connecté à une base de données dans laquelle importer une requête.

1. Dans le volet de navigation de gauche, cliquez sur **Requêtes**.
2. Sur la page **Requêtes personnalisées**, cliquez sur **Nouveau**.
3. Sur la page **Modifier la requête**, cliquez sur le bouton **Importer** de la barre d'outils.
4. Sélectionnez la requête à importer. Si vous souhaitez vérifier les paramètres de cette requête avant de l'importer, cliquez sur **Afficher**.
5. Cliquez sur **Importer** pour charger la requête dans la page **Modifier la requête**.
6. Une fois la requête chargée, faites défiler et cliquez sur **Enregistrer la requête** pour l'enregistrer dans cette base de données.

Gestion d'inventaire

Vous pouvez utiliser l'utilitaire d'analyse d'inventaire pour ajouter des périphériques à la base de données principale et pour collecter les données relatives aux logiciels et matériels des périphériques. Vous pouvez afficher, imprimer et exporter les données d'inventaire. Vous pouvez également employer cet utilitaire pour définir des requêtes, grouper des périphériques et générer des rapports spécialisés.

Cette section traite des sujets suivants :

Présentation de l'analyse d'inventaire

Lorsque vous configurez un périphérique à l'aide de la fonction de configuration de périphérique, le scanner d'inventaire est l'un des composants installé sur le périphérique. Lors de la création d'une configuration de client, vous pouvez spécifier le moment de l'exécution du scanner d'inventaire sur le périphérique.

Le scanner d'inventaire s'exécute automatiquement lors de la configuration initiale du périphérique. Le fichier exécutable du scanner est nommé LDISCAN32.EXE pour Windows et LDISCAN pour Linux. Le scanner d'inventaire 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. Pour configurer les paramètres d'analyse de logiciel sur le serveur principal, cliquez sur **Démarrer | Programmes | LANDesk | LANDesk Configuration des services**.

Pour plus d'informations sur la configuration du service Inventaire, reportez-vous à la section "Configuration du service Inventaire" de l'Annexe C.

Après l'analyse initiale, le scanner d'inventaire peut être exécuté à partir de la console en tant que tâche planifiée. L'agent de gestion standard doit être exécuté sur les périphériques distants pour planifier une analyse d'inventaire sur eux.

Remarque : Un périphérique ajouté à la base de données principale en utilisant la fonction de découverte n'a pas encore analysé ses données d'inventaire vers la base de données principale. Vous devez exécuter une analyse d'inventaire sur chaque périphérique pour que les données d'inventaire complètes apparaissent pour ce périphérique.

Vous pouvez visualiser les données d'inventaire et les utiliser pour :

- Personnaliser les colonnes de la liste **Tous les périphériques** afin d'afficher des attributs d'inventaire spécifiques
- Interroger la base de données principale sur des serveurs dotés d'attributs d'inventaire spécifiques

- Grouper des périphériques afin de simplifier les tâches de gestion
- Générer des rapports spécialisés basés sur des attributs d'inventaire
- Effectuer un suivi des modifications de matériel et de logiciel sur les périphériques, et générer des entrées de fichier journal ou des alertes lorsque de telles modifications se produisent.

Pour en savoir plus sur le fonctionnement du scanner d'inventaire, lisez les sections ci-dessous.

Analyses d'écart

Une fois que l'analyse complète initiale est exécutée sur un périphérique, la prochaine exécution du scanner d'inventaire capture uniquement les modifications d'écart et les envoie à la base de données principale. Utilisez l'option de scanner /RSS pour collecter des informations sur le logiciel à partir du registre Windows.

Forçage d'une analyse complète

Si vous souhaitez forcer une analyse complète des données de matériel et logiciel du périphérique, vous pouvez supprimer le fichier d'analyse delta existant et modifier un paramètre dans l'applet **Configuration des services logiciel LANDesk**.

1. Supprimez le fichier **invdelta.dat** du serveur. Une copie intégrale de la dernière analyse est stockée localement sous forme d'un fichier masqué nommé invdelta.dat situé à la racine du disque dur. (La variable d'environnement LDMS_LOCAL_DIR du client définit l'emplacement de ce fichier.)
2. Ajoutez l'option **/sync** à la ligne de commande de l'utilitaire du scanner d'inventaire. Pour modifier la ligne de commande, cliquez sur **Démarrer | Programmes | LANDesk Management**, cliquez avec le bouton droit sur l'icône de raccourci **Analyse d'inventaire**, sélectionnez **Propriétés | Raccourci**, puis modifiez le chemin **Cible**.
3. Dans le serveur principal, cliquez sur **Démarrer | Programmes | LANDesk | Configuration des services LANDesk**.
4. Cliquez sur l'onglet **Inventaire**, puis cliquez sur **Paramètres avancés**.
5. Cliquez sur le paramètre **Do Delta**. Dans la zone **Valeur** tapez **0**.
6. Cliquez deux fois sur **OK**, puis cliquez sur **Oui** à l'invite pour relancer le service.

Compression d'analyse

Les analyses d'inventaire réalisées par le scanner d'inventaire Windows (LDISCAN32.EXE) sont compressées par défaut. Le scanner compresse les analyses complètes et d'écart avec un taux de compression d'environ 8:1. Les analyses sont d'abord entièrement générées en mémoire, puis compressées et envoyées au serveur principal en utilisant une taille de paquet élevée. La compression d'analyse requiert un nombre de paquets plus faible et réduit l'utilisation de bande passante.

Codage d'analyse

Les analyses d'inventaire sont codées (analyses TCP/IP uniquement) Vous pouvez désactiver le codage d'analyse d'inventaire en modifiant un paramètre dans l'applet Configuration des services LANDesk.

1. Dans le serveur principal, cliquez sur **Démarrer | Programmes | LANDesk | Configuration des services LANDesk**.
2. Cliquez sur l'onglet **Inventaire**, puis cliquez sur **Paramètres avancés**.
3. Cliquez sur le paramètre **Disable Encryption**. Dans la zone **Valeur** tapez **1**.
4. Cliquez sur **Définir**, puis cliquez sur **OK**.
5. Cliquez sur **OK**, puis cliquez sur **Oui** à l'invite pour relancer le service.

Affichage des données d'inventaire

Une fois un périphérique analysé par le scanner d'inventaire, vous pouvez afficher ses informations système dans la console.

Les inventaires de périphérique sont stockés dans la base de données principale et incluent des informations sur les matériels, les pilotes de périphérique, les logiciels, la mémoire et l'environnement. Vous pouvez utiliser l'inventaire pour vous aider à gérer et configurer les périphériques, ainsi que pour identifier rapidement les problèmes système.

Vous pouvez afficher les données d'inventaire des manières suivantes :

- Récapitulatif d'inventaire
- Inventaire complet
- Affichage de propriétés d'attribut
- Informations système

Vous pouvez également afficher les données d'inventaire dans des rapports que vous générez. Pour plus d'informations, reportez-vous à la section "Présentation des rapports".

Affichage du récapitulatif d'inventaire de la console d'informations du serveur

Le récapitulatif d'inventaire est disponible dans la page **Récapitulatif** de la console d'informations du serveur et fournit un examen rapide des informations de système et de configuration du système d'exploitation du périphérique.

Remarque : Si vous avez ajouté un périphérique à la base de données principale en utilisant l'outil de découverte, ses données d'inventaire n'ont pas encore été analysées vers la base de données principale. Vous devez exécuter une analyse d'inventaire sur le serveur pour que la fonction de récapitulatif d'inventaire se termine avec succès.

Pour afficher le récapitulatif d'inventaire

1. Dans la vue **Tous les périphériques** de la console, cliquez deux fois sur un périphérique.

2. Dans le volet de navigation de gauche, cliquez sur **Informations système**, puis cliquez sur **Récapitulatif du système**.

Données de récapitulatif de serveur Windows 2000/2003

Ces informations apparaissent lorsque vous affichez le récapitulatif d'inventaire pour un serveur Windows 2000/2003.

- **Santé :** L'état de santé actuel du serveur.
- **Type :** Le type de serveur, tel que application, fichier, message électronique, etc.
- **Fabricant :** Le fabricant du serveur.
- **Modèle :** Le type de modèle du serveur.
- **Version du BIOS :** La version du BIOS de ROM.
- **Système d'exploitation :** Systèmes d'exploitation Windows ou Linux exécutés sur le serveur : 2000, 2003 ou Red Hat.
- **Version du SE :** Numéro de version du système d'exploitation Windows 2000/2003 ou Linux exécuté sur le serveur.
- **UC :** Type du ou des processeurs exécutés sur le serveur.
- **Scanner de vulnérabilités :** La version de l'agent installé.
- **Scanner d'inventaire :** La version de l'agent installé.
- **Surveillance :** La version du scanner de surveillance installé.
- **Dernière réinitialisation :** Le dernier redémarrage du serveur.
- **Utilisation de l'UC :** Le pourcentage du processeur actuellement utilisé.
- **Mémoire physique utilisée :** Quantité de mémoire RAM disponible sur le serveur.
- **Mémoire virtuelle utilisée :** Quantité de mémoire disponible sur le serveur, y compris la mémoire RAM et la mémoire d'échange de fichiers.
- **Espace de disque utilisé :** Le pourcentage d'espace de disque actuellement utilisé. Si vous disposez de plusieurs disques durs, chaque lecteur est répertorié.

Les serveurs dotés de IPMI afficheront des données supplémentaires spécifiques à IPMI. Les serveurs Linux affichent également des informations similaires dans la vue **Récapitulatif**.

Affichage d'un inventaire complet

Un inventaire complet fournit une liste complète des composants matériels et logiciels détaillés d'un périphérique. La liste contient des objets et des attributs d'objet.

Pour afficher un inventaire complet

1. Dans la vue **Tous les périphériques** de la console, cliquez sur un périphérique.
2. Dans l'onglet **Propriétés**, cliquez sur **Afficher l'inventaire**.

Affichage des propriétés d'attribut

Vous pouvez afficher les propriétés d'attribut des objets d'inventaire d'un périphérique à partir de la liste d'inventaire. Les propriétés d'attribut indiquent les caractéristiques et valeurs d'un objet d'inventaire. Vous pouvez également créer des attributs personnalisés et modifier des attributs définis par l'utilisateur.

Pour afficher les propriétés d'un attribut, cliquez sur l'attribut dans le volet de gauche.

Pour imprimer ces informations dans Internet Explorer, cliquez avec le bouton droit de la souris dans le cadre, puis cliquez sur **Imprimer**. Pour imprimer dans Mozilla, cliquez avec le bouton droit de la souris dans le cadre, cliquez sur **Ce cadre | Enregistrer le cadre sous**, cliquez sur **Enregistrer**, puis ouvrez le fichier dans une application et cliquez sur **Imprimer**.

Informations système

Vous pouvez afficher et modifier les informations système du périphérique à partir de la console d'informations du serveur. Les informations dans les catégories **Matériel**, **Logiciel**, **Journaux** et **Autres** sont des données stockées ou en temps réel. Lorsque vous cliquez sur un lien d'informations, vous pouvez afficher des informations détaillées sur le composant sélectionné et, lorsque possible, définir des seuils et entrer des informations.

1. Dans la vue **Tous les périphériques** de la console, cliquez deux fois sur un périphérique.
2. Dans le volet de navigation de gauche de la console d'informations du serveur, cliquez sur **Informations système**.
3. Développez le groupe et cliquez sur le lien d'information que vous souhaitez afficher.

Personnalisation des options d'inventaire

La console inclut l'utilitaire Configuration de services que vous pouvez utiliser pour personnaliser les options d'inventaire. Les valeurs par dfaut de la plupart des options sont suffisantes mais vous pouvez tout de mme utiliser cet utilitaire pour les modifier, le cas chant. Pour lancer l'applet Configuration des service sur le serveur principal, cliquez sur **Dmarrer | Programmes | LANDesk | Configuration des services LANDesk**. (Le nom de fichier de cet utilitaire est svccfg.exe.)

Utiliser l'utilitaire Configuration de services pour configurer :

- Le nom de base de donnes, le nom d'utilisateur et le mot de passe
- L'intervalle d'analyse de logiciel de priphrique, la maintenance, les jours de conservation d'analyses d'inventaire et la dure de l'historique de connexion client
- Le traitement des doublons d'ID de priphrique
- Configuration du Planificateur, y compris les tches planifies et les intervalles entre valuations de requte
- Configuration d'une tche personnalise, y compris le dlai d'excution distante

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

Edition du fichier LDAPPL3.TEMPLATE

Les informations concernant spécifiquement les paramètres d'inventaire du scanner sont contenues dans le fichier LDAPPL3.TEMPLATE. Ce fichier fonctionne avec le fichier LDAPPL3 .INI pour identifier l'inventaire logiciel d'un périphérique. Ce fichier est placé sur les périphériques gérés Windows lors de la configuration d'agent. Ses paramètres sont réglés dans l'onglet Inventaire de Configuration d'agent.

Sur les périphériques Linux, un fichier de configuration identique (/etc/ldappl.conf) contient des informations sur les paramètres du scanner. Vous pouvez modifier ce fichier pour changer la façon dont le scanner fonctionne. Le fichier indique comment modifier le fonctionnement du scanner Linux.

Vous pouvez modifier la section [LANDesk Inventory] du fichier modèle afin de configurer les paramètres qui déterminent la manière dont le scanner identifie l'inventaire logiciel. Par défaut, LDAPPL3.TEMPLATE est situé sur le partage LDLogon du serveur principal.

Utilisez ce tableau pour vous aider à modifier la section [Inventaire LANDesk] dans un éditeur de texte.

Option	Description
Mode	Détermine comment le scanner analyse les logiciels sur les périphériques. La valeur par défaut est Listed. Voici les paramètres : • **Listed :** Enregistre les fichiers répertoriés dans le fichier LDAPPL3.INI. • **Unlisted :** Enregistre les noms et dates de tous les fichiers dotés d'une extension répertoriée sur la ligne ScanExtensions mais non définie dans le fichier LDAPPL3.INI. Ce mode aide à découvrir les logiciels non autorisés sur le réseau. • **Tous :** Découvre les fichiers répertoriés et non répertoriés.
Duplicate	Enregistre les doublons d'instances de fichiers. Définissez la valeur sur OFF pour enregistrer uniquement la première instance, ou sur ON pour enregistrer toutes les instances détectées. La valeur par défaut est ON.
ScanExtensions	Définit les extensions de fichier (.EXE, .COM, .CFG, etc.) à analyser. Utilisez un espace pour séparer les extensions de fichier. Par défaut, seuls les fichiers .EXE sont analysés.
Version	Le numéro de version du fichier LDAPPL3.
Revision	Le numéro de révision du fichier LDAPPL3 ; aide à assurer la compatibilité future.
CfgFiles 1-4	Enregistre la date, l'heure, la taille de fichier et le contenu des fichiers spécifiés. Vous pouvez omettre la lettre de lecteur (par exemple, c:) si vous souhaitez effectuer une recherche sur tous les lecteurs locaux. Vous pouvez spécifier plusieurs fichiers sur chacune des quatre lignes, mais la longueur de ligne est limitée à 80 caractères. Séparez les noms de chemin sur la même ligne par un espace.

Option	Description
	Le scanner compare les date et heure du fichier actuel avec celles de l'analyse précédente. En cas de discordance, l'analyse enregistre le contenu du fichier en tant que nouvelle révision.
ExcludeDir 1-3	Exclut des répertoires spécifiques d'une analyse. Vous pouvez omettre la lettre de lecteur (par exemple, c:) si vous souhaitez exclure tous les lecteurs locaux. L'énumération doit démarrer par 1 et être continue. Vous devez terminer chaque ligne par "\".
MifPath	Spécifie l'emplacement de stockage des fichiers MIF sur le lecteur local d'un client. L'emplacement par défaut est c:\DMI\DOS\MIFS.
UseDefaultVersion	Si ce paramètre est défini sur TRUE, le scanner rapporte une concordance lorsqu'un fichier correspond exactement à une entrée de nom et de taille de fichier du fichier LDAPPL3 sur le nom de fichier uniquement (la version sera rapportée en tant que EXISTS). Ceci peut générer des positifs faux dans le cas d'applications qui partagent un nom de fichier commun avec une application inconnue. Dans le fichier LDAPPL3.TEMPLATE tel que livré, ce paramètre est défini sur FALSE. En d'autres termes, ajoutez uniquement une entrée si la concordance est exacte. Si le paramètre est manquant, il est défini par défaut sur TRUE.
SendExtraFileData	Si ce paramètre est défini sur TRUE, envoie les données supplémentaires de fichier au serveur principal. La valeur par défaut est FALSE. Cela signifie que, par défaut, seuls les chemin, nom et version sont entrés dans la base de données principale.

Pour modifier le fichier LDAPPL3.TEMPLATE

1. À partir du serveur principal, allez dans le répertoire \Program Files\LANDesk\ManagementSuite\LDLogon et ouvrez le fichier LDAPPL3.TEMPLATE dans le Bloc-notes ou tout autre éditeur de texte.
2. Faites défiler la liste vers le paramètre à mettre à jour et apportez les modifications.
3. Enregistrez le fichier.

Mise à jour de la liste d'applications

Les données de la liste d'applications, DEFAULTS.XML, sont stockées dans la base de données du serveur principal. Les noms et les numéros de version des logiciels couramment utilisés étant souvent modifiés, LANDesk publie un nouveau fichier DEFAULTS.XML plusieurs fois par an (ce fichier était nommé LDAPPL.INI dans les versions précédentes du logiciel LANDesk).

Pour mettre à jour la liste d'applications

1. Téléchargez un nouveau fichier DEFAULTS.XML ou LDAPPL3.TEMPLATE du site http://www.landesk.com/support/downloads. Sélectionnez un produit et cliquez sur **Mise à jour du logiciel** pour télécharger le fichier.
2. Enregistrez le fichier dans le répertoire LDLOGON.
3. Publiez un nouveau fichier LDAPPL3.INI en suivant les étapes dans la section "Publication de la liste d'application".

Publication de la liste d'applications

La publication de la liste d'applications nécessite l'importation de la liste d'applications la plus récente de DEFAULTS.XML dans la base de données, puis la combinaison de la liste d'applications avec le contenu du fichier LDAPPL3.TEMPLATE pour générer un fichier LDAPPL3.INI actualisé. Le répertoire \Program Files\LANDesk\ManagementSuite possède un utilitaire autonome COREDBUTIL.EXE qui est utilisé pour exécuter ces deux étapes automatiquement.

Pour publier la liste d'applications

1. Lancez CoreDBUtil.exe
2. Cliquez sur le bouton **Publier la liste d'applications**.

Il est recommandé de publier la liste d'applications après la modification ou le téléchargement d'une version mise à jour de LDAPPL3.TEMPLATE ou DEFAULTS.XML.

Configuration du matériel

Prise en charge d'Intel* AMT

System Manager prend en charge les périphériques utilisant Intel* Active Management Technology (Intel* AMT), une fonction de matériel et Firmware qui permet de gérer le périphérique à distance. Intel AMT utilise la communication hors bande (OOB) pour accéder aux périphériques quel que soit l'état du système d'exploitation ou l'alimentation du périphérique.

La prise en charge Intel AMT de ce produit inclut les versions 1 et 2. Le processus d'approvisionnement des périphériques Intel AMT 2 inclut des nouvelles fonctions qui n'existent pas dans la version 1. Pour plus d'informations sur l'approvisionnement avec la version 2, reportez-vous à la section Configuration des périphériques Intel AMT. Les informations présentées dans cette section s'appliquent aux deux versions, excepté lorsque noté.

L'outil de configuration de matériel inclut les fonctions suivantes pour la gestion des périphériques Intel AMT :

- Génération automatique des ID d'approvisionnement (PID et PPS) (version 2)
- Modification du nom d'utilisateur et du mot de passe pour les périphériques gérés
- Configuration et activation des stratégies System Defense (version 2)
- Configuration et activation de la surveillance Agent Presence (version 2)

Gestion des périphériques avec ou sans agents de gestion

Lorsque les périphériques sont configurés avec Intel AMT, un nombre limité de fonctions de gestion est disponible même si le périphérique ne dispose pas d'un agent LANDesk. Tant que les périphériques sont connectés au réseau et qu'ils fonctionnent sur une alimentation en veille, ils peuvent être découverts et ajoutés à l'inventaire pour être gérés avec les autres périphériques du réseau.

Si un périphérique est doté d'Intel AMT, mais ne dispose pas d'un agent de gestion, il peut être découvert à l'aide d'une découverte de périphériques non gérés, placé dans la base de données d'inventaire, puis affiché dans la liste **Mes périphériques**. Toutefois, de nombreuses options de gestion System Manager ne sont pas disponibles. Ces options ne sont disponibles que lorsque l'agent LANDesk est installé. Les fonctions de gestion disponibles pour les périphériques configurés avec Intel AMT incluent :

- **Récapitulatif d'inventaire :** un sous ensemble de données d'inventaire normales peut être interrogé et affiché en temps réel pour les périphériques même si le périphérique est hors tension.
- **Journal d'événement :** un journal contenant les événements spécifiques à Intel AMT, affichant la sévérité et la description des événements et pouvant être affiché en temps réel.

- **Gestionnaire de démarrage distant :** les cycles d'alimentation et plusieurs options de démarrage peuvent être initialisés à partir de la console de gestion, quel que soit l'état du système d'exploitation ou de l'alimentation du périphérique. Les options disponibles sont basées sur la prise en charge des options sur le périphérique. Certains périphériques peuvent ne pas prendre en charge toutes les options de démarrage.
- **Forcer l'analyse de vulnérabilité et désactiver le réseau de système d'exploitation :** si un périphérique semble avoir exécuté un logiciel malfaisant, une analyse de vulnérabilité peut être exécutée lors du prochain redémarrage. Si nécessaire, le niveau d'OS du périphérique peut être désactivé pour empêcher les paquets non désirés d'être déployés sur le réseau.

Pour plus d'informations sur les options de gestion, reportez-vous à la section Gestion des périphériques Intel AMT.

Exigences d'approvisionnement de la version d'Intel AMT

Les périphériques peuvent être découverts comme étant des périphériques Intel AMT uniquement après que vous avez accédé à l'écran de configuration d'Intel AMT du périphérique et remplacé le mot de passe par défaut du fabricant par un mot de passe sécurisé. (Consultez la documentation du fabricant pour obtenir plus d'informations pour accéder à l'écran de configuration d'Intel AMT.) Si vous ne complétez pas ces étapes, les périphériques sont découverts mais ils ne sont pas identifiés comme étant des périphériques Intel AMT et les informations de récapitulatif d'inventaire affichées peuvent ne pas correspondre.

Pour que le serveur principal s'authentifie aux périphériques découverts d'Intel AMT, les références de nom d'utilisateur/mot de passe AMT doivent correspondre aux références configurées à l'aide de l'utilitaire Configuration des services. Vous pouvez modifier les références en utilisant l'écran de Configuration d'Intel AMT.

Lorsqu'un périphérique Intel AMT est ajouté à la base de données principale à gérer, System Manager l'approvisionne automatiquement selon le mode sélectionné dans l'utilitaire Configuration des services, qu'il ait déjà été approvisionné ou pas. Le mode Small Business offre une gestion de base sans des services d'infrastructure de réseau et n'est pas sécurisé, alors que le mode Enterprise est approprié pour des grandes sociétés et utilise DHCP, DNS et le service d'autorité de certification TLS pour offrir une communication sécurisée entre le périphérique géré et le serveur principal.

Lorsque vous approvisionnez un périphérique Intel AMT au mode Enterprise, le serveur principal installe un certificat sur le périphérique pour garantir une communication sécurisée. Si le périphérique doit être géré par un autre serveur principal, il doit être désapprovisionné puis réapprovisionné par le nouveau serveur principal. Sinon, l'accès Intel AMT du périphérique ne répond pas car le nouveau serveur principal ne possède pas un certificat correspondant. De même, tout autre ordinateur tentant d'accéder à la fonction Intel AMT du périphérique échoue car il ne dispose pas d'un certificat correspondant.

Configuration des périphériques Intel* AMT

Les périphériques équipés de la fonction Intel AMT doivent être configurés dès qu'ils ont été installés et mis sous tension. Le processus d'approvisionnement inclut plusieurs mesures de sécurité qui garantissent que seuls les utilisateurs autorisés puissent accéder aux fonctions de gestion Intel AMT.

Les périphériques Intel AMT communiquent avec le serveur d'approvisionnement du réseau. Ce serveur d'approvisionnement reste à l'écoute des messages envoyés par les périphériques Intel AMT sur le réseau et permet aux techniciens informatiques de gérer les serveurs via la communication hors bande indépendamment de l'état du système d'exploitation du périphérique. System Manager fonctionne en tant que serveur d'approvisionnement pour les périphériques Intel AMT et inclut des fonctions qui facilitent l'approvisionnement des périphériques lors de leur configuration. Vous pouvez alors gérer les périphériques avec ou sans agents de gestion System Manager supplémentaires.

Cette section présente le processus recommandé à suivre pour configurer les nouveaux périphériques Intel AMT (version 2). Durant ce processus, vous utiliserez System Manager pour générer un ensemble d'ID d'approvisionnement (PID et PPS). Une fois saisies dans l'écran de configuration d'Intel AMT du périphérique, ces ID assurent une connexion sécurisée avec le serveur d'approvisionnement, qui est conscient de leur présence, afin que le périphérique Intel AMT puisse terminer son processus d'approvisionnement initial.

Les périphériques dotés de la version 1 d'Intel AMT utilisent un processus similaire sans les clés PID et PPS. Pour plus de détails, reportez-vous aux remarques à la fin de cette section.

Approvisionnement pour les périphériques Intel AMT 2

Lorsqu'un périphérique Intel AMT 2 est reçu, le technicien informatique assemble l'ordinateur et le met sous tension. Une fois le périphérique mis sous tension, le technicien se connecte à l'écran de configuration du moteur de gestion ME (Management Engine) d'Intel basé sur le BIOS et remplace le mot de passe par défaut (admin) par un mot de passe plus sécurisé. Ceci permet d'accéder à l'écran de configuration d'Intel AMT.

Dans l'écran de configuration d'Intel AMT, les informations de pré-approvisionnement suivantes sont entrées :

- Une ID d'approvisionnement (PID)
- Une clé de passage de pré-approvisionnement (PPS), également appelée clé pré-partagée (PSK)
- L'adresse IP du serveur d'approvisionnement
- Le port 9982 comme port de communication avec le serveur d'approvisionnement
- Sélectionnez le mode Enterprise
- Le nom d'hôte du périphérique Intel AMT

Le serveur d'approvisionnement et le périphérique géré doivent connaître la clé PPS mais cette dernière ne peut pas être transmise sur le réseau pour des raisons de sécurité. Elle doit être entrée manuellement sur le périphérique (dans l'écran de configuration d'Intel AMT) et stockée

sur le serveur d'approvisionnement, qui est dans ce cas également le serveur principal de System Manager. Les paires PID/PPS sont générées par System Manager et stockées dans la base de données. Vous pouvez imprimer une liste des paires d'ID générées à utiliser pour l'approvisionnement.

Le technicien informatique devrait entrer l'adresse IP du serveur principal System Manager en tant que serveur d'approvisionnement et spécifier le port 9982. Autrement, par défaut, le périphérique Intel AMT envoie une diffusion générale qui peut être reçue si le serveur de configuration écoute sur le port 9971.

Le nom d'utilisateur et le mot de passe pour accéder à l'écran de configuration d'Intel AMT sont "admin" et "admin". Ces derniers sont modifiés durant le processus d'approvisionnement. Il n'est pas nécessaire de modifier le nom d'utilisateur mais le mot de passe doit être remplacé par un mot de passe plus sécurisé. La nouvelle combinaison de nom d'utilisateur et de mot de passe est entrée dans l'utilitaire Configuration des services fournit avec System Manager, comme décrit dans les étapes ci-dessous. Une fois que chaque périphérique est configuré, vous pouvez modifier la combinaison de nom d'utilisateur et de mot de passe individuellement par périphérique ; mais pour l'approvisionnement, utilisez la combinaison trouvée dans Configuration des services.

Une fois les informations ci-dessous entrées dans l'écran de configuration d'Intel AMT, le périphérique tente de communiquer avec le serveur d'approvisionnement en envoyant des messages "hello" lorsqu'il se connecte pour la première fois au réseau. Si ce message est reçu par le serveur d'approvisionnement, le processus d'approvisionnement débute lorsque le serveur établit une connexion au périphérique géré.

Lorsque le serveur principal reçoit un message "hello" et vérifie les clés PID/PPS, il approvisionne le périphérique Intel AMT au mode TLS. Le mode
TLS (Transport Layer Security) établit un canal sécurisé de communications entre le serveur principal et le serveur géré lorsque l'approvisionnement est terminé. Ce processus inclut la création d'un enregistrement dans la base de données avec les références codées et UUID du périphérique. Lorsque les données du périphérique sont dans la base de données, le périphérique s'affiche dans la liste des périphériques non gérés.

Une fois un périphérique Intel AMT approvisionné par le serveur principal, il peut être géré en utilisant uniquement la fonction Intel AMT. Vous pouvez le sélectionner dans la liste des périphériques non gérés et l'ajouter à vos périphériques gérés. Vous pouvez également déployer des agents de gestion System Manager pour utiliser plus de fonctions de gestion.

Le processus recommandé pour utiliser System Manager pour approvisionner les périphériques Intel AMT 2 est le suivant. Des instructions spécifiques pour les éléments 1 et 2 sont données dans les étapes suivantes.

1. Exécuter l'utilitaire Configuration des services pour spécifier un nouveau mot de passe sécurisé pour l'approvisionnement des périphériques Intel AMT. (Voir les étapes ci-dessous.)
2. Utilisez System Manager pour générer un lot d'ID d'approvisionnement Intel AMT (PID et PPS) et imprimez la liste des clés. (Voir les étapes ci-dessous.)
3. Dans le BIOS, connectez-vous à l'écran de configuration d'Intel ME et remplacez le mot de passe par défaut par un mot de passe sécurisé.

4. Connectez-vous à l'écran de configuration d'Intel AMT. Choisissez dans la liste d'ID d'approvisionnement que vous avez imprimée une paire de clés PID/PPS. Entrez l'adresse IP du serveur principal (serveur d'approvisionnement) et spécifiez le port 9982. Assurez-vous que le mode Enterprise est sélectionné pour l'approvisionnement. Entrez le nom d'hôte du périphérique Intel AMT.
5. Lorsque vous quittez l'écran BIOS, le périphérique commence à envoyer des messages "hello".
6. Le serveur principal reçoit un message "hello" et confirme la validité de la paire PIK/PPS dans la liste des clés générées. Si elle correspond, le périphérique est approvisionné au mode TLS.
7. Le périphérique est ajouté à la liste de découverte de périphériques non gérés.
8. Sélectionnez le périphérique et ajoutez-le aux périphériques gérés. Il sera géré par défaut comme un périphérique sans agent et vous pouvez également y déployer des agents de gestion.

Pour définir le nom d'utilisateur et le mot de passe Intel AMT dans Configuration des services

1. Dans le serveur principal, cliquez sur **Démarrer |** LANDesk **| Configuration des services**.
2. Cliquez sur l'onglet **Configuration Intel AMT**.
3. Saisissez **admin** comme nom d'utilisateur et mot de passe sous **Références Intel AMT actuelles**.
4. Entrez un nouveau nom d'utilisateur (facultatif) et un mot de passe sécurisé sous **Approvisionner avec des nouvelles références Intel AMT**.
5. Cliquez sur **OK**.

Ces champs de nom d'utilisateur et de mot de passe doivent être renseignés ici avant de pouvoir générer un lot d'ID d'approvisionnement.

Pour générer un lot d'ID d'approvisionnement Intel AMT

1. Dans le serveur principal, cliquez sur **Configuration de matériel** dans le volet de navigation de gauche.
2. Développez **AMT** et explorez en cascade depuis **Approvisionnement** jusqu'à **Générer des ID AMT**.
3. Entrez le nombre d'ID à générer (en général le nombre de périphériques que vous voulez approvisionner).
4. Si vous voulez utiliser un préfixe différent pour les PID, entrez-le dans la zone de texte **Préfixe PID**. Ce préfixe peut contenir uniquement des chiffres et des lettre en majuscule provenant de l'ensemble de caractères ASCII Le préfixe est limité à 7 caractères.
5. Entrez un nom de lot qui permettra d'identifier ce groupe d'ID générées.
6. Cochez l'option **Afficher les ID AMT générées** pour afficher les ID générées dans la liste. Si vous ne cochez pas cette option, les ID sont générées et enregistrées dans la base de données mais ne s'afficheront pas ici.
7. Cliquez sur **Générer des ID**.
8. Une fois les ID générées, cliquez sur **Imprime la liste des ID** pour ouvrir une nouvelle fenêtre contenant la liste des ID. (Seules les ID actuellement affichées dans la liste s'affichent dans la nouvelle fenêtre.) Utilisez la fonction Imprimer de votre navigateur pour imprimer la liste.

9. Pour afficher toutes les ID précédemment générées, ne renseignez pas la zone **Nom du lot** et cliquez sur **Afficher les ID par lot**.
10. Pour afficher un lot d'ID générées, entrez le nom du lot dans la zone de texte **Nom du lot** et cliquez sur **Afficher les ID par lot**.

Vous pouvez générer un nombre illimité de clés d'approvisionnement simultanément. Les clés sont stockées dans la base de données pour une référence ultérieure lorsque vous approvisionnez les nouveaux périphériques Intel AMT. Lorsque les périphériques sont approvisionnés et les clés d'approvisionnement utilisées, les ID utilisées sont grisées dans la page **Générer des ID AMT** pour faciliter leur suivi.

Un préfixe de PID est ajouté pour faciliter l'identification des ID comme PID, mais vous n'êtes pas requis de l'utiliser. Il est recommandé d'utiliser les caractères 0-4 ; le préfixe est limité à 7 caractères.

Pour identifier les lots de clés d'approvisionnement, spécifiez un nom de lot. Ce nom doit être descriptif et indiquer à quels périphériques les ID s'appliquent. Par exemple, vous pouvez générer des lots pour chaque service de votre entreprise et nommer les lots, Développement, Marketing, Finance, etc. Si plus tard vous voulez afficher les ID générées, tapez le nom de lot ici et cliquez sur **Afficher les ID par lot** pour afficher uniquement ces ID.

Mots de passe sécurisés

Intel AMT requiert l'utilisation d'un mot de passe sécurisé pour activer les communications sécurisées. Le mot de passe doit satisfaire les exigences suivantes :

- Il doit contenir au moins 8 caractères.
- Il doit inclure au moins un chiffre (0-9)
- Il doit inclure au moins un caractère ASCII non-alphanumérique (tels que !, &, %)
- Il doit contenir des caractères latins en majuscule et minuscule ou des caractères non-ASCII (UTF+00800 et ultérieur)

Erreurs lors du processus d'approvisionnement

Si vous entrez une paire PID et PPS incorrectement associée (par exemple, la clé PPS devrait être associée à une PID différente), un message d'erreur s'affiche dans le journal d'alerte et l'approvisionnement de ce périphérique est interrompu. Vous devrez redémarrer le périphérique et entrer une paire PID/PPS correcte dans l'écran de configuration d'Intel AMT.

Si un message d'erreur s'affiche dans l'écran de configuration d'Intel AMT lorsque vous entrez une PID, une erreur de frappe s'est produite lors de la saisie de la PID. Une somme de contrôles est réalisée pour s'assurer que la PID est correcte.

Découverte des périphériques Intel AMT 1.0

Lorsque vous exécutez une analyse de découverte de périphérique, les périphériques Intel AMT version 1 sont découverts et ajoutés au dossier Intel AMT dans la liste des périphériques **Non gérés**. Les périphériques sont reconnus comme étant des périphériques Intel AMT s'ils ont été configurés avec un nom d'utilisateur et un mot de passe sécurisés qui remplacent ceux définit par défaut par le fabricant.

Lorsque vous ajoutez un nom d'utilisateur et un mot de passe sécurisés à l'écran de configuration d'Intel AMT, vous pouvez également entrer l'adresse IP du serveur d'approvisionnement et spécifier le port 9982, comme pour les périphériques Intel AMT 2. Toutefois, aucune paire PID/PPS n'est utilisée dans l'approvisionnement des périphériques Intel AMT 1. Si vous spécifiez une adresse IP pour le serveur d'approvisionnement, le serveur principal fonctionne comme un serveur d'approvisionnement et vous pouvez gérer le périphérique comme un périphérique sans agent.

Notez que la version 1 d'Intel AMT n'utilise pas le même niveau de sécurité que la version 2. Intel recommande que les périphériques utilisant la version 1 soient configurés sur un réseau isolé sécurisé. Une fois la configuration terminée, ils peuvent être déplacés vers un réseau moins sécurisé pour la gestion.

Modification du nom d'utilisateur et du mot de passe pour les périphériques Intel* AMT

Un nom d'utilisateur et un mot de passe sécurisés sont requis pour approvisionner les nouveaux périphériques Intel AMT (version 1). Pour les périphériques gérés via System Manager, le nom d'utilisateur et le mot de passe entrés dans l'écran de configuration d'Intel AMT doivent être identiques à ceux entrés dans l'utilitaire Configuration des services de System Manager. Le nom d'utilisateur et le mot de passe de l'utilitaire Configuration des services sont enregistrés dans la base de données et appliqués globalement pour l'approvisionnement des périphériques Intel AMT.

Intel AMT requiert l'utilisation d'un mot de passe sécurisé pour activer les communications sécurisées. Le mot de passe doit satisfaire les exigences suivantes :

- Il doit contenir au moins 8 caractères.
- Il doit inclure au moins un chiffre (0-9)
- Il doit inclure au moins un caractère ASCII non-alphanumérique (tels que !, &, %)
- Il doit contenir des caractères latins en majuscule et minuscule ou des caractères non-ASCII (UTF+00800 et ultérieur)

Une fois l'approvisionnement terminé, il est recommandé de changer régulièrement les noms d'utilisateur et les mots de passe lors de la maintenance informatique. Vous pouvez utiliser une combinaison différente de nom d'utilisateur et mot de passe pour chaque périphérique Intel AMT ou vous pouvez appliquer une combinaison à plusieurs périphériques. Les nouvelles combinaisons de nom d'utilisateur et mot de passe entrées dans la page Configuration de matériel sont stockées dans la base de données et utilisées par System Manager pour communiquer en toute sécurité avec les périphériques Intel AMT.

Pour modifier le nom d'utilisateur et le mot de passe des périphériques Intel* AMT

1. Dans le serveur principal, cliquez sur **Configuration de matériel** dans le volet de navigation de gauche.
2. Développez **AMT** et explorez en cascade jusqu'à **Configuration**.

3. Dans la liste **Tous les périphériques**, sélectionnez un ou plusieurs périphériques pour lesquels vous voulez modifier le nom d'utilisateur et le mot de passe. Cliquez sur **Cible** dans la barre d'outils.
4. Dans le volet inférieur, entrez le nouveau nom d'utilisateur, puis tapez et confirmer le nouveau mot de passe.
5. Cliquez sur **Périphériques ciblés**, puis sur **Appliquer**.

   Pour un ou plusieurs périphériques d'une même liste, vous pouvez sélectionner les périphériques et cliquer sur **Périphériques sélectionnés**, puis cliquez sur **Appliquer**.

Configuration des stratégies System Defense

Intel AMT* 2.0 possède une fonction System Defense qui applique les stratégies de sécurité sur les périphériques dotés de AMT 2.0. Vous pouvez sélectionner et appliquer les stratégies System Defense sur des périphériques gérés grâce à l'outil **Configuration du matériel**.

Lorsqu'une stratégie System Defense est appliquée sur un périphérique Intel AMT, celui-ci filtre les paquets entrants et sortants selon les critères des stratégies définies. Lorsque le trafic réseau correspond aux conditions d'alerte définies dans un filtre, une alerte est créée et l'accès réseau du périphérique est bloqué. Le périphérique est alors isolé du réseau jusqu'à la fin des étapes de correction de cette stratégie.

System Managercontient des stratégies System Defense que vous pouvez appliquer à vos périphériques AMT. Chaque stratégie contient un ensemble de filtres qui définissent le type de trafic réseau non autorisé et les actions mises en place lorsque le trafic respecte les critères du filtre. Comment sélectionner et appliquer les stratégie :

1. Choisissez un ou plusieurs périphériques
2. Sélectionnez une stratégie System Defense à appliquer ; le cas échéant, modifiez la stratégie
3. Déployez la stratégie sur les périphériques ciblés

Une fois que la stratégie System Defense est activée sur un périphérique géré, le périphérique surveille tout le trafic réseau entrant et sortant. Lorsque les conditions d'un filtre sont détectées :

1. Le périphérique géré envoie une alerte ASF au serveur principal et une entrée est ajoutée dans le fichier journal d'alertes
2. Le serveur principal détermine quelles stratégies ont été enfreintes et interdit l'accès au réseau sur le périphérique géré
3. Le périphérique s'inscrit dans la file d'attente de correction System Defense (dans l'outil **Configuration du matériel**)
4. Pour rétablir l'accès réseau sur le périphérique, l'administrateur suit les étapes de correction appropriées puis supprime le périphérique de la file d'attente de correction. La stratégie System Defense d'origine est alors rétablie sur le périphérique

Ce processus est décrit plus en détails dans les sections suivantes.

Sélection et application des stratégies System Defense

System Managercontient les stratégies System Defense suivantes qui peuvent être appliquées aux périphériques Intel AMT 2.0. Les stratégies sont définies avec des paramètres tels que numéro de port, type de paquet, et nombre de paquets dans une durée déterminée. Lorsque vous activez une stratégie, celle-ci s'enregistre dans Intel AMT sur les périphériques sélectionnés. Les stratégies sont enregistrées en tant que fichiers XML sur le périphérique géré, dans le dossier CircuitBreakerConfig.

- **BlockFTPSrvr :** cette stratégie empêche le trafic par le port FTP. Lorsque des paquets sont envoyés ou reçus sur le port FTP 21, ceux-ci sont ignorés et l'accès réseau est interrompu.
- **LDCBKillNics :** cette stratégie bloque le trafic sur tous les ports réseau sauf les ports de gestion suivants :

Description de port	Numéros	Direction du trafic	Protocole
LANDesk Management	9593-9595	Envoyer/Recevoir	TCP, UDP
Intel AMT management	16992-16993	Envoyer/Recevoir	TCP uniquement
DNS	53	Envoyer/Recevoir	UDP uniquement
DHCP	67-68	Envoyer/Recevoir	UDP uniquement

Lorsque le serveur principal interrompt le trafic réseau sur un périphérique géré, il applique en fait cette stratégie. Puis, lorsque le périphérique est supprimé de la file d'attente de correction, la stratégie d'origine est de nouveau appliquée au périphérique.

- **LDCBSYNFlood :** cette stratégie détecte une attaque de refus de service d'inondation SYN : en une minute, elle n'autorise pas plus de 10 000 paquets TCP avec indicateur SYN activé. Lorsque ce chiffre est dépassé, l'accès réseau est interrompu.
- **LDCBSYNFlood :** cette stratégie détecte une attaque de refus de service d'inondation UDP : elle n'autorise pas plus de 20 000 paquets UDP par minute sur les ports 0 à 1023. Lorsque ce chiffre est dépassé, l'accès réseau est interrompu.

Pour sélectionner une stratégie System Defense

1. Cliquez sur **Configuration du matériel** dans le volet de navigation de gauche.
2. Ouvrez **AMT** et explorez en cascade l'arborescence jusqu'à **Stratégies**.
3. Dans la liste des périphériques, sélectionnez ceux auxquels vous allez appliquer la stratégie (utilisez Ctrl+clic ou Maj+clic pour sélectionner plusieurs périphériques).
4. Cliquez sur le bouton **Cible** de la barre d'outils pour ajouter le périphérique à la liste **Périphériques ciblés**.

5. Dans le volet inférieur, sélectionnez une stratégie dans la liste déroulante.
6. Cliquez sur **Périphériques ciblés** puis sur **Appliquer**.

Restauration de l'accès réseau sur les périphériques inscrits dans la file d'attente de correction

Si l'accès réseau d'un périphérique est interrompu à cause d'une stratégie System Defense, le périphérique s'affiche dans la file d'attente de correction. Il y reste jusqu'à ce que vous le supprimiez de la liste, ce qui rétablit la stratégie en vigueur sur ce périphérique. Avant de procéder, il faut résoudre le problème initial de la mise en file d'attente. Par exemple, si un trafic FTP a été détecté, il faut prendre les mesures nécessaires pour l'empêcher sur le périphérique.

Pour supprimer un périphérique de la fichier d'attente de correction

1. Cliquez sur **Configuration du matériel** dans le volet de navigation de gauche.
2. Ouvrez **AMT** et explorez en cascade l'arborescence jusqu'à **Correction**.
3. Sélectionnez les périphériques sur lesquels vous pouvez restaurer la stratégie System Defense d'origine et cliquez sur **Supprimer**.

Configuration de Intel* AMT Agent Presence

Intel* AMT 2.0 possède l'outil de sécurité Agent Presence qui permet de détecter la présence d'agents logiciels sur des périphériques gérés. Agent Presence permet de s'assurer que des agents de gestion sont constamment exécutés sur vos périphériques et vous prévient lorsqu'un agent s'arrête même lorsque d'autres agents basés sur des logiciels ne détectent pas le problème.

System Manager utilise Intel AMT Agent Presence pour surveiller deux agents : l'agent de gestion standard et le service de surveillance. Ceci est particulièrement utile lorsque les voies de surveillance normales ne sont pas disponibles. Par exemple, les couches de communication d'un périphérique ne fonctionnent pas ou l'agent de surveillance ne s'exécute plus. Par défaut, Agent Presence surveille aussi son propre processus de surveillance et vous prévient si celui-ci cesse de fonctionner.

Le fonctionnement d'Agent Presence s'effectue en configurant une horloge qui écoute les "battements" des agents de gestion sur le périphérique, pour vérifier qu'ils sont exécutés. Si l'horloge s'arrête parce qu'elle n'a pas détecté de battement, Intel AMT envoie une alerte au serveur principal.

Lorsque vous configurez Agent Presence, l'agent présent sur le périphérique s'enregistre auprès d'Intel AMT afin de lui envoyer directement des battements. Si les battements s'arrêtent, Intel AMT informe le serveur principal bar le biais de communications hors bande que l'agent de périphérique ne répond pas. Intel AMT envoie une trappe d'événement de plate-forme (platform event trap - PET) au serveur principal avec la description de l'état modifié. Par défaut, cette alerte est consignée avec l'état de santé du périphérique. Vous pouvez configurer l'initialisation d'autres actions d'alerte lorsque cette alerte est détectée (pour plus d'informations sur la configuration des actions d'alerte, voir Configuration des actions d'alerte).

Lorsque vous configurez Agent Presence, vous pouvez activer ou désactiver la surveillance de deux agents et définir les valeurs suivantes :

- **Battement :** la durée maximale (en secondes) entre deux battements. Si aucun battement n'est reçu avant la fin de ce temps, on considère que l'agent ne répond pas. La valeur par défaut est de 120 secondes pour l'agent de gestion standard et 180 secondes pour le service de surveillance. La valeur minimal est de 30 secondes pour les deux.
- **Durée initiale :** la durée maximale (en secondes) qui peut s'écouler après le démarrage du système d'exploitation avant qu'un battement d'agent doive obligatoirement être envoyé. Si cette durée est dépassée, on considère que l'agent ne répond pas. Agent Presence est configuré sur Intel AMT lorsque l'agent est installé. L'agent a donc suffisamment de temps pour s'éxécuter et envoyer son premier battement. La valeur par défaut est de 360 secondes. La valeur minimale est de 30 secondes.

Pour modifier la configuration de Intel AMT Agent Presence

1. Cliquez sur **Configuration du matériel** dans le volet de navigation de gauche.
2. Ouvrez **AMT** et explorez en cascade l'arborescence jusqu'à **Configuration AP**.
3. Pour désactiver Agent Presence sur les périphériques Intel AMT 2.0, désectionnez la case **Activer Agent Presence**.
4. Pour désactiver la surveillance d'un agent spécifique, désélectionnez la case qui lui correspond. (Même lorsque ces deux cases sont désélectionnées, Agent Presence continue de surveiller son propre processus de surveillance tant qu'il est exécuté.)
5. Entrez une nouvelle valeur dans le champ **Battement** pour changer la durée maximale permise entre chaque battement (minimum 30 secondes).
6. Entrez une nouvelle valeur dans le champ **Durée intiale** pour changer la durée maximale permise avant de recevoir le premier battement d'un agent une fois que le système d'exploitation a démarré sur le périphérique (minimum 30 secondes ; 120 secondes recommandé).

Prise en charge d'interface IPMI

System Manager inclut la prise en charge de Intelligent Platform Management Interface (IPMI), version 1.5 et 2.0. IPMI est une spécification développée par Intel,* H-P,* NEC,* et Dell* pour définir l'interface système et de message des matériels gérables. IPMI contient des fonctions de contrôle et de récupération qui permettent d'accéder à de nombreuses fonctions que l'ordinateur soit sous tension ou pas, ou indépendamment de l'état du système d'exploitation. Pour plus d'informations sur IPMI, consultez le site Web d'Intel.

Le contrôle IPMI est géré par le BMC (Contrôleur de gestion de la carte de base). Ce dernier fonctionne sur une alimentation en veille et interroge de manière autonome l'état de santé du système. Si le BMC détecte des éléments en dehors de la plage, vous pouvez configurer les actions IPMI résultantes, telles que la consignation de l'événement, la création d'alertes ou l'exécution d'opérations de récupération automatiques comme la mise hors tension ou la réinitialisation du système.

Vous devez disposer de SMBIOS version 2.3.1 ou ultérieure pour que le BMC soit détecté sur le système. Si le BMC n'est pas détecté, certaines informations IPMI ne s'afficheront pas dans les rapports, exportations, etc.

IPMI définit les interfaces courantes du matériel utilisé pour contrôler les caractéristiques de santé physiques, telles que la température, tension, ventilateurs, sources d'alimentation et intrusions de châssis. Outre le contrôle de santé, IPMI inclut d'autres fonctions de gestion système y compris les alertes automatiques, le redémarrage et l'arrêt automatique du système, les fonctions de contrôle de mise sous tension et de redémarrage distant et le suivi de parcs.

Les options de menu System Manager varient légèrement pour un périphérique doté de PXE en fonction de l'état du système d'exploitation.

Fonctions de gestion pour les périphériques dotés de IPMI

Les fonctions de contrôle dépendent des composants installés sur le périphérique surveillé, ainsi que de l'état du périphérique. Tout périphérique doté de IPMI disposant d'un BMC (Contrôleur de gestion de la carte de base) peut être contrôlé par la console administrative d'une manière limitée sans agents de gestion supplémentaires une fois le BMC configuré. Cela inclut la gestion hors bande lorsque le périphérique est hors tension ou lorsque le système d'exploitation n'est pas en état de marche. Une gestion complète est disponible lorsque l'agent de gestion est installé, un BMC est présent, le périphérique est sous tension et le système d'exploitation est en état de marche. Le tableau ci-dessous compare les fonctions disponibles avec ces configurations différentes.

	BMC uniquement*	**BMC + agent**	**Agent (sans IPMI)**
Gestion hors bande activée	X	X	
Gestion de bande activée		X	X
Le périphérique peut être découvert**	X	X	X
Lire les détecteurs d'environnement	X	X	Dépendant du matériel
Mettre sous/hors tension à distance	X	X	X
Lire et effacer le journal d'événements	X	X	
Configurer les alertes	X	X	X

	BMC uniquement*	BMC + agent	Agent (sans IPMI)
Lire les informations sur le système d'exploitation		X	X
Arrêt gracieux		X	X
Lire les informations de SMBIOS (processeur, logements, mémoire)		X	X
Synchronisation IP (SE vers BMC)		X	
Horloge de surveillance		X	
BMC communique avec le serveur principal	X	X	
Les composants System Manager locaux communiquent avec le serveur principal		X	X
Gamme complète des fonctions de gestion de System Manager		X	

*BMC Standard. Le mini BMC est une version réduite d'un contrôleur de gestion de la carte de base. Il offre les fonctions répertoriées ci-dessus, mais comprend les limitations suivantes :

- Ne prend pas en charge la redirection SOL (Serial over LAN)
- Possède un seul nom d'utilisateur pour la gestion BMC
- Utilise un seul canal pour la communication avec le BMC
- Possède un référentiel SEL (journal d'événement système) plus petit

**Si le 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 déployez un agent de gestion, le fichier exécutable de configuration du serveur analysera le système et détecte qu'il correspond à IPMI et configure le BMC.

Présente un conflit avec d'autres pilotes IPMI

Si vous avez installé d'autres logiciels de gestion qui incluent des pilotes IPMI sur les périphériques que vous voulez gérer avec System Manager, vous devrez auparavant les désinstaller avant de déployer les agents Management Suite avec les fonctions de gestion IPMI.

Par exemple, Microsoft* Windows* Server 2003 prend en charge IPMI via l'installation de Windows Remote Management (WinRM), qui inclut un fournisseur Windows Management Instrumentation (WMI) et un pilote IPMI. Toutefois, System Manager ne prend pas en charge l'installation de ce pilote IPMI et installe son propre pilote IPMI. Si WinRM a été installé sur un périphérique que vous voulez gérer avec System Manager, vous devez auparavant désinstaller WinRM à l'aide de l'option Ajout/Suppression de programmes de Windows (**Démarrer | Panneau de configuration | Ajout ou Suppression de programmes | Ajouter/Supprimer des composants Windows | Outils de gestion et d'analyse |** désélectionnez la case à cocher **Gestion de matériel** | cliquez sur **OK**).

Configuration IPMI BMC

La page **Configuration IPMI BMC** permet de personnaliser les paramètres pour communiquer avec les périphériques dotés de IPMI. Les fonctions décrites ci-dessous sont disponibles pour les périphériques en bande ; pour les périphériques hors bande, seuls les paramètres d'utilisateur de configuration d'alimentation et de BMC sont disponibles.

ATTENTION : Il est fortement recommandé de ne pas modifer les paramètres IPMI à moins de connaître la spécification IPMI et de comprendre les technologies associées impliquées dans ces paramètres. Une utilisation incorrecte de ces options de configuration peut empêcher System Manager de communiquer avec les périphériques dotés de IPMI.

Les options de configuration suivantes sont disponibles :

- Horloge de surveillance
- Configuration de l'alimentation
- Paramètres d'utilisateur
- Mot de passe BMC
- Configuration LAN
- Configuration SOL
- Configuration IMM

Modification des paramètres de l'horloge de surveillance

IPMI fournit une interface pour l'horloge de surveillance BMC. Cette horloge peut être réglée de manière à expirer régulièrement et est configurée pour initialiser certaines actions lorsqu'elle expire (telles que des cycles d'alimentation). System Manager est configuré pour réinitialiser régulièrement l'horloge afin qu'elle n'expire pas ; si le périphérique n'est plus disponible (par exemple, s'il se bloque ou s'il est mis hors tension), l'horloge n'est par réinitialisée et expire, ce qui initialise l'action.

Vous pouvez spécifier la période avant que l'horloge expire et sélectionner une action qui est exécutée lorsqu'elle expire. Vous pouvez choisir de ne pas agir, d'effectuer une réinitialisation matérielle (arrêt et redémarrage) du périphérique, de mettre le périphérique hors tension gracieusement ou d'exécuter un cycle d'alimentation (mettre hors tension gracieusement, puis redémarrer).

Vous pouvez également définir le BMC pour qu'il arrête la diffusion de messages ARP (Address Resolution Protocol) lorsque l'horloge de surveillance est activée, ce qui réduit le trafic réseau généré. Si vous interrompez les messages ARP, ils reprennent automatiquement lorsque l'horloge de surveillance expire.

Pour modifier les paramètres de l'horloge de surveillance

1. Dans la vue **Mes périphériques**, cliquez deux fois sur le périphérique que vous souhaitez configurer.
2. Dans le volet de navigation de gauche de la console d'informations du serveur, cliquez sur **Configuration de matériel**.
3. Développez **Configuration IPMI BMC** et cliquez sur **Horloge de surveillance**.
4. Cochez l'option **Activer l'horloge de surveillance** pour activer l'horloge.
5. Spécifiez la fréquence de vérification de l'horloge (en minutes ou secondes).
6. Sélectionnez une action à initialiser lorsque l'horloge de surveillance expire.
7. Si vous souhaitez que le BMC ne diffuse plus des messages ARP lorsque l'horloge de surveillance est activée, cliquez sur **Suspendre les ARP de BMC**.
8. Cliquez sur **Appliquer**.
9. Si vous avez modifié les paramètres de l'horloge de surveillance, vous pouvez restaurer les paramètres par défaut en cliquant sur **Restaurer les paramètres par défaut**.

Modification des paramètres de configuration d'alimentation

Lorsque l'alimentation est interrompue sur un ordinateur doté d'IPMI, vous pouvez spécifier l'action à prendre lorsque l'alimentation est restaurée. Il est recommandé de restaurer l'ordinateur vers son état au moment de l'interruption de l'alimentation, mais vous pouvez également choisir de le garder hors tension ou de toujours le remettre sous tension.

Pour modifier les paramètres de configuration d'alimentation

1. Dans la vue **Mes périphériques**, cliquez deux fois sur le périphérique que vous souhaitez configurer.
2. Dans le volet de navigation de gauche de la console d'informations du serveur, cliquez sur **Configuration de matériel**.
3. Développez **Configuration IPMI BMC** et cliquez sur **Configuration de l'alimentation**.
4. Sélectionnez une option à utiliser lorsque l'alimentation est rétablie.
5. Cliquez sur **Appliquer**.
6. Si vous avez modifié les paramètres de la configuration de l'alimentation, vous pouvez restaurer les paramètres par défaut en cliquant sur **Restaurer les paramètres par défaut**.

Modification des paramètres d'utilisateur de BMC

System Manager s'authentifie auprès d'un BMC en utilisant une combinaison de nom d'utilisateur et de mot de passe spécifique au BMC (distincte de tout autre nom d'utilisateur System Manager). System Manager réserve le premier nom d'utilisateur afin de pouvoir toujours communiquer avec le BMC. Si le BMC autorise la définition d'autres noms d'utilisateur, vous pouvez définir des noms d'utilisateur avec des mots de passe pour l'authentification BMC.

Vous pouvez également spécifier les niveaux de privilège de chaque utilisateur. Pour les IMM avancés, vous pouvez spécifier des niveaux de privilège de protocole (telnet, http, and https) pour chaque canal.

ATTENTION : Procédez avec prudence lorsque vous modifiez ces paramètres. L'utilisation de paramètres erronés peut désactiver la communication BMC du périphérique avec ce produit.

Pour modifier les paramètres d'utilisateur de BMC

1. Dans la vue **Mes périphériques**, cliquez deux fois sur le périphérique que vous souhaitez configurer.
2. Dans le volet de navigation de gauche de la console d'informations du serveur, cliquez sur **Configuration de matériel**.
3. Développez **Configuration IPMI BMC** et cliquez sur **Paramètres d'utilisateur**.
4. Pour effacer les données pour un nom d'utilisateur, cliquez le numéro d'index puis sur **Effacer**.
5. Pour ajouter ou modifier un nom d'utilisateur, cliquez sur le numéro d'index puis sur **Modifier**.
6. Entrez un nom d'utilisateur.
7. Pour définir le mot de passe, cochez la case **Définir le mot de passe**, puis tapez et confirmez le mot de passe.
8. Sélectionnez les niveaux de privilèges pour l'accès série et LAN.
9. Cliquez sur **Enregistrer les modifications**.

Modification du mot de passe BMC

System Manager s'authentifie auprès du BMC d'un périphérique à l'aide du nom d'utilisateur par défaut (user 1) et d'un mot de passe. Vous ne pouvez pas modifier le nom d'utilisateur mais vous pouvez changer le mot de passe. La modification de ce mot de passe est enregistrée dans la base de données et sur le BMC.

Pour modifier le mot de passe BMC par défaut

1. Dans la vue **Mes périphériques**, cliquez deux fois sur le périphérique que vous souhaitez configurer.
2. Dans le volet de navigation de gauche de la console d'informations du serveur, cliquez sur **Configuration de matériel**.
3. Développez **Configuration IPMI BMC** et cliquez sur **Mot de passe**.
4. Entrez le nouveau mot de passe et confirmez-le.
5. Cliquez sur **Appliquer**.

Modification des configurations LAN

Les messages IPMI peuvent être transmis directement du BMC via des interfaces LAN en plus de l'interface système du périphérique. L'activation de la communication LAN permet au serveur principal de recevoir des alertes spécifiques à IMPI, même si le périphérique est hors tension. Le serveur principal maintient cette communication tant que le périphérique dispose d'une connexion réseau physique avec une adresse réseau valide et tant que la source d'alimentation principale du périphérique est connectée.

ATTENTION : Si vous choisissez de définir une configuration personnalisée pour la communication LAN ou en série avec le BMC, procédez avec prudence lorsque vous modifiez les paramètres. L'utilisation de paramètres erronés peut désactiver la communication BMC du périphérique avec ce produit.

Si vous avez défini un canal LAN, vous pouvez utiliser les paramètres par défaut pour le BMC du périphérique, ou vous pouvez modifier l'adresse IP et les paramètres de passerelle. Utilisez ces options pour configurer des destinations pour les interruptions SNMP envoyées par le BMC pour chaque événement PET (trappe d'événement de plate-forme).

Vous pouvez également modifier les paramètres de la chaîne de communauté SNMP afin d'envoyer des alertes via LAN. Lorsque vous configurez ces paramètres, vous devez spécifier la chaîne de communauté SNMP utilisée pour l'authentification SNMP. Pour chaque configuration, vous pouvez modifier les informations de destination d'interruption pour spécifier quand et comment les interruptions sont envoyées et si elles sont reconnues.

Pour définir les propriétés pour la configuration de canal LAN

1. Dans la vue **Mes périphériques**, cliquez deux fois sur le périphérique que vous souhaitez configurer.
2. Dans le volet de navigation de gauche de la console d'informations du serveur, cliquez sur **Configuration de matériel**.
3. Développez **Configuration IPMI BMC** et cliquez sur **Configuration LAN**.
4. Sélectionnez **Toujours disponible** dans la liste déroulante de la communication LAN pour que l'accès au BMC soit toujours disponible. Si vous sélectionnez **Désactivé**, le BMC n'offrira plus un accès au LAN lorsque le périphérique est hors bande.
5. Sélectionnez le niveau de privilège utilisateur pour le canal : Le **Niveau-Administrateur** permet d'accéder à toutes les commandes, alors que le **Niveau-Utilisateur** n'offre qu'un accès en lecture seule (l'accès est limité si vous sélectionnez le niveau Utilisateur).
6. Cochez la case **Désactiver de manière permanente les ARP BMC** pour désactiver les messages ARP (Address Resolution Protocol) du BMC Ceci permet de réduire le trafic réseau mais peut empêcher la communication avec le BMC lorsque le périphérique est hors bande.
7. Cochez la case **Désactiver les réponses ARP** pour que le BMC n'envoie plus de réponses ARP lorsque le système d'exploitation n'est pas disponible. Si vous activez ce paramètre vous pouvez éventuellement empêcher la communication avec le BMC lorsque le périphérique est hors bande.

8. Les paramètres IP du canal LAN sont automatiquement définis si le BMC est synchronisé avec le canal de SE. Sinon, la case à cocher sous l'onglet **Paramètres IP** est activée. Vous pouvez laisser la coche pour utiliser les paramètres DHCP fournis automatiquement ou vous pouvez décocher la case et modifier les champs de texte avec des paramètres statiques. Il est recommandé d'utiliser les paramètres automatiques.
9. Cliquez sur l'onglet **Envoyer des alertes via LAN** pour configurer les paramètres de chaîne de communauté SNMP (voir les détails ci-dessous).
10. Cliquez sur **Appliquer** pour enregistrer vos modifications.

Pour modifier les propriétés d'envoi des alertes via LAN

1. Ouvrez la page **Configuration LAN** (étapes 1 à 3 ci-dessus).
2. Cliquez sur l'onglet **Envoyer des alertes via LAN**.
3. Cochez la case **Activé** pour activer l'envoi des alertes SNMP.
4. Spécifiez la **Chaîne de communauté SNMP** à utiliser pour l'authentification SNMP.
5. Pour configurer les destinations d'interruption, cliquez deux fois sur le numéro d'index pour ouvrir la boîte de dialogue **Propriétés**.
6. Spécifiez l'adresse IP à laquelle le BMC enverra des alertes, ainsi que l'adresse MAC correspondante.
7. Spécifiez le nombre de tentative, leur fréquence et la passerelle préférée à utiliser.
8. Si vous voulez que les alertes soient reconnues (ce qui augmente le trafic réseau généré), cochez la case **Reconnaître les alertes**.
9. Cliquez sur **OK**.
10. A la page Configuration LAN, cliquez sur **Appliquer** lorsque tous les paramètres sont renseignés.

Modification des configurations Serial Over LAN (SOL)

Utilisez les options de configuration SOL (Serial Over LAN) pour personnaliser les paramètres du modem série pour des utilisations spéciales, telles que la redirection des messages BIOS POST vers le port série. Si le BMC doit utiliser une connexion modem, les paramètres spécifiques du modem, tels que les chaînes d'initialisation et de composition doivent également être spécifiées.

Pour l'opération du modem en série, vous pouvez avoir à configurer les paramètres des cavaliers et du BIOS de la carte du périphérique. Pour plus d'informations, reportez-vous à la documentation du périphérique donné.

ATTENTION : Si vous choisissez de définir une configuration personnalisée pour la communication LAN ou en série avec le BMC, procédez avec prudence lorsque vous modifiez les paramètres. L'utilisation de paramètres erronés peut désactiver la communication BMC du périphérique avec ce produit.

Pour modifier les paramètres de configuration SOL

1. Dans la vue **Mes périphériques**, cliquez deux fois sur le périphérique que vous souhaitez configurer.
2. Dans le volet de navigation de gauche de la console d'informations du serveur, cliquez sur **Configuration de matériel**.
3. Développez **Configuration IPMI BMC** et cliquez sur **Configuration SOL**.
4. Pour activer SOL, cochez la case **Activer la communication Serial-over-LAN**.

5. Sélectionnez le **Niveau utilisateur requis pour activer SOL** minimal.
6. Sélectionnez la **Vitesse en bauds des sessions SOL** appropriée pour la configuration du matériel du périphérique.
7. Cliquez sur **Appliquer**.

Modification des configurations IMM

La page **Configuration IMM** s'affiche uniquement pour les périphériques IPMI dotés d'une carte complémentaire IMM avancée. Les options de cette page vous permettent d'activer ou de désactiver des protocoles et fonctions utilisés avec le périphérique doté de IMM Consultez la documentation du fabricant du IMM avant de modifier ces paramètres.

Pour modifier les paramètres de configuration IMM

1. Dans la vue **Mes périphériques**, cliquez deux fois sur le périphérique que vous souhaitez configurer.
2. Dans le volet de navigation de gauche de la console d'informations du serveur, cliquez sur **Configuration du matériel**.
3. Développez **Configuration IPMI BMC** et cliquez sur **Configuration IMM**.
4. Cochez les cases des protocoles et les fonctions que vous voulez activer et ajoutez les paramètres requis. Les options disponibles incluent :
   - KVM
   - SNMP
   - telnet
   - Alerte SMTP
   - HTTP
   - HTTPS
5. Cliquez sur **Appliquer**.

Gestion des périphériques Dell* DRAC

Ce produit gère l'intégration des périphériques dotés d'un contrôleur Dell* DRAC (Remote Access Controller). Le DRAC est un contrôleur matériel distant qui fournit une interface au matériel de gestion de serveur compatible avec IPMI sur le périphérique Dell. Une adresse IP a été attribuée au DRAC. Cette adresse est utilisée pour identifier le périphérique DRAC lors de la découverte de périphérique et de la gestion du périphérique.

Les périphériques qui contiennent un contrôleur Dell DRAC peuvent être gérés avec les mêmes fonctions que les autres périphériques compatibles avec IPMI. Lorsque le périphérique est découvert et ajouté à la liste des périphériques gérés, il est géré de la même manière que les autres périphériques IPMI. En outre, System Manager offre également des fonctions Dell DRAC uniques.

OpenManage Server Administrator est une console Web fournie par Dell pour gérer le périphérique Dell DRAC. En général, il est accessible en tapant l'adresse IP du DRAC dans un navigateur et en vous connectant à l'aide d'un nom d'utilisateur et mot de passe. Lorsqu'un périphérique Dell DRAC est géré via System Manager, vous pouvez également ouvrir cet utilitaire directement depuis l'interface de System Manager.

En outre, System Manager vous permet de gérer les noms d'utilisateur et les mots de passe qui permettent d'accéder à OpenManager Server Administrator et affiche trois journaux associés à cet utilitaire dans la console d'informations du serveur.

Pour ouvrir OpenManage Server Administrator pour un périphérique Dell DRAC

1. Cliquez deux fois sur le périphérique dans la liste **Tous les périphériques**.
2. Dans la console d'informations du serveur, développez **Matériel** et cliquez sur **Dell DRAC**. L'adresse IP du périphérique et d'autres informations d'identification s'affichent.
3. Cliquez sur **Lancer l'utilitaire Dell DRAC** pour ouvrir l'utilitaire OpenManage Server Administrator du périphérique dans une nouvelle fenêtre.

Journaux Dell DRAC disponibles dans System Manager

Trois journaux provenant de l'utilitaire OpenManage Server Administrator s'affichent dans la console d'informations du serveur System Manager.

- **Journal Dell DRAC** : effectue un suivi de tous les événements enregistrés par Server Administrator, tels que la connexion, l'état de la session, l'état de la mise à jour de Firmware et l'interaction entre le DRAC et d'autres composants de périphérique. Les informations affichées dans System Manager incluent la sévérité de l'événement, la description et des suggestions pour corriger les erreurs.
- **Journal des commandes Dell DRAC** : effectue un suivi des commandes envoyées à Server Administrator. Ce journal affiche les commandes exécutées, l'utilisateur à l'origine de cette commande, la date et l'heure de l'exécution ainsi que les tentatives de connexion et déconnexion et les erreurs d'accès.
- **Journal de suivi Dell DRAC** : utile pour suivre les détails sur les événements de communication réseau, tels que les alertes, les radiomessages ou les connexions réseau depuis le DRAC.

Pour afficher les journaux pour un périphérique Dell DRAC

1. Cliquez deux fois sur le périphérique dans la liste **Tous les périphériques**.
2. Dans la console d'information du serveur, développez **Journaux**.
3. Cliquez sur **Journal Dell DRAC**, **Journal des commandes Dell DRAC** ou **Journal de suivi Dell DRAC**.

Gestion des noms d'utilisateurs pour les périphériques dotés de Dell DRAC

Pour accéder à l'interface de l'utilitaire OpenManage Server Administrator, connectez-vous à l'aide du nom d'utilisateur et du mot de passe définis pour le périphérique. L'utilisateur **racine** par défaut est le premier utilisateur de la liste et ne peut pas être supprimé. Toutefois, son mot de passe peut être modifié et jusqu'à 15 utilisateurs supplémentaires peuvent être ajoutés. Bien que les niveaux d'accès des noms d'utilisateur DRAC peuvent varier, System Manager définit uniquement des noms d'utilisateur au niveau Administrateur.

Pour ajouter ou modifier des noms d'utilisateurs et des mots de passe pour un périphérique doté de DRAC

1. Cliquez deux fois sur le périphérique dans la liste **Tous les périphériques**.
2. Dans la console d'informations du serveur, cliquez sur **Configuration de matériel**.
3. Dans la console de configuration du matériel, développez **Configuration Dell DRAC** et cliquez sur **Utilisateurs Dell DRAC**. Une liste des utilisateurs actuellement définis s'affiche.
4. Pour modifier le mot de passe d'un utilisateur, cliquez sur le numéro de l'utilisateur, puis cliquez sur **Modifier le mot de passe**. Tapez et confirmez le nouveau mot de passe, puis cliquez sur **Appliquer**. (Pour attribuer le même mot de passe à plusieurs utilisateurs, sélectionnez-les en utilisant Ctrl + Clic ou Maj + Clic.)
5. Pour ajouter un utilisateur, cliquez sur **Ajouter un utilisateur**. Tapez un nom d'utilisateur et un mot de passe, confirmez le mot de passe, puis cliquez sur **Appliquer**. L'utilisateur est ajouté à la liste.

   Remarque : Si vous tapez un nom d'utilisateur qui existe déjà dans la liste, le nouveau mot de passe spécifié écrase le mot de passe existant pour ce nom d'utilisateur ; un deuxième utilisateur portant le même nom ne sera pas ajouté à la liste.

6. Pour supprimer un utilisateur, sélectionnez le numéro d'utilisateur et cliquez sur **Supprimer l'utilisateur**, puis cliquez sur **OK**. (Pour supprimer plusieurs utilisateurs, sélectionnez-les en utilisant Ctrl + Clic ou Maj + clic.)

Tous les utilisateurs de cette liste disposent d'un niveau d'accès Administrateur à l'utilitaire OpenManage Server Administrator.

Installation et maintenance de la base de données principale

Installation de la base de données principale

L'installation par défaut utilise une base de données MSDE Microsoft sur votre serveur principal. Cette base de données est la seule option disponible pour System Manager et vous ne pouvez installer qu'une seule base de données principale. La base de données doit uniquement être installée sur un serveur autonome.

Le schéma de la base de données prend en charge Microsoft SQL Server 2000 avec SP4. Tous les serveurs de base de données doivent être dotés de MDAC 2.8.

La base de données installée sur votre serveur principal doit être entièrement nouvelle. Si vous installez System Manager sur un serveur qui possède déjà une copie de LANDesk® Management Suite ou Server Manager, vous ne pouvez pas utiliser la structure de la base de données existante pour installer System Manager.

L'interface de l'utilitaire de configuration des services de LANDesk permet de configurer une variété de services. L'onglet Généralités de cet utilitaire affiche le nom du serveur actuel, le nom de la base de données et le nom d'utilisateur et mot de passe nécessaires pour accéder à la base de données principale. Ces références d'authentification sont utilisées par tous les services qui ont accès à la base de données principale. Puisque System Manager ne peut utiliser qu'une seule base de données principale, vous n'aurez pas besoin de modifier le nom de la base de données ou celui du serveur. Le cas échéant, vous pouvez modifier les références d'authentification. Pour plus d'informations, reportez-vous à l'Annexe C : Configuration de services.

Annexe A : Exigences système et utilisation des ports

Le serveur principal doit disposer d'une adresse IP statique.

Serveur principal administratif

Le serveur principal administratif prend en charge les systèmes d'exploitation suivants :

- Microsoft Windows 2000 Server (avec SP4)
- Microsoft Windows 2000 Advanced Server (avec SP4)
- Microsoft Windows 2003 Server Standard Edition (avec SP1)
- Microsoft Windows 2003 Server Enterprise Edition (avec SP1)

Prise en charge de serveur (agents)

- Microsoft Windows 2000 Server (avec SP4)
- Microsoft Windows 2000 Advanced Server (avec SP4)
- Microsoft Windows 2000 Professional (avec SP4)
- Microsoft Windows 2003 Server Standard Edition x86 (avec SP1)
- Microsoft Windows 2003 Server Standard x64 Edition (avec SP1)
- Microsoft Windows 2003 Server Enterprise Edition x86 (avec SP1)
- Microsoft Windows 2003 Server Enterprise x64 Edition (avec SP1)
- 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 - U2
- Red Hat Enterprise Linux v4 (ES) EM64t - U2
- Red Hat Enterprise Linux v4 (AS) 32 bits - U2
- Red Hat Enterprise Linux v4 (AS) EM64t - U2
- Red Hat Enterprise Linux v4 WS 32 bits - U2
- Red Hat Enterprise Linux v4 WS EM64t - U2

- 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

Navigateurs

- Microsoft Internet Explorer 6.x (avec SP1)
- Mozilla 1,7 et version ultérieure
- Firefox 1.5 et ultérieur

Bases de données

- MSDE (avec SP4)

Microsoft Data Access Components

- MDAC 2.8 ou version ultérieure

Si vous souhaitez que plusieurs produits de gestion LANDesk utilisent la même base de données, vous devez installer les produits sur le même ordinateur "principal". En conséquence, si vous voulez tous les installer sur le même ordinateur "principal", vous devez utiliser la même base de données. Si les deux produits utilisent une base de donnée identique, ils doivent également être la version 8.70.

Utilisation des ports

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 génériques 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
9595, 9594	console vers périphérique	TCP	Configuration du serveur
9595	console vers périphérique	UDP	découverte
623	console vers périphérique	UDP	découverte ASF, IPMI
5007	console vers périphérique	TCP	inventaire
9535	console vers périphérique	TCP	contrôle distant
139, 145	console vers périphérique	TCP	partage de fichiers et d'imprimantes
137, 138	console vers périphérique	UDP	partage de fichiers et d'imprimantes

Ce produit doit découvrir des nœuds dotés de l'agent de gestion standard 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).

Annexe B : Activation du serveur principal

Avant de pouvoir utiliser la console, vous devez d'abord activer votre serveur principal à l'aide de l'utilitaire d'activation du serveur principal. Il s'agit normalement d'une procédure unique qui ne doit être répétée que si vous achetez des licences supplémentaires. L'utilitaire d'activation du serveur principal permet d'effectuer les opérations suivantes :

- activer un nouveau serveur pour la première fois ;
- mettre à jour un serveur principal existant ou passer à Management Suite ou Server Manager ;
- activer un nouveau serveur avec une licence d'évaluation de 45 jours.

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 nœuds", plus loin dans cette section.

Chaque serveur principal doit utiliser un certificat d'autorisation unique. Plusieurs serveurs principaux ne peuvent pas partager le même certificat d'autorisation mais peuvent vérifier le nombre de nœuds sur le même compte LANDesk. Cet utilitaire s'exécute automatiquement lors du premier redémarrage après l'installation de System Manager.

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 invalide le contenu et le rapport d'utilisation suivant au 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 manuelle de votre part. Si le serveur principal n'est pas connecté, cliquez sur **Fermer** au redémarrage et envoyez le fichier d'autorisation à licensing@landesk.com.

L'utilitaire Activation du serveur principal ne démarre pas automatiquement une connexion Internet à distance, mais si vous la lancez manuellement 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 nœuds manuellement, comme décrit plus loin dans cette section.

Activation d'un serveur avec un compte LANDesk Software

Avant d'activer un nouveau serveur avec une licence d'utilisation intégrale, vous devez configurer un compte avec LANDesk Software qui vous accorde une licence pour le nombre de nœuds et

les produits LANDesk Software que vous avez achetés. Pour activer votre serveur, vous aurez besoin des informations de compte (nom de contact et mot de passe). Si vous ne disposez pas de ces informations, contactez votre représentant LANDesk Software.

Ne modifiez pas la date ou l'heure du serveur principal entre l'installation du produit et l'activation du serveur principal. Cette activation échouera. Vous devrez désinstaller puis réinstaller le produit.

Pour activer un serveur

1. Cliquez sur **Démarrer | Programmes | LANDesk | Activation du serveur principal**.
2. Cliquez sur **Activer**.

Activation d'un serveur avec une licence d'évaluation

La licence d'évaluation de 45 jours active votre serveur auprès du serveur de mise sous licence de LANDesk Software. Une fois la période d'évaluation de 45 jours terminée, vous ne pouvez plus vous connecter au serveur principal et ce dernier n'accepte plus d'analyses d'inventaire, mais vous ne perdez aucune données existante dans le logiciel ou la base de données. Durant ou après les 45 jours d'évaluation, vous pouvez exécuter à nouveau l'utilitaire d'activation du serveur principal et passer à une activation complète qui utilise un compte LANDesk Software. Le serveur principal est réactivé lorsque la licence d'évaluation expirée est remplacée par une licence d'utilisation intégrale.

Pour activer une licence d'évaluation de 45 jours

1. Cliquez sur **Démarrer | Programmes | LANDesk | Activation du serveur principal**.
2. Cliquez sur **Activer ce serveur principal pour une période d'évaluation de 45 jours**.
3. Cliquez sur **Evaluer**.

Mise à jour d'un compte existant

L'option de mise à jour envoie des informations sur l'utilisation au serveur de mise sous licence de LANDesk Software. Les données d'utilisation sont automatiquement envoyées si vous utilisez une connexion Internet. Par conséquent, cette option n'est normalement pas nécessaire pour envoyer une vérification du nombre de nœuds. Vous pouvez également utiliser cette option pour modifier le serveur principal associé au compte LANDesk Software. Cette option peut aussi remplacer la licence d'évaluation du serveur principal par une licence d'utilisation intégrale.

Pour mettre à jour un compte existant

1. Cliquez sur **Démarrer | Programmes | LANDesk | Activation du serveur principal**.
2. Cliquez sur **Mettre à jour ce serveur principal à l'aide de votre nom de contact et mot de passe LANDesk**.
3. Entrez le **nom de contact** et le **mot de passe** qui seront utilisés par le serveur principal. Si vous entrez un nom et mot de passe différents de ceux utilisés à l'origine pour activer le serveur principal, le serveur principal passe au nouveau compte.
4. Cliquez sur **Activer**.

Activation d'un serveur principal ou vérification des données de nombre de nœuds 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 nœuds. Un message vous invite à envoyer manuellement les données de vérification de nombre de nœuds 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 nœuds manuellement

1. Lorsque le serveur principal vous invite à vérifier manuellement les données de nombre de nœuds, il crée un fichier de données nommé ACTIVATE.TXT dans le dossier \Program Files\LANDesk\Authorization Files. Attachez ce ficher 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.

Annexe C : Configuration de services

Vous pouvez utiliser l'applet Configuration des services pour configurer les services suivants pour tous les serveurs principaux et les bases de données :

- Sélection d'un serveur principal et d'une base de données
- Configuration du service Inventaire
- Configuration du traitement des doublons de nom de périphérique
- Configuration du traitement des doublons d'ID de périphérique
- Configuration du service Planificateur
- Configuration du service Tâches personnalisées
- Configuration du service Multicast
- Configuration du mot de passe BMC
- Configuration du mot de passe AMT d'Intel

Pour lancer l'applet Configuration des services sur le serveur principal, cliquez sur **Démarrer | Programmes | LANDesk | Configuration des services LANDesk**.

Deux boutons s'affichent en dehors des onglets :

- **Références d'authentification :** Ouvre la boîte de dialogue Références d'authentification du serveur dans laquelle vous pouvez ajouter les périphériques qui peuvent fonctionner comme des serveurs préférés. Pour ajouter un périphérique, cliquez sur **Ajouter**. La boîte de dialogue **Nom d'utilisateur et mot de passe** s'affiche (voir la description ci-dessous).
- **Validation OSD :** Pour créer des environnements de pré-démarrage basés sur Windows PE ou DOS, vous devez avoir accès aux CD d'installation Windows PE 2005 et Windows NT 4. Cliquez sur **Valider maintenant** sous les deux environnements de mise en image, entrez le chemin d'accès au CD approprié et cliquez sur **OK**.

Boîte de dialogue Nom d'utilisateur et mot de passe

Utilisez la boîte de dialogue **Nom d'utilisateur et mot de passe** pour fournir des informations sur le serveur préféré que vous voulez ajouter.

Pour entrer les informations sur le serveur préféré

1. Dans l'applet Configuration des services, cliquez sur **Références d'authentification**.
2. Dans la boîte de dialogue Références d'authentification du serveur, cliquez sur **Ajouter**.
3. Entrez une description, les informations d'authentification et les plages d'adresses IP.
4. Cliquez sur **Tester les références d'authentification** pour vérifier la validité de vos informations.
5. Cliquez sur **OK** pour ajouter le serveur préféré à la boîte de dialogue Références d'authentification du serveur.

- **Nom du serveur :** Le nom du serveur préféré.
- **Nom d'utilisateur :** Le nom d'utilisateur utilisé pour s'authentifier au serveur. Il doit s'agir d'un nom de domaine pleinement qualifié (par exemple, Mondomaine\nom d'utilisateur).
- **Description :** Une description du serveur préféré.
- **Mot de passe :** Le mot de passe du serveur préféré.

- **Adresse IP de début :** Entrez l'adresse IP de début de la plage d'adresses auxquelles le serveur préféré sera limité. L'adresse IP de début ne peut pas être supérieure à l'adresse IP de fin. Les trois premiers octets des adresses IP de début et de fin doivent être identiques, par exemple 10.100.10.1 et 10.100.10.255.
- **Adresse IP de fin :** Entrez l'adresse IP de fin de la plage d'adresses à analyser.
- **Ajouter :**Ajoute les plages d'adresses IP dans la file d'attente de travail au bas de la boîte de dialogue.
- **Supprimer :**Supprime la plage d'adresses IP sélectionnée de la file d'attente de travail.

Configuration des onglets des services

Avant de configurer un service, utilisez l'onglet **Général** pour spécifier le serveur principal et la base de données pour lesquels configurer le service.

Remarque : Toutes les modifications de configuration de service que vous apportez pour un serveur principal et une base de données ne prendront effet qu'une fois le service redémarré sur ce serveur principal.

Sélection d'un serveur principal et d'une base de données

L'onglet **Général** permet de sélectionner un serveur principal et une base de données et fournit des références d'authentification afin de pouvoir configurer des services pour ce serveur principal.

Boîte de dialogue Configuration des services : Onglet Général

Utilisez cette boîte de dialogue pour sélectionner le serveur principal et la base de données pour lesquels configurer un service spécifique. Ensuite, sélectionnez l'onglet de service et spécifiez les paramètres de ce service.

- **Nom du serveur :** Affiche le nom du serveur principal auquel vous êtes actuellement connecté.
- **Serveur :** Permet d'entrer le nom d'un serveur principal différent et son répertoire de base de données.
- **Base de données :** Permet d'entrer le nom de la base de données principale.
- **Nom d'utilisateur :** Identifie un utilisateur doté de références d'authentification auprès de la base de données principale (spécifiées durant l'installation).
- **Mot de passe :** Identifie le mot de passe d'utilisateur requis pour accéder à la base de données principale (spécifié durant l'installation).
- **Il s'agit d'une base de données Oracle :** Indique que la base de données principale spécifiée ci-dessus est une base de données Oracle. (Ne s'applique pas à System Manager.)
- **Actualiser les paramètres :** Restaure les paramètres sur ceux présents à l'ouverture de la boîte de dialogue Configuration de services.

Configuration du service Inventaire

Utilisez l'onglet **Inventaire** pour configurer le service Inventaire pour le serveur principal et la base de données sélectionnés via l'onglet Général.

Présentation de la boîte de dialogue Configuration des services : Onglet Inventaire

Utilisez cet onglet pour spécifier les options suivantes du service Inventaire :

- **Nom du serveur** : Affiche le nom du serveur principal auquel vous êtes actuellement connecté.
- **Consigner les statistiques** : Conserve un journal d'actions et de statistiques relatives à la base de données principale.
- **Transport de données codées :** Permet au scanner d'inventaire de renvoyer des données d'inventaire de périphérique du périphérique analysé au serveur principal en tant que données codées via SSL.
- **Analyser le serveur à** : Spécifie l'heure à laquelle analyser le serveur principal.
- **Effectuer la maintenance à** : Spécifie l'heure d'exécution de la maintenance standard de la base de données principale.
- **Jours de conservation d'analyses d'inventaire** : Définit le nombre de jours avant que l'enregistrement d'analyse d'inventaire ne soit supprimé.
- **Connexions de propriétaire principal** : Spécifie le nombre de fois que le scanner d'inventaire suit des connexions pour déterminer le propriétaire principal d'un périphérique. Le propriétaire principal est l'utilisateur qui s'est connecté le plus de fois dans ce nombre de connexion spécifié. La valeur par défaut est 5 et les valeurs minimum et maximum sont respectivement 1 et 16. Si toutes les connexions sont uniques, le dernier utilisateur à se connecter est considéré être le propriétaire principal. Un périphérique ne peut avoir qu'un seul propriétaire principal associé à tout moment. Les données de connexion d'un utilisateur principal incluent le nom complet de l'utilisateur au format ADS, NDS, nom de domaine ou nom local (dans cet ordre), ainsi que la date de la dernière connexion.
- **Paramètres avancés :** Ouvre la boîte de dialogue **Paramètres avancés** qui permet de définir de nombreux paramètres avancés différents associés au scanner d'inventaire. Pour modifier un paramètre, cliquez sur le paramètre, modifiez-le dans la zone de texte **Valeur**, puis cliquez sur **Définir**. Pour afficher la description d'un paramètre, cliquez sur le paramètre et affichez les détails dans la case **Description**.
- **Logiciel :** Ouvre la boîte de dialogue **Paramètres d'analyse de logiciel** qui permet de configurer les paramètres d'heure et d'historique de l'analyse de logiciels du serveur.
- **Attributs :** Ouvre la boîte de dialogue Sélection d'attributs à stocker qui permet de sélectionner les attributs d'analyse d'inventaire stockés dans la base de données.
- **Gérer les doublons : Périphériques** : Ouvre la boîte de dialogue Configuration du traitement des doublons de nom de périphérique qui permet de choisir une option pour supprimer les périphériques avec des doublons de nom de périphérique, d'adresse Mac ou les deux (voir la section **Doublons de périphériques** ci-dessous).

- **Gérer les doublons : ID de périphériques :** Ouvre la boîte de dialogue **Doublon d'ID de périphérique** qui permet de sélectionner des attributs qui identifient les périphériques de manière unique. Vous pouvez utiliser cette option pour éviter que des doublons d'ID de périphérique soient intégrés dans la base de données principale (voir la section Configuration du traitement des doublons d'ID de périphérique, ci-dessous).
- **Etat du service d'inventaire** : Indique si le service est démarré ou arrêté sur le serveur principal.
- **Démarrer** : Démarre le service sur le serveur principal.
- **Arrêter** : Arrête le service sur le serveur principal.

Boîte de dialogue Paramètres d'analyse de logiciels

Utilisez cette boîte de dialogue pour configurer la fréquence des analyses de logiciels. Le matériel d'un périphérique est analysé à chaque fois que le scanner d'inventaire est exécuté sur le périphérique, mais les logiciels sont uniquement analysés suivant l'intervalle que vous spécifiez ici.

- **Chaque connexion :** Analyse tous les logiciels installés sur le périphérique à chaque fois que l'utilisateur se connecte.
- **Une fois tous les (jours) :** Analyse les logiciels du périphérique uniquement suivant l'intervalle quotidien spécifié, en tant qu'analyse automatique.
- **Enregistrer l'historique (jours) :** Spécifie la durée d'enregistrement de l'historique d'inventaire du périphérique.

Configuration du traitement des doublons de nom de périphérique

Utilisez la boîte de dialogue Doublons de périphériques pour supprimer des doublons de périphériques de la base de données.

1. Dans l'onglet Inventaire, cliquez sur **Périphériques**.
2. Dans la boîte de dialogue Doublons de périphériques, cliquez sur l'option que vous souhaitez utiliser lors de la suppression des doublons de périphériques, puis cliquez sur **OK**.

   Supprimer le doublon quand :
   - **Les noms de périphériques sont identiques :** Supprime l'enregistrement le plus ancien lorsque deux ou plusieurs noms de périphérique de la base de données sont identiques.
   - **Les adresses MAC sont identiques :** Supprime l'enregistrement le plus ancien lorsque deux ou plusieurs adresses MAC de la base de données sont identiques.
   - **Les noms de périphérique et les adresses MAC sont identiques :** Supprime l'enregistrement le plus ancien UNIQUEMENT lorsque deux ou plusieurs noms de périphérique et adresses MAC (du même enregistrement) sont identiques.

Configuration du traitement des doublons d'ID de périphérique

Le transfert d'image étant souvent utilisé pour configurer les périphériques d'un réseau, la possibilité de doublons d'ID de périphérique parmi les périphériques est accrûe. Vous pouvez éviter ce problème en spécifiant d'autres attributs uniques au périphérique qui, combinés à l'ID de périphérique, créent un identificateur unique pour les périphériques. Des exemples d'autres attributs incluent le nom du périphérique, le nom de domaine, le BIOS, le bus, le coprocesseur, etc.

La fonction de doublon d'ID permet de sélectionner des attributs de périphérique qui peuvent être utilisés pour identifier le serveur de manière unique. Vous spécifiez quels sont ces attributs et le nombre d'entre eux pouvant être manquants avant que le périphérique soit désigné comme doublon d'un autre périphérique. Si le scanner d'inventaire détecte un doublon de périphérique, il écrit un événement dans le journal d'événements des applications afin d'indiquer l'ID de périphérique du doublon de périphérique. La boîte de dialogue Doublon d'ID de périphérique contient les options suivantes :

- **Liste d'attributs :** Répertorie tous les attributs que vous pouvez choisir pour identifier de manière unique un périphérique.
- **Attributs d'identité :** Affiche les attributs que vous avez sélectionnés pour identifier de manière unique un périphérique.
- **Déclencheurs de doublons d'ID de périphérique :**
  - **Attributs d'identité :** Identifie le nombre d'attributs non satisfaits par un périphérique déterminant qu'il s'agit d'un doublon d'un autre périphérique.
  - **Attributs de matériel :** Identifie le nombre d'attributs de matériel non satisfaits par un périphérique déterminant qu'il s'agit d'un doublon d'un autre périphérique.
- **Rejeter les doublons d'identité :** Spécifie au scanner d'inventaire d'enregistrer l'ID de périphérique du doublon de périphérique et de rejeter toute tentative suivante d'analyse de cet ID de périphérique. Le scanner d'inventaire génère ensuite un nouvel ID de périphérique.

Pour configurer le traitement des doublons d'ID

1. Dans la boîte de dialogue Configuration des services, cliquez sur l'onglet **Inventaire**, puis cliquez sur **ID de périphérique**.
2. Dans **Liste Attributs**, sélectionnez l'attribut à utiliser pour identifier un périphérique de manière unique, puis cliquez sur le bouton de flèche vers la droite pour l'ajouter à la liste **Attributs d'identité**. Vous pouvez ajouter autant d'attributs que vous le souhaitez.
3. Sélectionnez le nombre d'attributs d'identité (et d'attributs de matériel) non satisfaits par un périphérique déterminant qu'il s'agit d'un doublon d'un autre périphérique.
4. Si vous souhaitez que le scanner d'inventaire rejette les doublons d'ID de périphérique, cochez l'option **Rejeter les doublons d'identité**.

Configuration du service Planificateur

Utilisez l'onglet **Planificateur** pour configurer le service Planificateur pour le serveur principal et la base de données sélectionnés via l'onglet **Général**. Vous devez disposer des droits appropriés pour effectuer ces tâches, y compris des privilèges complets d'administrateur sur les

périphériques gérés, afin qu'ils puissent recevoir des distributions de paquet à partir de System Manager. Vous pouvez spécifier plusieurs références de connexion à utiliser sur les périphériques en cliquant **Modifier la connexion**.

Présentation de la boîte de dialogue Configuration des services : Onglet Planificateur

Utilisez cet onglet pour afficher le nom du serveur principal et celui de la base de données sélectionnés précédemment, ainsi que pour spécifier les options suivantes de tâches planifiées :

- **Nom d'utilisateur** : Nom d'utilisateur sous lequel le service de tâches planifiées est exécuté. Vous pouvez modifier ce nom en cliquant sur le bouton **Modifier la connexion**.
- **Nombre de secondes entre les essais** : Lorsqu'une tâche planifiée est configurée avec des essais multiples, ce paramètre contrôle le nombre de secondes que le service Tâches planifiées attend avant de retenter la tâche.
- **Nombre de secondes pour tentative d'éveil** : Lorsqu'une tâche planifiée est configurée pour utiliser la technologie Wake On LAN, ce paramètre contrôle le nombre de secondes que le service de tâches planifiées attend avant qu'un périphérique se réveille.
- **Intervalle entre évaluations de requête** : Un nombre qui indique la durée entre des évaluations de requête et une unité de mesure pour le nombre (minutes, heures, jours ou semaines).
- **Paramètres Wake On LAN** : Le **Port IP** utilisé par le paquet Wake On LAN défini par les tâches planifiées pour réveiller les périphériques.
- **Etat du service Planificateur** : Indique si le service est démarré ou arrêté sur le serveur principal.
- **Démarrer** : Démarre le service sur le serveur principal.
- **Arrêter** : Arrête le service sur le serveur principal.
- **Redémarrer :** Redémarre le service sur le serveur principal.
- **Options avancées :** Ouvre la boîte de dialogue **Paramètres avancés du Planificateur** qui permet de modifier les paramètres qui contrôlent le fonctionnement du Planificateur. Pour modifier un paramètre, cliquez sur le paramètre à modifier, cliquez sur **Modifier**, apportez la modification voulue, puis cliquez sur **OK**.

Boîte de dialogue Configuration des services : Modifier la connexion

Utilisez la boîte de dialogue **Modifier la connexion** (cliquez sur **Modifier la connexion** sur l'onglet **Planificateur**) pour changer la connexion par défaut du planificateur. Vous pouvez également spécifier d'autres références d'authentification que le servive de Planificateur peut utiliser lorsqu'il doit exécuter une tâche sur les périphériques non gérés.

Pour installer des agents System Manager sur des périphériques non gérés, le service Planificateur doit pouvoir se connecter aux périphériques avec un compte administratif. Le compte par défaut utilisé par le service Planificateur est LocalSystem. Les références d'authentification LocalSystem fonctionnent en général sur les périphériques qui ne sont pas présents dans un domaine. Si les périphériques sont situés dans un domaine, vous devez spécifier un compte d'administrateur de domaine.

Si vous souhaitez modifier les références de connexion au service Planificateur, spécifiez un autre compte d'administration au niveau du domaine à utiliser sur les périphériques. Si vous gérez des périphériques sur plusieurs domaines, vous pouvez ajouter des références d'authentification supplémentaires que le service Planificateur peut essayer. Si vous souhaitez que le service Planificateur utilise un compte autre que LocalSystem ou que vous voulez fournir des références d'authentification secondaires, vous devez spécifier une connexion principale au service Planificateur dotée de droits administratifs au serveur principal. Les références d'authentification secondaires n'exigent pas de droits administratifs sur le serveur serveur principal, mais doivent êtres dotées de droits administratifs sur les périphériques.

Le service Planificateur essaye les références d'authentification par défaut, puis utilise toutes les références que vous avez spécifiées dans la liste **Références d'authentification alternatives** jusqu'à ce que l'authentification réussisse ou que toutes les références aient été utilisées. Les références d'authentification spécifiées sont codées et stockées de manière sûre dans le registre du serveur principal.

Vous pouvez définir ces options pour les références par défaut du Planificateur :

- **Nom d'utilisateur :** Entrez le domaine\nom d'utilisateur par défaut ou nom d'utilisateur que le Planificateur doit employer.
- **Mot de passe :** Entrez le mot de passe des références d'authentification spécifiées.
- **Confirmer le mot de passe :** Retapez le mot de passe pour le confirmer.

Vous pouvez définir ces options pour les références supplémentaires du Planificateur :

- **Ajouter :** Cliquez pour ajouter le nom d'utilisateur et le mot de passe spécifiés dans la liste Références d'authentification alternatives.
- **Supprimer :** Cliquez pour supprimer les références sélectionnées de la liste.
- **Modifier :** Cliquez pour modifier les références d'authentification sélectionnées.

Lorsque vous ajoutez des références d'authentification alternatives, spécifiez les options suivantes :

- **Nom d'utilisateur :** Entrez le nom d'utilisateur que le Planificateur doit utiliser.
- **Domaine :** Entrez le domaine du nom d'utilisateur spécifié.
- **Mot de passe :** Entrez le mot de passe des références d'authentification spécifiées.
- **Confirmer le mot de passe :** Retapez le mot de passe pour le confirmer.

Configuration du service Tâches personnalisées

Utilisez l'onglet **Tâches personnalisées** afin de configurer le service correspondant pour le serveur principal et la base de données sélectionnés dans l'onglet Général. Il s'agit notamment d'analyses d'inventaire ou de distributions de logiciel.

Lorsque vous désactivez le protocole d'exécution distante TCP, les tâches personnalisées utilisent le protocole de l'agent de gestion standard par défaut, qu'il soit désactivé ou non. De même, si les exécutions distantes TCP et de l'agent de gestion standard sont désactivées, les tâches personnalisées tentent d'utiliser l'exécution distante TCP en premier et, en cas d'absence, l'exécution distante du produit standard.

L'onglet **Tâches personnalisées** permet également de choisir des options pour la découverte de serveur. Pour traiter une tâche, le service des tâches personnalisées doit découvrir chaque adresse IP actuelle du serveur. Cet onglet permet de configurer comment le service contacte les serveurs.

Présentation de la boîte de dialogue Configuration des services : Onglet Tâches personnalisées

Utilisez cet onglet pour spécifier les options suivantes du service des tâches personnalisées :

Options d'exécution distante :

- **Désactiver l'exécution TCP** : Désactive TCP comme protocole d'exécution distante et force donc l'utilisation du protocole CBA par défaut.
- **Désactiver l'exécution CBA / Transfert de fichiers** : Désactive l'agent de gestion standard comme protocole d'exécution à distance. Si l'agent de gestion standard est désactivé et que le protocole d'exécution distante TCP est introuvable sur le périphérique, l'exécution distante échoue.
- **Activer le délai d'exécution distante** : Active un délai d'exécution distante et spécifie le nombre de secondes après lequel le délai expire. L'exécution distante temporise le déclenchement lorsque le périphérique envoie des battements, mais la tâche sur le périphérique est bloquée ou en boucle. Ce paramètre s'applique aux deux protocoles (TCP ou agent de gestion standard). Cette valeur peut être comprise entre 300 secondes (5 minutes) et 86 400 secondes (1 jour).
- **Activer le délai du client** : Active un délai de périphérique et spécifie le nombre de secondes après lequel le délai expire. Par défaut, l'exécution distante TCP envoie un battement d'un périphérique à un autre à intervalles de 45 secondes jusqu'à ce que l'exécution distante se termine ou soit abandonnée. Le client temporise le déclenchement lorsque le périphérique n'envoie pas de battement au périphérique.
- **Port d'exécution distante (12174 par défaut)** : Port via lequel l'exécution distante TCP se produit. Si ce port est modifié, il doit également l'être dans la configuration du client.

Options de distribution :

- **Distribuer vers <nn> serveurs simultanément** : Nombre maximal de périphériques vers lesquels la tâche personnalisée sera distribuée simultanément.

Options de découverte :

- **UDP :** La sélection d'UDP utilise un ping d'agent de gestion standard via UDP. La majorité des composants System Manager dépendent de l'agent de gestion standard et par conséquent les périphériques gérés doivent être dotés de l'agent de gestion standard. Cette méthode de découverte est la plus rapide et il s'agit de la méthode par défaut. Avec UDP, vous pouvez aussi sélectionner **Tentatives** et **Délai** de ping UDP.

- **TCP :** En sélectionnant TCP, vous utilisez une connexion HTTP au serveur sur le port 9595. Cette méthode de découverte a l'avantage de fonctionner via un pare-feu si le port 9595 est ouvert, mais elle est soumise aux délais de connexion HTTP en l'absence des périphériques. Ces délais peuvent durer 20 secondes ou plus. Si beaucoup de périphériques cible ne répondent pas à la connexion TCP, le démarrage de la tâche peut prendre un certain temps.
- **Les deux :** La sélection de cette option indique au service de tenter la découverte avec UDP, puis avec TCP, et enfin avec DNS/WINS s'il est sélectionné.
- **Désactiver la diffusion de sous-réseau :** Lorsque cette option est sélectionnée, la découverte via une diffusion de sous-réseau est désactivée.
- **Désactiver l'examen DNS/WINS :** Lorsque que cette option est sélectionnée, la recherche de service de nom est désactivée pour chaque périphérique si la méthode de découverte TCP/UDP sélectionnée échoue.

Configuration du service Multicast

Utilisez l'onglet **Multicast** pour configurer les options de découverte de représentants de domaine Multicast pour le serveur principal et la base de données sélectionnés via l'onglet **Général**.

Présentation de la boîte de dialogue Configuration des services : Onglet Multicast

Utilisez cet onglet pour définir les options suivantes du service Multicast :

- **Utiliser un représentant de domaine Multicast :** Utilise la liste de représentants de domaine Multicast stockés dans le groupe **Configuration > Représentants de domaine Multicast** de la vue de réseau.
- **Utiliser le fichier mis en cache :** Interroge chaque domaine Multicast pour déterminer qui peut déjà avoir le fichier dans la mémoire cache. Le fichier en mémoire cache peut alors être utilisé au lieu d'avoir à télécharger le fichier vers un représentant.
- **Utiliser le fichier mis en cache avantle représentant de domaine préféré :**Modifie l'ordre de découverte pour que l'option **Utiliser le fichier mis en cache** soit la première option tentée.
- **Utiliser la diffusion :** Envoie une diffusion dirigée par sous-réseau pour trouver tout périphérique sur ce sous-réseau qui pourrait être un représentant de domaine Multicast.
- **Consigner la période de rejet (jours) :** Spécifie le nombre de jours que les entrées du journal sont conservées avant d'être supprimées.

Configuration du mot de passe BMC

Utilisez l'onglet **Mot de passe** pour créer un mot de passe pour le contrôleur de gestion de la carte de base (BMC) IPMI.

- Dans l'onglet **Mot de passe BMC**, renseignez la zone de texte **Mot de passe**, entrez de nouveau 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/minuscules de a à z.

Configuration des options Intel AMT

Utilisez l'onglet **Configuration d'Intel AMT** pour créer ou modifier le mot de passe des périphériques dotés d'Intel Active Management Technology et pour afficher les instructions sur la découverte des périphériques AMT.

Pour configurer un mot de passe d'Intel AMT

1. Entrez le nom d'utilisateur et le mot de passe 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 être un mot de passe sécurisé. 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

Découverte et approvisionnement des périphériques Intel AMT

Pour découvrir les périphériques AMT, entrez l'adresse IP du serveur principal dans le champ Serveur d'approvisionnement du BIOS AMT et utilisez le port 9982. Pour plus d'informations, appuyez sur **Aide** dans **Configuration des services**. Lorsqu'un périphérique Intel AMT est découvert et placé dans la liste **Mes périphériques**, il est automatiquement approvisionné à l'aide du mode TLS.

Annexe D : Sécurité d'agents et certificats approuvés

Chaque serveur principal possède un certificat unique et une clé privée créés par le programme d'installation lorsque vous installez le serveur principal pour la première fois sur un périphérique. Les périphériques communiqueront uniquement avec les serveurs principaux pour lesquels ils possèdent un fichier de certificat approuvé correspondant.

Voici les fichiers de clé privée et de certificat qui sont installés :

- **<nom_clé>.key :** Le fichier .KEY est la clé privée pour le serveur principal et réside uniquement sur ce dernier. Si cette clé est compromise, le serveur principal et les communications de serveur ne seront pas sécurisées. Gardez cette clé en lieu sûr. Par exemple, n'utilisez pas le courrier électronique pour la déplacer.
- **<nom_clé>.crt :** Le fichier .CRT contient la clé publique pour le serveur principal. Le fichier .CRT est une version lisible conviviale de la clé publique que vous pouvez afficher pour obtenir des informations supplémentaires sur celle-ci.
- **<charabia>.0 :** Le fichier .0 est un fichier de certificat approuvé dont le contenu est identique à celui du fichier .CRT. Toutefois, il est nommé de telle manière que l'ordinateur peut rapidement trouver le fichier de certificat dans un répertoire contenant plusieurs certificats différents. Le nom est un charabia (somme de contrôle) des informations d'objet du certificat. Pour déterminer le nom du fichier de charabia pour un certificat donné, affichez le fichier <nom_clé>.CRT. Ce fichier contient une section [LDMS] de fichier .INI. La paire charabia=valeur indique la valeur <charabia>.

Toutes les clés sont stockées dans le répertoire \Programmes\LANDesk\Shared Files\Keys du serveur principal. La clé publique <charabia>.0 est également dans le répertoire LDLOGON et doit s'y trouver par défaut. <nom_clé> est le nom du certificat fourni durant l'installation du serveur principal. Durant l'exécution du programme d'installation, il est utile de fournir un nom de clé descriptif, tel que le nom du serveur principal (ou même son nom complet) comme nom de clé (par exemple : serveurld ou serveurld.org.com). Ceci devrait simplifier l'identification du fichier de certificat/clé privé dans un environnement multi-serveurs.

Sauvegarde et restauration de fichiers de certificat / clé privée entre des serveurs principaux

Lorsque vous installez un serveur principal, le programme d'installation crée un nouveau certificat. Si vous réinstallez sur un serveur principal existant, l'installation crée tout de même un nouveau certificat. Si le certificat des périphériques que vous avez installés ne correspond pas au certificat de votre nouveau serveur principal, le serveur principal et les clients ne peuvent pas communiquer. Si vous devez réinstaller votre serveur principal, deux options sont disponibles :

1. Réinstallez manuellement les agents en utilisant une configuration créée sur votre nouveau serveur principal. Vous ne pouvez pas utiliser la distribution de logiciel pour mettre à jour les agents car la clé et le certificat du serveur principal et ceux des périphériques ne correspondent pas.

2. Avant de réinstaller le serveur principal, sauvegardez les fichiers de clé et de certificat dans un emplacement sûr. Une fois la réinstallation terminée, copiez les anciennes clés dans le nouveau serveur principal. Les nouvelles et anciennes clés peuvent coexister. Le serveur principal utilisera automatiquement la clé correcte.

Les serveurs principaux peuvent contenir plusieurs fichiers de certificat/clé privée. Tant qu'un client peut s'authentifier avec l'une des clés sur un serveur principal, il peut communiquer avec ce dernier.

Un utilitaire est inclus dans ce produit et exécute la deuxième option décrite ci-dessus. L'utilitaire de migration des données du serveur principal (CoreDataMigration.exe) est installé dans le dossier \ProgramFiles\LANDesk\ManagementSuite. Il gère la sauvegarde et la copie des données telles que les clés et les certificats lorsque vous installez un nouveau serveur principal.

Pour enregistrer et restaurer un ensemble de certificat/clé privée

1. Sur le serveur principal source, accédez au dossier \Programmes\LANDesk\Shared Files\Keys.
2. Copiez les fichiers <nom_clé>.key, <nom_clé>.crt et <charabia>.0 du serveur source sur une disquette ou tout autre emplacement sûr.
3. Sur le serveur principal de destination, copiez les fichiers du serveur principal source vers le même dossier (\Programmes\LANDesk\Shared Files\Keys). Les clés prennent effet immédiatement.

Avertissement : Gardez le fichier de clé privé dans un lieu sûr
Assurez-vous que la clé privée <nom_clé>.key n'est pas compromise. N'utilisez pas une méthode non sécurisée de transfert, comme un courrier électronique ou un partage de fichier public. Le serveur principal utilise ce fichier pour authentifier les périphériques et tout serveur principal doté du fichier <nom_clé>.key approprié peut effectuer des exécutions distantes et des transferts de fichiers sur un périphérique géré.

Astuces de dépannage

Les astuces de dépannage suivantes sont destinées aux problèmes rencontrés le plus fréquemment lors de l'utilisation de la console.

Je ne peux pas activer le serveur principal.
Si vous avez installé un serveur principal, puis modifié l'heure du périphérique, vous ne pourrez pas l'activer. Pour activer le serveur principal, vous devez réinstaller le produit.

Lorsque j'essaye d'activer le serveur principal, un message d'erreur indiquant qu'il est impossible de lire la base de données du serveur principal s'affiche.
Assurez-vous que le serveur principal est physiquement connecté au réseau et qu'il dispose d'une connexion Internet valide. Si un câble est débranché ou si la connexion Internet du serveur principal n'est pas valide, il est impossible de terminer le processus d'activation.

Je ne connais pas l'URL des pages de la console.
Contactez la personne qui a installé le serveur principal. Il s'agit en toute probabilité de l'administrateur réseau pour votre site. En général, l'URL pour Server Manager et System Manager est http://*nom de l'ordinateur du serveur principal*/ldsm. L'URL pour Management Suite est http://*nom de l'ordinateur du serveur principal*/remote.

Sous quel utilisateur suis-je connecté ?
Examinez la zone au-dessus de la barre sous le nom LANDeskSystem Manager, dans la section **Connecté en tant que**.

À quel ordinateur suis-je connecté ?
Examinez la zone au-dessus de la barre sous le nom LANDeskSystem Manager, dans la section **Connecté à**.

Je lance System Manager et j'obtiens immédiatement le message "Expiration de la session".
Si vous ouvrez System Manager à partir du menu Favoris ou Signets avec l'extension "/frameset.aspx" à la fin de l'URL, il ne démarre pas correctement. Pour corriger ce problème, supprimez cette extension dans le lien du menu Signets ou Favoris, ou collez l'URL (sans l'extension) directement dans la fenêtre du navigateur.

Je ne vois pas certains liens dans le volet de navigation de gauche.
Ceci se produit car l'administrateur réseau utilise l'administration basée sur les rôles de LANDeskSystem Manager ou des options de sécurité au niveau des fonctions vous empêchent d'effectuer certaines tâches que vous avez le droit d'exécuter.

Le scanner ne peut pas se connecter au périphérique.
Si le scanner ne peut pas se connecter au périphérique, assurez-vous que la configuration du répertoire d'applications Web est correcte. Si vous utilisez des http, votre certificat doit être valide. Veuillez vous assurer que vous avez un certificat valide.

Je reçois une erreur "autorisation refusée" lorsque je tente d'accéder à la console.
Pour utiliser la sécurité au niveau des fonctions sur Windows 2000 et 2003, vous devez désactiver l'authentification anonyme. Vérifiez les paramètres d'authentification sur le site Web et le dossier ..\LANDesk\ldsm sous le site Web.

1. Sur le serveur qui héberge la console Web, cliquez sur **Démarrer | Outils d'administration | Internet Information Services (IIS) Manager**.
2. Depuis le menu contextuel **Site Web par défaut**, cliquez sur **Propriétés**.
3. Dans l'onglet **Sécurité de répertoire**, cliquez sur **Modifier** dans la zone **Connexions anonymes et contrôle d'authentification**. Désactivez l'option **Activer la connexion anonyme** et sélectionnez l'option **Authentification intégrée Windows**.
4. Cliquez sur **OK** pour fermer les boîtes de dialogue.
5. Depuis le sous-dossier .\LANDesk\ldsm du site Web par défaut, cliquez sur **Propriétés**. Répétez les étapes 3 et 4.

J'obtiens une session non valide lorsque j'affiche la console.
Il est possible que la session du navigateur ait expiré. Pour lancer une nouvelle session, cliquez sur le bouton **Actualiser** du navigateur.

Une erreur ASP.NET s'affiche lorsque je tente de lancer la console Web.
Si un message d'erreur ASP.NET apparaît lorsque vous tentez de vous connecter à la console Web, il est possible que ASP et les autorisations de répertoire ASP ne soient pas correctement configurés. Réinitialisez la configuration ASP.NET en exécutant la commande suivante :

```
ASPNET_REGIIS.EXE -i
```

Le nombre d'éléments par page est différent du nombre que j'ai spécifié.
Lorsque vous spécifiez le nombre d'éléments à afficher par page, ce paramètre est stocké dans le répertoire des cookies du navigateur Web et expire lorsque la session de la console expire.

La console expire trop fréquemment.
Vous pouvez modifier le délai d'expiration de session par défaut pour les pages Web de la console. Le délai d'inactivité IIS par défaut est 20 minutes avant qu'une connexion n'expire. Pour modifier le délai de session IIS :

1. Sur le serveur Web, ouvrez le Gestionnaire de services Internet IIS.
2. Développez le site Web par défaut.
3. Cliquez avec le bouton droit de la souris sur le dossier **LDSM**, puis cliquez sur **Propriétés**.
4. Sous l'onglet **Répertoire virtuel**, cliquez sur **Configuration**.
5. Cliquez sur l'onglet **Options d'application**, puis modifiez le délai de session sur la valeur souhaitée.

Remarque :LANDeskSystem Manager8.70 est un produit basé sur une session. Ne désactivez pas l'état de la session.

Les diagrammes de rapport ne s'affichent pas correctement.
Pour afficher les diagrammes et graphes à barres interactifs qui s'affichent dans de nombreux rapports, Macromedia Flash Player* doit être installé. Assurez-vous que Flash est installé, puis exécuter à nouveau le rapport.

Pourquoi est-ce que je vois deux instances du même périphérique dans ma base de données ?
Avez-vous supprimé puis réinstallé un périphérique de la base de données principale à l'aide de UninstallWinClient.exe ?

UninstallWinClient.exe se trouve dans le partage LDMain, qui correspond au dossier programme

ManagementSuite principal. Seuls les administrateurs ont accès à ce partage. Ce programme désinstalle les agents LANDesk sur tout périphérique sur lequel il est exécuté. Vous pouvez le placer dans un dossier ou l'ajouter à un script de connexion. Il s'agit d'une application Windows qui s'exécute en mode silencieux sans afficher une interface. Deux instances du périphérique 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. Reportez-vous au *Guide de déploiement* pour obtenir plus d'informations sur UninstallWinClient.exe.

Lorsque je tente de découvrir un périphérique IPMI, celui-ci n'est pas ne s'affiche pas dans le dossier IPMI de la page Périphériques non gérés.
Les périphériques IPMI doivent disposer d'un BMC (Contrôleur de gestion de la carte de base) qui est configuré pour être découvert comme périphérique IMPI et pour utiliser des fonctions IPMI complètes. Si le contrôleur BMC n'est pas configuré, le périphérique peut être découvert comme un ordinateur. Vous pouvez alors ajouter le périphérique à la liste des périphériques gérés et exécuter l'utilitaire Configuration des services pour configurer un mot de passe BMC. Les fonctions IPMI du périphérique seront alors reconnues par ce produit.

J'ai ajouté un lecteur S.M.A.R.T. sur un serveur, mais aucune surveillance du lecteur S.M.A.R.T. ne s'affiche dans la liste d'inventaire de ce serveur.
La surveillance de matériel dépend des possibilités du matériel installé sur un périphérique, ainsi que sur la configuration correcte du matériel. Si un disque dur muni de fonctions de surveillance S.M.A.R.T. est installé sur un périphérique mais que la détection S.M.A.R.T n'est pas activée dans les paramètres BIOS du périphérique, ou si le BIOS du périphérique ne prend pas en charge les lecteurs S.M.A.R.T., la surveillance des données ne sera pas disponible et aucune alerte ne sera générée.

Un périphérique de disque USB ne s'affiche pas dans la liste d'inventaire tant que l'analyse d'inventaire n'a pas été exécutée.
Lorsqu'un périphérique de disque est connecté via un câble USB à un périphérique géré, il ne s'affiche pas immédiatement dans la liste Disques durs dans l'inventaire du périphérique. Il s'affiche sous Lecteurs logiques après avoir été connecté au périphérique. Il ne s'affichera pas sous Disques durs tant qu'une analyse d'inventaire n'aura pas été exécutée sur le périphérique.

Sur les périphériques gérés Linux, un périphérique de disque USB doit être monté pour être répertorié dans l'inventaire. S'il est monté, mais qu'aucune analyse d'inventaire n'a été exécutée, il s'affiche sous Lecteurs logiques ; une fois l'analyse d'inventaire exécutée, il s'affiche également sous Disques durs. Lorsque le périphérique est déconnecté, il doit être démonté du système. Sur certains systèmes Linux qui exécutent un ancien noyau, le périphérique peut également rester dans la liste d'inventaire, même après la déconnexion et le démontage. Si tel est le cas, le périphérique géré doit être redémarré avant que le périphérique ne soit supprimé de la liste d'inventaire.

Lorsque j'affiche l'index d'aide de la console Web, ce dernier est vide.
L'aide en ligne au format HTML de la console Web comporte une fonction de recherche texte intégral qui dépend du Service d'indexation Windows. Normalement, cette fonction est activée par défaut. Pour activer l'indexation sur le serveur Web, procédez comme suit :

1. Cliquez sur **Démarrer | Programmes | Outils d'administration | Services**.
2. Cliquez deux fois sur **Service d'indexation**, puis cliquez sur **Démarrer**.
3. Cliquez sur **OK** pour quitter les boîtes de dialogue.

Vous devrez patienter pendant un certain temps (jusqu'à quelques heures) pour que le service d'indexation indexe votre serveur.