Référence de la gestion à distance

Novell®
ZENworks® 10 Configuration Management avec SP3

10.3

30 mars 2010

www.novell.com

Mentions légales

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

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

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

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

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

Marques de Novell

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

Éléments tiers

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

Table des matières

À propos de ce guide

Le présent guide *Référence de gestion à distance de Novell ZENworks 10 Configuration Management* contient des informations sur la gestion à distance. Il est organisé de la manière suivante :

Public

Le présent guide est destiné aux administrateurs de Novell® ZENworks®.

Commentaires

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

Documentation complémentaire

D'autres manuels (aux formats PDF et HTML) viennent compléter la documentation relative à ZENworks Configuration Management. Ils facilitent l'apprentissage et la mise en œuvre de ce produit. Pour obtenir de la documentation supplémentaire, consultez le site Web de documentation de ZENworks 10 Configuration Management avec SP3 (http://www.novell.com/documentation/zcm10/).

Conventions relatives à la documentation

Dans la documentation Novell, le symbole «supérieur à» (>) est utilisé pour séparer deux opérations dans une étape de procédure ainsi que deux éléments dans un chemin de références croisées.

Un symbole de marque déposée (®, ™, etc.) indique qu'il s'agit d'une marque de Novell. Un astérisque (*) indique une marque commerciale de fabricant tiers.

Lorsqu'un nom de chemin peut s'écrire avec une barre oblique pour certaines plates-formes et une barre oblique inverse pour d'autres, il sera toujours présenté avec une barre oblique inverse. Les utilisateurs des plates-formes nécessitant l'utilisation de barres obliques (Linux*, par exemple) doivent les utiliser en fonction de leurs logiciels.

Présentation

1

Novell® ZENworks® Configuration Management permet de gérer des périphériques à distance à partir de la console de gestion. La gestion à distance permet :

- de contrôler à distance le périphérique géré ;
- de lancer à distance les exécutables sur le périphérique géré ;
- de transférer des fichiers entre la console de gestion et le périphérique géré ;
- d'analyser les problèmes sur le périphérique géré ;
- d'activer à distance un périphérique géré désactivé.

Reportez-vous aux sections suivantes :

1.1 Terminologie de la gestion à distance

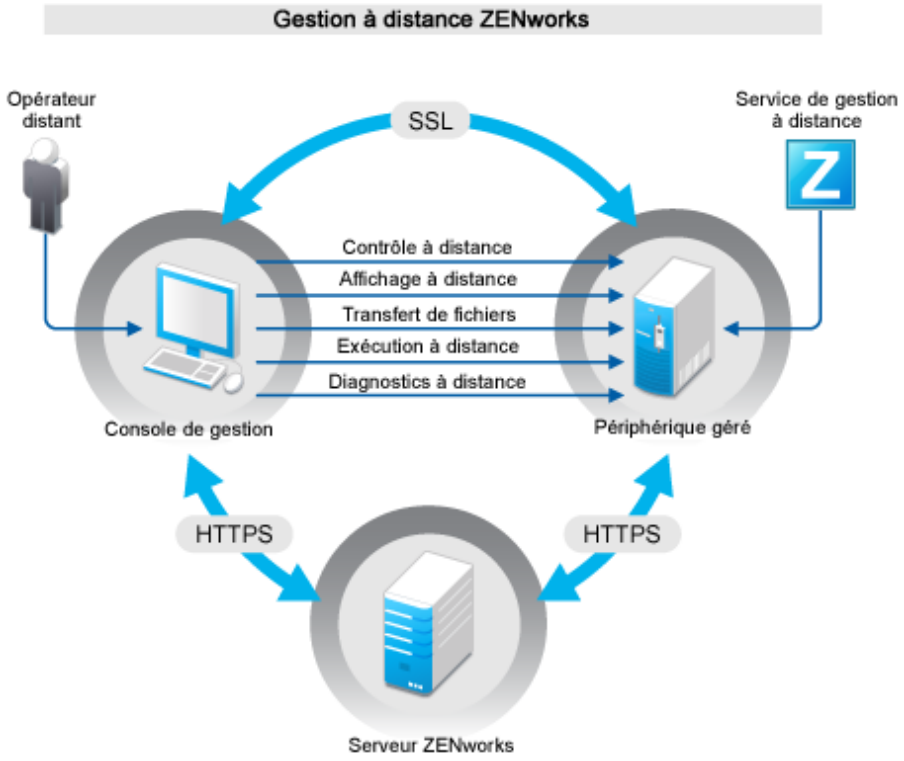
Termes	Description
Périphérique géré	Périphérique que vous souhaitez gérer à distance. Pour gérer un périphérique à distance, vérifiez que le composant de gestion à distance est bien installé et que le service correspondant est exécuté sur le périphérique.
Serveur de gestion	Périphérique sur lequel est installé le serveur ZENworks Configuration Management.
Console de gestion	Interface de gestion et d'administration des périphériques. Pour exécuter des opérations à distance, vous devez installer la visionneuse de gestion à distance sur la console.
administrateur	Personne autorisée à configurer les stratégies et paramètres de gestion à distance et à accorder des droits de gestion à distance aux opérateurs distants.
Service de gestion à distance	Composant de périphérique géré qui permet aux opérateurs à distance d'exécuter des opérations à distance sur le périphérique.
Visionneuse de gestion à distance	Application de la console de gestion qui permet à un opérateur à distance d'exécuter des opérations à distance sur le périphérique géré. La visionneuse permet à l'opérateur à distance de visualiser le bureau du périphérique géré, ainsi que de transférer des fichiers et d'exécuter des applications sur ce périphérique.
Module d'écoute de gestion à distance	Application de la console de gestion qui permet à un opérateur distant d'accepter les demandes d'assistance distante envoyées par les utilisateurs du périphérique géré.

Termes	Description
Proxy de gestion à distance	Serveur proxy qui transmet des demandes d'opération de Gestion à distance depuis la visionneuse de gestion à distance vers un périphérique géré. Le proxy est utile lorsque la visionneuse ne peut pas directement accéder à un périphérique géré qui se trouve dans un réseau privé ou de l'autre côté d'un pare-feu ou d'un routeur qui utilise la traduction d'adresses réseau (NAT). L'installation du proxy sur un périphérique géré Windows ou sur un périphérique Linux (serveur primaire ou satellite) est une condition préalable.

1.2 Présentation des opérations de gestion à distance

La gestion à distance permet aux administrateurs de contrôler un périphérique sans avoir à effectuer de visite en ligne. Elle vous permet, à vous comme à votre organisation, de gagner du temps et de l'argent. Elle permet par exemple, à vous ou au service d'assistance de votre organisation, d'analyser et de corriger à distance les problèmes survenant sur un périphérique géré, et ce sans avoir à contrôler physiquement le poste de travail de l'utilisateur. Il s'agit d'un excellent moyen de réduire les temps de résolution des problèmes et d'augmenter votre productivité.

Figure 1-1 *Opérations de gestion à distance*



Les sections suivantes vous présentent les différentes opérations de gestion à distance :

- Section 1.2.1, « Contrôle à distance », page 13
- Section 1.2.2, « Affichage à distance », page 13
- Section 1.2.3, « Exécution à distance », page 13

1.2.1 Contrôle à distance

Le contrôle à distance permet de contrôler le périphérique géré depuis la console de gestion de façon à pouvoir assister les utilisateurs et les aider à résoudre les problèmes survenant au niveau du périphérique.

Le contrôle à distance établit une connexion entre la console de gestion et le périphérique géré. Grâce à ces connexions, vous pouvez exécuter sur le périphérique toutes les opérations qui sont à la portée d'un utilisateur. Pour plus d'informations, reportez-vous à la Section 3.1, « Gestion d'une session d'affichage à distance », page 53.

1.2.2 Affichage à distance

L'affichage à distance permet de vous connecter à distance à un périphérique géré et de le visualiser simplement, sans le contrôler. Cela vous aide à résoudre les problèmes rencontrés par l'utilisateur. Vous pouvez par exemple examiner la manière dont l'utilisateur d'un périphérique géré effectue certaines tâches afin d'en vérifier la bonne exécution. Pour plus d'informations, reportez-vous à la Section 3.2, « Gestion d'une session d'affichage à distance », page 57.

1.2.3 Exécution à distance

L'exécution à distance permet de lancer n'importe quel exécutable sur le périphérique géré depuis la console de gestion à l'aide de privilèges système. Pour exécuter une application à distance, vous devez spécifier le nom de l'exécutable dans la fenêtre Exécution à distance. Par exemple, vous pouvez exécuter la commande `regedit` pour ouvrir l'éditeur de registre sur le périphérique. Pour plus d'informations, reportez-vous à la Section 3.3, « Gestion d'une session d'exécution à distance », page 58.

1.2.4 Diagnostic à distance

Le diagnostic à distance permet de diagnostiquer et d'analyser à distance les problèmes survenant sur le périphérique géré. Les bureaux étant opérationnels, la productivité de l'utilisateur s'en trouve accrue. Pour plus d'informations, reportez-vous à la Section 3.4, « Gestion d'une session de diagnostic à distance », page 59.

Le diagnostic fournit des informations en temps réel que vous pouvez utiliser pour diagnostiquer et corriger les problèmes sur le périphérique géré. Le service comprend différentes applications de diagnostic par défaut :

- Informations système
- Gestion de l'ordinateur
- Services
- Éditeur de registre

1.2.5 Transfert de fichier

Le transfert de fichier permet d'effectuer différentes opérations de fichier sur la console de gestion et sur le périphérique géré, par exemple :

- copier des fichiers entre la console de gestion et le périphérique géré ;
- renommer des fichiers ou dossiers ;
- supprimer des fichiers ou dossiers ;
- créer des dossiers ;
- afficher les propriétés des fichiers et des dossiers ;
- ouvrir des fichiers avec les applications associées sur la console de gestion.

Pour plus d'informations, reportez-vous à la Section 3.5, « Gestion d'une session de transfert de fichiers », page 60.

Important : le programme de transfert de fichier permet également d'accéder aux lecteurs réseau du périphérique géré.

1.2.6 Activation à distance

L'activation à distance permet d'activer un nœud unique ou un groupe de noeuds mis hors tension sur votre réseau à condition que la carte réseau sur le nœud soit compatible avec le service Wake-on-LAN. Pour plus d'informations, reportez-vous à la Section 3.7, « Activation d'un périphérique distant », page 64.

1.3 Présentation des fonctions de gestion à distance

Les sections suivantes présentent les différentes fonctions de gestion à distance :

1.3.1 Signal visible

Cette indication apparaît sur le bureau du périphérique géré pour informer l'utilisateur que le périphérique est géré à distance. Le signal visible affiche l'identification de l'opérateur distant ainsi que les détails de session, tels que le type de session distante et l'heure de début de la session. L'utilisateur peut mettre fin à une session distante donnée ou fermer la boîte de dialogue du signal pour mettre fin à toutes les sessions distantes.

1.3.2 Détection d'intrus

La fonction de détection d'intrus réduit considérablement le risque de piratage du périphérique géré. Si l'opérateur distant ne parvient pas à se connecter au périphérique avec le nombre de tentatives autorisé (5 par défaut), le service de gestion à distance est automatiquement bloqué et refuse toute requête de session distante jusqu'à ce qu'il soit débloqué.

1.3.3 Codage de session

Les sessions distantes sont sécurisées à l'aide du protocole Secured Socket Layer (protocole TLSv1).

1.3.4 Bip sonore

Si une session à distance est active sur le périphérique géré, vous pouvez générer un bip sonore à intervalles réguliers sur le périphérique géré conformément à la configuration de la stratégie de gestion à distance.

1.3.5 Verrouillage du clavier et de la souris

Permet de verrouiller les commandes du clavier et de la souris du périphérique géré au cours de la session à distance.

Remarque : sur les périphériques gérés Windows Vista, le verrouillage du clavier et de la souris ne fonctionne pas si le thème Aero est activé.

1.3.6 Suppression du contenu de l'écran

Cette fonction permet de supprimer le contenu de l'écran sur le périphérique géré au cours d'une session distante afin d'éviter que l'utilisateur ne voie les actions exécutées par l'opérateur distant durant cette session. Les commandes du clavier et de la souris du périphérique géré sont également verrouillées.

Remarque : la suppression du contenu à l'écran d'un périphérique géré Tablet PC pendant une session à distance affecte les performances de la session.

1.3.7 Fin anormale

Cette fonction permet de verrouiller le périphérique géré ou de déconnecter l'utilisateur du périphérique géré en cas de déconnexion soudaine d'une session distante.

1.3.8 Remplacement de l'écran de veille

Cette fonction permet de remplacer un écran de veille protégé par un mot de passe sur le périphérique géré au cours d'une session distante.

Remarque : cette fonction n'est pas disponible sur un périphérique géré Windows Vista*, Windows Server 2008 ou Windows 7.

1.3.9 Fin automatique de la session

Met fin automatiquement à une session à distance au terme de la durée d'inactivité spécifiée.

1.3.10 Connexion initiée par l'agent

Cette fonction permet à l'utilisateur du périphérique géré de demander de l'aide à un opérateur distant. Vous pouvez préconfigurer la liste des opérateurs distants disponibles pour l'utilisateur. Pour plus d'informations, reportez-vous à la Section 2.8.2, « Lancement d'une session à partir du périphérique géré », page 44.

Remarque : cette fonction n'est actuellement prise en charge que sous Windows.

1.3.11 Collaboration de session

Cette fonction permet à un groupe d'opérateurs distants de participer ensemble à une session distante. L'opérateur distant principal peut inviter d'autres opérateurs distants à rejoindre la session, déléguer les droits de contrôle distant à un autre opérateur distant afin de résoudre un problème, reprendre le contrôle à l'opérateur distant et mettre fin à une session distante. Pour plus d'informations, reportez-vous à la Section 3.1.2, « Collaboration de session », page 55.

1.3.12 Audit de gestion à distance

Cette fonction permet de générer des rapports d'audit pour chaque session distante exécutée sur le périphérique géré. Le journal d'audit est conservé sur le périphérique géré et est consultable par l'utilisateur.

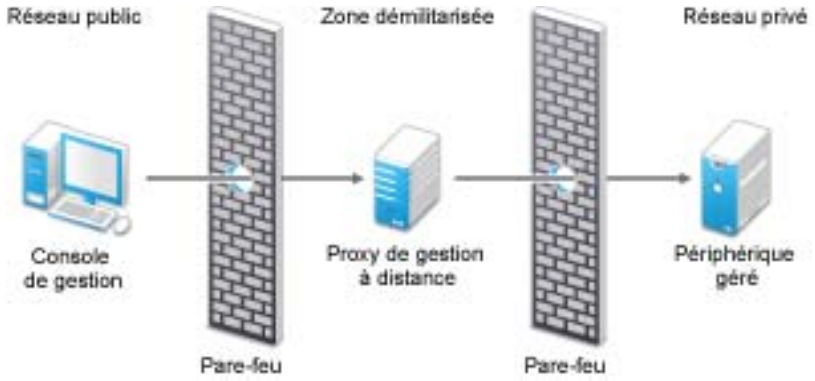
1.4 Présentation du proxy de gestion à distance

Vous ne pouvez pas effectuer d'opération de gestion à distance sur un périphérique géré qui se trouve sur un réseau privé ou de l'autre côté d'un pare-feu ou d'un routeur qui utilise la traduction d'adresses réseau (NAT). En effet, le pare-feu NAT masque l'adresse IP du périphérique depuis le réseau externe et bloque ainsi les demandes de connexion au périphérique. Afin de gérer à distance ce type de périphérique, les opérations à distance doivent être routées via un proxy de gestion à distance.

Pour plus d'informations sur le routage de l'opération à distance via un proxy au moment du lancement d'une session à distance depuis la console de gestion, consultez la description du champ Router via le proxy au point « Lancement d'une session de gestion à distance depuis le contexte de périphérique » page 37.

Pour plus d'informations sur le routage de l'opération à distance via un proxy au moment du lancement d'une session à distance depuis le périphérique, consultez la description du champ Router via le proxy au point « Lancement d'une session de gestion à distance à partir du contexte utilisateur » page 40.

Figure 1-2 *Proxy de gestion à distance*



Vous devez installer le proxy sur un périphérique situé dans une zone démilitarisée. Le périphérique sur lequel vous installez le proxy doit être accessible depuis le réseau public qui comporte la console de gestion et doit avoir accès à des périphériques relevant d'un réseau privé. Pour plus d'informations sur l'installation du proxy de gestion à distance, consultez la Section 2.10, « Installation d'un proxy de gestion à distance », page 49.

Le proxy de gestion à distance écoute sur le port 5750 par défaut pour les requêtes de gestion à distance entrantes provenant de la visionneuse de gestion à distance et les transfère au périphérique.

Installation de la gestion à distance

2

Les sections suivantes fournissent des informations concernant le déploiement du composant de gestion à distance de Novell® ZENworks® 10 Configuration Management dans un environnement de production :

2.1 Configuration des paramètres de gestion à distance

Les paramètres de gestion à distance sont des règles qui déterminent le comportement ou l'exécution du service de gestion à distance sur le périphérique géré. Ces paramètres englobent la configuration des ports, les paramètres de session ainsi que les paramètres de performance pendant la session à distance. Ces paramètres peuvent être appliqués au niveau de la zone, du dossier et du périphérique.

Les sections suivantes fournissent des informations sur la configuration des paramètres de gestion à distance à ces différents niveaux :

2.1.1 Configuration des paramètres de gestion à distance au niveau de la zone

Les paramètres de gestion à distance configurés au niveau de la zone s'appliquent par défaut à tous les périphériques gérés.

1. Dans le Centre de contrôle ZENworks, cliquez sur *Configuration*.
2. Dans le panneau Paramètres de la zone de gestion, cliquez sur *Gestion des périphériques*, puis sur *Gestion à distance*.
3. Sélectionnez *Exécuter le service de gestion distante sur le port* et spécifiez le port pour activer l'exécution du service de gestion à distance sur ce port.

   Par défaut, le service de gestion à distance reçoit les données sur le port 5950.
4. Sélectionnez les options de paramètres de session :

Champ	Détails
Rechercher le nom DNS de la visionneuse au début de la session distante	Permet au service de gestion à distance de rechercher le nom DNS de la console de gestion au démarrage de la session à distance. Le nom est enregistré dans les journaux d'audit et s'affiche dans les informations de session des sessions à distance. Si cette option n'est pas sélectionnée ou si le service de gestion à distance ne parvient pas à trouver le nom de la console, ce dernier apparaît comme *inconnu*. Si la consultation du nom DNS n'est pas activée sur votre réseau, nous vous recommandons de désactiver ce paramètre afin d'éviter tout retard important lors du démarrage de la session à distance.
Autoriser une session distante lorsqu'aucun utilisateur n'est logué au périphérique géré	Permet à un opérateur à distance de gérer un périphérique à distance lorsque la stratégie autorise l'opération à distance et qu'aucun utilisateur n'est logué au périphérique. Cette option est sélectionnée par défaut.

5. Dans la liste suivante, sélectionnez les options de votre choix afin d'améliorer les performances des sessions à distance.

Champ	Détails
Supprimer le papier peint	Supprime le papier peint sur le périphérique géré au cours d'une session distante. Permet d'éviter que les données bitmap du papier peint soient envoyées plusieurs fois à la console de gestion à distance et d'améliorer ainsi les performances de la session distante.
Activer le pilote d'optimisation	Active le pilote d'optimisation qui est installé par défaut sur chaque périphérique géré. Si vous sélectionnez cette option, seule la partie de l'écran du périphérique géré est capturée et mise à jour sur la console de gestion à distance au cours de la session distante, ce qui améliore les performances de la session distante.

6. (Facultatif) Configurez un proxy de gestion à distance pour l'exécution des opérations à distance sur le périphérique géré.

Si le périphérique géré se trouve sur un réseau privé ou de l'autre côté d'un pare-feu ou routeur qui utilise la traduction d'adresses réseau (NAT), l'opération de gestion à distance du périphérique peut être routée via un proxy de gestion à distance. Le proxy doit être installé séparément. Pour plus d'informations sur l'installation du proxy de gestion à distance, consultez la Section 2.10, « Installation d'un proxy de gestion à distance », page 49.

Tâche	Détails
Ajouter un proxy de gestion à distance	1. Cliquez sur *Ajouter* pour afficher la boîte de dialogue Ajouter des paramètres de proxy. 2. Renseignez les champs suivants : **Proxy :** indiquez l'adresse IP ou le nom DNS du proxy de gestion à distance. **Plage d'adresses IP :** indiquez les adresses IP des périphériques que vous souhaitez gérer à distance via le proxy de gestion à distance. Vous pouvez définir la plage d'adresses IP de l'une des manières suivantes : ◆ Spécifiez la plage d'adresses IP à l'aide de la notation CIDR (Classless Inter-Domain Routing). Avec CIDR, la portion décimale en pointillés de l'adresse IP est interprétée comme un nombre binaire 32 bits qui a été séparé en quatre octets de 8 bits. Le nombre suivant la barre oblique (/n) est la longueur du préfixe, c'est-à-dire le nombre de bits initiaux partagés à partir du côté gauche de l'adresse. Le nombre /n peut varier de 0 à 32, 8, 16, 24 et 32 étant des valeurs couramment utilisées. Exemples : 123.45.678.12/16 : spécifie toutes les adresses IP qui commencent par 123.45. 123.45.678.12/24 : spécifie toutes les adresses IP qui commencent par 123.45.678. ◆ Spécifiez la plage d'adresses IP au format suivant : **première adresse IP** - **dernière adresse IP**. Exemple : 123.45.678.12 - 123.45.678.15 : spécifie toutes les adresses IP comprises entre 123.45.678.12 et 123.45.678.15.
Supprimer un proxy de gestion à distance	1. Sélectionnez le proxy à supprimer. 2. Cliquez sur Supprimer, puis sur *OK*.

7 (Facultatif) Configurez une application à exécuter sur le périphérique géré pendant la session de diagnostic à distance en l'ajoutant simplement à la liste *Applications de diagnostic*. Par défaut, cette liste comprend les applications suivantes :

- Informations système
- Gestion de l'ordinateur
- Services
- Éditeur de registre

Le tableau suivant décrit les tâches que vous pouvez exécuter pour personnaliser la liste *Applications de diagnostic* :

Tâche	Détails
Ajouter une application	1. Cliquez sur *Ajouter.* 2. Indiquez le nom et le chemin de l'application sur le périphérique géré. 3. Cliquez sur *OK*.
Supprimer une application	1. Sélectionnez l'application que vous souhaitez supprimer. 2. Cliquez sur Supprimer, puis sur *OK*.
Rétablir les applications par défaut	1. Cliquez sur *Rétablir*, puis sur *OK*.

8 Cliquez sur *Appliquer*, puis sur *OK*.

Ces modifications sont effectives sur le périphérique au moment de son rafraîchissement.

2.1.2 Configuration des paramètres de gestion à distance au niveau du dossier

Les paramètres de gestion à distance configurés au niveau de la zone sont appliqués par défaut à tous les périphériques gérés. Vous pouvez toutefois modifier ces paramètres pour les périphériques contenus dans un dossier :

1 Dans le Centre de contrôle ZENworks, cliquez sur *Périphériques*.

2 Cliquez sur le dossier (détails) dont vous voulez configurer les paramètres de gestion à distance.

3 Cliquez sur *Paramètres*, puis sur *Gestion des périphériques* > *Gestion à distance*.

4 Cliquez sur *Remplacer*.

5 Apportez les modifications nécessaires aux paramètres de gestion à distance.

6 Pour appliquer les changements, cliquez sur *Appliquer*.

ou

Pour rétablir les paramètres du système au niveau de la zone, cliquez sur *Rétablir*.

7 Cliquez sur *OK*.

Ces modifications seront effectives sur le périphérique au moment de son rafraîchissement.

2.1.3 Configuration des paramètres de gestion à distance au niveau du périphérique

Les paramètres de gestion à distance configurés au niveau de la zone sont appliqués par défaut à tous les périphériques gérés. Vous pouvez toutefois modifier ces paramètres pour le périphérique géré :

1 Dans le Centre de contrôle ZENworks, cliquez sur *Périphériques*.

2 Cliquez sur *Serveurs* ou *Postes de travail* pour afficher la liste des périphériques gérés.

3 Cliquez sur le périphérique dont vous voulez configurer les paramètres de gestion à distance.

4 Cliquez sur *Paramètres*, puis sur *Gestion des périphériques* > *Gestion à distance*.

5 Cliquez sur *Remplacer*.

6 Apportez les modifications nécessaires aux paramètres de gestion à distance.

7 Pour appliquer les changements, cliquez sur *Appliquer*.

ou

Pour rétablir les paramètres système configurés précédemment sur le périphérique, cliquez sur *Rétablir*.

Si les paramètres de gestion à distance du périphérique étaient configurés au niveau du dossier, les paramètres rétablis sont ceux qui étaient au niveau du dossier configuré. Dans le cas contraire, ce sont ceux de la zone par défaut qui sont rétablis.

8 Cliquez sur *OK*.

Ces modifications seront effectives sur le périphérique au moment de son rafraîchissement.

2.2 Activation du module d'écoute de gestion à distance

Pour activer un module d'écoute de gestion à distance afin d'écouter les connexions depuis un périphérique géré, procédez comme suit :

1 Dans le Centre de contrôle ZENworks, cliquez sur *Périphériques*.

2 Dans le champ *Tâches du périphérique* à gauche de l'écran, cliquez sur *Module d'écoute de gestion à distance*.

3 Dans la boîte de dialogue Module d'écoute de gestion à distance, indiquez le port à utiliser pour écouter les connexions distantes. Par défaut, le numéro de port est le 5550.

4 Cliquez sur *OK*.

L'icône Module d'écoute de ZENworks Remote Management apparaît dans la zone de notification.

2.3 Création de la stratégie de gestion à distance

La stratégie de gestion à distance permet de configurer le comportement ou l'exécution de la session de gestion à distance sur le périphérique géré. La stratégie inclut les paramètres pour les opérations de gestion à distance telles que le Contrôle à distance, l'Affichage à distance, l'Exécution à distance, le Diagnostic à distance et le Transfert de fichier, et permet de contrôler les paramètres de sécurité.

Par défaut, une stratégie de gestion à distance sécurisée est créée sur le périphérique géré lors du déploiement de ZENworks Adaptive Agent sur le périphérique avec le composant de gestion à distance. La stratégie par défaut peut être utilisée pour la gestion à distance d'un périphérique. Pour ignorer la stratégie par défaut, vous devez explicitement créer une stratégie de gestion à distance pour le périphérique.

1 Dans le Centre de contrôle ZENworks, cliquez sur l'onglet *Stratégies*.

2 Dans la liste *Stratégies*, cliquez sur *Nouveau*, puis sur *Stratégie* pour afficher la page Sélectionner le type de stratégie.

3 Sélectionnez *Stratégie de gestion à distance*, cliquez sur *Suivant* pour afficher la page Définir les détails, puis renseignez les champs :

Nom de la stratégie : indiquez un nom unique pour votre stratégie. Le nom de la stratégie doit être différent de celui d'un autre élément quel qu'il soit (groupe, dossier, etc.) se trouvant dans le même dossier.

Dossier : saisissez le nom ou recherchez et sélectionnez le dossier du Centre de contrôle ZENworks dans lequel vous voulez que la stratégie réside. Le choix par défaut est `/policies`, mais vous pouvez créer des dossiers supplémentaires pour organiser vos stratégies.

Description : fournissez une brève description du contenu de la stratégie. Cette description est affichée dans la page Résumé de la stratégie du Centre de contrôle ZENworks.

4 Cliquez sur *Suivant* pour afficher la page Paramètres généraux de gestion à distance. Pour accepter les paramètres par défaut, passez à l'étape suivante ou utilisez les informations spécifiées dans le tableau suivant pour changer les paramètres par défaut.

Champ	Détails
Permettre à l'utilisateur de demander une session à distance	Permet à l'utilisateur du périphérique géré de demander à un opérateur distant de démarrer une session distante. L'opérateur distant doit s'assurer que le module d'écoute de gestion à distance est en cours d'exécution.
Mettre fin à la session à distance lorsqu'une autorisation est requise de la part d'un nouvel utilisateur se connectant au périphérique géré	Met fin à une session à distance en cours lorsqu'une autorisation est requise de la part d'un nouvel utilisateur qui s'est connecté à un périphérique géré à distance.
Afficher les informations de vérification de la session à distance pour l'utilisateur sur le périphérique géré	Permet à l'utilisateur du périphérique géré d'afficher les informations d'audit des sessions distantes à partir de l'icône ZENworks.
Afficher les propriétés de la gestion à distance dans ZENworks Icon	Permet à l'utilisateur du périphérique géré d'afficher les propriétés associées à la stratégie de gestion à distance dans l'icône ZENworks.
Modifier	Pour éditer le message affiché à l'utilisateur sur le périphérique géré avant de démarrer une session distante : 1. Cliquez sur *Modifier* pour afficher la boîte de dialogue Modifier le message. 2. Modifiez le message. 3. Cliquez sur *OK*.
Restaurer les valeurs par défaut	Pour restaurer le message par défaut : 1. Cliquez sur *Restaurer les valeurs par défaut* pour restaurer le message par défaut.
Ajouter un module d'écoute à distance	Pour ajouter un module d'écoute à distance : 1. Cliquez sur *Ajouter*. 2. Dans la boîte de dialogue Ajouter un module d'écoute à distance, indiquez le nom DNS ou l'adresse IP de la console de gestion et le numéro du port sur lequel le module d'écoute de la gestion à distance écoutera les demandes de session à distance. 3. Cliquez sur *OK*.

Champ	Détails
Supprimer un module d'écoute à distance	Pour supprimer un module d'écoute à distance : 1. Sélectionnez le module d'écoute à distance à supprimer. 2. Cliquez sur *Supprimer*.

5 Cliquez sur *Suivant* pour afficher la page Paramètres de contrôle distant. Pour accepter les paramètres par défaut, passez à l'étape suivante ou utilisez les informations spécifiées dans le tableau suivant pour changer les paramètres par défaut.

Champ	Détails
Autoriser le contrôle à distance du périphérique géré	Autorise les sessions de contrôle distant sur le périphérique géré. La sélection de cette option active les options de la page qui en découlent. La désélection de cette option désactive l'opération de contrôle distant sur le périphérique.
Demander l'autorisation de l'utilisateur du périphérique géré avant de démarrer le contrôle à distance	Permet de demander l'autorisation à l'utilisateur du périphérique géré avant de démarrer une session de contrôle à distance.
Émettre un signal visible à l'utilisateur sur le périphérique géré au cours du contrôle à distance	Affiche un signal visible dans le coin supérieur droit du bureau du périphérique géré au cours de la session de contrôle à distance. Le signal visible permet à l'utilisateur du périphérique géré de savoir qu'une session de contrôle à distance est en cours.
Émettre un signal sonore audible pour l'utilisateur sur le périphérique géré toutes les [ ] secondes au cours du contrôle à distance	Génère un signal sonore sur le périphérique géré au cours d'une session de Contrôle distant. Le signal sonore est généré périodiquement lorsque le nombre de secondes spécifié est écoulé.
Autoriser la mise en veille de l'écran du périphérique géré lors du contrôle à distance	Active le vidage de l'écran du périphérique géré au cours d'une session de contrôle à distance. Cette option verrouille également le clavier et la souris du périphérique géré.
Autoriser le verrouillage de la souris et du clavier du périphérique géré lors du contrôle à distance	Permet de verrouiller la souris et le clavier du périphérique géré lors d'une session de Contrôle distant.
Autoriser le déverrouillage automatique de l'écran de veille lors du contrôle à distance	Autorise le déverrouillage de l'écran de veille protégé par mot de passe à partir de la visionneuse du contrôle à distance avant le démarrage d'une session de contrôle à distance sur le périphérique géré.
Terminer automatiquement la session de contrôle à distance après un délai d'inactivité de [ ] minutes	Termine une session de Contrôle à distance sur le périphérique géré s'il est resté inactif pendant le délai spécifié.

6 Cliquez sur *Suivant* pour afficher la page Paramètres de visualisation à distance. Pour accepter les paramètres par défaut, passez à l'étape suivante ou utilisez les informations spécifiées dans le tableau suivant pour changer les paramètres par défaut.

Champ	Détails
Autoriser l'Affichage à distance du périphérique géré	Autorise les sessions d'Affichage à distance sur le périphérique géré. La sélection de cette option active les options de la page qui en découlent. La désélection de cette option désactive l'opération d'Affichage à distance sur le périphérique.
Demander l'autorisation de l'utilisateur du périphérique géré avant de démarrer l'Affichage à distance	Permet de demander l'autorisation à l'utilisateur du périphérique géré avant de démarrer une session d'Affichage à distance.
Émettre un signal visible pour l'utilisateur du périphérique géré au cours de l'Affichage à distance	Affiche le signal visible dans l'angle supérieur droit du bureau du périphérique géré au cours de la session d'Affichage à distance. Le signal visible permet à l'utilisateur du périphérique géré de savoir qu'une session d'Affichage à distance est en cours.
Émettre un bip sonore pour l'utilisateur du périphérique géré toutes les [ ] secondes au cours de l'Affichage à distance	Génère un signal sonore sur le périphérique géré au cours d'une session d'Affichage à distance. Le signal sonore est généré périodiquement lorsque le nombre de secondes spécifié est écoulé.

7 Cliquez sur *Suivant* pour afficher la page Paramètres de diagnostic distant. Pour accepter les paramètres par défaut, passez à l'étape suivante ou utilisez les informations spécifiées dans le tableau suivant pour changer les paramètres par défaut.

Champ	Détails
Autoriser le diagnostic à distance du périphérique géré	Autorise les sessions de Diagnostic à distance sur le périphérique géré. La sélection de cette option active les options de la page qui en découlent. La désélection de cette option désactive l'opération de Diagnostic à distance sur le périphérique.
Demander l'autorisation de l'utilisateur du périphérique géré avant de lancer les diagnostics à distance	Vérifie que l'opérateur distant demande l'autorisation de l'utilisateur du périphérique géré avant de démarrer une session de Diagnostics distants.
Émettre un signal visible pour l'utilisateur du périphérique géré au cours des diagnostics distants	Affiche le signal visible dans l'angle supérieur droit du bureau du périphérique géré au cours de la session de Diagnostic à distance. Le signal visible permet à l'utilisateur du périphérique géré de savoir qu'une session de Diagnostic à distance est en cours.
Émettre un signal sonore audible pour l'utilisateur sur le périphérique géré toutes les [ ] secondes au cours des diagnostics distants	Génère un signal sonore sur le périphérique géré au cours d'une session de Diagnostics distants. Le signal sonore est généré périodiquement lorsque le nombre de secondes spécifié est écoulé.
Autoriser la mise en veille de l'écran du périphérique géré lors du diagnostic à distance	Active le vidage de l'écran du périphérique géré au cours d'une session de Diagnostic à distance. Le clavier et la souris du périphérique géré sont toujours verrouillés au cours d'une session de diagnostic à distance. La sélection de cette option désactive également le signal visible sur le périphérique géré.

Champ	Détails
Afficher un message d'avertissement avant le redémarrage pendant [ ] secondes	Affiche un message d'avertissement sur le périphérique géré au début de la session de Diagnostic à distance, en rappelant à l'utilisateur d'enregistrer toutes les applications existantes. Ce message d'avertissement s'affiche pendant la durée spécifiée pour éviter que l'utilisateur ne perde les données non enregistrées, car l'opérateur distant est susceptible d'effectuer un redémarrage du système au cours de la session de diagnostic à distance.
Terminer automatiquement la session de diagnostic à distance après un délai d'inactivité de [ ] minutes	Termine la session de Diagnostic à distance après le délai d'inactivité indiqué.

8 Cliquez sur *Suivant* pour afficher la page Paramètres d'exécution à distance. Pour accepter les paramètres par défaut, passez à l'étape suivante ou utilisez les informations spécifiées dans le tableau suivant pour changer les paramètres par défaut.

Champ	Détails
Autoriser l'exécution à distance des programmes sur le périphérique géré	Autorise l'exécution à distance des programmes sur le périphérique géré. La sélection de cette option active les options de la page qui en découlent. La désélection de cette option désactive l'opération d'exécution à distance sur le périphérique.
Demander l'autorisation de l'utilisateur du périphérique géré avant de démarrer l'exécution à distance	Vérifie que l'opérateur distant demande l'autorisation de l'utilisateur du périphérique géré avant de démarrer une session d'Exécution à distance.
Émettre un signal visible pour l'utilisateur sur le périphérique géré au cours de l'exécution à distance	Affiche un signal visible dans le coin supérieur droit du bureau du périphérique géré au cours de la session d'Exécution à distance. Le signal visible permet à l'utilisateur du périphérique géré de savoir qu'une session d'exécution à distance est en cours.
Terminer automatiquement la session de diagnostic à distance après un délai d'inactivité de [ ] minutes	Termine la session Exécution à distance après le délai d'inactivité indiqué.

9 Cliquez sur *Suivant* pour afficher la page Paramètres du transfert de fichier. Passez à l'étape suivante pour accepter les paramètres par défaut ou utilisez les informations du tableau suivant pour modifier les paramètres de sécurité par défaut.

Champ	Détails
Autoriser le transfert de fichiers sur un périphérique géré	Active le transfert des fichiers entre la console de gestion et le périphérique géré. La sélection de cette option active les options de la page qui en découlent. La désélection de cette option désactive l'opération de transfert de fichiers sur le périphérique.
Demander l'autorisation de l'utilisateur du périphérique géré avant de démarrer le transfert de fichiers	Vérifie que l'opérateur distant demande l'autorisation de l'utilisateur du périphérique géré avant de démarrer une session de Transfert de fichiers.

Champ	Détails
Émettre un signal visible à l'utilisateur sur le périphérique géré au cours du transfert de fichiers	Affiche un signal visible dans le coin supérieur droit du bureau du périphérique géré au cours de la session de Transfert de fichiers. Le signal visible permet à l'utilisateur du périphérique géré de savoir qu'une session de Transfert de fichiers est en cours.
Autoriser le téléchargement des fichiers à partir d'un périphérique géré	Permet à un opérateur distant d'ouvrir des fichiers sur le périphérique géré et de les transférer vers la console de gestion. Si cette option n'est pas sélectionnée, l'opérateur distant ne peut transférer des fichiers que depuis la console de gestion vers le périphérique géré.
Répertoire racine du transfert de fichiers	Indiquez le répertoire du périphérique géré que l'opérateur doit afficher au cours d'une session de transfert de fichier. L'opérateur distant ne peut transférer des fichiers que vers et à partir de ce répertoire et de ses sous-répertoires. Le répertoire par défaut est Poste de travail, ce qui signifie que l'opérateur distant peut afficher et transférer des fichiers de l'ensemble du système de fichiers du périphérique géré.

10 Cliquez sur *Suivant* pour afficher la page Paramètres de sécurité. Passez à l'étape suivante pour accepter les paramètres par défaut ou utilisez les informations du tableau suivant pour modifier les paramètres de sécurité par défaut.

Authentification par mot de passe

Champ	Détails
Activer l'authentification par mot de passe	Permet à l'opérateur distant d'utiliser un mot de passe pour s'authentifier sur le périphérique géré. Sélectionnez cette option pour configurer les paramètres du type de mot de passe.
Longueur minimum du mot de passe	Permet d'indiquer la longueur minimale du mot de passe. Elle est de 6 caractères par défaut.
Mot de passe de la session	Sélectionnez cette option pour inviter l'utilisateur du périphérique géré à définir un mot de passe avant le début d'une nouvelle session à distance. Cette option est recommandée. En effet, le mot de passe n'est pas stocké sur le périphérique géré et n'est valide que pour la session en cours.
Mot de passe persistant	Sélectionnez cette option pour définir les mots de passe ZENworks et VNC. La définition du mot de passe ZENworks est recommandée ; en effet, elle est plus sûre que la définition du mot de passe VNC. Ce mot de passe peut être défini par l'administrateur, par l'intermédiaire de la stratégie de gestion à distance ou par l'utilisateur du périphérique géré à l'aide de l'icône ZENworks. La sélection de cette option active les options qui en découlent. Pour permettre à l'utilisateur de définir le mot de passe via l'icône ZENworks, choisissez l'option *Autoriser l'utilisateur à remplacer les mots de passe par défaut sur le périphérique géré*.

Champ	Détails
Mot de passe ZENworks	Pour effacer le mot de passe ZENworks : 1. Cliquez sur *Effacer le mot de passe*. 2. Cliquez sur *Appliquer*, puis sur *OK*. Pour définir le mot de passe ZENworks : 1. Cliquez sur *Définir le mot de passe*. 2. Entrez le mot de passe. La longueur maximale des mots de passe est de 255 caractères. 3. Cliquez sur *Appliquer*, puis sur *OK*.
Mot de passe VNC	Pour effacer le mot de passe VNC : 1. Cliquez sur *Effacer le mot de passe*. 2. Cliquez sur *Appliquer*, puis sur *OK*. Pour Définir le mot de passe VNC : 1. Cliquez sur *Définir le mot de passe*. 2. Entrez le mot de passe. La longueur maximale des mots de passe est de 8 caractères. 3. Cliquez sur *Appliquer*, puis sur *OK*.

Détection d'intrus

Champ	Détails
Activer la détection d'intrusion	Sélectionnez cette option pour autoriser la détection des tentatives non valides ou non autorisées de lancer une session à distance sur le périphérique géré. La sélection de cette option active les options de la section Détection d'intrus qui en découlent.
Suspendre l'acceptation des connexions après [ ] tentatives successives non valides	Indiquez le nombre maximal de tentatives non valides consécutives que peut effectuer un opérateur avant que le service de gestion à distance sur le périphérique géré ne soit bloqué. Par défaut, il y a cinq tentatives.
Commencer à accepter automatiquement les connexions après [ ] minutes	Indiquez le délai en minutes à l'issue duquel l'agent de gestion à distance accepte automatiquement une connexion au périphérique géré. Pour débloquer manuellement le service de gestion à distance, double-cliquez sur l'icône ZENworks Adaptive Agent, cliquez sur *Paramètres de sécurité*, puis sur *Autoriser l'acceptation des connexions si blocage en cours pour détection d'intrusion.* La valeur par défaut est 10 minutes.

Sécurité de la session

Champ	Détails
Activer le codage de session	Active le codage SSL de la session (protocole TLSv1). La sélection de cette option active les options de la section Sécurité de la session qui en découlent.

Champ	Détails
Autoriser la connexion lorsque la console de gestion à distance n'a pas de certificat SSL	Lorsqu'une session à distance est lancée depuis le Centre de contrôle ZENworks, un certificat est généré automatiquement pour un opérateur à distance. Ce certificat est utilisé au cours de l'authentification. Sélectionnez cette option pour permettre les connexions à partir d'une console de gestion à distance lancée en dehors du Centre de contrôle ZENworks qui ne posséderait pas de certificat SSL.
Autoriser jusqu'à [ ] niveaux dans la chaîne de certificat de la visionneuse	Les schémas d'authentification de Novell basés sur les droits et basés sur les mots de passe sont exécutés sur un canal codé SSL. L'établissement de ce canal nécessite que la visionneuse présente un certificat. Ce certificat peut être signé par une autorité intermédiaire ou une autorité de certificat root, créant ainsi une chaîne de certificats. Cette propriété définit le nombre maximal de niveaux autorisés dans la chaîne de certificats de la visionneuse. Lorsque l'autorité de certification interne ZENworks est utilisée (installée par défaut), une chaîne de certificats de la visionneuse à deux niveaux est créée automatiquement lors du lancement d'une session à distance à partir du Centre de contrôle ZENworks.

Fin anormale

Champ	Détails
Verrouiller un périphérique	Verrouille le périphérique géré en cas de fin anormale de la session distance.
Déloguer l'utilisateur	Délogue l'utilisateur du périphérique géré en cas de fin anormale de la session distance.

11 Cliquez sur *Suivant* pour afficher la page Résumé.

12 Cliquez sur *Terminer* pour créer la stratégie maintenant ou sur *Définir des propriétés supplémentaires* pour spécifier des informations complémentaires telles que les assignations, les applications et l'état de la stratégie ou encore le groupe auquel la stratégie appartient.

2.4 Configuration des droits de gestion à distance

Vous pouvez assigner à un opérateur distant les droits lui permettant d'exécuter des sessions distantes sur le périphérique géré. L'opérateur distant peut avoir à la fois des droits spécifiques au périphérique et des droits spécifiques à l'utilisateur.

1 Dans le centre de contrôle ZENworks, cliquez sur *Configuration.*

2 Dans le volet Administrateurs, cliquez sur le nom de l'administrateur auquel vous souhaitez affecter les droits de gestion à distance.

3 Dans le volet Droits assignés, cliquez sur *Ajouter*, puis sur *Droits de gestion à distance* pour afficher la boîte de dialogue des droits de gestion à distance.

4 Sélectionnez le périphérique ou l'utilisateur auquel vous souhaitez affecter les droits.

Le tableau suivant fournit des informations sur les droits de gestion à distance :

Droits de gestion à distance	Détails
Contrôle à distance	Permet d'assigner à l'opérateur distant le droit de contrôler à distance le périphérique.
Affichage à distance	Permet d'assigner à l'opérateur distant le droit de visualiser à distance le périphérique.
Diagnostic à distance	Permet d'assigner à l'opérateur distant le droit d'effectuer un diagnostic à distance sur le périphérique.
Exécution à distance	Permet d'assigner à l'opérateur distant le droit d'exécuter des applications à distance sur le périphérique.
Transférer les fichiers	Assignez à l'opérateur distant les droits lui permettant de transférer des fichiers vers ou à partir des périphériques.
Débloquer le service de gestion à distance	Assignez à l'opérateur distant les droits lui permettant de débloquer le service de gestion à distance qui a été bloqué du fait de la détection d'un intrus.

Remarque : les droits de gestion à distance exigent une authentification basée sur les droits. Toutefois, l'opérateur distant peut s'authentifier par son mot de passe pour assurer la gestion à distance, si la stratégie de gestion à distance le permet.

5 Cliquez sur *OK*.

2.5 Configuration du mot de passe de gestion à distance

Les sections suivantes décrivent la procédure à suivre pour configurer le mot de passe de gestion à distance pour le service de gestion à distance sur le périphérique géré :

- Section 2.5.1, « Configuration du mot de passe de gestion à distance à l'aide du Centre de contrôle ZENworks », page 31
- Section 2.5.2, « Configuration du mot de passe de gestion à distance à l'aide de ZENworks Adaptive Agent », page 32
- Section 2.5.3, « Effacement du mot de passe de gestion à distance à l'aide du Centre de contrôle ZENworks », page 33
- Section 2.5.4, « Effacement du mot de passe de gestion à distance à l'aide de ZENworks Adaptive Agent », page 33

2.5.1 Configuration du mot de passe de gestion à distance à l'aide du Centre de contrôle ZENworks

L'administrateur peut définir un mot de passe de gestion à distance dans la page Paramètres de sécurité lors de la création d'une stratégie de gestion à distance ou après sa création.

Si vous souhaitez définir le mot de passe lors de la création de la stratégie de gestion à distance, reportez-vous à la Section 2.3, « Création de la stratégie de gestion à distance », page 23.

Pour modifier le mot de passe défini dans la stratégie de gestion à distance :

1. Dans le Centre de contrôle ZENworks, cliquez sur *Stratégies*.
2. Cliquez sur la stratégie de gestion à distance, puis sur l'onglet *Paramètres*.
3. Dans le panneau Paramètres de sécurité, sélectionnez le mot de passe et remplacez-le par un nouveau.
4. Cliquez sur *Appliquer*.
5. Augmentez la version de cette stratégie dans la page Résumé ou dans les Tâches communes pour mettre à jour les modifications apportées aux mots de passe sur le périphérique géré.

Si vous souhaitez définir le mot de passe après avoir créé la stratégie de gestion à distance :

1. Dans le Centre de contrôle ZENworks, cliquez sur *Stratégies*.
2. Cliquez sur la stratégie de gestion à distance, puis sur l'onglet *Paramètres*.
3. Dans le panneau Paramètres de sécurité, sélectionnez *Activer l'authentification par mot de passe*, puis sélectionnez *Persistante*.
4. Cliquez sur *Définir le mot de passe* et indiquez le mot de passe. Si vous avez déjà défini le mot de passe lors de la création de la stratégie de gestion à distance, vous pouvez le modifier. Pour modifier le mot de passe, sélectionnez-le et remplacez-le par un nouveau.
5. Cliquez sur *Appliquer*.
6. Augmentez la version de cette stratégie dans la page Résumé ou dans les Tâches communes pour mettre à jour les modifications apportées aux mots de passe sur le périphérique géré.

2.5.2 Configuration du mot de passe de gestion à distance à l'aide de ZENworks Adaptive Agent

L'utilisateur du périphérique géré peut définir un mot de passe pour le service de gestion à distance si l'option *Autoriser l'utilisateur à remplacer le mot de passe par défaut sur le périphérique géré* est activée dans la stratégie de gestion à distance active sur le périphérique géré. Ce mot de passe est prioritaire sur le mot de passe défini dans la stratégie de gestion à distance.

Pour définir un mot de passe sur le périphérique géré, procédez comme suit :

1. Double-cliquez sur l'icône *ZENworks Adaptive Agent* pour afficher la fenêtre correspondante.
2. Dans la sous-fenêtre de gauche, allez dans *Gestion à distance*, puis cliquez sur *Sécurité*.
3. Dans la sous-fenêtre de droite, cliquez sur *Définir le mot de passe* pour configurer les mots de passe suivants :
   - **Mot de passe ZENworks (recommandé) :** utilisé dans l'authentification ZENworks. Cet identificateur peut compter jusqu'à 255 caractères.
   - **Mot de passe VNC :** utilisé dans l'authentification VNC pour garantir l'interopérabilité avec les visualiseurs VNC open source. Cet identificateur peut compter jusqu'à 8 caractères.
4. Cliquez sur *OK*.

2.5.3 Effacement du mot de passe de gestion à distance à l'aide du Centre de contrôle ZENworks

Pour effacer le mot de passe de gestion à distance défini à l'aide de la stratégie, procédez comme suit :

1. Dans le Centre de contrôle ZENworks, cliquez sur *Stratégies*.
2. Cliquez sur la stratégie de gestion à distance, puis sur l'onglet *Paramètres*.
3. Dans le panneau Paramètres de sécurité, sélectionnez *Effacer le mot de passe*, puis cliquez sur *Appliquer*.
4. Incrémentez la version de cette stratégie dans la page Résumé ou dans les tâches communes pour appliquer les changements dans la stratégie du périphérique géré.

Pour effacer le mot de passe de gestion à distance défini par l'utilisateur du périphérique géré, procédez comme suit :

1. Dans le Centre de contrôle ZENworks, cliquez sur *Stratégies*.
2. Cliquez sur la stratégie de gestion à distance, puis sur l'onglet *Paramètres*.
3. Dans le panneau Paramètres de sécurité, décochez l'option *Autoriser l'utilisateur à remplacer les mots de passe par défaut sur le périphérique géré*, puis cliquez sur *Appliquer*.
4. Incrémentez la version de cette stratégie dans la page Résumé ou dans les tâches communes pour appliquer les changements dans la stratégie du périphérique géré.

2.5.4 Effacement du mot de passe de gestion à distance à l'aide de ZENworks Adaptive Agent

L'utilisateur du périphérique géré peut redéfinir le mot de passe de gestion à distance qu'il a lui-même défini.

1. Double-cliquez sur l'icône *ZENworks Adaptive Agent* pour afficher la fenêtre correspondante.
2. Dans la sous-fenêtre de gauche, allez dans *Gestion à distance*, puis cliquez sur *Sécurité*.
3. Dans la sous-fenêtre de droite, cliquez sur *Effacer le mot de passe* pour effacer les mots de passe.
4. Cliquez sur *OK*.

Le mot de passe configuré dans la stratégie sera effectif car aucun mot de passe n'a été défini par l'utilisateur.

2.6 Installation de la visionneuse de gestion à distance

La visionneuse de gestion à distance désigne une application de la console de gestion qui permet à un opérateur d'exécuter à distance des opérations sur le périphérique géré. La visionneuse permet à l'opérateur à distance de visualiser le bureau du périphérique géré, ainsi que de transférer des fichiers et d'exécuter des applications sur ce périphérique.

Pour l'installer, cliquez sur le lien *Installer la visionneuse de gestion à distance* qui apparaît dans le Centre de contrôle ZENworks lorsque vous exécutez une opération de gestion à distance sur le périphérique géré. Ce lien ne s'affiche que si vous exécutez une opération de gestion à distance sur le périphérique géré pour la première fois et si la visionneuse n'est pas encore installée sur le périphérique.

Si une version antérieure de la visionneuse de gestion à distance est déjà installée sur le périphérique, le lien *Mettre à niveau la visionneuse de gestion à distance* est affiché. Cliquez sur ce lien pour mettre à niveau la version de la visionneuse installée sur le périphérique.

Remarque : pour pouvoir installer la visionneuse de gestion à distance sous SLES (SUSE® Linux Enterprise Server) 11 ou SLED (SUSE Linux Enterprise Desktop) 11, vous devez disposer d'un paquetage glitz associé. Ce dernier doit être installé à partir du site Web openSUSE® (http://software.opensuse.org/112/en).

Sous Windows :

1. Dans le Centre de contrôle ZENworks, cliquez sur *Configuration*.
2. Dans le volet de navigation de gauche, cliquez sur *Télécharger les outils ZENworks*.
3. Dans le volet de navigation de gauche sur la page de téléchargement ZENworks, cliquez sur *Outils administratifs*.
4. Cliquez sur le fichier `novell-zenworks-rm-viewer-<version>.msi`.
5. (Conditionnel) Si vous avez lancé le Centre de contrôle ZENworks à l'aide d'Internet Explorer*, procédez de l'une des manières suivantes :
   - Cliquez sur *Exécuter* pour installer la visionneuse.
   - Cliquez sur *Enregistrer* pour sauvegarder le fichier à un emplacement temporaire. Double-cliquez sur le fichier pour installer la visionneuse.
6. (Facultatif) Si vous avez lancé le Centre de contrôle ZENworks à l'aide de Firefox, cliquez sur *Enregistrer le fichier* pour enregistrer le fichier à un emplacement temporaire, puis double-cliquez sur le fichier pour installer la visionneuse.

Sous Linux :

1. Dans le Centre de contrôle ZENworks, cliquez sur *Configuration*.
2. Dans le volet de navigation de gauche, cliquez sur *Télécharger les outils ZENworks*.
3. Dans le volet de navigation de gauche sur la page de téléchargement ZENworks, cliquez sur *Outils administratifs*.
4. Cliquez sur le fichier `novell-zenworks-rm-viewer-<version>.noarch.rpm`.
5. Choisissez si vous souhaitez installer immédiatement la visionneuse ou si vous préférez enregistrer son fichier RPM pour une installation ultérieure.
   - Pour l'installer directement, cliquez sur *Ouvrir avec* afin d'ouvrir la visionneuse de gestion à distance avec zen-installer, spécifiez le mot de passe de l'utilisateur root, puis cliquez sur *OK*.
   - Pour enregistrer le fichier RPM de la visionneuse dans le répertoire de téléchargement par défaut afin de pouvoir l'installer plus tard, cliquez sur *Enregistrer sur le disque*. Pour installer le RPM, effectuez l'une des opérations suivantes:
     - Cliquez sur le fichier RPM de la visionneuse, spécifiez le mot de passe de l'utilisateur root, puis cliquez sur *OK*.

- Exécutez la commande suivante en tant que superutilisateur ou utilisateur root :

  ```
  rpm -ivh novell-zenworks-rm-viewer-<version>.noarch.rpm
  ```

2.7 Mise à niveau de la visionneuse de gestion à distance

Si vous effectuez une opération de gestion à distance sur un périphérique géré Windows sur lequel une version antérieure de la visionneuse de gestion à distance est déjà installée, le lien *Mettre à niveau la visionneuse de gestion à distance* s'affiche dans le Centre de contrôle ZENworks. Cliquez sur ce lien pour mettre à niveau la version de la visionneuse installée sur le périphérique.

Pour mettre à niveau la visionneuse de gestion à distance sur un périphérique Linux de Novell ZENworks 10 Configuration Management avec SP2 (10.2) vers Novell ZENworks 10 Configuration Management avec SP3 (10.3) ou version ultérieure, exécutez la commande suivante en tant que superutilisateur ou qu'utilisateur root :

```
rpm -Uvh --nopostun novell-zenworks-rm-viewer-<version>.noarch.rpm
```

Sinon, désinstallez l'ancienne version de `novell-zenworks-rm-viewer-10.x.x.rpm`, puis installez la nouvelle. Pour plus d'informations sur l'installation de la visionneuse, reportez-vous à la Section 2.6, « Installation de la visionneuse de gestion à distance », page 33.

2.8 Démarrage des opérations de gestion à distance

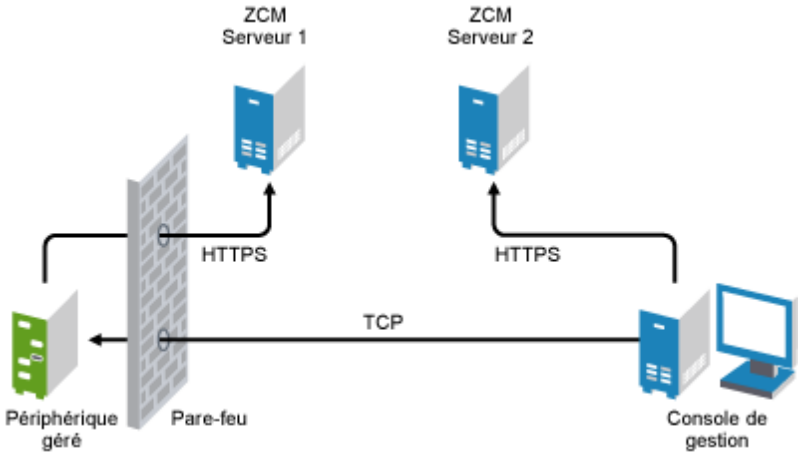
L'opération à distance peut être lancée de plusieurs manières :

- Section 2.8.1, « Lancement d'une session à partir de la console de gestion », page 35
- Section 2.8.2, « Lancement d'une session à partir du périphérique géré », page 44

2.8.1 Lancement d'une session à partir de la console de gestion

Dans ce scénario, la session distante est lancée par l'administrateur sur la console de gestion. La console de gestion est généralement placée dans un réseau d'entreprise et le périphérique géré peut se trouver à l'intérieur ou à l'extérieur du réseau d'entreprise. L'illustration suivante montre une session distante lancée sur le périphérique géré à partir de la console de gestion.

Figure 2-1 *Session lancée à partir de la console de gestion*



L'agent de gestion à distance démarre automatiquement lorsque le périphérique géré démarre. Une stratégie de gestion à distance par défaut est créée sur le périphérique géré lors de son déploiement. Vous pouvez gérer le périphérique à distance en utilisant cette stratégie par défaut en mode d'authentification basée sur les droits seulement. Lorsque vous créez une nouvelle stratégie de gestion à distance, elle remplace la stratégie par défaut.

Si le paramétrage de la zone de gestion ZENworks est étendu sur plusieurs réseaux privés NAT interconnectés par le biais d'un réseau public, vous devez déployer DNS_ALG sur les passerelles de ces réseaux privés. DNS_ALG veille à ce que les requêtes de recherche DNS initiées par les composants ZENworks renvoient le nom de l'hôte assigné à la bonne adresse privée et permet la communication entre la console de gestion et les périphériques gérés. Pour plus d'informations sur DNS_ALG, reportez-vous au document DNS ALG RFC - 2694 (http://www.ietf.org/rfc/rfc2694) (en anglais).

Si vous souhaitez gérer à distance un périphérique en utilisant son nom DNS, assurez-vous que le service DNS dynamique est déployé sur le réseau.

L'opérateur distant peut démarrer une session de plusieurs manières :

- « Démarrage d'une opération de gestion à distance dans le centre de contrôle ZENworks » page 36
- « Démarrage d'une opération de gestion à distance en mode autonome » page 43
- « Démarrage d'une opération de gestion à distance à l'aide des options de ligne de commande » page 43

Démarrage d'une opération de gestion à distance dans le centre de contrôle ZENworks

Vous pouvez exécuter les différentes opérations de gestion à distance à partir du contexte de périphérique ou du contexte d'utilisateur.

- « Lancement d'une session de gestion à distance depuis le contexte de périphérique » page 37
- « Lancement d'une session de gestion à distance à partir du contexte utilisateur » page 40

Lancement d'une session de gestion à distance depuis le contexte de périphérique

Pour lancer une session de gestion à distance sur un périphérique, procédez comme suit :

1. Dans le Centre de contrôle ZENworks, cliquez sur l'onglet *Périphériques*.
2. Cliquez sur *Serveurs* ou *Postes de travail*, puis sélectionnez le périphérique que vous voulez gérer à distance. Cliquez sur *Action*, puis sélectionnez l'opération de gestion à distance que vous voulez effectuer.

   ou

   Dans la sous-fenêtre *Tâches du périphérique* du volet de gauche, sélectionnez l'opération de gestion à distance que vous voulez exécuter.

   Vous pouvez choisir l'une des opérations à distance suivantes :

   - **Contrôle à distance :** affiche la boîte de dialogue Gestion à distance, qui permet d'effectuer une opération de contrôle à distance, d'affichage à distance ou d'exécution à distance sur le périphérique géré.
   - **Diagnostics à distance :** affiche la boîte de dialogue Diagnostics à distance, qui permet d'effectuer une opération de diagnostic à distance sur le périphérique géré.
   - **Transférer les fichiers :** affiche la boîte de dialogue Transfert de fichiers, qui permet d'effectuer une opération de transfert de fichiers sur le périphérique géré.
3. Renseignez les options de la boîte de dialogue qui s'affiche. Le tableau suivant contient des informations sur les différentes options disponibles :

Champ	Détails
Périphérique	Indiquez le nom d'hôte ou l'adresse IP du périphérique que vous souhaitez gérer à distance.
Opération	Sélectionnez le type d'opération à distance que vous souhaitez effectuer sur le périphérique géré : Cette option est uniquement disponible dans la boîte de dialogue Gestion à distance.
Application	Sélectionnez l'application que vous voulez lancer sur le périphérique à diagnostiquer à distance. Cette option est uniquement disponible dans la boîte de dialogue Diagnostics à distance.
Authentification	Sélectionnez le mode que vous voulez utiliser pour authentifier le périphérique géré. Les modes d'authentification sont les suivants : ◆ Authentification par droits ◆ Authentification par mot de passe
Port	Indiquez le numéro de port sur lequel le service de gestion à distance écoute. Par défaut, le numéro de port est le 5950.
Mode de la session	Sélectionnez l'un des modes suivants pour la session : ◆ **Collaborer :** permet de lancer une session de contrôle à distance et une session d'affichage à distance en mode collaboration. Ce mode est sélectionné par défaut pour l'opération de contrôle à distance. Si vous lancez d'abord la session de contrôle à distance sur le périphérique géré, vous obtenez les privilèges d'un opérateur distant maître : ◆ Invitation d'autres opérateurs distants à rejoindre la session distante. ◆ Délégation des droits de contrôle à distance à un opérateur distant. ◆ Reprise du contrôle sur l'opérateur distant. ◆ Fin d'une session à distance. Les sessions consécutives lancées sont des sessions de visualisation à distance. **Remarque :** le mode collaboration n'est pas encore pris en charge sous Linux. ◆ **Partagée :** permet à plusieurs opérateurs distants de contrôler simultanément le périphérique géré. ◆ **Exclusif :** permet d'avoir une session à distance exclusive sur le périphérique géré. Aucune autre session à distance ne peut être démarrée sur le périphérique géré lorsqu'une session a été lancée en mode exclusif. Ce mode est sélectionné par défaut pour l'opération d'affichage à distance. Cette option est uniquement disponible dans la boîte de dialogue Gestion à distance.
Codage de session	Vérifiez que la session distante est sécurisée avec le codage SSL (protocole TLSv1).
Activer le caching	Active le caching des données de session de gestion distantes pour améliorer les performances. Cette option est disponible pour les opérations de contrôle à distance, d'affichage à distance et de diagnostics à distance. Cette option n'est actuellement prise en charge que sous Windows.

Champ	Détails
Activer l'optimisation dynamique de la bande passante	Active la détection de la bande passante disponible du réseau et ajuste en conséquence les paramètres de la session afin d'améliorer les performances. Cette option est disponible pour les opérations de contrôle à distance, d'affichage à distance et de diagnostics à distance.
Activation de la consignation	Consigne des informations de session et de débogage dans le fichier `novell-zenworks-vncviewer.txt`. Le fichier est enregistré par défaut sur le bureau si vous lancez le centre de contrôle ZENworks à partir d'Internet Explorer et dans le répertoire installé par Mozilla si vous le lancez à partir de Mozilla* Firefox*.
Router via le proxy	Permet à l'opération de gestion à distance du périphérique géré d'être routée via un proxy de gestion à distance. Si le périphérique géré se trouve sur un réseau privé ou de l'autre côté d'un pare-feu ou routeur qui utilise la traduction d'adresses réseau (NAT), L'opération de gestion à distance du périphérique peut être routée via un proxy de gestion à distance. Cette option n'est actuellement prise en charge que sous Windows. Renseignez les champs suivants : **Proxy :** Indiquez le nom DNS ou l'adresse IP du proxy de gestion à distance. Par défaut, le proxy configuré dans le panneau Paramètres de proxy pour exécuter l'opération à distance sur le périphérique est renseigné dans ce champ. Vous pouvez spécifier un autre proxy. **Port Proxy :** Indiquez le numéro de port sur lequel le proxy de gestion à distance écoute. Le port par défaut est 5750. **Remarque :** l'audit de la gestion à distance affiche l'adresse IP du périphérique qui exécute le proxy de gestion à distance, et non celle de la console de gestion.
Utiliser la paire de clés suivante pour l'identification	Si une autorité de certification interne est déployée, les options suivantes ne s'affichent pas. Si une autorité de certification externe est déployée, renseignez les champs suivants : **Clé privée :** cliquez sur *Parcourir* pour rechercher et sélectionner la clé privée de l'opérateur à distance. **Certificat :** cliquez sur *Parcourir* pour rechercher et sélectionner le certificat correspondant à la clé privée. Ce certificat doit être chaîné à l'autorité de certification configurée pour la zone. Les formats pris en charge pour la clé et le certificat sont les suivants : DER, PEM et PFX. Si le format PFX est utilisé, la clé et le certificat doivent se trouver dans le même fichier. Ce fichier doit être fourni comme entrée pour la clé et le certificat. **Activer le chemin du cache :** permet de mettre en cache les chemins de la clé primaire et du certificat sur la console de gestion. Cette option n'est actuellement prise en charge que sous Windows.

4 Cliquez sur *OK* pour lancer l'opération à distance sélectionnée.

Lancement d'une session de gestion à distance à partir du contexte utilisateur

Si vous voulez aider un utilisateur en exécutant une session à distance sur le périphérique géré sur lequel il s'est connecté, procédez comme suit :

1. Dans le centre de contrôle ZENworks, cliquez sur l'onglet *Utilisateurs*.
2. Cliquez sur *Source d'utilisateurs*.
3. Sélectionnez l'utilisateur pour gérer à distance le périphérique sur lequel il s'est connecté.
4. Cliquez sur *Action*, puis sélectionnez l'opération de gestion à distance que vous voulez exécuter.

   Les opérations disponibles sont les suivantes :

   - **Contrôle à distance :** affiche la boîte de dialogue Gestion à distance, qui permet d'effectuer une opération de contrôle à distance, d'affichage à distance ou d'exécution à distance sur le périphérique géré.
   - **Diagnostics à distance :** affiche la boîte de dialogue Diagnostics à distance, qui permet d'effectuer une opération de diagnostic à distance sur le périphérique géré.
   - **Transférer les fichiers :** affiche la boîte de dialogue Transfert de fichiers, qui permet d'effectuer une opération de transfert de fichiers sur le périphérique géré.
5. Renseignez les options de la boîte de dialogue qui s'affiche. Le tableau suivant contient des informations sur les différentes options disponibles :

Champ	Détails
Périphérique	Indiquez le nom d'hôte ou l'adresse IP du périphérique que vous souhaitez gérer à distance.
Opération	Sélectionnez le type d'opération à distance que vous souhaitez effectuer sur le périphérique géré : Cette option est uniquement disponible dans la boîte de dialogue Gestion à distance.
Application	Sélectionnez l'application que vous voulez lancer sur le périphérique à diagnostiquer à distance. Cette option est uniquement disponible dans la boîte de dialogue Diagnostics à distance.
Authentification	Sélectionnez le mode que vous voulez utiliser pour authentifier le périphérique géré. Les modes d'authentification sont les suivants : ◆ Authentification par droits ◆ Authentification par mot de passe
Port	Indiquez le numéro de port sur lequel le service de gestion à distance écoute. Par défaut, le numéro de port est le 5950.
Mode de la session	Sélectionnez l'un des modes suivants pour la session : ◆ **Collaborer :** permet de lancer une session de contrôle à distance et une session d'affichage à distance en mode collaboration. Ce mode est sélectionné par défaut pour l'opération de contrôle à distance. Si vous lancez d'abord la session de contrôle à distance sur le périphérique géré, vous obtenez les privilèges d'un opérateur distant maître : ◆ Invitation d'autres opérateurs distants à rejoindre la session distante. ◆ Délégation des droits de contrôle à distance à un opérateur distant. ◆ Reprise du contrôle sur l'opérateur distant. ◆ Fin d'une session à distance. Les sessions consécutives lancées sont des sessions de visualisation à distance. **Remarque :** le mode collaboration n'est pas encore pris en charge sous Linux. ◆ **Partagée :** permet à plusieurs opérateurs distants de contrôler simultanément le périphérique géré. ◆ **Exclusif :** permet d'avoir une session à distance exclusive sur le périphérique géré. Aucune autre session à distance ne peut être démarrée sur le périphérique géré lorsqu'une session a été lancée en mode exclusif. Ce mode est sélectionné par défaut pour l'opération d'affichage à distance. Cette option est uniquement disponible dans la boîte de dialogue Gestion à distance.
Codage de session	Vérifiez que la session distante est sécurisée avec le codage SSL (protocole TLSv1).
Activer le caching	Active le caching des données de session de gestion distantes pour améliorer les performances. Cette option est disponible pour les opérations de contrôle à distance, d'affichage à distance et de diagnostics à distance. Cette option n'est actuellement prise en charge que sous Windows.

Champ	Détails
Activer l'optimisation dynamique de la bande passante	Active la détection de la bande passante disponible du réseau et ajuste en conséquence les paramètres de la session afin d'améliorer les performances. Cette option est disponible pour les opérations de contrôle à distance, d'affichage à distance et de diagnostics à distance.
Activation de la consignation	Consigne des informations de session et de débogage dans le fichier `novell-zenworks-vncviewer.txt`. Le fichier est enregistré par défaut sur le bureau si vous lancez le centre de contrôle ZENworks à partir d'Internet Explorer et dans le répertoire installé par Mozilla si vous le lancez à partir de Mozilla* Firefox*.
Router via le proxy	Permet à l'opération de gestion à distance du périphérique géré d'être routée via un proxy de gestion à distance. Si le périphérique géré se trouve sur un réseau privé ou de l'autre côté d'un pare-feu ou routeur qui utilise la traduction d'adresses réseau (NAT), L'opération de gestion à distance du périphérique peut être routée via un proxy de gestion à distance. Cette option n'est actuellement prise en charge que sous Windows. Renseignez les champs suivants : **Proxy :** indiquez le nom DNS ou l'adresse IP du proxy de gestion à distance. Par défaut, le proxy configuré dans le panneau Paramètres de proxy pour exécuter l'opération à distance sur le périphérique est renseigné dans ce champ. Vous pouvez spécifier un autre proxy. **Port Proxy :** indiquez le numéro de port sur lequel le proxy de gestion à distance écoute. Le port par défaut est 5750. **Remarque :** l'audit de la gestion à distance affiche l'adresse IP du périphérique qui exécute le proxy de gestion à distance, et non celle de la console de gestion.
Utiliser la paire de clés suivante pour l'identification	Si une autorité de certification interne est déployée, les options suivantes ne s'affichent pas. Si une autorité de certification externe est déployée, renseignez les champs suivants : **Clé privée :** cliquez sur *Parcourir* pour rechercher et sélectionner la clé privée de l'opérateur à distance. **Certificat :** cliquez sur *Parcourir* pour rechercher et sélectionner le certificat correspondant à la clé privée. Ce certificat doit être chaîné à l'autorité de certification configurée pour la zone. Les formats pris en charge pour la clé et le certificat sont les suivants : DER, PEM et PFX. Si le format PFX est utilisé, la clé et le certificat doivent se trouver dans le même fichier. Ce fichier doit être fourni comme entrée pour la clé et le certificat. **Activer le chemin du cache :** permet de mettre en cache les chemins de la clé primaire et du certificat sur la console de gestion. Cette option n'est actuellement prise en charge que sous Windows.

6 Cliquez sur *OK* pour lancer l'opération à distance sélectionnée.

Démarrage d'une opération de gestion à distance en mode autonome

Avant de démarrer l'opération de gestion à distance en mode autonome, installez la visionneuse de gestion à distance. Pour plus d'informations sur l'installation de la visionneuse, reportez-vous à la Section 2.6, « Installation de la visionneuse de gestion à distance », page 33.

Pour démarrer une opération de gestion à distance en mode autonome :

1. Double-cliquez sur le fichier `nzrViewer.exe` pour lancer le client Gestion à distance de ZENworks.
2. Dans la fenêtre Connexion ZENworks Remote Management qui s'affiche, indiquez le nom DNS ou l'adresse IP du périphérique géré, ainsi que le numéro de port en utilisant le format *Adresse IP~~Port*. Exemple : 10.0.0.0~~1000.
3. Spécifiez le nom DNS ou l'adresse IPdu proxy de gestion à distance, ainsi que son numéro de port dans l'un des formats suivants :
   - *adresse IP~~Port*. Par exemple : 10.0.0.0~~5750.
   - *adresse IP~Port*. Par exemple : 10.0.0.0~50.
4. Cliquez sur *Connecter*.

   Lorsque l'authentification est acceptée, la session distante démarre. Par défaut, une session de contrôle à distance démarre.

Démarrage d'une opération de gestion à distance à l'aide des options de ligne de commande

Installez la visionneuse de gestion à distance avant de lancer une opération de gestion à distance depuis la ligne de commande. Pour plus d'informations sur l'installation de la visionneuse, reportez-vous à la Section 2.6, « Installation de la visionneuse de gestion à distance », page 33.

Pour démarrer l'opération de gestion à distance en utilisant les options de ligne de commande :

1. À l'invite de commande, accédez au répertoire dans lequel la visionneuse est installée. La visionneuse est installée par défaut dans le répertoire `<dossier_données_application_utilisateur>\Novell\ZENworks\Remote Management\bin`.
2. Exécutez la commande suivante :

   `nzrViewer [/options<paramètres le cas échéant>][adresse IP du périphérique géré] [~~port]`

   Le port par défaut du périphérique géré est 5950.

   Pour plus d'informations sur les options de ligne de commande disponibles, reportez-vous à la Section 2.9.1, « Options de ligne de commande pour le lancement d'une opération à distance », page 46.
3. Cliquez sur *Connecter*.

   Lorsque l'authentification est acceptée, la session distante démarre. Si vous n'avez pas indiqué le type d'opération à distance dans la ligne de commande, la session lancée par défaut est une session de contrôle à distance.

Le démarrage d'une opération de gestion à distance à l'aide des options de ligne de commande présente toutefois les limites suivantes :

- Si vous ne souhaitez pas spécifier les options de ligne de commande `key`, `cert` et `CAcert` dans la commande `nzrViewer` pour l'authentification SSL, assurez-vous que l'option *Autoriser la connexion lorsque la console de gestion à distance n'a pas de certificat SSL* est activée dans les paramètres de sécurité de la stratégie de gestion à distance. Toutefois, cette opération n'est pas recommandée car elle réduit le niveau de sécurité du périphérique.
- Si le périphérique géré appartient à la zone de gestion, vérifiez que le certificat soumis par la visionneuse est valide, signé et chaîné à l'autorité de certification, faute de quoi l'authentification SSL échoue.

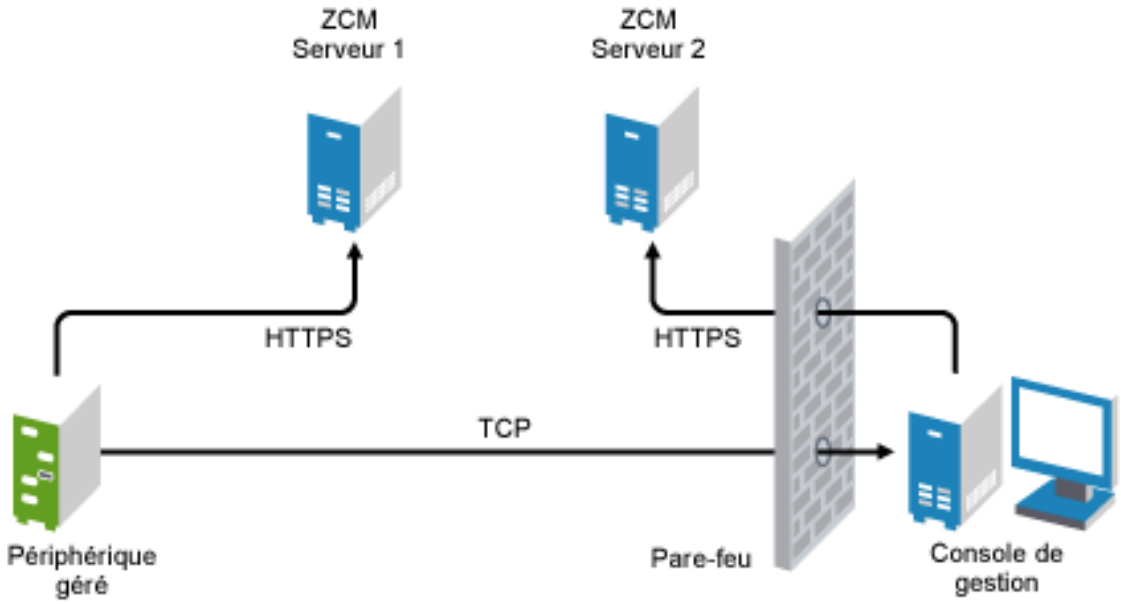
  Remarque : lorsque vous lancez une session à distance à partir du Centre de contrôle ZENworks (ZCC), ce dernier génère automatiquement le certificat et le transmet à la visionneuse afin de démarrer la session. Ce certificat n'est valable que pendant quatre jours.

- Le périphérique géré utilise le certificat fourni par la visionneuse pour identifier l'opérateur à distance. Si la visionneuse ne fournit aucun certificat, l'utilisateur n'est pas identifié et est enregistré comme *inconnu* dans le message d'autorisation, le signal visible et les journaux d'audit.

2.8.2 Lancement d'une session à partir du périphérique géré

Dans ce scénario, la session distante est lancée par l'utilisateur sur le périphérique géré. Ceci est utile si la console de gestion ne peut pas se connecter au périphérique géré. L'illustration suivante montre une session distante lancée par l'utilisateur sur le périphérique géré.

Figure 2-2 *Session lancée par l'agent*



L'utilisateur du périphérique géré peut demander qu'un opérateur distant effectue une session distante sur le périphérique si :

- L'opérateur distant a lancé le module d'écoute de gestion à distance pour écouter les requêtes de session distante de l'utilisateur.
- L'option *Autoriser l'utilisateur à demander une session distante* est activée dans la stratégie de gestion distante.
- Le port sur lequel le module d'écoute de gestion à distance écoute les connexions distantes doit être ouvert dans le pare-feu de la console de gestion. Le numéro de port par défaut est 5550.

Pour demander une session :

1. Double-cliquez sur l'icône ZENworks dans la zone de notification.
2. Dans le volet gauche, recherchez *Gestion à distance*, puis cliquez sur *Général*.
3. Cliquez sur *Demander une session de gestion à distance* pour afficher la boîte de dialogue Demander une session.

   La possibilité de demander une session de gestion à distance est contrôlée par votre administrateur, ce qui signifie que cette option peut être désactivée, en particulier si votre entreprise ou votre service ne dispose pas de personnel de service d'assistance pour servir d'opérateurs à distance. Si l'option *Demander une session de gestion à distance* ne s'affiche pas sous forme de lien, elle est désactivée.
4. Dans la liste *Opérateurs à distance à l'écoute*, sélectionnez l'opérateur distant avec lequel vous voulez ouvrir la session à distance.

   ou

   Si l'opérateur distant n'est pas répertorié, renseignez les informations de connexion de l'opérateur dans les champs *Demander la connexion*.
5. Dans le champ *Opération*, sélectionnez le type d'opération (contrôle à distance, affichage à distance, diagnostic à distance, transfert de fichier ou exécution à distance) que vous voulez ouvrir.

   Pour obtenir des informations concernant chaque opération, reportez-vous à la Section 1.2, « Présentation des opérations de gestion à distance », page 12.
6. Cliquez sur *Demander* pour lancer la session.

Si vous voulez autoriser les connexions entre un réseau public et un réseau privé, vous devez déployer la passerelle DNS_ALG (DNS Application Level Gateway). Pour plus d'informations sur DNS_ALG, reportez-vous à RFC 2694 (http://www.ietf.org/rfc/rfc2694).

2.9 Options de lancement d'une opération de gestion à distance

Lorsque vous lancez une opération de gestion à distance depuis la ligne de commande, vous pouvez spécifier des options qui permettent de contrôler le comportement de la session à distance. Par exemple, l'option `remotecontrol` permet de lancer une opération de gestion à distance sur le périphérique et l'option `notoolbar` masque la barre d'outils de la fenêtre d'affichage.

La gestion à distance fait appel à certaines options en interne lorsque vous lancez une opération de gestion à distance sur un périphérique. Par exemple, l'option `zenrights` permet de spécifier l'authentification des droits ZENworks comme schéma d'authentification. Ces options en interne ne

doivent pas être spécifiées lorsque vous utilisez la ligne de commande pour lancer une opération de gestion à distance sur un périphérique. Pour plus d'informations sur les options utilisées en interne, reportez-vous à la Section 2.9.2, « Options internes de lancement d'une opération à distance », page 49.

Reportez-vous aux sections suivantes pour plus d'informations sur les options de gestion à distance :

- Section 2.9.1, « Options de ligne de commande pour le lancement d'une opération à distance », page 46
- Section 2.9.2, « Options internes de lancement d'une opération à distance », page 49

2.9.1 Options de ligne de commande pour le lancement d'une opération à distance

Pour contrôler une opération à distance, utilisez les options de ligne de commande suivantes :

Tableau 2-1 *Options de ligne de commande pour le lancement d'une opération à distance*

Option de ligne de commande	Paramètre	Description
listen	*port*	Permet au module d'écoute d'écouter les requêtes de session distante sur le port spécifié. Le port par défaut est 5550.
restricted		Masque la barre d'outils et le menu système.
viewonly		Lance une opération d'affichage à distance sur le périphérique géré.
remotecontrol		Lance une opération de contrôle à distance sur le périphérique géré.
ftponly		Lance une opération de transfert de fichiers sur le périphérique géré.
remoteexecute		Lance une opération d'exécution à distance sur le périphérique géré.
diagnostics	*appname*	Lance une opération de diagnostics à distance sur le périphérique géré. Si le paramètre appname est spécifié, l'application correspondante est lancée sur le périphérique géré.
filecompressionlevel	*level*	Offre des méthodes permettant d'optimiser le processus de compression de fichier pour améliorer la vitesse ou la compression lors d'une opération de transfert de fichiers. Le niveau de compression est compris entre 0 et 9 : ◆ 0 correspond à l'absence de compression ◆ 1 indique la vitesse la plus élevée ◆ 9 correspond à la compression la plus élevée Si le niveau de compression n'est pas indiqué, la valeur par défaut utilisée est 6 (optimisée à la fois pour la vitesse et la compression).
noencrypt		Lance la session distante en mode non codé.

Option de ligne de commande	Paramètre	Description
fullscreen		Lance une opération distante en mode plein écran sur le périphérique géré.
notoolbar		Masque la barre d'outils de la fenêtre de visualisation.
exclusive		Lance la session distante en mode exclusif.
8bit		Spécifie la profondeur de couleur à utiliser pour afficher les données de la session.
shared		Active une connexion partagée qui vous permet de partager le bureau avec les clients qui l'utilisent déjà. Cette option est vraie par défaut.
collaborate		Lance la session distante en mode collaboratif. Cette option n'est pas encore prise en charge sous Linux.
noshared		Active une connexion non partagée qui déconnecte les autres clients connectés ou refuse votre connexion, selon la configuration du serveur.
swapmouse		Inverse les boutons de la souris.
nocursor		N'affiche que le pointeur de la souris du périphérique géré. Le pointeur de la souris locale n'est pas affiché.
dotcursor		Affiche le pointeur de la souris locale sous la forme d'un point. Cette option est vraie par défaut.
smalldotcursor		Affiche le pointeur de la souris locale sous la forme d'un petit point.
normalcursor		Affiche le pointeur de la souris locale sous la forme par défaut.
belldeiconify		Permet la transmission d'un caractère d'appel et génère un signal sonore sur la visionneuse. Cette option provoque également l'agrandissement de la fenêtre d'une visionneuse VNC précédemment réduite à la taille d'une icône lorsque le caractère d'appel est reçu.
emulate3		Les utilisateurs possédant une souris à deux boutons peuvent émuler un troisième bouton en appuyant simultanément sur les deux boutons. Cette option est vraie par défaut.
noemulate3		N'émule pas une souris à trois boutons.
nojpeg		Désactive la compression JPEG avec perte. Ceci n'est pas recommandé car l'efficacité du codeur peut s'en trouver réduite. Vous pouvez utiliser cette option s'il est absolument nécessaire d'obtenir une image d'une qualité parfaite.
nocursorshape		Désactive les mises à jour de forme du curseur pour gérer les mouvements du curseur distant. L'utilisation des mises à jour de forme du curseur réduit le retard des mouvements du curseur distant et peut améliorer de façon très importante l'utilisation de la bande passante.
noremotecursor		N'affiche pas le curseur distant.
fitwindow		Masque la barre de défilement de la fenêtre de visualisation.

Option de ligne de commande	Paramètre	Description
scale	*percentage*	Agrandit la fenêtre d'affichage au pourcentage spécifié.
emulate3timeout	*ms*	Spécifie le timeout pour émuler une souris à trois boutons.
disableclipboard		Désactive la copie des données dans le presse-papiers.
delay		Présente une zone d'affichage et attend le délai spécifié avant de récupérer la mise à jour suivante.
loglevel	*n*	Spécifie les niveaux de consignation des informations.
Web		Consigne les informations dans une fenêtre de la console.
logfile	*Nom du fichier*	Nom du fichier journal dans lequel les informations doivent être consignées.
config	*Nom du fichier*	Nom de la configuration à utiliser pour le chargement des paramètres de configuration prédéfinis.
clé	*Nom du fichier*	Nom du fichier dans lequel la clé privée est stockée. Cette clé est utilisée au cours d'un contrôle de flux SSL avec le périphérique géré. **Important :** la clé et les options cert doivent être utilisées ensemble. Si vous utilisez ces options avec la commande `nzrViewer`, pour des raisons de sécurité, vous devez désactiver l'option *Autoriser la connexion lorsque la console de gestion à distance n'a pas de certificat* dans les paramètres de sécurité de la stratégie de gestion à distance.
cert	*Nom du fichier*	Nom du fichier dans lequel le certificat correspondant à la clé privée est stocké. **Important :** la clé et les options cert doivent être utilisées ensemble. Si vous utilisez ces options avec la commande `nzrViewer`, pour des raisons de sécurité vous devez désactiver l'option *Autoriser la connexion lorsque la console de gestion à distance n'a pas de certificat* dans les paramètres de sécurité de la stratégie de gestion à distance.
CAcert	*Nom du fichier*	Nom du fichier dans lequel le certificat racine est stocké. Ce certificat est utilisé pour vérifier le certificat du périphérique géré au cours d'un contrôle de flux SSL.
encoding	*encname*	Spécifie le codage désiré à utiliser pour la session. Les types différents de codage sont Raw, CopyRect, RRE, CoRRE, Hextile, Zlib et Tight.
compresslevel	*n*	Spécifie le niveau de compression afin de compresser les données de la session à distance de 0 à 9. Le niveau 1 utilise un minimum de temps d'UC avec de faibles rapports de compression, et le niveau 9 offre une meilleure compression mais est plus lent en termes de consommation de temps d'UC du côté du serveur. Utilisez des niveaux élevés avec les connexions réseau très lentes et des niveaux faibles lorsque vous travaillez avec des LAN à haute vitesse. Nous recommandons de ne pas utiliser le niveau de compression 0.

Option de ligne de commande	Paramètre	Description
quality	*n*	Spécifie le niveau de qualité JPEG entre 0 et 9. Le niveau de qualité 0 indique une qualité d'image médiocre mais des rapports de compression impressionnants, et le niveau 9 offre une très bonne qualité d'image à des rapports de compression plus faibles.
zenpasswd		Indique que le schéma d'authentification à utiliser est l'authentification ZENworks basée sur les mots de passe.
locale		Spécifie les paramètres régionaux à utiliser pour l'affichage des ressources. L'anglais est la langue utilisée par défaut. Les valeurs de cette option sont : Anglais, Français, Allemand, Espagnol, Portugais, Japonais, Italien, Chinois (simplifié) et Chinois (traditionnel).
proxy	serveur_proxy	Spécifie le nom DNS ou l'adresse IP du proxy de gestion à distance, ainsi que le numéro de port dans l'un des formats suivants : ◆ *adresse IP~~Port*. Par exemple : 10.0.0.0~~5750. ◆ *adresse IP~Port*. Par exemple : 10.0.0.0~50. Le port par défaut du proxy est 5750.

2.9.2 Options internes de lancement d'une opération à distance

Le tableau ci-dessous répertorie les options utilisées en interne par la gestion à distance. Ces options ne doivent pas être utilisées pour le lancement d'une opération de gestion à distance depuis la ligne de commande.

Tableau 2-2 *Options internes de lancement d'une opération à distance*

Option	Description
zenrights	Spécifie les droits d'authentification ZENworks comme schéma d'authentification.
pipe	Donne des informations sur l'authentification.

2.10 Installation d'un proxy de gestion à distance

Si un périphérique géré se trouve sur un réseau privé ou de l'autre côté d'un pare-feu ou routeur qui utilise la traduction d'adresses réseau (NAT), l'opération de gestion à distance du périphérique peut être routée via un proxy de gestion à distance. Le proxy peut être installé sur un périphérique géré Windows ou sur un périphérique Linux (serveur primaire ou satellite). Par défaut, le proxy de gestion à distance reçoit les données sur le port 5750.

Pour plus d'informations sur le proxy de gestion à distance, reportez-vous à la Section 1.4, « Présentation du proxy de gestion à distance », page 16.

Pour plus d'informations sur la configuration système requise pour un périphérique géré Windows ou un périphérique Linux afin de pouvoir y installer le proxy, reportez-vous à la section « Configuration système requise » du *Guide d'installation de ZENworks 10 Configuration Management*.

Pour installer le proxy, procédez comme suit :

Sous Windows :

1. Sur le périphérique, ouvrez la page de téléchargement ZENworks dans un navigateur Web :

   https://*server*/zenworks-setup

   où *serveur* est le nom DNS ou l'adresse IP d'un serveur ZENworks.
2. Dans le volet de navigation de gauche, cliquez sur *Outils d'administration*.
3. Cliquez sur le fichier `novell-zenworks-rm-repeater-<version>.msi` et enregistrez-le à un emplacement temporaire.

   version correspond à la version du produit ZENworks.
4. Installez l'application proxy en exécutant la commande suivante :

   ```
   msiexec /i novell-zenworks-rm-repeater-<version>.msi
   TARGETDIR="répertoire_installation_ZENworks”.
   ```

Sur Linux:

1. Sur le périphérique, ouvrez la page de téléchargement ZENworks dans un navigateur Web :

   https://*server*/zenworks-setup

   où *serveur* est le nom DNS ou l'adresse IP d'un serveur ZENworks.
2. Dans le volet de navigation de gauche, cliquez sur *Outils d'administration*.
3. Cliquez sur le fichier `novell-zenworks-rm-repeater-<version>.noarch.rpm`.
4. Choisissez si vous souhaitez installer immédiatement le proxy ou si vous préférez enregistrer son fichier RPM pour une installation ultérieure.
   - Pour l'installer directement, cliquez sur *Ouvrir avec* afin d'ouvrir le proxy de gestion à distance avec zen-installer, spécifiez le mot de passe de l'utilisateur root, puis cliquez sur *OK*.
   - Pour enregistrer le fichier RPM du proxy dans le répertoire de téléchargement par défaut afin de l'installer plus tard, cliquez sur *Enregistrer sur le disque*. Pour installer le RPM, effectuez l'une des opérations suivantes:
     - Cliquez sur le fichier RPM du proxy, spécifiez le mot de passe de l'utilisateur root, puis cliquez sur *OK*.
     - Exécutez la commande suivante en tant que superutilisateur ou utilisateur root :

       ```
       rpm -ivh novell-zenworks-rm-repeater-<version>.noarch.rpm
       ```

Le proxy de gestion à distance est conçu pour s'exécuter automatiquement à l'installation. Pour personnaliser son comportement, vous pouvez modifier les paramètres par défaut du périphérique. Pour plus d'informations sur les paramètres du proxy de gestion à distance, reportez-vous à la Section 2.11, « Configuration d'un proxy de gestion à distance », page 51.

2.11 Configuration d'un proxy de gestion à distance

Lorsque vous installez un proxy de gestion à distance sur un périphérique, certains paramètres sont configurés sur le périphérique par défaut. Vous avez la possibilité de modifier ces paramètres.

- Section 2.11.1, « Paramètres de proxy de gestion à distance sur un périphérique Windows », page 51
- Section 2.11.2, « Paramètres de proxy de gestion à distance sur un serveur primaire ou satellite Linux », page 51

2.11.1 Paramètres de proxy de gestion à distance sur un périphérique Windows

Sur un périphérique Windows, les paramètres de registre du proxy de gestion à distance sont disponibles sous `HKLM\SOFTWARE\Novell\ZCM\Remote Management\Proxy`.

ClientPort : indique le numéro du port que le proxy utilise pour recevoir les demandes de session à distance depuis la visionneuse de gestion à distance. La valeur par défaut est 5750.

SessionEncryption : indique si le flux de données initial entre le proxy et la visionneuse de gestion à distance est codé. La valeur par défaut est True. Ce paramètre ne s'applique pas une fois que le proxy a établi la connexion avec le périphérique géré. Le codage de la session est ensuite géré par la stratégie de gestion à distance et les préférences de l'opérateur à distance. Il est conseillé de laisser ce paramètre défini sur True car sa définition sur False autorise des processus externes non authentifiés, autres que la visionneuse de gestion à distance, à réaliser des connexions avec les périphériques au sein du réseau privé.

SSLClientAuthentication : indique si le proxy doit accepter les demandes de connexion provenant d'une visionneuse qui ne dispose pas d'un certificat valide. Les valeurs possibles sont True ou False. La valeur par défaut est True.

2.11.2 Paramètres de proxy de gestion à distance sur un serveur primaire ou satellite Linux

Sur un serveur primaire ou satellite Linux, les paramètres du proxy de gestion à distance sont disponibles dans le fichier `/etc/opt/novell/zenworks/repeater/nzrepeater.ini`. Voici quelques exemples de ces paramètres :

viewerport : indique le numéro du port que le proxy de gestion à distance utilise pour recevoir les demandes de session à distance depuis la visionneuse de gestion à distance. La valeur par défaut est 5750.

runasuser : indique l'utilisateur auquel doit être associé le proxy. Pour réaliser des opérations à distance, le proxy de gestion à distance ne nécessite que des privilèges utilisateur. La valeur par défaut est zenworks, mais vous pouvez spécifier un autre utilisateur.

strictimpersonation : indique si la session à distance doit se poursuivre en tant que `root` lorsque l'utilisateur spécifié pour runasuser n'existe pas. Les valeurs possibles sont True ou False. La valeur par défaut est False, ce qui signifie que la session à distance se poursuit en tant que `root` dans ce cas.

sslauth : indique si l'authentification SSL est activée ou non. Les valeurs possibles sont 0 ou 1. La valeur par défaut est 1, qui indique que l'authentification SSL est activée.

Avertissement : il est déconseillé de désactiver l'authentification SSL car cela autorise des processus externes à accéder aux périphériques du réseau sans authentification.

---

verifyViewerCert : indique si les certificats de la visionneuse de gestion à distance nécessitent une vérification. Ce paramètre n'est applicable que lorsque l'authentification SSL est activée. Les valeurs possibles sont 0 ou 1. La valeur par défaut est 1, ce qui signifie que les certificats de la visionneuse de gestion à distance doivent être vérifiés. Lorsqu'une session est initiée à partir d'une visionneuse autonome, il se peut que l'opérateur à distance ne dispose pas des certificats requis qui sont associés à l'autorité de certification racine. Dans ce cas, la connexion du proxy au serveur échoue.

loggingenabled : indique si les messages doivent être consignés sur le périphérique. Les valeurs possibles sont True ou False. La valeur par défaut est True.

Pour obtenir des informations sur les autres paramètres du registre, reportez-vous au fichier `/etc/opt/novell/zenworks/repeater/nzrepeater.ini`.

Gestion des sessions distantes

3

Les sections suivantes fournissent des informations qui vous aideront à gérer efficacement les sessions à distance de Novell® ZENworks® 10 Configuration Management :

3.1 Gestion d'une session d'affichage à distance

La gestion à distance vous permet de contrôler un périphérique géré à distance. Avec des connexions de contrôle à distance, l'opérateur distant n'est plus limité au simple affichage du périphérique géré mais peut désormais le contrôler, ce qui facilite les tâches d'assistance et de résolution des problèmes sur le périphérique géré. Pour plus d'informations sur le lancement d'une session de contrôle à distance, reportez-vous à la Section 2.8, « Démarrage des opérations de gestion à distance », page 35.

3.1.1 Utilisation des options de la barre d'outils dans la visionneuse de gestion à distance

Le tableau suivant décrit les différentes options de barre d'outils disponibles dans la visionneuse de gestion à distance pendant une session de contrôle à distance. Il répertorie également les touches de raccourci lorsqu'elles existent.

Tableau 3-1 *Options de barre d'outils dans la visionneuse de gestion à distance*

Option	Touche de raccourci	Fonction
Options de connexion 	Ctrl+Alt+Maj+P	Permet de configurer différents paramètres de session, tels que le format et le codage, afin d'améliorer les performances de la session, la consignation et la gestion locale et distante du curseur.
Infos de connexion 	Ctrl+Alt+Maj+I	Fournit le nom d'hôte, le port, la résolution de l'écran et la version du protocole du périphérique géré.

Option	Touche de raccourci	Fonction
Plein écran 	Ctrl+Alt+Maj+F	Permet de basculer entre les modes d'affichage normal et plein écran.
Demander un rafraîchissement de l'écran 	Ctrl+Alt+Maj+H	Rafraîchit la fenêtre d'affichage.
Envoyer Ctrl-Alt-Suppr 		Envoie la séquence Ctrl+Alt+Suppr au périphérique géré. La fonction de simulation de la fonctionnalité Ctrl+Alt+Suppr sur un périphérique Windows 7 est actuellement désactivée.
Envoyer Ctrl-Ech 		Ouvre le menu Démarrer sur les périphériques gérés.
Envoyer Appuyer/ relâcher la touche Alt 		Cliquez sur cette option et appuyez sur la touche ALT du clavier pour envoyer la séquence au périphérique géré.
Mettre en veille/ activer l'écran 	Ctrl+Alt+Maj+B	Vide ou affiche l'écran sur le périphérique géré. Lorsque l'écran est vidé, les opérations exécutées par l'opérateur distant sur le périphérique ne sont plus visibles pour l'utilisateur du périphérique. Les commandes du clavier et de la souris du périphérique géré sont également verrouillées. Cette option est activée uniquement si l'option *Autoriser la mise en veille de l'écran du périphérique géré* est cochée dans la stratégie de gestion à distance active sur le périphérique géré.
Verrouiller/ déverrouiller le clavier et la souris 	Ctrl+Alt+Maj+L	Verrouille ou déverrouille les commandes du clavier et de la souris pour le périphérique géré. Lorsque les commandes de la souris et du clavier sont verrouillées, l'utilisateur du périphérique géré ne peut pas les utiliser. Cette option est activée uniquement si l'option *Autoriser le verrouillage de la souris et du clavier du périphérique géré* est cochée dans la stratégie de gestion à distance active sur le périphérique géré.

Option	Touche de raccourci	Fonction
Transférer les fichiers 	Ctrl+Alt+Maj+T	Lance une session pour transférer des fichiers vers et à partir du périphérique géré. Cette option est activée uniquement si l'option *Autoriser le transfert de fichiers sur le périphérique géré* est cochée dans la stratégie de gestion à distance active sur le périphérique géré. Pour plus d'informations sur le transfert de fichiers, reportez-vous à la Section 3.5, « Gestion d'une session de transfert de fichiers », page 60.
Collaboration 		Lance une session de collaboration ZENworks Remote Management sur le périphérique géré, ce qui permet d'inviter plusieurs opérateurs à distance à rejoindre la session de gestion à distance. Vous pouvez également déléguer les droits du contrôle à distance à un autre opérateur à distance afin qu'il vous aide à résoudre le problème. Cette option n'est actuellement prise en charge que sous Windows. Pour plus d'informations sur la collaboration de session, reportez-vous à la Section 3.1.2, « Collaboration de session », page 55.
Exécution à distance 	Ctrl+Alt+Maj+U	Lance une session d'exécution à distance sur le périphérique géré afin de lancer à distance n'importe quel exécutable du périphérique géré. Cette option est activée uniquement si l'option *Autoriser l'exécution à distance des programmes sur le périphérique géré* est cochée dans la stratégie de gestion à distance active sur le périphérique géré.
Remplacer l'économiseur d'écran 	Ctrl+Alt+Maj+O	Remplace un éventuel économiseur d'écran protégé par mot de passe sur le périphérique géré au cours de la session à distance. Cette option est activée uniquement si l'option *Autoriser le déverrouillage automatique de l'économiseur d'écran lors du contrôle à distance* est cochée dans la stratégie de gestion à distance active sur le périphérique géré.
Déconnecter 	Alt+F4	Ferme la session à distance.

3.1.2 Collaboration de session

La fonction Collaboration de session permet d'inviter plusieurs opérateurs distants à rejoindre la session de gestion distante si les opérateurs distants ont lancé le module d'écoute de la gestion à distance pour écouter les requêtes de session distante. Vous pouvez également déléguer les droits de contrôle à distance à un opérateur à distance pour aider à résoudre un problème et lui reprendre le contrôle par la suite. Cette option n'est actuellement prise en charge que sous Windows.

Si vous lancez d'abord la session de contrôle à distance sur le périphérique, vous obtenez les privilèges d'un opérateur distant principal. Vous pouvez utiliser la collaboration de session pour :

- Inviter plusieurs opérateurs distants à participer à la session de contrôle à distance.
- Déléguer les droits de contrôle à distance à un opérateur distant pour vous aider à résoudre un problème avant de les lui reprendre.
- Fermer une session à distance.

Pour lancer une collaboration de session, procédez comme suit :

1. Lancez la session de contrôle à distance sur le périphérique géré en mode de collaboration.

   Pour obtenir des informations sur le lancement d'une session de contrôle à distance, reportez-vous à la Section 2.8, « Démarrage des opérations de gestion à distance », page 35.
2. Dans la barre d'outils de la visionneuse de gestion à distance, cliquez sur  pour afficher la fenêtre Collaboration de session.

La fenêtre Collaboration de session répertorie les opérateurs à distance ajoutés à la stratégie de gestion à distance effective sur le périphérique. Chaque opérateur distant apparaît comme une entrée séparée précédée d'un cercle de couleur :

- Un cercle gris indique que l'opérateur à distance n'a pas rejoint la session.
- Un cercle rouge indique que l'opérateur distant a rejoint la session et se trouve en mode Affichage à distance.
- Un cercle vert indique que l'opérateur distant a rejoint la session et dispose des droits délégués de contrôle à distance dans la session.

Pour plus d'informations sur l'ajout des opérateurs à distance, reportez-vous à la Section 2.3, « Création de la stratégie de gestion à distance », page 23.

Le tableau suivant décrit les actions qu'un opérateur distant principal peut effectuer lors d'une collaboration de session :

Tableau 3-2 *Options de la fenêtre Collaboration de session*

Tâche	Étapes	Détails complémentaires
Invitez un opérateur distant à participer à une session à distance.	1. Sélectionnez un opérateur distant figurant dans la fenêtre de collaboration de session. 2. Cliquez sur *Inviter.*	Si l'opérateur distant accepte la demande et rejoint la session, le cercle gris de l'opérateur devient rouge. Par défaut, la nouvelle session démarre en mode Affichage à distance.
Déléguer les droits de contrôle à distance à l'opérateur distant.	1. Sélectionnez l'opérateur à distance auquel vous voulez déléguer les droits de contrôle à distance. 2. Cliquez sur *Déléguer.*	L'opérateur distant sélectionné se trouve désormais en mode Contrôle à distance et son cercle rouge devient vert. L'opérateur distant principal passe automatiquement en mode Affichage à distance.

Tâche	Étapes	Détails complémentaires
Reprendre les droits de contrôle à distance à l'opérateur distant	1. Cliquez sur *Reprendre le contrôle.*	L'opérateur distant passe en mode Affichage à distance et son cercle vert devient rouge. L'opérateur distant passe automatiquement en mode Contrôle à distance.
Mettre fin à la session distante	1. Sélectionnez l'opérateur distant à partir duquel vous voulez mettre fin à la session distante. 2. Cliquez sur *Arrêter.*	Si l'opérateur distant sélectionné se trouve en mode Contrôle à distance, vous reprenez les droits de contrôle à distance. La session de l'opérateur distant se termine et la couleur de son cercle devient grise.
Inviter un opérateur distant externe	1. Cliquez sur *Inviter un opérateur à distance externe* pour inviter à une session à distance les opérateurs distants qui ne figurent pas dans la fenêtre Collaboration de session. 2. Indiquez le nom DNS ou l'adresse IP du périphérique de l'opérateur distant ainsi que le numéro de port. Par exemple, 10.0.0.0 ~~1000. 3. Cliquez sur *Inviter.*	

Si l'opérateur distant principal se déconnecte de la session distante, la session est arrêtée pour tous les opérateurs distants.

3.2 Gestion d'une session d'affichage à distance

L'affichage à distance vous permet de vous connecter à un périphérique géré à distance afin de visualiser le bureau du périphérique géré. Pour plus d'informations sur l'exécution d'une session d'affichage à distance, reportez-vous à la Section 2.8, « Démarrage des opérations de gestion à distance », page 35.

Le tableau suivant décrit les différentes options de barre d'outils disponibles dans la visionneuse de gestion à distance lors d'une session d'affichage à distance.

Tableau 3-3 *Options de barre d'outils dans la visionneuse de gestion à distance*

Option	Touche de raccourci	Fonction
Options de connexion 	Ctrl+Alt+Maj+P	Permet de configurer différents paramètres de session, tels que le format et le codage, afin d'améliorer les performances de la session, la consignation et la gestion locale et distante du curseur.

Option	Touche de raccourci	Fonction
Infos de connexion 	Ctrl+Alt+Maj+I	Fournit le nom d'hôte, le port, la résolution de l'écran et la version du protocole du périphérique géré.
Plein écran 	Ctrl+Alt+Maj+F	Permet de basculer entre les modes d'affichage normal et plein écran.
Demander un rafraîchissement de l'écran 	Ctrl+Alt+Maj+H	Rafraîchit la fenêtre d'affichage.
Déconnecter 	Alt+F4	Ferme la session à distance.

3.3 Gestion d'une session d'exécution à distance

L'exécution à distance vous permet de lancer à distance des exécutables avec des privilèges système sur le périphérique géré. Pour exécuter une application sur le périphérique géré, vous devez lancer la session d'exécution à distance.

1. Lancez la session d'exécution à distance.

   Pour plus d'informations sur le lancement d'une session d'exécution à distance, reportez-vous à la Section 2.8, « Démarrage des opérations de gestion à distance », page 35.

2. Spécifiez le nom de l'exécutable.

   Indiquez le chemin d'accès complet de l'application si elle n'est pas dans le chemin d'accès système du périphérique géré. Si vous ne précisez pas l'extension du fichier que vous souhaitez exécuter sur le périphérique géré, le programme d'exécution à distance ajoute automatiquement l'extension `.exe`.

3. Cliquez sur *Exécuter*.

L'exécution à distance de l'application spécifiée peut échouer si l'application n'est pas disponible dans le chemin spécifié du périphérique géré.

Avertissement : par défaut, le module d'exécution à distance est exécuté comme un service avec des privilèges système sur le périphérique géré. Toutes les applications lancées pendant la session d'exécution à distance sont donc exécutées avec des privilèges système. Pour des raisons de sécurité, nous vous recommandons de fermer l'application après utilisation.

3.4 Gestion d'une session de diagnostic à distance

La gestion à distance permet d'établir un diagnostic à distance et d'analyser les problèmes sur le périphérique géré. Cela vous aide à réduire le temps nécessaire pour résoudre des problèmes et à assister les utilisateurs sans demander à un technicien de visiter physiquement le périphérique concerné. Les bureaux étant opérationnels, la productivité de l'utilisateur s'en trouve accrue.

Lorsque vous lancez une session de diagnostic à distance sur le périphérique géré, vous pouvez accéder uniquement aux applications de diagnostic configurées dans les paramètres de gestion à distance pour établir le diagnostic et corriger les problèmes sur le périphérique. Durant la session, les applications de diagnostic apparaissent sous forme d'icônes dans une barre d'outils. Par défaut, les applications de diagnostic suivantes sont configurées dans les paramètres de gestion à distance :

Tableau 3-4 *Options de barre d'outils dans la visionneuse de gestion à distance*

Option	Touche de raccourci	Fonction
Options de connexion 	Ctrl+Alt+Maj+P	Permet de configurer différents paramètres de session, tels que le format et le codage, afin d'améliorer les performances de la session, la consignation et la gestion locale et distante du curseur.
Infos de connexion 	Ctrl+Alt+Maj+I	Fournit le nom d'hôte, le port, la résolution de l'écran et la version du protocole du périphérique géré.
Plein écran 	Ctrl+Alt+Maj+F	Permet de basculer entre les modes d'affichage normal et plein écran.
Demander un rafraîchissement de l'écran 	Ctrl+Alt+Maj+H	Rafraîchit la fenêtre d'affichage.
Transférer les fichiers 	Ctrl+Alt+Maj+T	Lance une session pour transférer des fichiers vers et à partir du périphérique géré. Cette option est activée uniquement si l'option *Autoriser le transfert de fichiers sur le périphérique géré* est cochée dans la stratégie de gestion à distance active sur le périphérique géré. Pour plus d'informations sur le transfert de fichiers, reportez-vous à la Section 3.5, « Gestion d'une session de transfert de fichiers », page 60.
Déconnecter 	Alt+F4	Ferme la session à distance.

Tableau 3-5 *Applications de diagnostic à distance*

Icône	Application
	*Informations système*
	*Gestion de l'ordinateur*
	*Services*
	*Éditeur de registre*

Vous pouvez configurer les applications à exécuter sur le périphérique géré lors de la session de diagnostic à distance. Pour plus d'informations sur la configuration des applications de diagnostic, reportez-vous à la Section 2.1, « Configuration des paramètres de gestion à distance », page 19.

3.5 Gestion d'une session de transfert de fichiers

La gestion à distance vous permet de transférer les fichiers entre la console de gestion et le périphérique géré. Pour plus d'informations sur le lancement d'une session de transfert de fichiers, reportez-vous à la Section 2.8, « Démarrage des opérations de gestion à distance », page 35.

Dans la fenêtre Transfert de fichiers, la sous-fenêtre Ordinateur local affiche tous les fichiers et dossiers de la console de gestion et la sous-fenêtre Ordinateur distant affiche les fichiers et dossiers présents dans le répertoire spécifié dans l'option *Répertoire racine du transfert de fichiers* dans la stratégie de gestion à distance. Si le *Répertoire racine du transfert de fichiers* n'est pas spécifié dans la stratégie ou si aucune stratégie n'est associée au périphérique géré, vous pouvez exécuter les opérations de transfert de fichiers sur le système de fichiers complet du périphérique distant.

Le tableau suivant explique les commandes du transfert de fichiers et les options qui sont disponibles pour travailler avec des fichiers provenant de la fenêtre Transfert de fichiers. L'option de menu *Opérations* n'est pas encore prise en charge sous Linux. Vous pouvez néanmoins effectuer cette opération en cliquant sur l'icône correspondante de la barre d'outils.

Tableau 3-6 *Options de la fenêtre Transfert de fichiers*

Tâches	Raccourcis clavier	Étapes	Détails complémentaires
Créer un nouveau dossier local	Alt+L	1. Cliquez sur *Opérations* > *Nouveau dossier local*. ou Cliquez sur dans le volet Ordinateur local. 2. Suivez les invites à l'écran.	
Créer un nouveau dossier à distance	Alt+W	1. Cliquez sur *Opérations* > *Nouveau dossier à distance*. ou Cliquez sur dans le volet Ordinateur à distance. 2. Suivez les invites à l'écran.	
Ouvrir un fichier		1. Double-cliquez sur le fichier pour l'ouvrir dans l'application associée.	
Renommer des fichiers ou dossiers	Alt+N	1. Sélectionnez le fichier ou dossier à renommer. 2. Cliquez sur *Opérations* > *Renommer.* ou Cliquez sur . 3. Suivez les invites à l'écran.	
Supprimer des fichiers ou dossiers	Alt+D	1. Sélectionnez les fichiers ou dossiers à supprimer. 2. Cliquez sur *Opérations* > *Supprimer.* ou Cliquez sur . 3. Suivez les invites à l'écran.	Vous pouvez utiliser les touches Maj ou Ctrl pour sélectionner plusieurs fichiers.

Tâches	Raccourcis clavier	Étapes	Détails complémentaires
Rafraîchir un dossier local	Alt+E	1. Cliquez sur *Opérations* > *Rafraîchir un dossier local*. ou Cliquez sur dans le volet Ordinateur local.	
Rafraîchir un dossier à distance	Alt+M	1. Cliquez sur *Opérations* > *Rafraîchir un dossier à distance*. ou Cliquez sur dans le volet Ordinateur à distance.	
Trier les fichiers locaux		1. Cliquez sur *Opérations* > *Tri local*. 2. Sélectionnez le type de tri. Vous pouvez trier les fichiers par nom, par taille ou par date.	Vous pouvez également trier les fichiers en cliquant sur les en-têtes des colonnes respectives.
Trier les fichiers à distance		1. Cliquez sur *Opérations* > *Tri à distance*. 2. Sélectionnez le type de tri. Vous pouvez trier les fichiers par nom, par taille ou par date	Vous pouvez également trier les fichiers en cliquant sur les en-têtes des colonnes respectives.
Télécharger des fichiers/ dossiers		1. Sélectionnez les fichiers à télécharger sur l'ordinateur à distance. 2. Sélectionnez le répertoire de destination dans le tableau de bord de l'ordinateur à distance. 3. Cliquez sur *Opérations* > *Télécharger.* ou Cliquez sur ➡	L'option *Opérations* > *Télécharger* n'est disponible que si le focus est sur l'ordinateur local. Vous pouvez utiliser les touches Maj ou Ctrl pour sélectionner plusieurs fichiers.

Tâches	Raccourcis clavier	Étapes	Détails complémentaires
Télécharger des fichiers/ dossiers	Alt+O	1. Sélectionnez les fichiers à télécharger sur l'ordinateur local. 2. Sélectionnez le répertoire de destination dans le tableau de bord de l'ordinateur local 3. Cliquez sur *Opérations* > *Charger*. ou Cliquez sur ⬅	L'option *Opérations* > *Charger* n'est disponible que si le focus est sur l'ordinateur à distance. Vous pouvez utiliser les touches Maj ou Ctrl pour sélectionner plusieurs fichiers.
Annuler le transfert de fichier	Alt+C	1. Cliquez sur *Opérations* > *Annuler le transfert de fichiers*	Vous pouvez également annuler l'opération de transfert des fichiers en cliquant sur le bouton Annuler.
Afficher les propriétés des fichiers	Alt+P	1. Sélectionnez les fichiers. 2. Cliquez sur *Opérations* > *Propriétés*. ou Cliquez sur 	Vous pouvez utiliser les touches Maj ou Ctrl pour sélectionner plusieurs fichiers. Affiche la taille cumulée des fichiers et dossiers sélectionnés.
Placer dans le dossier parent		1. Cliquez sur  pour le placer dans le dossier parent.	

3.6 Administration d'une session de proxy de gestion à distance

Un proxy de gestion à distance vous permet d'effectuer une opération de gestion à distance sur un périphérique géré qui se trouve sur un réseau privé ou de l'autre côté d'un pare-feu ou d'un routeur utilisant la traduction d'adresses réseau (NAT).

Pour plus d'informations sur le proxy de gestion à distance, reportez-vous à la Section 1.4, « Présentation du proxy de gestion à distance », page 16.

Pour plus d'informations sur l'installation d'un proxy de gestion à distance, reportez-vous à la Section 2.10, « Installation d'un proxy de gestion à distance », page 49.

Pour plus d'informations sur la configuration d'un proxy de gestion à distance, reportez-vous à la Section 2.11, « Configuration d'un proxy de gestion à distance », page 51.

3.7 Activation d'un périphérique distant

L'activation à distance permet d'activer à distance un nœud unique ou un groupe de noeuds mis hors tension sur votre réseau si la carte réseau sur le nœud est activée dans un environnement Wake-on-LAN.

La sortie de veille d'un périphérique qui présente plusieurs cartes d'interface réseau réussit uniquement si au moins l'une de ces cartes est configurée pour un sous-réseau contenant le périphérique qui diffuse le paquet Wake-on-LAN.

3.7.1 Conditions préalables

Avant d'activer les périphériques gérés, les conditions suivantes doivent être remplies.

- Vérifiez que la carte réseau du périphérique géré prend en charge Wake-on-LAN. Assurez-vous que l'option Wake-on-LAN est bien activée dans la configuration du BIOS du périphérique géré.
- Vérifiez que le périphérique géré est enregistré dans la zone de gestion ZENworks.
- Assurez-vous que le noeud distant est dans un état d'arrêt à chaud. Avec l'arrêt à chaud, le CPU est arrêté et une quantité d'énergie minimum est utilisée par sa carte d'interface réseau. Contrairement à l'arrêt à froid, avec l'arrêt à chaud, la connexion de courant vers la machine reste activée lorsque la machine est éteinte.

3.7.2 Activation à distance des périphériques gérés

Pour exécuter une activation à distance :

1. Dans le Centre de contrôle ZENworks, cliquez sur *Périphériques*.
2. Cliquez sur *Serveurs* ou *Postes de travail* pour afficher la liste des périphériques gérés.
3. Sélectionnez le périphérique à activer.
4. Cliquez sur *Tâches rapides* > *Activer* pour afficher la boîte de dialogue Activation.
5. Sélectionnez l'une des options suivantes afin de spécifier les serveurs pour l'envoi d'une requête de réveil aux périphériques gérés :
   - **Détecter automatiquement le serveur :** ZENworks détecte automatiquement le serveur primaire le plus proche du périphérique géré. Si le serveur et le périphérique à distance se trouvent dans des sous-réseaux différents, veillez à ce que le routeur qui les connecte soit configuré de manière à transmettre les diffusions orientées sous-réseau au port UDP 1761.
   - **Utilisez les périphériques suivants :** cliquez sur *Ajouter* pour sélectionner un périphérique proxy qui existe dans le même sous-réseau que le périphérique à réveiller.

     Si le routeur est configuré de manière à transmettre des diffusions orientées sous-réseau au port UDP 1761, aucun proxy n'est requis.

6 (Facultatif) Sélectionnez l'une des options suivantes pour spécifier l'adresse IP à utiliser pour envoyer la diffusion de réveil :

- **Détecter automatiquement l'adresse IP :** ZENworks détecte automatiquement l'adresse de diffusion par défaut du sous-réseau pour envoyer la diffusion de réveil au périphérique géré.
- **Utilisez l'adresse IP suivante :** spécifiez l'adresse IP pour l'envoi de la diffusion de réveil au périphérique géré, puis cliquez sur *Ajouter*.

7 Pour l'option *Nombre de réessais*, indiquez le nombre de tentatives pour sortir de veille le périphérique. Par défaut, il est de 1.

8 Pour l'option *Intervalle entre deux réessais*, indiquez la période entre deux tentatives. Par défaut, il est de 2 minutes.

9 Cliquez sur *OK*.

Les valeurs par défaut du *Nombre de réessais* et les options d'intervalle entre deux réessais sont configurées au niveau de la zone. Vous pouvez remplacer ces valeurs au niveau du périphérique.

3.8 Amélioration des performances de la gestion à distance

Les performances de gestion à distance pendant une session distante sur une liaison lente ou une liaison rapide varient en fonction du trafic du réseau. Pour un meilleur temps de réponse, procédez de l'une des manières suivantes :

- Section 3.8.1, « Sur la console de gestion », page 65
- Section 3.8.2, « Sur le périphérique géré », page 65

3.8.1 Sur la console de gestion

Dans la fenêtre Connexion de ZENworks Remote Management de la console, cliquez sur *Options* et définissez les valeurs suivantes :

- Pour optimiser les performances de gestion à distance sur une liaison lente :
  - Sélectionnez l'option *Utiliser la couleur 8 bits*.
  - Configurez le *Niveau de compression personnalisé* sur 6.
- Sélectionnez l'option *Bloquer les événements de déplacement de la souris*.
- Activez l'option *Supprimer le papier peint* dans les paramètres de gestion à distance.

3.8.2 Sur le périphérique géré

- La vitesse de la session de gestion à distance dépend de la vitesse de traitement des données du périphérique géré. Nous vous recommandons d'utiliser un processeur Pentium* III, 700 MHz (ou version ultérieure) avec au moins 256 Mo de RAM.
- Ne définissez pas un modèle de papier peint.

Sécurité

4

Les sections suivantes fournissent des informations de sécurité que vous devriez connaître avant d'utiliser le composant de gestion à distance de Novell® ZENworks® 10 Configuration Management :

4.1 Authentification

Le service de gestion à distance doit être installé sur un périphérique pour permettre à l'opérateur distant de gérer le périphérique à distance. Le service démarre automatiquement au démarrage du périphérique géré. Lorsqu'un opérateur distant exécute une session à distance sur le périphérique géré, le service démarre la session à distance uniquement si l'opérateur distant est autorisé à effectuer des opérations à distance sur le périphérique géré.

Pour empêcher tout accès non-autorisé sur le périphérique géré, le service de gestion à distance du périphérique géré utilise les modes d'authentification suivants :

4.1.1 Authentification de gestion à distance par droits

Dans l'authentification par droits, les droits sont assignés à l'opérateur distant pour lancer une session à distance sur le périphérique géré. Par défaut, l'administrateur et le super administrateur ZENworks ont le droit d'effectuer des opérations à distance sur tous les périphériques gérés, quel que soit l'utilisateur connecté au périphérique (utilisateur local ou utilisateur ZENworks).

L'opérateur distant n'a pas besoin de droits exclusifs pour exécuter une session à distance sur le périphérique géré si aucun utilisateur ne s'est connecté sur le périphérique géré ou si un utilisateur s'est connecté sur le périphérique géré mais pas sur ZENworks. En revanche, l'opérateur distant doit disposer de droits exclusifs de gestion à distance pour exécuter l'opération à distance sur le périphérique géré lorsqu'un utilisateur ZENworks s'est connecté au périphérique. Pour des raisons de sécurité, nous vous recommandons vivement d'utiliser l'authentification par droits.

L'utilisation de l'authentification basée sur les droits nécessite l'installation de ZENworks Adaptive Agent sur le périphérique. L'installation du service de gestion à distance uniquement sur le périphérique ne suffit pas.

Ce mode d'authentification n'est pas pris en charge dans le cadre du lancement d'une opération de gestion à distance en mode autonome ou depuis la ligne de commande.

4.1.2 Authentification de gestion à distance par mot de passe

Avec l'authentification par mot de passe, l'opérateur distant est invité à saisir un mot de passe pour pouvoir lancer la session à distance sur le périphérique géré.

Les deux types de schémas d'authentification utilisés sont :

- **Mot de passe ZENworks :** ce schéma est basé sur le protocole Secure Remote Password (SRP) (version 6a). Un mot de passe ZENworks peut contenir au maximum 255 caractères.
- **Mot de passe VNC :** schéma d'authentification par mot de passe VNC traditionnel. Un mot de passe VNC peut contenir au maximum 8 caractères. Ce schéma de mot de passe est faible par nature et est fourni uniquement pour garantir l'interopérabilité avec les composants open source.

Si vous utilisez l'authentification basée sur les mots de passe, nous vous recommandons vivement d'utiliser le modèle de mot de passe ZENworks car il est davantage sécurisé que le modèle de mot de passe VNC.

Les schémas de mot de passe fonctionnent dans les modes suivants :

- **Mode de la session :** le mot de passe défini dans ce mode est valable uniquement pour la session en cours. L'utilisateur du périphérique géré doit définir un mot de passe au début de la session à distance et le communiquer à l'opérateur à distance par des méthodes « hors bande », comme le téléphone. Lors de l'initialisation d'une session à distance avec le périphérique géré, l'opérateur distant doit saisir le mot de passe correct dans la boîte de dialogue de mot de passe de la session. Si l'opérateur distant n'indique pas le mot de passe correct dans un délai de deux minutes après l'ouverture de la boîte de dialogue, la session se ferme automatiquement pour des raisons de sécurité. Si vous utilisez une authentification par mot de passe, nous vous recommandons d'utiliser ce mode d'authentification car le mot de passe est valable uniquement pour la session en cours et n'est pas enregistré sur le périphérique géré.
- **Mode permanent :** dans ce mode, le mot de passe peut être défini par l'administrateur via la stratégie de gestion à distance ou par l'utilisateur du périphérique géré via l'icône ZENworks si l'option *Autoriser l'utilisateur à remplacer les mots de passe par défaut sur le périphérique géré* est sélectionnée dans les paramètres de sécurité de la stratégie de gestion à distance.

  Si le mot de passe est défini par l'utilisateur du périphérique géré et dans la stratégie, le mot de passe défini par l'utilisateur est prioritaire sur celui qui a été configuré dans la stratégie.

  L'administrateur peut interdire à l'utilisateur du périphérique géré de définir le mot de passe et est également autorisé à redéfinir le mot de passe défini par l'utilisateur afin de s'assurer que le mot de passe configuré dans la stratégie demeure toujours appliqué pendant l'authentification. Pour plus d'informations sur la redéfinition du mot de passe défini par l'utilisateur du périphérique géré, reportez-vous à la Section 2.5.3, « Effacement du mot de passe de gestion à distance à l'aide du Centre de contrôle ZENworks », page 33.

4.2 Fiabilité du mot de passe

Utilisez des mots de passe sécurisés. Gardez à l'esprit les consignes suivantes :

- **Longueur :** la longueur minimale recommandée est de 6 caractères. Un mot de passe sécurisé comprend au moins 8 caractères. Plus les mots de passe sont longs, plus il sont fiables. Un mot de passe ZENworks comprend au maximum 255 caractères et un mot de passe VNC 8 caractères.
- **Complexité :** un mot de passe sécurisé comprend une combinaison de lettres et de chiffres. Il doit contenir des lettres minuscules et majuscules et au moins un caractère numérique. L'introduction de chiffres, surtout lorsqu'ils sont ajoutés au milieu et non pas seulement au début ou à la fin, peut améliorer la fiabilité du mot de passe. Les caractères spéciaux tels que &, *, $ et > peuvent améliorer considérablement la fiabilité d'un mot de passe. N'utilisez pas de mots reconnaissables, tels que des noms propres ou des termes d'un dictionnaire, et évitez toute information personnelle telle que numéro de téléphone, date de naissance, date anniversaire, adresse ou code postal.

4.3 Ports

Par défaut, le service de gestion à distance utilise le port 5950 et le module d'écoute de gestion à distance le port 5550. Le pare-feu est configuré pour autoriser n'importe quel port utilisé par le service de gestion à distance, mais vous devez le configurer pour autoriser le port utilisé par le module d'écoute de la gestion à distance.

Par défaut, le proxy de gestion à distance reçoit les données sur le port 5750.

4.4 Audit

ZENworks Configuration Management tient à jour un journal de toutes les sessions à distance effectuées sur le périphérique géré. Ce journal est conservé sur le périphérique géré et peut être visualisé par l'utilisateur et par l'administrateur. L'administrateur peut visualiser les journaux de toutes les sessions à distance effectuées sur le périphérique. L'utilisateur peut afficher les journaux de toutes les sessions à distance exécutées sur le périphérique lorsqu'il y est logué.

Pour afficher le journal d'audit, procédez comme suit :

1. Double-cliquez sur l'icône ZENworks dans la zone de notification du périphérique géré.
2. Dans la sous-fenêtre de gauche, allez dans *Gestion à distance*, puis cliquez sur *Sécurité*.
3. Cliquez sur *Afficher les informations d'audit* pour afficher les informations d'audit des opérations distantes exécutées sur le périphérique.

Champ	Description
Utilisateur ZENworks	Nom de l'utilisateur ZENworks connecté sur le périphérique géré au début de la session à distance.
Opérateurs à distance	Nom de l'opérateur distant qui a effectué l'opération.
Machine console	Nom d'hôte du périphérique sur lequel l'opération à distance a été exécutée.

Champ	Description
IP de la console	Adresse IP du périphérique à partir duquel l'opération à distance a eu lieu. **Remarque :** si l'opération de gestion à distance du périphérique est routée à l'aide d'un proxy de gestion à distance, l'adresse IP du périphérique qui exécute le proxy s'affiche.
Opération	Type d'opération effectuée : contrôle à distance, exécution à distance, affichage à distance, diagnostic à distance, transfert de fichiers.
Heure de début	Heure de début de l'opération à distance.
Heure de fin	Heure de fin de l'opération à distance.
État	État de l'opération à distance : Réussite, En cours d'exécution ou Échec. Le motif de l'échec apparaît également.

4.5 Demander l'autorisation de l'utilisateur du périphérique géré

L'administrateur peut configurer la stratégie de gestion à distance pour permettre aux opérateurs distants de demander l'autorisation de l'utilisateur du périphérique géré avant de démarrer une opération à distance sur le périphérique.

Lorsque l'opérateur distant initie une session à distance sur le périphérique géré, le service de gestion à distance vérifie si l'option *Demander l'autorisation de l'utilisateur du périphérique géré* pour l'opération à distance concernée est activée dans la stratégie active du périphérique. Si l'option est activée et qu'aucun utilisateur ne s'est connecté au périphérique, la session à distance se poursuit. Mais si l'option est activée et qu'un utilisateur s'est connecté au périphérique géré, un message configuré dans la stratégie de gestion à distance apparaît pour demander la permission à l'utilisateur d'exécuter une session à distance sur le périphérique. La session démarre uniquement si l'utilisateur donne son autorisation.

4.6 Fin anormale

Lorsqu'une session distante est brusquement déconnectée, la fonction de fin anormale vous permet de verrouiller le périphérique géré ou de déconnecter l'utilisateur du périphérique géré, selon les paramètres de sécurité configurés sur la stratégie de gestion à distance. La session à distance se termine anormalement dans les circonstances suivantes :

- Le réseau est interrompu et la visionneuse de gestion à distance et le service de gestion à distance ne peuvent pas communiquer.
- La visionneuse de gestion à distance est brutalement fermée depuis le gestionnaire des tâches.
- Le réseau est désactivé sur le périphérique géré ou sur la console de gestion.

Dans certains cas, le service de gestion à distance peut prendre une minute pour déterminer la fin anormale de la session.

4.7 Détection d'intrus

La fonction de détection d'intrus réduit considérablement le risque de piratage du périphérique géré. Si l'opérateur distant ne parvient pas à se connecter au périphérique avec le nombre de tentatives autorisé (5 par défaut), le service de gestion à distance est automatiquement bloqué et refuse toute requête de session distante jusqu'à ce qu'il soit débloqué. L'administrateur peut débloquer le service de gestion à distance manuellement ou automatiquement.

4.7.1 Déblocage automatique du service de gestion à distance

Le service de gestion à distance est débloqué automatiquement après le délai spécifié pour l'option *Démarrer automatiquement l'acceptation des connexions après [] minutes* dans la stratégie de gestion à distance. Le délai par défaut est de 10 minutes. Vous pouvez modifier cette durée par défaut dans les paramètres de sécurité de la stratégie de gestion à distance.

4.7.2 Déblocage manuel du service de gestion à distance

Vous pouvez débloquer manuellement le service de gestion à distance depuis le périphérique géré ou le Centre de contrôle ZENworks.

Pour débloquer le service de gestion à distance à partir du Centre de contrôle ZENworks, l'opérateur distant doit avoir les droits Débloquer le service de gestion à distance sur le périphérique géré.

1. Dans le Centre de contrôle ZENworks, cliquez sur *Périphériques*.
2. Cliquez sur *Serveurs* ou *Postes de travail* pour afficher la liste des périphériques gérés.
3. Sélectionnez le périphérique à débloquer.
4. Cliquez sur *Opérations*, puis sur *Débloquer la gestion à distance*.
5. Cliquez sur *OK*.

Pour débloquer le service de gestion à distance depuis le périphérique géré, procédez comme suit :

1. Double-cliquez sur l'icône ZENworks dans la zone de notification du périphérique géré.
2. Dans la sous-fenêtre de gauche, allez dans *Gestion à distance*, puis cliquez sur *Sécurité*.
3. Cliquez sur *Autoriser l'acceptation des connexions si blocage en cours pour détection d'intrusion*.

4.8 Identification de l'opérateur distant

Lorsqu'un opérateur distant exécute une session à distance depuis le centre de contrôle ZENworks, un certificat est automatiquement généré pour aider le périphérique géré à identifier l'opérateur distant. Toutefois, si l'opérateur distant exécute la session en mode autonome, le certificat n'est pas généré et l'opérateur distant est enregistré en tant qu'*Utilisateur inconnu* dans les journaux d'audit et dans les boîtes de dialogue Signal visible et Demander l'autorisation de l'utilisateur. Le service de gestion à distance récupère l'identité de l'opérateur distant en utilisant le certificat fourni par la console de gestion pendant le contrôle de flux SSL. Le contrôle de flux SSL est activé pour tous les types d'authentification à l'exception de l'authentification par mot de passe VNC.

Le service de gestion à distance sur le périphérique affiche les détails de l'opérateur distant dans la boîte de dialogue Signal visible si l'option *Émettre un signal visible à l'utilisateur sur le périphérique géré* est activée dans la stratégie active sur le périphérique. Il consigne également les informations de l'opérateur à distance dans les journaux d'audit de la gestion à distance.

4.9 Configuration du navigateur

Si vous utilisez Internet Explorer pour lancer le Centre de contrôle ZENworks sur les périphériques Windows Vista, désactivez le mode protégé dans les paramètres de sécurité du navigateur (*Outils* > *Options Internet* > *Sécurité*) et redémarrez-le.

4.10 Sécurité de la session

ZENworks Configuration Management utilise le protocole Secure Socket Layer (SSL) pour sécuriser les sessions à distance. Mais les sessions à distance exécutées à partir de l'authentification par mot de passe VNC ne sont pas sécurisées. Le processus d'authentification à lieu sur un canal sécurisé lorsque la reconnaissance mutuelle SSL se produit, que le codage de la session soit configuré ou non dans la stratégie de gestion à distance.

Lorsque l'authentification est terminée, la session à distance passe en mode non sécurisé lorsque l'option *Activer le codage de session* est désactivée dans la stratégie de gestion à distance et que l'option *Codage de la session* est désactivée par l'opérateur distant lorsqu'il lance une session distante sur le périphérique géré. Nous vous recommandons toutefois de poursuivre la session en mode sécurisé par ceci n'a pas d'impact majeur sur ses performances.

4.10.1 Contrôle de flux SSL

Lors de l'installation de ZENworks Adaptive Agent sur un périphérique géré, le service de gestion à distance génère un certificat autosigné valide pendant 10 ans.

Lorsqu'un opérateur distant exécute une session à distance sur le périphérique géré, la visionneuse de gestion à distance demande à l'opérateur distant de vérifier le certificat du périphérique géré. Le certificat affiche les détails tels que le nom du périphérique géré, l'autorité de délivrance du certificat, la validité du certificat et l'empreinte digitale. Pour des raisons de sécurité, l'opérateur distant doit vérifier les références du périphérique géré en comparant l'empreinte digitale du certificat à celle communiquée par l'utilisateur du périphérique géré via une communication hors bande. L'opérateur distant peut ensuite :

- **Accepter le certificat définitivement :** si un utilisateur connecté à la console de gestion accepte le certificat définitivement, le certificat ne s'affiche pas dans les prochaines sessions à distance initiées par les utilisateurs connectés à cette console.
- **Accepter le certificat temporairement :** si un utilisateur connecté à la console de gestion accepte le certificat temporairement, le certificat est accepté uniquement pour la session en cours. L'utilisateur est invité à vérifier le certificat à la prochaine connexion sur le périphérique géré.
- **Rejeter le certificat :** si un utilisateur connecté à la console de gestion rejette le certificat, la session à distance est terminée.

4.10.2 Régénération du certificat

Le périphérique géré regénère un nouveau certificat signé automatiquement si :

- le nom du périphérique géré a été modifié
- le certificat est postdaté et n'est pas valide au moment de la vérification
- le certificat a expiré
- le certificat est sur le point d'expirer
- le certificat est introuvable

Par défaut, le certificat est régénéré une fois tous les 10 ans.

Dépannage

5

Les sections suivantes décrivent les scénarios que vous pouvez rencontrer lorsque vous utilisez le composant de gestion à distance de Novell® ZENworks® 10 Configuration Management.

- « Lorsque vous cliquez sur l'icône Ctrl+Alt+Suppr dans la visionneuse de gestion à distance pendant la session de contrôle à distance, la fenêtre de séquence de touches de sécurité (Secure Attention Sequence - SAS) peut s'afficher sans aucune commande » page 81
- « Le bureau d'un périphérique peut ne pas être visible lorsque vous contrôlez ou affichez ce dernier à distance » page 82
- « Impossible de transférer des fichiers à distance vers des dossiers restreints sur un périphérique Windows Vista, Windows 7, Windows Server 2008 ou Windows Server 2008 R2 » page 82
- « Impossible de lancer une session à distance sur un dispositif SLES (SUSE Linux Enterprise Server) 11 via Mozilla Firefox » page 82
- « Le lien Mettre à niveau la visionneuse de gestion à distance ne s'affiche pas si vous lancez le Centre de contrôle ZENworks via Internet Explorer 8 » page 83

Impossible de remplacer l'économiseur d'écran sur le périphérique géré

Source : ZENworks 10 Configuration Management ; Gestion à distance.

Explication : Lorsqu'un économiseur d'écran protégé par mot de passe est activé sur le périphérique géré avant le démarrage d'une session de contrôle à distance, le service de gestion à distance tente de remplacer l'économiseur d'écran pour permettre à l'opérateur distant d'afficher le bureau de l'utilisateur. L'opérateur distant peut également remplacer l'économiseur d'écran pendant la session distante en cliquant sur l'icône *Remplacer l'économiseur d'écran* sur la barre d'outils de la visionneuse de gestion à distance.

Cause possible : Si l'économiseur d'écran s'active parce que la session à distance est inactive.

Action : Cliquez sur l'icône *Remplacer l'économiseur d'écran* dans la barre d'outils de la visionneuse de gestion à distance. Vous devez cliquer sur l'icône plusieurs fois jusqu'à ce qu'il soit remplacé.

Cause possible : La fonction Remplacement de l'économiseur d'écran n'est pas prise en charge sur les périphériques Windows Vista, Windows 7, Windows Server 2008 et Windows Server 2008 R2.

Action : Aucune.

Cause possible : L'économiseur d'écran peut être interrompu si des mouvements de souris sont envoyés au périphérique géré.

Action : Sélectionnez l'option *Bloquer les événements de déplacement de la souris* dans la fenêtre d'options de la visionneuse ZENworks Remote Management pour empêcher que les mouvements de souris soient envoyés au périphérique géré.

Cause possible : L'identification et l'authentification graphique (GINA) sur le périphérique géré est activée en raison de l'interruption de l'économiseur d'écran sur le périphérique géré.

Action : Reconnectez-vous au périphérique géré.

Au cours d'une session de gestion à distance, si vous vous déloguez et vous loguez à un ordinateur Windows 2000* Professionnel, il se peut que le papier peint défini sur la machine ne soit pas restauré

Source : ZENworks 10 Configuration Management ; Gestion à distance.

Action : Aucune.

Impossible de lancer une session à distance sur le périphérique utilisant une qualité de couleur est très médiocre

Source : ZENworks 10 Configuration Management ; Gestion à distance.

Explication : Il se peut que vous ne parveniez pas à lancer une session de contrôle à distance, d'affichage à distance ou de diagnostic à distance sur un périphérique géré qui utilise une qualité de couleur très faible (moins de 8 bits par pixel).

Action : Procédez comme suit pour augmenter la qualité de couleur du périphérique à au moins 16 bits par pixel.

1. Cliquez avec le bouton droit sur le bureau.
2. Cliquez sur *Propriétés*.
3. Dans la fenêtre Propriétés de l'affichage, cliquez sur *Paramètres*.
4. Sélectionnez la qualité de couleur appropriée, puis cliquez sur *OK*.

Impossible d'exécuter la visionneuse de gestion à distance

Source : ZENworks 10 Configuration Management ; Gestion à distance.

Cause possible : La visionneuse de gestion à distance peut ne pas s'exécuter si le fichier exécutable de la visionneuse de gestion à distance est supprimé ou renommé.

Action : Réinstallez la visionneuse de gestion à distance en téléchargeant la dernière version de `novell-zenworks-rm-viewer.msi` dans `https://`*`Adresse_IP_du_serveur_ZENworks`*`/zenworks-remote-management`.

Risque d'échec de la fin de session anormale sur un périphérique Windows Vista, Windows 7, Windows Server 2008 ou Windows Server 2008 R2

Source : ZENworks 10 Configuration Management ; Gestion à distance.

Explication : Au cours d'une session distante, si l'utilisateur désactive la connexion réseau sur les périphériques Windows Vista, Windows 7, Windows Server 2008 et Windows Server 2008 R2, ZENworks risque de ne pas détecter qu'il s'agit d'une fin anormale et de ne pas verrouiller le périphérique ou déloguer l'utilisateur du périphérique géré.

Action : Aucune.

Le module d'écoute de gestion à distance n'accepte pas les demandes de session à distance sur le périphérique géré si le port qu'il utilise n'est pas ouvert dans le pare-feu de la console de gestion

Source : ZENworks 10 Configuration Management ; Gestion à distance.

Action : Dans le pare-feu de la console de gestion, ouvrez le port du module d'écoute.

Résolution de messages d'erreur rencontrés pendant l'utilisation du composant de gestion à distance

Source : ZENworks 10 Configuration Management ; Gestion à distance.

Action : Pour résoudre les messages d'erreur générés lors de l'utilisation du composant Gestion à distance, envoyez les fichiers journaux suivants au support Novell (http://support.novell.com) :

- Fichiers `WinVNCApp.log` et `WinVNC.log` pour les périphériques Windows Vista, Windows 7, Windows Server 2008 et Windows Server 2008 R2
- Fichier `WinVNC.log` pour tous les autres périphériques gérés

Pour accéder au fichier journal, procédez comme suit :

1. Ouvrez l'éditeur de registre.
2. Accédez au répertoire `HKLM\Software\Novell\ZCM\Remote Management\Agent`.
3. Créez un DWORD appelé DebugMode et définissez sa valeur sur 2.
4. Créez un DWORD appelé DebugLevel et définissez sa valeur hexadécimale sur `a` (valeur décimale égale à 10).
5. Redémarrez le service de gestion à distance.

Les fichiers journaux de la gestion à distance sont créés sous *répertoire_d'installation_ZENworks*`\logs`:

- `WinVNC.log`
- `WinVNCApp.log`

Comment activer le journal de débogage de la gestion à distance sur le périphérique qui lance le centre de contrôle ZENworks

Source : ZENworks 10 Configuration Management ; Gestion à distance.

Action : Pour activer les journaux, reportez-vous à l'article TID 3418069 dans la base de connaissances du support technique Novell (http://support.novell.com/search/kb_index.jsp).

Installer une nouvelle version du pilote du miroir

Source : ZENworks 10 Configuration Management ; Gestion à distance.

Cause possible : Lorsque vous installez ZENworks Adaptive Agent sur un périphérique géré Windows 2003 64 bits, le pilote du miroir n'est pas installé sur le périphérique. Le message `Installer la nouvelle version du pilote du miroir` est consigné dans le Centre de contrôle ZENworks.

Vous pouvez exécuter des sessions à distance sur le périphérique, mais les performances s'en trouveront ralenties.

Action : Ignorez ce message.

Cause possible : Si vous contrôlez à distance un périphérique déjà connecté à l'aide de la connexion au bureau distant, le message `Installer la nouvelle version du pilote du miroir` est consigné dans le Centre de contrôle ZENworks.

Vous pouvez exécuter des sessions distantes sur le périphérique, mais les performances sont ralenties.

Action : Ignorez ce message.

Le périphérique géré n'a pas pu initialiser le schéma de codage Novell pour la session. Assurez-vous que le périphérique géré est configuré à l'heure UTC synchronisée avec ce système. Si le problème persiste, contactez les services techniques de Novell

Source : ZENworks 10 Configuration Management ; Gestion à distance.

Cause possible : Le périphérique géré a été mis à niveau ou enregistré et il se peut que ces informations ne soient pas à jour dans son registre.

Action : Lors de la mise à jour ou de l'enregistrement du périphérique géré, procédez comme suit :

1. Mettez à jour le nom de domaine du nouveau certificat CA dans le registre avec les nouveaux détails :

   Clé : HKLM\Software\Novell\ZCM

   Valeur : CASubject
2. Importez le certificat CA de la nouvelle zone vers la zone de stockage des certificats de racine approuvée.
3. Supprimez de la zone de stockage des certificats de racine approuvée le certificat CA de l'ancienne zone.

Cause possible : Le périphérique géré a été déplacé dans une nouvelle zone de gestion.

Action : Gérez le périphérique depuis la nouvelle zone de gestion.

Les applications telles que Regedit lancées sur un périphérique géré 64 bits par l'intermédiaire de l'exécution à distance n'ont pas accès à certaines clés de registre

Source : ZENworks 10 Configuration Management ; Gestion à distance.

Cause possible : Les applications lancées sur un périphérique géré 64 bits pendant l'exécution à distance sont exécutées dans un environnement Windows On Windows (WOW).

Action : Lancez les applications à l'aide de la fonction de diagnostic à distance.

L'option d'écran vide peut ne pas fonctionner lors du contrôle à distance d'un périphérique Windows

Source : ZENworks 10 Configuration Management ; Gestion à distance.

Cause possible : Les pilotes hérités de Windows n'autorisent pas l'option d'écran vide.

Action : Vous devez installer le pilote graphique correspondant au système.

Lors du lancement d'une session de gestion à distance sur un périphérique géré Windows 2000 Professionnel, le périphérique redémarre

Source : ZENworks 10 Configuration Management ; Gestion à distance.

Cause possible : Le pilote vidéo n'est pas installé sur le périphérique.

Action : Vous devez installer le pilote vidéo correspondant au système.

Plusieurs instances de la visionneuse de gestion à distance sont lancées sur le périphérique disposant du navigateur Internet Explorer 7

Source : ZENworks 10 Configuration Management ; Gestion à distance.

Cause possible : Si vous lancez une opération de gestion à distance sur un périphérique doté du navigateur Internet Explorer 7, plusieurs instances de la visionneuse sont lancées sur ce périphérique si un logiciel d'accélération du téléchargement tel que FlashGet est installé sur la console de gestion.

Action : Désactivez temporairement les modules complémentaires des accélérateurs de téléchargement :

1. Lancez le navigateur Internet Explorer 7.
2. Cliquez sur *Outils* > *Gérer les modules complémentaires*.
3. Cliquez sur *Activer ou désactiver les modules complémentaires*, puis désactivez le module complémentaire de l'accélérateur de téléchargement.
4. Lancez l'opération de gestion à distance.

Action : Tentez d'utiliser le navigateur Firefox pour effectuer cette opération.

Impossible d'utiliser l'icône Ctrl-Alt-Suppr lors du contrôle à distance d'un périphérique Windows Vista, Windows Server 2008 ou Windows Server 2008 R2

Source : ZENworks 10 Configuration Management ; Gestion à distance.

Explication : Si vous lancez une opération de contrôle à distance sur un périphérique Windows Vista, Windows Server 2008 ou Windows Server 2008 R2 pour lequel le contrôle de compte d'utilisateur (User Account Control, UAC) est désactivé, l'icône *Ctrl-Alt-Suppr* est grisée.

Opération : Activer le contrôle de compte utilisateur (UAC).

Le mode de session par défaut n'est pas sélectionné dans le snap-in de gestion à distance

Source : ZENworks 10 Configuration Management ; Gestion à distance.

Explication : Si vous utilisez Internet Explorer pour ouvrir le Centre de contrôle ZENworks et effectuer une opération de gestion à distance sur un périphérique, le mode de session par défaut n'est pas sélectionné dans le snap-in de gestion à distance. En revanche, si vous ne sélectionnez pas de mode de session, l'opération de gestion à distance est lancée dans le mode de collaboration par défaut et l'opération d'affichage à distance est lancée dans le mode exclusif par défaut.

Action : Sélectionnez le mode de session pour effectuer l'opération distante.

Le lien Installer la visionneuse de gestion à distance reste actif sur un périphérique Windows Vista, Windows 7, Windows Server 2008 ou Windows Server 2008 R2 doté du navigateur Internet Explorer 7

Source : ZENworks 10 Configuration Management ; Gestion à distance.

Explication : Sur un périphérique Windows Vista, Windows 7, Windows Server 2008 ou Windows Server 2008 R2 doté du navigateur Internet Explorer 7, l'installation de la *visionneuse de gestion à distance* peut échouer si le contrôle ActiveX* n'est pas activé.

Action : Procédez de la façon suivante pour activer le contrôle de compte utilisateur (UAC) sur le périphérique Vista :

1. Cliquez sur *Démarrer* > *Paramètres* > *Panneau de configuration* > *Comptes d'utilisateurs* > *Comptes d'utilisateurs* > *Activer ou désactiver le contrôle de compte utilisateur*.
2. Sélectionnez *Utiliser le contrôle des comptes d'utilisateurs pour vous aider à protéger votre ordinateur*.
3. Cliquez sur *OK*.

Action : Si vous ne souhaitez pas activer le contrôle des comptes d'utilisateurs sur le périphérique Windows Vista, vous devez procéder à une mise à niveau vers Windows Vista avec SP1.

L'installation de la visionneuse de gestion à distance risque d'échouer

Source : ZENworks 10 Configuration Management ; Gestion à distance.

Explication : L'installation de la visionneuse de gestion à distance risque d'échouer. Cette erreur est liée à l'infrastructure MSI.

Action : Procédez de l'une des manières suivantes :

- Désinstallez la visionneuse de gestion à distance à l'aide du menu Ajout/suppression de programmes, puis réinstallez-la
- Nettoyez l'application à l'aide de l'utilitaire de nettoyage de Microsoft Windows installer, puis réinstallez-la. Vous pouvez télécharger cet utilitaire depuis le site de support Microsoft (http://support.microsoft.com/kb/290301)

Échec du lancement de la visionneuse de gestion à distance sur un périphérique Windows Vista, Windows 7, Windows Server 2008 ou Windows Server 2008 R2

Source : ZENworks 10 Configuration Management ; Gestion à distance.

Explication : Sur un périphérique Windows Vista, Windows 7, Windows Server 2008 ou Windows Server 2008 R2, la visionneuse de gestion à distance échoue même lorsque l'invite de sécurité aboutit.

Action : Ajoutez le serveur exécutant le Centre de contrôle ZENworks à la liste des sites approuvés et réessayez.

Lorsque vous cliquez sur l'icône Ctrl+Alt+Suppr dans la visionneuse de gestion à distance pendant la session de contrôle à distance, la fenêtre de séquence de touches de sécurité (Secure Attention Sequence - SAS) peut s'afficher sans aucune commande

Source : ZENworks 10 Configuration Management ; Gestion à distance.

Action : Cliquez sur l'icône *Ctrl+Alt+Suppr* de la visionneuse de gestion à distance, puis appuyez sur la touche Échap pour quitter la fenêtre SAS. Cliquez de nouveau sur l'icône *Ctrl+Alt+Suppr* de la visionneuse de gestion à distance.

Le bureau d'un périphérique peut ne pas être visible lorsque vous contrôlez ou affichez ce dernier à distance

Source : ZENworks 10 Configuration Management ; Gestion à distance.

Explication : Si vous contrôlez ou affichez à distance un périphérique sur lequel une session RDP a été exécutée, un écran noir risque de s'afficher au lieu du bureau du périphérique.

Action : Pour afficher le bureau du périphérique :

1. Déverrouillez manuellement le bureau.
2. Réinitialisez une session RDP sur la session de console du périphérique en exécutant la commande suivante :

   ```
   mstsc /console
   ```

Impossible de transférer des fichiers à distance vers des dossiers restreints sur un périphérique Windows Vista, Windows 7, Windows Server 2008 ou Windows Server 2008 R2

Source : ZENworks 10 Configuration Management ; Gestion à distance.

Explication : Si vous lancez une opération de transfert de fichiers afin de transférer à distance des fichiers vers des dossiers restreints sur un périphérique Windows Vista, Windows 7, Windows Server 2008 ou Windows Server 2008 R2 sur lequel le contrôle de compte d'utilisateur est activé, cette opération échoue.

Action : Procédez comme suit afin de désactiver le contrôle de compte d'utilisateur sur le périphérique Windows Vista :

1. Cliquez sur *Démarrer > Paramètres > Panneau de configuration > Comptes d'utilisateurs > Comptes d'utilisateurs > Activer ou désactiver le contrôle de compte utilisateur*.
2. Désélectionnez *Utiliser le contrôle de compte d'utilisateur pour protéger votre ordinateur*.
3. Cliquez sur *OK*.

Action : Procédez comme suit afin de désactiver le contrôle de compte d'utilisateur sur le périphérique Windows 7 :

1. Cliquez sur *Démarrer > Panneau de configuration > Comptes d'utilisateurs > Modifier les paramètres du contrôle de compte d'utilisateur.*
2. Glissez le curseur vers la valeur minimale (vers *Ne jamais avertir*), qui affiche la description Ne jamais m'avertir.
3. Cliquez sur *OK*.
4. Redémarrez le périphérique.

Impossible de lancer une session à distance sur un dispositif SLES (SUSE Linux Enterprise Server) 11 via Mozilla Firefox

Source : ZENworks 10 Configuration Management ; Gestion à distance.

Explication : Le plug-in de gestion à distance pour Firefox est installé dans le répertoire `/usr/lib/firefox`, qui est également le répertoire d'installation par défaut de Firefox. Si vous avez installé Firefox dans un autre répertoire du périphérique SLES 11 et que vous essayez de lancer une session à distance via Firefox sur le périphérique, celle-ci échoue.

Action : Copiez le fichier `nsZenworksPluginSample.so` du répertoire `/usr/lib/firefox/plugins` dans le répertoire de plug-ins de Firefox.

Le lien Mettre à niveau la visionneuse de gestion à distance ne s'affiche pas si vous lancez le Centre de contrôle ZENworks via Internet Explorer 8

Source : ZENworks 10 Configuration Management ; Gestion à distance.

Explication : Si vous procédez à une mise à niveau vers ZENworks Configuration Management avec SP3 depuis ZENworks Configuration Management avec SP2 et que vous lancez le Centre de contrôle ZENworks via Internet Explorer 8, le lien *Mettre à niveau la visionneuse de gestion à distance* ne s'affiche pas dans le Centre de contrôle ZENworks.

Action : Pour afficher le lien *Mettre à niveau la visionneuse de gestion à distance*, procédez comme suit :

1. Lancez le navigateur Internet Explorer 8.
2. Cliquez sur *Outils* > *Options Internet* pour afficher la boîte de dialogue Options Internet.
3. Cliquez sur l'onglet *Sécurité*.
4. Cliquez sur l'option *Personnaliser le niveau*.
5. Vérifiez que les paramètres suivants sont activés :
   - *Exécuter les contrôles ActiveX et les plug-ins*
   - *Contrôles d'initialisation et de script ActiveX non marqués comme sécurisés*
6. Redémarrez le navigateur.

Détails cryptographiques

A

Les sections suivantes contiennent les détails des différents certificats générés lorsque vous utilisez le composant de gestion à distance de Novell® ZENworks® 10 Configuration Management.

A.1 Détails relatifs à la paire de clés du périphérique géré

Certificat généré par : service de gestion à distance
Certificat généré à l'aide de : OpenSSL v0.9.8e (version Novell)
Certificat signé par : signature automatique
Certificate signé à l'aide de : OpenSSL v0.9.8e (version Novell)
Certificat vérifié par : visionneuse de gestion à distance
Certificat vérifié à l'aide de : OpenSSL v0.9.8e (version Novell)
Utilisé par : service de gestion à distance
Utilisé pour : établir une session sécurisée avec la visionneuse de gestion à distance
Type de clé privée : RSA
Puissance de la clé : 1024 bits
Algorithme de signature : RSA-SHA256
Validité : 10 ans

A.2 Détails relatifs à la paire de clés de l'opérateur distant

Ce certificat n'est valide que lorsqu'un CA interne est déployé.

Certificat généré par : serveur ZENworks hébergeant le Centre de contrôle ZENworks
Certificat généré en utilisant : bibliothèque Bouncy Castle (`bcprov-jdk15-134.jar`)
Certificat signé par : serveur ZENworks hébergeant le Centre de contrôle ZENworks
Certificat signé en utilisant : bibliothèque Bouncy Castle (`bcprov-jdk15-134.jar`)
Certificat vérifié par : service de gestion à distance
Certificat vérifié en utilisant : OpenSSL v0.9.8e (version Novell)
Utilisé par : visionneuse de gestion à distance et service de gestion à distance
Utilisé pour : établissement d'une session sécurisée et identification de l'opérateur distant
Type de clé privée : RSA
Force de la clé : 1024 bits
Algorithme de signature : RSA-SHA1
Validité : 4 jours

A.3 Détails du ticket de gestion distante

Ce certificat n'est valide que pour l'authentification des droits.

Ticket généré par : serveur ZENworks hébergeant le Centre de contrôle ZENworks
Ticket généré en utilisant : bibliothèque Bouncy Castle (`bcprov-jdk15-134.jar`)
Certificat signé par : serveur ZENworks hébergeant le Centre de contrôle ZENworks
Ticket signé en utilisant : bibliothèque Bouncy Castle (`bcprov-jdk15-134.jar`)
Certificat vérifié par : service Web de gestion à distance (sur le serveur ZENworks)
Certificat vérifié en utilisant : bibliothèque Bouncy Castle (`bcprov-jdk15-134.jar`)
Utilisé par : visionneuse de gestion à distance et service Web de gestion à distance
Utilisé pour : authentification de l'opérateur distant et vérification des droits pour effectuer une opération
Algorithme de signature : RSA-SHA1
Validité : 2 minutes

A.4 Détails de codage de session

Session établie entre : service de gestion à distance et visionneuse de gestion à distance
Protocole de codage : SSL (TLSv1)
Chiffrement de session : AES256-SHA
Mode d'authentification SSL : mutuel/serveur

Meilleures pratiques

B

Les sections suivantes expliquent les pratiques recommandées lorsque vous utilisez le composant de gestion à distance de Novell® ZENworks® 10 Configuration Management.

B.1 Fermeture du module d'écoute de gestion à distance

Lorsqu'un opérateur distant lance le module d'écoute de gestion à distance pour écouter les demandes de session à distance émises par l'utilisateur du périphérique géré, ZENworks génère un ticket pour permettre à l'opérateur distant de s'authentifier sur le périphérique géré. La durée de vie de ce ticket est de deux jours.

Le module d'écoute de gestion à distance continue son exécution après la déconnexion de l'opérateur distant ou la fermeture du centre de contrôle ZENworks. Si le ticket est encore valide, n'importe quel autre opérateur distant peut utiliser le module d'écoute pour écouter les demandes de session distante des utilisateurs du périphérique géré. Pour des raisons de sécurité, vous devez fermer le module d'écoute de gestion à distance avant de vous déconnecter ou de fermer le navigateur.

Pour fermer le module d'écoute de gestion à distance, cliquez avec le bouton droit sur l'icône *Module d'écoute de ZENworks Remote Management* dans la zone de notification, puis cliquez sur *Fermer le daemon d'écoute*.

B.2 Fermeture des applications lancées lors de l'opération d'exécution à distance

Le module Gestion à distance est exécuté par défaut en tant que service avec des privilèges système sur le périphérique géré. Ainsi, toutes les applications lancées au cours de la session d'exécution à distance s'exécutent également avec des privilèges système. Pour des raisons de sécurité, nous vous recommandons de fermer les applications après utilisation.

B.3 Identification de l'opérateur à distance sur le périphérique géré

Lorsqu'un opérateur à distance lance une session à distance sur un périphérique géré à l'aide du Centre de contrôle ZENworks, un certificat qui permet au périphérique géré d'identifier l'opérateur à distance est généré automatiquement par ZENworks en cas d'utilisation d'une autorité de certification interne. Toutefois, en cas d'utilisation d'une autorité de certification externe, l'opérateur doit fournir manuellement le certificat lié à l'autorité de certification externe déployée et est certifié pour l'authentification du client SSL. Pour plus d'informations sur l'utilisation de l'autorité de certification externe, reportez-vous aux informations concernant le champ *Utiliser la paire de clés suivante pour l'identification* de la Section 2.8, « Démarrage des opérations de gestion à distance », page 35.

Si un opérateur à distance lance une opération à distance sur un périphérique géré sans fournir de certificat, le nom de cet opérateur est enregistré comme *un utilisateur inconnu* dans les journaux d'audit, la boîte de dialogue Signal visible et la boîte de dialogue Demander l'autorisation de l'utilisateur. Pour s'assurer que l'opérateur à distance fournisse le certificat, désélectionnez l'option *Autoriser la connexion lorsque la console de gestion à distance n'a pas de certificat SSL* dans la stratégie de gestion à distance.

B.4 Exécution d'une session de contrôle à distance sur un périphérique qui est déjà connecté à l'aide d'une connexion au bureau distant

Pour contrôler à distance un périphérique qui est déjà connecté à l'aide de la connexion au bureau distant (RDP), vérifiez que l'une des conditions suivantes est remplie :

- La session RDP est en cours sur le périphérique géré
- Le périphérique géré a été déverrouillé manuellement après la fin de la session RDP sur le périphérique.

B.5 Définition du nom de la console de gestion

Si l'option *Afficher le nom DNS de la visionneuse au début de la session à distance* est activée dans la stratégie de gestion à distance, le périphérique géré tente de déterminer le nom de la console de gestion au début d'une session à distance. Cette situation peut entraîner un retard considérable au niveau du lancement de la session à distance si aucune consultation du DNS inversée n'est activée sur le réseau. Pour éviter ce retard, désactivez l'option *Afficher le nom DNS de la visionneuse au début de la session à distance* dans la stratégie.

B.6 Utilisation du thème Aero sur les périphériques Windows Vista, Windows 7, Windows Server 2008 et Windows Server 2008 R2

Afin d'améliorer les performances d'une session à distance, la gestion à distance utilise un pilote de miroir pour détecter les modifications à l'écran. Si le pilote du miroir n'est pas compatible avec le thème Aero du Bureau, une tentative de chargement du pilote de miroir sur un périphérique affichant le thème Aero modifie le thème du Bureau du périphérique sur celui par défaut. Ceci peut affecter l'expérience de l'utilisateur. Il n'est donc pas recommandé d'utiliser le thème Aero sur un périphérique à gérer à distance.

Si vous souhaitez conserver le thème Aero pendant la session à distance du périphérique géré, désactivez le pilote de mise en miroir. Pour désactiver le pilote de mise en miroir, désélectionnez le paramètre *Activer le pilote d'optimisation*. Pour plus d'informations sur le paramètre Activer le pilote d'optimisation, reportez-vous à la section Configuration des paramètres de gestion à distance au niveau de la zone.

Cependant, l'activation du thème Aero sur le périphérique géré risque de nuire aux performances de la session à distance.

B.7 L'activation du bouton Séquence de touches de sécurité (Ctrl+Alt+Suppr) lors du contrôle à distance d'un périphérique Windows Vista ou Windows Server 2008

Pour activer l'icône (Ctrl+Alt+Suppr) dans la barre d'outils de la visionneuse de gestion à distance lors du contrôle à distance d'un périphérique Windows Vista ou Windows Server 2008, veillez à ce que le contrôle de compte utilisateur (UAC) soit activé sur le périphérique géré.

B.8 Installation du service de gestion à distance sur un périphérique Windows XP à l'aide de RDP

Lors de l'installation du service de gestion à distance sur un périphérique géré, ZENworks installe automatiquement un pilote de miroir appelé DFMirage sur le périphérique. Si vous souhaitez installer le service de gestion à distance sur un périphérique Windows XP à l'aide d'une session utilisant la connexion au bureau distant, veillez à ce que le correctif fourni sur le site Web d'assistance de Microsoft (http://support.microsoft.com/kb/952132) soit installé sur le périphérique.

B.9 Performances de la gestion à distance

Les performances de gestion à distance pendant une session à distance sur une liaison lente ou une liaison rapide varient en fonction du trafic sur le réseau. Pour un meilleur temps de réponse, consultez la Section 3.8, « Amélioration des performances de la gestion à distance », page 65.

Mises à jour de la documentation

C

Cette section contient des informations sur les modifications du contenu de la documentation qui ont été apportées dans ce manuel *Référence de ZENworks Remote Management* pour Novell® ZENworks® 10 Configuration Management avec SP3. Ces informations peuvent vous aider à vous tenir au courant des mises à jour apportées à la documentation.

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

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

Les mises à jour suivantes ont été apportées au document :

- Section C.1, « 30 mars 2010 : SP3 (10.3) », page 91

C.1 30 mars 2010 : SP3 (10.3)

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

Emplacement	Modification
« Proxy de gestion à distance » page 12	Mise à jour de la section.
Section 1.3, « Présentation des fonctions de gestion à distance », page 14	Mise à jour de la section.
Section 2.5, « Configuration du mot de passe de gestion à distance », page 31	Mise à jour de la section.
Section 2.9, « Options de lancement d'une opération de gestion à distance », page 45	Section ajoutée.
Section 2.10, « Installation d'un proxy de gestion à distance », page 49	Mise à jour de la section afin d'y ajouter la prise en charge de l'installation d'un proxy de gestion à distance sous Linux.
Section 2.11, « Configuration d'un proxy de gestion à distance », page 51	Section ajoutée.
Section 3.7, « Activation d'un périphérique distant », page 64	Mise à jour de la section afin d'y ajouter des informations sur la sortie de veille d'un périphérique doté de plusieurs cartes d'interface réseau.
Section 3.6, « Administration d'une session de proxy de gestion à distance », page 63	Section ajoutée.

Emplacement	Modification
Chapitre 5, « Dépannage », page 75	Ajout des scénarios suivants : ◆ « Impossible de lancer une session à distance sur un dispositif SLES (SUSE Linux Enterprise Server) 11 via Mozilla Firefox » page 82 ◆ « Le lien Mettre à niveau la visionneuse de gestion à distance ne s'affiche pas si vous lancez le Centre de contrôle ZENworks via Internet Explorer 8 » page 83
Chapitre 5, « Dépannage », page 75	Le scénario suivant a été ajouté : Impossible de transférer des fichiers à distance vers des dossiers restreints sur un périphérique Windows Vista ou Windows 7
Section B.6, « Utilisation du thème Aero sur les périphériques Windows Vista, Windows 7, Windows Server 2008 et Windows Server 2008 R2 », page 89	Mise à jour de la section.