

**Référence de la gestion à distance**

# **Novell® ZENworks® 10 Configuration Management SP2**

**10.2**

27 mai 2009

[www.novell.com](http://www.novell.com)



## Mentions légales

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

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

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

Copyright © 2007 - 2009 Novell, Inc. Tous droits réservés. Cette publication ne peut être reproduite, photocopiée, stockée sur un système de recherche documentaire ou transmise, même en partie, sans le consentement écrit explicite préalable de l'éditeur.

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

Novell, Inc.  
404 Wyman Street, Suite 500  
Waltham, MA 02451  
États-Unis  
[www.novell.com](http://www.novell.com)

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

<b>À propos de ce guide</b>	<b>9</b>
<b>1 Présentation</b>	<b>11</b>
1.1 Terminologie de la gestion à distance	11
1.2 Présentation des opérations de gestion à distance	12
1.2.1 Contrôle à distance	13
1.2.2 Affichage à distance	13
1.2.3 Exécution à distance	13
1.2.4 Diagnostic à distance	13
1.2.5 Transfert de fichier	13
1.2.6 Activation à distance	14
1.3 Présentation des fonctions de gestion à distance	14
1.3.1 Signal visible	14
1.3.2 Détection d'intrus	15
1.3.3 Codage de session	15
1.3.4 Bip sonore	15
1.3.5 Verrouillage du clavier et de la souris	15
1.3.6 Suppression du contenu de l'écran	15
1.3.7 Fin anormale	15
1.3.8 Remplacement de l'écran de veille	15
1.3.9 Fin automatique de la session	15
1.3.10 Connexion initiée par l'agent	16
1.3.11 Collaboration de session	16
1.3.12 Audit de gestion à distance	16
1.4 Présentation du proxy de gestion à distance	16
<b>2 Installation de la gestion à distance</b>	<b>17</b>
2.1 Configuration des paramètres de gestion à distance	17
2.1.1 Configuration des paramètres de gestion à distance au niveau de la zone	17
2.1.2 Configuration des paramètres de gestion à distance au niveau du dossier	20
2.1.3 Configuration des paramètres de gestion à distance au niveau du périphérique	20
2.2 Activation du module d'écoute de gestion à distance	21
2.3 Création de la stratégie de gestion à distance	21
2.4 Configuration des droits de gestion à distance	29
2.5 Configuration du mot de passe de gestion à distance	29
2.5.1 Configuration du mot de passe de gestion à distance à l'aide du Centre de contrôle ZENworks	30
2.5.2 Configuration du mot de passe de gestion à distance à l'aide de l'agent adaptatif ZENworks	30
2.5.3 Effacement du mot de passe de gestion à distance à l'aide du Centre de contrôle ZENworks	31
2.5.4 Effacement du mot de passe de gestion à distance à l'aide de l'agent adaptatif ZENworks	31
2.6 Installation de la visionneuse de gestion à distance	32
2.7 Mise à niveau de la visionneuse de gestion à distance	33
2.8 Démarrage des opérations de gestion à distance	33
2.8.1 Lancement d'une session à partir de la console de gestion	33
2.8.2 Lancement d'une session à partir du périphérique géré	46
2.9 Installation d'un proxy de gestion à distance	47

<b>3</b>	<b>Gestion des sessions distantes</b>	<b>49</b>
3.1	Gestion d'une session d'affichage à distance	49
3.1.1	Utilisation des options de la barre d'outils de la visionneuse de gestion à distance	49
3.1.2	Collaboration de session	51
3.2	Gestion d'une session d'affichage à distance	53
3.3	Gestion d'une session d'exécution à distance	54
3.4	Gestion d'une session de diagnostics à distance	54
3.5	Gestion d'une session de transfert de fichiers	56
3.6	Sortie de veille d'un périphérique distant	59
3.6.1	Conditions préalables	59
3.6.2	Activation à distance des périphériques gérés	59
3.7	Amélioration des performances de la gestion à distance	60
3.7.1	Sur la console de gestion	60
3.7.2	Sur le périphérique géré	60
<b>4</b>	<b>Sécurité</b>	<b>61</b>
4.1	Authentification	61
4.1.1	Authentification de la gestion à distance basée sur les droits	61
4.1.2	Authentification de la gestion à distance basée sur les mots de passe	62
4.2	Force des mots de passe	63
4.3	Ports	63
4.4	Audit	63
4.5	Demander l'autorisation de l'utilisateur du périphérique géré	64
4.6	Fin anormale	64
4.7	Détection d'intrus	65
4.7.1	Déblocage automatique du service de gestion à distance	65
4.7.2	Déblocage manuel du service de gestion à distance	65
4.8	Identification de l'opérateur à distance	65
4.9	Configuration du navigateur	66
4.10	Sécurité de la session	66
4.10.1	Reconnaissance mutuelle SSL	66
4.10.2	Régénération du certificat	67
<b>5</b>	<b>Dépannage</b>	<b>69</b>
<b>A</b>	<b>Détails cryptographiques</b>	<b>75</b>
A.1	Détails de paire de clés du périphérique géré	75
A.2	Détails de paire de clés de l'opérateur distant	75
A.3	Détails du ticket de gestion distante	76
A.4	Détails de codage de session	76
<b>B</b>	<b>Meilleures pratiques</b>	<b>77</b>
B.1	Fermeture du module d'écoute de gestion à distance	77
B.2	Fermeture des applications lancées lors de l'opération d'exécution à distance	77
B.3	Identification de l'opérateur à distance sur le périphérique géré	78
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	78
B.5	Définition du nom de la console de gestion	78
B.6	Utilisation d'un thème Aero sur les périphériques Windows Vista et Windows Server 2008	78

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. . . . .	79
B.8	Installation du service de gestion à distance sur un périphérique Windows XP à l'aide de RDP . . . . .	79
B.9	Performances de la gestion à distance . . . . .	79
<b>C</b>	<b>Mises à jour de la documentation</b>	<b>81</b>
C.1	Le 27 mai 2009 : SP2 (10.2) . . . . .	81
C.1.1	Présentation. . . . .	81
C.1.2	Installation de la gestion à distance. . . . .	81
C.1.3	Sécurité . . . . .	82





# À propos de ce guide

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

- ♦ Chapitre 1, « Présentation », page 11
- ♦ Chapitre 2, « Installation de la gestion à distance », page 17
- ♦ Chapitre 3, « Gestion des sessions distantes », page 49
- ♦ Chapitre 4, « Sécurité », page 61
- ♦ Chapitre 5, « Dépannage », page 69
- ♦ Annexe A, « Détails cryptographiques », page 75
- ♦ Annexe B, « Meilleures pratiques », page 77
- ♦ Annexe C, « Mises à jour de la documentation », page 81

## 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) (<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 oeuvre de ce produit. Pour obtenir de la documentation supplémentaire, consultez le [site Web de documentation de ZENworks 10 Configuration Management SP2](http://www.novell.com/documentation/zcm10/) (<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.



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 :

- ♦ [Section 1.1, « Terminologie de la gestion à distance », page 11](#)
- ♦ [Section 1.2, « Présentation des opérations de gestion à distance », page 12](#)
- ♦ [Section 1.3, « Présentation des fonctions de gestion à distance », page 14](#)
- ♦ [Section 1.4, « Présentation du proxy de gestion à distance », page 16](#)

## 1.1 Terminologie de la gestion à distance

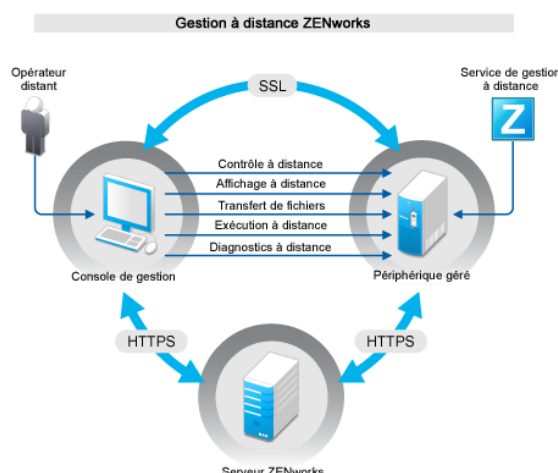
Termes	Description
Périphérique géré	Périphérique que vous souhaitez gérer à distance. Pour gérer un périphérique à distance, assurez-vous que le composant Gestion à distance est installé et que le service de gestion à distance est exécuté sur ce périphérique.
Serveur de gestion	Périphérique sur lequel 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). Le proxy doit être installé au préalable sur un périphérique géré Windows.

## 1.2 Présentation des opérations de gestion à distance

La gestion à distance permet aux administrateurs de contrôler un périphérique sans devoir se déplacer sur le site correspondant. Elle peut vous permettre, ainsi qu'à votre organisation, de gagner du temps et de faire des économies. 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](#)
- ♦ [Section 1.2.4, « Diagnostic à distance », page 13](#)
- ♦ [Section 1.2.5, « Transfert de fichier », page 13](#)
- ♦ [Section 1.2.6, « Activation à distance », page 14](#)

## 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 cette connexion, 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 49](#).

## 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 53](#).

## 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 54](#).

## 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 restant 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 diagnostics à distance », page 54](#).

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 sur le 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 des dossiers ;
- ♦ supprimer des fichiers ou des 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 56](#)

---

**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 nœuds mis hors tension sur votre réseau, à condition que leur carte réseau soit compatible avec le service Wake-on-LAN. Pour plus d'informations, reportez-vous à la [Section 3.6, « Sortie de veille d'un périphérique distant », page 59](#)

# 1.3 Présentation des fonctions de gestion à distance

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

- ♦ [Section 1.3.1, « Signal visible », page 14](#)
- ♦ [Section 1.3.2, « Détection d'intrus », page 15](#)
- ♦ [Section 1.3.3, « Codage de session », page 15](#)
- ♦ [Section 1.3.4, « Bip sonore », page 15](#)
- ♦ [Section 1.3.5, « Verrouillage du clavier et de la souris », page 15](#)
- ♦ [Section 1.3.6, « Suppression du contenu de l'écran », page 15](#)
- ♦ [Section 1.3.7, « Fin anormale », page 15](#)
- ♦ [Section 1.3.8, « Remplacement de l'écran de veille », page 15](#)
- ♦ [Section 1.3.9, « Fin automatique de la session », page 15](#)
- ♦ [Section 1.3.10, « Connexion initiée par l'agent », page 16](#)
- ♦ [Section 1.3.11, « Collaboration de session », page 16](#)
- ♦ [Section 1.3.12, « Audit de gestion à distance », page 16](#)

## 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 Détection d'intrus réduit de façon significative le risque de piratage du périphérique géré. Si l'opérateur distant n'est pas parvenu à se loguer au périphérique géré après un nombre défini de tentatives (5 par défaut), le service de gestion à distance est bloqué et n'accepte aucune requête de session distante tant qu'il n'a pas été débloqué.

### 1.3.3 Codage de session

Les sessions distantes sont sécurisées en SSL (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

Cette fonction permet de verrouiller les commandes du clavier et de la souris du périphérique géré au cours d'une session distante pour éviter que son utilisateur n'interrompe la session.

### 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.

### 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 mot de passe sur le périphérique géré au cours d'une session distante.

---

**Remarque :** cette fonction n'est pas disponible sur les périphériques gérés Windows Vista\*.

---

### 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 46](#).

---

**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 conjointement 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 51](#).

### 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, le fonctionnement à distance du périphérique doit être routé à l'aide d'un proxy de gestion à distance. Vous devez installer le proxy sur un périphérique généralement placé dans une zone démilitarisée. Vous devez pouvoir accéder à ce périphérique depuis le réseau public possédant la console de gestion, ainsi qu'aux périphériques qui se trouvent sur un réseau privé et qui doivent être gérés à distance. Pour plus d'informations sur l'installation du proxy de gestion à distance, consultez la [Section 2.9, « Installation d'un proxy de gestion à distance », page 47](#).

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



# Installation de la gestion à distance

# 2

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

- Section 2.1, « Configuration des paramètres de gestion à distance », page 17
- Section 2.2, « Activation du module d'écoute de gestion à distance », page 21
- Section 2.3, « Création de la stratégie de gestion à distance », page 21
- Section 2.4, « Configuration des droits de gestion à distance », page 29
- Section 2.5, « Configuration du mot de passe de gestion à distance », page 29
- Section 2.6, « Installation de la visionneuse de gestion à distance », page 32
- Section 2.7, « Mise à niveau de la visionneuse de gestion à distance », page 33
- Section 2.8, « Démarrage des opérations de gestion à distance », page 33
- Section 2.9, « Installation d'un proxy de gestion à distance », page 47

## 2.1 Configuration des paramètres de gestion à distance

Les paramètres de gestion à distance constituent des règles déterminant le comportement ou l'exécution du service de gestion à distance sur le périphérique géré. Ces paramètres incluent la configuration des ports, les paramètres de session et les paramètres de performances au cours de la session distante. 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 :

- Section 2.1.1, « Configuration des paramètres de gestion à distance au niveau de la zone », page 17
- Section 2.1.2, « Configuration des paramètres de gestion à distance au niveau du dossier », page 20
- Section 2.1.3, « Configuration des paramètres de gestion à distance au niveau du périphérique », page 20

### 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 *Rechercher le nom DNS de la visionneuse au début de la session distante* pour permettre au service de gestion à distance de rechercher le nom DNS de la console de gestion au début de la session à distance.

Le nom est enregistré dans les journaux d'audit et affiché avec les informations de session des sessions à distance. Si cette option n'est pas sélectionnée ou si le service de gestion à distance ne trouve pas le nom de la console, ce dernier est affiché en tant qu'*inconnu*.

Si la consultation du DNS inversée n'est pas activée sur votre réseau, nous vous conseillons de désactiver ce paramètre pour éviter tout retard significatif du lancement de la session distante.

5 Sélectionnez parmi les options suivantes celles qui permettront d'améliorer les performances des sessions distantes :

Champ	Détails
<i>Supprimer le papier peint</i>	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.
<i>Activer le pilote d'optimisation</i>	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 2.9, « Installation d'un proxy de gestion à distance », page 47](#).

Tâche	Détails
Ajouter un proxy de gestion à distance	<ol style="list-style-type: none"> <li>1. Cliquez sur <i>Ajouter</i> pour afficher la boîte de dialogue Ajouter des paramètres de proxy.</li> <li>2. Renseignez les champs suivants : <p><b>Proxy</b> : indiquez l'adresse IP ou le nom DNS du proxy de gestion à distance.</p> <p><b>Plage d'adresses IP</b> : 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 :</p> <ul style="list-style-type: none"> <li>♦ 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 : <p>123.45.678.12/16 : spécifie toutes les adresses IP qui commencent par 123.45.</p> <p>123.45.678.12/24 : spécifie toutes les adresses IP qui commencent par 123.45.678.</p> </li> <li>♦ Spécifiez la plage d'adresses IP au format suivant : <b>première adresse IP - dernière adresse IP</b>. Exemple : <p>123.45.678.12 - 123.45.678.15 : spécifie toutes les adresses IP comprises entre 123.45.678.12 et 123.45.678.15.</p> </li> </ul> </li> </ol>
Supprimer un proxy de gestion à distance	<ol style="list-style-type: none"> <li>1. Sélectionnez le proxy à supprimer.</li> <li>2. Cliquez sur Supprimer, puis sur <i>OK</i>.</li> </ol>

**7** (Facultatif) Configurez l'application à exécuter sur le périphérique géré au cours de 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 sur le système
- ♦ Gestion de l'ordinateur
- ♦ Services
- ♦ Éditeur de registre

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

Tâche	Détails
Ajouter une application	<ol style="list-style-type: none"> <li>1. Cliquez sur <i>Ajouter</i>.</li> <li>2. Indiquez le nom de l'application et le chemin de l'application sur le périphérique géré.</li> <li>3. Cliquez sur OK.</li> </ol>
Supprimer une application	<ol style="list-style-type: none"> <li>1. Sélectionnez l'application que vous souhaitez supprimer.</li> <li>2. Cliquez sur Supprimer, puis sur OK.</li> </ol>
Rétablir les applications par défaut	<ol style="list-style-type: none"> <li>1. Cliquez sur <i>Rétablir</i>, puis sur OK.</li> </ol>

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. Toutefois, vous pouvez modifier ces paramètres pour les périphériques situés dans un dossier :

- 1 Dans le Centre de contrôle ZENworks, cliquez sur *Périphériques*.
- 2 Cliquez sur le dossier (détails) dont vous souhaitez configurer les paramètres de gestion à distance.
- 3 Cliquez sur *Paramètres*, puis sur *Gestion des périphériques > Gestion à distance*.
- 4 Cliquez sur *Remplacer*.
- 5 Modifiez les paramètres de gestion à distance, selon vos besoins.
- 6 Pour appliquer les modifications, 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. Toutefois, vous pouvez modifier ces paramètres pour le périphérique géré :

- 1 Dans le Centre de contrôle ZENworks, cliquez sur *Périphériques*.
- 2 Cliquez sur *Serveurs* ou sur *Postes de travail* pour afficher la liste des périphériques gérés.
- 3 Cliquez sur le périphérique dont vous souhaitez configurer les paramètres de gestion à distance.
- 4 Cliquez sur *Paramètres*, puis sur *Gestion des périphériques > Gestion à distance*.

- 5 Cliquez sur *Remplacer*.
- 6 Modifiez les paramètres de gestion à distance, selon vos besoins.
- 7 Pour appliquer les modifications, 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 le 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 gestion à distance de ZENworks 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 d'une session de gestion à distance sur le périphérique géré. La stratégie comprend les paramètres des opérations de gestion à distance, comme le contrôle à distance, l'affichage à distance, l'exécution à distance, le diagnostic à distance et le transfert de fichiers 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 l'agent adaptatif ZENworks 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 la stratégie. Le nom de la stratégie doit être différent de celui des autres éléments quel qu'ils soient (groupe, dossier, etc.) se trouvant dans le même dossier.

**Dossier :** saisissez le nom ou recherchez le dossier du Centre de contrôle ZENworks dans lequel la stratégie doit résider. Le dossier 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 de résumé de la stratégie du Centre de contrôle ZENworks.

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

Champ	Détails
<i>Permettre à l'utilisateur de demander une session à distance</i>	Permet à l'utilisateur du périphérique géré de demander à un opérateur distant de réaliser une session distante. L'opérateur distant doit s'assurer que le module d'écoute de gestion à distance est en cours d'exécution.
<i>Mettre fin à la session à distance lorsqu'une autorisation est requise de la part d'un nouvel utilisateur se connectant au périphérique géré</i>	Met fin à une session distante en cours lorsqu'un nouvel utilisateur qui s'est identifié sur un périphérique géré à distance doit fournir une autorisation.
<i>Afficher les informations de vérification de la session à distance pour l'utilisateur sur le périphérique géré</i>	Permet à l'utilisateur du périphérique géré de se reporter aux informations d'audit pour les sessions distantes depuis l'icône ZENworks.
<i>Afficher les propriétés de la gestion à distance dans l'icône ZENworks</i>	Permet à l'utilisateur du périphérique géré d'afficher les propriétés associées à la stratégie de gestion à distance dans l'icône ZENworks.
<i>Modifier</i>	Pour modifier le message affiché pour l'utilisateur sur le périphérique géré avant de lancer une session à distance, procédez comme suit : <ol style="list-style-type: none"> <li>1. Cliquez sur <i>Modifier</i> pour afficher la boîte de dialogue Modifier un message.</li> <li>2. Modifiez le message.</li> <li>3. Cliquez sur <i>OK</i>.</li> </ol>
<i>Restaurer les valeurs par défaut</i>	Pour restaurer le message par défaut : <ol style="list-style-type: none"> <li>1. Cliquez sur <i>Restaurer les valeurs par défaut</i> pour restaurer le message par défaut.</li> </ol>

Champ	Détails
<i>Ajouter un module d'écoute à distance</i>	Pour ajouter un module d'écoute à distance : <ol style="list-style-type: none"> <li>1. Cliquez sur <i>Ajouter</i>.</li> <li>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.</li> <li>3. Cliquez sur <i>OK</i>.</li> </ol>
<i>Supprimer un module d'écoute à distance</i>	Pour supprimer un module d'écoute à distance : <ol style="list-style-type: none"> <li>1. Sélectionnez le module d'écoute à distance à effacer.</li> <li>2. Cliquez sur <i>Retirer</i>.</li> </ol>

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

Champ	Détails
<i>Autoriser le contrôle à distance du périphérique géré</i>	Permet des sessions de contrôle à distance sur le périphérique géré. Cette option active les autres options de la page. Désélectionnez l'option pour désactiver l'opération de contrôle à distance sur le périphérique.
<i>Demander l'autorisation de l'utilisateur du périphérique géré avant de démarrer le contrôle à distance</i>	Permet de demander l'autorisation de l'utilisateur sur le périphérique géré avant de démarrer une session de contrôle à distance.
<i>Émettre un signal visible à l'utilisateur sur le périphérique géré au cours du contrôle à distance</i>	Affiche un signal visible en haut à droite du bureau du périphérique géré pendant 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.
<i>Émettre un bip sonore pour l'utilisateur sur le périphérique géré toutes les [ ] secondes au cours du contrôle à distance</i>	Génère un signal sonore sur le périphérique géré lors d'une session de contrôle à distance. Le signal sonore est généré périodiquement lorsque le nombre de secondes spécifié est écoulé.
<i>Autoriser la mise en veille de l'écran du périphérique géré lors du contrôle à distance</i>	Permet de mettre en veille l'écran du périphérique géré pendant une session de contrôle à distance. Cette option verrouille également le clavier et la souris du périphérique géré.
<i>Autoriser le verrouillage de la souris et du clavier du périphérique géré lors du contrôle à distance</i>	Permet de verrouiller la souris et le clavier du périphérique géré lors d'une session de contrôle à distance.
<i>Autoriser le déverrouillage automatique de la mise en veille de l'écran lors du contrôle à distance</i>	Permet de déverrouiller un écran de veille protégé par mot de passe depuis la visionneuse du contrôle à distance avant le début d'une session de contrôle à distance sur le périphérique géré.

Champ	Détails
<i>Terminer automatiquement la session de contrôle à distance après un délai d'inactivité de [ ] minutes</i>	Met fin à une session de contrôle à distance sur le périphérique géré s'il a été inactif pendant la durée spécifiée.

- 6 Cliquez sur *Suivant* pour afficher la page des paramètres d'affichage à distance. Passez à l'étape suivante pour accepter les paramètres par défaut ou utilisez les informations du tableau suivant pour modifier les paramètres par défaut.

Champ	Détails
<i>Autoriser la visualisation à distance du périphérique géré</i>	Permet des sessions d'affichage à distance sur le périphérique géré. Cette option active les autres options de la page. Désélectionnez l'option pour désactiver l'opération d'affichage à distance sur le périphérique.
<i>Demander l'autorisation de l'utilisateur du périphérique géré avant de démarrer la visualisation à distance</i>	Permet de demander l'autorisation à l'utilisateur sur le périphérique géré avant de lancer une session d'affichage à distance.
<i>Émettre un signal visible pour l'utilisateur du périphérique géré au cours de la visualisation à distance</i>	Affiche un signal visible en haut à droite du bureau du périphérique géré pendant la session de contrôle à distance. Le signal visible permet à l'utilisateur du périphérique géré de savoir qu'une session d'affichage à distance est en cours.
<i>Émettre un bip sonore pour l'utilisateur du périphérique géré toutes les [ ] secondes au cours de la visualisation à distance</i>	Génère un son sur le périphérique géré pendant la 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 des paramètres du diagnostic à distance. Passez à l'étape suivante pour accepter les paramètres par défaut ou utilisez les informations du tableau suivant pour modifier les paramètres par défaut.

Champ	Détails
<i>Autoriser le diagnostic à distance du périphérique géré</i>	Autorise les sessions de diagnostic à distance sur le périphérique géré. Cette option active les autres options de la page. Désélectionnez l'option pour désactiver l'opération de diagnostic à distance sur le périphérique.
<i>Demander l'autorisation de l'utilisateur du périphérique géré avant de démarrer le contrôle à distance</i>	Garantit que l'opérateur à distance demande l'autorisation à l'utilisateur du périphérique géré avant de démarrer une session de transfert de fichiers.
<i>Émettre un signal visible pour l'utilisateur du périphérique géré au cours des diagnostics à distance</i>	Affiche un signal visible en haut à droite du bureau du périphérique géré pendant la session de contrôle à distance. Le signal visible permet à l'utilisateur du périphérique géré de savoir qu'une session de diagnostic à distance est en cours.



Champ	Détails
<i>Émettre un bip sonore pour l'utilisateur sur le périphérique géré toutes les [ ] secondes au cours des diagnostics à distance</i>	Émet un son sur le périphérique géré pendant la session de diagnostic à distance. Le signal sonore est généré périodiquement lorsque le nombre de secondes spécifié est écoulé.
<i>Autoriser la mise en veille de l'écran du périphérique géré lors des diagnostics à distance</i>	Permet de mettre en veille l'écran du périphérique géré pendant 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.
<i>Afficher un message d'avertissement avant le redémarrage pendant [ ] secondes</i>	Affiche un message d'avertissement sur le périphérique géré au début de la session de diagnostic à distance, pour rappeler 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 à distance est susceptible d'effectuer un redémarrage du système au cours de la session de diagnostic à distance.
<i>Terminer automatiquement la session de diagnostic à distance après un délai d'inactivité de [ ] minutes</i>	Met fin à la session de diagnostic à distance si elle est inactive pendant la durée indiquée.

- 8 Cliquez sur *Suivant* pour afficher la page Paramètres d'exécution à distance. Passez à l'étape suivante pour accepter les paramètres par défaut ou utilisez les informations du tableau suivant pour modifier les paramètres par défaut.

Champ	Détails
<i>Autoriser l'exécution à distance des programmes sur le périphérique géré</i>	Permet d'exécuter les programmes à distance sur le périphérique géré. Cette option active les autres options de la page. Désélectionnez l'option pour désactiver l'opération d'exécution à distance sur le périphérique.
<i>Demander l'autorisation de l'utilisateur du périphérique géré avant de démarrer l'exécution à distance</i>	Garantit que l'opérateur à distance demande l'autorisation à l'utilisateur du périphérique géré pour démarrer une session d'exécution à distance.
<i>Émettre un signal visible pour l'utilisateur sur le périphérique géré au cours de l'exécution à distance</i>	Affiche un signal visible en haut à droite du bureau du périphérique géré pendant la session de contrôle à distance. Le signal visible permet à l'utilisateur du périphérique géré de savoir qu'une session d'exécution à distance est en cours.
<i>Terminer automatiquement la session de diagnostic à distance après un délai d'inactivité de [ ] minutes</i>	Met fin à la session d'exécution à distance si elle est inactive pendant la durée spécifiée.

- 9 Cliquez sur *Suivant* pour afficher la page Paramètres du transfert de fichiers. 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
<i>Autoriser le transfert de fichiers sur un périphérique géré</i>	Permet le transfert de fichiers entre la console de gestion et le périphérique géré. Cette option active les autres options de la page. Désélectionnez l'option pour désactiver l'opération de transfert de fichiers sur le périphérique.
<i>Demander l'autorisation de l'utilisateur du périphérique géré avant de démarrer le transfert de fichiers</i>	Garantit que l'opérateur à distance demande l'autorisation à l'utilisateur du périphérique géré avant de démarrer une session de transfert de fichiers.
<i>Émettre un signal visible à l'utilisateur sur le périphérique géré au cours du transfert de fichiers</i>	Affiche un signal visible dans le coin supérieur droit du bureau du périphérique géré pendant 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.
<i>Autoriser le téléchargement des fichiers à partir d'un périphérique géré</i>	Permet à un opérateur à distance d'ouvrir des fichiers sur le périphérique géré et de les transférer sur la console de gestion. Si cette option n'est pas sélectionnée, l'opérateur à distance ne peut transférer des fichiers que depuis la console de gestion vers le périphérique géré.
<i>Répertoire racine du transfert de fichiers</i>	Indiquez le répertoire du périphérique géré que l'opérateur doit afficher au cours d'une session de transfert de fichier. L'opérateur à distance ne peut transférer des fichiers qu'à partir de ce répertoire et ses sous-répertoires et à destination de ceux-ci. Le répertoire par défaut est Poste de travail, ce qui signifie que l'opérateur à distance 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
<i>Activer l'authentification par mot de passe</i>	Permet à l'opérateur à distance d'utiliser un mot de passe pour s'authentifier sur le périphérique géré. Cette option permet de configurer le type du mot de passe.
<i>Longueur minimum du mot de passe</i>	Permet de préciser la longueur minimale du mot de passe. Elle est, par défaut, de 6 caractères.
<i>Mot de passe de la session</i>	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 car le mot de passe n'est pas stocké sur le périphérique géré et n'est valide que pour la session en cours.

Champ	Détails
<i>Mot de passe persistant</i>	<p>Sélectionnez cette option pour définir les mots de passe ZENworks et VNC. Il est recommandé de sélectionner le mot de passe ZENworks car il est plus sûr et plus sécurisé que le mot de passe VNC. Ce mot de passe peut être défini par l'administrateur grâce à la stratégie de gestion à distance ou par l'utilisateur du périphérique géré à partir de l'icône ZENworks. La sélection de cette option active les options qui en découlent.</p> <p>Pour permettre à l'utilisateur de définir le mot de passe via l'icône ZENworks, choisissez l'option <i>Autoriser l'utilisateur à remplacer les mots de passe par défaut sur le périphérique géré</i>.</p>
<i>Mot de passe ZENworks</i>	<p>Pour effacer le mot de passe ZENworks :</p> <ol style="list-style-type: none"> <li>1. Cliquez sur <i>Effacer le mot de passe</i>.</li> <li>2. Cliquez sur <i>Appliquer</i>, puis sur <i>OK</i>.</li> </ol> <p>Pour définir le mot de passe ZENworks :</p> <ol style="list-style-type: none"> <li>1. Cliquez sur <i>Définir le mot de passe</i>.</li> <li>2. Entrez le mot de passe. La longueur maximale des mots de passe est de 255 caractères.</li> <li>3. Cliquez sur <i>Appliquer</i>, puis sur <i>OK</i>.</li> </ol>
<i>Mot de passe VNC</i>	<p>Pour effacer le mot de passe VNC :</p> <ol style="list-style-type: none"> <li>1. Cliquez sur <i>Effacer le mot de passe</i>.</li> <li>2. Cliquez sur <i>Appliquer</i>, puis sur <i>OK</i>.</li> </ol> <p>Pour définir le mot de passe VNC :</p> <ol style="list-style-type: none"> <li>1. Cliquez sur <i>Définir le mot de passe</i>.</li> <li>2. Entrez le mot de passe. La longueur maximale des mots de passe est de 8 caractères.</li> <li>3. Cliquez sur <i>Appliquer</i>, puis sur <i>OK</i>.</li> </ol>

## Détection d'intrus

Champ	Détails
<i>Activer la détection d'intrusion</i>	Sélectionnez cette option pour autoriser la détection des tentatives non valides ou non autorisées de lancer une session à distance sur le périphérique géré. Cette option active les autres options de la section Détection d'intrus.
<i>Suspendre l'acceptation des connexions après [ ] tentatives successives non valides</i>	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.

Champ	Détails
<i>Commencer à accepter automatiquement les connexions après [ ] minutes</i>	Indiquez le délai en minutes à l'issue duquel l'agent de gestion à distance accepte automatiquement une connexion au périphérique géré. Pour débloquent manuellement le service de gestion à distance, double-cliquez sur l'icône de l'agent adaptatif ZENworks, cliquez sur <i>Paramètres de sécurité</i> , puis sur <i>Autoriser l'acceptation des connexions si blocage en cours pour détection d'intrusion</i> . Par défaut, il est de 10 minutes.

## Sécurité de la session

Champ	Détails
<i>Activer le codage de session</i>	Active le codage SSL de la session (protocole TLSv1). Cette option active les autres options de la section Sécurité de la session.
<i>Autoriser la connexion lorsque la console de gestion à distance n'a pas de certificat SSL</i>	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.
<i>Autoriser jusqu'à [ ] niveaux dans la chaîne de certificat de la visionneuse</i>	<p>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.</p> <p>Cette propriété définit le nombre maximal de niveaux autorisés dans la chaîne de certificats de la visionneuse. Lorsque l'autorité interne de certificat 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.</p>

## Fin anormale

Champ	Détails
<i>Verrouiller le périphérique</i>	Verrouille le périphérique géré en cas de fin anormale de la session distance.
<i>Déloguer l'utilisateur</i>	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 sélectionnez *Définir des propriétés supplémentaires* pour préciser d'autres informations, comme l'assignation de stratégies, l'application, l'état et le groupe dont la stratégie est membre.

## 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 disposer de droits spécifiques pour un périphérique et de droits spécifiques pour un utilisateur.

- 1 Dans le Centre de contrôle ZENworks, cliquez sur *Configuration*.
- 2 Dans le panneau Administrateurs, cliquez sur le nom de l'administrateur auquel vous souhaitez assigner les droits de gestion à distance.
- 3 Dans le panneau Droits assignés, cliquez sur *Ajouter*, puis sur *Droits de gestion à distance* pour afficher la boîte de dialogue Droits de gestion à distance.
- 4 Sélectionnez le périphérique ou l'utilisateur auquel assigner les droits.

Le tableau ci-dessous fournit des informations sur les droits de gestion à distance :

Droits de gestion à distance	Détails
Contrôle à distance	Assignez à l'opérateur distant les droits lui permettant de contrôler des périphériques à distance.
Affichage à distance	Assignez à l'opérateur distant les droits lui permettant d'afficher des périphériques à distance.
Diagnostic à distance	Assignez à l'opérateur distant les droits lui permettant de diagnostiquer des périphériques à distance.
Exécution à distance	Assignez à l'opérateur distant les droits lui permettant d'exécuter des applications sur des périphériques à distance.
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 débloquent 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 fournissent des informations sur la configuration du 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 30](#)
- ♦ [Section 2.5.2, « Configuration du mot de passe de gestion à distance à l'aide de l'agent adaptatif ZENworks », page 30](#)

- [Section 2.5.3, « Effacement du mot de passe de gestion à distance à l'aide du Centre de contrôle ZENworks », page 31](#)
- [Section 2.5.4, « Effacement du mot de passe de gestion à distance à l'aide de l'agent adaptatif ZENworks », page 31](#)

## 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 21](#) ».

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 l'agent adaptatif ZENworks

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 les mots de passe par défaut sur le périphérique géré* est activée dans la stratégie de gestion à distance effective sur le périphérique géré. Ce mot de passe a priorité sur celui défini dans la stratégie de gestion à distance.

Pour définir un mot de passe sur le périphérique géré :

- 1 Double-cliquez sur l'icône *Agent adaptatif ZENworks* pour ouvrir la fenêtre Agent adaptatif ZENworks.

- 2 Dans le volet gauche, recherchez *Gestion à distance*, puis cliquez sur *Sécurité*.
- 3 Dans le volet droit, cliquez sur *Définir le mot de passe* pour définir 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 dans le cadre de l'interopérabilité avec les visionneuses 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 :

- 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 Augmentez la version de cette stratégie dans la page Résumé ou dans les Tâches communes pour mettre à jour les modifications apportées à la stratégie sur le périphérique géré.

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

- 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 Augmentez la version de cette stratégie dans la page Résumé ou dans les Tâches communes pour mettre à jour les modifications apportées à la stratégie sur le périphérique géré.

### 2.5.4 Effacement du mot de passe de gestion à distance à l'aide de l'agent adaptatif ZENworks

L'utilisateur du périphérique géré peut réinitialiser le mot de passe de gestion à distance qu'il a défini précédemment.

- 1 Double-cliquez sur l'icône *Agent adaptatif ZENworks* pour ouvrir la fenêtre Agent adaptatif ZENworks.
- 2 Dans le volet gauche, recherchez *Gestion à distance*, puis cliquez sur *Sécurité*.
- 3 Dans le volet droit, 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.

La visionneuse de gestion à distance peut également être installée sur le périphérique manuellement :

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 (Facultatif) 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-install, 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 SP1 (10.1) vers Novell ZENworks 10 Configuration Management SP2 (10.2), 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-10.1.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 32](#).

## 2.8 Démarrage des opérations de gestion à distance

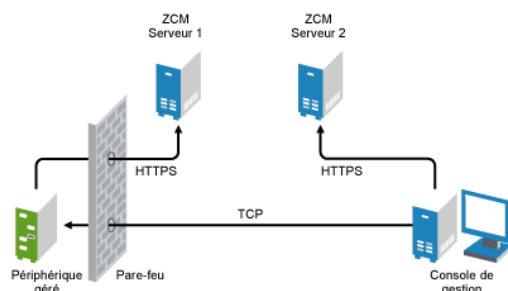
L'opération à distance peut être lancée de plusieurs manières :

- ♦ [Section 2.8.1, « Lancement d'une session à partir de la console de gestion », page 33](#)
- ♦ [Section 2.8.2, « Lancement d'une session à partir du périphérique géré », page 46](#)

### 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 vous souhaitez que des connexions s'effectuent d'un réseau public vers un réseau privé, déployez la passerelle d'application DNS (DNS\_ALG). Pour plus d'informations sur DNS\_ALG, reportez-vous au document [RFC 2694](http://www.ietf.org/rfc/rfc2694) (<http://www.ietf.org/rfc/rfc2694>).

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 à distance peut lancer une session de plusieurs manières :

- ♦ « Démarrage d'une opération de gestion à distance dans le Centre de contrôle ZENworks » page 34
- ♦ « Démarrage d'une opération de gestion à distance en mode autonome » page 41
- ♦ « Démarrage d'une opération de gestion à distance à l'aide des options de ligne de commande » page 41

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

Vous pouvez lancer les différentes opérations de gestion à distance à partir du contexte du périphérique ou du contexte de l'utilisateur :

- ♦ « Lancement d'une session de gestion à distance depuis le contexte de périphérique » page 34
- ♦ « Lancement d'une session de gestion à distance à partir du contexte utilisateur » page 38

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

Pour lancer une session de gestion à distance sur un périphérique

- 1 Dans le Centre de contrôle ZENworks, cliquez sur l'onglet *Périphériques*.
- 2 Cliquez sur *Serveur(s)* ou sur *Postes de travail* et 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 *Tâches du périphérique* dans le volet gauche, sélectionnez l'opération de gestion à distance que vous voulez effectuer.

Les opérations distantes disponibles sont les suivantes :

- ♦ **Contrôle à distance** : affiche la boîte de dialogue Gestion à distance qui permet d'effectuer les opérations 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 les opérations de diagnostics à distance sur le périphérique géré.
  - ♦ **Transférer les fichiers** : affiche la boîte de dialogue Transfert de fichiers qui permet d'effectuer les opérations de transfert de fichiers sur le périphérique géré.
- 3** Renseignez les champs de la boîte de dialogue qui s'affiche. Le tableau ci-dessous fournit des informations sur les différentes options disponibles :

Champ	Détails
Périphérique	Indiquez le nom d'hôte ou l'adresse IP du périphérique que vous voulez 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	<p>Sélectionnez le mode que vous voulez utiliser pour authentifier le périphérique géré. Les modes d'authentification sont les suivants :</p> <ul style="list-style-type: none"> <li>♦ Authentification basée sur les droits</li> <li>♦ Authentification basée sur les mots de passe</li> </ul>
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	<p>Sélectionnez l'un des modes suivants pour la session :</p> <ul style="list-style-type: none"> <li>♦ <b>Collaborer</b> : 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 : <ul style="list-style-type: none"> <li>♦ Invitation d'autres opérateurs à distance à rejoindre la session à distance.</li> <li>♦ Délégation des droits de contrôle à distance à un opérateur à distance.</li> <li>♦ Reprise du contrôle sur l'opérateur à distance.</li> <li>♦ Fin d'une session à distance.</li> </ul> <p>Les sessions consécutives lancées sont des sessions d'affichage à distance.</p> </li> <li>♦ <b>Partagée</b> : permet à plusieurs opérateurs à distance de contrôler simultanément le périphérique géré.</li> <li>♦ <b>Exclusif</b> : 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.</li> </ul> <p>Cette option est uniquement disponible dans la boîte de dialogue Gestion à distance.</p>
Codage de session	Vérifiez que la session à distance 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 <code>novell-zenworks-vncviewer.txt</code> . Le fichier est enregistré par défaut sur le bureau si vous lancez le Centre de contrôle ZENworks (ZCC) par l'intermédiaire d'Internet Explorer et dans le répertoire mozilla installé si vous lancez ZCC par l'intermédiaire de Mozilla* Firefox*.
Router via le proxy	<p>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.</p> <p>Renseignez les champs suivants :</p> <p><b>Proxy</b> : indiquez le nom DNS ou l'adresse IP du proxy de gestion à distance. Par défaut, le proxy configuré dans le panneau <b>Paramètres de proxy</b> pour exécuter l'opération à distance sur le périphérique est renseigné dans ce champ. Vous pouvez spécifier un autre proxy.</p> <p><b>Port Proxy</b> : indiquez le numéro de port sur lequel le proxy de gestion à distance écoute. Le port par défaut est 5750.</p> <hr/> <p><b>Remarque</b> : 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.</p> <hr/> <p>Utiliser la paire de clés suivante pour l'identification</p> <p>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 :</p> <p><b>Clé privée</b> : cliquez sur <i>Parcourir</i> pour rechercher et sélectionner la clé privée de l'opérateur à distance.</p> <p><b>Certificat</b> : cliquez sur <i>Parcourir</i> 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.</p> <p>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.</p> <p><b>Activer le chemin du cache</b> : permet de mettre en cache les chemins de la clé primaire et du certificat sur la console de gestion</p> <p>Cette option n'est actuellement prise en charge que sous Windows.</p>

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 souhaitez aider un utilisateur en exécutant une session à distance sur le périphérique géré auquel il est logué :

- 1** Dans le Centre de contrôle ZENworks, cliquez sur l'onglet *Utilisateurs*.
- 2** Cliquez sur la *source d'utilisateurs*.
- 3** Sélectionnez l'utilisateur afin de gérer à distance le périphérique auquel il est logué.
- 4** Cliquez sur *Action*, puis sélectionnez l'opération de gestion à distance que vous voulez effectuer.

Les opérations disponibles sont les suivantes :

- ♦ **Contrôle à distance** : affiche la boîte de dialogue Gestion à distance qui permet d'effectuer les opérations 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 les opérations de diagnostics à distance sur le périphérique géré.
  - ♦ **Transférer les fichiers** : affiche la boîte de dialogue Transfert de fichiers qui permet d'effectuer les opérations de transfert de fichiers sur le périphérique géré.
- 5** Renseignez les champs de la boîte de dialogue qui s'affiche. Le tableau ci-dessous fournit des informations sur les différentes options disponibles :

Champ	Détails
Périphérique	Indiquez le nom d'hôte ou l'adresse IP du périphérique que vous voulez 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	<p>Sélectionnez le mode que vous voulez utiliser pour authentifier le périphérique géré. Les modes d'authentification sont les suivants :</p> <ul style="list-style-type: none"> <li>♦ Authentification basée sur les droits</li> <li>♦ Authentification basée sur les mots de passe</li> </ul>
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	<p>Sélectionnez l'un des modes suivants pour la session :</p> <ul style="list-style-type: none"> <li>♦ <b>Collaborer</b> : 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 : <ul style="list-style-type: none"> <li>♦ Invitation d'autres opérateurs à distance à rejoindre la session à distance.</li> <li>♦ Délégation des droits de contrôle à distance à un opérateur à distance.</li> <li>♦ Reprise du contrôle sur l'opérateur à distance.</li> <li>♦ Fin d'une session à distance.</li> </ul> <p>Les sessions consécutives lancées sont des sessions d'affichage à distance.</p> </li> <li>♦ <b>Partagée</b> : permet à plusieurs opérateurs à distance de contrôler simultanément le périphérique géré.</li> <li>♦ <b>Exclusif</b> : 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.</li> </ul> <p>Cette option est uniquement disponible dans la boîte de dialogue Gestion à distance.</p>
Codage de session	Vérifiez que la session à distance 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 <code>novell-zenworks-vncviewer.txt</code> . Le fichier est enregistré par défaut sur le bureau si vous lancez le Centre de contrôle ZENworks (ZCC) par l'intermédiaire d'Internet Explorer et dans le répertoire mozilla installé si vous lancez ZCC par l'intermédiaire de Mozilla* Firefox*.
Router via le proxy	<p>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.</p> <p>Renseignez les champs suivants :</p> <p><b>Proxy</b> : indiquez le nom DNS ou l'adresse IP du proxy de gestion à distance. Par défaut, le proxy configuré dans le panneau <b>Paramètres de proxy</b> pour exécuter l'opération à distance sur le périphérique est renseigné dans ce champ. Vous pouvez spécifier un autre proxy.</p> <p><b>Port Proxy</b> : indiquez le numéro de port sur lequel le proxy de gestion à distance écoute. Le port par défaut est 5750.</p> <hr/> <p><b>Remarque</b> : 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.</p> <hr/>
Utiliser la paire de clés suivante pour l'identification	<p>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 :</p> <p><b>Clé privée</b> : cliquez sur <i>Parcourir</i> pour rechercher et sélectionner la clé privée de l'opérateur à distance.</p> <p><b>Certificat</b> : cliquez sur <i>Parcourir</i> 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.</p> <p>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.</p> <p><b>Activer le chemin du cache</b> : permet de mettre en cache les chemins de la clé primaire et du certificat sur la console de gestion</p> <p>Cette option n'est actuellement prise en charge que sous Windows.</p>

**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 :

Procédez comme suit pour installer la visionneuse :

- 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` et enregistrez-le à un emplacement temporaire.
- 5 Double-cliquez sur le fichier `.msi` pour installer la dernière version de la visionneuse de gestion à distance ZENworks.

Ce fichier est installé automatiquement dans le répertoire `C:\Document And Settings\nom d'utilisateur\ApplicationData\Novell\Zenworks\Remote Management\bin`.

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 de gestion à distance ZENworks 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 IP du 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

Avant de lancer une opération de gestion à distance à partir de la ligne de commande, assurez-vous que l'option *Autoriser la connexion lorsque la console de gestion à distance n'a pas de certificat SSL* dans les paramètres de sécurité de la stratégie de gestion à distance est activée.

Pour installer la visionneuse de gestion à distance :

- 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` et enregistrez-le à un emplacement temporaire.

- 5 Double-cliquez sur le fichier .msi pour installer la dernière version de la visionneuse de gestion à distance ZENworks.

Ce fichier est installé automatiquement dans le répertoire C:\Document And Settings\nom d'utilisateur\ApplicationData\Novell\Zenworks\Remote Management\bin.

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 le fichier novell-zenworks-rm-viewer-version.msi est installé.

- 2 Exécutez la commande suivante :

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

Le port par défaut pour le périphérique géré est le 5950 et le proxy est le 5750.

Pour plus d'informations sur les options de ligne de commande disponibles, reportez-vous au [Tableau 2-1](#).

- 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 une autorité de certification interne est déployée, vous devez spécifier les options de ligne de commande `key`, `cert` et `CACert` dans la commande `nzrViewer` pour l'authentification SSL. Si vous ne souhaitez pas les spécifier, assurez-vous que l'option *Autoriser la connexion lorsque la console de gestion à distance n'a pas de certificat SSL* dans les paramètres de sécurité de la stratégie de gestion à distance est activée. 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.

**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.

Option de ligne de commande	Paramètre	Description
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	<i>appname</i>	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	<i>level</i>	<p>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 :</p> <ul style="list-style-type: none"> <li>♦ 0 correspond à l'absence de compression</li> <li>♦ 1 indique la vitesse la plus élevée</li> <li>♦ 9 correspond à la compression la plus élevée</li> </ul> <p>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).</p>
noencrypt		Lance la session distante en mode non codé.
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.
partage		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.
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.

Option de ligne de commande	Paramètre	Description
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.
scale	<i>percentage</i>	Agrandit la fenêtre d'affichage au pourcentage spécifié.
emulate3timeout	<i>ms</i>	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	<i>n</i>	Spécifie les niveaux de consignment des informations.
Web		Consigne les informations dans une fenêtre de la console.
fichierjournal	<i>Nom du fichier</i>	Nom du fichier journal dans lequel les informations doivent être consignées.
config	<i>Nom du fichier</i>	Nom de la configuration à utiliser pour le chargement des paramètres de configuration prédéfinis.

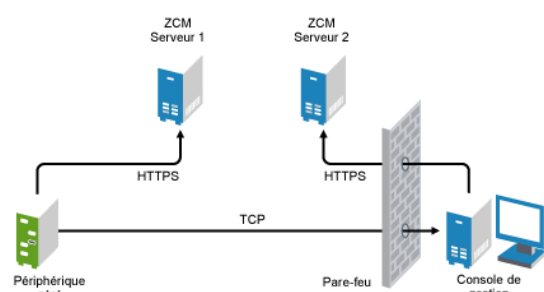
Option de ligne de commande	Paramètre	Description
key	<i>Nom du fichier</i>	Nom du fichier dans lequel la clé privée est stockée. Cette clé est utilisée au cours d'un contrôle de flux SSL avec le périphérique géré.  <b>Important</b> : la clé et les options cert doivent être utilisées ensemble. Si vous utilisez ces options avec la commande <code>nzrViewer</code> , pour des raisons de sécurité, vous devez désactiver l'option <i>Autoriser la connexion lorsque la console de gestion à distance n'a pas de certificat</i> dans les paramètres de sécurité de la stratégie de gestion à distance.
cert	<i>Nom du fichier</i>	Nom du fichier dans lequel le certificat correspondant à la clé privée est stocké.  <b>Important</b> : la clé et les options cert doivent être utilisées ensemble. Si vous utilisez ces options avec la commande <code>nzrViewer</code> , pour des raisons de sécurité vous devez désactiver l'option <i>Autoriser la connexion lorsque la console de gestion à distance n'a pas de certificat</i> dans les paramètres de sécurité de la stratégie de gestion à distance.
CAcert	<i>Nom du fichier</i>	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	<i>encname</i>	Spécifie le codage désiré à utiliser pour la session. Les types différents de codage sont Raw, CopyRect, RRE, CoRRE, Hextile, Zlib et Tight.
compresslevel	<i>n</i>	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.
quality	<i>n</i>	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.
zenrights		Indique que le schéma d'authentification à utiliser est l'authentification ZENworks basée sur les droits.
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).

Option de ligne de commande	Paramètre	Description
proxy	serveur_proxy	<p>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 :</p> <ul style="list-style-type: none"> <li>♦ <i>adresse IP~Port</i>. Par exemple : 10.0.0.0~5750.</li> <li>♦ <i>adresse IP~Port</i>. Par exemple : 10.0.0.0~50.</li> </ul>

## 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 à distance avec lequel vous voulez ouvrir la session à distance.

ou

Si l'opérateur à distance n'est pas répertorié, indiquez les informations de connexion de l'opérateur dans les champs *Demande de 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 souhaitez que des connexions s'effectuent d'un réseau public vers un réseau privé, déployez la passerelle d'application DNS (DNS\_ALG). Pour plus d'informations sur DNS\_ALG, reportez-vous au document [RFC 2694](http://www.ietf.org/rfc/rfc2694) (<http://www.ietf.org/rfc/rfc2694>).

## 2.9 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 ne peut être installé que sur un périphérique géré Windows.

Pour installer le proxy, procédez comme suit :

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

`https://serveur/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_produit.msi` et enregistrez-le à un emplacement temporaire.

La valeur *version\_produit* 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"
```





# Gestion des sessions distantes

# 3

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

- ♦ [Section 3.1, « Gestion d'une session d'affichage à distance », page 49](#)
- ♦ [Section 3.2, « Gestion d'une session d'affichage à distance », page 53](#)
- ♦ [Section 3.3, « Gestion d'une session d'exécution à distance », page 54](#)
- ♦ [Section 3.4, « Gestion d'une session de diagnostics à distance », page 54](#)
- ♦ [Section 3.5, « Gestion d'une session de transfert de fichiers », page 56](#)
- ♦ [Section 3.6, « Sortie de veille d'un périphérique distant », page 59](#)
- ♦ [Section 3.7, « Amélioration des performances de la gestion à distance », page 60](#)




## 3.1 Gestion d'une session d'affichage à distance








La gestion à distance permet de contrôler à distance un périphérique géré. Avec des connexions de contrôle à distance, l'opérateur distant peut aller au-delà de l'affichage du périphérique géré et en prendre le contrôle, ce qui permet d'aider un utilisateur et de résoudre les problèmes du périphérique géré. 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 33](#).





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

Le tableau ci-dessous décrit les différentes options de barre d'outils disponibles dans la Visionneuse de gestion à distance au cours d'une session de contrôle à distance. Il répertorie également les touches de raccourci lorsqu'elles existent.

**Tableau 3-1** Options de la barre d'outils de 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 telles que le format et le codage pour améliorer les performances de la session, la consignment, ainsi que la gestion locale et à distance du curseur.
 Infos de connexion	Ctrl+Alt+Maj+I	Fournit le nom d'hôte, le port, la résolution d'écran et la version du protocole du périphérique géré.
 Plein écran	Ctrl+Alt+Maj+F	Permet de basculer entre le mode plein écran et le mode normal.

Option	Touche de raccourci	Fonction
 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.
 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 pour envoyer la touche Alt au périphérique géré.
 Mettre en veille/ activer l'écran	Ctrl+Alt+Maj+B	<p>Vide ou affiche l'écran sur le périphérique géré. Lorsque le contenu de l'écran du périphérique est vidé, les opérations exécutées par l'opérateur distant sur ce périphérique ne sont pas visibles par l'utilisateur. Les commandes du clavier et de la souris du périphérique géré sont également verrouillées.</p> <p>Cette option est activée uniquement si l'option <i>Autoriser la mise en veille de l'écran du périphérique géré</i> est activée dans la stratégie de gestion à distance effective sur le périphérique géré.</p>
 Verrouiller/ déverrouiller le clavier et la souris	Ctrl+Alt+Maj+L	<p>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.</p> <p>Cette option est activée uniquement si l'option <i>Autoriser le verrouillage de la souris et du clavier du périphérique géré lors du contrôle à distance</i> est activée dans la stratégie de gestion à distance effective sur le périphérique géré.</p>
 Transférer les fichiers	Ctrl+Alt+Maj+T	<p>Lance une session pour transférer des fichiers vers et à partir du périphérique géré.</p> <p>Cette option est activée uniquement si l'option <i>Autoriser le transfert de fichiers sur le périphérique géré</i> est activée dans la stratégie de gestion distante effective sur le périphérique géré. Pour plus d'informations sur le transfert de fichiers, reportez-vous à la <a href="#">Section 3.5, « Gestion d'une session de transfert de fichiers »</a>, page 56.</p>

Option	Touche de raccourci	Fonction
<b>Collaboration</b> 		<p>Lance une session de collaboration ZENworks Remote Management sur le périphérique géré, 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.</p> <p>Pour plus d'informations sur la collaboration de session, reportez-vous à la <a href="#">Section 3.1.2, « Collaboration de session », page 51</a>.</p>
<b>Exécution à distance</b> 	Ctrl+Alt+Maj+U	<p>Lance une session d'exécution à distance sur le périphérique géré afin de lancer à distance n'importe quel exécutable du périphérique géré.</p> <p>Cette option est activée uniquement si l'option <i>Autoriser l'exécution à distance des programmes sur le périphérique géré</i> est activée dans la stratégie de gestion distante effective sur le périphérique géré.</p>
<b>Remplacer l'économiseur d'écran</b> 	Ctrl+Alt+Maj+O	<p>Remplace un éventuel économiseur d'écran protégé par mot de passe sur le périphérique géré au cours de la session à distance.</p> <p>Cette option est activée uniquement si l'option <i>Autoriser le déverrouillage automatique de l'économiseur d'écran lors du contrôle à distance</i> est activée dans la stratégie de gestion distante effective sur le périphérique géré.</p>
<b>Déconnecter</b> 	Alt+F4	<p>Ferme la session à distance.</p>

### 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 géré, vous obtenez les privilèges d'un opérateur distant maître. La collaboration de session permet de :

- ♦ Inviter plusieurs opérateurs distants à rejoindre la session de contrôle à distance.
- ♦ Déléguer les droits de contrôle distant à un opérateur distant pour aider à résoudre un problème, et lui reprendre le contrôle par la suite.
- ♦ Fermer une session à distance.

Pour lancer la Collaboration de session :

- 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 33](#).

- 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 sous la forme d'une entrée distincte 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 à distance a rejoint la session et se trouve en mode Affichage à distance.
- ♦ Un cercle vert indique que l'opérateur à distance 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 21](#) ».

Le tableau suivant répertorie les opérations que vous pouvez effectuer en tant qu'opérateur distant maître au cours de la collaboration de session :

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

Tâche	Étapes	Détails complémentaires
Inviter un opérateur distant à rejoindre une session distante	<ol style="list-style-type: none"> <li>1. Sélectionnez un opérateur à distance figurant dans la fenêtre Collaboration de session.</li> <li>2. Cliquez sur <i>Inviter</i>.</li> </ol>	<p>Si l'opérateur à distance accepte la demande et rejoint la session, le cercle gris de l'opérateur devient rouge.</p> <p>Par défaut, la nouvelle session démarre en mode Affichage à distance.</p>
Déléguer les droits de contrôle à distance à l'opérateur à distance	<ol style="list-style-type: none"> <li>1. Sélectionnez l'opérateur à distance auquel vous voulez déléguer les droits de contrôle à distance.</li> <li>2. Cliquez sur <i>Déléguer</i>.</li> </ol>	<p>L'opérateur à distance sélectionné se trouve désormais en mode Contrôle à distance et son cercle rouge devient vert.</p> <p>L'opérateur distant maître passe automatiquement en mode Affichage à distance.</p>
Reprendre les droits de contrôle à distance à l'opérateur à distance	<ol style="list-style-type: none"> <li>1. Cliquez sur <i>Reprendre le contrôle</i>.</li> </ol>	<p>L'opérateur à distance passe en mode Affichage à distance et son cercle vert devient rouge.</p> <p>L'opérateur distant maître passe automatiquement en mode Contrôle à distance.</p>

Tâche	Étapes	Détails complémentaires
Mettre fin à la session à distance	<ol style="list-style-type: none"> <li>1. Sélectionnez l'opérateur à distance à partir duquel vous voulez mettre fin à la session à distance.</li> <li>2. Cliquez sur <i>Arrêter</i>.</li> </ol>	<p>Si l'opérateur à distance sélectionné se trouve en mode Contrôle à distance, vous reprenez les droits de contrôle à distance.</p> <p>La session de l'opérateur à distance se termine et la couleur de son cercle devient grise.</p>
Inviter un opérateur à distance externe	<ol style="list-style-type: none"> <li>1. Cliquez sur <i>Inviter externe</i> pour inviter des opérateurs à distance non répertoriés dans la fenêtre Collaboration de session à se joindre à la session à distance.</li> <li>2. Indiquez le nom DNS ou l'adresse IP du périphérique de l'opérateur à distance, ainsi que son numéro de port. Par exemple, 10.0.0.0 ~1000.</li> <li>3. Cliquez sur <i>Inviter</i>.</li> </ol>	




Si l'opérateur distant maître déconnecte la session distante, tous les opérateurs distants sont exclus de la session.




## 3.2 Gestion d'une session d'affichage à distance

L'affichage à distance permet de vous connecter à distance à un périphérique géré pour en visualiser le bureau. Pour obtenir des informations sur le lancement d'une session d'affichage à distance, reportez-vous à la [Section 2.8, « Démarrage des opérations de gestion à distance », page 33](#).

Le tableau ci-dessous décrit les différentes options de barre d'outils disponibles dans la Visionneuse de gestion à distance au cours d'une session d'affichage à distance.

**Tableau 3-3** Options de la barre d'outils de 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 telles que le format et le codage pour améliorer les performances de la session, la consignation, ainsi que la gestion locale et à distance du curseur.
Infos de connexion 	Ctrl+Alt+Maj+I	Fournit le nom d'hôte, le port, la résolution d'écran et la version du protocole du périphérique géré.
Plein écran 	Ctrl+Alt+Maj+F	Permet de basculer entre le mode plein écran et le mode normal.

Option	Touche de raccourci	Fonction
 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 permet d'exécuter des exécutables à distance avec les privilèges système sur le périphérique géré. Pour exécuter une application sur un périphérique géré, ouvrez la session d'exécution à distance.

**1** Ouvrez la session d'exécution à distance.

Pour obtenir des 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 33](#).

**2** Indiquez 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 distante de l'application spécifiée peut échouer si l'application n'est pas disponible sur le périphérique géré dans le chemin défini.







**Avertissement :** 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 l'application après utilisation.

### 3.4 Gestion d'une session de diagnostics 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 diagnostics à distance sur le périphérique géré, vous ne pouvez accéder qu'aux applications de diagnostic configurées pour le périphérique dans les paramètres de gestion à distance pour diagnostiquer et résoudre les problèmes qui le concernent. Au cours de la session, les applications de diagnostic sont affichées sous forme d'icônes dans une barre d'outils. Les applications de diagnostic suivantes sont configurées par défaut dans les paramètres de gestion à distance :

**Tableau 3-4** Options de la barre d'outils de 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 telles que le format et le codage pour améliorer les performances de la session, la consignment, ainsi que la gestion locale et à distance du curseur.
Infos de connexion 	Ctrl+Alt+Maj+I	Fournit le nom d'hôte, le port, la résolution d'écran et la version du protocole du périphérique géré.
Plein écran 	Ctrl+Alt+Maj+F	Permet de basculer entre le mode plein écran et le mode normal.
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 <i>Autoriser le transfert de fichiers sur le périphérique géré</i> est activée dans la stratégie de gestion distante effective sur le périphérique géré. Pour plus d'informations sur le transfert de fichiers, reportez-vous à la <a href="#">Section 3.5, « Gestion d'une session de transfert de fichiers »</a> , page 56.
Déconnecter 	Alt+F4	Ferme la session à distance.

**Tableau 3-5** Applications de diagnostic à distance

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

Vous pouvez configurer les applications pour qu'elles soient lancées sur le périphérique géré au cours 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 17.



## 3.5 Gestion d'une session de transfert de fichiers

La gestion à distance permet de transférer des fichiers entre la console de gestion et le périphérique géré. Pour obtenir des 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 33.





Dans la fenêtre Transfert de fichiers, le panneau Ordinateur local affiche tous les fichiers et les dossiers de la console de gestion, alors que le panneau Ordinateur à distance affiche tous les fichiers et les dossiers du répertoire spécifié dans *Répertoire root du transfert de fichier* dans la stratégie de gestion à distance. Si *Répertoire root du transfert de fichier* n'est pas renseigné dans la stratégie ou si le périphérique géré n'a aucune stratégie associée, vous pouvez exécuter des transferts de fichiers sur tout le système de fichiers du périphérique à distance.


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 <i>Opérations &gt; Nouveau dossier local</i> .  OU  Cliquez sur  sur le volet Ordinateur local.  2. Suivez les invites à l'écran.	
Créer un nouveau dossier à distance	Alt+W	1. Cliquez sur <i>Opérations &gt; Nouveau dossier à distance</i> .  OU  Cliquez sur  sur 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.	



Tâches	Raccourcis clavier	Étapes	Détails complémentaires
Renommer des fichiers ou dossiers	Alt+N	<ol style="list-style-type: none"> <li>1. Sélectionnez le fichier ou dossier à renommer.</li> <li>2. Cliquez sur <i>Opérations &gt; Renommer.</i> OU Cliquez sur .</li> <li>3. Suivez les invites à l'écran.</li> </ol>	
Supprimer des fichiers ou dossiers	Alt+D	<ol style="list-style-type: none"> <li>1. Sélectionnez les fichiers ou dossiers à supprimer.</li> <li>2. Cliquez sur <i>Opérations &gt; Supprimer.</i> OU Cliquez sur .</li> <li>3. Suivez les invites à l'écran.</li> </ol>	Vous pouvez utiliser les touches Maj ou Ctrl pour sélectionner plusieurs fichiers.
Rafraîchir un dossier local	Alt+E	<ol style="list-style-type: none"> <li>1. Cliquez sur <i>Opérations &gt; Rafraîchir un dossier local.</i> OU Cliquez sur  dans le volet Ordinateur local.</li> </ol>	
Rafraîchir un dossier à distance	Alt+M	<ol style="list-style-type: none"> <li>1. Cliquez sur <i>Opérations &gt; Rafraîchir un dossier à distance.</i> OU Cliquez sur  sur le volet Ordinateur à distance.</li> </ol>	
Trier les fichiers locaux		<ol style="list-style-type: none"> <li>1. Cliquez sur <i>Opérations &gt; Tri local.</i></li> <li>2. Sélectionnez le type de tri. Vous pouvez trier les fichiers par nom, par taille ou par date.</li> </ol>	Vous pouvez également trier les fichiers en cliquant sur les en-têtes des colonnes respectives.

Tâches	Raccourcis clavier	Étapes	Détails complémentaires
Trier les fichiers à distance		<ol style="list-style-type: none"> <li>1. Cliquez sur <i>Opérations &gt; Tri à distance</i>.</li> <li>2. Sélectionnez le type de tri. Vous pouvez trier les fichiers par nom, par taille ou par date</li> </ol>	Vous pouvez également trier les fichiers en cliquant sur les en-têtes des colonnes respectives.
Télécharger des fichiers/ dossiers		<ol style="list-style-type: none"> <li>1. Sélectionnez les fichiers à télécharger sur l'ordinateur à distance.</li> <li>2. Sélectionnez le répertoire cible dans le panneau de l'ordinateur distant.</li> <li>3. Cliquez sur <i>Opérations &gt; Télécharger</i>. OU Cliquez sur ➡</li> </ol>	<p>L'option <i>Opérations &gt; Télécharger</i> n'est disponible que si le focus est sur l'ordinateur local.</p> <p>Vous pouvez utiliser les touches Maj ou Ctrl pour sélectionner plusieurs fichiers.</p>
Télécharger des fichiers/ dossiers	Alt+O	<ol style="list-style-type: none"> <li>1. Sélectionnez les fichiers à télécharger sur l'ordinateur local.</li> <li>2. Sélectionnez le répertoire cible dans le panneau de l'ordinateur local.</li> <li>3. Cliquez sur <i>Opérations &gt; Charger</i>. OU Cliquez sur ⬅</li> </ol>	<p>L'option <i>Opérations &gt; Charger</i> n'est disponible que si le focus est sur l'ordinateur à distance.</p> <p>Vous pouvez utiliser les touches Maj ou Ctrl pour sélectionner plusieurs fichiers.</p>
Annuler le transfert de fichiers	Alt+C	<ol style="list-style-type: none"> <li>1. Cliquez sur <i>Opérations &gt; Annuler le transfert de fichiers</i>.</li> </ol>	Vous pouvez également annuler l'opération de transfert de fichiers en cliquant sur le bouton Annuler.
Afficher les propriétés des fichiers	Alt+P	<ol style="list-style-type: none"> <li>1. Sélectionnez les fichiers.</li> <li>2. Cliquez sur <i>Opérations &gt; Propriétés</i>. OU Cliquez sur </li> </ol>	<p>Vous pouvez utiliser les touches Maj ou Ctrl pour sélectionner plusieurs fichiers.</p> <p>Affiche la taille cumulée des fichiers et dossiers sélectionnés.</p>

Tâches	Raccourcis clavier	Étapes	Détails complémentaires
Placer dans le dossier parent		1. Cliquez sur  pour le placer dans le dossier parent.	

## 3.6 Sortie de veille d'un périphérique distant

L'activation à distance permet d'activer un nœud unique ou un groupe de nœuds mis hors tension sur votre réseau si la carte réseau sur le nœud soit compatible avec le service Wake-on-LAN.

- ♦ [Section 3.6.1, « Conditions préalables », page 59](#)
- ♦ [Section 3.6.2, « Activation à distance des périphériques gérés », page 59](#)

### 3.6.1 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 nœud distant est dans un état d'arrêt à chaud. Avec l'arrêt à chaud de l'alimentation, l'UC est arrêtée et sa carte d'interface réseau utilise une quantité minime de courant. 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.

### 3.6.2 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 sur *Postes de travail* pour afficher la liste des périphériques gérés.
- 3 Sélectionnez le périphérique à sortir de veille.
- 4 Cliquez sur *Tâches rapides* > *Réveiller* pour afficher la boîte de dialogue Réveiller.
- 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.

## 3.7 Amélioration des 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 obtenir un meilleur temps de réponse, essayez une ou plusieurs des options suivantes :

- ♦ [Section 3.7.1, « Sur la console de gestion », page 60](#)
- ♦ [Section 3.7.2, « Sur le périphérique géré », page 60](#)

### 3.7.1 Sur la console de gestion

Dans la fenêtre Connexion à 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 des couleurs 8 bits*.
  - ♦ Définissez le niveau *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.

### 3.7.2 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 Pentium\* III à 700 MHz (ou plus), doté d'au moins 256 Mo de RAM.
- ♦ Ne définissez pas un modèle de papier peint.

Les sections suivantes donnent des informations que vous devez connaître au sujet de la sécurité lorsque vous utilisez le composant de gestion à distance de Novell® ZENworks® 10 Configuration Management :

- ♦ [Section 4.1, « Authentification », page 61](#)
- ♦ [Section 4.2, « Force des mots de passe », page 63](#)
- ♦ [Section 4.3, « Ports », page 63](#)
- ♦ [Section 4.4, « Audit », page 63](#)
- ♦ [Section 4.5, « Demander l'autorisation de l'utilisateur du périphérique géré », page 64](#)
- ♦ [Section 4.6, « Fin anormale », page 64](#)
- ♦ [Section 4.7, « Détection d'intrus », page 65](#)
- ♦ [Section 4.8, « Identification de l'opérateur à distance », page 65](#)
- ♦ [Section 4.9, « Configuration du navigateur », page 66](#)
- ♦ [Section 4.10, « Sécurité de la session », page 66](#)

## 4.1 Authentification

Le service de gestion à distance doit être installé sur un périphérique pour que l'opérateur distant puisse le gérer à distance. Le service démarre automatiquement lorsque le périphérique géré démarre. Lorsqu'un opérateur distant lance une session à distance sur le périphérique géré, le service ne démarre la session à distance que si l'opérateur distant est autorisé à exécuter des opérations à distance sur le périphérique géré.

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

- ♦ [Section 4.1.1, « Authentification de la gestion à distance basée sur les droits », page 61](#)
- ♦ [Section 4.1.2, « Authentification de la gestion à distance basée sur les mots de passe », page 62](#)

### 4.1.1 Authentification de la gestion à distance basée sur les droits

Lors de l'authentification basée sur les droits, ces derniers sont assignés à l'opérateur distant pour qu'il puisse lancer une session distante sur le périphérique géré. L'administrateur ZENworks et le super administrateur disposent par défaut des droits permettant d'effectuer des opérations à distance sur tous les périphériques gérés que l'utilisateur logués au périphérique soit l'utilisateur local ou l'utilisateur ZENworks.

L'opérateur distant n'a pas besoin des droits exclusifs pour exécuter une session distante sur le périphérique géré si aucun utilisateur n'est logué au périphérique géré ou si un utilisateur s'est logué au périphérique géré mais pas à ZENworks. En revanche, l'opérateur distant a besoin des droits

exclusifs de gestion à distance pour exécuter l'opération distante sur le périphérique géré lorsqu'un utilisateur ZENworks s'est logué au périphérique. Nous vous recommandons vivement d'utiliser l'authentification basée sur les droits car elle est sûre.

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

### 4.1.2 Authentification de la gestion à distance basée sur les mots de passe

Lors de l'authentification basée sur les mots de passe, l'opérateur distant est invité à saisir un mot de passe pour qu'il puisse lancer la session distante sur le périphérique géré.

Les deux types de schémas d'authentification basée sur les mots de passe utilisés sont les suivants :

- ♦ **Mot de passe ZENworks** : ce schéma est basé sur le protocole SRP (Secure Remote Password) (version 6a). La longueur maximale d'un mot de passe ZENworks est de 255 caractères.
- ♦ **Mot de passe VNC** : il s'agit du schéma d'authentification par mot de passe VNC traditionnel. La longueur maximale d'un mot de passe VNC est de 8 caractères. Ce schéma de mot de passe est intrinsèquement faible et n'est fourni que pour 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 n'est valide que 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. Lorsqu'il initialise une session distante avec le périphérique géré, l'opérateur doit saisir le mot de passe correct dans la boîte de dialogue du mot de passe de la session qui s'affiche. Si l'opérateur distant ne parvient pas à saisir le mot de passe correct dans les deux minutes qui suivent l'apparition de la boîte de dialogue, la session se ferme pour des raisons de sécurité. Si vous utilisez l'authentification basée sur les mots de passe, nous vous recommandons vivement d'utiliser ce mode car le mot de passe n'est valide que pour la session en cours et n'est pas enregistré sur le périphérique géré.
- ♦ **Mode persistant** : dans ce mode, le 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 par l'intermédiaire de 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 un mot de passe est défini à la fois par l'utilisateur du périphérique géré et dans la stratégie, le mot de passe défini par l'utilisateur a priorité sur le mot de passe configuré dans la stratégie.

L'administrateur peut empêcher l'utilisateur d'un périphérique géré de définir le mot de passe et peut même réinitialiser le mot de passe que ce dernier a défini pour s'assurer que le mot de passe configuré dans la stratégie est toujours appliqué au cours de l'authentification. Pour plus

d'informations sur la réinitialisation 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 31.](#)

## 4.2 Force des mots de passe

Utilisez des mots de passe sécurisés. Gardez à l'esprit les conseils suivants :

- ♦ **Longueur** : la longueur minimale recommandée est de 6 caractères. Un mot de passe sécurisé comporte au moins 8 caractères ; les mots de passe plus longs sont préférables. La longueur maximale est de 255 caractères pour un mot de passe ZENworks et de 8 caractères pour un mot de passe VNC.
- ♦ **Complexité** : un mot de passe sécurisé contient un mélange de lettres et de nombres. Il doit contenir à la fois des lettres en majuscule et en minuscule et au moins un caractère numérique. L'ajout de chiffres aux mots de passe, en particulier au milieu et non uniquement au début ou à la fin, permet de les renforcer. Les caractères spéciaux tels que &, \*, \$ et > peuvent améliorer sensiblement la force d'un mot de passe. N'utilisez pas de mots reconnaissables tels que des noms propres ou les mots d'un dictionnaire, ni d'informations personnelles telles que des numéros de téléphone, des dates de naissance, des dates d'anniversaire, des adresses ou des codes postaux.

## 4.3 Ports

Le service de gestion à distance est exécuté par défaut sur le port 5950 et le module d'écoute de la gestion à distance, sur 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.

## 4.4 Audit

ZENworks Configuration Management gère un journal de toutes les sessions distantes exécutées sur le périphérique géré. Ce journal est conservé sur le périphérique géré et est consultable par l'utilisateur et l'administrateur. L'administrateur peut afficher les journaux de toutes les sessions distantes exécutées 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 :

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

Champ	Description
<i>Utilisateur ZENworks</i>	Nom de l'utilisateur ZENworks logué au périphérique géré au démarrage de la session distante.
<i>Opérateurs à distance</i>	Nom de l'opérateur à distance qui a effectué l'opération.

Champ	Description
<i>Machine console</i>	Nom d'hôte du périphérique à partir duquel l'opération à distance a eu lieu.
<i>IP de la console</i>	Adresse IP du périphérique à partir duquel l'opération à distance a eu lieu.
	<b>Remarque :</b> 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.
<i>Opération</i>	Type d'opération effectuée : Contrôle à distance, Exécution à distance, Affichage à distance, Diagnostics à distance, Transfert de fichiers.
<i>Heure de début</i>	Heure à laquelle l'opération à distance a démarré.
<i>Heure de fin</i>	Heure à laquelle l'opération à distance s'est terminée.
<i>État</i>	État de l'opération à distance : Réussite, En cours d'exécution ou Échec. La cause de l'échec s'affiche également.

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

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

Lorsque l'opérateur distant démarre une session distante sur le périphérique géré, le service de gestion à distance vérifie si l'option *Demander l'autorisation de l'utilisateur du périphérique géré* pour cette opération distante est activée dans la stratégie effective sur le périphérique. Si l'option est activée et si aucun utilisateur n'est logué au périphérique, la session distante se poursuit. Mais si l'option est activée et si un utilisateur s'est logué au périphérique géré, un message configuré dans la stratégie de gestion à distance s'affiche pour l'utilisateur demandant l'autorisation de lancer une session distante sur le périphérique. La session ne démarre que si l'utilisateur accorde l'autorisation.

## 4.6 Fin anormale

Lorsqu'une session distante est déconnectée brusquement, la fonction de fin anormale permet de verrouiller le périphérique géré ou de déloguer l'utilisateur du périphérique géré, selon la configuration des paramètres de sécurité de la stratégie de gestion distante. La session distante se termine de façon anormale dans les circonstances suivantes :

- ♦ Le réseau est en échec et la visionneuse de gestion à distance et le service de gestion à distance sont dans l'incapacité de communiquer.
- ♦ La visionneuse de gestion à distance se ferme brusquement par l'intermédiaire du gestionnaire de tâches.
- ♦ Le réseau est désactivé sur le périphérique géré ou sur la console de gestion.

Dans certaines circonstances, le service de gestion à distance peut prendre jusqu'à une minute pour déterminer la fin anormale de la session.



## 4.7 Détection d'intrus

La fonction Détection d'intrus réduit de façon significative le risque de piratage du périphérique géré. Si l'opérateur distant n'est pas parvenu à se loguer au périphérique géré après un nombre défini de tentatives (5 par défaut), le service de gestion à distance est bloqué et n'accepte aucune requête de session distante tant qu'il n'a pas été 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 changer le délai 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 sur *Postes de travail* pour afficher la liste des périphériques gérés.
- 3 Sélectionnez le périphérique à déverrouiller.
- 4 Cliquez sur *Action*, puis sur *Débloquent la gestion à distance*.
- 5 Cliquez sur *OK*.

Pour débloquer le service de gestion à distance sur le périphérique géré :

- 1 Double-cliquez sur l'icône ZENworks dans la zone de notification du périphérique géré.
- 2 Dans le volet gauche, accédez à *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 à distance

Lorsqu'un opérateur distant lance une session distante à partir du Centre de contrôle ZENworks, un certificat aidant le périphérique géré à identifier cet opérateur distant est généré automatiquement. En revanche, si l'opérateur distant lance la session en mode autonome, le certificat n'est pas généré et l'opérateur distant 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. Le service de gestion à distance récupère l'identité de l'opérateur distant en utilisant le certificat fourni par la console de gestion au cours du contrôle de flux SSL (Secure Socket Layer). Le contrôle de flux SSL a lieu pour tous les types d'authentification excepté pour 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 *Afficher un signal visible pour l'utilisateur sur le périphérique géré* est activée dans la stratégie effective 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 SSL (Secure Socket Layer) pour sécuriser les sessions distantes. En revanche, les sessions distantes lancées en utilisant l'authentification basée par mot de passe VNC ne sont pas sécurisées. Le processus d'authentification a 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 Reconnaissance mutuelle SSL

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

Lorsqu'un opérateur distant lance une session à distance sur le périphérique géré, la visionneuse de gestion à distance invite l'opérateur distant à en vérifier le certificat. Le certificat affiche des détails tels que le nom du périphérique géré, l'autorité ayant émis le certificat, la validité du certificat et l'empreinte. Pour des raisons de sécurité, l'opérateur distant doit vérifier les références du périphérique géré en faisant correspondre l'empreinte du certificat à celle communiquée par l'utilisateur du périphérique géré par des méthodes hors bande. Ensuite, l'opérateur distant peut effectuer l'une des opérations suivantes :

- ♦ **Accepter définitivement le certificat** : si un utilisateur qui s'est logué à la console de gestion accepte définitivement le certificat, ce dernier n'est pas affiché dans les sessions distantes suivantes que les utilisateurs logués à cette console lanceront.
- ♦ **Accepter temporairement le certificat** : si un utilisateur qui s'est logué à la console de gestion accepte temporairement le certificat, ce dernier n'est accepté que pour la session en cours. L'utilisateur est invité à vérifier le certificat la prochaine fois qu'une connexion au périphérique géré est initiée.
- ♦ **Rejeter le certificat** : si un utilisateur qui s'est logué à la console de gestion rejette le certificat, il met fin à la session distante.

## 4.10.2 Régénération du certificat

Le périphérique géré régénère un nouveau certificat autosigné si :

- ♦ Le nom du périphérique géré a changé
- ♦ Le certificat est postdaté et n'est pas actuellement valide
- ♦ Le certificat a expiré
- ♦ Le certificat est sur le point d'expirer
- ♦ Le certificat est manquant

Le certificat est régénéré par défaut tous les 10 ans.



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

- ♦ « Impossible de passer outre l'économiseur d'écran sur le périphérique géré. » page 69
- ♦ « Au cours d'une session de gestion à distance, si vous vous déconnectez et vous connectez à un ordinateur Windows 2000\* Professionnel, il se peut que le papier peint défini sur la machine ne soit pas restauré. » page 70
- ♦ « Impossible de lancer une session à distance sur le périphérique utilisant une qualité de couleur est très médiocre. » page 70
- ♦ « Impossible de lancer la visionneuse de gestion à distance. » page 71
- ♦ « La fin anormale de session peut échouer sur les périphériques gérés Windows Vista. » page 71
- ♦ « Le module d'écoute de gestion à distance ne parvient pas à accepter les requêtes de session distante à partir du périphérique géré si le port auquel le module d'écoute se relie n'est pas ouvert dans le pare-feu de la console de gestion. » page 71
- ♦ « Dépannage des messages d'erreur rencontrés lors de l'utilisation du composant Gestion à distance. » page 71
- ♦ « Comment activer le journal de débogage de la gestion à distance sur le périphérique qui lance le centre de contrôle ZENworks. » page 72
- ♦ « Installer une nouvelle version du pilote du miroir. » page 72
- ♦ « Le périphérique géré n'a pas pu initialiser le schéma de codage Novell pour la session. Assurez-vous que le périphérique géré est synchronisé (UTC) avec ce système. Si le problème persiste, contactez les Services Techniques de Novell. » page 72
- ♦ « 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. » page 73
- ♦ « L'option d'écran vide peut ne pas fonctionner lors du contrôle à distance d'un périphérique Windows. » page 73
- ♦ « Lors du lancement d'une session de gestion à distance sur un périphérique géré Windows 2000 Professionnel, le périphérique redémarre. » page 73
- ♦ « Plusieurs instances de la visionneuse de gestion à distance sont lancées sur le périphérique disposant du navigateur Internet Explorer 7. » page 73
- ♦ « Impossible d'utiliser l'icône Ctrl-Alt-Suppr lors du contrôle à distance d'un périphérique Windows Vista ou Windows Server 2008\*. » page 73
- ♦ « Le mode de session par défaut n'est pas sélectionné dans le snap-in de gestion à distance. » page 74
- ♦ « Le lien Installer la visionneuse de gestion à distance reste actif sur un périphérique Windows Vista doté du navigateur Internet Explorer 7. » page 74

**Impossible de passer outre 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 le remplacer pour permettre à l'opérateur distant d'afficher le bureau de l'utilisateur. L'opérateur distant peut également remplacer l'économiseur d'écran au cours de la session distante en cliquant sur l'icône *Passer outre l'économiseur d'écran* sur la barre d'outils de la visionneuse de gestion à distance.

Cause possible : L'économiseur d'écran s'active du fait de l'inactivité de la session distante.

Action : Cliquez sur l'icône *Passer outre l'économiseur d'écran* sur la barre d'outils de la visionneuse de gestion à distance. Il se peut que vous deviez cliquer sur cette icône plusieurs fois.

Cause possible : La fonction *Passer outre l'économiseur d'écran* n'est pas prise en charge sur la plate-forme Windows Vista.

Opération : Aucune.

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

Action : Sélectionnez l'option *Bloquer les événements de déplacement de la souris* dans la fenêtre des options de la visionneuse de gestion à distance ZENworks pour empêcher l'envoi des mouvements de la souris au périphérique géré.

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

Action : Loguez-vous de nouveau 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.

Opération : 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 puissiez pas lancer une session Contrôle à distance, Affichage à distance ou Diagnostics à distance sur un périphérique géré qui fonctionne avec une très médiocre qualité de couleur (moins de 8 bits par pixel (bpp)).

Action : Définissez la qualité de couleur du périphérique sur 16 bpp ou plus à l'aide de la procédure suivante :

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

### **Impossible de lancer la visionneuse de gestion à distance.**

Source : ZENworks 10 Configuration Management ; Gestion à distance.

Cause possible : Il se peut que la visionneuse de gestion à distance ne démarre pas si son fichier exécutable a été 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`.

### **La fin anormale de session peut échouer sur les périphériques gérés Windows Vista.**

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 gérés Windows Vista, ZENworks risque de ne pas détecter qu'il s'agit d'une fin anormale et de ne pas verrouiller le périphérique ou de déloguer l'utilisateur du périphérique géré.

Opération : Aucune.

### **Le module d'écoute de gestion à distance ne parvient pas à accepter les requêtes de session distante à partir du périphérique géré si le port auquel le module d'écoute se relie n'est pas ouvert dans le pare-feu de la console de gestion.**

Source : ZENworks 10 Configuration Management ; Gestion à distance.

Action : Ouvrez le port du module d'écoute dans le pare-feu de la console de gestion.

### **Dépannage des messages d'erreur rencontrés lors de l'utilisation du composant Gestion à distance.**

Source : ZENworks 10 Configuration Management ; Gestion à distance.

Action : Pour dépanner les messages d'erreur rencontrés lors de l'utilisation du composant Gestion à distance, envoyez les fichiers `WinVNCApp.log` et `WinVNC.log` pour les périphériques Windows Vista ou le fichier `WinVNC.log` pour les autres périphériques gérés au [Support Novell \(http://support.novell.com\)](http://support.novell.com).

Pour accéder au fichier journal, procédez comme suit :

1. Ouvrez l'éditeur de registre.
2. Accédez à `HKLM\Software\Novell\ZENworks\Remote Management\Agent`.
3. Créez un DWORD nommé `DebugMode`, et définissez la valeur sur 2.
4. Créez un DWORD nommé `DebugLevel` et définissez la valeur hexadécimale sur `a` (la valeur décimale est 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
- ♦ WinVNCAApp.log (Windows Vista seulement)

**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 \(http://support.novell.com/search/kb\\_index.jsp\)](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 l'agent adaptatif ZENworks 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 distantes sur le périphérique, mais les performances sont 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 synchronisé (UTC) avec ce système. Si le problème persiste, contactez les Services Techniques de Novell.**

Source : ZENworks 10 Configuration Management ; Gestion à distance

Action : Lorsque le périphérique géré est mis à niveau ou enregistré, procédez de la façon suivante :

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

**Clé :** HKLM\Software\Novell\ZENworks

**Valeur :** CASubject

2. Importez le certificat CA de la nouvelle zone dans la zone de stockage des certificats racine fiables.
3. Supprimez le certificat CA de l'ancienne zone de la zone de stockage des certificats racine fiables.



**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 à l'aide de l'exécution à distance sont exécutées dans l'environnement WOW (Windows On Windows).

Action : Lancez les applications en utilisant les diagnostics 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 ou Windows Server 2008\***

Source : ZENworks 10 Configuration Management ; Gestion à distance.

Explication : Si vous lancez une opération de contrôle à distance sur un périphérique Windows Vista ou Windows Server 2008 pour lequel le contrôle de compte utilisateur (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 doté du navigateur Internet Explorer 7.**

Source : ZENworks 10 Configuration Management ; Gestion à distance.

Explication : Sur un périphérique Windows Vista doté du navigateur Internet Explorer 7, la *Visionneuse de gestion à distance* peut ne pas s'installer 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 voulez pas activer UAC, vous devez effectuer la mise à niveau vers Windows Vista SP1.

# 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.

- ♦ [Section A.1, « Détails de paire de clés du périphérique géré », page 75](#)
- ♦ [Section A.2, « Détails de paire de clés de l'opérateur distant », page 75](#)
- ♦ [Section A.3, « Détails du ticket de gestion distante », page 76](#)
- ♦ [Section A.4, « Détails de codage de session », page 76](#)

## A.1 Détails de paire de clés du périphérique géré

Certificat généré par : service de gestion à distance

Certificat généré en utilisant : OpenSSL v0.9.8e (version Novell)

Certificat signé par : autosigné

Certificat signé en utilisant : OpenSSL v0.9.8e (version Novell)

Certificat vérifié par : visionneuse de gestion à distance

Certificat vérifié en utilisant : OpenSSL v0.9.8e (version Novell)

Utilisé par : service de gestion à distance

Utilisé pour : établissement d'une session sécurisée avec la visionneuse de gestion à distance

Type de clé privée : RSA

Force de la clé : 1024 bits

Algorithme de signature : RSA-SHA256

Validité : 10 ans

## A.2 Détails de 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 la session : AES256-SHA

Mode d'authentification SSL : Mutuel/Serveur

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

- ♦ [Section B.1, « Fermeture du module d'écoute de gestion à distance », page 77](#)
- ♦ [Section B.2, « Fermeture des applications lancées lors de l'opération d'exécution à distance », page 77](#)
- ♦ [Section B.3, « Identification de l'opérateur à distance sur le périphérique géré », page 78](#)
- ♦ [Section 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 », page 78](#)
- ♦ [Section B.5, « Définition du nom de la console de gestion », page 78](#)
- ♦ [Section B.6, « Utilisation d'un thème Aero sur les périphériques Windows Vista et Windows Server 2008 », page 78](#)
- ♦ [Section 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 », page 79](#)
- ♦ [Section B.8, « Installation du service de gestion à distance sur un périphérique Windows XP à l'aide de RDP », page 79](#)
- ♦ [Section B.9, « Performances de la gestion à distance », page 79](#)

## 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 requêtes de session distante depuis le l'utilisateur du périphérique géré, ZENworks émet un ticket pour permettre à l'opérateur distant de s'authentifier auprès du périphérique géré. La durée de vie de ce ticket est de deux jours.

Le Module d'écoute de gestion à distance continue de s'exécuter même lorsque l'opérateur distant se délogue ou ferme le Centre de contrôle ZENworks. Si le ticket était toujours valide, tout autre opérateur distant pourrait utiliser le module d'écoute pour écouter les requêtes de session distante à partir des utilisateurs du périphérique géré. Pour des raisons de sécurité, vous devez fermer le module d'écoute de gestion à distance avant de vous déloguer 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 gestion à distance de ZENworks* 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 33](#).

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 d'un thème Aero sur les périphériques Windows Vista et Windows Server 2008

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.

## **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 \(http://support.microsoft.com/kb/952132\)](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 3.7, « Amélioration des performances de la gestion à distance », page 60](#)





# Mises à jour de la documentation

# C

Cette section contient des informations concernant les modifications de contenu de la documentation apportées par la présente *référence de ZENworks Remote Management* après la sortie initiale de Novell® ZENworks® 2 Configuration Management SP2. Les modifications sont répertoriées en fonction de leur date de publication.

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

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

La documentation a été mise à jour aux dates suivantes :

- ♦ [Section C.1, « Le 27 mai 2009 : SP2 \(10.2\) », page 81](#)

## C.1 Le 27 mai 2009 : SP2 (10.2)

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

- ♦ [Section C.1.1, « Présentation », page 81](#)
- ♦ [Section C.1.2, « Installation de la gestion à distance », page 81](#)
- ♦ [Section C.1.3, « Sécurité », page 82](#)

### C.1.1 Présentation

Les modifications suivantes ont été apportées :

Emplacement	Changer
<a href="#">Section 1.1, « Terminologie de la gestion à distance », page 11</a>	Cette section a été mise à jour.
<a href="#">Section 1.4, « Présentation du proxy de gestion à distance », page 16</a>	Section ajoutée.

### C.1.2 Installation de la gestion à distance

Les modifications suivantes ont été apportées :

Emplacement	Modification
<a href="#">Étape 6 page 18</a>	Informations supplémentaires sur la configuration du serveur de proxy de gestion à distance pour effectuer une opération à distance sur des périphériques NAT.

Emplacement	Modification
« Démarrage d'une opération de gestion à distance dans le Centre de contrôle ZENworks » page 34	Informations supplémentaires sur la spécification d'un serveur de proxy pour effectuer une opération à distance sur un périphérique NAT.
« Démarrage d'une opération de gestion à distance dans le Centre de contrôle ZENworks » page 34	Informations supplémentaires sur la fourniture de détails sur la paire de clés pour gérer à distance un périphérique si une autorité de certification externe est déployée dans la zone.
Section 2.9, « Installation d'un proxy de gestion à distance », page 47	Informations supplémentaires sur l'installation du serveur de proxy de gestion à distance.
« Démarrage d'une opération de gestion à distance en mode autonome » page 41	Mise à jour de la section.
« Démarrage d'une opération de gestion à distance à l'aide des options de ligne de commande » page 41	Mise à jour de la section.
Section 2.6, « Installation de la visionneuse de gestion à distance », page 32	Section ajoutée
Section 2.7, « Mise à niveau de la visionneuse de gestion à distance », page 33	Section ajoutée.

### C.1.3 Sécurité

Les modifications suivantes ont été apportées :

Emplacement	Changer
Section 4.1.1, « Authentification de la gestion à distance basée sur les droits », page 61	Cette section a été mise à jour.