

Fichier lisezmoi de ZENworks 2017 Update 4

Janvier 2019

Les informations reprises dans ce fichier lisezmoi concernent la version ZENworks 2017 Update 4.

- ♦ « Nouveautés de ZENworks 2017 Update 4 » page 1
- ♦ « Planification du déploiement de ZENworks 2017 Update 4 » page 1
- ♦ « Téléchargement et déploiement de ZENworks 2017 Update 4 » page 3
- ♦ « Problèmes résolus dans ZENworks 2017 Update 4 » page 4
- ♦ « Problèmes encore non résolus dans ZENworks 2017 Update 4 » page 4
- ♦ « Problèmes connus » page 4
- ♦ « Documentation supplémentaire » page 8
- ♦ « Mentions légales » page 8

Nouveautés de ZENworks 2017 Update 4

Pour plus d'informations sur les nouvelles fonctionnalités incluses dans cette version, reportez-vous au manuel [Nouveautés de ZENworks](#).

Planification du déploiement de ZENworks 2017 Update 4

Suivez les recommandations ci-dessous pour planifier le déploiement de ZENworks 2017 Update 4 dans votre zone de gestion :

- ♦ Si vous utilisez le chiffrement de disque et que vous souhaitez mettre à jour l'agent Full Disk Encryption à partir d'une version antérieure à ZENworks 2017 Update 1, vous DEVEZ supprimer la stratégie de chiffrement de disque de ces périphériques gérés avant de les mettre à jour vers ZENworks 2017 Update 4.

Si vous mettez à jour l'agent Full Disk Encryption depuis ZENworks 2017 Update 1 ou 2017 Update 2 vers ZENworks 2017 Update 4, conservez la stratégie de chiffrement de disque. Aucune modification n'est requise avant la mise à jour système.

Pour plus d'informations sur la mise à jour de Full Disk Encryption dans ZENworks 2017 4 à partir d'une version antérieure à ZENworks 2017 Update 1, reportez-vous au manuel ZENworks 2017 Update 1 - Full Disk Encryption Update Reference (ZENworks 2017 Update 1 - Référence de la mise à jour de Full Disk Encryption).

- ◆ Commencez par mettre à niveau les serveurs primaires, puis mettez à jour les serveurs satellites et enfin les périphériques gérés vers ZENworks 2017 Update 4. Ne procédez pas à la mise à niveau des périphériques gérés ni des serveurs satellites (ou n'ajoutez aucun nouvel agent ZENworks 2017 Update 4 dans la zone) avant d'avoir mis à niveau tous les serveurs primaires vers la version ZENworks 2017 Update 4.

REMARQUE : tant que tous les serveurs primaires n'ont pas été mis à niveau, les agents risquent de recevoir des données incohérentes de la zone. Cette partie du processus doit donc être effectuée aussi rapidement que possible, idéalement juste après la mise à niveau du premier serveur primaire.

- ◆ Vous pouvez déployer directement la version 2017 Update 4 sur les périphériques suivants :

Type de périphérique	Système d'exploitation	Version minimale de ZENworks
Serveurs primaires	Windows et Linux	ZENworks 2017 et versions ultérieures
Serveurs satellites	Windows, Linux et Mac	ZENworks 11.x et versions ultérieures
Périphériques gérés	Windows	ZENworks 11.x et versions ultérieures
	Linux	ZENworks 11.x et versions ultérieures
	Mac	ZENworks 11.2 et versions ultérieures

- ◆ Le système redémarre après la mise à niveau vers ZENworks 2017 Update 4. Deux redémarrages seront toutefois nécessaires dans les cas suivants :
 - ◆ Si vous effectuez une mise à jour de la version 11.x vers ZENworks 2017 ou une version ultérieure (2017 Update 1, Update 2, Update 3 ou Update 4) avec Endpoint Security activé, vous devez effectuer un deuxième redémarrage pour charger le pilote ZESNETAccess.
 - ◆ Si un périphérique géré utilise Windows 10 avec l'auto-défense du client activée et que vous effectuez une mise à niveau de la version 11.4.x vers ZENworks 2017 ou une version ultérieure (2017 Update 1, Update 2, Update 3 ou Update 4), vous devez désactiver l'auto-défense du client dans le centre de contrôle ZENworks, redémarrer le périphérique géré, puis exécuter la mise à jour, ce qui nécessite un deuxième redémarrage sur le périphérique.
 - ◆ Si une stratégie de chiffrement de disque est appliquée à un périphérique géré et que vous souhaitez mettre à jour l'agent Full Disk Encryption depuis une version antérieure à ZENworks 2017 Update 1 vers ZENworks 2017 Update 4, vous devez tout d'abord supprimer la stratégie et déchiffrer le périphérique, ce qui nécessite son redémarrage. Mettez ensuite à jour le périphérique vers 2017 Update 4, ce qui nécessite un deuxième redémarrage.

IMPORTANT : les périphériques gérés exécutant des versions antérieures à 11.x doivent tout d'abord être mis à niveau vers 11.x. Le système redémarre après la mise à niveau vers 11.x, puis à nouveau lorsque la mise à jour système ZENworks 2017 Update 4 est déployée.

- ♦ Avant d'installer la mise à jour système, assurez-vous de disposer de suffisamment d'espace libre aux emplacements suivants :

Emplacement	Description	Espace disque
Windows : %zenworks_home%\install\downloads Linux : opt/novell/zenworks/install/downloads	Pour mettre à jour les paquetages d'agent.	5,7 Go
Windows : %zenworks_home%\work\content-repo Linux : /var/opt/novell/zenworks/content-repo	Pour importer le fichier ZIP dans le système de contenu.	5,7 Go
Cache de l'agent	Pour télécharger le contenu de la mise à jour système nécessaire à la mise à jour du serveur ZENworks.	1,5 Go
Emplacement de copie du fichier de mise à jour système. cela s'applique uniquement au serveur ZENworks utilisé pour importer le fichier ZIP de mise à jour système	Pour stocker le fichier ZIP de mise à jour système qui a été téléchargé.	5,7 Go

Téléchargement et déploiement de ZENworks 2017 Update 4

Pour obtenir des instructions sur le téléchargement et le déploiement de ZENworks 2017 Update 4, consultez le document *ZENworks System Updates Reference* (Référence des mises à jour système ZENworks).

Si votre zone de gestion se compose de serveurs primaires comportant une version antérieure à ZENworks 2017, vous pouvez déployer ZENworks 2017 Update 4 sur ces serveurs uniquement après les avoir tous mis à niveau vers ZENworks 2017. Pour plus d'informations, reportez-vous au *Guide de mise à niveau de ZENworks*.

Pour les tâches d'administration, consultez la documentation relative à [ZENworks 2017 Update 4](#).

IMPORTANT : ne mettez pas à jour la visionneuse de gestion à distance (RM) tant que tous les serveurs satellites de proxy de jointure n'ont pas été mis à jour dans la zone. Pour exécuter la gestion à distance via le proxy de jointure, vous devez vous assurer que la version de la visionneuse RM et celle du proxy de jointure sont identiques.

Veillez lire la « [Planification du déploiement de ZENworks 2017 Update 4](#) » page 1 avant de télécharger et de déployer la mise à jour ZENworks 2017 Update 4.

IMPORTANT : lors du déploiement de la mise à jour de ZENworks, dans la phase de préparation, le service ZENworks Updater (ZeUS) sur les serveurs primaires est remplacé par le nouveau paquetage inclus dans la mise à jour.

Ne déployez pas ZENworks 2017 Update 4 tant que tous les serveurs primaires de la zone n'ont pas été mis à niveau vers ZENworks 2017.

Cette mise à jour nécessite des modifications du schéma de la base de données. Au cours de l'installation initiale du correctif, les services s'exécutent uniquement sur le serveur primaire dédié ou maître. De cette façon, les autres serveurs primaires n'essaient pas d'accéder aux tables en cours de modification dans la base de données.

Une fois que le serveur primaire dédié ou maître a été mis à jour, les services reprennent sur les serveurs restants et la mise à jour est appliquée simultanément.

REMARQUE : vous n'avez pas besoin d'arrêter ou de démarrer manuellement les services sur les serveurs au cours de la mise à jour. Les services sont arrêtés et démarrés automatiquement.

Lorsque vous reportez une mise à jour système et que vous vous déconnectez du périphérique géré, la mise à jour système est appliquée sur le périphérique.

Pour la liste des versions prises en charge des périphériques gérés et serveurs satellites dans une zone de gestion avec ZENworks 2017 Update 4, reportez-vous au document [Supported Managed Devices and Satellite Server Versions](#) (Versions prises en charge des périphériques gérés et serveurs satellites).

Problèmes résolus dans ZENworks 2017 Update 4

Certains des problèmes identifiés dans les versions précédentes ont été résolus dans cette version. Pour obtenir la liste des problèmes résolus, reportez-vous à l'article TID 7023612 de la [Base de connaissances du support technique](#).

Problèmes encore non résolus dans ZENworks 2017 Update 4

Certains des problèmes identifiés dans des versions antérieures à ZENworks 2017 Update 4 n'ont pas encore été résolus. Pour plus d'informations, consultez les fichiers lisezmoi suivants :

- ♦ [Fichier lisezmoi ZENworks 2017](#)
- ♦ [Fichier lisezmoi de ZENworks 2017 Update 1](#)
- ♦ [Fichier lisezmoi de ZENworks 2017 Update 2](#)
- ♦ [Fichier lisezmoi de ZENworks 2017 Update 3](#)

Problèmes connus

Cette section contient des informations relatives aux problèmes que vous pourriez rencontrer lors de l'utilisation de ZENworks 2017 Update 4 :

- ♦ « [Le pourcentage de luminosité défini dans le cadre de la stratégie de contrôle du périphérique mobile ne peut pas être appliqué aux périphériques Android](#) » page 5
- ♦ « [Non-prise en charge du démarrage direct sur les périphériques Android P \(9.0\)](#) » page 5
- ♦ « [Les paramètres de protection des touches du périphérique ne fonctionnent pas sur les périphériques dont l'appli ZENworks Agent est mise à niveau à partir d'une version antérieure vers la version 17.4.0](#) » page 5
- ♦ « [Les paramètres de protection des touches du périphérique ne s'appliquent pas aux périphériques Android Lollipop et Marshmallow enregistrés en mode Profil professionnel](#) » page 5
- ♦ « [La tâche rapide Déverrouiller le périphérique ne parvient pas à s'appliquer aux périphériques Android Lollipop et Marshmallow enregistrés en mode Profil professionnel](#) » page 6
- ♦ « [Après avoir mis à jour ZENworks, le RPM novell-zenworks-xplat-uninstall affiche une version incorrecte dans ZDC](#) » page 6
- ♦ « [Caractères indésirables dans le nom de dossier des périphériques Intel AMT](#) » page 6

- ♦ « La règle de contrôle d'accès Non approuvé ne bloque pas le trafic réseau sur les périphériques auxquels la stratégie de pare-feu de sécurité des noeuds d'extrémité est appliquée » page 6
- ♦ « La connexion à ZENworks en mode passif ne fonctionne pas après la mise à niveau vers Windows v1709, v1803 ou v1809 » page 6
- ♦ « Les tâches rapides et les mises à jour système ne sont pas exécutées sur les agents ZENworks » page 7
- ♦ « Le service novell-proxydhcp peut ne pas fonctionner sur les serveurs satellites de création d'image RHEL 7.5 et 7.6 » page 7

Le pourcentage de luminosité défini dans le cadre de la stratégie de contrôle du périphérique mobile ne peut pas être appliqué aux périphériques Android

Si une stratégie de contrôle du périphérique mobile, avec un pourcentage de luminosité spécifique défini dans le champ **Définir le pourcentage de luminosité**, est assignée à un périphérique géré par l'entreprise Android, la valeur de la luminosité ne s'applique pas au périphérique et un message d'erreur signalant que l'application n'est pas prise en charge s'affiche dans les messages État de la stratégie.

Solution : aucune.

Non-prise en charge du démarrage direct sur les périphériques Android P (9.0)

Comme le reconnaît Google, la fonction de démarrage direct ne fonctionne pas sur les périphériques Android P.

Solution : aucune.

Les paramètres de protection des touches du périphérique ne fonctionnent pas sur les périphériques dont l'appli ZENworks Agent est mise à niveau à partir d'une version antérieure vers la version 17.4.0

Lorsque l'appli ZENworks Agent sur un périphérique est mise à niveau vers la version 17.4.0, les paramètres de protection des touches du périphérique, activés dans le cadre de la stratégie de contrôle du périphérique mobile assignée, ne fonctionnent pas sur le périphérique.

Solution : annulez l'enregistrement du périphérique à l'aide de la tâche rapide **Annuler l'enregistrement** dans ZCC, puis réenregistrez-le. Réassignez la même stratégie de contrôle du périphérique mobile. Les paramètres de protection des touches du périphérique seront correctement activés sur le périphérique.

Les paramètres de protection des touches du périphérique ne s'appliquent pas aux périphériques Android Lollipop et Marshmallow enregistrés en mode Profil professionnel

Lorsque les paramètres de protection des touches du périphérique sont activés dans le cadre de la stratégie de contrôle du périphérique mobile, cette dernière ne parvient pas à s'appliquer aux périphériques Android Lollipop et Marshmallow qui sont enregistrés en mode Profil professionnel. L'état de la stratégie apparaît comme ayant échoué dans ZCC et un message d'erreur indiquant qu'il n'est pas possible de définir la configuration des agents de confiance pour un profil géré est consigné dans les journaux des périphériques.

Solution : aucune.

La tâche rapide Déverrouiller le périphérique ne parvient pas à s'appliquer aux périphériques Android Lollipop et Marshmallow enregistrés en mode Profil professionnel

La tâche rapide Déverrouiller le périphérique ne parvient pas à s'appliquer aux périphériques Android Lollipop et Marshmallow qui sont enregistrés en mode Profil professionnel. L'état de la tâche rapide est affiché comme ayant échoué dans ZCC et un message d'erreur indiquant qu'il n'est pas possible de réinitialiser le mot de passe pour un profil géré est consigné dans les journaux des périphériques.

Solution : aucune.

Après avoir mis à jour ZENworks, le RPM novell-zenworks-xplat-uninstall affiche une version incorrecte dans ZDC

Après avoir mis à niveau la zone de gestion ZENworks, le RPM novell-zenworks-xplat-uninstall affiche une version incorrecte dans ZDC.

Solution : aucune.

Attendez que l'opération de rafraîchissement soit effectuée sur le serveur primaire.

Caractères indésirables dans le nom de dossier des périphériques Intel AMT

Dans **ZCC > Périphériques** > onglet **Découvert**, des caractères indésirables apparaissent dans le nom de dossier **Périphériques Intel AMT**.

Solution : aucune.

La règle de contrôle d'accès Non approuvé ne bloque pas le trafic réseau sur les périphériques auxquels la stratégie de pare-feu de sécurité des noeuds d'extrémité est appliquée

Lorsqu'une liste de contrôle d'accès (ACL) est configurée avec une ou plusieurs règles ACL Non approuvé dans la stratégie de pare-feu, l'accès réseau basé sur les paramètres de règle n'est pas bloqué.

Solution : utilisez les configurations natives de port du pare-feu pour bloquer l'accès réseau.

La connexion à ZENworks en mode passif ne fonctionne pas après la mise à niveau vers Windows v1709, v1803 ou v1809

Après avoir mis à niveau le périphérique vers Windows 10 v1709 (Fall Creator Update), v1803 ou Windows 10 v1809 (April 2018 Update), la connexion à ZENworks en mode passif ne fonctionne pas.

Solution : reportez-vous au document TID 7022478 dans la [base de connaissances](#) de Micro Focus.

Les tâches rapides et les mises à jour système ne sont pas exécutées sur les agents ZENworks

Lorsque vous assignez une tâche rapide ou une mise à jour système à un agent ZENworks, la tâche ou la mise à jour assignée n'est pas exécutée sur l'agent, et un message **TaskNotifier** signalant le renvoi d'une erreur 503 par le serveur est consigné dans le journal ZeUS.

Pour vérifier l'erreur 503 TaskNotifier, procédez comme suit :

1. Sur l'agent, dans l'application du technicien (cliquez avec le bouton droit sur l'**icône ZENworks**, sélectionnez **Application du technicien**), la consignation doit être définie sur **Erreurs, Avertissements, Info, Débogage**.
2. Après avoir modifié le niveau de journalisation sur l'agent, assignez une quelconque tâche rapide ou mise à jour système.
3. Un message **TaskNotifier** signalant que le serveur a renvoyé une erreur 503 est consigné dans le fichier `zeus-messages.log` (emplacement : `%ZENWORKS_HOME%\ZeUS\logs\`).

Le message d'erreur **TaskNotifier** indique que le serveur a refusé la connexion, car il est pratiquement au maximum de sa capacité par défaut (10000).

Cette erreur se produit lorsque le nombre d'agents se connectant à un serveur est trop important par rapport à la valeur `maxConnections` du fichier `server.xml`. Par défaut, la valeur `maxConnections` est de 10000.

Solution :

Ajoutez le paramètre `maxConnections` au fichier `server.xml`.

Pour ajouter la valeur maxConnections au fichier server.xml :

1. Au niveau de la ligne suivante du fichier `server.xml`, ajoutez le paramètre `maxConnections="20000"`, comme illustré ci-dessous :

```
<!-- Définir un connecteur non-SSL HTTP/1.1 sur le port 80 --> <Connector acceptCount="1000"
connectionTimeout="60000" maxConnections="20000" disableUploadTimeout="true"
enableLookups="false" maxHttpHeaderSize="8192" maxSpareThreads="75" maxThreads="600"
minSpareThreads="25" port="80" protocol="org.apache.coyote.http11.Http11NioProtocol"
redirectPort="443" />
```

REMARQUE : par défaut, la valeur du paramètre `maxConnections` est de 10000 et n'est pas listée dans le fichier `server.xml`. Si le nombre 10000 n'est pas suffisant, ajoutez le paramètre et augmentez sa valeur en fonction du nombre d'agents dans la zone. Dans cet exemple, le nombre `maxConnections` est de 20000.

2. Redémarrez les services ZENworks.

Le service novell-proxydhcp peut ne pas fonctionner sur les serveurs satellites de création d'image RHEL 7.5 et 7.6

Le service `novell-proxydhcp` peut ne pas fonctionner sous RHEL 7.5 et 7.6, car le port 67 dont il a besoin est utilisé par le service `dnsmasq`.

Solution : exécutez la commande `systemctl disable libvirt.service`, puis redémarrez le périphérique :

Documentation supplémentaire

Ce document contient des informations spécifiques à la version ZENworks 2017 Update 4. Pour consulter la documentation de ZENworks 2017, reportez-vous au [site Web de documentation de ZENworks 2017](#).

Mentions légales

Pour plus d'informations sur les mentions légales, les marques, les exclusions de garantie, les garanties, les limitations en matière d'exportation et d'utilisation, les droits du gouvernement américain, la politique relative aux brevets et la compatibilité avec la norme FIPS, consultez le site <https://www.novell.com/company/legal/>.

© Copyright 2008 - 2019 Micro Focus ou l'une de ses sociétés affiliées.

Les seules garanties pour les produits et services de Micro Focus et ses sociétés affiliées et concédants de licence (« Micro Focus ») sont définies dans les clauses de garantie expresse qui accompagnent ces produits et services. Rien dans le présent accord ne doit être interprété comme constituant une garantie supplémentaire. Micro Focus ne sera en aucun cas tenu responsable des erreurs ou omissions techniques ou de rédaction contenues dans ce document. Les informations contenues dans le présent document sont susceptibles de changer sans préavis.