ZENworks 2020 Update 2

Nouveautés

Août 2021

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/.

Table des matières

À propos de ce guide

Ce manuel *Nouveautés de ZENworks* décrit les nouvelles fonctionnalités de la version ZENworks 2020 Update 2. Ce guide comporte les sections suivantes :

Public

Le présent guide est destiné aux administrateurs de ZENworks.

Commentaires

Nous souhaiterions connaître vos commentaires et suggestions sur ce guide et les autres documentations fournies avec ce produit. Utilisez la fonction **Commenter cette rubrique** disponible au bas de chaque page de la documentation en ligne.

Documentation supplémentaire

D'autres manuels (aux formats PDF et HTML) viennent compléter la documentation relative à ZENworks. Ils facilitent l'apprentissage et la mise en œuvre de ce produit. Pour de la documentation supplémentaire, reportez-vous au site Web de documentation de ZENworks.

1 Nouveautés de ZENworks 2020 Update 2

Les sections suivantes décrivent les nouvelles fonctionnalités et améliorations apportées dans ZENworks 2020 Update 2 :

Prise en charge des plates-formes

Les nouvelles plates-formes suivantes sont prises en charge dans cette version :

- CentOS en tant que périphérique géré
- macOS 11 (Big Sur) en tant que périphérique géré
- Android 11
- iOS 14
- SLES 15 SP2
  - SLES 15 SP2 (serveur primaire)
  - SLES 15 SP2 (périphérique géré - y compris SLES for SAP)
  - SLED 15 SP2 (périphérique géré)
- Nouvelles plates-formes RHEL et Scientific Linux
  - Scientific Linux 7.7 et 7.8
  - RHEL 7.8 et 8.2

Installation et mise à niveau

Dans la mesure où ZENworks vise à adopter une architecture plus robuste et plus flexible, et à s'aligner sur les normes Micro Focus, certaines améliorations ont été apportées au processus d'installation et de mise à niveau dans la version ZENworks 2020 Update 2. Les modifications apportées dans cette version sont les suivantes :

Installation de Docker et Docker Compose

Avant d'installer ZENworks 2020 Update 2 ou d'effectuer la mise à niveau sur un serveur Linux primaire, vous devez installer Docker et Docker Compose sur ce dernier. Pour plus d'informations sur les produits Docker, consultez le site https://docs.docker.com/.

Migration des données du serveur vers un nouveau chemin de fichier

Après la mise à niveau vers ZENworks 2020 Update 2 sur un serveur Windows, Linux ou d'applicatifs primaire, les données ZENworks Server telles que les fichiers MSI, RPM, journaux et les fichiers de configuration qui se trouvaient précédemment dans le chemin d'accès aux fichiers Novell sont déplacées vers le nouveau chemin d'accès aux fichiers Micro Focus.

Par exemple, sur un serveur Linux, les fichiers de configuration qui se trouvaient précédemment dans `/etc/opt/novell/zenworks` sont désormais disponibles dans `/etc/opt/microfocus/zenworks`. De même, sur un serveur Windows, les fichiers de configuration qui se trouvaient précédemment dans `C:\Program Files (x86)\Novell\ZENworks\conf` sont désormais disponibles dans `C:\Program Files (x86)\Micro Focus\ZENworks\conf`.

Les fichiers et données associés à l'agent ZENworks sont conservés à l'ancien emplacement Novell.

Changement de nom des services du serveur ZENworks

Après la mise à niveau vers ZENworks 2020 Update 2 sur un serveur Windows, Linux ou d'applicatifs primaire, certains services du serveur ZENworks, tels que les services ZENserver, ZENloader et ZENjoinproxy, sont renommés de Novell en Micro Focus. Par exemple, sur un serveur Linux, `novell-zenserver.service` sera renommé `microfocus-zenserver.service`.

Introduction d'une nouvelle variable d'environnement

Pour un serveur Windows, une nouvelle variable d'environnement `%ZENSERVER_HOME%` a été ajoutée afin de pointer vers l'emplacement d'installation du serveur pour un chemin autre que celui par défaut (`C:\Program Files(x86)\Micro Focus\ZENworks`.)

Version TLS

Si vous avez récemment installé ZENworks 2020 Update 2, TLS 1.2 est activé par défaut dans la zone et lorsque vous essayez d'enregistrer des périphériques avec une version de Microsoft .NET antérieure à 4.7, l'enregistrement du périphérique échoue. Toutefois, l'agent est installé sur le périphérique.

Si vous mettez à niveau une zone existante vers ZENworks 2020 Update 2, TLS 1.2 n'est pas activé par défaut. Si vous activez TLS 1.2 dans la zone, certaines fonctionnalités risquent de ne pas fonctionner comme prévu ; veillez par ailleurs à installer Microsoft .NET 4.7 sur tous les périphériques de la zone.

Si vous avez activé TLS 1.2 dans la zone, pour enregistrer le périphérique, celui-ci doit être équipé de Microsoft .NET 4.7.

Remplacement des serveurs primaires

Pour plus d'informations sur le remplacement du premier serveur primaire par le deuxième serveur primaire ou sur le remplacement d'un serveur primaire existant par un nouveau serveur primaire, reportez-vous à la section *Replacing Primary Servers* (Remplacement des serveurs primaires) du manuel *ZENworks Disaster Recovery Reference* (Référence de reprise après sinistre de ZENworks).

Déplacement d'un serveur primaire vers un applicatif

Pour plus de détails sur la procédure de déplacement d'un serveur primaire existant (Windows ou Linux) vers un serveur d'applicatifs, reportez-vous à la section *Moving from a Windows or Linux Primary Server to Appliance* (Déplacement d'un serveur Windows ou Linux primaire vers l'applicatif) du manuel *ZENworks Primary Server and Satellite Reference* (Référence de serveur primaire et satellite ZENworks).

ZENworks Configuration Management

Gestion des périphériques Windows 10

Dans la version ZENworks 2020 Update 2, de nouvelles fonctionnalités ont été ajoutées pour vous permettre de gérer l'intégralité du cycle de vie des périphériques Windows 10 à l'aide de l'agent MDM intégré à ces derniers. Pour résoudre les cas d'utilisation qui dépassent les fonctionnalités des périphériques Windows 10, vous pouvez également déployer l'agent ZENworks sur les périphériques qui utilisent les agents Windows 10 MDM.

Pour plus d'informations sur chacune des fonctionnalités répertoriées dans cette section, reportez-vous au manuel Windows MDM Reference (Référence de Windows MDM).

Les nouvelles fonctionnalités sont les suivantes :

Fonctionnalités de configuration

Vous pouvez désormais configurer le service de notification Windows (WNS) pour envoyer des notifications Push aux périphériques Windows gérés via Windows Modern Management.

Fonctionnalités d'enregistrement

Les fonctionnalités d'enregistrement suivantes ont été introduites.

Méthodes d'enregistrement : les périphériques Windows 10 peuvent être enregistrés auprès de ZENworks à l'aide des méthodes suivantes.

- Enregistrement du paquetage de provisioning (PPKG)
- Jointure Azure Active Directory (Azure AD)
- Enregistrement AutoPilot

Déploiement de ZENworks Agent : vous pouvez désormais déployer ZENworks Agent sur des périphériques Windows 10 déjà enregistrés à l'aide du mode d'enregistrement MDM.

Configuration des conditions d'utilisation : vous pouvez assigner la stratégie des conditions d'utilisation aux périphériques pour ajouter le contenu des conditions d'utilisation à afficher sur l'agent lors de l'enregistrement des périphériques Windows 10 à l'aide de l'enregistrement Azure AD Join ou Auto Pilot.

Fonctionnalités de gestion

Les fonctionnalités de gestion suivantes ont été introduites :

Déploiement des ensembles Windows 10 MDM : vous pouvez désormais déployer les ensembles suivants sur des périphériques Windows 10 MDM :

REMARQUE : la prise en charge de ces ensembles s'effectue à titre expérimental et ne doit être utilisée qu'à des fins d'évaluation.

- À l'aide de l'ensemble Windows 10 MDM - Installer MSI, déployez un paquetage Microsoft Installer (MSI) sur les périphériques Windows 10 MDM.
- À l'aide de l'ensemble Windows 10 MDM CSP, distribuez des fournisseurs de services de configuration (CSP) pour déployer les différentes configurations disponibles via des CSP sur des périphériques Windows 10 MDM.

Lancement de tâches rapides : les tâches rapides suivantes sont prises en charge sur les périphériques Windows 10 MDM :

- Supprimer le périphérique
- Supprimer le périphérique du registre
- Retirer un périphérique
- Annuler le retrait d'un périphérique
- Périphérique perdu
- Annuler l'enregistrement du périphérique

Autres fonctionnalités

Certaines des autres fonctionnalités introduites pour la fonction Windows 10 MDM sont les suivantes :

- Les périphériques Windows 10 prennent en charge le rapprochement automatique.

- Le processus de renouvellement de l'autorité de certification émet désormais des certificats vers les périphériques Windows 10 MDM.
- Le paramètre de l'API MS Graph a été renommé Application Azure MDM et doit être reconfiguré pour bénéficier des nouvelles améliorations apportées dans cette version.

Démarrage de Modern Management

La page Mobile Management Getting Started (Démarrage de ZENworks Mobile Management) a été révisée pour inclure également l'enregistrement et la gestion des périphériques Windows 10 MDM. Pour plus d'informations, reportez-vous au manuel Modern Management Reference (Référence de Modern Management).

Imagerie ZENworks

Restauration de l'image à l'aide du nom d'ensemble sous WinPE : sous ZENworks 2020 Update 1 et les versions antérieures, la distribution WinPE prenait en charge la restauration de l'image en fournissant le nom de l'image à l'aide de la commande IMG, et la commande ne reconnaissait pas si l'ensemble était transmis via la commande. À partir de ZENworks 2020 Update 2, les commandes d'ensemble IMG sont prises en charge sur la distribution WinPE. Pour plus d'informations, reportez-vous au guide Référence de la création d'image et des services de pré-lancement de ZENworks.

Nouvel outil pour lire les informations d'image ZENworks : l'outil zmginfo permet de rassembler des informations sur une image. Cela est particulièrement utile pour gagner du temps lorsque l'espace de stockage ou le chemin partagé contient plusieurs images et que vous devez collecter des informations sur chaque d'elles. À l'aide de l'outil zmginfo, vous pouvez rassembler les informations de base ou complètes sur l'image. zmginfo permet également à l'administrateur de créer l'ensemble XML pouvant être importé en tant qu'ensemble et utilisé pour convertir toutes les images de base Linux en images de base WinPE.

Pour plus d'informations, reportez-vous au guide Référence de la création d'image et des services de pré-lancement de ZENworks.

ZENworks Remote Management

Contrôle à distance d'un périphérique ayant une session RDP active : vous pouvez désormais lancer une session à distance sur un périphérique avec une session RDP active, tout comme une session de gestion à distance normale. Pour plus d'informations, reportez-vous au guide Remote Management Reference (Référence de gestion à distance).

Enregistrement d'une session de gestion à distance (support expérimental) : permet aux utilisateurs du périphérique géré d'enregistrer la session de gestion à distance. Pour plus d'informations, reportez-vous au guide Remote Management Reference (Référence de gestion à distance).

Mobile Management

Activation des assignations de périphériques pour les ensembles Android : les ensembles Android créés pour les applications Play Store approuvées qui étaient auparavant limitées aux assignations d'utilisateurs peuvent désormais également être assignés à des périphériques. Pour plus d'informations, reportez-vous au manuel Mobile Management Reference (Référence de Mobile Management).

Provisioning d'applications système : à l'aide de la fonction Ensembles, vous pouvez activer ou désactiver les applications système sur les périphériques Android. Les applications système sont des applications intégrées qui sont déjà préinstallées sur le périphérique. Pour plus d'informations, reportez-vous au manuel Mobile Management Reference (Référence de Mobile Management).

Démarrage de Modern Management : la page Mobile Management Getting Started (Démarrage de ZENworks Mobile Management) a été révisée pour inclure également l'enregistrement et la gestion des périphériques Windows 10 MDM. En outre, certaines fonctionnalités supplémentaires associées à l'enregistrement et à la gestion des périphériques Apple et Android ont été incluses dans cette page. Pour plus d'informations, reportez-vous au manuel Modern Management Reference (Référence de Modern Management).

Modification de l'emplacement du journal des périphériques Android Les journaux de l'application ZENworks sur les périphériques Android se trouvent désormais à l'emplacement `Android/data/com.novell.zapp/files/Documents/zapp.log`. Pour partager ces journaux, vous devez déployer l'application Files sur les périphériques Android.

Gestion des ensembles

Une nouvelle option **Continuer en cas d'échec** a été introduite dans le workflow Copier des relations. Lors de la copie de relations d'un périphérique vers un autre ensemble d'objets, si une erreur se produit, l'opération se poursuit pour le reste des objets. Les détails des erreurs s'affichent à la fin de l'opération, ainsi qu'une option permettant d'exporter les détails de l'opération pour référence et action. Pour plus d'informations, reportez-vous au manuel Référence de distribution des logiciels.

Divers

Possibilité pour les clients d'utiliser la dernière version du paquetage puppet-agent : auparavant, ZENworks fournissait le paquetage puppet-agent en tant que partie intégrante du build, ce qui permettait aux utilisateurs d'utiliser la stratégie Puppet. Cependant, avec les mises à jour continues de la version de puppet-agent, postérieures à la version de ZENworks, les utilisateurs ne pouvaient pas utiliser la version la plus récente du paquetage. À partir de cette version, pour que la stratégie Puppet soit effective sur les périphériques gérés Linux ZENworks 2020 Update 2 et versions ultérieures, vous devez vous assurer que le paquetage puppet-agent est installé sur ces périphériques. Pour plus d'informations, reportez-vous au manuel Configuration Policies Reference (Référence des stratégies de configuration).

Améliorations de la sécurité dans ZENworks

Les améliorations de sécurité introduites dans cette version vous permettent d'enregistrer et de communiquer en toute sécurité avec les périphériques, même dans un environnement de zone démilitarisée (DMZ).

- Si vous venez d'installer ZENworks 2020 Update 2, les paramètres de sécurité sont activés par défaut sur tous les serveurs primaires.
- Si vous mettez à niveau les serveurs primaires, les paramètres de sécurité sont désactivés par défaut.
- Si vous avez ajouté un nouveau serveur primaire à la zone, après la mise à niveau vers ZENworks 2020 Update 2, les paramètres de sécurité sont activés par défaut.

Pour activer les paramètres, vous devez exécuter la commande zman suivante :

- `zman ssassc` (Security-Set-Agent-Server-Secure-Communication) permet d'activer ou de désactiver l'authentification pour la communication entre l'agent ZENworks et les serveurs ZENworks.

Pour plus d'informations sur les améliorations de sécurité introduites dans cette version, reportez-vous au manuel ZENworks Securing Devices Reference (Référence de sécurisation des périphériques ZENworks).

Enregistrement des périphériques

Pré-approbation de l'enregistrement des périphériques

Les périphériques pré-approuvés sont les périphériques approuvés par les administrateurs pour faire partie de la zone. Cette fonction est particulièrement utile lorsque vous devez pré-approuver des périphériques lors de l'enregistrement en bloc d'un ensemble connu de périphériques. Elle peut également être utilisée pour permettre le rapprochement de périphériques connus, si nécessaire.

Utilisation de la clé d'autorisation

Une clé d'autorisation peut être utilisée par l'agent ZENworks pour s'autoriser lui-même à s'enregistrer auprès de la zone et pour toute communication avec le serveur au cours de l'installation.

Sécurisation de l'enregistrement des périphériques gérés et iOA

Pour enregistrer de nouveaux agents iOA ou un périphérique géré auprès de la zone, vous devez spécifier une clé d'autorisation lors de l'enregistrement du périphérique ou vous assurer que le périphérique fait partie de la liste des périphériques pré-approuvés.

Communication des périphériques

Utilisation d'OSP pour la communication des périphériques, y compris la connexion à ZCC

Pour la plupart des fonctions, ZENworks utilise désormais le protocole O-Auth afin d'établir l'identité des utilisateurs. Par conséquent, un nouveau service appelé OSP a été introduit et est utilisé pour la connexion à ZCC, la communication inter-services et la communication entre les périphériques et les serveurs.

Sécurisation du contenu et de la collecte entre les périphériques, les serveurs primaires et les serveurs satellites

Avec l'introduction de cette nouvelle fonction de sécurité, la collecte et le transfert de contenu de bout en bout entre les périphériques gérés, les serveurs primaires et les serveurs satellites s'effectuent via SSL. Pour ce faire, vous devez configurer le paramètre dans ZCC ou utiliser les commandes zman nouvellement introduites.

Sécurisation de la communication de service Web entre le périphérique et le serveur primaire ou satellite

Pour sécuriser davantage la communication de service Web entre l'agent ZENworks et les serveurs ZENworks primaires et satellites, des améliorations de sécurité ont été apportées aux appels de service Web dans cette version.

Exclusions d'unités de la stratégie de chiffrement des données Microsoft

Les unités de données amovibles peuvent désormais être exclues du chiffrement par type d'unité dans la stratégie de chiffrement des données Microsoft lorsque la stratégie est appliquée sur des périphériques gérés.

Logiciel anti-programme malveillant

ZENworks Antimalware est un nouveau composant de ZENworks Endpoint Security Management sous le groupe Sécurité dans le Centre de contrôle ZENworks. Antimalware est une solution compressive qui protège les périphériques gérés contre toutes les menaces de logiciels malveillants les plus récentes. Lorsqu'il est déployé sur les périphériques de votre zone, l'agent Antimalware reçoit en permanence des mises à jour des fichiers de signature de logiciels malveillants de la part du service cloud Antimalware afin de détecter les infections de logiciels malveillants à l'aide d'analyses sur accès et à la demande. Les fichiers infectés sont mis en quarantaine jusqu'à ce qu'ils soient désinfectés.

Pour plus d'informations sur les rubriques de cette section, reportez-vous au document suivant :

- ZENworks Endpoint Security Antimalware Reference (Référence de ZENworks Endpoint Security Antimalware)

Protection contre les logiciels malveillants - Page Démarrage

La page Démarrage de la sécurité comprend une page à onglets supplémentaire intitulée « Protection contre les logiciels malveillants ». Vous pouvez utiliser cette page comme point d'accès unique pour configurer, déployer et personnaliser toutes les fonctions offertes par ZENworks Antimalware.

Droit de mise à jour Antimalware

Le droit de mise à jour Antimalware est requis pour déployer des stratégies Antimalware sur les périphériques. Le droit est automatiquement activé pour la période d'évaluation lors de l'activation de Endpoint Security Management en mode d'évaluation.

Stratégies Windows Endpoint Security

Quatre nouvelles stratégies sont utilisées pour gérer le déploiement, la personnalisation et la continuité d'Antimalware :

Stratégie d'application Antimalware : il s'agit de la stratégie de base qui installe l'agent Antimalware sur les périphériques gérés. Cette stratégie doit être déployée pour utiliser n'importe laquelle des autres stratégies Antimalware. Elle comprend des configurations pour tous les types d'analyses de logiciels malveillants, y compris les analyses sur accès et à la demande, complètes, rapides, contextuelles et de périphériques externes. Il existe également des paramètres pour le comportement de mise en quarantaine et la définition de contenus à exclure des analyses.

Si les paramètres par défaut des notifications et des droits de l'utilisateur final sont conservés lors du déploiement de la stratégie, les utilisateurs finaux ont accès à la console État des agents sur leurs noeuds d'extrémité, ce qui leur permet de lancer leurs propres analyses, d'afficher l'état de l'analyse et de la mise à jour de l'agent, et de recevoir des notifications de l'activité de l'agent contrôlée par la stratégie.

Stratégie d'exclusion d'analyse Antimalware : Antimalware comporte des exclusions d'analyse qui sont à la fois des exclusions d'analyse intégrées et personnalisées que vous pouvez ajouter à n'importe quelle stratégie Antimalware. La stratégie d'exclusion d'analyse est utilisée par l'assignation de périphérique lorsque d'autres stratégies Antimalware sont également assignées aux mêmes périphériques, ce qui simplifie la propagation des exclusions d'analyse dans la zone. Les exclusions peuvent être activées ou désactivées pour des types d'analyse spécifiques.

Stratégie d'analyse personnalisée Antimalware : la stratégie d'analyse personnalisée est utilisée pour une approche plus ciblée afin d'analyser les unités locales sur les périphériques gérés lorsqu'une menace spécifique est suspectée ou pour cibler les analyses sur des emplacements spécifiques de ces périphériques. Elle inclut sa propre planification, contrairement à la planification de zone configurée pour la stratégie d'application Antimalware.

Stratégie d'analyse réseau Antimalware : la stratégie d'analyse réseau est également utilisée pour une approche plus ciblée, mais elle sert explicitement pour l'analyse des dossiers et des fichiers sur les unités réseau. Elle possède également sa propre planification et inclut un paramètre supplémentaire pour l'authentification auprès des emplacements réseau.

Dashlets de sécurité Antimalware

Quatre nouveaux dashlets qui s'affichent par défaut dans le tableau de bord de sécurité permettent de surveiller les menaces, les analyses et les mises à jour de signatures concernant les logiciels malveillants.

État du périphérique concernant les logiciels malveillants : ce dashlet affiche l'état relatif aux logiciels malveillants de périphériques individuels de la zone concernant une période de détection sélectionnée.

Dernière analyse des logiciels malveillants du périphérique : ce dashlet affiche l'état de santé des périphériques de votre zone par rapport aux menaces de logiciels malveillants. Par défaut, il affiche des informations sur tout type d'analyse effectuée sur les périphériques pendant une période donnée.

Principales menaces des logiciels malveillants : ce dashlet affiche la liste des principales menaces des logiciels malveillants dans la zone. Par défaut, celles-ci apparaissent en fonction du nombre de périphériques infectés.

Version de la signature des logiciels malveillants du périphérique : ce dashlet affiche la liste des versions des signatures de logiciels malveillants et des versions de l'agent Antimalware installées sur les périphériques de la zone.

Page Antimalware des périphériques

Cette page est un nouvel onglet accessible lorsqu'un périphérique est sélectionné. Elle fournit un instantané de l'état des menaces de logiciels malveillants, la planification de l'analyse et des informations sur les fichiers mis en quarantaine pour le périphérique sélectionné. Vous pouvez également effectuer des opérations spécifiques sur les fichiers, lancer des analyses et mettre à jour les versions de l'agent Antimalware et des signatures de logiciels malveillants sur le périphérique.

Page des détails des menaces de logiciels malveillants

Pour accéder à cette page, cliquez sur un lien de menace de logiciel malveillant dans la section Menaces de logiciels malveillants de la page Antimalware d'un périphérique. Elle fournit des informations détaillées sur la menace sélectionnée et des détails sur les périphériques infectés par cette dernière.

Tâches rapides Antimalware

Lorsqu'un ou plusieurs périphériques sur lesquels l'agent Antimalware est installé sont sélectionnés dans le groupe Périphériques du centre de contrôle ZENworks, cinq nouvelles tâches rapides peuvent être exécutées sur ces périphériques. Il s'agit des tâches rapides suivantes :

- Lancer l'analyse des logiciels malveillants
- Mettre à jour la signature des logiciels malveillants
- Mettre à jour l'agent Antimalware
- Restaurer le fichier depuis la quarantaine
- Supprimer le fichier de la quarantaine

Commandes zac Antimalware

Antimalware est fourni avec plusieurs nouvelles commandes zac spécifiques à ce composant. Il s'agit notamment de commandes permettant de lancer des analyses de logiciels malveillants sur les périphériques, de vérifier l'état de l'agent Antimalware concernant les logiciels malveillants, d'installer, de mettre à jour ou de supprimer l'agent, et de supprimer des fichiers de la quarantaine.

Pages de configuration de zone Antimalware

Trois nouvelles pages de configuration de zone sont désormais incluses dans le groupe Sécurité de la page de configuration ZENworks principale. Chacune de ces pages inclut des paramètres par défaut que vous pouvez personnaliser. Ces pages sont les suivantes :

Planifications de l'agent Antimalware : permet de configurer les planifications des analyses de logiciels malveillants et des mises à jour de signatures de logiciels malveillants. Vous pouvez ignorer cette planification au niveau du périphérique ou du dossier de périphériques.

Notifications de l'agent Antimalware : permet de configurer les alertes et les notifications affichées par l'agent Antimalware sur les périphériques gérés. Vous pouvez remplacer ces paramètres au niveau du périphérique et du dossier de périphériques.

Configuration Antimalware : permet de définir le serveur ZENworks primaire à utiliser comme serveur Antimalware, qui doit être configuré manuellement pour déployer le composant Antimalware. Permet également de configurer la planification de maintenance de l'agent Antimalware.

Page de configuration du contenu à la demande

Cette nouvelle page de configuration de zone est désormais incluse dans les groupes Ensemble, Stratégie et Contenu de la page de configuration ZENworks principale. Elle gère le taux de téléchargement du contenu et la taille du cache de contenu pour la distribution de contenu dans la zone, notamment les fichiers de signature Antimalware et les mises à jour de l'agent Antimalware.

État du service Antimalware

L'état du service Antimalware est désormais accessible sur la page Diagnostic de ZCC.

Base de données Antimalware

La base de données Antimalware est une nouveauté de ZENworks 2020 Update 2. Son objectif est de fournir des données pour les fonctionnalités de surveillance d'Antimalware via la page Antimalware et les dashlets de sécurité Antimalware. Une fois configurée, cette base de données se synchronise avec la base de données ZENworks et doit donc être du même type. Par exemple : PostgreSQL, Microsoft SQL Server ou Oracle.

La base de données Antimalware est configurée à partir de la page Protection contre les logiciels malveillants - Démarrage pour la sécurité dans le centre de contrôle ZENworks. Si la base de données Antimalware doit être configurée à l'aide d'une base de données externe qui n'existe pas encore, vous pouvez en créer une à partir d'une commande CLI à l'aide du fichier `setup.exe`.