paloalto TECHDOCS

Guide de mise à niveau de PAN-OS

11.0

docs.paloaltonetworks.com

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Last Revised

March 29, 2023

Table of Contents

Mises à jour logicielles et de contenu

PAN-OS est le logiciel qui exécute tous les pare-feu nouvelle génération de Palo Alto Networks. De plus, Palo Alto Networks publie fréquemment des mises à jour pour équiper le pare-feu des fonctions de sécurité les plus récentes. Le pare-feu peut appliquer la politique en fonction des signatures des applications et des menaces (et plus) qui les mises à jour de contenu fournissent, sans vous obliger à mettre à jour la configuration du pare-feu.

Après avoir téléchargé et installé avec succès une mise à jour du logiciel PAN-OS sur votre pare-feu physique, la mise à jour de logiciel est validée après le redémarrage du pare-feu physique dans le cadre de la procédure d’installation du logiciel afin de garantir l’intégrité du logiciel PAN-OS. Cela permet de s'assurer que la nouvelle mise à jour du logiciel en cours d'exécution est bonne et que le pare-feu n'est pas compromis par une exploitation à distance ou physique.

Mises à jour logicielles de PAN-OS

PAN-OS est le logiciel qui exécute tous les pare-feu nouvelle génération de Palo Alto Networks. La version du logiciel PAN-OS qu'un pare-feu utilise s'affiche sur le **Dashboard (Tableau de bord)** du pare-feu.

Vous pouvez vérifier la présence de nouvelles versions de PAN-OS directement dans le pare-feu ou sur le portail d'assistance de Palo Alto Networks. Pour mettre à niveau le pare-feu vers la dernière version de PAN-OS :

STEP 1 | Passez en revue les dernières Notes de version PAN-OS pour prendre connaissance des nouveautés. Jetez également un coup d'œil à Considérations de mise à niveau/rétrogradation pour vous assurer que vous comprenez tous les changements potentiels que la version PAN-OS pourrait introduire.

STEP 2 | Vérifiez la présence de nouvelles versions PAN-OS :

- **On the support portal (Sur le portail d'assistance)** : accédez à support.paloaltonetworks.com et, sur la barre de menu de gauche, sélectionnez **Updates (Mises à jour)** > **Software Updates (Mises à jour logicielles)**. Téléchargez et enregistrez la version que vous voulez utiliser pour mettre à niveau le pare-feu.
- **On the firewall (Sur le pare-feu)** : sélectionnez **Device (Périphérique)** > **Software (Logiciel)** et **Check Now (Vérifier maintenant)** pour que le pare-feu vérifie auprès du serveur de mises à jour de Palo Alto Networks si des nouvelles versions de PAN-OS existent.

Vous rencontrez des difficultés pour vérifier les mises à jour logicielles ? Reportez-vous à cet article pour obtenir des solutions à certains des problèmes de connectivité courants.

STEP 3 | Après avoir choisi la version souhaitée, suivez le workflow complet jusqu'à Mettre à niveau le pare-feu vers PAN-OS 11.0. Les étapes que vous prendrez peuvent dépendre de la version qui vous utilisez actuellement, si vous utilisez la HA et si vous utilisez ou non Panorama pour gérer les pare-feu.

Mises à jour de contenu dynamiques

Palo Alto Networks publie fréquemment des mises à jour que le pare-feu peut utiliser pour appliquer la politique de sécurité, sans que vous deviez mettre à niveau le logiciel PAN-OS ou modifier la configuration du pare-feu. Ces mises à jour dotent le pare-feu des fonctions et de renseignements sur les menaces les plus à jour.

À l'exception des mises à jour des applications et de certaines mises à jour antivirus—que le pare-feu continue de recevoir—les mises à jour de contenu dynamiques qui vous sont disponibles peuvent dépendant de vos subscriptions (abonnements). Vous pouvez établir un calendrier de mises à jour dynamiques pour chaque mise à jour de contenu dynamique afin de définir la fréquence à laquelle le pare-feu vérifie la présence de nouvelles mises à jour et, le cas échéant, les télécharge ou les installe (**Device [Périphérique]** > **Dynamic Updates [Mises à jour dynamiques]**).

Mises à jour de contenu dynamiques	Que contient la trousse ?
Antivirus	Les mises à jour antivirus sont publiées toutes les 24 heures et incluent: • les signatures WildFire pour les logiciels malveillants nouvellement découverts. Pour obtenir ces mises à jour aux cinq minutes plutôt qu'une fois par jour, vous aurez besoin d'un WildFire subscription (abonnement WildFire). • (Exige la Threat Prevention) Les signatures de command-and-control (commande et contrôle ; C2) générées automatiquement qui détectent certains modèles dans le trafic C2. Ces signatures permettent au pare-feu de détecter l'activité C2 même lorsque l'hôte C2 est inconnu ou change rapidement. • (Exige la Threat Prevention) Les entrées de la liste nouvelles et mises à jour pour les listes dynamiques externes intégrées. Ces listes comprennent les adresses IP malveillantes, à risque élevé et fournies par un hôte à toute épreuve, et peuvent vous aider à vous protéger contre les hôtes malveillants. • (Exige la Threat Prevention) Mises à jour apportées à l'ensemble de signatures DNS local que le pare-feu utilise pour identifier les domaines malveillants qui sont connus. Si vous avez défini la mise en entonnoir DNS, le pare-feu peut identifier les hôtes sur votre réseau qui tentent de se connecter à ces domaines. Pour permettre au pare-feu de vérifier les domaines en les comparant à la base de données de signatures DNS complètes, définissez la DNS Security (Sécurité DNS).
Applications	Les mises à jour des applications fournissent des signatures d'applications nouvelles et modifiées ou des App-IDs. Cette mise à jour ne nécessite aucun abonnement supplémentaire, mais requiert néanmoins un contrat de maintenance/support valide. Les nouvelles mises à jour des applications ne sont publiées que le troisième mardi de chaque mois, pour vous donner le temps de préparer à l'avance les mises à jour de politique nécessaires.

Mises à jour de contenu dynamiques	Que contient la trousse ?
	Dans de rares cas, la publication de la mise à jour contenant les nouveaux App-ID peut être retardée d'un ou deux jours. Les modifications apportées aux App-ID sont publiées plus fréquemment. Tandis que les ID d'application nouveaux et modifiés permettent au pare-feu de renforcer votre stratégie de sécurité avec une précision toujours croissante, ce que entraîne des modifications de la politique de sécurité qui peuvent affecter la disponibilité des applications. Pour tirer le meilleur parti des mises à jour des applications, suivez nos conseils pour Manage New and Modified App-IDs (gérer les ID d'application nouveaux et modifiés).
Applications et menaces	Inclut les nouvelles signatures d'applications et de menaces, ainsi que celles mises à jour. Cette mise à jour est disponible si vous disposez d'un abonnement Prévention des menaces (dans ce cas, vous l'obtenez à la place de la mise à jour Applications). Les nouvelles mises à jour des menaces sont publiées fréquemment, parfois plusieurs fois par semaine, en même temps que les App-ID mises à jour. Les nouveaux App-ID ne sont publiés que le troisième mardi de chaque mois. *Dans de rares cas, la publication de la mise à jour contenant les nouveaux App-ID peut être retardée d'un ou deux jours.* Le pare-feu peut récupérer les dernières mises à jour des menaces et des applications en moins de 30 minutes de disponibilité. Pour obtenir des directives sur la meilleure façon d'activer les mises à jour des menaces et des applications pour garantir la disponibilité des applications et une protection contre les menaces les plus récentes, passez en revue la section Meilleures pratiques pour les mises à jour du contenu de menace et des applications.
Dictionnaire des appareils	Le dictionnaire de périphériques est un fichier XML pour les pare-feu à utiliser dans les règles de stratégie de sécurité basées sur Device-ID (ID de l'appareil). Il contient des entrées pour divers attributs de périphérique et est complètement actualisé sur une base régulière et affiché comme un nouveau fichier sur le serveur de mise à jour. En cas de modification d'une entrée du dictionnaire, un fichier révisé sera affiché sur le serveur de mise à jour afin que Panorama et les pare-feu le téléchargent et l'installent automatiquement lors de la prochaine vérification du serveur de mise à jour, ce qu'ils font automatiquement toutes les deux heures.
Fichier de données GlobalProtect	Contient les informations spécifiques au fournisseur pour la définition et l'évaluation des données du profil d'informations sur l'hôte (HIP) renvoyées par les applications GlobalProtect. Vous devez disposer d'un abonnement de passerelle GlobalProtect pour pouvoir recevoir ces mises à jour. De plus, vous devez créer un calendrier de téléchargement et d'installation des mises à jour pour que GlobalProtect fonctionne.

Mises à jour de contenu dynamiques	Que contient la trousse ?
VPN sans client GlobalProtect	Contient les nouvelles signatures d'applications et celles mises à jour pour permettre au VPN sans client d'accéder aux applications Web courantes à partir du portail GlobalProtect. Vous devez disposer d'un abonnement à GlobalProtect pour recevoir ces mises à jour. De plus, vous devez créer un calendrier de téléchargement et d'installation des mises à jour pour que le VPN sans client GlobalProtect fonctionne. Il est recommandé de toujours installer les dernières mises à jour de contenu pour le VPN sans client GlobalProtect.
WildFire	Donne accès aux signatures de logiciels malveillants et d'antivirus générées par le cloud public WildFire en temps réel. En option, vous pouvez configurer PAN-OS pour qu'il récupère les packages de mise à jour des signatures WildFire à la place. Vous pouvez configurer le pare-feu pour qu'il vérifie la présence de nouvelles mises à jour aux minutes pour veiller à ce que le pare-feu récupère les dernières signatures WildFire dans la minute qui suit leur disponibilité. Sans abonnement WildFire, vous devez attendre au moins 24 heures pour que les signatures soient fournies dans la mise à jour antivirus.
WF Privé	Fournit des signatures antivirus et de logiciels malveillants en temps quasi réel, créées suite à l'analyse effectuée par un appareil WildFire. Pour recevoir des mises à jour de contenu d'un appareil WildFire, le pare-feu et l'appareil doivent tous deux exécuter PAN-OS 6.1 ou une version ultérieure, et le pare-feu doit être configuré de manière à transférer les fichiers et les liens contenus dans les e-mails au cloud WildFire privé.

Installation des mises à jour de contenu

Afin d'être toujours protégé contre les dernières menaces (y compris celles qui n'ont pas encore été découvertes), vous devez vous assurer de garder vos pare-feu à jour avec les dernières mises à jour de contenu et logicielles publiées par Palo Alto Networks. La Mises à jour de contenu dynamiques à votre disposition dépend des subscriptions (abonnements) dont vous disposez.

Suivez ces étapes pour installer les mises à jour de contenu. Vous pouvez également établir un calendrier pour les mises à jour de contenu, pour définir la fréquence à laquelle le pare-feu récupère et installe les mises à jour.

Les mises à jour du contenu des menaces et des applications fonctionnent un peu différemment des autres types de mises à jour. Pour tirer le maximum des connaissances les plus récentes sur les applications et de la Threat Prevention, suivez les lignes directrices pour Déploiement des mises à jour du contenu de menace et des applications plutôt que les étapes décrites ici.

STEP 1 | Assurez-vous que le pare-feu a accès au serveur de mises à jour.

1. Par défaut, le pare-feu accède au **Update Server (serveur de mise à jour)** sur **`updates.paloaltonetworks.com`** afin que le pare-feu reçoive les mises à jour de contenu du serveur dont il est le plus proche. Si votre pare-feu a un accès limité à Internet, il peut être nécessaire de configurer votre liste d'autorisation pour permettre l'accès aux serveurs impliqués dans les téléchargements de mises à jour. Pour plus d'informations sur les serveurs de mise à jour de contenu, reportez-vous à Content Delivery Network Infrastructure for Dynamic Updates (Infrastructure de réseau de livraison de contenu pour les mises à jour dynamiques). Si vous souhaitez des informations de référence supplémentaires ou rencontrez des problèmes de connectivité et de téléchargement de mise à jour, veuillez vous référer à https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u0000001UtRCAU.

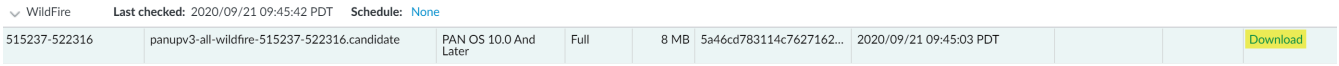
   *Si votre appareil se trouve en Chine continentale, Palo Alto Networks recommande d'utiliser le serveur **`updates.paloaltonetworks.cn`** pour les téléchargements de mises à jour.*

2. (Facultatif) Cliquez sur **Vérifier l'identité du serveur de mises à jour** pour obtenir un niveau de confirmation supplémentaire afin de permettre au pare-feu de vérifier que le certificat SSL du serveur est signé par une autorité de confiance. Cette option est activée par défaut.
3. (Facultatif) Si le pare-feu doit utiliser un serveur proxy pour accéder aux services de mises à jour Palo Alto Networks, à la fenêtre **Proxy Server (Serveur proxy)**, saisissez :
   - **Serveur** : adresse IP ou nom d'hôte du serveur proxy.
   - **Port** : port du serveur proxy. Plage entre 1 et 65535.
   - **User (Utilisateur)** : Le nom d'utilisateur qui permet d'accéder au serveur.
   - **Password (Mot de passe)** : Le mot de passe que l'utilisateur utilise pour accéder au serveur proxy. Saisissez à nouveau le mot de passe et **Confirmez le mot de passe**.
4. (Facultatif) Configurez jusqu'à trois tentatives de reconnexion en cas d'échec de la connexion. Utilisez **`debug set-content-download-retry attempts`** pour définir le nombre de tentatives de connexion. La valeur par défaut est 0.

STEP 2 | Recherchez les dernières mises à jour de contenu.

Sélectionnez **Device (Périphérique)** > **Dynamic Updates (Mises à jour dynamiques)**, puis cliquez sur **Check Now (Vérifier maintenant)** (dans le coin inférieur gauche de la fenêtre) pour rechercher les dernières mises à jour. Le lien se trouvant dans la colonne **Action (Action)** indique si une mise à jour est disponible:

- **Download (Télécharger)** : indique qu'un nouveau fichier de mise à jour est disponible. Cliquez sur ce lien pour commencer à télécharger le fichier directement sur le pare-feu. Une fois le téléchargement terminé, le lien se trouvant dans la colonne **Action** passe de **Télécharger (Télécharger)** à **Install (Installer)**.



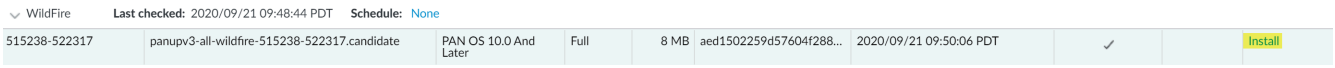
Vous ne pouvez pas télécharger la mise à jour antivirus avant que vous n'ayez installé la mise à jour Applications et menaces.

- **Rétablir** : indique qu'une version précédemment installée de la version de contenu ou de logiciel est disponible. Vous pouvez choisir de rétablir la version précédemment installée.

STEP 3 | Installez les mises à jour de contenu.

L'installation peut prendre jusqu'à 10 minutes sur un pare-feu PA-220 jusqu'à deux minutes sur un pare-feu PA-5200 Series, PA-7000 Series ou VM-Series.

Cliquez sur le lien **Installer** dans la colonne **Action**. Une fois l'installation terminée, une coche s'affiche dans la colonne **Currently Installed (Actuellement installé)**.



STEP 4 | Planifiez chaque mise à jour de contenu.

Répétez cette étape pour chaque mise à jour que vous souhaitez planifier.

Échelonnez les calendriers de mises à jour car le pare-feu ne peut télécharger qu'une seule mise à jour à la fois. Si vous planifiez le téléchargement des mises à jour lors du même intervalle de temps, seul le premier téléchargement réussira.

1. Définissez le calendrier pour chaque type de mise à jour en cliquant sur le lien **Aucun(e)**.

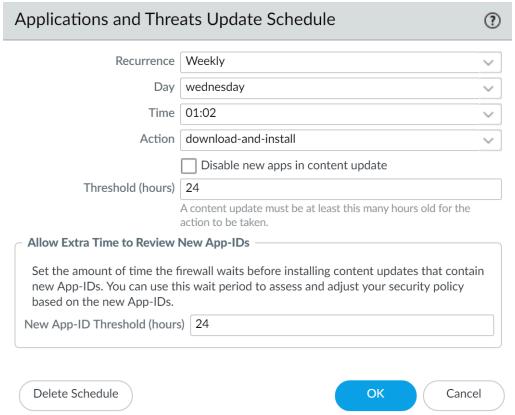
2. Indiquez la fréquence de téléchargement et d'installation des mises jour en sélectionnant une valeur dans la liste déroulante **Récurrence**. Les valeurs disponibles peuvent varier selon le type de contenu (les mises à jour WildFire sont disponibles en **Real-time (Temps réel)**, **Every Minute (Toutes les minutes)**, **Every 15 Minutes (Toutes les 15 minutes)**, **Every 30 minutes (Toutes les 30 minutes)** ou **Every Hour (Toutes les heures)** tandis que les mises à jour des applications et des menaces peuvent être planifiés pour la mise à jour **Weekly (Toutes les semaines)**, **Daily (Tous les jours)**, **Hourly (Toutes les heures)** ou **Every 30 Minutes (Toutes**

les 30 minutes) et les mises à jour antivirus peuvent être planifiées pour une mise à jour **Hourly (Toutes les heures)**, **Daily (Tous les jours)** ou **Weekly (Toutes les semaines)**).

Vous pouvez également sélectionner **Aucun (Manuel)** pour Applications et menaces ou pour les mises à jour antivirus. Cela signifie qu'il n'y a pas de calendrier récurrent pour cet élément et que vous devez installer manuellement les mises à jour. Pour supprimer complètement le nœud de planification, sélectionnez **Supprimer la planification**.

3. Indiquez l'**heure** et (ou, les minutes après l'heure dans le cas de WildFire), le cas échéant, selon la valeur de **Recurrence (récurrence)**sélectionnée, le **Day (jour)** de la semaine de téléchargement des mises à jour.
4. Indiquez si vous souhaitez que le système **Download Only (Télécharge uniquement)** la mise à jour (recommandé) ou qu'il la **Download And Install (télécharge et installe)** .
5. Dans le champ **Threshold (Hours) (Seuil (heures))**, indiquez le délai d'attente après une publication avant de procéder à l'installation d'une mise à jour de contenu. Dans de rares cas, il se peut que les mises à jour de contenu contiennent des erreurs. C'est pour cela que vous devez différer l'installation de nouvelles mises à jour quelques heures après leur publication.

   Si vous possédez des applications stratégiques qui doivent être entièrement disponibles, indiquez un seuil applicable aux mises à jour d'applications ou aux mises à jour d'applications et de menaces minimal de 24 heures ou plus et suivez les Meilleures pratiques pour les mises à jour du contenu de menace et des applications*. De plus, bien que l'établissement d'un calendrier des mises à jour de contenu soit une tâche ponctuelle, peu fréquente, vous devrez continuer à effectuer la* Gestion des App-ID nouveaux et modifiés *qui sont inclus dans les versions de contenu, puisque ces App-ID pourraient modifier l'application de la politique de sécurité.*
6. (Facultatif) Saisissez les **New App-ID Thresholds (Nouveaux seuils App-ID)** en heures pour définir le temps d'attente du pare-feu avant d'installer les mises à jour de contenu qui contiennent les nouvelles App-ID.



7. Cliquez sur **OK** pour enregistrer les paramètres de la planification.
8. Cliquez sur **Commit (Valider)** pour enregistrer les paramètres de la configuration active.

STEP 5 | Mettez PAN-OS à jour.

Mettez toujours le contenu à jour avant de mettre à jour PAN-OS. Chaque version PAN-OS possède une version de contenu minimum prise en charge.

1. Passez en revue les Notes de version.
2. Mettez à jour le logiciel PAN-OS.

Mises à jour du contenu de menace et des applications

Les mises à jour du contenu de menace et des applications procurent les plus récentes signatures des applications et des menaces au pare-feu. La portion de la trousse qui concerne les applications comprend des App-ID nouveaux ou modifiés. Une licence n'est pas requise pour y accéder. La trousse complète du contenu des applications et des menaces, qui comprend également les signatures de menaces nouvelles et modifiées, exige une licence de prévention contre les menaces. Lorsque le pare-feu récupère et installe automatiquement les dernières signatures des applications et des menaces (selon vos paramètres personnalisés), il peut commencer à appliquer la politique de sécurité en fonction des derniers App-ID et de la plus récente protection contre les menaces sans que vous ayez à effectuer de configuration supplémentaire.

Les signatures de menaces nouvelles et modifiées, ainsi que les App-ID modifiés, sont lancées au moins une fois par semaine et bien souvent à une fréquence plus élevée. De nouveaux App-ID sont lancés le troisième mardi de chaque mois.

Dans de rares cas, la publication de la mise à jour contenant les nouveaux App-ID peut être retardée d'un ou deux jours.

Comme les nouveaux App-ID peuvent modifier la façon dont la politique de sécurité met le trafic en œuvre, ce lancement plus limité des nouveaux App-ID vise à fournir une fenêtre plus prévisible au cours de laquelle vous pouvez vous préparer et mettre à jour votre politique de sécurité. De même, les mises à jour de contenu sont cumulatives, ce qui signifie que la plus récente mise à jour de contenu inclut toujours les signatures des applications et des menaces lancées dans les versions précédentes.

Comme les signatures des applications et des menaces sont livrées dans une seule trousse (les mêmes décodeurs qui permettent aux signatures d'applications d'identifier les applications permettent également aux signatures des menaces d'inspecter le trafic), vous devez vous demander si vous souhaitez déployer les signatures ensemble ou séparément. La manière de déployer les mises à jour de contenu pour laquelle vous optez dépend des exigences en matière de disponibilité des applications et de sécurité du réseau de votre organisation. Pour commencer, déterminez que votre organisation jouit de l'une des positions suivantes (ou peut-être les deux, selon l'emplacement du pare-feu) :

- Une organisation disposant d'un niveau de sécurité *optimal* accorde la priorité à la protection à l'aide des plus récentes signatures de menaces plutôt qu'à la disponibilité des applications. Vous utilisez principalement le pare-feu pour ses fonctions de prévention des menaces. Toutes les modifications à App-ID qui influent sur la manière dont la politique de sécurité application le trafic des applications sont secondaires.
- Un réseau *stratégique* accorde la priorité à la disponibilité des applications plutôt qu'à la protection à l'aide des plus récentes signatures de menaces. Votre réseau ne tolère aucunement les temps d'interruption. Le pare-feu est déployé en ligne afin de mettre en œuvre la politique de sécurité. De plus, si vous utilisez App-ID dans la politique de sécurité, toute modification qu'une version de contenu introduit qui touche App-ID pourrait provoquer une interruption.

Vous pouvez adopter une approche axée sur la sécurité ou une approche stratégique en matière de déploiement des mises à jour de contenu. Vous pouvez également appliquer un mélange des deux approches pour répondre aux besoins de l'organisation. Passez en revue les Meilleures pratiques pour les mises à jour du contenu de menace et des applications, et tenez-en compte, pour décider la manière de mettre en œuvre les mises à jour de menaces et d'applications. Ensuite :

- Procédez au Déploiement des mises à jour du contenu de menace et des applications.

- Suivez nos Conseils relatifs aux mises à jour de contenu.

Bien que l'établissement d'un calendrier des mises à jour de contenu soit une tâche ponctuelle, peu fréquente, vous devrez continuer à effectuer la Gestion des App-ID nouveaux et modifiés qui sont inclus dans les versions de contenu, puisque ces App-ID pourraient modifier l'application de la politique de sécurité.

Déploiement des mises à jour du contenu de menace et des applications

Avant de prendre les mesures nécessaires pour configurer les mises à jour du contenu des applications et des menaces, découvrez comment Mises à jour du contenu de menace et des applications fonctionne et décidez comment vous souhaitez mettre en œuvre Meilleures pratiques pour les mises à jour du contenu de menace et des applications.

De plus, Panorama vous permet de déployer rapidement et efficacement des mises à jour de contenu sur le pare-feu. Si vous utilisez Panorama pour gérer les pare-feu, suivez ces étapes pour déployer les mises à jour de contenu plutôt que celles ci-dessous.

STEP 1 | Pour obtenir la trousse complète du contenu des applications et des menaces, obtenez une licence de prévention contre les menaces et activez la licence sur le pare-feu.

1. Sélectionnez **Device (Périphérique)** > **Licenses (Licences)**.
2. Chargez manuellement la clé de licence ou récupérez-la du serveur de licence Palo Alto Networks.
3. Vérifiez que la licence de prévention contre les menaces est active.

STEP 2 | Définissez le calendrier d'obtention des mises à jour de contenu et de leur installation sur le pare-feu.

Lorsque vous effectuez les étapes suivantes, il est particulièrement important de tenir compte de l'approche adoptée par votre organisation, soit stratégique ou niveau de sécurité optimal (ou une combinaison des deux) et d'avoir passé en revue les Meilleures pratiques pour les mises à jour du contenu de menace et des applications.

1. Sélectionnez **Device (Périphérique)** > **Dynamic Updates (Mises à jour dynamiques)**.
2. Sélectionnez le **Schedule (Calendrier)** des mises à jour du contenu des menaces et des applications.
3. Définissez la fréquence (la **Recurrence (Récurrence)**) à laquelle le pare-feu vérifie auprès du serveur de mises à jour Palo Alto Networks la présence de nouvelles versions de contenu des applications et des menaces, de même que le **Day (Jour)** et la **Time (Heure)**.
4. Définissez l'**Action** que le pare-feu doit prendre lorsqu'il trouve et obtient une nouvelle version de contenu.
5. Définissez un **Threshold (Seuil)** d'installation pour les mises à jour de contenu. Les versions de contenu doivent être disponibles sur le serveur de mises à jour Palo Alto Networks au moins pendant cette durée de temps avant que le pare-feu puisse l'obtenir et effectuer l'action que vous avez configurée à l'étape précédente.
6. Si vous disposez d'un réseau stratégique, où vous n'avez aucune tolérance à l'égard de l'indisponibilité des applications (la disponibilité des applications est aussi importante que la plus récente prévention contre les menaces), vous pouvez définir un **New App-ID Threshold (Seuil de téléchargement des nouveaux App-ID)**. Le pare-feu ne récupère les mises à jour

de contenu qui contiennent de nouveaux App-ID que lorsqu'elles sont disponibles depuis cette durée de temps.

7. Cliquez sur **OK** pour enregistrer le calendrier des mises à jour de contenu des menaces et des applications, puis **Commit (Validez)**.

STEP 3 | Configurez le transfert de journaux pour envoyer des alertes de contenu stratégiques Palo Alto Networks aux services externes que vous utilisez pour surveiller l'activité du réseau et du pare-feu. Cela vous permet de vous assurer que le personnel concerné est informé des problèmes qui surviennent dans le contenu stratégique, afin qu'il puisse prendre les mesures nécessaires. Les alertes de mise à jour du contenu critiques sont également journalisées en tant qu'entrées du journal système sous le type dynamic-updates (mises à jour dynamiques) et l'événement palo-alto-networks-message.

STEP 4 | Bien que l'établissement d'un calendrier des mises à jour de contenu soit une tâche ponctuelle, peu fréquente, vous devrez continuer à effectuer la Gestion des App-ID nouveaux et modifiés qui sont inclus dans les versions de contenu, puisque ces App-ID pourraient modifier l'application de la politique de sécurité.

Conseils relatifs aux mises à jour de contenu

Les versions de contenu des applications et des menaces de Palo Alto Networks sont soumises à des contrôles de la qualité et du rendement rigoureux. Cependant, puisqu'il existe de nombreuses variables possibles dans un environnement client, il arrive, dans de rares occasions, qu'une version de contenu ait une incidence inattendue sur un réseau. Suivez ces conseils pour atténuer ou résoudre un problème pouvant découler d'une version de contenu, et minimiser ainsi ses répercussions sur votre réseau.

- **Suivez les meilleures pratiques pour les mises à jour du contenu de menace et des applications**

  Passez en revue les Meilleures pratiques pour les mises à jour du contenu de menace et des applications et mettez-les en œuvre. La manière de déployer les mises à jour de contenu pour laquelle vous optez peut dépendre des exigences en matière de disponibilité des applications et de sécurité de votre réseau.

- **Assurez-vous d'utiliser le contenu le plus à jour.**

  Obtenez la plus récente mise à jour de contenu si vous n'avez pas configuré le pare-feu pour qu'il la télécharge et l'installe automatiquement.

  Le pare-feu valide que les mises à jour de contenu téléchargées sont toujours recommandées par Palo Alto Networks au moment de leur installation. Cette vérification, que le pare-feu mène par défaut, s'avère utile dans les situations où les mises à jour de contenu sont téléchargées du serveur de mises à jour de Palo Alto Networks (manuellement ou selon un horaire établi) avant leur installation. Puisqu'il peut arriver dans des cas rares que Palo Alto Networks rende une mise à jour de contenu indisponible, cette option empêche le pare-feu d'installer une mise à jour de contenu que Palo Alto Networks a supprimée, même si le pare-feu l'a déjà téléchargée. Si un message d'erreur vous indique que la mise à jour de contenu que vous tentez d'installer n'est plus valide, **Check Now (Vérifiez maintenant)** pour obtenir la plus récente mise à jour du contenu et installer celle-ci à la place (**Device (Périphérique)** > **Dynamic Updates (Mises à jour dynamiques)**).

- **Activez la télémétrie des renseignements sur les menaces.**

  Activez la télémétrie des renseignements sur les menaces que le pare-feu envoie à Palo Alto Networks. Nous utilisons les données télémétriques pour identifier et régler les problèmes touchant les mises à jour de contenu.

  Les données télémétriques nous aident à rapidement reconnaître une mise à jour de contenu qui a une incidence inattendue sur le rendement du pare-feu ou sur l'application de la politique de sécurité à l'échelle de la clientèle de Palo Alto Networks. Le plus rapidement nous arrivons à identifier un problème, le plus rapidement nous pouvons faire en sorte d'éradiquer le problème ou d'atténuer son incidence sur votre réseau.

  Pour permettre au pare-feu de recueillir les données télémétriques et de les transmettre à Palo Alto Networks :

  1. Sélectionnez **Device (Périphérique)** > **Setup (configuration)** > **Telemetry (Télémétrie)**.
  2. Modifiez les paramètres de **Telemetry (Télémétrie)** et **Select All (Sélectionnez tout)**.
  3. Cliquez sur **OK (OK)** puis sur **Commit (Valider)** pour enregistrer vos modifications.

- **Transmettez les alertes relatives aux mises à jour de contenu aux bonnes personnes.**

  Activez le transfert des journaux pour les alertes de contenu critique de Palo Alto Networks pour que les messages importants concernant les problèmes de mises à jour de contenu soient directement transmis au personnel approprié.

  Palo Alto Networks peut désormais émettre des alertes concernant des problèmes de mise à jour du contenu directement à l'interface Web du pare-feu ou, si votre transfert des journaux est activé, au service externe que vous utilisez pour la surveillance. Les alertes de contenu critique décrivent le problème pour que vous puissiez comprendre l'incidence qu'il a sur vous et présentent les étapes à suivre pour prendre des mesures, au besoin.

  Dans l'interface Web du pare-feu, les alertes critiques concernant les problèmes de contenu s'affichent d'une manière analogue au Message du jour. Lorsque Palo Alto Networks émet une alerte critique relativement à une mise à jour du contenu, l'alerte s'affiche par défaut lorsque vous vous connectez à l'interface Web du pare-feu. Si vous êtes déjà connecté à l'interface Web du pare-feu, vous remarquerez un point d'exclamation qui apparaît au-dessus de l'icône des messages dans la barre de menus située au bas de l'interface Web ; cliquez sur l'icône des messages pour afficher l'alerte.

  Les alertes de mise à jour du contenu critiques sont également journalisées en tant qu'entrées du journal système sous le type **dynamic-updates** (mises à jour dynamiques) et l'événement **palo-alto-networks-message**. Utilisez le filtre suivant pour afficher ces entrées du journal : (subtype eq dynamic-updates) et (eventid eq palo-alto-networks-message).

- **Au besoin, utilisez Panorama pour revenir à une version de contenu antérieure.**

  Après avoir été avisé d'un problème concernant une mise à jour du contenu, vous pouvez utiliser Panorama pour rétablir rapidement la version des mises à jour de contenu précédente sur les pare-feu gérés plutôt que de devoir le faire manuellement sur chaque pare-feu :Rétablir les mises à jour du contenu depuis Panorama.

Meilleures pratiques pour les mises à jour du contenu de menace et des applications

Les meilleures pratiques pour déployer des mises à jour de contenu permettent d'assurer une application transparente des stratégies, car le pare-feu est continuellement équipé de nouvelles applications et signatures de menaces. Même si les signatures d'application et de menace sont livrées ensemble dans un seul paquet de mise à jour de contenu (en savoir plus sur les Mises à jour du contenu de menace et des applications), vous avez la flexibilité de les déployer différemment selon vos besoins de sécurité et de disponibilité :

- Une organisation disposant d'un niveau de sécurité *optimal* accorde la priorité à la protection à l'aide des plus récentes signatures de menaces plutôt qu'à la disponibilité des applications. Vous utilisez principalement le pare-feu pour ses fonctions de prévention des menaces.
- Un réseau *stratégique* accorde la priorité à la disponibilité des applications plutôt qu'à la protection à l'aide des plus récentes signatures de menaces. Votre réseau ne tolère aucunement les temps d'interruption. Le pare-feu est déployé en ligne afin de mettre en œuvre la politique de sécurité. De plus, si vous utilisez App-ID dans la politique de sécurité, toute modification du contenu qui touche App-ID pourrait provoquer une interruption.

Vous pouvez adopter une approche axée sur la sécurité ou une approche stratégique en matière de déploiement des mises à jour de contenu. Vous pouvez également appliquer un mélange des deux approches pour répondre aux besoins de l'organisation. Tenez compte de l'approche que vous souhaitez adopter lorsque vous appliquez les meilleures pratiques suivantes afin de tirer le meilleur parti des signatures des applications et des menaces nouvelles et modifiées :

- Meilleures pratiques pour les mises à jour de contenu : stratégiques
- Meilleures pratiques pour les mises à jour de contenu : niveau de sécurité optimal

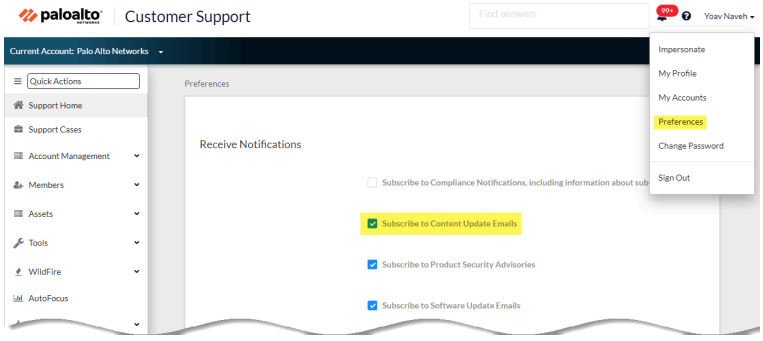
Meilleures pratiques pour les mises à jour de contenu : stratégiques

Les Meilleures pratiques pour les mises à jour du contenu de menace et des applications aident à procurer une application transparente des politiques au fur et à mesure que de nouvelles signatures d'applications et de menaces sont publiées. Suivez ces meilleures pratiques pour déployer des mises à jour de contenu dans un *réseau stratégique*, où la disponibilité des applications est la priorité absolue.

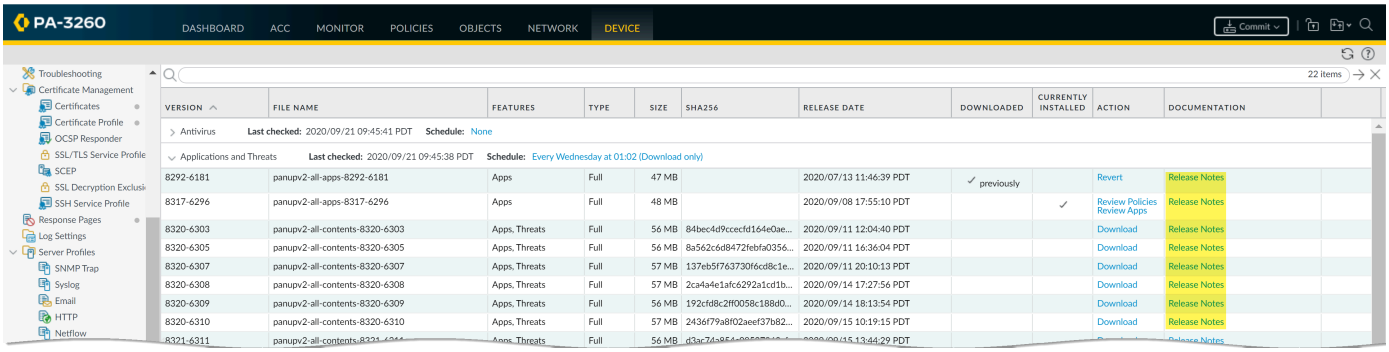
- Passez toujours en revue les notes de version pour connaître la liste des signatures d'applications et de menaces nouvellement identifiées et modifiées que la version de contenu introduit. Les notes de version décrivent également l'incidence éventuelle de la mise à jour sur la mise en œuvre actuelle de

la politique de sécurité et fournissent des recommandations sur les modifications possibles que vous pouvez apporter à votre politique de sécurité afin de tirer le meilleur profit des nouveautés.

Pour recevoir des avis lorsque de nouvelles mises à jour de contenu sont disponibles, rendez-vous sur le portail d'assistance, modifiez vos **Preferences (Préférences)** et sélectionnez **Subscribe to Content Update Emails (S'abonner à l'envoi de mises à jour de contenu par e-mail)**.



Vous pouvez également lire la section Notes de version des signatures d'applications et de menaces sur le portail d'assistance de Palo Alto Networks ou directement dans l'interface Web du pare-feu : sélectionnez **Device (Périphérique)** > **Dynamic Updates (Mises à jour dynamiques)** et ouvrez les **Release Note (Notes de version)** concernant une version de contenu donnée.

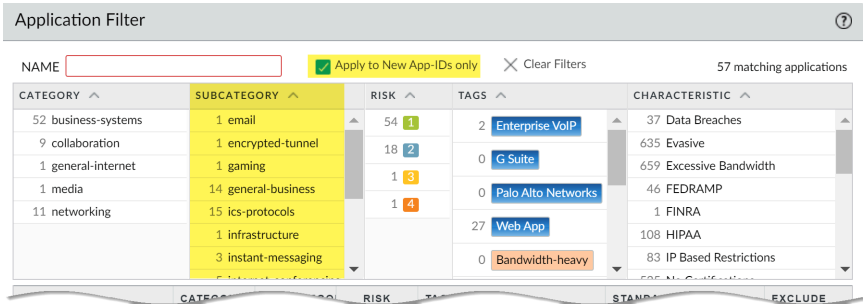


La section Notes des Notes de version présente les mises à jour ultérieures qui, selon Palo Alto Networks, pourraient éventuellement avoir une incidence considérable sur la protection : par exemple, de nouveaux App-ID ou décodeurs. Soyez à l'affût de ces mises à jour ultérieures ; vous pourrez donc tenir compte de l'incidence qu'elles pourraient avoir sur votre politique avant leur lancement.

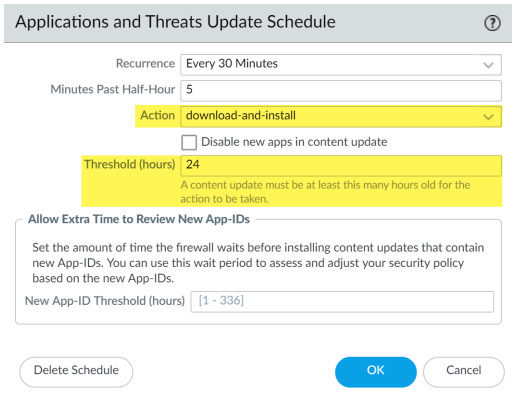
- Créez une règle de politique de sécurité pour toujours autoriser certaines catégories de nouveaux App-IP, comme les applications d'authentification ou de développement logiciel sur lesquelles reposent les fonctions essentielles de l'entreprise. Cela signifie que lorsqu'une version de contenu introduit ou modifie la couverture d'une application d'entreprise importante, le pare-feu continue d'autoriser l'application de manière transparente sans que vous ayez besoin de mettre à jour votre politique de sécurité. Vous éliminez ainsi toute incidence éventuelle sur la disponibilité des App-ID dans les

catégories stratégique et disposez de 30 jours (de nouveaux App-ID sont publiés mensuellement) pour ajuster votre stratégie de sécurité afin d'autoriser les App-ID stratégiques.

Pour ce faire, créez un filtre d'application pour les nouveaux App-ID des catégories stratégiques (**Objects > Application Filters (Objets> Filtres d'application)**) et ajoutez le filtre d'application à une règle de politique de sécurité.



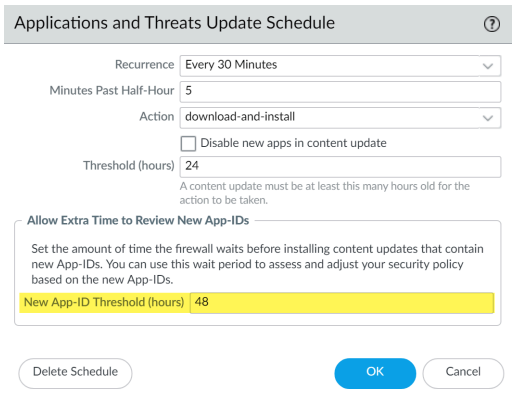
- Pour atténuer toute incidence sur l'application des politiques de sécurité associées à l'activation de nouvelles signatures d'applications et de menaces, échelonnez le déploiement du nouveau contenu. Fournissez le nouveau contenu aux emplacements qui présentent un risque moindre pour l'entreprise (moins d'utilisateurs dans les bureaux satellites) avant de les déployer dans les emplacements qui présentent un risque supérieur (comme les emplacements qui hébergent des applications critiques). En confinant les plus récentes mises à jour de contenu à certains pare-feu avant de les déployer dans l'ensemble de votre réseau, vous aurez également plus de facilité à résoudre les problèmes qui se présenteront. Vous pouvez utiliser Panorama pour qu'il transmette des planifications échelonnées et des seuils d'installation aux pare-feu et aux groupes de périphériques en fonction de l'organisation ou de l'emplacement (Utilisation de Panorama pour déployer des mises à jour sur les pare-feu).
- Planifiez des mises à jour de contenu afin qu'elles soient **download-and-install (téléchargées et installées)** automatiquement. Ensuite, définissez un **Threshold (Seuil)** qui détermine la période de temps pendant laquelle le pare-feu attend avant d'installer le contenu le plus récent. Dans un réseau critique, planifiez jusqu'à un seuil de 48 heures.



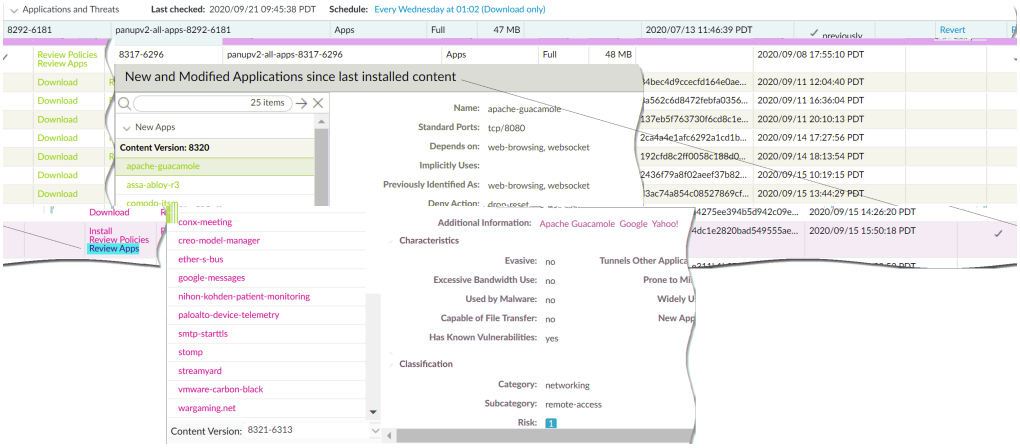
Le délai d'installation garantit que le pare-feu installe uniquement le contenu disponible et fonctionnant dans les environnements clients pour la durée spécifiée. Pour schedule content updates (planifier les mises à jour de contenu), sélectionnez **Device (Périphérique)** > **Dynamic Updates (Mises à jour dynamiques)** > **Schedule (Calendrier)**.

- Accordez-vous plus de temps pour ajuster votre politique de sécurité en fonction des nouveaux App-ID avant de les installer. Pour ce faire, définissez un seuil d'installation qui s'applique uniquement aux mises à jour de contenu contenant de nouveaux App-ID. Les mises à jour du contenu contenant

de nouveaux ID App-ID ne sont publiées qu'une fois par mois, et les seuils d'installation ne sont déclenchés qu'à ce moment-là. Planifiez des mises à jour de contenu pour configurer un **New App-ID Threshold (Nouveau seuil d'App-ID)** (**Device (Périphérique)** > **Dynamic Updates (Mises à jour dynamiques)** > **Schedule (Calendrier)**).

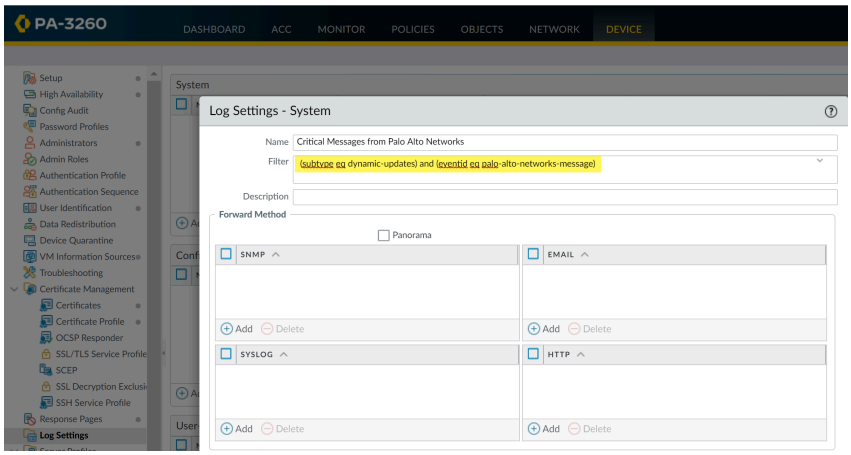


- Passez toujours en revue les App-ID nouveaux et modifiés introduits par une version de contenu, afin d'évaluer l'incidence des modifications sur votre politiques de sécurité. La rubrique suivante décrit les options que vous pouvez utiliser pour mettre à jour votre politique de sécurité avant et après l'installation de nouveaux App-ID : Gestion des App-ID nouveaux et modifiés.



- Configurez le transfert de journaux pour envoyer des alertes de contenu stratégiques Palo Alto Networks aux services externes que vous utilisez pour surveiller l'activité du réseau et du pare-feu. Cela vous permet de vous assurer que le personnel concerné est informé des problèmes qui surviennent dans le contenu stratégique, afin qu'il puisse prendre les mesures nécessaires. Les alertes de mise à jour du contenu critiques sont également journalisées en tant qu'entrées du journal système sous le type

dynamic-updates (mises à jour dynamiques) et l'événement palo-alto-networks-message.



Dans la version 8.1.2 de PAN-OS le type de journal pour les alertes de contenu critique est passé de ***general*** *(général) à* ***dynamic-updates*** *(mises à jour dynamiques). Si vous utilisez PAN-OS 8.1.0 ou PAN-OS 8.1.1, le contenu critique est journalisé sous forme d'entrées du journal système comportant le Type et l'Événement suivants, et vous devriez configurer la transmission de ces alertes au moyen du filtre suivant :* ***(subtype eq general) et (eventid eq palo-alto-networks-message)***.

- Examinez les nouvelles mises à jour de contenu des menaces et des applications dans un environnement de simulation avant de les activer dans votre environnement de production. La façon la plus simple de tester de nouvelles applications et menaces consiste à utiliser un pare-feu test pour exploiter le trafic de production. Installez la plus récente mise à jour de contenu sur le pare-feu test et surveillez le pare-feu lorsqu'il traite le trafic copié de votre environnement de production. Vous pouvez également vous servir de clients test et d'un pare-feu ou de captures de paquets (PCAP) test pour simuler le trafic de production. L'utilisation de PCAP fonctionne bien pour simuler le trafic de divers déploiements lorsque la politique de sécurité du pare-feu varie d'un emplacement à l'autre.

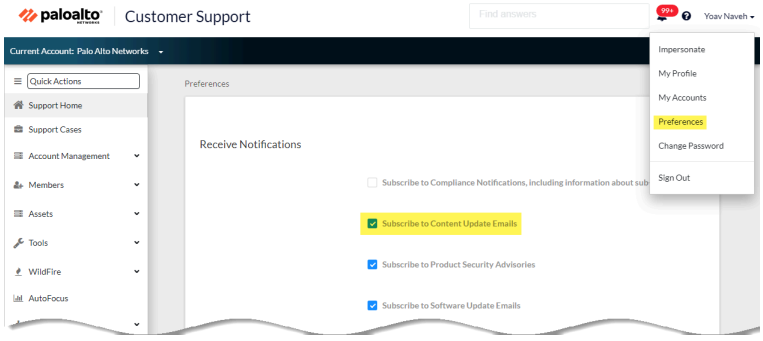
Meilleures pratiques pour les mises à jour de contenu : niveau de sécurité optimal

Les Meilleures pratiques pour les mises à jour du contenu de menace et des applications aident à procurer une application transparente des politiques au fur et à mesure que de nouvelles signatures d'applications et de menaces sont publiées. Suivez ces meilleures pratiques pour déployer des mises à jour de contenu dans *un doté d'un niveau de sécurité optimal*, où vous utilisez principalement le pare-feu pour ses fonctionnalités de prévention des menaces et que votre première priorité est la protection contre les attaques.

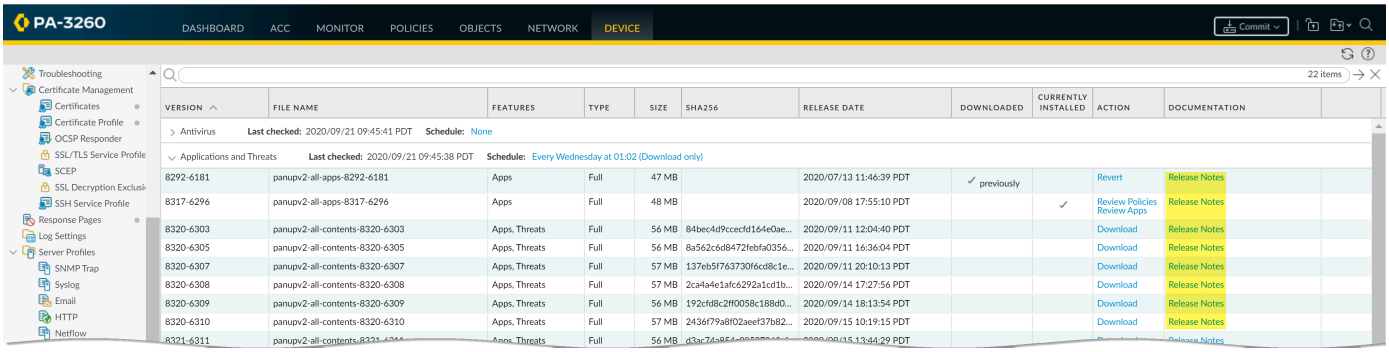
- Passez toujours en revue les notes de version pour connaître la liste des signatures d'applications et de menaces nouvellement identifiées et modifiées que la version de contenu introduit. Les notes de version décrivent également l'incidence éventuelle de la mise à jour sur la mise en œuvre actuelle de

la politique de sécurité et fournissent des recommandations sur les modifications possibles que vous pouvez apporter à votre politique de sécurité afin de tirer le meilleur profit des nouveautés.

Pour recevoir des avis lorsque de nouvelles mises à jour de contenu sont disponibles, rendez-vous sur le portail d'assistance, modifiez vos **Preferences (Préférences)** et sélectionnez **Subscribe to Content Update Emails (S'abonner à l'envoi de mises à jour de contenu par e-mail)**.



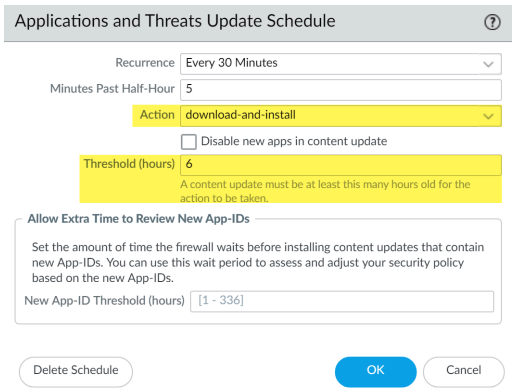
Vous pouvez également lire la section Notes de version des signatures d'applications et de menaces sur le portail d'assistance de Palo Alto Networks ou directement dans l'interface Web du pare-feu : sélectionnez **Device (Périphérique)** > **Dynamic Updates (Mises à jour dynamiques)** et ouvrez les **Release Note (Notes de version)** concernant une version de contenu donnée.



La section Notes des Notes de version présente les mises à jour ultérieures qui, selon Palo Alto Networks, pourraient éventuellement avoir une incidence considérable sur la protection : par exemple, de nouveaux App-ID ou décodeurs. Soyez à l'affût de ces mises à jour ultérieures ; vous pourrez donc tenir compte de l'incidence qu'elles pourraient avoir sur votre politique avant leur lancement.

- Pour atténuer toute incidence sur l'application des politiques de sécurité associées à l'activation de nouvelles signatures d'applications et de menaces, échelonnez le déploiement du nouveau contenu. Fournissez le nouveau contenu aux emplacements qui présentent un risque moindre pour l'entreprise (moins d'utilisateurs dans les bureaux satellites) avant de les déployer dans les emplacements qui présentent un risque supérieur (comme les emplacements qui hébergent des applications critiques). En confinant les plus récentes mises à jour de contenu à certains pare-feu avant de les déployer dans l'ensemble de votre réseau, vous aurez également plus de facilité à résoudre les problèmes qui se présenteront. Vous pouvez utiliser Panorama pour qu'il transmette des planifications échelonnées et des seuils d'installation aux pare-feu et aux groupes de périphériques en fonction de l'organisation ou de l'emplacement (Utilisation de Panorama pour déployer des mises à jour sur les pare-feu).
- Planifiez des mises à jour de contenu afin qu'elles soient **download-and-install (téléchargées et installées)** automatiquement. Ensuite, définissez un **Threshold (Seuil)** qui détermine la période de

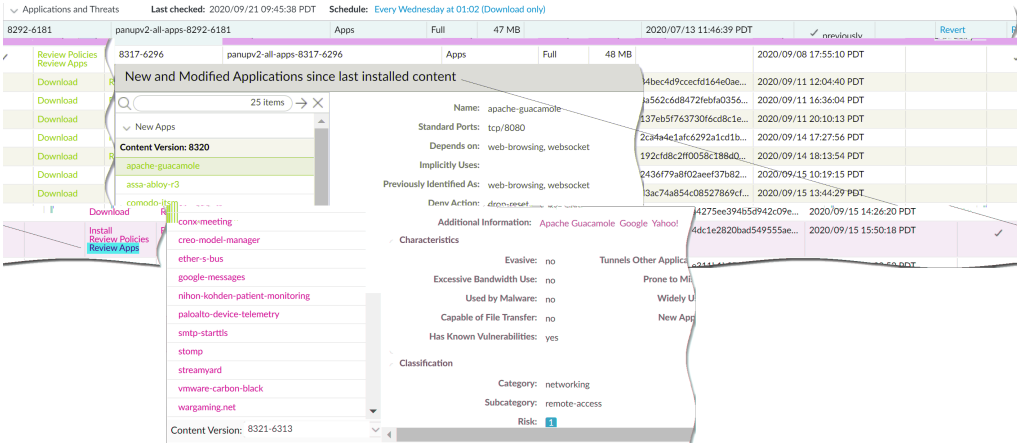
temps pendant laquelle le pare-feu attend avant d'installer le contenu le plus récent. Dans un réseau doté d'un niveau de sécurité optimal, planifiez un seuil de six à douze heures.



Le délai d'installation garantit que le pare-feu installe uniquement le contenu disponible et fonctionnant dans les environnements clients pour la durée spécifiée. Pour planifier les mises à jour de contenu, sélectionnez **Device (Périphérique)** > **Dynamic Updates (Mises à jour dynamiques)** > **Schedule (Calendrier)**.

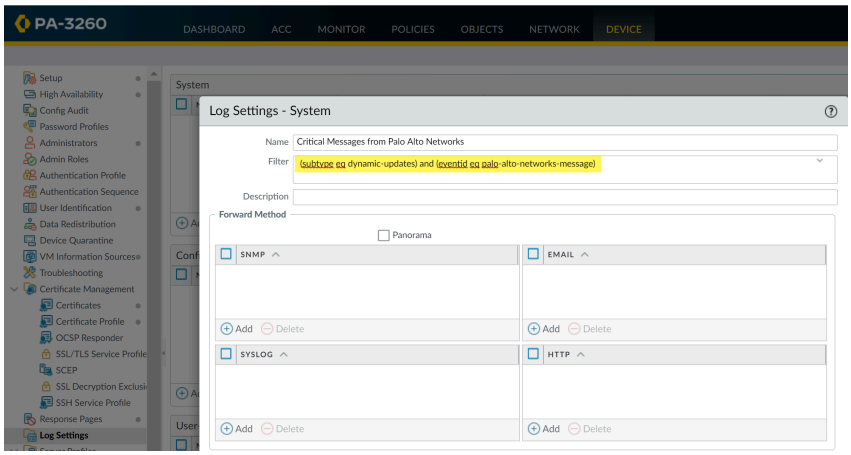
*Ne planifiez pas de **New App-ID Threshold (Nouveau seuil d'App-ID)**. Ce seuil permet aux organisations stratégiques de disposer de plus de temps pour ajuster l'application de la politique de sécurité en fonction des nouveaux App-ID. Toutefois, étant donné que ce seuil retarde également la mise à jour des dernières mises à jour de prévention contre les menaces, il n'est pas recommandé pour les organisations dotées d'un niveau de sécurité optimal.*

- Passez en revue les App-ID nouveaux et modifiés introduits par une version de contenu, afin d'évaluer l'incidence des modifications sur votre politique de sécurité. La rubrique suivante décrit les options que vous pouvez utiliser pour mettre à jour votre politique de sécurité avant et après l'installation de nouveaux App-ID : Gestion des App-ID nouveaux et modifiés.



- Configurez le transfert de journaux pour envoyer des alertes de contenu stratégiques Palo Alto Networks aux services externes que vous utilisez pour surveiller l'activité du réseau et du pare-feu. Cela vous permet de vous assurer que le personnel concerné est informé des problèmes qui surviennent dans le contenu stratégique, afin qu'il puisse prendre les mesures nécessaires. Les alertes de mise à jour du contenu critiques sont également journalisées en tant qu'entrées du journal système sous le

type `dynamic-updates (mises à jour dynamiques)` et l'`événement palo-alto-networks-message`.



Dans la version 8.1.2 de PAN-OS le type de journal pour les alertes de contenu critique est passé de ***`general`*** *(général) à* ***`dynamic-updates`*** *(mises à jour dynamiques). Si vous utilisez PAN-OS 8.1.0 ou PAN-OS 8.1.1, le contenu critique est journalisé sous forme d'entrées du journal système comportant le Type et l'Événement suivants, et vous devriez configurer la transmission de ces alertes au moyen du filtre suivant :* ***`(subtype eq general) et (eventid eq palo-alto-networks-message)`***.

Infrastructure réseau de distribution de contenu

Palo Alto Networks gère une infrastructure Content Delivery Network (réseau de distribution de contenu - CDN) pour fournir des mises à jour du contenu aux pare-feu Palo Alto Networks. Les pare-feu accèdent aux ressources Web dans le CDN pour exécuter différentes fonctions d'identification de contenu et d'application.

Le tableau suivant répertorie les ressources Web auxquelles accède le pare-feu pour une fonctionnalité ou une application :

Ressource	URL	Adresses statiques (si un serveur statique est requis)
Base de données d'une application Base de données des menaces/antivirus	• updates.paloaltonetworks.com (Global, hors Chine continentale) updates.paloaltonetworks.cn (Chine continentale uniquement) • Ajoutez les URL suivantes à votre liste d'autorisation de pare-feu si votre pare-feu dispose d'un accès limité à Internet : • downloads.paloaltonetworks.com:443 • proditpdownloads.paloaltonetworks.com:443 Il est recommandé de définir le serveur de mise à jour sur updates.paloaltonetworks.com. Cela permet au pare-feu Palo Alto Networks de recevoir des mises à jour de contenu du serveur le plus proche de celui-ci dans l'infrastructure CDN.	us-static.updates.paloaltonetworks.com Ajoutez les jeux d'adresses de serveur statiques IPv4 ou IPv6 suivants à votre liste d'autorisation de pare-feu : • **IPv4**— 35.186.202.45:443 et 34.120.74.244:443 • **IPv6**— [2600:1901:0:669::]:443 et [2600:1901:0:5162::]:443

Ressource	URL	Adresses statiques (si un serveur statique est requis)
	Si vous souhaitez obtenir des informations de référence supplémentaires ou si vous rencontrez des problèmes de connectivité et de téléchargement des mises à jour, reportez-vous à : https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u0000001UtRCAU La base de données Palo Alto Networks ThreatVault contient des informations sur les vulnérabilités, les exploits, les virus et les menaces de logiciels espions. Les fonctionnalités de pare-feu, y compris la sécurité DNS et le profil antivirus, utilisent la ressource suivante pour récupérer les informations d'identification de la menace afin de créer des exceptions : • data.threatvault.paloaltonetworks.com	*Les deux adresses IP fournies pour un type de protocole donné doivent être ajoutées à la liste d'autorisation pour une fonctionnalité appropriée.*
Filtrage d'URL PAND-DB | Filtrage d'URL avancé	*.urlcloud.paloaltonetworks.com Résout l'URL principale s0000.urlcloud.paloaltonetworks.com qui est ensuite redirigée vers le serveur régional le plus proche : • s0100.urlcloud.paloaltonetworks.com • s0200.urlcloud.paloaltonetworks.com • s0300.urlcloud.paloaltonetworks.com • s0500.urlcloud.paloaltonetworks.com	Les adresses IP statiques ne sont pas possibles. Vous pouvez toutefois résoudre manuellement une URL en adresse IP et autoriser l'accès à l'adresse IP du serveur régional.
Services Cloud	Résout en hawkeye.services-edge.paloaltonetworks.com puis est redirigé vers le serveur régional le plus proche : • États-Unis—**us.hawkeye.services-edge.paloaltonetworks.com** • Europe—**eu.hawkeye.services-edge.paloaltonetworks.com** • Royaume-Uni—**uk.hawkeye.services-edge.paloaltonetworks.com**	Les adresses IP statiques ne sont pas possibles.

Ressource	URL	Adresses statiques (si un serveur statique est requis)
	• APAC—**apac.hawkeye.services-edge.paloaltonetworks.com**	
Sécurité DNS	• Cloud—dns.service.paloaltonetworks.com:443 • Télémétrie—io.dns.service.paloaltonetworks.com:443 Lors du téléchargement d'une liste verte, dns.service.paloaltonetworks.com est résolu sur le serveur suivant : • static.dns.service.paloaltonetworks.com:443 • data.threatvault.paloaltonetworks.com (utilisé pour créer des exceptions DNS)	Les adresses IP statiques ne sont pas possibles.
ML en ligne basé sur un pare-feu : • URL Filtering Inline ML • WildFire Inline ML	• ml.service.paloaltonetworks.com:443	Les adresses IP statiques ne sont pas possibles.
WildFire	• Cloud (récupération de rapports) : wildfire.paloaltonetworks.com:443 Régions du cloud WildFire : • Global—wildfire.paloaltonetworks.com • Union européenne—eu.wildfire.paloaltonetworks.com • Japon—jp.wildfire.paloaltonetworks.com • Singapour—sg.wildfire.paloaltonetworks.com • Royaume-Uni—uk.wildfire.paloaltonetworks.com • Canada—ca.wildfire.paloaltonetworks.com • Australie—au.wildfire.paloaltonetworks.com • Allemagne—de.wildfire.paloaltonetworks.com • Inde—in.wildfire.paloaltonetworks.com	Les adresses IP statiques ne sont pas possibles.

Mise à niveau de Panorama

- Installer les mises à jour de contenu et les mises à niveau logicielles pour Panorama
- Résoudre les problèmes liés à votre mise à niveau Panorama
- Déployer des mises à niveau vers des pare-feu, des collecteurs de journaux et des appareils WildFire à l'aide de Panorama

Installer les mises à jour de contenu et les mises à niveau logicielles pour Panorama

Un abonnement de support valide permet d'accéder à l'image du logiciel et aux notes de version Panorama. Pour profiter des dernières corrections et améliorations de la sécurité, passez à la dernière mise à jour de logiciel et de contenu que votre revendeur ou un ingénieur système de Palo Alto Networks® recommande pour votre déploiement. La procédure d'installation des mises à jour de logiciel et de contenu dépend de si Panorama dispose d'une connexion directe à Internet et d'une configuration haute disponibilité (HD).

- Mettre à niveau Panorama avec une connexion Internet
- Mettre à niveau Panorama sans connexion Internet
- Installer des mises à jour de contenu automatiques de Panorama sans connexion Internet
- Mettre à niveau Panorama dans une configuration HA
- Migrer les journaux de Panorama vers le nouveau format de journal
- Mise à niveau de Panorama pour la capacité de gestion accrue des périphériques
- Mettre à niveau Panorama et les périphériques gérés en mode FIPS-CC
- Downgrader depuis Panorama 11.0

Mettre à niveau Panorama avec une connexion Internet

Si Panorama™ dispose d'une connexion directe à Internet, suivez les étapes suivantes pour installer les mises à jour du logiciel Panorama et du contenu au besoin. Si Panorama s'exécute dans une configuration haute disponibilité (HA), mettez à niveau le logiciel Panorama sur chaque homologue (voir Mettre à niveau Panorama dans une configuration HA). Si vous mettez à niveau Panorama et les périphériques gérés en mode FIPS-CC vers PAN-OS® 11.0 à partir de PAN-OS 10.2 ou version antérieure, vous devez effectuer les étapes supplémentaires de réinitialisation de l'état de connexion sécurisée des périphériques en mode FIPS-CC s'ils sont ajoutés à la gestion de Panorama lors de l'exécution d'une version de PAN-OS® 10.2. Pour plus de détails sur la mise à niveau des périphériques Panorama et FIPS-CC en mode FIPS-CC, reportez-vous à la section Mettre à niveau Panorama et les périphériques gérés en mode FIPS-CC.

La mise à niveau du logiciel sur l'appareil virtuel Panorama ne modifie pas le mode du système ; le passage en mode Panorama ou en mode de Gestion est une tâche manuelle qui nécessite des paramètres supplémentaires tels que décrits lorsque vous Set Up the Panorama Virtual Appliance with a Local Log Collector (configurez l'appareil virtuel Panorama avec le collecteur de journaux local).

Palo Alto Networks a introduit de nouveaux formats de données de journal à différents points de votre chemin de mise à niveau en fonction de la version de PAN-OS à partir de laquelle vous effectuez la mise à niveau.

- ***Upgrade from PAN-OS 8.1 to PAN-OS 9.0 (mise à niveau à partir de PAN-OS 8.1 vers PAN-OS 9.0)** : PAN-OS 9.0 a introduit un nouveau format de données de journal pour les collecteurs de journaux locaux et dédiés. Lorsque vous passez à PAN-OS 11.0, les données de journaux existantes sont automatiquement converties au nouveau format lors de la mise à niveau de PAN-OS 8.1 vers PAN-OS 9.0.*
- ***Upgrade from PAN-OS 10.0 to PAN-OS 10.1 (Mise à niveau à partir de PAN-OS 10.0 vers PAN OS 10.1)** : PAN-OS 10.1 a introduit un nouveau format de données de journal pour les collecteurs de journaux locaux et dédiés. Sur votre chemin de mise à niveau vers PAN-OS 11.0, les journaux générés dans PAN-OS 8.1 ou version antérieure ne sont plus disponibles. Cela inclut les journaux migrés dans le cadre de la mise à niveau vers PAN-OS 9.0. Après la mise à niveau vers PAN-OS 10.1, vous avez la possibilité de récupérer et de migrer ces journaux au format de journal PAN-OS 10.1.*

Vous devez mettre à niveau tous les collecteurs de journaux d'un groupe de collecteurs en même temps afin d'éviter de perdre des données de journal. Aucun transfert de journaux ou collecte de journaux ne se produit si les collecteurs de journaux d'un groupe de collecteurs n'utilisent pas tous la même version de PAN-OS. De plus, les données des journaux des collecteurs de journaux du groupe de collecteur ne sont pas visibles dans les onglets **ACC** ou **Monitor (Surveillance)** jusqu'à ce que tous les collecteurs de journaux exécutent la même version PAN-OS. Par exemple, si vous disposez de trois collecteurs de journaux dans un groupe de collecteurs et que vous mettez à niveau deux d'entre eux, aucun journal n'est alors transmis aux collecteurs de journaux du groupe de collecteurs.

Avant de mettre à jour Panorama, reportez-vous aux Release Notes (Notes de version) pour la version de contenu minimum requise pour PAN-OS 11.0.

STEP 1 | Vérifiez que les mises à jour que vous prévoyez d'installer sont appropriées pour votre déploiement Panorama.

Palo Alto Networks recommande fortement que Panorama, les collecteurs de journaux et tous les pare-feu gérés exécutent la même version de contenu.

- ☐ Consultez les Notes de version pour la version de contenu minimum requise pour une version de logiciel Panorama. Si vous souhaitez mettre à niveau des pare-feu et des collecteurs de journaux vers une version particulière, vous devez d'abord mettre à niveau Panorama à cette version (ou à une version ultérieure).
- ☐ Pour un appareil virtuel Panorama qui fonctionne sur un hyperviseur, assurez-vous que l'instance respecte la configuration prérequise pour l'appareil virtuel Panorama.

STEP 2 | Déterminer le chemin de mise à niveau vers PAN-OS 11.0..

Vous ne pouvez pas sauter l'installation de versions de fonctions dans le chemin de la version PAN-OS en cours vers PAN-OS 11.0.

Consultez Liste de contrôle de mise à niveau de PAN-OS, les problèmes connus et les modifications apportées au comportement par défaut dans les Release Notes (notes de version) et Considérations de mise à niveau/rétrogradation pour chaque version par laquelle vous passez dans le cadre de votre chemin de mise à niveau.

STEP 3 | Enregistrez une sauvegarde du fichier de configuration Panorama en cours que vous pouvez utiliser pour restaurer la configuration si vous rencontrez des problèmes avec la mise à niveau.

Bien que Panorama crée automatiquement une sauvegarde de la configuration, l'idéal consiste à créer et à stocker à l'extérieur une sauvegarde avant la mise à niveau.

1. Connectez-vous à l’interface Web Panorama.
2. Cliquez sur **Save named Panorama configuration snapshot (Enregistrer un instantané de configuration nommé Panorama)** (**Panorama** > **Setup (Configuration)** > **Operations (Opérations)**), entrez un **Name (Nom)** pour la configuration et cliquez sur **OK**.
3. Cliquez sur **Export named Panorama configuration snapshot (Exporter l'instantané de configuration nommé Panorama)**, sélectionnez le **Name (Nom)** de la configuration que vous venez d'enregistrer, cliquez sur **OK**, et enregistrez le fichier exporté à un emplacement qui est externe à Panorama.

STEP 4 | (Best Practices (Meilleures pratiques)) Si vous utilisez Cortex Data Lake (CDL), install the Panorama device certificate (installez le certificat de périphérique Panorama).

Panorama passe automatiquement à l'utilisation du certificat de périphérique pour l'authentification avec l'ingestion de CDL et les points de terminaison de requête lors de la mise à niveau vers PAN-OS 11.0.

Si vous n’installez pas le certificat de périphérique avant la mise à niveau vers PAN-OS 11.0, Panorama continue d’utiliser le certificat de service de journalisation existant pour l’authentification.

STEP 5 | Installez les dernières mises à jour de contenu.

Si Panorama n'exécute pas les versions de contenu minimum requises pour la version Panorama vers laquelle vous souhaitez effectuer la mise à niveau, vous devez mettre à jour les versions de contenu vers les versions minimales (ou ultérieures) avant d'installer les mises à jour logicielles. Consultez les Notes de version *pour la version de contenu minimale pour une version de Panorama.*

Palo Alto Networks® recommande fortement que Panorama, les collecteurs de journaux et tous les pare-feu gérés exécutent la même version de contenu. De plus, nous vous recommandons de planifier des mises à jour automatiques et récurrentes afin que vous exécutiez toujours les dernières versions de contenu (reportez-vous à 14*).*

1. Sélectionnez **Panorama** > **Dynamic Updates (Mises à jour dynamiques)** et **Check Now (Vérifiez maintenant)** pour obtenir les dernières mises à jour. Si la valeur dans la colonne Action est **Download (Télécharger)**, une mise à jour est disponible.

   Assurez-vous que Panorama exécute la même version de contenu, mais pas une version ultérieure à celle exécutée sur les pare-feu gérés et les collecteurs de journaux.

2. Avant de mettre à jour la version du contenu sur Panorama, assurez-vous de Mettre à niveau le pare-feu vers PAN-OS 11.0 à partir de Panorama puis les collecteurs de journaux (voir Upgrade Log Collectors When Panorama Is Internet-Connected (Mettre à niveau les collecteurs de journaux lorsque Panorama est connecté à Internet) à la même version de contenu (ou une version ultérieure).

   Si vous n'avez pas besoin d'installer de mises à jour de contenu pour le moment, passez directement à la prochaine étape.

3. Installez les mises à jour de contenu restantes en fonction des besoins. Lorsque l'installation est terminée, la colonne Currently Installed (Actuellement installé) affiche une coche.

   1. **Download (Téléchargez)** et **Install (installez)** les applications ou les applications et mises à jour des menaces. Indépendamment de votre abonnement, Panorama installe et n'a besoin que de la mise à jour de contenu des applications, et non du contenu des menaces. Pour plus d'informations, consultez la section Compatibilité des versions de Panorama, des collecteurs de journaux, des pare-feu et de WildFire .
   2. **Download (Téléchargez)** et **Install (Installez)** toutes les autres mises à jour (antivirus, WildFire® ou filtrage d'URL) une à la fois, dans n'importe quel ordre.

STEP 6 | Sélectionnez **Panorama** > **Plugins** et **Download (Télécharger)** la version du plug-in prise en charge sur PAN-OS 11.0 pour tous les plugins actuellement installés sur Panorama.

Consultez la Compatibility Matrix (matrice de compatibilité) pour la version du plug-in Panorama prise en charge pour votre version PAN-OS 11.0 cible.

Cela est nécessaire pour réussir la mise à niveau de Panorama de PAN-OS 10.2 vers PAN-OS 11.0. La mise à niveau vers PAN-OS 11.0 est bloquée si la version du plug-in prise en charge n'est pas téléchargée.

Les plug-ins téléchargés requis pour effectuer la mise à niveau vers PAN-OS 11.0 s'installent automatiquement après la mise à niveau réussie de Panorama vers PAN-OS 11.0. Si un plug-in téléchargé ne s'installe pas automatiquement, vous devez installer manuellement le plug-in concerné après la mise à niveau vers PAN-OS 11.0.

STEP 7 | Mettez à niveau Panorama vers les versions PAN-OS le long de votre chemin de mise à niveau vers PAN-OS 11.0.

1. Upgrade Panorama with an Internet Connection (Mettez à niveau Panorama avec une connexion Internet) vers PAN-OS 8.1.
2. Upgrade Panorama with an Internet Connection (Mettez à niveau) Panorama avec une connexion Internet vers PAN-OS 9.0.

   PAN-OS 9.0 a introduit un nouveau format de journal. Si un Collecteur de journaux local est configuré, les journaux sont automatiquement migrés vers le nouveau format après la mise à niveau réussie de Panorama vers PAN-OS 9.0.

   Ne poursuivez pas votre chemin de mise à niveau tant que vous n'avez pas vérifié que la migration automatique du journal s'est terminée avec succès.
3. Upgrade Panorama with an Internet Connection (Mettez à niveau Panorama avec une connexion Internet) vers PAN-OS 9.1.
4. Upgrade Panorama with an Internet Connection (Mettez à niveau Panorama avec une connexion Internet) vers PAN-OS 10.0.

   *(Panorama in Legacy mode only (Panorama en mode hérité uniquement)) **Download (Téléchargez)** PAN-OS 10.0.0, puis **Download (téléchargez)** et **Installe (installez)** PAN-OS 10.0.8 ou version ultérieure avant de poursuivre votre chemin de mise à niveau.*

   Ceci est nécessaire pour conserver tous les journaux stockés sur la partition de stockage NFS. Certains journaux stockés sur la partition de stockage NFS d'un Panorama en mode hérité sont supprimés si vous installez PAN-OS 10.0.7 ou une version antérieure de PAN-OS 10.0.
5. Upgrade Panorama with an Internet Connection (Mettez à niveau Panorama avec une connexion Internet) vers PAN-OS 10.1.

   PAN-OS 10.1 introduit un nouveau format de journal. Lors de la mise à niveau de PAN-OS 10.0 vers PAN-OS 10.1, vous pouvez choisir de migrer les journaux générés dans PAN-OS 8.1 ou une version antérieure. Sinon, ces journaux sont automatiquement supprimés lors de la mise à niveau réussie vers PAN-OS 10.1. Lors de la migration, les données des journaux ne sont pas

visibles dans les onglets ACC ou Monitor (Surveillance). Pendant la migration, les données de journal continuent d'être transmises au collecteur de journaux approprié, mais vous pouvez avoir un impact sur les performances.

> *(Panorama in Legacy mode only (Panorama en mode hérité uniquement))* ***Download (Téléchargez)*** *PAN-OS 10.1.0, puis* ***Download (téléchargez)*** *et* ***Install (installez)*** *PAN-OS 10.1.3 ou version ultérieure.*
>
> *Ceci est nécessaire pour conserver tous les journaux stockés sur la partition de stockage NFS. Certains journaux stockés sur la partition de stockage NFS d'un panorama en mode hérité sont supprimés si vous installez PAN-OS 10.1.2 ou une version antérieure de PAN-OS 10.1.*

6. Upgrade Panorama with an Internet Connection (Mettez à niveau Panorama avec une connexion Internet) vers PAN-OS 10.2.

STEP 8 | Mettez à niveau Panorama vers PAN-OS 11.0.

1. Cliquez sur **Check Now (Vérifier maintenant)** (**Panorama** > **Software (Logiciel)**) pour rechercher les dernières mises à jour. Si une version logicielle est disponible, la colonne Action affiche **Download (Télécharger)**.
2. Recherchez et **Download (téléchargez)** l'image PAN-OS 11.0.0. Après un téléchargement réussi, la colonne Action passe de **Download (Télécharger)** à **Install (Installer)** pour l'image téléchargée.
3. Installez l'image téléchargée, puis redémarrez.
   1. Installez l'image.
   2. Une fois l'installation terminée, redémarrez en utilisant l'une des méthodes suivantes :
      - Si vous êtes invité à redémarrer, cliquez sur **Yes (Oui)**. Si une invite CMS Login s'affiche, appuyez sur Entrée sans saisir de nom d'utilisateur ou de mot de passe. Lorsque l'invite de connexion Panorama s'affiche, saisissez le nom d'utilisateur et le mot de passe que vous avez spécifiés lors de la configuration initiale.
      - Si vous n'êtes pas invité à redémarrer, cliquez sur **Reboot Panorama (Redémarrer Panorama)** dans la section Device Operations (Opérations de périphérique) (**Panorama** > **Setup (Configuration)** > **Operations (Opérations)**).

STEP 9 | Après le redémarrage de Panorama, vérifiez que les versions de votre plug-in Panorama sont prises en charge par PAN-OS 11.0.

Vous devez vérifier et installer la version du plug-in Panorama prise en charge sur PAN-OS 11.0 après avoir correctement mis à niveau Panorama. Consultez la Compatibility Matrix (matrice de compatibilité) pour plus d'informations sur les plug-ins Panorama pris en charge sur PAN-OS 11.0.

1. Connectez-vous à l'interface Web de Panorama et consultez le widget Informations générales dans le **tableau de bord** pour vérifier que les versions du plug-in compatibles PAN-OS 11.0 ont été correctement installées.

   Vous pouvez également vous connecter à l'interface de ligne de commande Panorama et entrer la commande `show plugins installed (afficher les plugins installés)` pour afficher la liste des plugins actuellement installés.
2. Sélectionnez **Panorama** > **Plugins** et recherchez le plugin qui n'a pas été installé.
3. **Installez** la version du plug-in prise en charge sur PAN-OS 11.0.
4. Répétez les étapes ci-dessus jusqu'à ce que tous les plug-ins installés sur Panorama exécutent la version prise en charge sur PAN-OS 11.0.

STEP 10 | (Si le collecteur de journaux locaux dans un groupe de collecteurs uniquement) Mettez à niveau les collecteurs de journaux restants dans le groupe de collecteurs.

- Mettre à niveau les collecteurs de journaux lorsque Panorama est connecté à Internet
- Mettre à niveau les collecteurs de journaux lorsque Panorama n'est pas connecté à Internet

STEP 11 | (Panorama and managed devices in FIPS-CC mode (Panorama et périphériques gérés en mode FIPS-CC)) Mettre à niveau Panorama et les périphériques gérés en mode FIPS-CC.

La mise à niveau de Panorama et des périphériques gérés en mode FIPS-CC nécessite que vous réinitialisiez l'état de connexion sécurisée des périphériques en mode FIPS-CC s'ils sont ajoutés à la gestion de Panorama lors de l'exécution d'une version de PAN-OS 11.0. Vous devez réintégrer les appareils gérés suivants à la gestion Panorama :

- Appareils gérés en mode FIPS-CC ajoutés à Panorama à l'aide de la clé d'authentification d'enregistrement de périphérique.
- Appareils gérés en mode de fonctionnement normal ajoutés à Panorama à l'aide de la clé

d'authentification d'enregistrement de périphérique Vous n'avez pas besoin de réintégrer les appareils gérés ajoutés à la gestion Panorama lorsque l'appareil géré exécutait un PAN-OS 10.0 ou une version antérieure.

STEP 12 | (PAN-OS 10.2 et versions ultérieures) Régénérez ou réimportez tous les certificats pour respecter le niveau de sécurité OpenSSL 2.

Cette étape est requise si vous effectuez une mise à niveau de PAN-OS 10.1 ou version antérieure vers PAN-OS 11.0. Ignorez cette étape si vous effectuez une mise à niveau à partir de PAN-OS 10.2 et que vous avez déjà régénéré ou réimporté vos certificats.

Tous les certificats doivent satisfaire aux exigences minimales suivantes :

- RSA 2048 bits ou supérieur, ou ECDSA 256 bits ou supérieur
- Digest de SHA256 ou supérieur

Consultez le Guide de l'administrateur PAN-OS ou le Guide de l'administrateur de Panorama pour plus d'informations sur la régénération ou la réimportation de vos certificats.

STEP 13 | (Recommended for Panorama mode (Recommandé pour le mode Panorama) Augmentez la mémoire de l'appareil virtuel Panorama à 64 Go.

Après avoir correctement mis à niveau l'appareil virtuel Panorama en mode Panorama ers PAN-OS 11.0, Palo Alto Networks recommande d'augmenter la mémoire de l'appareil virtuel Panorama à 64 Go pour répondre à la configuration système requise accrue afin d'éviter tout problème de journalisation, de gestion et de performances opérationnelles lié à un appareil virtuel Panorama sous-provisionnée.

STEP 14 | (Recommandé) Programmez les mises à jour automatiques de contenu.

Panorama ne synchronise pas les calendriers de mise à jour de contenu dans les paires HD. Vous devez effectuer cette tâche à la fois sur le panorama actif et passif.

Dans la ligne d'en-tête pour chaque type (**Panorama** > **Dynamic Updates (Mises à jour dynamiques)**), le **Schedule (Calendrier)** est initialement défini sur **None (Aucune)**. Effectuez les étapes suivantes pour chaque type de journal.

1. Cliquez sur **None (Aucune)** et sélectionnez la fréquence de mise à jour (**Recurrence (récurrence)**). Les options de fréquence disponibles dépendent du type de la mise à jour.
2. Sélectionnez l'action de planification :
   - **Download And Install (Téléchargez et installez)** (recommandé) : Panorama installe automatiquement les mises à jour après les avoir téléchargées.

     Download Only (Télécharger uniquement) : vous devez installer manuellement les mises à jour après que panorama les télécharge.
3. En fonction des meilleures pratiques pour la posture de sécurité de votre organisation, configurez un délai (**Threshold (Seuil)**) après qu'une mise à jour devient disponible avant que Panorama ne télécharge la mise à jour.
4. Cliquez sur **OK** pour enregistrer vos modifications.
5. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements.

STEP 15 | (Enterprise DLP only (Enterprise DLP uniquement)) Edit the Enterprise DLP data filtering settings (Modifiez les paramètres de filtrage des données Enterprise DLP) pour réduire la **Max File Size (taille maximale du fichier)** à 20 Mo ou moins.

Ceci est nécessaire lors de la mise à niveau du plug-in Panorama pour Enterprise DLP 3.0.3 ou versions ultérieures vers Enterprise DLP 4.0.0 car cette version du plug-in ne prend pas en charge large file size inspection (l'inspection de la taille des fichiers volumineux).

Mettre à niveau Panorama sans connexion Internet

Si Panorama™ ne dispose pas d'une connexion directe à Internet, suivez les étapes suivantes pour installer le logiciel Panorama et les mises à jour logicielles et de contenu au besoin. Si Panorama est déployé dans une configuration haute disponibilité (HA), vous devez mettre à niveau chaque homologue (voir Mettre à niveau Panorama dans une configuration HA). Si vous mettez à niveau Panorama et les périphériques gérés en mode FIPS-CC vers PAN-OS 11.0 à partir de PAN-OS 10.2 ou version antérieure, vous devez effectuer les étapes supplémentaires de réinitialisation de l'état de connexion sécurisée des périphériques en mode FIPS-CC s'ils sont ajoutés à la gestion de Panorama lors de l'exécution d'une version de PAN-OS 10.2. Pour plus de détails sur la mise à niveau des périphériques Panorama et FIPS-CC en mode FIPS-CC, reportez-vous à la section Mettre à niveau Panorama et les périphériques gérés en mode FIPS-CC.

La mise à niveau du logiciel sur l'appareil virtuel Panorama ne modifie pas le mode du système ; le passage en mode Panorama ou en mode de Gestion est une tâche manuelle qui nécessite des paramètres supplémentaires tels que décrits lorsque vous Set Up the Panorama Virtual Appliance with a Local Log Collector (configurez l'appareil virtuel Panorama avec le collecteur de journaux local).

Palo Alto Networks a introduit de nouveaux formats de données de journal à différents points de votre chemin de mise à niveau en fonction de la version de PAN-OS à partir de laquelle vous effectuez la mise à niveau.

- ***Upgrade from PAN-OS 8.1 to PAN-OS 9.0 (mise à niveau à partir de PAN-OS 8.1 vers PAN-OS 9.0)** : PAN-OS 9.0 a introduit un nouveau format de données de journal pour les collecteurs de journaux locaux et dédiés. Lorsque vous passez à PAN-OS 11.0, les données de journaux existantes sont automatiquement converties au nouveau format lors de la mise à niveau de PAN-OS 8.1 vers PAN-OS 9.0.*
- ***Upgrade from PAN-OS 10.0 to PAN-OS 10.1 (Mise à niveau à partir de PAN-OS 10.0 vers PAN OS 10.1)** : PAN-OS 10.1 a introduit un nouveau format de données de journal pour les collecteurs de journaux locaux et dédiés. Sur votre chemin de mise à niveau vers PAN-OS 11.0, les journaux générés dans PAN-OS 8.1 ou version antérieure ne sont plus disponibles. Cela inclut les journaux migrés dans le cadre de la mise à niveau vers PAN-OS 9.0. Après la mise à niveau vers PAN-OS 10.1, vous avez la possibilité de récupérer et de migrer ces journaux au format de journal PAN-OS 10.1.*

Vous devez mettre à niveau tous les collecteurs de journaux d'un groupe de collecteurs en même temps afin d'éviter de perdre des données de journal. Aucun transfert de journaux ou collecte de journaux ne

se produit si les collecteurs de journaux d'un groupe de collecteurs n'utilisent pas tous la même version de PAN-OS. De plus, les données des journaux des collecteurs de journaux du groupe de collecteur ne sont pas visibles dans les onglets **ACC** ou **Monitor (Surveillance)** jusqu'à ce que tous les collecteurs de journaux exécutent la même version PAN-OS. Par exemple, si vous disposez de trois collecteurs de journaux dans un groupe de collecteurs et que vous mettez à niveau deux d'entre eux, aucun journal n'est alors transmis aux collecteurs de journaux du groupe de collecteurs.

Avant de mettre à jour Panorama, reportez-vous aux Release Notes (Notes de version) pour la version de contenu minimum requise pour PAN-OS® 11.0.

STEP 1 | Vérifiez que les mises à jour que vous prévoyez d'installer sont appropriées pour votre déploiement Panorama.

Palo Alto Networks recommande fortement que Panorama, les collecteurs de journaux et tous les pare-feu gérés exécutent la même version de contenu.

- Consultez les Notes de version pour la version minimale du contenu que vous devez installer pour une version de Panorama. Si vous souhaitez mettre à niveau des pare-feu et des collecteurs de journaux vers une version particulière, vous devez d'abord mettre à niveau Panorama à cette version (ou à une version ultérieure).
- Pour un appareil virtuel Panorama, assurez-vous que l'instance respecte la configuration prérequise pour l'appareil virtuel Panorama.

STEP 2 | Déterminer le chemin de mise à niveau vers PAN-OS 11.0..

Vous ne pouvez pas sauter l'installation de versions de fonctions dans le chemin de la version PAN-OS en cours vers PAN-OS 11.0.

Consultez Liste de contrôle de mise à niveau de PAN-OS, les problèmes connus et les modifications apportées au comportement par défaut dans les Release Notes (notes de version) et Considérations de mise à niveau/rétrogradation pour chaque version par laquelle vous passez dans le cadre de votre chemin de mise à niveau.

STEP 3 | Enregistrez une sauvegarde du fichier de configuration Panorama en cours que vous pouvez utiliser pour restaurer la configuration si vous rencontrez des problèmes avec la mise à niveau.

Bien que Panorama crée automatiquement une sauvegarde de la configuration, l'idéal consiste à créer et à stocker à l'extérieur une sauvegarde avant la mise à niveau.

1. Connectez-vous à l'interface Web Panorama.
2. Cliquez sur **Save named Panorama configuration snapshot (Enregistrer un instantané de configuration nommé Panorama)** (**Panorama** > **Setup (Configuration)** > **Operations (Opérations)**), entrez un **Name (Nom)** pour la configuration et cliquez sur **OK**.
3. Cliquez sur **Export named Panorama configuration snapshot (Exporter l'instantané de configuration nommé Panorama)**, sélectionnez le **Name (Nom)** de la configuration que vous venez d'enregistrer, cliquez sur **OK**, et enregistrez le fichier exporté à un emplacement qui est externe à Panorama.

STEP 4 | Téléchargez des mises à jour de contenu vers un hôte qui peut se connecter et chargez le contenu sur Panorama via SCP ou HTTPS.

Si vous n'avez pas besoin d'installer de mises à jour de contenu pour le moment, passez directement à l'étape 6.

1. Utilisez un hôte qui dispose d'un accès à Internet pour ouvrir une session sur le site Web d'assistance client de Palo Alto Networks.
2. Téléchargez les mises à jour de contenu au besoin :
   1. Cliquez sur **Updates (Mises à jour)** > **Dynamic Updates (Mises à jour dynamiques)** dans la section Ressources.
   2. **Download (Téléchargez)** les mises à jour de contenu appropriées et enregistrez les fichiers sur l'hôte. Effectuez cette étape pour chaque type de contenu que vous devez mettre à jour.

STEP 5 | Installez les dernières mises à jour de contenu.

Vous devez installer les mises à jour de contenu et vous devez premièrement Mettre à niveau le pare-feu vers PAN-OS 11.0 à partir de Panorama *et ensuite* Mettre à jour les collecteurs de journaux *avant de les installer sur le serveur de gestion Panorama.*

Installez d'abord les mises à jour des applications ou des applications et menaces, puis installez toutes les autres mises à jour (Antivirus, WildFire® ou Filtrage d'URL) une à la fois dans n'importe quel ordre.

Peu importe si votre abonnement comprend le contenu Applications et Menaces, Panorama installe et n'a besoin que du contenu Applications. Pour plus d'informations, consultez la section Compatibilité des versions de Panorama, des collecteurs de journaux, des pare-feu et de WildFire .

Log in to the Panorama web interface (Connectez-vous à l'interface Web Panorama) et effectuez les étapes suivantes pour chaque type de contenu :

1. Sélectionnez **Panorama** > **Dynamic Updates (Mises à jour dynamiques)**.
2. Cliquez sur **Download (Télécharger)**, sélectionnez le **Type** de contenu, **Browse (Recherchez)** l'emplacement sur l'hôte sur lequel vous avez téléchargé la mise à jour, sélectionnez la mise à jour, puis cliquez sur **OK**.
3. Cliquez sur **Install From File (Installer depuis le fichier)**, sélectionnez le **Package Type (Type de package)** et cliquez **OK**.

STEP 6 | Téléchargez la version du plug-in prise en charge sur PAN-OS 11.0 pour tous les plug-ins actuellement installés sur Panorama.

Consultez la Compatibility Matrix (matrice de compatibilité) pour la version du plug-in Panorama prise en charge pour votre version PAN-OS 11.0 cible.

Cela est nécessaire pour réussir la mise à niveau de Panorama de PAN-OS 10.2 vers PAN-OS 11.0. La mise à niveau vers PAN-OS 11.0 est bloquée si la version du plug-in prise en charge n'est pas téléchargée.

Les plug-ins téléchargés requis pour effectuer la mise à niveau vers PAN-OS 11.0 s'installent automatiquement après la mise à niveau réussie de Panorama vers PAN-OS 11.0. Si un plug-in téléchargé ne s'installe pas automatiquement, vous devez installer manuellement le plug-in concerné après la mise à niveau vers PAN-OS 11.0

1. Téléchargez la version du plugin prise en charge sur PAN-OS 11.0.
   1. Connectez-vous au portail de support de Palo Alto Networks.
   2. Sélectionnez **Updates (Mises à jour)** > **Software Updates (mises à jour logicielles)** et sélectionnez le plug-in dans le menu déroulant.
   3. **Download (Téléchargez)** la version du plugin prise en charge sur PAN-OS 10.2.
   4. Répétez cette étape pour tous les plug-ins actuellement installés sur Panorama.
2. Se connecter à l'interface Web Panorama
3. Sélectionnez **Panorama** > **Plugins** et **Upload (Téléchargez)** la version du plugin que vous avez téléchargée à l'étape précédente.

   Répétez cette étape pour tous les plug-ins actuellement installés sur Panorama.

STEP 7 | Mettez à niveau Panorama vers les versions PAN-OS le long de votre chemin de mise à niveau vers PAN-OS 10.2.

1. Upgrade Panorama When Not Internet Connected (Mettez à niveau Panorama lorsque vous n'êtes pas connecté à Internet) vers PAN-OS 8.1.
2. Upgrade Panorama When Not Internet Connected (Mettez à niveau Panorama lorsque vous n'êtes pas connecté à Internet) vers PAN-OS 9.0.

   PAN-OS 9.0 a introduit un nouveau format de journal. Si un Collecteur de journaux local est configuré, les journaux sont automatiquement migrés vers le nouveau format après la mise à niveau réussie de Panorama vers PAN-OS 9.0.

   Ne poursuivez pas votre chemin de mise à niveau tant que vous n'avez pas vérifié que la migration automatique du journal s'est terminée avec succès.
3. Upgrade Panorama When Not Internet Connected (Mettez à niveau Panorama lorsque vous n'êtes pas connecté à Internet) vers PAN-OS 9.1.
4. Upgrade Panorama When Not Internet Connected (Mettez à niveau Panorama lorsque vous n'êtes pas connecté à Internet) vers PAN-OS 10.0.

   (Panorama in Legacy mode only (Panorama en mode hérité uniquement)) ***Download (Téléchargez)*** *PAN-OS 10.0.0, puis* ***Download (téléchargez)*** *et* ***Installe (installez)*** *PAN-OS 10.0.8 ou version ultérieure avant de poursuivre votre chemin de mise à niveau.*

   Ceci est nécessaire pour conserver tous les journaux stockés sur la partition de stockage NFS. Certains journaux stockés sur la partition de stockage NFS d'un Panorama en mode hérité sont supprimés si vous installez PAN-OS 10.0.7 ou une version antérieure de PAN-OS 10.0.
5. Upgrade Panorama When Not Internet Connected (Mettez à niveau Panorama lorsque vous n'êtes pas connecté à Internet) vers PAN-OS 10.1.

   PAN-OS 10.1 introduit un nouveau format de journal. Lors de la mise à niveau de PAN-OS 10.0 vers PAN-OS 10.1, vous pouvez choisir de migrer les journaux générés dans PAN-OS 8.1 ou une version antérieure. Sinon, ces journaux sont automatiquement supprimés lors de la mise à niveau réussie vers PAN-OS 10.1. Lors de la migration, les données des journaux ne sont pas visibles dans les onglets ACC ou Monitor (Surveillance). Pendant la migration, les données de

journal continuent d'être transmises au collecteur de journaux approprié, mais vous pouvez avoir un impact sur les performances.

(Panorama in Legacy mode only (Panorama en mode hérité uniquement)) ***Download (Téléchargez)*** *PAN-OS 10.1.0, puis* ***Download (téléchargez)*** *et* ***Install (installez)*** *PAN-OS 10.1.3 ou version ultérieure.*

Ceci est nécessaire pour conserver tous les journaux stockés sur la partition de stockage NFS. Certains journaux stockés sur la partition de stockage NFS d'un panorama en mode hérité sont supprimés si vous installez PAN-OS 10.1.2 ou une version antérieure de PAN-OS 10.1.

6. Upgrade Panorama When Not Internet Connected (Mettez à niveau Panorama lorsque vous n'êtes pas connecté à Internet) vers PAN-OS 10.2.

STEP 8 | Téléchargez la dernière image de la version PAN-OS 11.0 sur un hôte qui peut se connecter et télécharger du contenu vers Panorama via SCP ou HTTPS.

1. Utilisez un hôte avec accès à Internet pour ouvrir une session sur le site Web d'assistance client de Palo Alto Networks.
2. Télécharger les mises à jour logicielles :
   1. Sur la page principale du site d'assistance client de Palo Alto Networks, cliquez sur **Updates (Mises à jour)** > **Software Updates (Mises à jour logicielles)**.
   2. Recherchez le modèle spécifique à la dernière image de la version PAN-OS 11.0. Par exemple, pour mettre à niveau un appareil M-Series vers Panorama 11.0.0, téléchargez l'image `Panorama_m-11.0.0`. Pour mettre à niveau un appareil virtuel Panorama vers Panorama 11.0.0, téléchargez l'image `Panorama_pc-11.0.0`.

      Vous pouvez rapidement localiser les images de Panorama en sélectionnant ***Panorama M Images (Images M Panorama)*** *(appareils de série M) ou* ***Panorama Updates (Mises à jour de Panorama)*** *(appareils virtuels) du menu déroulant* ***Filter By (Filtrer par)***.
   3. Cliquez sur le nom du fichier et enregistrez le fichier sur l'hôte.

STEP 9 | Mettez à niveau Panorama vers PAN-OS 11.0.

1. Connectez-vous à l'interface Web Panorama.
2. Sélectionnez **Panorama** > **Software (logiciel)** et **Upload (téléchargez)** l'image PAN-OS 11.0 que vous avez téléchargée à l'étape précédente.
3. **Browse (Naviguez)** vers l'emplacement de l'hôte sur lequel vous avez téléchargé la mise à jour, sélectionnez la mise à jour, **Sync to peer (Synchronisez avec l'homologue)** si Panorama est

dans une configuration HD (pour appliquer l'image du logicielle à l'homologue secondaire), puis cliquez sur **OK**.

4. Installez l'image du logiciel et redémarrez.

   Pour une configuration HA, Mettre à niveau Panorama dans une configuration HA ; sinon :

   1. **Install (Installez)** l'image téléchargée.
   2. Après avoir terminé l'installation avec succès, redémarrez en utilisant l'une des méthodes suivantes :

      - Si vous êtes invité à redémarrer, cliquez sur **Yes (Oui)**. Si une invite CMS Login s'affiche, appuyez sur Entrée sans saisir de nom d'utilisateur ou de mot de passe. Lorsque l'invite de connexion Panorama s'affiche, saisissez le nom d'utilisateur et le mot de passe que vous avez spécifiés lors de la configuration initiale.
      - Si vous n'êtes pas invité à redémarrer, cliquez sur **Reboot Panorama (Redémarrer Panorama)** dans la section Device Operations (Opérations de périphérique) (**Panorama** > **Setup (Configuration)** > **Operations (Opérations)**).

STEP 10 | Après le redémarrage de Panorama, vérifiez que les versions de votre plug-in Panorama sont prises en charge par PAN-OS 11.0.

Vous devez vérifier et installer la version du plug-in Panorama prise en charge sur PAN-OS 11.0 après avoir correctement mis à niveau Panorama. Consultez la Compatibility Matrix (matrice de compatibilité) pour plus d'informations sur les plug-ins Panorama pris en charge sur PAN-OS 11.0.

1. Connectez-vous à l'interface Web de Panorama et consultez le widget Informations générales dans le **tableau de bord** pour vérifier que les versions du plug-in compatibles PAN-OS 11.0 ont été correctement installées.

   Vous pouvez également vous connecter à l'interface de ligne de commande Panorama et entrer la commande `show plugins installed (afficher les plugins installés)` pour afficher la liste des plugins actuellement installés.
2. Sélectionnez **Panorama** > **Plugins** et recherchez le plugin qui n'a pas été installé.
3. **Installez** la version du plug-in prise en charge sur PAN-OS 11.0.
4. Répétez les étapes ci-dessus jusqu'à ce que tous les plug-ins installés sur Panorama exécutent la version prise en charge sur PAN-OS 11.0.

STEP 11 | (Si le collecteur de journaux locaux dans un groupe de collecteurs uniquement) Mettez à niveau les collecteurs de journaux restants dans le groupe de collecteurs.

- Mettre à niveau les collecteurs de journaux lorsque Panorama est connecté à Internet
- Mettre à niveau les collecteurs de journaux lorsque Panorama n'est pas connecté à Internet

STEP 12 | (Panorama and managed devices in FIPS-CC mode (Panorama et périphériques gérés en mode FIPS-CC)) Mettre à niveau Panorama et les périphériques gérés en mode FIPS-CC.

La mise à niveau de Panorama et des périphériques gérés en mode FIPS-CC nécessite que vous réinitialisiez l'état de connexion sécurisée des périphériques en mode FIPS-CC s'ils sont ajoutés à la

gestion de Panorama lors de l'exécution d'une version de PAN-OS 11.0. Vous devez réintégrer les appareils gérés suivants à la gestion Panorama :

- Appareils gérés en mode FIPS-CC ajoutés à Panorama à l'aide de la clé d'authentification d'enregistrement de périphérique.
- Appareils gérés en mode de fonctionnement normal ajoutés à Panorama à l'aide de la clé

d'authentification d'enregistrement de périphérique Vous n'avez pas besoin de réintégrer les appareils gérés ajoutés à la gestion Panorama lorsque l'appareil géré exécutait un PAN-OS 10.0 ou une version antérieure.

STEP 13 | (PAN-OS 10.2 et versions ultérieures) Régénérez ou réimportez tous les certificats pour respecter le niveau de sécurité OpenSSL 2.

Cette étape est requise si vous effectuez une mise à niveau de PAN-OS 10.1 ou version antérieure vers PAN-OS 11.0. Ignorez cette étape si vous effectuez une mise à niveau à partir de PAN-OS 10.2 et que vous avez déjà régénéré ou réimporté vos certificats.

Tous les certificats doivent satisfaire aux exigences minimales suivantes :

- RSA 2048 bits ou supérieur, ou ECDSA 256 bits ou supérieur
- Digest de SHA256 ou supérieur

Consultez le Guide de l'administrateur PAN-OS ou le Guide de l'administrateur de Panorama pour plus d'informations sur la régénération ou la réimportation de vos certificats.

STEP 14 | (Recommended for Panorama mode (Recommandé pour le mode Panorama) Augmentez la mémoire de l'appareil virtuel Panorama à 64 Go.

Après avoir correctement mis à niveau l'appareil virtuel Panorama en mode Panorama ers PAN-OS 11.0, Palo Alto Networks recommande d'augmenter la mémoire de l'appareil virtuel Panorama à 64 Go pour répondre à la configuration système requise accrue afin d'éviter tout problème de journalisation, de gestion et de performances opérationnelles lié à un appareil virtuel Panorama sous-provisionnée.

Installer des mises à jour de contenu automatiques de Panorama sans connexion Internet

Téléchargez automatiquement des mises à jour de contenu vers les pare-feux, les Collecteurs de journaux et les appareil WildFire® sur les réseaux à air gap lorsque le serveur de gestion Panorama™, les pare-feux gérés, les Collecteurs de journaux et les appareils WildFire ne sont pas connectés à Internet. Afin de faire cela, vous devez déployer un Panorama supplémentaire avec un accès internet et un serveur SCP. Après avoir déployé le Panorama avec un accès internet, vous configurez le Panorama connecté à internet afin qu'il télécharge automatiquement les mises à jour de contenu sur le serveur SCP. Depuis le serveur SCP, la Panorama à air gap est configuré afin de télécharger et installer automatiquement les mises à jour de contenu selon votre programme de mises à jour de contenu. Panorama génère un journal système lorsque le Panorama avec un accès à internet télécharge des mises à jour de contenu sur le serveur SCP ou lorsque le Panorama à air gap télécharge et installe les mises à jour de contenu depuis le serveur SCP.

Seuls les programmes de mises à jour de contenu suivants depuis un Panorama connecté à internet vers un Panorama sans connexion internet sont possibles :

Ne manipulez pas et ne modifiez pas le nom du fichier de mise à jour de contenu après l'avoir téléchargé sur le serveur SCP. Panorama ne peut pas télécharger et installer des mises à jour de contenu ayant des noms de fichiers modifiés. Par ailleurs, pour que la mise à jour de contenu réussisse, vous devez vous assurer qu'il y a assez d'espace disque sur le serveur SCP, que le serveur SCP fonctionne lorsqu'un téléchargement est sur le point de commencer et que les deux Panoramas sont alimentés et non au milieu d'un redémarrage.

Le présent exemple montre comment configurer les mises à jour de contenu automatiques pour les mises à jour de contenu des Applications et des Menaces.

STEP 1 | Déployer un serveur SCP.

Les mises à jour de contenu pare-feux gérés, Collecteurs de journaux et appareils WildFire sont téléchargées depuis le Panorama connecté à internet. Le Panorama air gap télécharge les mises à jour de contenu depuis le serveur SCP et les installe sur les pare-feux gérés, les appareils WildFire et les Collecteurs de journaux.

Lorsque vous créez le répertoire de dossiers pour des mises à jour de contenu, les bonnes pratiques consistent à créer un dossier pour chaque type de mise à jour de contenu. C'est l'inconvénient de gérer un gros volume de mises à jour de contenu et cela réduit la possibilité de supprimer des mises à jour de contenu qui ne devraient pas être supprimées du serveur SCP.

STEP 2 | Déployez le Panorama connecté à internet.

Ce Panorama communique avec le serveur de mises à jour Palo Alto Networks et télécharge les mises à jour de contenu sur le serveur SCP.

1. Configurez le serveur de gestion Panorama.
   - Configuration de l'appareil de série M
   - Configuration de l'appareil virtuel Panorama
2. Appliquez la configuration Panorama initiale.
   - Effectuer la configuration initiale de l'appareil de série M
   - Effectuer la configuration initiale de l'appareil virtuel Panorama

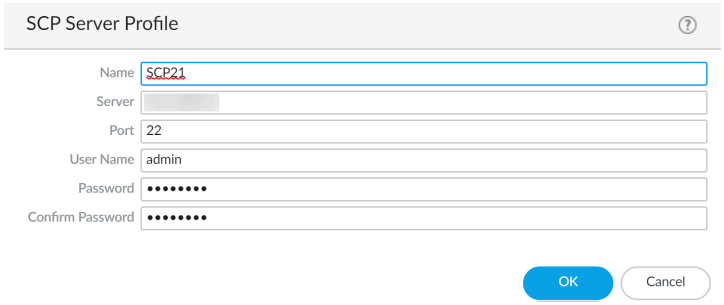
STEP 3 | Installez le Panorama sans connexion Internet.

Ce Panorama communique avec le serveur SCP pour télécharger et installer les mises à jour de contenu sur les pare-feux gérés, les Collecteurs de journaux et les appareils WildFire.

1. Configurez le serveur de gestion Panorama.
   - Configuration de l'appareil de série M
   - Configuration de l'appareil virtuel Panorama
2. Appliquez la configuration Panorama initiale.
   - Effectuer la configuration initiale de l'appareil de série M
   - Effectuer la configuration initiale de l'appareil virtuel Panorama
3. Ajoutez vos pare-feux gérés, Collecteurs de journaux et appareils WildFire.
   - Ajouter un pare-feu en tant que périphérique géré
   - Configurer un collecteur géré
   - Add a Standalone Wildfire Appliance to Manage with Panorama (Ajouter des appareils WildFire autonomes à gérer avec Panorama)

STEP 4 | Configurez le Panorama connecté à internet pour télécharger les mises à jour de contenu sur votre serveur SCP.

1. Connectez-vous à l'interface Web Panorama.
2. Créez un profil de serveur SCP.
   1. Sélectionnez **Panorama** > **Server Profiles (Profils de serveur)** > **SCP** et **Add (Ajoutez)** un nouveau profil de serveur SCP.
   2. Saisissez un **Name (Nom)** descriptif pour le profil de serveur SCP.
   3. Saisissez l'adresse IP du **Server (serveur)** SCP.
   4. Saisissez le **Port**.
   5. Saisissez le**User Name (Nom d'utilisateur)** du serveur SCP.
   6. Saisissez le **Password (Mot de passe)** du serveur SCP et **Confirm Password (Confirmez le mot de passe)**.
   7. Cliquez sur **OK** pour enregistrer vos modifications.



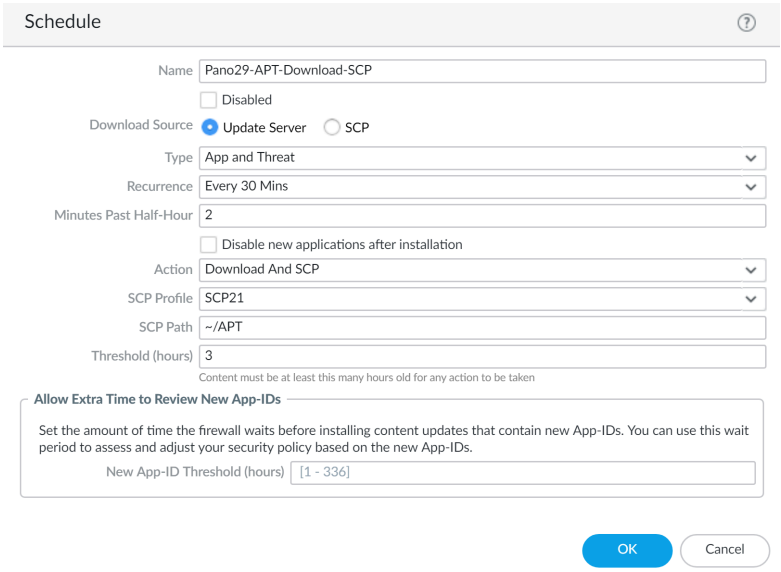
3. Créez un calendrier de mises à jour de contenu pour télécharger régulièrement les mises à jour de contenu sur le serveur SCP.

   Vous devez créer un programme pour chaque type de mise à jour de contenu que vous avez l'intention de télécharger et installer sur vos pare-feux gérés, Collecteurs de journaux et appareils WildFire.

   1. Sélectionnez **Panorama** > **Device Deployment (Déploiement de périphériques)** > **Dynamic Updates (Mises à jour dynamiques)**, sélectionnez **Schedules (Programmes)** et **Add (Ajoutez)** un programme de mise à jour de contenu.
   2. Saisissez un **Name (Nom)** descriptif pour le programme de mises à jour de contenu.
   3. Pour la **Download Source (Source de téléchargement)**, sélectionnez**Update Server (Serveur de mise à jour)**.
   4. Sélectionnez le **Type** de mise à jour de contenu .
   5. Sélectionnez la **Recurrence (Récurrence)** pour définir l'intervalle selon lequel Panorama recherchera de nouvelles mises à jour de contenu sur le serveur de mises à jour Palo Alto Networks.

      Pour configurer un programme de récurrence plus précis, saisissez le nombre de minutes à côté de l'intervalle de récurrence sélectionné. Si vous avez plusieurs mises à jour de contenu programmées pour un téléchargement en utilisant le même intervalle de récurrence, échelonnez les afin d'éviter de surcharger le Panorama et le serveur SCP.

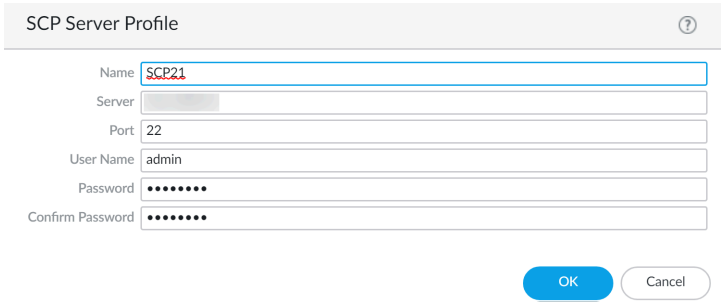
6. Pour l'**Action**, sélectionnez **Télécharger et SCP**.
7. Sélectionnez le **SCP Profile (Profil SCP)** que vous avez configuré au cours des étapes antérieures.
8. Entrez le **SCP Path (chemin SCP)** pour le type de mises à jour de contenu.
9. (Optional (Facultatif)) saisissez le **Threshold (Seuil)**, en heures, pour les mises à jour de contenu. Panorama ne télécharge que les mises à jour de contenu qui existent depuis le nombre d'heures indiqué (ou plus anciennes)
10. Cliquez sur **OK** pour enregistrer vos modifications.



4. **Commit (Validez)** vos modifications.

STEP 5 | Configurez le Panorama air gap pour qu'il télécharge les mises à jour de contenu depuis le serveur SCP et les installe sur les pare-feux gérés, les Collecteurs de journaux et les appareils WildFire.

1. Connectez-vous à l'interface Web Panorama.
2. Créez un profil de serveur SCP.
   1. Sélectionnez **Panorama** > **Server Profiles (Profils de serveur)** > **SCP** et **Add (Ajoutez)** un nouveau profil de serveur SCP.
   2. Saisissez un **Name (Nom)** descriptif pour le profil de serveur SCP.
   3. Saisissez l'adresse IP du **Server (serveur)** SCP.
   4. Saisissez le **Port**.
   5. Saisissez le**User Name (Nom d'utilisateur)** du serveur SCP.
   6. Saisissez le **Password (Mot de passe)** du serveur SCP et **Confirm Password (Confirmez le mot de passe)**.
   7. Cliquez sur **OK** pour enregistrer vos modifications.



3. Créez un programme de mises à jour de contenu afin de télécharger et d'installer régulièrement des mises à jour de contenu depuis le serveur SCP.

   Vous devez créer un programme pour chaque type de mise à jour de contenu que vous avez l'intention de télécharger et installer sur vos pare-feux gérés, Collecteurs de journaux et appareils WildFire.

   1. Sélectionnez **Panorama** > **Device Deployment (Déploiement de périphériques)** > **Dynamic Updates (Mises à jour dynamiques)**, sélectionnez **Schedules (Programmes)** et **Add (Ajoutez)** un programme de mise à jour de contenu.
   2. Saisissez un **Name (Nom)** descriptif pour le programme de mises à jour de contenu.
   3. Pour la **Download Source (Source de téléchargement)**, sélectionnez**SCP**.
   4. Sélectionnez le **SCP Profile (Profil SCP)** que vous avez configuré au cours des étapes antérieures.
   5. Entrez le **SCP Path (chemin SCP)** pour le type de mises à jour de contenu.
   6. Sélectionnez le **Type** de mise à jour de contenu .
   7. Sélectionnez la **Recurrence (Récurrence)** pour définir l'intervalle selon lequel Panorama recherchera de nouvelles mises à jour de contenu sur le serveur de mises à jour Palo Alto Networks.

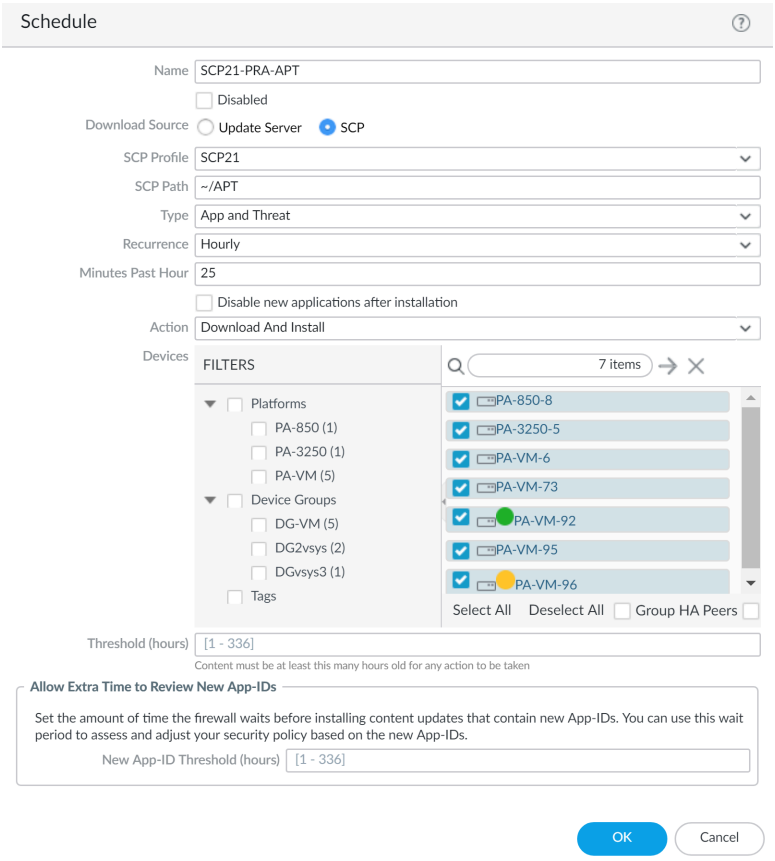
Pour configurer un programme de récurrence plus précis, saisissez le nombre de minutes à côté de l'intervalle de récurrence sélectionné. Si vous avez plusieurs mises à jour de contenu programmées pour un téléchargement en utilisant le même intervalle de récurrence, échelonnez les afin d'éviter de surcharger le Panorama et le serveur SCP.

8. Pour **Action**, sélectionnez**Download (Télécharger)** ou **Download And Install (télécharger et installer)**.

   *Seuls **Download (Télécharger)** et **Download and Install (télécharger et installer)** sont possibles lorsque la **Download Source (Source de téléchargement)** est **SCP**.*

   *Si vous sélectionnez **Download (Télécharger)**, vous devez lancer manuellement l'installation de la mise à jour de contenu sur vos pare-feux gérés.*

9. Sélectionnez les **Devices (Périphériques)** sur lesquels installer les mises à jour de contenu.
10. (Optional (Facultatif)) saisissez le **Threshold (Seuil)**, en heures, pour les mises à jour de contenu. Panorama ne télécharge que les mises à jour de contenu qui existent depuis le nombre d'heures indiqué (ou plus anciennes)
11. Cliquez sur **OK** pour enregistrer vos modifications.



4. **Commit (Validez)** vos modifications.

Mettre à niveau Panorama dans une configuration HA

Pour assurer un basculement transparent lorsque vous mettez à jour le logiciel Panorama dans une configuration haute disponibilité (HD), les homologues Panorama actifs et passifs doivent exécuter la même version Panorama avec la même version de la base de données Applications. L'exemple suivant décrit comment mettre à jour une paire HD (l'homologue actif est nommé Primaire_A et l'homologue passif est nommé Secondaire_B).

Si vous mettez à niveau Panorama et les périphériques gérés en mode FIPS-CC vers PAN-OS 11.0 à partir de PAN-OS 10.2 ou version antérieure, vous devez effectuer les étapes supplémentaires de réinitialisation de l'état de connexion sécurisée des périphériques en mode FIPS-CC s'ils sont ajoutés à la gestion de Panorama lors de l'exécution d'une version de PAN-OS 10.2. Pour plus de détails sur la mise à niveau des périphériques Panorama et FIPS-CC en mode FIPS-CC, reportez-vous à la section Mettre à niveau Panorama et les périphériques gérés en mode FIPS-CC .

Avant de mettre à jour Panorama, reportez-vous aux Notes de version pour la version de contenu minimum requise pour PAN-OS 11.0.

STEP 1 | Mettez à niveau le logiciel Panorama sur l'homologue Secondaire_B (passif).

Effectuez l'une des tâches suivantes sur l'homologue Secondaire_B :

- Mettre à niveau Panorama avec une connexion Internet
- Mettre à niveau Panorama sans connexion Internet

Après la mise à niveau, ce Panorama passera à un état non fonctionnel car les homologues n'exécutent plus la même version de logiciel.

STEP 2 | (Best Practices (Meilleures pratiques)) Si vous utilisez Cortex Data Lake (CDL), install the Panorama device certificate (installez le certificat de périphérique Panorama) sur chaque homologue Panorama HA.

Panorama passe automatiquement à l'utilisation du certificat de périphérique pour l'authentification avec l'ingestion de CDL et les points de terminaison de requête lors de la mise à niveau vers PAN-OS 11.0.

Si vous n'installez pas le certificat de périphérique avant la mise à niveau vers PAN-OS 11.0, Panorama continue d'utiliser les certificats de service de journalisation existants pour l'authentification.

STEP 3 | Suspendez l'homologue Primaire_A pour forcer un basculement.

Sur l'homologue Primaire_A :

1. Dans la section **Operational Commands (Commandes opérationnelles)** (**Panorama** > **High Availability (Haute disponibilité)**), cliquez sur le lien **Suspend local Panorama (Suspendre le Panorama local)**.
2. Vérifiez que l'état est `suspended` (suspendu) (affiché dans le coin inférieur droit de l'interface Web).

   Le basculement qui en résulte devrait provoquer la transition de l'homologue Secondaire_B vers l'état `active` (actif).

STEP 4 | Mettez à niveau le logiciel Panorama sur l'homologue Primaire_A (actuellement passif).

Effectuez l'une des tâches suivantes sur l'homologue Primaire_A :

- Mettre à niveau Panorama avec une connexion Internet
- Mettre à niveau Panorama sans connexion Internet

Après le redémarrage, l'homologue Primaire_A est initialement toujours à l'état passif. Ensuite, si la préemption est activée (par défaut), l'homologue Primaire_A passe automatiquement à l'état actif et l'homologue Secondaire_B revient à l'état passif.

Si vous désactivez la préemption, restaurez manuellement le panorama principal à l'état actif.

STEP 5 | Vérifiez que les deux homologues exécutent maintenant les versions de mise à jour de contenu nouvellement installées et la version Panorama nouvellement installée.

Sur le **Dashboard (Tableau de bord)** de chaque homologue Panorama, vérifiez la version du logiciel Panorama et la version de l'application, et confirmez qu'elles sont identiques sur les deux homologues et que la configuration en cours est synchronisée.

STEP 6 | (Collecteurs de journaux locaux dans un groupe de collecteurs uniquement) Mettez à niveau les collecteurs de journaux restants dans le groupe de collecteurs.

- Mettre à niveau les collecteurs de journaux lorsque Panorama est connecté à Internet
- Mettre à niveau les collecteurs de journaux lorsque Panorama n'est pas connecté à Internet

STEP 7 | (Panorama and managed devices in FIPS-CC mode (Panorama et périphériques gérés en mode FIPS-CC)) Mettre à niveau Panorama et les périphériques gérés en mode FIPS-CC.

La mise à niveau de Panorama et des périphériques gérés en mode FIPS-CC nécessite que vous réinitialisiez l'état de connexion sécurisée des périphériques en mode FIPS-CC s'ils sont ajoutés à la gestion de Panorama lors de l'exécution d'une version de PAN-OS 11.0. Vous devez réintégrer les appareils gérés suivants à la gestion Panorama :

- Appareils gérés en mode FIPS-CC ajoutés à Panorama à l'aide de la clé d'authentification d'enregistrement de périphérique.
- Appareils gérés en mode de fonctionnement normal ajoutés à Panorama à l'aide de la clé

d'authentification d'enregistrement de périphérique Vous n'avez pas besoin de réintégrer les appareils gérés ajoutés à la gestion Panorama lorsque l'appareil géré exécutait un PAN-OS 10.0 ou une version antérieure.

STEP 8 | (PAN-OS 10.2 et versions ultérieures) Régénérez ou réimportez tous les certificats pour respecter le niveau de sécurité OpenSSL 2.

Cette étape est requise si vous effectuez une mise à niveau de PAN-OS 10.1 ou version antérieure vers PAN-OS 11.0. Effectuez cette étape si vous effectuez une mise à niveau à partir de PAN-OS 10.2 et que vous avez déjà régénéré ou réimporté vos certificats.

Tous les certificats doivent satisfaire aux exigences minimales suivantes :

- RSA 2048 bits ou supérieur, ou ECDSA 256 bits ou supérieur
- Digest de SHA256 ou supérieur

Consultez le Guide de l'administrateur PAN-OS ou le Guide de l'administrateur de Panorama pour plus d'informations sur la régénération ou la réimportation de vos certificats.

STEP 9 | (Recommended for Panorama mode (Recommandé pour le mode Panorama) Augmentez la mémoire de l'appareil virtuel Panorama à 64 Go.

Après avoir correctement mis à niveau l'appareil virtuel Panorama en mode Panorama ers PAN-OS 11.0, Palo Alto Networks recommande d'augmenter la mémoire de l'appareil virtuel Panorama à 64 Go pour répondre à la configuration système requise accrue afin d'éviter tout problème de journalisation, de gestion et de performances opérationnelles lié à un appareil virtuel Panorama sous-provisionnée.

Migrer les journaux de Panorama vers le nouveau format de journal

Après la mise à niveau vers une version Panorama 8.0 (ou ultérieure), le collecteur de journaux de Panorama utilise un nouveau format de stockage de journaux. Panorama ne pouvant pas générer de rapports ou de données ACC à partir de journaux dans le format de journal antérieur à la version 8.0, vous devez migrer les journaux existants dès la mise à niveau de Panorama et de ses collecteurs de journaux de puis une version de PAN-OS® 7.1 ou antérieure vers une version PAN-OS 8.0 ou ultérieure, et vous devez le faire avant de mettre à niveau vos pare-feu gérés. Panorama continuera à collecter les journaux des périphériques gérés pendant la migration des journaux, mais stockera les journaux entrants dans le nouveau format de journal après la mise à niveau vers PAN-OS 8.0 ou une version ultérieure. Pour cette raison, vous ne verrez que des données partielles dans l'ACC et dans les rapports tant que Panorama n'a pas terminé le processus de migration des journaux.

La migration du journal vers le nouveau format est une tâche ponctuelle que vous devez effectuer lorsque vous effectuez une mise à niveau vers la version PAN-OS 8.0 ou une version ultérieure (ou lorsque vous effectuez une mise à niveau vers la version PAN-OS 8.0 dans le cadre de votre chemin de mise à niveau) ; vous n'avez plus besoin d'effectuer cette migration lorsque vous effectuez une mise à niveau vers une version ultérieure de PAN-OS.

Le temps nécessaire à Panorama pour terminer le processus de migration des journaux dépend du volume des nouveaux journaux écrits dans Panorama et de la taille de la base de données de journaux que vous migrez. Étant donné que la migration de journaux est un processus gourmand en ressources processeur, commencez la migration à un moment où le taux de journalisation est inférieur. Vous pouvez toujours arrêter la migration pendant les périodes de pointe si vous remarquez que les taux d'utilisation du processeur sont élevés et reprendre la migration lorsque le débit de journalisation entrant est inférieur.

Après la Installer les mises à jour de contenu et de logiciel pour Panorama et pour la mise à niveau des collecteurs de journaux, migrez les journaux comme suit :

- Affichez le taux de journalisation entrant.

  Pour de meilleurs résultats, démarrez la migration des journaux lorsque le taux de journalisation entrant est faible. Pour vérifier le débit, exécutez la commande suivante depuis la CLI du collecteur de journaux :

  ```
  admin@FC-M500-1> debug log-collector log-collection-stats show
   incoming-logs
  ```

  Une utilisation élevée du processeur (proche de 100 %) pendant la migration des journaux est attendue et les opérations continueront à fonctionner normalement. La migration des journaux est limitée en faveur des journaux entrants et d'autres processus en cas de conflit de ressources.

- Commencez à migrer les journaux sur chaque collecteur de journaux au nouveau format.

  Pour commencer la migration, entrez la commande suivante depuis la CLI de chaque collecteur de journaux :

  ```
  admin@FC-M500-1> request logdb migrate lc serial-number <ser_num>
   start
  ```

- Consultez l'état de la migration des journaux pour estimer le temps nécessaire à la migration de tous les journaux existants vers le nouveau format.

  ```
  admin@FC-M500-1> request logdb migrate lc serial-number <ser_num>
   status Slot: all Migration State: En cours Pourcentage
   d'achèvement : 0,04 Temps restant estimé : 451 heure(s), 47
   min(s)
  ```

- Arrêtez le processus de migration des journaux.

  Pour arrêter temporairement le processus de migration des journaux, entrez la commande suivante depuis la CLI du collecteur de journaux :

  ```
  admin@FC-M500-1 request logdb migrate lc serial-number <ser_num>
   stop
  ```

Mise à niveau de Panorama pour la capacité de gestion accrue des périphériques

Procédez à la mise à niveau vers PAN-OS 9.1 ou une version ultérieure pour utiliser votre licence de gestion de périphériques existante sur votre appareil M-600 et gérer jusqu'à 5 000 pare-feux ou sur votre appareil virtuel Panorama™ pour gérer jusqu'à 2 500 pare-feux.

STEP 1 | Increase CPUs and Memory for the Panorama Virtual Appliance Augmentez les processeurs et la mémoire du périphérique virtuel Panorama si le dispositif virtuel Panorama ne répond pas déjà aux besoins minimaux en ressources pour une gestion accrue des périphériques.

Passez en revue la configuration requise pour augmenter la capacité de gestion des périphériques pour vérifier si votre périphérique virtuel Panorama existante répond à la configuration minimale requise avant la mise à niveau.

STEP 2 | Connectez-vous à l'CLI de Panorama.

STEP 3 | Faites passer le serveur de gestion Panorama au mode Gestion uniquement si Panorama n'est pas encore défini sur ce mode.

- (M-600 appliances only (Appareils M-600 uniquement)) Commencez à l’étape 5 pour Set Up an M-Series Appliance in Management Only Mode (configurer un appareil M-Series en mode gestion uniquement).

ou

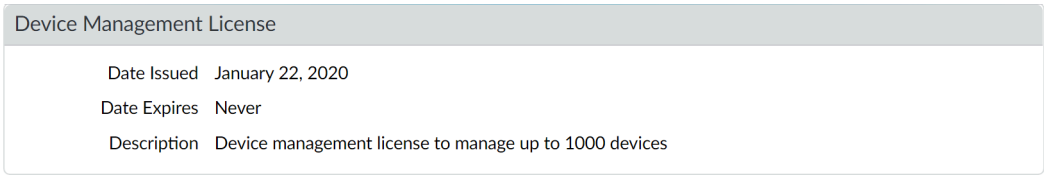
- Set Up a Panorama Virtual Appliance in Management Only Mode (Configurer un appareil virtuel Panorama en mode de Gestion seulement).

STEP 4 | Connectez-vous à l’interface Web Panorama.

STEP 5 | Mettez à niveau le serveur de gestion Panorama.

- Mettre à niveau Panorama avec une connexion Internet.
- Mettre à niveau Panorama sans connexion Internet.
- Mettre à niveau Panorama dans une configuration HA.

STEP 6 | Sélectionnez **Panorama** > **Licenses (Licences)** et vérifiez que la licence de gestion des périphériques est activée avec succès.



Si vous avez activé votre licence de gestion des périphériques, puis que vous avez procédé à la mise à niveau vers PAN-OS 9.1 ou une version ultérieure, vous pouvez gérer un maximum de 5 000 pare-feux avec un appareil M-600, ou jusqu'à 2 500 pare-feux avec un appareil virtuel Panorama, mais la description suivante s’affiche `Device management license to manage up to 1000 devices`.

Mettre à niveau Panorama et les périphériques gérés en mode FIPS-CC

Une fois la mise à niveau réussie vers PAN-OS 11.0, tous les périphériques gérés en mode FIPS-CC et tout périphérique géré ajouté à Panorama lorsque le périphérique exécutait une version de PAN-OS 11.0 doivent être réintégrés à la gestion Panorama. Pour ce faire, vous devez réinitialiser l’état de la connexion sécurisée pour Panorama en mode FIPS-CC et pour tous les périphériques gérés en mode FIPS-CC. Après avoir réinitialisé l’état de la connexion sécurisée, vous devez ajouter le pare-feu, Log Collector et l’appareil WildFire ajoutés à Panorama à l’aide de la clé d’authentification d’enregistrement de périphérique à la

gestion Panorama. Cette procédure n'est pas requise et n'a pas d'impact sur les périphériques gérés ajoutés à Panorama lors de l'exécution de PAN-OS 10.0 ou d'une version antérieure. Ceci est requis pour tous les Panorama models (modèles Panorama) pris en charge, Next-Generation firewall hardware and VM-Series models (le matériel de pare-feu de nouvelle génération et les modèles VM-Series) en mode FIPS-CC.

STEP 1 | Créez une liste de vos périphériques gérés en mode FIPS-CC et de tout périphérique géré ajouté à Panorama à l'aide de la clé d'authentification d'enregistrement de périphérique. Cela vous aidera plus tard à concentrer vos efforts lorsque vous réintégrerez vos appareils gérés à la gestion Panorama.

STEP 2 | Mettez à niveau Panorama et les périphériques gérés vers PAN-OS 11.0.

- Mettre à niveau Panorama avec une connexion Internet
- Mettre à niveau Panorama sans connexion Internet
- Mettre à niveau Panorama dans une configuration HA

STEP 3 | Après la mise à niveau vers PAN-OS 11.0, consultez les journaux système sur Panorama pour identifier les périphériques gérés en mode FIPS-CC qui ne peuvent pas se connecter à Panorama.

STEP 4 | Réinitialisez l'état de connexion sécurisée sur Panorama.

Cette étape réinitialise la connectivité pour tout périphérique géré ajouté à la gestion Panorama lors de l'exécution d'une version PAN-OS 11.0 et est irréversible. Cette étape n'a aucun impact sur l'état de connectivité des pare-feu ajoutés lors de l'exécution de PAN-OS 10.0 ou d'une version antérieure qui sont mis à niveau vers PAN-OS 11.0.

1. Connectez-vous à l'CLI de Panorama.
2. Réinitialisez l'état de la connexion sécurisée.

```
admin> request sc3 reset
```

3. Redémarrez le serveur d'administration sur Panorama.

```
admin> debug software restart process management-server
```

4. (HA uniquement (HA uniquement)) Répétez cette étape pour chaque homologue dans la configuration haute disponibilité (HA).

STEP 5 | Réinitialisez l’état de connexion sécurisée sur le périphérique géré en mode FIPS-CC.

Cette étape réinitialise la connexion du dispositif géré et est irréversible.

1. Connectez-vous à l’interface de ligne de commande du périphérique géré.
   - Connectez-vous à l'ILC du pare-feu.
   - Log in to the Log Collector CLI (Connectez-vous à l'interface de ligne de commande du collecteur de journaux).
   - Log in to the WildFire appliance CLI (Connectez-vous à l’interface de ligne de commande de l’appareil WildFire).
2. Réinitialisez l’état de la connexion sécurisée.

   ```
   admin> request sc3 reset
   ```
3. Redémarrez le serveur d’administration sur le périphérique géré.

   ```
   admin> debug software restart process management-server
   ```

STEP 6 | Ajoutez les appareils gérés concernés à Panorama.

- Ajouter un pare-feu en tant que périphérique géré
- Configurer un collecteur géré
- Ajouter des appareils WildFire autonomes à gérer avec Panorama

STEP 7 | Régénérez ou réimportez tous les certificats pour respecter le niveau de sécurité OpenSSL 2.

Lors de la mise à niveau vers PAN-OS 11.0, tous les certificats doivent répondre aux exigences minimales suivantes :

- RSA 2048 bits ou supérieur, ou ECDSA 256 bits ou supérieur
- Digest de SHA256 ou supérieur

Consultez le Guide de l’administrateur PAN-OS ou le Guide de l’administrateur de Panorama pour plus d’informations sur la régénération ou la réimportation de vos certificats.

Downgrader depuis Panorama 11.0

PAN-OS 11.0 introduit la prise en charge avancée de la prévention des menaces pour la prévention des exploits Zero-day qui tire parti de l’apprentissage profond en ligne, de la mise à niveau logicielle simplifiée et de la rétrogradation pour Panorama et les appareils gérés afin de réduire la charge opérationnelle liée à la mise à niveau des appareils gérés sur plusieurs versions de PAN-OS®, de l’évaluation proactive des meilleures pratiques (BPA) utilisant AIOps pour éliminer davantage l’exposition d’une posture de sécurité compromise, du proxy Web local pour faciliter la transition vers le cloud sans sacrifier la sécurité ou l’efficacité, la prise en charge du pare-feu pour un client DHCPv6 avec état afin d’obtenir des adresses IPv6, une visibilité accrue du contexte utilisateur pour Cloud Identity Engine (CIE), la prise en charge TLSv1.3 pour l’accès de gestion et des recommandations de règles de stratégie de sécurité IoT améliorées pour faciliter la mise à l’échelle et la gestion des recommandations de règles de stratégie. Utilisez le flux de travail suivant pour rétrograder les pare-feu avant de rétrograder les collecteurs de journaux et Panorama exécutant une version Panorama 11.0 dans une version antérieure. Cette procédure fonctionne à la fois pour Panorama qui gère un collecteur de journaux local et pour Panorama qui gère un ou de plusieurs collecteurs de journaux dédiés.

Pour passer de PAN-OS 11.0 à une version antérieure de PAN-OS, vous devez télécharger et installer la version PAN-OS 10.2 préférée ou ultérieure de PAN-OS 10.2 préférée avant de pouvoir poursuivre votre mise à niveau vers votre version PAN-OS cible. La rétrogradation à partir de PAN-OS 11.0 échoue si vous tentez de rétrograder vers PAN-OS 10.1 ou une version antérieure de PAN-OS.

Consultez la Matrice de compatibilité de Palo Alto Networks pour confirmer que les pare-feu et les appareils que vous avez l'intention de rétrograder sont compatibles avec la version de PAN-OS que vous voulez rétrograder. Pour les pare-feu et les appareils que vous pouvez rétrograder, vous devez également consulter les Considérations de mise à niveau/rétrogradation pour vous assurer que vous tenez compte de toutes les fonctionnalités et paramètres de configuration qui seront différents ou indisponibles après la rétrogradation.

STEP 1 | Connectez-vous à l'interface Web Panorama.

STEP 2 | Enregistrez une sauvegarde des fichiers de configuration de Panorama et des périphériques gérés.

1. **Export Panorama and device configuration snapshot (Exporter un instantané de la configuration de l'appareil et de Panorama)** (**Panorama** > **Setup (Configuration)** > **Operations (Opérations)**).
2. Enregistrez le fichier .tgz exporté dans un emplacement externe à Panorama, aux collecteurs de journaux ou aux pare-feu. Vous pouvez utiliser cette sauvegarde pour restaurer la configuration en cas de problème qui vous forcerait à recommencer la procédure.

STEP 3 | Si vous avez configured authentication for a Dedicated Log Collector (configuré une authentification pour un Collecteur de journaux dédié) et avez supprimé l'utilisateur `admin`, configurez et validez un nouvel utilisateur`admin` pour vos collecteurs de journaux dédiés.

Les Collecteurs de journaux dédiés doivent avoir l'utilisateur `admin` configuré afin de downgrader vers PAN-OS 9.1 et les versions antérieures.

STEP 4 | Sélectionnez **Panorama** > **Plugins** et **téléchargez** la version du plugin prise en charge sur PAN-OS 10.2 pour tous les plugins actuellement installés sur Panorama.

Consultez la matrice de compatibilité des plug-ins Panorama pour connaître la version du plug-in Panorama prise en charge sur PAN-OS 10.2 et versions antérieures.

Cela est nécessaire pour rétrograder Panorama de PAN-OS 11.0 vers PAN-OS 10.2 et versions antérieures. La version téléchargée du plugin est automatiquement installée lors de la rétrogradation vers PAN-OS 10.2. La rétrogradation vers PAN-OS 10.2 est bloquée si la version du plug-in prise en charge n'est pas téléchargée.

(plug-in ZTP uniquement) Pour réussir la rétrogradation de Panorama vers PAN-OS 10.2, vous devez désinstaller le plug-in ZTP avant de commencer le processus de rétrogradation. Après avoir réussi la rétrogradation vers PAN-OS 10.2, vous devez réinstaller le plug-in ZTP sur Panorama.

STEP 5 | Downgradez chaque pare-feu exécutant une version de PAN-OS 11.0.

La rétrogradation de PAN-OS 11.0 vers une version de fonctionnalité précédente nécessite que vous deviez d'abord rétrograder vers la version préférée de PAN-OS 10.2 ou une version ultérieure de PAN-OS 10.2. Après avoir réussi à rétrograder vers la version préférée de PAN-OS 10.2 ou ultérieure de PAN-OS 10.2, vous pouvez continuer à rétrograder vers votre version PAN-OS cible.

Si vous rétrogradez plus d'un pare-feu, rationalisez le processus en transférant chaque image PAN-OS 10.2 spécifique à un pare-feu vers Panorama avant de commencer la rétrogradation. Par exemple, pour downgrader les pare-feu PA-220 vers PAN-OS 10.2, téléchargez les images `PanOS_220-10.2.0` *ou* `PanOS_3000-10.2.0`.

Panorama exige que tous les pare-feu exécutent la même version ou une version antérieure de PAN-OS. Ainsi, avant de rétrograder Panorama, utilisez et répétez les tâches appropriées ci-dessous en fonction de votre environnement pour rétrograder tous les pare-feu gérés :

1. **Check Now (Vérifier maintenant)** les images disponibles (**Panorama** > **Device Deployment (Déploiement de périphériques)** > **Software (Logiciel)**).
2. Localisez l'image PAN-OS 10.2 pour chaque modèle ou série de pare-feu que vous souhaitez rétrograder. Si l'image n'est pas déjà téléchargée, cliquez sur **Download (Télécharger)** pour la télécharger.

Pare-feu sans Haute Disponibilité / HD (High Availability / HA)

Cliquez sur **Install (Installer)** dans la colonne Action de la version de PAN-OS 10.2, sélectionnez tous les pare-feux que vous souhaitez rétrograder, sélectionnez **Reboot device after install (Redémarrer le périphérique après l'installation)** et cliquez sur **OK**.

Pare-feu HD actifs / actifs

1. Cliquez sur **Install (Installer)**, désactivez **Group HA Peers (Regrouper les homologues HD)**, sélectionnez un des homologues HD, sélectionnez **Reboot device after install (Redémarrer le périphérique après l'installation)**, puis cliquez sur **OK**. Attendez que le pare-feu termine le redémarrage avant de poursuivre.
2. Cliquez sur **Install (Installer)**,désactivez **Group HA Peers (Regrouper les homologues HD)**, sélectionnez l'homologue HD que vous n'avez pas mis à jour à l'étape précédente, sélectionnez

Reboot device after install (Redémarrer le périphérique après l'installation), puis cliquez sur **OK**.

Pare-feu HD actifs / passifs

Dans cet exemple, le pare-feu actif est appelé fw1 et le pare-feu passif fw2 :

1. Cliquez sur **Installer** dans la colonne Action de la mise à jour appropriée, désactivez **Group HA Peers (Regrouper les homologues HD)**, sélectionnez fw2, **Reboot device after install (Redémarrer le périphérique après l'installation)** et cliquez sur **OK**.
2. Après le redémarrage de fw2, vérifiez sur fw1 (widget **Dashboard (Tableau de bord)** > **High Availability (Haute disponibilité)**) que fw2 est toujours l'homologue passif (l'état du pare-feu local est `active` et l'homologue fw2 est `passive`).
3. Accédez à fw1 et **Suspend local device (Suspendre le périphérique local)** (**Device (Périphérique)** > **High Availability (Haute disponibilité)** > **Operational Commands (Commandes opérationnelles)**).
4. Accédez à fw2 (**Dashboard (Tableau de bord)** > **High Availability (Haute disponibilité)**) et vérifiez que l'état du pare-feu local est `active` et que l'homologue est `suspended`.
5. Accédez à Panorama, sélectionnez **Panorama** > **Device Deployment (Déploiement de périphériques)** > **Software (Logiciel)**, cliquez sur **Install (Installer)** dans la colonne Action de la mise à jour appropriée, désactivez **Group HA Peers (Regrouper les homologues HD)**, sélectionnez fw1, **Reboot device after install (Redémarrer le périphérique après l'installation)**, puis cliquez sur **OK**. Attendez que fw1 termine le redémarrage avant de poursuivre.
6. Accédez à fw1 (widget **Dashboard (Tableau de bord)** > **High Availability (Haute disponibilité)**) et vérifiez que l'état du pare-feu local est `passive` et que l'homologue (fw2) est `active`.

> *Si vous avez activé la préemption dans les paramètres d'élection (**Device (Périphérique)** > **High Availability (Haute disponibilité)** > **General (Général)**), alors fw1 sera rétabli en tant qu'homologue actif après le redémarrage.*

STEP 6 | Downgradez chaque collecteur de journaux exécutant Panorama 11.0.

> *La rétrogradation de PAN-OS 11.0 vers une version de fonctionnalité précédente nécessite que vous deviez d'abord rétrograder vers la version préférée de PAN-OS 10.2 ou ultérieure de PAN-OS 10.2. Après avoir réussi à rétrograder vers la version préférée de PAN-OS 10.2 ou ultérieure de PAN-OS 10.2, vous pouvez continuer à rétrograder vers votre version PAN-OS cible.*

1. **Check Now (Vérifier maintenant)** les images disponibles (**Panorama** > **Device Deployment (Déploiement de périphériques)** > **Software (Logiciel)**).
2. Localisez l'image de Panorama 10.2. Si l'image n'est pas déjà téléchargée, alors cliquez sur **Download (Télécharger)** pour la télécharger (colonne Action).
3. Une fois le téléchargement terminé, **Install (Installer)** l'image sur chaque collecteur de journaux exécutant Panorama 10.2. Sélectionnez **Reboot device after install (Redémarrer le périphérique après l'installation)** pour redémarrer automatiquement le périphérique lorsque la mise à niveau est terminée.

STEP 7 | Rétrogradez Panorama.

La rétrogradation de PAN-OS 11.0 vers une version de fonctionnalité précédente nécessite que vous deviez d'abord rétrograder vers la version préférée de PAN-OS 10.2 ou ultérieure de PAN-OS 10.2. Après avoir réussi à rétrograder vers la version préférée de PAN-OS 10.2 ou ultérieure de PAN-OS 10.2, vous pouvez continuer à rétrograder vers votre version PAN-OS cible.

1. Sélectionnez **Panorama** > **Software (Logiciel)** et **Check now (vérifiez maintenant)** pour trouver les images disponibles.
2. Localisez l'image de Panorama 10.2. Si l'image n'est pas déjà téléchargée, cliquez sur **Download (Télécharger)** pour la télécharger.
3. Une fois le téléchargement terminé, **Install (Installer)** l'image sur Panorama.
4. Rédémarrez Panorama comme suit :
   - Si vous êtes invité à redémarrer, cliquez sur **Yes (Oui)**. Si une invite **CMS Login (Connexion CMS)** s'affiche, appuyez sur Entrée sans saisir de nom d'utilisateur ou de mot de passe. Lorsque l'invite de connexion Panorama s'affiche, saisissez le nom d'utilisateur/mot de passe définis lors de la configuration initiale.
   - Si vous n'êtes pas invité à redémarrer, sélectionnez **Panorama (Panorama)** > **Setup (Configuration)** > **Operations (Opérations)** et cliquez sur **Reboot Panorama (Redémarrer Panorama)** dans la section des opérations de périphérique.

STEP 8 | (plug-in ZTP uniquement) Réinstallez le plug-in ZTP.

1. Connectez-vous à l'interface Web Panorama.
2. Installez le plug-in ZTP.
3. Sélectionnez **Panorama** > **Zero Touch Provisioning** et cochez (activer) **ZTP**.

Résoudre les problèmes liés à votre mise à niveau Panorama

Pour dépanner votre mise à niveau de Panorama, utilisez le tableau suivant pour passer en revue les problèmes possibles et la façon de les résoudre.

Symptôme	Résolution
La licence de garantie du logiciel a expiré.	À partir de la CLI, supprimez la clé de licence expirée : 1. Entrez **`delete licence key (supprimer la clé de licence)<software license key>`**. 2. Entrez **`delete license key Software_Warranty<expiredate>.key`**.
Les dernières versions du logiciel PAN-OS n'étaient pas disponibles.	Vous ne pouvez voir que les versions logicielles qui sont une version de fonctionnalité avant la version installée actuelle. Par exemple, si une version 8.1 est installée, seules les versions 9.0 seront disponibles. Pour voir les versions 9.1, vous devez d'abord effectuer une mise à niveau vers la version 9.0.
(Dispositif virtuel Panorama en mode hérité uniquement) La version de mise à niveau n'a pas pu être préchargée dans le gestionnaire de logiciels.	Ce problème se produit lorsqu'il n'y a pas suffisamment de ressources disponibles. Vous pouvez augmenter la capacité de la machine virtuelle ou migrer du mode Hérité vers le mode Panorama.

Déployer des mises à niveau vers des pare-feu, des collecteurs de journaux et des appareils WildFire à l'aide de Panorama

Vous pouvez utiliser Panorama™ pour qualifier des mises à jour logicielles et de contenu en les déployant sur un sous-ensemble de pare-feu, de collecteurs de journaux dédiés ou d'appareils et et de clusters d'appareils WildFire® avant d'installer les mises à jour sur le reste de vos appareils gérés. Si vous souhaitez planifier des mises à jour de contenu régulières, Panorama nécessite une connexion directe à Internet. Pour déployer des mises à jour du logiciel ou du contenu sur demande (non programmée), la procédure diffère selon que Panorama est connecté à Internet. Panorama affiche un avertissement si vous déployez manuellement une mise à jour de contenu lorsqu'un processus de mise à jour planifiée a commencé ou commencera dans les cinq minutes.

Lors du déploiement de mises à jour, Panorama notifie les appareils gérées (pare-feu, collecteurs de journaux et appareils WildFire) que des mises à jour sont disponibles et les appareils récupèrent ensuite les packages de mise à jour depuis Panorama. Par défaut, les appareils gérés récupèrent les mises à jour via l'interface de gestion (MGT) sur Panorama. Toutefois, si vous souhaitez réduire la charge de trafic sur l'interface MGT en utilisant une autre interface pour les appareils pour récupérer les mises à jour, vous pouvez Configurer Panorama pour utiliser plusieurs interfaces.

Vous pouvez rapidement rétablir une version de contenu pour un ou plusieurs pare-feu à la version de contenu précédemment installée en utilisant Panorama. Après l'installation d'une nouvelle version de contenu sur le pare-feu, vous pouvez revenir à la version précédemment installée si la version de contenu nouvellement installée déstabilise ou perturbe autrement vos opérations réseau.

Par défaut, vous pouvez télécharger les logiciels ou les mises à jour de chaque type sur Panorama. Lorsque vous commencez n'importe quel téléchargement au-delà de ce plafond, Panorama supprime la plus ancienne mise à jour du type sélectionné. Pour modifier le maximum, consultez Gestion du stockage de Panorama pour les mises à jour logicielles et de contenu.

- Quelles mises à jour Panorama peut-il envoyer à d'autres appareils ?
- Compatibilité des versions de Panorama, des collecteurs de journaux, des pare-feu et de WildFire
- Planifier une mise à jour de contenu à l'aide de Panorama
- Mettre à niveau les pare-feu lorsque Panorama est connecté à Internet
- Mettre à niveau les pare-feu lorsque Panorama n'est pas connecté à Internet
- Mettre à niveau les collecteurs de journaux lorsque Panorama est connecté à Internet
- Mettre à niveau les collecteurs de journaux lorsque Panorama n'est pas connecté à Internet
- Mettre à niveau un cluster WildFire à partir de Panorama avec une connexion Internet
- Mettre à niveau un cluster WildFire à partir de Panorama sans connexion Internet
- Mettre à niveau un pare-feu ZTP
- Rétablir les mises à jour du contenu depuis Panorama

Quelles mises à jour Panorama peut-il envoyer à d'autres appareils ?

Les mises à jour logicielles et de contenu que vous pouvez installer dépendent des abonnements actifs sur chaque pare-feu, collecteur de journaux et appareil et cluster d'appareils WildFire® :

Type d'appareil	Mises à jour logicielles	Mises à jour du contenu
Collecteur de journaux	Panorama™	Applications (les collecteurs de journaux n'ont pas besoin de signatures de menaces) Antivirus WildFire®
Pare-feu	PAN-OS® Agent / application GlobalProtect™	Applications Applications et menaces Antivirus WildFire
WildFire	PAN-OS Images VM	WildFire

Planifier une mise à jour de contenu à l'aide de Panorama

Panorama™ nécessite une connexion Internet directe pour la planification des mises à jour prises en charge sur les pare-feu, les collecteurs de journaux et les appareils et clusters d'appareils WildFire®. Sinon, vous pouvez effectuer uniquement les mises à jour sur demande. (Pour planifier des mises à jour Antivirus, WildFire ou URL BrightCloud pour les collecteurs de journaux, doivent exécuter Panorama 7.0.3 ou une version ultérieure.) Chaque pare-feu, collecteur de journaux ou appareil et cluster d'appareils WildFire recevant une mise à jour génère un journal pour indiquer que l'installation a réussi (un journal de configuration) ou échoué (un journal système). Pour planifier des mises à jour sur le serveur de gestion Panorama, consultez Installer des mises à jour pour Panorama avec une connexion Internet.

Avant de déployer des mises à jour, reportez-vous à Compatibilité des versions de Panorama, des collecteurs de journaux, des pare-feu et de WildFire *pour des détails importants sur la compatibilité des versions de contenu. Consultez les* Notes de version *pour la version de contenu minimale que vous devez installer pour une version de Panorama.*

Panorama ne peut télécharger qu'une seule mise à jour à la fois pour les mises à jour du même type. Si vous planifiez le téléchargement simultané de plusieurs mises à jour du même type de récurrence, seul le premier téléchargement réussit.

*Si vos pare-feu se connectent directement au serveur de mise à jour de Palo Alto Networks®, vous pouvez également utiliser des modèles Panorama (**Device (Périphérique)** > **Dynamic Updates (Mises à jour dynamiques)**) pour appliquer des* horaires de mise à jour de contenu *sur les pare-feux. Si vous souhaitez retarder l'installation des mises à jour pour une période après leur publication, vous devez déployer des calendriers à l'aide de modèles. Dans de rares cas, une mise à jour inclura des erreurs, ce qui spécifie qu'un délai augmente la probabilité que Palo Alto Networks identifie et supprime cette mise à jour du serveur de mise à jour avant que vos pare-feu ne les installent.*

Procédez comme suit pour chaque type de mise à jour que vous souhaitez planifier.

STEP 1 | Sélectionnez **Panorama** > **Device Deployment (Déploiement de périphériques)** > **Dynamic Updates (Mises à jour dynamiques)**, cliquez sur **Schedules (Horaires)** et **Add (Ajoutez)** un horaire.

STEP 2 | Spécifiez un **Name (Nom)** pour identifier l'horaire, le **Type** de la mise à jour et la fréquence de mise à jour (**Recurrence (Récurrence)**). Les options de fréquence disponibles dépendent du **Type** de la mise à jour.

PAN-OS® utilise le fuseau horaire de Panorama pour la planification des mises à jour.

Si vous définissez le **Type** sur **App and Threat (Applications et menaces)**, les collecteurs de journaux l'installent et n'ont besoin que du contenu des applications, pas du contenu des menaces. Les pare-feux utilisent et les applications et le contenu des menaces. Pour plus d'informations, consultez la section Compatibilité des versions de Panorama, des collecteurs de journaux, des pare-feu et de WildFire .

STEP 3 | Sélectionnez l'une des actions de planification suivantes, puis sélectionnez les pare-feux ou les collecteurs de journaux :

- **Download And Install (Télécharger et installer)** (Recommandé) : sélectionnez **Devices (Périphériques)** (pare-feu), **Log Collectors (Collecteurs de journaux)**, ou **WildFire Appliances and Clusters (Appareils et clusters WildFire)**.
- **Download Only (Télécharger uniquement)** : Panorama télécharge la mise à jour mais ne l'installe pas.

STEP 4 | Cliquez sur **OK**.

STEP 5 | Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)**, puis **Commit (Validez)** vos changements.

Compatibilité des versions de Panorama, des collecteurs de journaux, des pare-feu et de WildFire

Pour de meilleurs résultats, respectez les consignes de compatibilité Panorama™ suivantes :

- Installez la même version de Panorama sur le serveur de gestion Panorama et sur les collecteurs de journaux dédiés.
- Panorama doit exécuter la même version ou une version ultérieure de PAN-OS que du pare-feu qu'il gère. Voir Panorama Management Compatibility (Compatibilité de la gestion de Panorama) pour plus d'informations.

  Avant de mettre à niveau les pare-feux vers PAN-OS 11.0, vous devez d'abord mettre à niveau Panorama vers la version 11.0.
- Panorama exécutant PAN-OS 11.0 peut gérer les appareils et les clusters d'appareils WildFire® qui exécutent la même version ou une version antérieure de PAN-OS. Voir Panorama Management Compatibility (Compatibilité de la gestion de Panorama) pour plus d'informations.

  Il est recommandé que le serveur de gestion Panorama, les appareils WildFire et les clusters d'appareils WildFire exécutent la même version de PAN-OS.
- La version de contenu sur le serveur de gestion Panorama doit être identique (ou antérieure) à celle des collecteurs de journaux dédiés ou des pare-feu gérés. Voir Panorama Management Compatibility (Compatibilité de la gestion de Panorama) pour plus d'informations.

  Palo Alto Networks® vous recommande d'installer la même version de la base de données des applications sur Panorama que celle des collecteurs de journaux dédiés et ses pare-feu.

  Indépendamment de si vos abonnements incluent la base de données des applications ou des applications et des menaces, Panorama n'installe que la base de données des applications. Panorama et les collecteurs de journaux dédiés n'appliquent pas les règles de stratégie et n'ont donc pas besoin des signatures de menaces de la base de données des menaces. La base de données des applications contient des métadonnées de menace (telles que les ID de menace et les noms) que vous utilisez sur Panorama et les collecteurs de journaux dédiés lors de la définition des règles de stratégie pour insérer vers les pare-feu gérés et lors de l'interprétation des informations de menace dans les journaux et les rapports. Cependant, les pare-feu requièrent la base de données complète des applications et des menaces pour faire correspondre les identifiants enregistrés dans les journaux avec les noms de menace, d'URL, ou d'application correspondants. Consultez les Notes de publication pour la version de contenu minimale que vous devez installer pour une version de Panorama.

Mettre à niveau les collecteurs de journaux lorsque Panorama est connecté à Internet

Pour obtenir la liste des logiciels et le contenu des mises à jour, vous pouvez installer sur collecteurs de journaux, voir Mises à jour prises en charge.

Si vous effectuez une mise à niveau à partir de PAN-OS 8.1, PAN-OS 9.0 a introduit un nouveau format de données de journal pour les collecteurs de journaux locaux et dédiés. Lorsque vous passez à PAN-OS 10.1, les données de journaux existantes sont automatiquement converties au nouveau format lors de la mise à niveau de PAN-OS 8.1 vers PAN-OS 9.0.

Vous devez mettre à niveau tous les collecteurs de journaux d'un groupe de collecteurs en même temps afin d'éviter de perdre des données de journal. Aucun transfert de journaux ou collecte de journaux ne se produit si les collecteurs de journaux d'un groupe de collecteurs n'utilisent pas tous la même version de PAN-OS. De plus, les données des journaux des collecteurs de journaux du groupe de collecteur ne sont pas visibles dans les onglets **ACC** ou **Monitor (Surveillance)** jusqu'à ce que tous les collecteurs de journaux exécutent la même version PAN-OS. Par exemple, si vous disposez de trois collecteurs de journaux dans un groupe de collecteurs et que vous mettez à niveau deux d'entre eux, aucun journal n'est alors transmis aux collecteurs de journaux du groupe de collecteurs.

Palo Alto Networks vous recommande de mettre à niveau les collecteurs de journaux lors d'une fenêtre de maintenance. En raison de la migration du format des journaux, la procédure de mise à niveau complète prend un nombre supplémentaire d'heures, selon la quantité de données de journaux sur les collecteur de journaux dédiés et locaux.

STEP 1 | Avant de mettre à niveau les collecteurs de journaux, vérifiez que vous exécutez la version du logiciel Panorama™ appropriée sur le serveur de gestion Panorama.

Palo Alto Networks® recommande vivement que Panorama et les Collecteurs de journaux exécutent la même version du logiciel Panorama et que Panorama, les Collecteurs de journaux et tous les pare-x gérés exécutent la même version de contenu. Pour les détails de compatibilité de logiciels et de contenus importants, voir Compatibilité des versions de Panorama, des collecteurs de journaux, des pare-feu et de WildFire.

Panorama doit exécuter la même version de logiciel (ou une version ultérieure) que le Collecteur de journaux, mais doit avoir la même version ou une version antérieure :

- **Software release version (Version du logiciel)** : si votre serveur de gestion Panorama n'exécute pas déjà la même version de logiciel ou une version ultérieure que la version à laquelle vous souhaitez mettre à jour les Collecteurs de journaux, vous devez installer la même version ou une version ultérieure sur Panorama (voir Installer les mises à jour de contenu et les mises à niveau logicielles pour Panorama) avant de mettre à jour les Collecteurs de journaux.
- **Version du contenu** : pour les versions de publication de contenu, vous devez vous assurer que tous les collecteurs de journaux exécutent la dernière version de contenu ou, au minimum, une version ultérieure à celle de Panorama. Sinon, commencez par Mettre à niveau le pare-feu vers PAN-OS

11.0 à partir de Panorama, puis mettez à jour les collecteurs de journaux avant de mettre à jour la version de contenu sur le serveur de gestion Panorama.

Pour vérifier les versions de logiciel et de contenu :

- **Serveur de gestion Panorama** : pour déterminer quelles versions de logiciel et de contenu sont en cours d'exécution sur le serveur de gestion Panorama, connectez-vous à l'interface Web Panorama et accédez aux paramètres informations générales (**Dashboard (Tableau de bord)**).
- **Collecteurs de journaux** : pour déterminer quelles versions de logiciel et de contenu sont en cours d'exécution sur les collecteurs de journaux, connectez-vous à la CLI de chaque collecteur de journaux et exécutez la commande **`show system info`**

STEP 2 | Déterminer le chemin de mise à niveau vers PAN-OS 11.0..

Vous ne pouvez pas sauter l'installation de versions majeures dans le chemin de mise à jour depuis la version PAN-OS en cours vers PAN-OS 11.0.0.

Consultez Liste de contrôle de mise à niveau de PAN-OS, *les problèmes connus et les modifications apportées au comportement par défaut dans les* Release Notes (notes de version) *et* Considérations de mise à niveau/rétrogradation *pour chaque version par laquelle vous passez dans le cadre de votre chemin de mise à niveau.*

STEP 3 | Installez les dernières mises à jour de contenu.

Consultez les Notes de version *pour les versions de contenu minimum requises pour une version de logiciel Panorama.*

1. Connectez-vous à l'interface Web Panorama.
2. Sélectionnez **Panorama** > **Device Deployment (Déploiement de périphériques)** > **Dynamic Updates (Mises à jour dynamiques)** et **Check Now (Vérifiez maintenant)** pour obtenir les dernières mises à jour. Si une mise à jour est disponible, la colonne Action affiche un lien **Download (Télécharger)**.
3. Si elles ne sont pas déjà installées, **Download (Téléchargez)** les mises à jour de contenu appropriées. Une fois le téléchargement terminé, le lien se trouvant dans la colonne Action passe de **Download (Télécharger)** à **Install (Installer)**.
4. **Install (Installez)** la mise à jour de contenu (mise à jour des applications ou des applications et menaces) avant toute autre.

   Si votre abonnement inclut à la fois du contenu Applications et Menaces, installez d'abord le contenu `Apps (Applications)`. Cela installe automatiquement le contenu Application et Menaces.

   Peu importe si votre abonnement comprend le contenu Applications et Menaces, Panorama installe et n'a besoin que du contenu Applications. Pour plus d'informations, consultez la section Compatibilité des versions de Panorama, des collecteurs de journaux, des pare-feu et de WildFire .
5. Répétez les sous-étapes pour toutes les autres mises à jour (Antivirus, WildFire ou Filtrage d'URL) au besoin, une à la fois et dans n'importe quel ordre.

STEP 4 | Mettez à niveau le Collecteur de journaux vers les versions PAN-OS le long de votre chemin de mise à niveau vers PAN-OS 11.0.

Si vous mettez à niveau plusieurs collecteurs de journaux, rationalisez le processus en déterminant les chemins de mise à niveau pour tous les collecteurs de journaux que vous avez l'intention de mettre à niveau avant de commencer à télécharger des images.

1. Upgrade Log Collectors When Panorama is Internet-Connected (Mettre à niveau les collecteurs de journaux lorsque Panorama est connecté à Internet) vers PAN-OS 8.1.
2. Upgrade Log Collectors When Panorama is Internet-Connected (Mettre à niveau les collecteurs de journaux lorsque Panorama est connecté à Internet) vers PAN-OS 9.0.

   PAN-OS 9.0 a introduit un nouveau format de journal. Les journaux sont automatiquement migrés vers le nouveau format après la mise à niveau réussie du collecteur de journaux vers PAN-OS 9.0.

   Ne poursuivez pas votre chemin de mise à niveau tant que vous n'avez pas vérifié que la migration automatique du journal s'est terminée avec succès.
3. Upgrade Log Collectors When Panorama is Internet-Connected (Mettre à niveau les collecteurs de journaux lorsque Panorama est connecté à Internet) vers PAN-OS 9.1.
4. Upgrade Log Collectors When Panorama is Internet-Connected (Mettre à niveau les collecteurs de journaux lorsque Panorama est connecté à Internet) vers PAN-OS 10.0.
5. Upgrade Log Collectors When Panorama is Internet-Connected (Mettre à niveau les collecteurs de journaux lorsque Panorama est connecté à Internet) vers PAN-OS 10.1.

   PAN-OS 11.0 introduit un nouveau format de journal. Lors de la mise à niveau de PAN-OS 11.0 vers PAN-OS 10.1, vous pouvez choisir de migrer les journaux générés dans PAN-OS 8.1 ou une version antérieure. Sinon, ces journaux sont automatiquement supprimés lors de la mise à niveau réussie vers PAN-OS 10.1. Lors de la migration, les données des journaux ne sont pas visibles dans les onglets ACC ou Monitor (Surveillance). Pendant la migration, les données de journal continuent d'être transmises au collecteur de journaux approprié, mais vous pouvez avoir un impact sur les performances.
6. Upgrade Log Collectors When Panorama is Internet-Connected (Mettre à niveau les collecteurs de journaux lorsque Panorama est connecté à Internet) vers PAN-OS 10.2.

STEP 5 | Mettez à niveau le collecteur de journaux vers PAN-OS 11.0.

1. Sur Panorama, **Check Now (Vérifier maintenant)** (**Panorama** > **Device Deployment (Déploiement de périphériques)** > **Software (Logiciel)**) les dernières mises à jour. Si une mise à jour est disponible, la colonne Action affiche un lien **Download (Télécharger)**.
2. **Download (Téléchargez)** le fichier spécifique au modèle pour la version finale de pan-OS 11.0. Par exemple, pour mettre à niveau un appareil de série M vers Panorama 11.0.0, téléchargez l'image **Panorama_m-11.0.0**.

   Après un téléchargement réussi, la colonne Action passe de **Download (Télécharger)** à **Install (Installer)** pour cette image.
3. **Install (Installez)** PAN-OS 11.0 et sélectionnez les collecteurs de journaux appropriés.
4. Sélectionnez l'une des options suivantes en fonction de votre plate-forme :
   - **Upload only to device (do not install) (Charger sur le périphérique uniquement (ne pas Installer))**.
   - **Reboot device after install (Redémarrer le périphérique après l'installation)**.
5. Cliquez sur **OK** pour démarrer le chargement ou l'installation.

STEP 6 | Vérifiez le logiciel et/ou les versions de mise à jour de contenu qui sont installées sur le collecteur de journaux.

Saisissez la commande opérationnelle **`show system info`**. Le résultat sera semblable à ci-dessous :

```
Version du logiciel : 11.0.0 app-version: 8270-6076 app-release-
date: 2020/05/08 18:21:51
```

STEP 7 | (mode FIPS-CC uniquement) Mettre à niveau Panorama et les périphériques gérés en mode FIPS-CC.

La mise à niveau d'un collecteur de journaux dédié en mode FIPS-CC nécessite que vous réinitialisiez l'état de la connexion sécurisée si vous avez ajouté le collecteur de journaux dédié à la gestion de Panorama alors que le collecteur de journaux dédié exécutait une version de PAN-OS 11.0.

Vous n'avez pas besoin de réintégrer le collecteur de journaux dédié ajouté à la gestion de Panorama lorsque le collecteur de journaux dédié exécutait une version 10.0 ou antérieure de PAN-OS.

STEP 8 | (PAN-OS 10.2 et versions ultérieures) Régénérez ou réimportez tous les certificats pour respecter le niveau de sécurité OpenSSL 2.

Cette étape est requise si vous effectuez une mise à niveau de PAN-OS 10.1 ou version antérieure vers PAN-OS 11.0. Ignorez cette étape si vous effectuez une mise à niveau à partir de PAN-OS 10.2 et que vous avez déjà régénéré ou réimporté vos certificats.

Tous les certificats doivent satisfaire aux exigences minimales suivantes :

- RSA 2048 bits ou supérieur, ou ECDSA 256 bits ou supérieur
- Digest de SHA256 ou supérieur

Consultez le Guide de l'administrateur PAN-OS ou le Guide de l'administrateur de Panorama pour plus d'informations sur la régénération ou la réimportation de vos certificats.

STEP 9 | (Recommended for Panorama virtual appliance (Recommandé pour l'appareil virtuel Panorama))Augmentez la mémoire de l'appareil virtuel Panorama à 64 Go.

Après avoir correctement mis à niveau l'appareil virtuel Panorama en mode Log Collector vers PAN-OS 11.0, Palo Alto Networks recommande d'augmenter la mémoire de l'appareil virtuel Panorama à 64 Go pour répondre à la configuration système requise accrue afin d'éviter tout problème de journalisation, de gestion et de performances opérationnelles lié à un appareil virtuel Panorama sous-provisionnée.

Mettre à niveau les collecteurs de journaux lorsque Panorama n'est pas connecté à Internet

Pour obtenir la liste des logiciels et le contenu des mises à jour, vous pouvez installer sur collecteurs de journaux, voir Mises à jour prises en charge.

Si vous effectuez une mise à niveau à partir de PAN-OS 8.1, PAN-OS 9.0 a introduit un nouveau format de données de journal pour les collecteurs de journaux locaux et dédiés. Lorsque vous passez à PAN-OS 10.1, les données de journaux existantes sont automatiquement converties au nouveau format lors de la mise à niveau de PAN-OS 8.1 vers PAN-OS 9.0.

Vous devez mettre à niveau tous les collecteurs de journaux d'un groupe de collecteurs en même temps afin d'éviter de perdre des données de journal. Aucun transfert de journaux ou collecte de journaux ne se produit si les collecteurs de journaux d'un groupe de collecteurs n'utilisent pas tous la même version de PAN-OS. De plus, les données des journaux des collecteurs de journaux du groupe de collecteur ne sont pas visibles dans les onglets **ACC** ou **Monitor (Surveillance)** jusqu'à ce que tous les collecteurs de journaux exécutent la même version PAN-OS. Par exemple, si vous disposez de trois collecteurs de journaux dans un groupe de collecteurs et que vous mettez à niveau deux d'entre eux, aucun journal n'est alors transmis aux collecteurs de journaux du groupe de collecteurs.

Palo Alto Networks vous recommande de mettre à niveau les collecteurs de journaux lors d'une fenêtre de maintenance. En raison de la migration du format des journaux, la procédure de mise à niveau complète prend un nombre supplémentaire d'heures, selon la quantité de données de journaux sur les collecteur de journaux dédiés et locaux.

STEP 1 | Avant de mettre à niveau les collecteurs de journaux, vérifiez que vous exécutez la version du logiciel Panorama™ appropriée sur le serveur de gestion Panorama.

Palo Alto Networks® recommande vivement que Panorama et les Collecteurs de journaux exécutent la même version du logiciel Panorama et que Panorama, les Collecteurs de journaux et tous les pare-x gérés exécutent la même version de contenu. Pour les détails de compatibilité de logiciels et de contenus importants, voir Compatibilité des versions de Panorama, des collecteurs de journaux, des pare-feu et de WildFire.

Panorama doit exécuter la même version de logiciel (ou une version ultérieure) que le Collecteur de journaux, mais doit avoir la même version ou une version antérieure :

- **Version du logiciel** : si votre serveur de gestion Panorama n'exécute pas déjà la même version de logiciel ou une version ultérieure que la version à laquelle vous souhaitez mettre à jour les collecteurs de journaux, vous devez installer la même version ou une version ultérieure sur

Panorama (voir Installer les mises à jour de contenu et logicielles pour Panorama) avant de mettre à jour les collecteurs de journaux.

- **Content release version (Version du contenu)** : pour les versions de publication de contenu, vous devez vous assurer que tous les collecteurs de journaux exécutent la dernière version de contenu ou, au minimum, une version ultérieure à celle de Panorama. Sinon, commencez par Mettre à niveau le pare-feu vers PAN-OS 11.0 à partir de Panorama, puis mettez à jour les collecteurs de journaux avant de mettre à jour la version de contenu sur le serveur de gestion Panorama (voir Mettre à niveau le pare-feu vers PAN-OS 11.0 à partir de Panorama).

Pour vérifier les versions de logiciel et de contenu :

- **Serveur de gestion Panorama** : pour déterminer quelles versions de logiciel et de contenu sont en cours d'exécution sur le serveur de gestion Panorama, connectez-vous à l'interface Web Panorama et accédez aux paramètres informations générales (**Dashboard (Tableau de bord)**).
- **Collecteurs de journaux** : pour déterminer quelles versions de logiciel et de contenu sont en cours d'exécution sur les collecteurs de journaux, connectez-vous à la CLI de chaque collecteur de journaux et exécutez la commande **`show system info`**

STEP 2 | Déterminer le chemin de mise à niveau vers PAN-OS 11.0..

Consultez Liste de contrôle de mise à niveau de PAN-OS, les problèmes connus et les modifications apportées au comportement par défaut dans les Release Notes (notes de version) et Considérations de mise à niveau/rétrogradation pour chaque version par laquelle vous passez dans le cadre de votre chemin de mise à niveau.

Si vous mettez à niveau plusieurs collecteurs de journaux, rationalisez le processus en déterminant les chemins de mise à niveau pour tous les collecteurs de journaux que vous avez l'intention de mettre à niveau avant de commencer à télécharger des images.

STEP 3 | Téléchargez les mises à jour de contenu et logicielles sur un hôte qui peut se connecter et charger les fichiers sur Panorama via SCP ou HTTPS.

Consultez les Notes de version pour les versions de contenu minimum requises pour une version de logiciel Panorama.

1. Utilisez un hôte avec accès à Internet pour ouvrir une session sur le site Web d'assistance client de Palo Alto Networks.
2. Téléchargez la dernière mise à jour du contenu :
   1. Cliquez **Dynamic Updates (Mises à jour dynamique)** dans la section Ressources.
   2. **Download (Téléchargez)** les dernières mises à jour de contenu et enregistrez les fichiers sur l'hôte. Effectuez cette étape pour chaque type de contenu que vous allez mettre à jour.
3. Téléchargez les mises à jour logicielles :
   1. Retournez à la page principale du site d'assistance client de Palo Alto Networks et cliquez sur **Software Updates (Mises à jour logicielles)** dans la section Ressources.
   2. Consultez la colonne Télécharger pour déterminer la version à installer. Les noms de fichiers de package de mise à jour pour les appareils de série M commencent par « Panorama_m »

suivi du numéro de version. Par exemple, pour mettre à niveau un appareil de série M vers Panorama 11.0.0, téléchargez l'image **Panorama_m-11.0.0**.

*Vous pouvez rapidement localiser les images de Panorama en sélectionnant **Panorama M Images (Images M Panorama)** (pour les appareils de série M) depuis le menu déroulant **Filter By (Filtrer par)**.*

4. Cliquez sur le nom du fichier approprié et enregistrez le fichier sur l'hôte.

STEP 4 | Installez les dernières mises à jour de contenu.

Si vous devez installer des mises à jour de contenu, vous devez le faire avant d'installer les mises à jour logicielles. En outre, installez d'abord les mises à jour de contenu sur les pare-feu, puis sur les collecteurs de journaux avant de mettre à jour la version de contenu sur Panorama.

Installez d'abord les mises à jour des applications ou des applications et menaces, puis installez toutes les autres mises à jour (Antivirus, WildFire® ou Filtrage d'URL) au besoin, une à la fois et dans n'importe quel ordre.

Peu importe si votre abonnement comprend le contenu Applications et Menaces, Panorama installe et n'a besoin que du contenu Applications. Pour plus d'informations, consultez la section Compatibilité des versions de Panorama, des collecteurs de journaux, des pare-feu et de WildFire .

1. Connectez-vous à l'interface Web Panorama.
2. Sélectionnez **Panorama (Panorama)** > **Device Deployment (Déploiement du périphérique)** > **Dynamic Updates (Mises à jour dynamiques)**.
3. Cliquez sur **Upload (Charger)**, sélectionnez le **Type** de mise à jour, **Browse (Rechercher)** le fichier de mise à jour de contenu approprié sur l'hôte, puis cliquez sur **OK**.
4. Cliquez sur **Install From File (Installer depuis le fichier)**, sélectionnez le **Type** de mise à jour et sélectionnez le **File Name (Nom du fichier)** de la mise à jour que vous venez de charger.
5. Sélectionnez les collecteurs de journaux.
6. Cliquez sur **OK** pour démarrer l'installation.
7. Répétez ces étapes pour chaque mise à jour de contenu.

STEP 5 | Mettez à niveau le Collecteur de journaux vers les versions PAN-OS le long de votre chemin de mise à niveau vers PAN-OS 11.0.

1. update managed firewalls (using Panorama) (Mettre à niveau les collecteurs de journaux lorsque Panorama n'est pas connecté à Internet) vers PAN-OS 8.1.
2. Upgrade Log Collectors When Panorama is Not Internet-Connected (Mettre à niveau les collecteurs de journaux lorsque Panorama n'est pas connecté à Internet) vers PAN-OS 9.0.

   PAN-OS 9.0 a introduit un nouveau format de journal. Les journaux sont automatiquement migrés vers le nouveau format après la mise à niveau réussie du collecteur de journaux vers PAN-OS 9.0.

   Ne poursuivez pas votre chemin de mise à niveau tant que vous n'avez pas vérifié que la migration automatique du journal s'est terminée avec succès.
3. Upgrade Log Collectors When Panorama is Not Internet-Connected (Mettre à niveau les collecteurs de journaux lorsque Panorama n'est pas connecté à Internet) vers PAN-OS 9.1.
4. Upgrade Log Collectors When Panorama is Not Internet-Connected (Mettre à niveau les collecteurs de journaux lorsque Panorama n'est pas connecté à Internet) vers PAN-OS 10.0.
5. Upgrade Log Collectors When Panorama is Not Internet-Connected (Mettre à niveau les collecteurs de journaux lorsque Panorama n'est pas connecté à Internet) vers PAN-OS 10.1.

   PAN-OS 10.0 introduit un nouveau format de journal. Lors de la mise à niveau de PAN-OS 10.0 vers PAN-OS 10.1, vous pouvez choisir de migrer les journaux générés dans PAN-OS 8.1 ou une version antérieure. Sinon, ces journaux sont automatiquement supprimés lors de la mise à niveau réussie vers PAN-OS 10.1. Lors de la migration, les données des journaux ne sont pas visibles dans les onglets ACC ou Monitor (Surveillance). Pendant la migration, les données de journal continuent d'être transmises au collecteur de journaux approprié, mais vous pouvez avoir un impact sur les performances.
6. Upgrade Log Collectors When Panorama is Not Internet-Connected (Mettre à niveau les collecteurs de journaux lorsque Panorama n'est pas connecté à Internet) vers PAN-OS 10.2.

STEP 6 | Mettez à niveau le collecteur de journaux vers PAN-OS 11.0.

1. Sélectionnez **Panorama** > **Device Deployment (Déploiement de périphérique)** > **Software (Logiciel)**.
2. Cliquez sur **Upload (Charger)**, **Browse (Rechercher)** le fichier de mise à jour logicielle approprié sur l'hôte, puis cliquez sur **OK**.
3. Cliquez sur **Install (Installer)** dans la colonne Action pour la version que vous venez de charger.
4. **Install (Installez)** PAN-OS 11.0 et sélectionnez les collecteurs de journaux appropriés.
5. Sélectionnez l'une des options suivantes en fonction de votre plate-forme :
   - **Upload only to device (do not install) (Charger sur le périphérique uniquement (ne pas Installer))**.
   - **Reboot device after install (Redémarrer le périphérique après l'installation)**.
6. Cliquez sur **OK** pour démarrer le chargement ou l'installation.

STEP 7 | Vérifiez que le logiciel et/ou les versions de mise à jour de contenu sont installées sur le collecteur de journaux.

Ouvrez une session ILC du Collecteur de Journaux et rendez la commande **`montrer les informations système`** opérationnelle. Le résultat sera semblable à ci-dessous :

```
Version du logiciel : 11.0.0 app-version: 8270-6076 app-release-
date: 2020/05/08 18:21:51
```

STEP 8 | (mode FIPS-CC uniquement) Mettre à niveau Panorama et les périphériques gérés en mode FIPS-CC.

La mise à niveau d'un collecteur de journaux dédié en mode FIPS-CC nécessite que vous réinitialisiez l'état de la connexion sécurisée si vous avez ajouté le collecteur de journaux dédié à la gestion de Panorama alors que le collecteur de journaux dédié exécutait une version de PAN-OS 11.0.

Vous n'avez pas besoin de réintégrer le collecteur de journaux dédié ajouté à la gestion de Panorama lorsque le collecteur de journaux dédié exécutait une version 10.0 ou antérieure de PAN-OS.

STEP 9 | (PAN-OS 10.2 et versions ultérieures) Régénérez ou réimportez tous les certificats pour respecter le niveau de sécurité OpenSSL 2.

Cette étape est requise si vous effectuez une mise à niveau de PAN-OS 10.1 ou version antérieure vers PAN-OS 11.0. Ignorez cette étape si vous effectuez une mise à niveau à partir de PAN-OS 10.2 et que vous avez déjà régénéré ou réimporté vos certificats.

Tous les certificats doivent satisfaire aux exigences minimales suivantes :

- RSA 2048 bits ou supérieur, ou ECDSA 256 bits ou supérieur
- Digest de SHA256 ou supérieur

Consultez le Guide de l'administrateur PAN-OS ou le Guide de l'administrateur de Panorama pour plus d'informations sur la régénération ou la réimportation de vos certificats.

STEP 10 | (Recommended for Panorama virtual appliance (Recommandé pour l'appareil virtuel Panorama))Augmentez la mémoire de l'appareil virtuel Panorama à 64 Go.

Après avoir correctement mis à niveau l'appareil virtuel Panorama en mode Log Collector vers PAN-OS 11.0, Palo Alto Networks recommande d'augmenter la mémoire de l'appareil virtuel Panorama à 64 Go pour répondre à la configuration système requise accrue afin d'éviter tout problème de journalisation, de gestion et de performances opérationnelles lié à un appareil virtuel Panorama sous-provisionnée.

Mettre à niveau un cluster WildFire à partir de Panorama avec une connexion Internet

Les appareils WildFire d'un cluster peuvent être mis à niveau parallèlement lorsqu'ils sont gérés par Panorama. Si Panorama dispose d'une connexion directe à l'Internet, vous pouvez vérifier l'existence de nouvelles versions et les télécharger directement de Panorama.

Panorama ne peut gérer que des appareils et des clusters d'appareils WildFire qui utilisent la même version logicielle ou une version logicielle ultérieure.

STEP 1 | Faites passer Panorama à une version équivalente ou ultérieure que la version logicielle que vous souhaitez installer sur le cluster WildFire.

Pour plus de renseignements sur la mise à jour de Panorama, reportez-vous à la section Installer les mises à jour de contenu et logicielles pour Panorama.

STEP 2 | Suspendez temporairement les analyses des échantillons.

1. Cessez le transfert, par les pare-feu, des nouveaux échantillons vers l'appareil WildFire.
   1. Connectez-vous à l'interface Web du pare-feu.
   2. Sélectionnez **Device > Setup > WildFire (Périphérique > Configuration > WildFire)** et modifiez les **General Settings (Paramètres généraux)**.
   3. Décochez le champ **WildFire Private Cloud (Cloud WildFire privé)**.
   4. Cliquez sur **OK**, puis sur **Commit (Valider)**.
2. Confirmez que l'analyse des échantillons que le pare-feu a déjà soumis à l'appareil est terminée :
   1. Connectez-vous à l'interface Web Panorama.
   2. Sélectionnez **Panorama (Panorama) > Managed WildFire Clusters (Clusters WildFire gérés)** et **View (Afficher)** l'**Utilization (Utilisation)** de l'environnement d'analyse des clusters.
   3. Vérifiez qu'aucune analyse d'échantillons n'est en cours dans la **Virtual Machine Usage (Utilisation de la machine virtuelle)**.

   Si vous ne voulez pas attendre que l'appareil WildFire termine d'analyser les échantillons récemment envoyés, vous pouvez passer à l'étape suivante. Sachez toutefois que l'appareil WildFire abandonnera alors les échantillons en attente dans la file d'attente pour analyse.

STEP 3 | Installez la dernière mise à jour de contenu pour l'appareil WildFire.

Grâce à ces mises à jour, l'appareil dispose des renseignements sur les menaces les plus récentes, ce qui lui permet de bien détecter les logiciels malveillants.

Vous devez installer les mises à jour de contenu avant d'installer les mises à jour logicielles. Consultez les Notes de version pour la version de contenu minimale que vous devez installer pour une version de Panorama.

1. Téléchargez la mise à jour du contenu pour WildFire :
   1. Sélectionnez **Panorama (Panorama) > Device Deployment (Déploiement du périphérique) > Dynamic Updates (Mises à jour dynamiques)**.
   2. Sélectionnez un module de mise à jour du contenu WildFire, puis cliquez sur **Download (Télécharger)**.
2. Cliquez sur **Install (Installer)**.
3. Sélectionnez le ou les clusters d'appareils WildFire ou les appareils individuels que vous souhaitez mettre à niveau.
4. Cliquez sur **OK** pour démarrer l'installation.

STEP 4 | Téléchargez la version PAN-OS du logiciel sur l'appareil WildFire.

Lorsque vous mettez à jour l'appareil WildFire, vous ne pouvez sauter de versions principales. Par exemple, si vous souhaitez passer de la PAN-OS 9.1 à PAN-OS 11.0, vous devez d'abord télécharger et PAN-OS 10.0, PAN-OS 10.1 et PAN-OS 10.2.

1. Téléchargez la mise à niveau logicielle pour WildFire :
   1. Sélectionnez **Panorama** > **Device Deployment** > **Software (Panorama** > **Déploiement de périphérique** > **Logiciel)**.
   2. Cliquez sur **Check Now (Vérifier maintenant)** pour récupérer une liste à jour des versions.
   3. Sélectionnez la version de WildFire que vous souhaitez installer et cliquez sur **Download (Télécharger)**.
   4. Cliquez sur **Close (Fermer)** pour sortir de la fenêtre **Download Software (Télécharger le logiciel)**.
2. Cliquez sur **Install (Installer)**.
3. Sélectionnez le ou les clusters d'appareils WildFire que vous souhaitez mettre à niveau.
4. Sélectionnez Redémarrer le périphérique après l'installation :
5. Cliquez sur **OK** pour démarrer l'installation.
6. (Facultatif) Surveillez la progression de l'installation sur Panorama.

STEP 5 | (Optional (Facultatif)) Affichez l'état des tâches de redémarrage du nœud de contrôle WildFire.

Sur le contrôleur du cluster WildFire, exécutez la commande suivante et consultez le type de tâche **`Install`** et l'état **`FIN`** :

```
admin@WF-500(active-controller)> afficher les tâches en attente du
 cluster
```

STEP 6 | Vérifiez que l'appareil WildFire est prêt à reprendre l'analyse des échantillons.

1. Vérifiez que le champ sw-version indique 11.0.0:

   ```
   admin@WF-500 (contrôleur passif)> afficher les informations
    système | correspondre à la version logiciel
   ```

2. Confirmez que tous les processus fonctionnent :

   ```
   admin@WF-500(passive-controller)> show system software status
   ```

3. Confirmez que la tâche d'auto-validation(**`AutoCom`**) est terminée :

   ```
   admin@WF-500 (contrôleur passif)> afficher tous les travaux
   ```


Mettre à niveau un cluster WildFire à partir de Panorama sans connexion Internet

Les appareils WildFire d’un cluster peuvent être mis à niveau parallèlement lorsqu’ils sont gérés par Panorama. Si Panorama ne dispose pas d’une connexion directe à l’Internet, vous devez télécharger les mises à jour de contenu et logicielles sur le site de support Palo Alto Networks et les héberger sur un serveur interne avant qu’elles ne puissent être distribuées par Panorama.

Panorama ne peut gérer que des appareils et des clusters d’appareils WildFire qui utilisent la même version logicielle ou une version logicielle ultérieure.

STEP 1 | Faites passer Panorama à une version équivalente ou ultérieure que la version logicielle que vous souhaitez installer sur le cluster WildFire.

Pour plus de renseignements sur la mise à jour de Panorama, reportez-vous à la section Installer les mises à jour de contenu et logicielles pour Panorama.

STEP 2 | Suspendez temporairement les analyses des échantillons.

1. Cessez le transfert, par les pare-feu, des nouveaux échantillons vers l’appareil WildFire.
   1. Connectez-vous à l’interface Web du pare-feu.
   2. Sélectionnez **Device > Setup > WildFire (Périphérique > Configuration > WildFire)** et modifiez les **General Settings (Paramètres généraux)**.
   3. Décochez le champ **WildFire Private Cloud (Cloud WildFire privé)**.
   4. Cliquez sur **OK**, puis sur **Commit (Valider)**.
2. Confirmez que l’analyse des échantillons que le pare-feu a déjà soumis à l’appareil est terminée :
   1. Connectez-vous à l’interface Web Panorama.
   2. Sélectionnez **Panorama (Panorama) > Managed WildFire Clusters (Clusters WildFire gérés)** et **View (Afficher)** l’**Utilization (Utilisation)** de l’environnement d'analyse des clusters.
   3. Vérifiez qu’aucune analyse d’échantillons n'est en cours dans la **Virtual Machine Usage (Utilisation de la machine virtuelle)**.

   Si vous ne voulez pas attendre que l’appareil WildFire termine d’analyser les échantillons récemment envoyés, vous pouvez passer à l’étape suivante. Sachez toutefois que l’appareil WildFire abandonnera alors les échantillons en attente dans la file d'attente pour analyse.

STEP 3 | Téléchargez les mises à jour de contenu et logicielles de WildFire sur un hôte avec un accès Internet. Panorama doit avoir accès à l'hôte.

1. Utilisez un hôte avec accès à Internet pour ouvrir une session sur le site Web d’assistance client de Palo Alto Networks.
2. Téléchargez les mises à jour de contenu :
   1. Cliquez sur **Dynamic Updates (Mises à jour dynamique)** dans la section Tools (Outils).
   2. **Download (Téléchargez)** le contenu souhaité et enregistrez le fichier sur l'hôte. Effectuez cette étape pour chaque type de contenu que vous allez mettre à jour.
3. Télécharger les mises à jour logicielles :
   1. Revenez à la page principale du site de Support Clients de Palo Alto Networks et cliquez sur **Software Updates (Mises à jour de logiciel)** dans la section Tools (Outils).
   2. Consultez la colonne Télécharger pour déterminer la version à installer. Le nom de fichier du module de mise à jour indique le modèle et la version de la mise à niveau : WildFire_<release>.
   3. Cliquez sur le nom du fichier et enregistrez le fichier sur l'hôte.

STEP 4 | Installez la dernière mise à jour de contenu pour l’appareil WildFire.

Grâce à ces mises à jour, l'appareil dispose des renseignements sur les menaces les plus récentes, ce qui lui permet de bien détecter les logiciels malveillants.

Vous devez installer les mises à jour de contenu avant d’installer les mises à jour logicielles. Consultez les Notes de version pour la version de contenu minimale que vous devez installer pour une version de Panorama.

1. Téléchargez la mise à jour du contenu pour WildFire :
   1. Sélectionnez **Panorama (Panorama) > Device Deployment (Déploiement du périphérique) > Dynamic Updates (Mises à jour dynamiques)**.
   2. Cliquez sur **Upload (Télécharger)**, sélectionnez le **Type (Type)** de contenu, **Browse (Recherchez)** le fichier de mise à jour de contenu WildFire, puis cliquez sur **OK (OK)**.
   3. Cliquez sur **Install From File (Installer depuis le fichier)**, sélectionnez le **Type (Type)** de module, le **File Name (Nom de fichier)** et les appareils WildFire du cluster que vous souhaitez mettre à niveau, puis cliquez sur **OK (OK)**.
2. Cliquez sur **OK** pour démarrer l’installation.

STEP 5 | Téléchargez la version PAN-OS du logiciel sur l'appareil WildFire.

Lorsque vous mettez à jour l'appareil WildFire, vous ne pouvez sauter de versions principales. Par exemple, si vous souhaitez passer de la PAN-OS 9.1 à PAN-OS 11.0, vous devez d'abord télécharger et PAN-OS 10.0, PAN-OS 10.1 et PAN-OS 10.2.

1. Téléchargez la mise à niveau logicielle pour WildFire :
   1. Sélectionnez **Panorama > Device Deployment > Software (Panorama > Déploiement de périphérique > Logiciel)**.
   2. Cliquez sur **Check Now (Vérifier maintenant)** pour récupérer une liste à jour des versions.
   3. Sélectionnez la version de WildFire que vous souhaitez installer et cliquez sur **Download (Télécharger)**.
   4. Cliquez sur **Close (Fermer)** pour sortir de la fenêtre **Download Software (Télécharger le logiciel)**.
2. Cliquez sur **Install (Installer)**.
3. Sélectionnez le ou les clusters d'appareils WildFire que vous souhaitez mettre à niveau.
4. Sélectionnez Redémarrer le périphérique après l'installation :
5. Cliquez sur **OK** pour démarrer l'installation.
6. (Facultatif) Surveillez la progression de l'installation sur Panorama.

STEP 6 | (Optional (Facultatif)) Affichez l'état des tâches de redémarrage du nœud de contrôle WildFire.

Sur le contrôleur du cluster WildFire, exécutez la commande suivante et consultez le type de tâche **`Install`** et l'état **`FIN`** :

```
admin@WF-500(active-controller)> afficher les tâches en attente du
 cluster
```

STEP 7 | Vérifiez que l'appareil WildFire est prêt à reprendre l'analyse des échantillons.

1. Vérifiez que le champ sw-version indique 11.0.0:

   ```
   admin@WF-500 (contrôleur passif)> afficher les informations
    système | correspondre à la version logiciel
   ```

2. Confirmez que tous les processus fonctionnent :

   admin@WF-500(passive-controller)> **`show system software status`**

3. Confirmez que la tâche d'auto-validation(**`AutoCom`**) est terminée :

   ```
   admin@WF-500 (contrôleur passif)> afficher tous les travaux
   ```

Mettre à niveau les pare-feu lorsque Panorama est connecté à Internet

Passez en revue les PAN-OS 11.0 Release Notes (notes de publication de PAN-OS 11.0) puis utilisez la procédure suivante pour mettre à niveau les pare-feux que vous gérez avec Panorama. Cette procédure s'applique aux pare-feu autonomes et aux pare-feu déployés dans une configuration à haute disponibilité (HA).

Lorsque vous mettez à niveau des pare-feu HA sur plusieurs versions PAN-OS de fonctionnalités, vous devez mettre à niveau chaque pair HA vers la même version PAN-OS de fonctionnalités sur votre chemin de mise à niveau avant de continuer. Par exemple, vous mettez à niveau les pairs HA de PAN-OS 10.0 vers PAN-OS 11.0. Vous devez mettre à niveau les deux homologues HA vers PAN-OS 10.1 avant de pouvoir continuer la mise à niveau vers la version PAN-OS 11.0 cible. Lorsque les pairs HA sont espacés de deux versions de fonctionnalités ou plus, le pare-feu avec l'ancienne version installée entre dans un état `suspended (suspendu)` avec le message `Peer version too old (Peer version trop ancienne)`.

Si Panorama ne parvient pas à se connecter directement au serveur de mises à jour, suivez la procédure Mettre à niveau les pare-feu lorsque Panorama n'est pas connecté à Internet *afin de pouvoir télécharger manuellement des images dans Panorama, puis les distribuer les images sur le pare-feu.*

La nouvelle fonctionnalité Ignorer la mise à niveau des versions logicielles vous permet d'ignorer jusqu'à trois versions lors du déploiement de mises à niveau des appareils Panorama sur PAN-OS 11.0 vers des pare-feux sur PAN-OS 10.1 ou versions ultérieures.

Avant de faire la mise-à-jour du pare-feu sur Panorama, vous devez :

- Assurez-vous que Panorama exécute la même version ou une version ultérieure de PAN-OS que celle utilisée pour la mise à niveau. Vous devez mettre à niveau Panorama et ses Log Collectors (Collecteurs de journaux) vers la version 11.0 avant de mettre à niveau les pare-feu gérés vers cette version. Lorsque vous mettez à niveau les collecteurs de journaux vers la version 11.0, vous devez mettre à niveau tous les collecteurs de journaux en même temps en raison des modifications de l'infrastructure de journalisation.
- Assurez-vous que les pare-feu sont branchés à une source d'alimentation fiable. La perte de courant au cours d'une mise à niveau peut rendre les pare-feu inutilisables.
- Décidez si vous souhaitez rester en mode hérité si le périphérique virtuel Panorama est en mode hérité lors de la mise à niveau vers PAN-OS 11.0. Le mode hérité n'est pas pris en charge pour un nouveau déploiement de périphérique virtuel Panorama exécutant PAN-OS 9.1 ou une version ultérieure. Si vous mettez à niveau le périphérique virtuel Panorama de PAN-OS 9.0 ou d'une version antérieure vers PAN-OS 11.0, Palo Alto Networks recommande de revoir les Setup Prerequisites for the Panorama Virtual Appliance (Conditions préalables à la configuration du périphérique virtuel Panorama) et de passer en Panorama mode (mode Panorama) ou en Management Only mode (mode Gestion uniquement) en fonction de vos besoins.

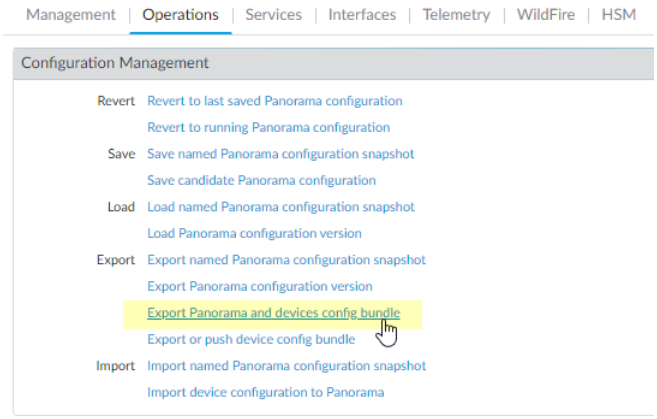
  Si vous souhaitez conserver le périphérique virtuel Panorama en mode hérité, increase CPUs and memory (augmentez les processeurs et la mémoire) alloués au périphérique virtuel Panorama à un minimum de 16 processeurs et 16 Go de mémoire pour réussir la mise à niveau vers PAN-OS 11.0. Consultez les Setup Prerequisites for the Panorama Virtual Appliance (conditions préalables à l'installation du périphérique virtuel Panorama) pour plus d'informations.

STEP 1 | Connectez-vous à l'interface Web Panorama.

STEP 2 | Effectuez une copie de sauvegarde du fichier de configuration actuel sur chaque pare-feu géré que vous envisagez de mettre à niveau.

Bien que le pare-feu crée automatiquement une sauvegarde de la configuration, il est recommandé de créer et de stocker une sauvegarde externe avant de procéder à la mise à niveau.

1. Sélectionnez **Panorama** > **Setup (Configuration)** > **Operations (Opérations)** et cliquez sur**Export Panorama and devices config bundle (Exporter la solution de configuration de Panorama et des périphériques)** pour générer et exporter la dernière la sauvegarde de configuration de Panorama et celle de chaque appareil géré.



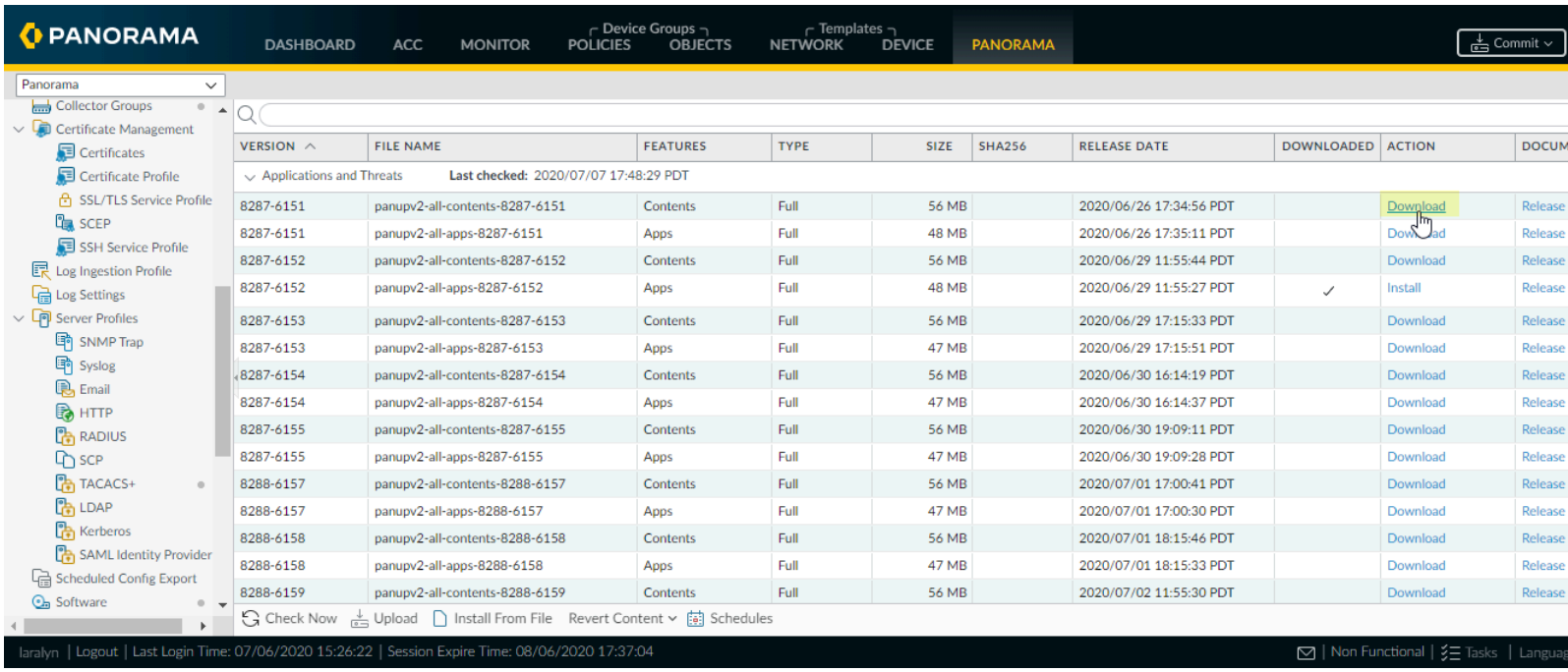
2. Enregistrez le fichier exporté dans un emplacement externe au pare-feu. Vous pouvez utiliser cette sauvegarde pour restaurer la configuration en cas de problème pendant la mise à niveau.

STEP 3 | Installez la dernière mise à jour de contenu.

Consultez les Release Notes (Notes de publication) de la version minimale de contenu que vous devez installer pour PAN-OS 11.0. Assurez-vous de suivre les Meilleures pratiques pour les mises à jour du contenu de menace et des applications lors du déploiement des mises à jour de contenu sur Panorama et les pare-feu gérés.

1. Sélectionnez **Panorama** > **Device Deployment (Déploiement de périphériques)** > **Dynamic Updates (Mises à jour dynamiques)** et **Check Now (Vérifiez maintenant)** pour obtenir les

dernières mises à jour. Si une mise à jour est disponible, la colonne Action affiche un lien **Download (Télécharger)**.



2. Cliquez sur **Install (Installer)** et sélectionnez les pare-feux sur lesquels vous voulez installer la mise à jour. Si vous mettez à niveau des pare-feu HA, vous devez mettre à jour le contenu des deux homologues.
3. Cliquez sur **OK**.

STEP 4 | Déterminer le chemin de mise à niveau vers PAN-OS 11.0..

Passez en revue la PAN-OS Upgrade Checklist (liste de vérification de mise à jour PAN-OS)*, les problèmes connus et les modifications du comportement par défaut dans les* Release Notes (Notes de version) *et les* upgrade/downgrade considerations (considérations de mise à niveau vers une version supérieure ou antérieure) *pour chaque version à travers laquelle vous passez dans le cadre de votre chemin de mise à niveau.*

Si vous mettez à niveau plusieurs pare-feu, rationalisez le processus en déterminant les chemins de mise à niveau de tous les pare-feu avant de commencer à télécharger des images.

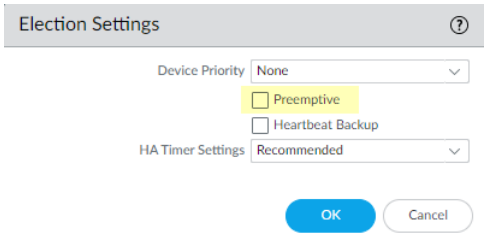
STEP 5 | (Best Practices (Meilleures pratiques)) Si vous utilisez Cortex Data Lake (CDL), install the device certificate (installez le certificat du périphérique).

Le pare-feu passe automatiquement à l'utilisation du certificat du périphérique pour l'authentification avec l'ingestion de CDL et les points de terminaison d'interrogation lors de la mise à niveau vers PAN-OS 11.0.

Si vous n'installez pas le certificat de périphérique avant la mise à niveau vers PAN-OS 11.0, le pare-feu continue d'utiliser les certificats de service de journalisation existants pour l'authentification.

STEP 6 | (HA firewall upgrades only) Si vous mettez à niveau des pare-feu faisant partie d'une paire haute disponibilité, désactivez la préemption. Vous devez uniquement désactiver ce paramètre sur un pare-feu dans chaque paire haute disponibilité.

1. Sélectionnez **Device (Périphérique)** > **High Availability (Haute disponibilité)** et modifiez les **Election Settings (Paramètres de sélection)**.
2. si cette option est activée, désactivez (effacez) le **Preemptive (paramètre préemptif)** et cliquez sur **OK**.



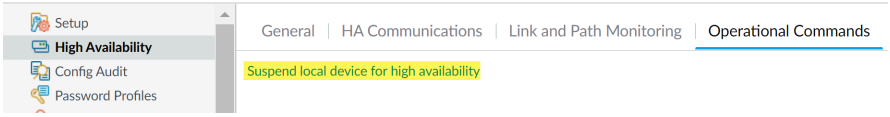
3. **Commit (Validez)** la modification. Assurez que la validation est un succès avant de procéder à la mise-à-jour.

STEP 7 | (HA firewall upgrades only (Mises à niveau du pare-feu HA uniquement)) Suspendez l'homologue HA principal pour forcer un basculement.

(Pare-feux actifs/passifs) Pour les pare-feux dans une configuration HA active/passive, suspendez et mettez à niveau le pair HA actif en premier.

(Pare-feux actifs/actifs) Pour les pare-feux dans une configuration HA active/active, suspendez et mettez à niveau d'abord le pair HA actif-primaire.

1. Log in to the firewall web interface (Connectez-vous à l'interface Web du pare-feu) principal actif de l'homologue HA du pare-feu.
2. Sélectionnez **Device (Équipement)** > **High Availability (Haute disponibilité)** > **Operational Commands (Commandes opérationnelles)**, puis cliquez sur le lien **Suspend local device (Suspendre le périphérique local)**.



3. Dans le coin inférieur droit, vérifiez que l'état est `suspended (suspendu)`.

   Le basculement qui en résulte doit entraîner la transition de l'homologue HA passif secondaire vers l'état `actif` .

   Le basculement résultant vérifie que le basculement HA fonctionne correctement avant la mise à niveau.

STEP 8 | (Facultatif) Mettez à niveau vos pare-feu gérés vers PAN-OS 10.1.

La fonctionnalité de mise à niveau de version logicielle ignore prend en charge les pare-feu gérés exécutant PAN-OS 10.1 ou versions ultérieures. Si vos pare-feu gérés sont sur PAN-OS 10.0 ou une version antérieure, commencez par effectuer une mise à niveau vers PAN-OS 10.1 ou une version ultérieure.

STEP 9 | (Optional (Facultatif)) **Export (Exportez)** le fichier vers un serveur SCP configuré.

Dans PAN-OS 11.0, les serveurs SCP sont disponibles en tant que source de téléchargement lors du déploiement de mises à niveau vers des pare-feu gérés. Exportez le fichier avant de télécharger le logiciel et les images de contenu à l'étape suivante.

STEP 10 | Validez et téléchargez les versions logicielles et de contenu requises pour la version cible.

Dans cette étape, vous pouvez afficher et télécharger les images logicielles et de contenu intermédiaires requises pour effectuer la mise à niveau vers PAN-OS 11.0.

Le téléchargement de logiciels et d'images de contenu à l'aide du téléchargement multi-images est facultatif. Vous pouvez toujours télécharger des images une à la fois.

1. Cliquez sur **Panorama** > **Device Deployment** > **Software** > **Action** > **Validate**.
2. Affichez les versions intermédiaires du logiciel et du contenu que vous devez télécharger.
3. Sélectionnez les pare-feux que vous souhaitez mettre à niveau et cliquez sur **Deploy (Déployer)**.
4. Sélectionnez une source de téléchargement et cliquez sur **Télécharger**.

STEP 11 | Installez PAN-OS 11.0.0 sur les pare-feux.

*(SD-WAN only (SD-WAN uniquement)) Pour conserver un état précis de vos liaisons SD-WAN, vous devez mettre à niveau vos pare-feu de concentrateur vers PAN-OS 11.0 avant de mettre à niveau vos pare-feu de succursale. La mise à jour des pare-feux de branche avant les pare-feux de plate-forme peut entraîner une mauvaise surveillance des données (**Panorama** > **SD-WAN** > **Monitoring (Surveillance)**) et les liens SD-WAN peuvent être affichés comme étant `down (en panne)` de façon erronée.*

1. Cliquez sur **Install (Installer)** dans la colonne Action correspondant aux modèles de pare-feu que vous souhaitez mettre à niveau. Par exemple, si vous souhaitez mettre à niveau vos pare-feux PA-220, cliquez sur **Install (installer)** dans la ligne correspondant à PanOS_220-11.0.0.
2. Dans la boîte de dialogue Déployer le fichier logiciel, sélectionnez tous les pare-feu que vous souhaitez mettre à niveau.

   (HA firewall upgrades only (Mises à niveau du pare-feu HA uniquement)) Pour réduire les temps d'arrêt, sélectionnez un seul homologue dans chaque paire HA. Pour les paires actives / passives, sélectionnez l'homologue passif; pour les paires actives / actives, sélectionnez l'homologue actif-secondaire.
3. (Mises à niveau des pare-feu HA uniquement) Assurez-vous que le **Group HA Peers (Groupe de paire HA)** n'est pas sélectionné.
4. Sélectionnez **Reboot device after install (Redémarrer le périphérique après l'installation)**.
5. Pour débuter la mise à jour, cliquez sur **OK**.
6. Une fois l'installation terminée, redémarrez en utilisant l'une des méthodes suivantes :
   - Si vous êtes invité à redémarrer, cliquez sur **Yes (Oui)**.
   - Si vous n'êtes pas invité à redémarrer, sélectionnez **Device (Périphérique)** > **Configuration** > **Operations (Opérations)** et **Reboot Device (Redémarrez le périphérique)**.
7. Après que le pare-feu a terminé le redémarrage, sélectionnez **Panorama** > **Managed Devices (Périphériques gérés)** et vérifiez que la version du logiciel est 11.0.0 pour les pare-feu que vous

avez mis à niveau. Vérifiez également que le statut HA de tous les pare-feu passifs mis à niveau est toujours passif.

STEP 12 | (HA firewall upgrades only (Mises à niveau du pare-feu HA uniquement)) Restaurez la fonctionnalité HA sur l'homologue HA principal.

1. Log in to the firewall web interface (Connectez-vous à l'interface Web) du pare-feu principal suspendu de l'homologue HA du pare-feu.
2. SélectionnezDevice (Appareil) > High Availability (Haute disponibilité) > Operational Commands (Commandes opérationnelles) et Make local device functional for high availability (Activez le périphérique local pour la haute disponibilité).
3. Dans le coin inférieur droit, vérifiez que l'état est `Passive (Passif)`. Pour les pare-feu dans une configuration active/active, vérifiez que l'état est `Active (Actif)`.
4. Attendez que la configuration de l'homologue HA en cours se synchronise.

   Dans **Dashboard (tableau de bord)**, surveillez l'état de la configuration d'exécution dans le widget Haute disponibilité.

STEP 13 | (HA firewall upgrades only (Mises à niveau du pare-feu HA uniquement)) Suspendez l'homologue HA secondaire pour forcer un basculement vers l'homologue HA principal.

1. Log in to the firewall web interface (Connectez-vous à l'interface Web) du pare-feu secondaire actif de l'homologue HA du pare-feu.
2. Sélectionnez **Device (Équipement)** > **High Availability (Haute disponibilité)** > **Operational Commands (Commandes opérationnelles)**, puis cliquez sur le lien **Suspend local device (Suspendre le périphérique local)**.
3. Dans le coin inférieur droit, vérifiez que l'état est `suspended (suspendu)`.

   Le basculement qui en résulte doit entraîner la transition de l'homologue HA passif principal vers l'état `actif` .

   Le basculement résultant vérifie que le basculement HA fonctionne correctement avant la mise à niveau.

STEP 14 | (Mise à niveau des pare-feu HA uniquement) Mettez à niveau le deuxième pair HA dans chaque paire HA.

1. Dans l'interface Web de Panorama, sélectionnez **Logiciel** > **de déploiement de** > **périphériques Panorama**.
2. Cliquez sur **Install (Installer)** dans la colonne Action correspondant aux modèles de HA que vous souhaitez mettre à niveau.
3. Dans la boîte de dialogue Déployer le fichier logiciel, sélectionnez tous les pare-feu que vous souhaitez mettre à niveau. Cette fois, sélectionnez uniquement les homologues des pare-feu HA que vous venez de mettre à jour.
4. Assurez-vous que le **Group HA Peers (Groupe de paire HA)** n'est pas sélectionné.
5. Sélectionnez **Reboot device after install (Redémarrer le périphérique après l'installation)**.
6. Pour débuter la mise à jour, cliquez sur **OK**.
7. Une fois l'installation terminée, redémarrez en utilisant l'une des méthodes suivantes :
   - Si vous êtes invité à redémarrer, cliquez sur **Yes (Oui)**.
   - Si vous n'êtes pas invité à redémarrer, sélectionnez **Device (Périphérique)** > **Configuration** > **Operations (Opérations)** et **Reboot Device (Redémarrez le périphérique)**.

STEP 15 | (HA firewall upgrades only (Mises à niveau du pare-feu HA uniquement) Restaurez la fonctionnalité HA sur l'homologue HA secondaire.

1. Log in to the firewall web interface (Connectez-vous à l'interface Web) du pare-feu de l'homologue HA du pare-feu secondaire suspendu.
2. Sélectionnez**Device (Appareil)** > **High Availability (Haute disponibilité)** > **Operational Commands (Commandes opérationnelles)** et **Make local device functional for high availability (Activez le périphérique local pour la haute disponibilité)**.
3. Dans le coin inférieur droit, vérifiez que l'état est `Passive (Passif)`. Pour les pare-feu dans une configuration active/active, vérifiez que l'état est `Active (Actif)`.
4. Attendez que la configuration de l'homologue HA en cours se synchronise.

   Dans **Dashboard (tableau de bord)**, surveillez l'état de la configuration d'exécution dans le widget Haute disponibilité.

STEP 16 | (mode FIPS-CC uniquement) Mettre à niveau Panorama et les périphériques gérés en mode FIPS-CC.

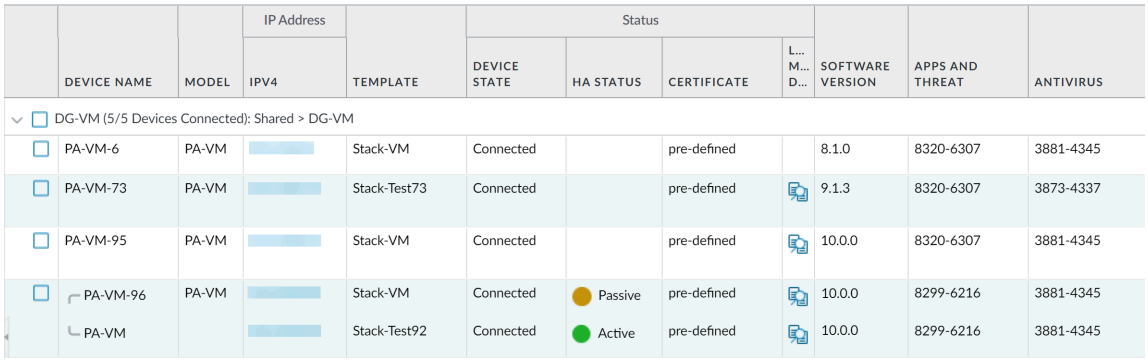
La mise à niveau d'un pare-feu géré en mode FIPS-CC nécessite que vous réinitialisiez l'état de la connexion sécurisée si vous avez ajouté le collecteur de journaux dédié à la gestion Panorama alors que le pare-feu géré exécutait une version de PAN-OS 11.0.

Vous n'avez pas besoin de réintégrer le pare-feu géré ajouté à la gestion Panorama lorsque le pare-feu géré exécutait PAN-OS 10.0 ou une version antérieure.

STEP 17 | Vérifiez la version du logiciel et du contenu qui s'exécute sur chaque pare-feu géré.

1. Sur Panorama, sélectionnez **Panorama** > **Managed Devices (Périphériques gérés)**.
2. Localisez les pare-feu et examinez les versions de contenu et logicielles dans le tableau.

   Pour les pare-feu HA, vous pouvez également vérifier que l'état HA de chaque homologue est conforme aux attentes.



	DEVICE NAME	MODEL	IP Address IPV4	TEMPLATE	Status DEVICE STATE	Status HA STATUS	Status CERTIFICATE	Status L... M... D...	SOFTWARE VERSION	APPS AND THREAT	ANTIVIRUS
	DG-VM (5/5 Devices Connected): Shared > DG-VM										
	PA-VM-6	PA-VM		Stack-VM	Connected		pre-defined		8.1.0	8320-6307	3881-4345
	PA-VM-73	PA-VM		Stack-Test73	Connected		pre-defined		9.1.3	8320-6307	3873-4337
	PA-VM-95	PA-VM		Stack-VM	Connected		pre-defined		10.0.0	8320-6307	3881-4345
	PA-VM-96	PA-VM		Stack-VM	Connected	Passive	pre-defined		10.0.0	8299-6216	3881-4345
	PA-VM			Stack-Test92	Connected	Active	pre-defined		10.0.0	8299-6216	3881-4345

STEP 18 | (Mises à niveau des pare-feu HA uniquement)Si vous avez désactivé la préemption sur l'un de vos pare-feu haute disponibilité avant de procéder à la mise à niveau, modifiez les **Election Settings (Paramètres d'élection)** (**Device (Périphérique)** > **High Availability (Haute disponibilité)**) et réactivez le paramètre **Preemptive (Préemptif)** pour ce pare-feu, puis **Commit (Validez)** le changement.

STEP 19 | Sur Panorama web interface (interface Web de Panorama), transférez l'ensemble de la configuration gérée de Panorama vers vos pare-feu gérés.

Cette étape est nécessaire pour activer la validation sélective et la diffusion des modifications de configuration des groupes de périphériques et des piles de modèles de Panorama vers vos pare-feu gérés.

Cela est nécessaire pour appliquer avec succès les modifications de configuration aux pare-feu multi-vsys gérés par Panorama après une mise à niveau réussie vers PAN-OS 11.0 à partir de PAN-OS 10.1 ou d'une version antérieure. Pour plus d'informations, consultez la modification du comportement par défaut des objets de configuration partagés pour les pare-feu multi-vsys gérés par Panorama.

1. Sélectionnez **Commit (valider)** > **Push to Devices (Appliquer aux périphériques)**.
2. **Push (Appliquer)**.

STEP 20 | Régénérez ou réimportez tous les certificats pour respecter le niveau de sécurité OpenSSL 2.

Lors de la mise à niveau vers PAN-OS 10.2 ou version ultérieure, tous les certificats doivent répondre aux exigences minimales suivantes. Ignorez cette étape si vous effectuez une mise à niveau à partir de PAN-OS 10.2 et que vous avez déjà régénéré ou réimporté vos certificats.

- RSA 2048 bits ou supérieur, ou ECDSA 256 bits ou supérieur
- Digest de SHA256 ou supérieur

Consultez le Guide de l'administrateur PAN-OS ou le Guide de l'administrateur de Panorama pour plus d'informations sur la régénération ou la réimportation de vos certificats.

STEP 21 | Affichez l'historique des mises à niveau logicielles du pare-feu.

1. Connectez-vous à l'interface Panorama.
2. Accédez à **Panorama** > **Managed Devices (appareils gérés)** > **Summary (Résumé)** et cliquez sur **Device History (Historique des appareils)**.

Mettre à niveau les pare-feu lorsque Panorama n'est pas connecté à Internet

Pour une liste des mises à jour de logiciels et de contenu que vous pouvez installer sur des pare-feu, voir Mises à jour prises en charge.

La nouvelle fonctionnalité Ignorer la mise à niveau des versions logicielles vous permet d'ignorer jusqu'à trois versions lors du déploiement de mises à niveau des appareils Panorama sur PAN-OS 11.0 vers des pare-feux sur PAN-OS 10.1 ou versions ultérieures.

STEP 1 | Avant de mettre à niveau des pare-feu gérés, assurez-vous que vous exécutez PAN-OS 11.0 sur le serveur d'administration Panorama et les collecteurs de journaux.

Palo Alto Networks® recommande vivement que Panorama et les collecteurs de journaux exécutent la même version du logiciel Panorama et que Panorama, les collecteurs de journaux et tous les pare-feu gérés exécutent la même version de contenu.

Pour les détails de compatibilité de logiciels et de contenus importants, voir Compatibilité des versions de Panorama, des collecteurs de journaux, des pare-feu et de WildFire.

Panorama doit exécuter la même version de logiciel (ou une version ultérieure) que les pare-feu, mais doit avoir la même version de contenu ou une version antérieure :

- **Version du logiciel** : si votre serveur de gestion Panorama ou les collecteurs de journaux n'exécutent pas déjà la même version de logiciel ou une version ultérieure que la version à laquelle vous souhaitez mettre à jour les pare-feu, vous devez installer la même version ou une version ultérieure sur Panorama, puis sur les collecteurs de journaux (voir Installer les mises à jour de contenu et logicielles pour Panorama) avant de mettre à jour les pare-feu.
- **Version du contenu** : pour les versions de publication de contenu, vous devez vous assurer que tous les pare-feu exécutent la dernière version de contenu ou, au minimum, qu'ils exécutent une version ultérieure de Panorama et des collecteurs de journaux ; sinon, mettez à jour les pare-feu gérés, puis mettez à niveau les collecteurs de journaux lorsque Panorama n'est pas connecté à Internet avant de mettre à jour la version du contenu sur le serveur de gestion Panorama (voir Installer les mises à jour de contenu et logicielles pour Panorama).

Pour vérifier les versions de logiciel et de contenu :

- **Serveur de gestion Panorama** : connectez-vous à l'interface Web Panorama et accédez aux paramètres General Information (Informations générales) (**Dashboard (Tableau de bord)**).
- **Collecteurs de journaux** : connectez-vous à l'ILC de chaque collecteur de journaux et exécutez la commande **`show system info`**.

STEP 2 | Effectuez une copie de sauvegarde du fichier de configuration actuel sur chaque pare-feu géré que vous envisagez de mettre à niveau.

Bien que le pare-feu crée automatiquement une sauvegarde de la configuration, il est recommandé de créer et de stocker une sauvegarde externe avant de procéder à la mise à niveau.

1. **Export Panorama and devices config bundle (Exporter la solution de configuration des périphériques et de Panorama)** (**Panorama** > **Setup (Configuration)** > **Operations (Opérations)**) pour générer et exporter la dernière la sauvegarde de configuration de Panorama et celle de chaque appareil géré.
2. Enregistrez le fichier exporté dans un emplacement externe au pare-feu. Vous pouvez utiliser cette sauvegarde pour restaurer la configuration en cas de problème pendant la mise à niveau.

STEP 3 | Déterminez les mises à jour de contenu à installer. Consultez les Notes de version pour la version de contenu minimale que vous devez installer pour une version de PAN-OS®.

Palo Alto Networks recommande fortement que Panorama, les collecteurs de journaux et tous les pare-feu gérés exécutent la même version de contenu.

Pour chaque mise à jour de contenu, déterminez si vous avez besoin de mises à jour et quelles mises à jour de contenu doivent être téléchargées à la prochaine étape.

Assurez-vous que Panorama exécute la même version de contenu, mais pas une version ultérieure à celle exécutée sur les pare-feu gérés et les collecteurs de journaux.

STEP 4 | Determine the software upgrade path (Déterminez le chemin de mise à niveau logicielle) pour les pare-feux que vous avez l'intention de mettre à jour vers Panorama 11.0.

Connectez-vous à Panorama, sélectionnez **Panorama** > **Managed Collectors (Collecteurs gérés)**, et notez la version du logiciel actuel des pare-feu que vous souhaitez mettre à niveau.

Consultez Liste de contrôle de mise à niveau de PAN-OS, *les problèmes connus et les modifications apportées au comportement par défaut dans les* Release Notes (notes de version) *et* Considérations de mise à niveau/rétrogradation *pour chaque version par laquelle vous passez dans le cadre de votre chemin de mise à niveau.*

STEP 5 | (Facultatif) Mettez à niveau vos pare-feu gérés vers PAN-OS 10.1.

La fonctionnalité de mise à niveau de version logicielle ignore prend en charge les pare-feu gérés exécutant PAN-OS 10.1 ou versions ultérieures. Si vos pare-feu gérés sont sur PAN-OS 10.0 ou une version antérieure, commencez par effectuer une mise à niveau vers PAN-OS 10.1 ou une version ultérieure.

STEP 6 | Effectuez un contrôle de validation de la version.

Dans cette étape, vous pouvez afficher les images logicielles et de contenu intermédiaires requises pour effectuer la mise à niveau vers la version 11.0.

1. Sélectionnez **Panorama** > **Device Deployment (Déploiement de périphérique)** > **Software (Logiciel)** > **Action** > **Validate (Valider)**.
2. Affichez les versions intermédiaires du logiciel et du contenu que vous devez télécharger.

STEP 7 | Téléchargez les mises à jour de contenu et logicielles sur un hôte qui peut se connecter et charger les fichiers sur Panorama ou un serveur SCP configuré via SCP ou HTTPS.

Par défaut, vous pouvez charger un maximum de deux mises à jour logicielles ou de contenu de chaque type vers un appareil Panorama. Si vous téléchargez une troisième mise à jour du même type, Panorama supprimera la mise à jour de la première version de ce type. Si vous devez télécharger plus de deux mises à jour logicielles ou mises à jour de contenu d'un seul type, utilisez la commande CLI **`set max-num-images count <number>`** pour augmenter le nombre maximum d'images que Panorama peut stocker.

1. Utilisez un hôte avec accès à Internet pour ouvrir une session sur le site Web d'assistance client de Palo Alto Networks.
2. Téléchargez les mises à jour de contenu :
   1. Cliquez **Dynamic Updates (Mises à jour dynamique)** dans la section Ressources.
   2. **Download (Téléchargez)** la dernière version de contenu (ou, au minimum, la même version ou une version ultérieure que celle que vous installerez ou exécuterez sur le serveur de gestion Panorama) et enregistrez le fichier sur l'hôte ; répétez pour chaque type de contenu que vous devez mettre à jour.
3. Télécharger les mises à jour logicielles :
   1. Retour à la page principale du site de Support Clients de Palo Alto Networks et cliquez sur **Software Updates (Mises à jour de logiciel)** dans la section Ressources.
   2. Consultez la colonne Télécharger pour déterminer les versions à installer. Le nom des packages de mise à jour indique le modèle. Par exemple, pour mettre à niveau un pare-feu PA-220 et PA-5260 vers PAN-OS 11.0.0, téléchargez les images `PanOS_200-11.0.0`, `PanOS_3000-11.0.0`, et `PanOS_5000-11.0.0`.

      *Vous pouvez rapidement localiser des images PAN-OS spécifiques en sélectionnant **PAN-OS for the PA (PAN-OS pour le PA)**-<series/model> depuis le menu déroulant **Filter By (Filtrer par)**.*
4. Cliquez sur le nom du fichier approprié et enregistrez le fichier sur l'hôte.

STEP 8 | Téléchargez les versions intermédiaires du logiciel et la dernière version du contenu.

Sur PAN-OS 11.0, vous pouvez télécharger plusieurs versions intermédiaires à l'aide de la fonctionnalité de téléchargement multi-images.

1. Sélectionnez les pare-feu que vous souhaitez mettre à niveau (**Required Deployments (Déploiements requis)** > **Deploy (Déployer)**).
2. Sélectionnez une source de téléchargement et cliquez sur **Télécharger**.

STEP 9 | Installez les mises à jour de contenu sur les pare-feu gérés.

Vous devez installer les mises à jour de contenu avant les mises à jour logicielles.

Installez d'abord les mises à jour des applications ou des applications et menaces, puis installez toutes les autres mises à jour (Antivirus, WildFire® ou Filtrage d'URL) au besoin, une à la fois et dans n'importe quel ordre.

1. Sélectionnez **Panorama (Panorama)** > **Device Deployment (Déploiement du périphérique)** > **Dynamic Updates (Mises à jour dynamiques)**.
2. Cliquez sur **Upload (Charger)**, sélectionnez le **Type** de mise à jour, **Browse (Rechercher)** le fichier de mise à jour de contenu approprié, puis cliquez sur **OK**.
3. Cliquez sur **Install From File (Installer depuis le fichier)**, sélectionnez le **Type** de mise à jour et sélectionnez le **File Name (Nom du fichier)** de la mise à jour de contenu que vous venez de charger.
4. Sélectionnez les collecteurs de journaux sur lesquels installer la mise à jour.
5. Cliquez sur **OK** pour démarrer l'installation.
6. Répétez ces étapes pour chaque mise à jour de contenu.

STEP 10 | (Pare-feu servant de portails GlobalProtect™ uniquement) Chargez et activez une mise à jour du logiciel de l'agent / application GlobalProtect sur les pare-feu.

Vous activez la mise à jour sur les pare-feu, afin que les utilisateurs puissent les télécharger sur leurs points de terminaison (systèmes client).

1. Utilisez un hôte avec accès à Internet pour ouvrir une session sur le site Web d'assistance client de Palo Alto Networks.
2. Téléchargez la mise à jour du logiciel de l'agent / application GlobalProtect appropriée.
3. Sur Panorama, sélectionnez **Panorama** > **Device Deployment (Déploiement de périphériques)** > **GlobalProtect Client (Client GlobalProtect)**.
4. Cliquez sur **Upload (Charger)**, **Browse (Rechercher)** la mise à jour du logiciel de l'agent / application GlobalProtect appropriée sur l'hôte pour lequel vous avez téléchargé le fichier, puis cliquez sur **OK**.
5. Cliquez sur **Activate from File (Activer depuis le fichier)** et sélectionnez le **File Name (Nom du fichier)** de la mise à jour de l'agent / application GlobalProtect que vous venez de charger.

   Vous ne pouvez activer qu'une seule version du logiciel de l'agent / application à la fois. Si vous activez une nouvelle version mais que certains agents nécessitent une version antérieure, vous devrez réactiver à nouveau la version antérieure pour que ces agents téléchargent la mise à jour précédente.
6. Sélectionnez les pare-feu sur lesquels installer la mise à jour.
7. Cliquez sur **OK** pour l'activer.

STEP 11 | Installez PAN-OS 11.0.

Pour éviter les pannes lors de mise à jour du logiciel sur le pare-feu haute disponibilité (HD), mettez à jour un homologue HD à la fois.

Pour les pare-feu actifs / actifs, l'homologue que vous mettez à jour en premier n'a pas d'importance.

Pour les pare-feu actifs / passifs, vous devez d'abord mettre à jour l'homologue passif, suspendre l'homologue actif (basculement), mettre à jour l'homologue actif, puis ramener l'homologue actif à un état fonctionnel (retour arrière).

*(SD-WAN only (SD-WAN uniquement)) Pour conserver un état précis de vos liaisons SD-WAN, vous devez mettre à niveau vos pare-feu de concentrateur vers PAN-OS 11.0 avant de mettre à niveau vos pare-feu de succursale. La mise à jour des pare-feux de branche avant les pare-feux de plate-forme peut entraîner une mauvaise surveillance des données (**Panorama** > **SD-WAN** > **Monitoring (Surveillance)**) et les liens SD-WAN peuvent être affichés comme étant `down (en panne)` de façon erronée.*

1. Effectuez les étapes qui s'appliquent à la configuration de votre pare-feu pour installer la mise à jour logicielle de PAN-OS que vous venez de charger.
   - **Pare-feu non-HD** : cliquez sur **Install (Installer)** dans la colonne Action, sélectionnez tous les pare-feu que vous mettez à niveau, sélectionnez **Reboot device after install (Redémarrer le périphérique après l'installation)**, puis cliquez sur **OK**.
   - **Pare-feu HD actifs / actifs :**
     1. Confirmez que le paramètre de préemption est désactivé sur le premier homologue que vous avez l'intention de mettre à niveau (**Device (Périphérique)** > **High Availability (Haute Disponibilité)** > Election Settings (Paramètres d'élection)). Si activés, modifiez les **Election Settings (Paramètres d'élection)** et désactivez le paramètre **Preemptive (Préemptif)**, puis **Commit (Validez)** votre modification. Vous devez uniquement désactiver ce paramètre sur un pare-feu dans chaque paire haute disponibilité, mais assurez-vous que la validation est réussie avant de continuer.
     2. Cliquez sur **Install (Installer)**, désactivez **Group HA Peers (Regrouper les homologues HD)**, sélectionnez un homologue HD, sélectionnez **Reboot device after install (Redémarrer le périphérique après l'installation)**, puis cliquez sur **OK**. Attendez que le pare-feu termine le redémarrage avant de poursuivre.
     3. Cliquez sur **Install (Installer)**,désactivez **Group HA Peers (Regrouper les homologues HD)**, sélectionnez l'homologue HD que vous n'avez pas mis à jour à l'étape précédente, sélectionnez **Reboot device after install (Redémarrer le périphérique après l'installation)**, puis cliquez sur **OK**.
   - **Pare-feu HA actifs/passifs**: dans cet exemple, le pare-feu actif est nommé fw1 et le pare-feu passif est nommé fw2 :
     1. Vérifiez que le paramètre de préemption est désactivé sur le premier homologue que vous souhaitez mettre à niveau (**Device (Appareil)** > **High Availability (Haute disponibilité)** > Election Settings (Paramètres de choix). Si activés, modifiez les **Election Settings**

(Paramètres d'élection) et désactivez le paramètre **Preemptive (Préemptif)**, puis **Commit (Validez)** votre modification. Vous devez uniquement désactiver ce paramètre sur un pare-feu dans chaque paire haute disponibilité, mais assurez-vous que la validation est réussie avant de continuer.

2. Cliquez sur **Install (Installer)** dans la colonne Action pour la mise à jour appropriée, désactivez (effacez) **Group HA Peers (Regrouper les homologues HA)**, select fw2, **Reboot device after install (Redémarrer le périphérique après installation)**, et cliquez sur **OK**. Attendez que fw2 termine le redémarrage avant de poursuivre.
3. Après le redémarrage de fw2, vérifiez sur fw1 (**Dashboard (Tableau de bord)** > High Availability (Haute disponibilité)) que fw2 est toujours l'homologue passif (l'état du pare-feu local est `active (actif)` et l'homologue fw2 est `passive (passif)`).
4. Accédez à fw1 et **Suspend local device (Suspendre le périphérique local)** (**Device (Périphérique)** > **High Availability (Haute disponibilité)** > **Operational Commands (Commandes opérationnelles)**).
5. Accédez à fw2 (**Dashboard (Tableau de bord)** > High Availability (Haute disponibilité)) et vérifiez que l'état du pare-feu local est `active (actif)` et que l'homologue est `suspended (suspendu)`.
6. Accédez à Panorama, sélectionnez **Panorama** > **Device Deployment (Déploiement de périphériques)** > **Software (Logiciel)**, cliquez sur **Install (Installer)** dans la colonne Action de la version appropriée, désactivez

   Group HA Peers (Regrouper les homologues HD)**, sélectionnez fw1, Reboot device after install (Redémarrer le périphérique après l'installation), puis cliquez sur OK. Attendez que fw1 termine le redémarrage avant de poursuivre.**
7. Accédez à fw1 (**Device (Périphérique)** > **High Availability (haute disponibilité)** > **Operational Commands (Commandes opérationnelles)**), cliquez sur **Make local device functional (Rendre l'appareil local fonctionnel)**, et attendez deux minutes avant de continuer.
8. Sur fw1 (**Dashboard (Tableau de bord)** > High Availability (Haute disponibilité)), vérifiez que l'état du pare-feu local est `passive (passif)` et que l'homologue (fw2) est `active (actif)`.

STEP 12 | (mode FIPS-CC uniquement) Mettre à niveau Panorama et les périphériques gérés en mode FIPS-CC.

La mise à niveau d'un pare-feu géré en mode FIPS-CC nécessite que vous réinitialisiez l'état de la connexion sécurisée si vous avez ajouté le collecteur de journaux dédié à la gestion Panorama alors que le pare-feu géré exécutait une version de PAN-OS 11.0.

Vous n'avez pas besoin de réintégrer le pare-feu géré ajouté à la gestion Panorama lorsque le pare-feu géré exécutait PAN-OS 10.0 ou une version antérieure.

STEP 13 | Vérifiez que le logiciel et/ou les versions de mise à jour de contenu sont installés sur chaque pare-feu géré.

1. Sélectionnez **Panorama** > **Managed Devices (Périphériques gérés)**.
2. Localisez le pare-feu et examinez les valeurs dans les colonnes de la Version du logiciel, applications et menace, Antivirus, filtrage d'URL et Client GlobalProtect.

STEP 14 | Si vous avez désactivé la préemption sur l'un de vos pare-feu HD avant de procéder à la mise à niveau, modifiez les **Election Settings (Paramètres d'élection)** (**Device (Périphérique)** > **High Availability (Haute disponibilité)**) et réactivez le paramètre **Préemptif** pour ce pare-feu.

STEP 15 | Sur Panorama web interface (interface Web de Panorama), transférez l'ensemble de la configuration gérée de Panorama vers vos pare-feu gérés.

Cette étape est nécessaire pour activer la validation sélective et la diffusion des modifications de configuration des groupes de périphériques et des piles de modèles de Panorama vers vos pare-feu gérés.

Cela est nécessaire pour appliquer avec succès les modifications de configuration aux pare-feu multi-vsys gérés par Panorama après une mise à niveau réussie vers PAN-OS 11.0. Pour plus d'informations, consultez la modification du comportement par défaut des objets de configuration partagés pour les pare-feu multi-vsys gérés par Panorama.

1. Sélectionnez **Commit (valider)** > **Push to Devices (Appliquer aux périphériques)**.
2. **Push (Appliquer)**.

STEP 16 | Régénérez ou réimportez tous les certificats pour respecter le niveau de sécurité OpenSSL 2.

Lors de la mise à niveau vers PAN-OS 11.0, tous les certificats doivent répondre aux exigences minimales suivantes :

- RSA 2048 bits ou supérieur, ou ECDSA 256 bits ou supérieur
- Digest de SHA256 ou supérieur

Consultez le Guide de l'administrateur PAN-OS ou le Guide de l'administrateur de Panorama pour plus d'informations sur la régénération ou la réimportation de vos certificats.

STEP 17 | Affichez l'historique des mises à niveau logicielles du pare-feu.

1. Connectez-vous à l'interface Panorama.
2. Accédez à **Panorama** > **Managed Devices (appareils gérés)** > **Summary (Résumé)** et cliquez sur **Device History (Historique des appareils)**.

Mettre à niveau un pare-feu ZTP

Après avoir ajouté avec succès un pare-feu ZTP au serveur de gestion Panorama™, configurez la version PAN-OS cible du pare-feu ZTP. Panorama vérifie si la version du PAN-OS installée sur le pare-feu ZTP est postérieure ou égale à la version du PAN-OS cible configurée après sa première connexion réussie à Panorama. Si la version PAN-OS installée sur le pare-feu ZTP est antérieure à la version PAN-OS cible, alors le pare-feu ZTP entre dans un cycle de mise à jour jusqu'à ce que la version PAN-OS cible soit installée.

STEP 1 | Log in to the Panorama Web Interface (Connectez-vous à l'interface Web Panorama) en tant qu'administrateur.

STEP 2 | Add a ZTP Firewall to Panorama (Ajouter un pare-feu ZTP à Panorama).

STEP 3 | Sélectionnez **Panorama** > **Device Deployment (Déploiement de périphériques)** > **Updates (Mises à jour)** et **Check Now (Vérifiez maintenant)** pour obtenir les dernières mises à jour PAN-OS.

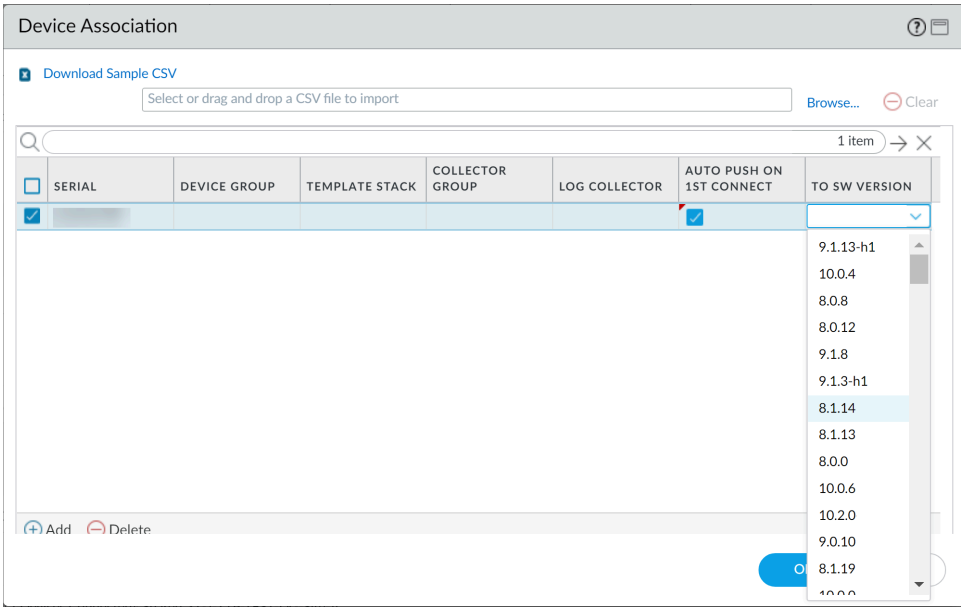
STEP 4 | Sélectionnez **Panorama** > **Managed Devices (Appareils gérés)** > **Summary (Résumé)** et sélectionnez un ou plusieurs pare-feux ZTP.

STEP 5 | **Réassocier** le(s) pare-feu(x) ZTP sélectionné(s).

STEP 6 | Cochez (activez) **Auto Push on 1st Connect (application automatique lors de la 1ère connexion)**.

STEP 7 | Dans la colonne **To SW Version (Vers la version SW)**, sélectionnez la version PAN-OS cible pour le pare-feu ZTP.

STEP 8 | Cliquez sur **OK** pour enregistrer votre configuration.



STEP 9 | Sélectionnez **Commit (Valider)** et **Commit to Panorama (Validez sur Panorama)**.

STEP 10 | Mettez le pare-feu ZTP sous tension.

Lorsque le pare-feu ZTP se connecte à Panorama pour la première fois, il passe automatiquement à la version PAN-OS que vous avez sélectionnée.

- **Panorama running PAN-OS 11.0.0 (Panorama exécutant PAN-OS 11.0.0)** — Si vous mettez à niveau des pare-feu gérés sur des versions majeures ou de maintenance de PAN-OS, les versions intermédiaires de PAN-OS sur votre chemin de mise à niveau sont installées en premier avant que la version cible de PAN-OS ne soit installée.

  Par exemple, vous avez configuré la cible **Version SW** pour le pare-feu géré en tant que PAN-OS 11.0.0 et le pare-feu exécute PAN-OS 10.1. Lors de la première connexion à Panorama, PAN-OS 10.2.0 est installé sur le pare-feu géré en premier. Après l'installation réussie de PAN-OS 10.2.0, le pare-feu est automatiquement mis à niveau vers la version PAN-OS 11.0.0 cible.
- **Panorama running PAN-OS 11.0.1 and later releases (Panorama exécutant PAN-OS 11.0.1 et versions ultérieures)** – Si vous mettez à niveau des pare-feux gérés à travers les versions majeures ou de maintenance PAN-OS, les versions majeures PAN-OS intermédiaires sur votre chemin de

mise à niveau sont installées et la version majeure PAN-OS de base est téléchargée avant que la version de maintenance PAN-OS cible ne soit installée.

Par exemple, vous avez configuré la cible **Version SW** pour le pare-feu géré en tant que PAN-OS 11.0.1 et le pare-feu exécute PAN-OS 10.0. Lors de la première connexion à Panorama, PAN-OS 10.1.0 et PAN-OS 10.2.0 sont installés sur le pare-feu géré. Après le redémarrage du pare-feu géré, PAN-OS 11.0.0 est téléchargé, puis le pare-feu s'installe automatiquement sur la version PAN-OS 11.0.1 cible.

STEP 11 | Vérifiez la mise à jour du logiciel de pare-feu ZTP.

1. Connectez-vous à l'interface Web Panorama.
2. Sélectionnez **Panorama** > **Managed Devices (Appareils gérés)** > **Summary (Résumé)** et naviguez vers le(s) pare-feu(x) ZTP.
3. Vérifiez que la colonne **Software Version (Version du logiciel)** affiche la bonne version PAN-OS cible.

STEP 12 | Pour toutes les futures mises à niveau de PAN-OS, voir Mettre à niveau le pare-feu vers PAN-OS 11.0 à partir de Panorama.

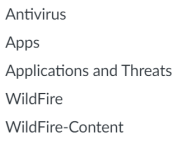
Rétablir les mises à jour du contenu depuis Panorama

Panorama ™ vous permet de rétablir rapidement les versions des Applications, Applications et Menaces, Antivirus, WildFire® et WildFire sur un ou plusieurs pare-feu, Collecteurs de journaux ou Applications WildFire directement à partir de Panorama. Utilisez Panorama pour rétablir les versions de contenu installées sur les périphériques gérés afin de tirer parti d'un flux de travail centralisé qui permet d'atténuer tout risque associé à l'introduction ou à la modification d'applications ou de nouvelles signatures de menaces dans une mise à jour de contenu. Panorama génère un journal système pour chaque périphérique lorsque vous inversez le contenu. Assurez-vous que vous utilisez Meilleures pratiques pour les mises à jour du contenu de menace et des applications lorsque vous déployez des mises à jour de contenu sur vos appareils gérés.

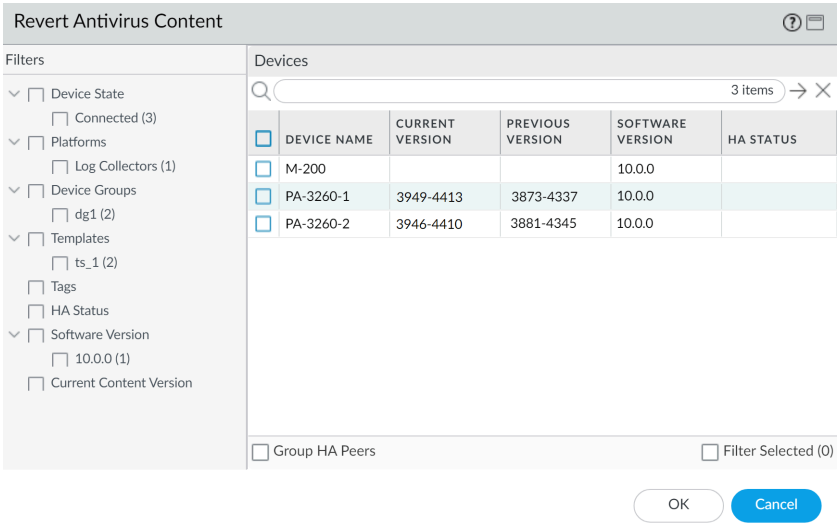
STEP 1 | Connectez-vous à l’interface Web Panorama.

STEP 2 | Sélectionnez **Panorama (Panorama)** > **Device Deployment (Déploiement de périphériques)** > **Dynamic Updates (Mises à jour dynamiques)** et **Revert Content (Rétablir le contenu)**.

STEP 3 | Sélectionnez le contenu que vous souhaitez rétablir.



STEP 4 | Sélectionnz un ou plusieurs pare-feu que vous souhaitez rétablir et cliquez sur **OK**. La version de contenu que vous rétablissez doit être antérieure à celle qui est actuellement installée sur l'appareil.



Mise à niveau de PAN-OS

Liste de contrôle de mise à niveau de PAN-OS

La planification de votre mise à niveau PAN-OS peut aider à assurer une transition plus fluide vers une version plus récente de PAN-OS pour votre Panorama ou vos pare-feux.

- Assurez-vous que l'appareil est enregistré et sous licence.
- Vérifiez l'espace disque disponible.

  L'espace disque requis varie en fonction de la version PAN-OS. Sélectionnez **Device (Périphérique)** > **Software (Logiciel)** et examinez la **Size (taille)** de la version PAN-OS cible pour déterminer l'espace disque requis.

  - Lancez **`show system disk-space (afficher l’espace disque du système)`**
- Vérifiez la version minimale du contenu.
- Identifiez la version préférée.

  Pour plus d’informations,reportez-vous au Palo Alto Networks Support Software Release Guidance (Guide de publication du logiciel de support de Palo Alto Networks) et au End-of-Life Summary (Résumé de fin de vie). De plus, passez en revue les problèmes connus et résolus, les considérations de mise à niveau et de rétrogradation et les limitations de votre version PAN-OS cible pour comprendre comment une mise à niveau PAN-OS peut vous affecter.
- Déterminez le chemin de mise à niveau.

  Lorsque vous effectuez une mise à niveau d’une version de fonctionnalité PAN-OS vers une version ultérieure, vous ne pouvez pas ignorer l’installation des versions de fonctionnalité dans le chemin d’accès à votre version cible.
- Passez en revue les considérations de mise à niveau/rétrogradation pour toutes les versions de votre chemin de mise à niveau.
- (Required for GlobalProtect (Requis pour GlobalProtect)) Vérifiez la version minimale de l'agent GlobalProtect™ pour empêcher les utilisateurs de GlobalProtect de perdre la connectivité VPN. GlobalProtect peut être mis à niveau directement vers la dernière version.
- Vérifiez les versions minimales de version de plug-in sur la version de version cible pour tous les plug-ins que vous avez installés.
- Vérifiez la connectivité de l'interface de gestion au serveur de mise à jour.

  - Sélectionnez **Device (Périphérique)** > **Troubleshooting (résolution des pannes)** et testez la **Update Server Connectivity (connectivité du serveur de mise à jour)** pour vérifier que le DNS peut résoudre l'adresse.

    Si cela ne se résout pas, changez le DNS en **`8.8.8.8`** (vous devez utiliser un serveur DNS public plutôt que votre propre serveur DNS) et ping à nouveau.

    Si cela ne résout pas, remplacez le serveur de mise à jour par **`staticupdates.paloaltonetworks.com`** et **Commit (validez)**.
- (SD-WAN only (SD-WAN uniquement)) Identifiez les pare-feux de hub et de succursale que vous avez l'intention de mettre à niveau vers PAN-OS 10.2.

  Pour conserver un état précis de vos liaisons SD-WAN, vous devez mettre à niveau vos pare-feu de concentrateur vers PAN-OS 11.0 avant de mettre à niveau vos pare-feu de succursale. La mise à jour

des pare-feux de branche avant les pare-feux de plate-forme peut entraîner une mauvaise surveillance des données (**Panorama** > **SD-WAN** > **Monitoring (surveillance)**) et les liens SD-WAN peuvent être affichés comme étant `down (en panne)` de façon erronée.

- Si des plug-ins sont actuellement installés, téléchargez la version du plug-in prise en charge sur PAN-OS 11.0 pour tous les plug-ins actuellement installés sur Panorama (**Panorama** > **Plugins**) ou votre pare-feu (**Device (périphérique)** > **Plugins**)avant la mise à niveau.

  Consultez Panorama Plugins Compatibility Matrix(matrice de compatibilité des plug-ins Panorama) pour connaître la version du plug-in Panorama prise en charge sur PAN-OS 10.2.

  Cela est nécessaire pour réussir la mise à niveau de Panorama et du pare-feu de PAN-OS 11.0 vers PAN-OS 10.2. La version téléchargée du plugin est automatiquement installée lors de la mise à niveau vers PAN-OS 10.2. La mise à niveau vers PAN-OS 11.0 est bloquée si la version du plug-in prise en charge n’est pas téléchargée.

Considérations de mise à niveau/rétrogradation

Le tableau suivant répertorie les nouvelles fonctionnalités qui ont un impact sur la mise à niveau ou la rétrogradation. Assurez-vous de bien comprendre toutes les considérations relatives à la mise à niveau/rétrogradation avant de procéder à la mise à niveau ou rétrogradation vers une version PAN-OS 11.0. Pour plus d'informations sur les versions PAN-OS 11.0, reportez-vous aux PAN-OS 11.0 Release Notes (notes de version PAN-OS 10.1).

Fonctionnalité	Considérations relatives à la mise à niveau	Considérations de rétrogradation
Plugin Cloud Services	La mise à niveau vers PAN-OS 11.0 avec la dernière version Cloud Services n'est pas prise en charge. La mise à niveau vers PAN-OS 11.0 avec une version non prise en charge du plugin Cloud Services peut entraîner des problèmes inconnus ou inattendus qui peuvent affecter à la fois Prisma Access et les fonctionnalités du plugin dépendant.	Aucun.
Configuration minimale requise pour l’appareil virtuel Panorama	Palo Alto Networks a augmenté la Panorama virtual appliance memory requirement (mémoire virtuelle Panorama recommandée) à un minimum de 64 Go, contre 32 Go auparavant. Cela impacte les Panorama virtual appliances (appareils virtuels Panorama) en mode Panorama et Log Collector pour éviter tout problème de journalisation, de gestion et de performance opérationnelle lié à un appareil virtuel Panorama sous-approvisionné. Pour les nouveaux déploiements d'appareils virtuels Panorama, Palo Alto Networks recommande de déployer la machine virtuelle avec un minimum de 64 Go. Pour les déploiements d'appareils	Aucun.

Fonctionnalité	Considérations relatives à la mise à niveau	Considérations de rétrogradation
	virtuels Panroama existants, voir Increase the CPUs and Memory of the Panorama Virtual Appliance (Augmenter les processeurs et la mémoire de l'appareil virtuel panorama) pour augmenter la mémoire d'un appareil virtuel Panorama existante après une mise à niveau réussie vers PAN-OS 11.0.	
TLSv1.3 Prise en charge de l'accès administratif	Le pare-feu définit automatiquement **Management TLS Mode (Gestion en mode TLS)** à **excludetlsv1.3_only** et **Certificate (Certificat)** à **none (aucun)** lorsque vous mettez à niveau le pare-feu. Si vous avez utilisé un profil de service SSL/TLS pour sécuriser les connexions de gestion avant la mise à niveau, le profil continue de fonctionner. Pour activer la prise en charge de TLSv1.3 pour l'accès administratif, vous devrez vous rendre dans Paramètres généraux (**Device (appareil)** > **Setup (Configuration)** > **Management (Gestion)** > **General Settings (Paramètres généraux)**), définir**Management TLS Mode (Gestion en mode TLS)** sur **tlsv1.3_only** ou **mixed-mode (mode mixte)**puis sélectionner un certificat de serveur de gestion.	La prise en charge de TLSv1.3 disparaît lorsque vous passez de PAN-OS 11.0 à une version antérieure de PAN-OS. Si vous aviez activé la prise en charge de TLSv1.3 ou n'utilisiez pas de profil de service SSL/TLS pour les connexions de gestion, le pare-feu prend en charge toutes les versions de TLS à l'exception de TLSv1.3 (TLSv1.0-TLSv1.2) et des suites de chiffrement associées. Toutefois, si vous avez utilisé un profil de service SSL/TLS avant de rétrograder, le pare-feu continue d'utiliser ce profil.

Fonctionnalité	Considérations relatives à la mise à niveau	Considérations de rétrogradation
	La configuration du support TLSv1.3 désactive le profil de service SSL/TLS utilisé pour les connexions de gestion avant la mise à niveau.	
Format Syslog personnalisé	Aucun.	Vous devez réduire le format syslog personnalisé (**Device (Appareil)** > **Server Profiles (Profils de serveur)** > **Syslog** et **Panorama** > **Server Profiles (Profils de serveur)** > **Syslog**) à un maximum de 2 346 caractères pour réussir la rétrogradation vers PAN-OS 10.2.
Contexte utilisateur pour le moteur d'identité sur le cloud	Palo Alto Networks recommande fortement de créer des enregistrements détaillés de l'architecture de mappage et de redistribution des tags avant d'activer User Context Cloud Service. Si une rétrogradation devient nécessaire, utilisez les enregistrements d'architecture pour recréer cette configuration après la rétrogradation afin de repeupler les mappages et les balises.	Après le passage de PANOS 11.0 à une version antérieure, l'option Service Cloud Contexte utilisateur n'est plus disponible. En outre, la rétrogradation efface les mappages d'adresse IP à nom d'utilisateur, les mappages d'adresse IP à numéro de port, les listes de quarantaine, les mappages d'adresse IP à balise et les étiquettes de groupe d'utilisateurs dynamiques de l'appareil rétrogradé. Avant la rétrogradation, si vous avez activé l'option Service Cloud Contexte utilisateur, activez la configuration précédente pour les sources des mappages, des balises et des listes de quarantaine sur le pare-feu ou Panorama afin que les informations se remplissent correctement après la rétrogradation.

Fonctionnalité	Considérations relatives à la mise à niveau	Considérations de rétrogradation
		Palo Alto Networks recommande d'utiliser les commandes CLI suivantes sur le pare-feu immédiatement avant la rétrogradation pour établir un enregistrement de référence des données. Si une rétrogradation est nécessaire, cela vous permet de comparer les données avant et après rétrogradation pour vérifier que toutes les données nécessaires sont disponibles sur le pare-feu post-rétrogradation: • Utilisez la commande `show user ip-user-mapping all` pour obtenir le nombre actuel de mappages d'adresse IP à nom d'utilisateur. • Utilisez la commande `show user ip-port-user-mapping all` pour obtenir le nombre actuel de mappages d'adresse IP à numéro de port. • Utilisez la commande `show object registered-ip all option count` pour obtenir le nombre actuel de mappages adresse IP-étiquette. • Utilisez la commande `show object registered-user all` pour obtenir le nombre actuel de mappages tag-to-username. • Utilisez la commande `debug user-id dump hip-profile-database` pour obtenir une liste de tous les périphériques associés à un profil HIP.

Fonctionnalité	Considérations relatives à la mise à niveau	Considérations de rétrogradation
		• Exporter la liste des appareils en quarantaine au format PDF ou CSV. À l'aide des commandes CLI, comparez la sortie avant et après la rétrogradation pour vérifier que la quantité de données est approximativement la même et assurez-vous que les données nécessaires sont disponibles sur le pare-feu avant d'utiliser le pare-feu pour appliquer la politique. Vous devez restaurer manuellement tous les mappages à partir de sources d'API XML et tous les périphériques qui ont été ajoutés manuellement à une liste de quarantaine. Si les mappages et les tags importés à l'aide de l'API XML et/ou des machines qui ont été ajoutées manuellement à la liste de quarantaine ne sont pas importés de nouveau et validés post downgrade, cela peut introduire un risque de sécurité, car les utilisateurs et périphériques précédemment mis en quarantaine peuvent ne plus être limités à l'accès aux ressources auxquelles ils ne sont pas autorisés à accéder. Par exemple, si une balise spécifique a été attribuée à un utilisateur via l'API XML qui l'a ajouté à un groupe d'utilisateurs dynamiques pour la quarantaine, cet utilisateur n'est plus dans le groupe d'utilisateurs dynamiques en quarantaine jusqu'à ce que vous l'ajoutiez manuellement après la rétrogradation. Si vous avez

Fonctionnalité	Considérations relatives à la mise à niveau	Considérations de rétrogradation
		ajouté un appareil manuellement à la liste de quarantaine avant la rétrogradation, vous devez ajouter cet appareil manuellement après la rétrogradation, sinon l'appareil ne sera plus mis en quarantaine, ce qui risque d'entraîner un risque de sécurité.
Cartographie utilisateur à l'aide de NetBIOS Client Probing	Dans le cadre de nos efforts continus visant à renforcer encore la sécurité de l'identifiant utilisateur et à éliminer toute faille de sécurité potentielle due à une mauvaise configuration, la méthode obsolète NetBIOS client probing de mappage utilisateur n'est plus prise en charge dans cette version. Si vous utilisez actuellement cette méthode pour collecter des mappages d'utilisateurs, vous devez configurer une autre méthode avant la mise à niveau pour vous assurer que l'identification de l'utilisateur continue sans interruption. Pour plus d'informations sur les autres méthodes de cartographie, reportez-vous à la PAN-OS documentation (documentation PAN-OS). Après la mise à niveau, NetBIOS Client Probing (**Device (Appareil)** > **User Identification (Identification de l’utilisateur)** > **User Mapping (Mappage de l’utilisateur)** > **Palo Alto Networks User-ID Agent Setup (Configuration ID utilisateur de l’agent Palo Alto Networks)** > **Client Probing (Test de client)**) n'est plus disponible. NetBIOS Client Probing n'est également plus	Aucun.

Fonctionnalité	Considérations relatives à la mise à niveau	Considérations de rétrogradation
	disponible dans la version 11.0 de l'agent Windows User-ID.	
OCSP sur proxy HTTP	Aucun.	Si vous passez à une version PAN-OS antérieure à PAN-OS 11.0, vous devrez utiliser la méthode CRL (Certificate Revocation List) pour confirmer l'état des certificats. Le trafic OCSP ne peut pas transiter par des proxys HTTP dans les versions PAN-OS antérieures à PAN-OS 11.0.

Mettre à niveau le pare-feu vers PAN-OS 11.0

La façon dont vous effectuez la mise à niveau vers PAN-OS 11.0 dépend si vous disposez de pare-feux autonomes ou de pare-feux dans une configuration à haute disponibilité (HA) et, pour l'un ou l'autre scénario, si vous utilisez Panorama pour gérer vos pare-feux. Consultez les PAN-OS 11.0 Release Notes (notes de publication de PAN-OS 10.1), puis suivez la procédure spécifique à votre déploiement :

- Déterminer le chemin de mise à niveau vers PAN-OS 11.0.
- Mettre à niveau le pare-feu vers PAN-OS 11.0 à partir de Panorama
- Mettre à niveau un pare-feu autonome
- Mettre à niveau une paire de pare-feux haute disponibilité

Lors de la mise à niveau des pare-feux que vous gérez avec Panorama ou des pare-feux configurés pour transférer du contenu vers un périphérique WildFire, vous devez d'abord upgrade Panorama (mettre à niveau Panorama) *et ses* Log Collectors (collecteurs de journaux)*, puis* upgrade the WildFire appliance (mettre à niveau le périphérique WildFire) *avant de mettre à niveau les pare-feux.*

De plus, il n'est pas recommandé de gérer des pare-feux utilisant une version plus récente que Panorama puisque cela peut faire en sorte que certaines fonctionnalités ne fonctionnent pas comme prévu. Par exemple, il n'est pas recommandé de gérer des pare-feux utilisant PAN-OS 10.1.1 ou une version ultérieure si Panorama utilise PAN-OS 10.1.0.

Déterminer le chemin de mise à niveau vers PAN-OS 11.0.

Lorsque vous effectuez une mise à niveau d'une version de fonctionnalité PAN-OS vers une version ultérieure, vous ne pouvez pas ignorer l'installation des versions de fonctionnalité dans le chemin d'accès à votre version cible. En outre, le chemin de mise à niveau recommandé inclut l'installation de la dernière version de maintenance dans chaque version avant de télécharger l'image de base pour la version suivante de la version de fonctionnalité. Pour réduire les temps d'arrêt pour vos utilisateurs, effectuez des mises à niveau en dehors des heures de travail.

Pour les mises à niveau manuelles, Palo Alto Networks recommande d'installer et de mettre à niveau à partir de la dernière version de maintenance pour chaque version de PAN-OS le long de votre chemin de mise à niveau. N'installez pas l'image de base PAN-OS pour une version de fonctionnalité, sauf s'il s'agit de la version cible vers laquelle vous souhaitez effectuer la mise à niveau.

Déterminez le chemin de mise à niveau comme suit :

STEP 1 | Identifiez la version actuellement installée.

- Dans Panorama, sélectionnez **Panorama** > **Managed Devices (Périphériques gérés)** et vérifiez la version du logiciel sur les pare-feu que vous prévoyez de mettre à niveau.
- Dans le pare-feu, sélectionnez **Device (Périphérique)** > **Software (logiciel)** et vérifiez quelle version a une coche dans la colonne Actuellement installé.

STEP 2 | Identifiez le chemin de mise à niveau :

Consultez, les problèmes connus et les modifications apportées au comportement par défaut dans les Release Notes (notes de version) et Considérations de mise à niveau/rétrogradation *pour chaque version par laquelle vous passez dans le cadre de votre chemin de mise à niveau.*

Version PAN-OS installée	Chemin de mise à niveau recommandé vers PAN-OS 11.0
10.2.x	• Si vous exécutez déjà une version de PAN-OS 10.2, vous pouvez effectuer une mise à niveau directement vers PAN-OS 11.0
10.1.x	Vous pouvez désormais utiliser la fonctionnalité Ignorer la mise à niveau de la version logicielle pour ignorer les versions logicielles lors de la mise à niveau de votre appareil à partir de PAN-OS 10.1 ou versions ultérieures. • Si vous exécutez déjà une version de PAN-OS 10.1, vous pouvez effectuer une mise à niveau directement vers PAN-OS 11.0.
10.0.x	• Téléchargez et installez la dernière version de maintenance PAN-OS 10.0 preferred (préférée) et redémarrez. • Télécharger PAN-OS 10.1.0 • Téléchargez et installez la dernière version de maintenance preferred (préférée) de PAN-OS 10.1 et redémarrez. • Télécharger PAN-OS 10.2.0 • Téléchargez et installez la dernière version de maintenance preferred (préférée) de PAN-OS 10.2 et redémarrez. • Passez à Mettre à niveau le pare-feu vers PAN-OS 11.0.
9.1.x	• Téléchargez et installez la dernière version de maintenance preferred (préférée) de PAN-OS 9.1 et redémarrez. • Télécharger PAN-OS 10.0.0. • Téléchargez et installez la dernière version de maintenance PAN-OS 10.0 preferred (préférée) et redémarrez. • Télécharger PAN-OS 10.1.0

Version PAN-OS installée	Chemin de mise à niveau recommandé vers PAN-OS 11.0
	• Téléchargez et installez la dernière version de maintenance preferred (préférée) de PAN-OS 10.1 et redémarrez. • Télécharger PAN-OS 10.2.0 • Téléchargez et installez la dernière version de maintenance preferred (préférée) de PAN-OS 10.2 et redémarrez. • Passez à Mettre à niveau le pare-feu vers PAN-OS 11.0.
9.0.x	• Téléchargez et installez la dernière version de maintenance preferred (préférée) de PAN-OS 9.0 et redémarrez.  *Passez en revue les* upgrade/downgrade considerations (considérations relatives à la mise à niveau/rétrogradation) *avant de mettre à niveau les collecteurs de journaux vers la dernière version de maintenance de PAN-OS 9.0.* • Télécharger PAN-OS 9.1.0. • Téléchargez et installez la dernière version de maintenance preferred (préférée) de PAN-OS 9.1 et redémarrez. • Télécharger PAN-OS 10.0.0. • Téléchargez et installez la dernière version de maintenance PAN-OS 10.0 preferred (préférée) et redémarrez. • Télécharger PAN-OS 10.1.0 • Téléchargez et installez la dernière version de maintenance preferred (préférée) de PAN-OS 10.1 et redémarrez. • Télécharger PAN-OS 10.2.0 • Téléchargez et installez la dernière version de maintenance preferred (préférée) de PAN-OS 10.2 et redémarrez. • Passez à Mettre à niveau le pare-feu vers PAN-OS 11.0.

Version PAN-OS installée	Chemin de mise à niveau recommandé vers PAN-OS 11.0
8.1.x	• Téléchargez et installez la dernière version de maintenance PAN-OS 8.1 preferred (préférée) et redémarrez. • Télécharger PAN-OS 9.0.0 • Téléchargez et installez la dernière version de maintenance preferred (préférée) de PAN-OS 9.0 et redémarrez. *Passez en revue les* upgrade/downgrade considerations (considérations relatives à la mise à niveau/rétrogradation) *avant de mettre à niveau les collecteurs de journaux vers la dernière version de maintenance de PAN-OS 9.0.* • Télécharger PAN-OS 9.1.0. • Téléchargez et installez la dernière version de maintenance preferred (préférée) de PAN-OS 9.1 et redémarrez. • Télécharger PAN-OS 10.0.0. • Téléchargez et installez la dernière version de maintenance PAN-OS 10.0 preferred (préférée) et redémarrez. • Télécharger PAN-OS 10.1.0 • Téléchargez et installez la dernière version de maintenance preferred (préférée) de PAN-OS 10.1 et redémarrez. • Télécharger PAN-OS 10.2.0 • Téléchargez et installez la dernière version de maintenance preferred (préférée) de PAN-OS 10.2 et redémarrez. • Passez à Mettre à niveau le pare-feu vers PAN-OS 11.0.
8.0.x	• Téléchargez et installez PAN-OS 8.0.20 et redémarrez. • Télécharger PAN-OS 8.1.0. • Téléchargez et installez la dernière version de maintenance PAN-OS 8.1 preferred (préférée) et redémarrez. • Télécharger PAN-OS 9.0.0

Version PAN-OS installée	Chemin de mise à niveau recommandé vers PAN-OS 11.0
	• Téléchargez et installez la dernière version de maintenance preferred (préférée) de PAN-OS 9.0 et redémarrez. *Passez en revue les* upgrade/downgrade considerations (considérations relatives à la mise à niveau/rétrogradation) *avant de mettre à niveau les collecteurs de journaux vers la dernière version de maintenance de PAN-OS 9.0.* • Télécharger PAN-OS 9.1.0. • Téléchargez et installez la dernière version de maintenance preferred (préférée) de PAN-OS 9.1 et redémarrez. • Télécharger PAN-OS 10.0.0. • Téléchargez et installez la dernière version de maintenance PAN-OS 10.0 preferred (préférée) et redémarrez. • Télécharger PAN-OS 10.1.0 • Téléchargez et installez la dernière version de maintenance preferred (préférée) de PAN-OS 10.1 et redémarrez. • Passez à Mettre à niveau le pare-feu vers PAN-OS 11.0.
7.1.x	• Téléchargez et installez la version de maintenance de PAN-OS 7.1.26 et redémarrez. • Télécharger PAN-OS 8.0.0. • Téléchargez et installez PAN-OS 8.0.20. • Télécharger PAN-OS 8.1.0. • Téléchargez et installez la dernière version de maintenance PAN-OS 8.1 preferred (préférée) et redémarrez. • Télécharger PAN-OS 9.0.0

Version PAN-OS installée	Chemin de mise à niveau recommandé vers PAN-OS 11.0
	• Téléchargez et installez la dernière version de maintenance preferred (préférée) de PAN-OS 9.0 et redémarrez. *Passez en revue les upgrade/downgrade considerations (considérations relatives à la mise à niveau/rétrogradation) avant de mettre à niveau les collecteurs de journaux vers la dernière version de maintenance de PAN-OS 9.0.* • Télécharger PAN-OS 9.1.0. • Téléchargez et installez la dernière version de maintenance preferred (préférée) de PAN-OS 9.1 et redémarrez. • Télécharger PAN-OS 10.0.0. • Téléchargez et installez la dernière version de maintenance PAN-OS 10.0 preferred (préférée) et redémarrez. • Télécharger PAN-OS 10.1.0 • Téléchargez et installez la dernière version de maintenance preferred (préférée) de PAN-OS 10.1 et redémarrez. • Passez à Mettre à niveau le pare-feu vers PAN-OS 11.0.

Mettre à niveau un pare-feu autonome

Consultez les PAN-OS 11.0 Release Notes (notes de publication de PAN-OS 11.0), puis utilisez la procédure suivante pour mettre à niveau un pare-feu qui n'est pas dans une configuration HA vers PAN-OS 10.1.

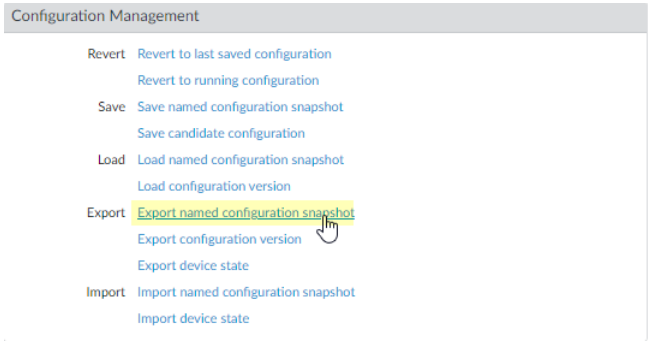
Si vos pare-feux sont configurés pour transférer des échantillons vers un appareil WildFire pour analyse, vous devez upgrade the WildFire appliance (mettre à niveau l'appareil WildFire) avant de mettre à niveau les pare-feux de transfert.

Pour éviter tout impact sur le trafic, procédez à la mise à niveau pendant l'intervalle d'interruption. Assurez-vous que le pare-feu est branché à une source d'alimentation fiable. La perte de courant au cours d'une mise à niveau peut rendre ls pare-feu inutilisable.

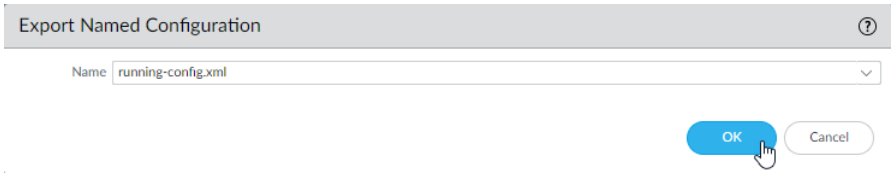
STEP 1 | Faites une sauvegarde du fichier de configuration actuel.

Bien que le pare-feu crée automatiquement une sauvegarde de la configuration, il est recommandé de créer et de stocker une sauvegarde externe avant de procéder à la mise à niveau.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Operations (Opérations)**, puis cliquez sur **Export named configuration snapshot (Exporter l'instantané de configuration nommé)**.



2. Sélectionnez le fichier XML contenant la configuration actuelle (par exemple, **running-config.xml**), puis cliquez sur **OK** pour exporter le fichier de configuration.



3. Enregistrez le fichier exporté dans un emplacement externe au pare-feu. Vous pouvez utiliser cette sauvegarde pour restaurer la configuration en cas de problème pendant la mise à niveau.

STEP 2 | (Optional (Facultatif)) Si vous avez activé User-ID, après la mise à niveau, le pare-feu efface les mappages nom d'utilisateur/adresse IP et de groupe, afin que ces champs puissent être complétés avec les attributs depuis les sources User-ID. Pour estimer le temps nécessaire pour que votre environnement complète à nouveau les mappages, exécutez les commandes CLI suivantes sur le pare-feu.

- Pour les mappages nom d'utilisateur/adresse IP :
  - **`show user user-id-agent state all`**
  - **`show user server-monitor state all`**
- Pour les mappages de groupe : **`show user group-mapping statistics`**

STEP 3 | Assurez-vous que le pare-feu exécute la dernière version du contenu.

Consultez les Release Notes (Notes de publication) pour la version de contenu minimale que vous devez installer pour une version de PAN-OS 11.0. Assurez-vous de suivre le Meilleures pratiques pour les mises à jour du contenu de menace et des applications.

1. Sélectionnez **Device (Périphérique)** > **Dynamic Updates (Mise à jour dynamiques)** et vérifiez les **Applications** ou **Applications and Threats (Applications et menaces)** pour déterminer la mise à jour qui est actuellement installée.

VERSION	FILE NAME	FEATURES	TYPE	SIZE	SHA256	RELEASE DATE	DOWNLOA...	CURRENTLY INSTALLED	ACTION	DOCUMENTAT...
Applications and Threats	**Last checked:** 2020/07/08 01:02:02 PDT	**Schedule:** Every Wednesday at 01:02 (Download only)								
8287-6151	panupv2-all-contents-8287-6151	Apps, Threats	Full	56 MB	36315eff...	2020/06/26 17:34:56 PDT		✓		Release Notes
8287-6152	panupv2-all-contents-8287-6152	Apps, Threats	Full	56 MB	dced5c69...	2020/06/29 11:55:44 PDT	✓ previously		Revert Review Policies Review Apps	Release Notes
8287-6153	panupv2-all-contents-8287-6153	Apps, Threats	Full	56 MB	14af053b...	2020/06/29 17:15:33 PDT			Download	Release Notes
8287-6154	panupv2-all-contents-8287-6154	Apps, Threats	Full	56 MB	c872552f...	2020/06/30 16:14:19 PDT			Download	Release Notes
8287-6155	panupv2-all-contents-8287-6155	Apps, Threats	Full	56 MB	3f0fcb9a6...	2020/06/30 19:09:11 PDT			Download Review Policies Review Apps	Release Notes
8288-6157	panupv2-all-contents-8288-6157	Apps, Threats	Full	56 MB	54f355a1...	2020/07/01 17:00:41 PDT			Download	Release Notes
8288-6158	panupv2-all-contents-8288-6158	Apps, Threats	Full	56 MB	db9e5a8f...	2020/07/01 18:15:46 PDT			Download	Release Notes
8288-6159	panupv2-all-contents-8288-6159	Apps, Threats	Full	56 MB	b6863c96...	2020/07/02 11:55:30 PDT			Download	Release Notes

2. Si le pare-feu n'exécute pas la dernière version du contenu requise ou une version supérieure requise pour PAN-OS 11.0, cliquez sur **Check Now (Vérifier maintenant)** pour consulter la liste des mises à jour disponibles.
3. Trouvez et **téléchargez** la version du contenu souhaitée.

   Après avoir téléchargé avec succès un fichier de mise à jour du contenu, le lien dans la colonne Action passe de **Télécharger** à **Installer** pour cette version du contenu.
4. **Installez** la mise à jour.

STEP 4 | Déterminer le chemin de mise à niveau vers PAN-OS 11.0.

Consultez Liste de contrôle de mise à niveau de PAN-OS, les problèmes connus et les modifications apportées au comportement par défaut dans les Release Notes (notes de version) et Considérations de mise à niveau/rétrogradation pour chaque version par laquelle vous passez dans le cadre de votre chemin de mise à niveau.

STEP 5 | (Best Practices (Meilleures pratiques)) Si vous utilisez Cortex Data Lake (CDL), install the device certificate (installez le certificat du périphérique).

Le pare-feu passe automatiquement à l'utilisation du certificat du périphérique pour l'authentification avec l'ingestion de CDL et les points de terminaison d'interrogation lors de la mise à niveau vers PAN-OS 11.0.

Si vous n'installez pas le certificat de périphérique avant la mise à niveau vers PAN-OS 11.0, le pare-feu continue d'utiliser les certificats de service de journalisation existants pour l'authentification.

STEP 6 | Mettez à niveau vers PAN-OS 11.0.

Si votre pare-feu ne possède pas d'accès Internet depuis le port de gestion, vous pouvez télécharger l'image logicielle depuis le portail d'assistance client Palo Alto Networks*, puis le* ***charger*** *manuellement sur votre pare-feu.*

1. Sélectionnez **Device (Périphérique)** > **Software (Logiciel)** et cliquez sur **Check Now (Vérifier maintenant)** pour afficher les dernières mises à jour PAN-OS.

   Seules les versions de la prochaine version PAN-OS disponible sont affichées. Par exemple, si PAN-OS 11.0 est installé sur le pare-feu, seules les versions PAN-OS 11.0 sont affichées.
2. Sélectionnez **Panorama** > **Device Deployment (Déploiement de périphérique)** > **Software (Logiciel)** > **Action** > **Validate (Valider)**

   Panorama > **Deployment Device (Dispositif de déploiement)** > **Software (logiciel)** > **Action** > **Validate (Validez)** pour afficher tous les logiciels intermédiaires et les images de contenu nécessaires à la mise à niveau vers 11.0.0.
3. Téléchargez le logiciel intermédiaire et les images de contenu.
4. Après avoir téléchargé l'image (ou après avoir chargé l'image pour une mise à niveau manuelle), **installez** l'image.
5. Une fois l'installation terminée, redémarrez en utilisant l'une des méthodes suivantes :
   - Si vous êtes invité à redémarrer, cliquez sur **Yes (Oui)**.
   - Si vous n'êtes pas invité à redémarrer, sélectionnez **Device (Périphérique)** > **Configuration** > **Operations (Opérations)** et cliquez sur **Reboot Device (Redémarrer le périphérique)**.

   Le pare-feu efface alors les mappages User-ID, puis se connecte aux sources User-ID pour remplir à nouveau les mappages.
6. Si vous avez activé User-ID, utilisez les commandes CLI suivantes pour vérifier que le pare-feu a rempli à nouveau les mappages adresse IP/nom d'utilisateur et de groupe avant d'autoriser le trafic.
   - `show user ip-user-mapping all`
   - `show user group list`

STEP 7 | Régénérez ou réimportez tous les certificats pour respecter le niveau de sécurité OpenSSL 2.

Lors de la mise à niveau vers PAN-OS 11.0, tous les certificats doivent répondre aux exigences minimales suivantes :

- RSA 2048 bits ou plus, ou ECDSA 256 bits ou plus
- Digest of SHA256 ou plus

. Consultez le Guide administrateur PAN-OS pour plus d'informations sur la régénération ou la réimportation de vos certificats.

STEP 8 | Vérifiez que le pare-feu fait passer le trafic.

Sélectionnez **Monitor (Surveiller)** > **Session Browser (Navigateur de session)** et vérifiez que vous voyez de nouvelles sessions.

	START TIME	FROM ZONE	TO ZONE	SOURCE	DESTINATI...	FROM PORT	TO PORT	PROTOC...	APPLICATI...	RULE	INGRESS I/F	EGRESS I/F	BYTES	VIRTUAL SYSTEM
⊞	07/08 11:29:02	z1	z2			56622	44060	6	ftp-data	rules6-1	ethernet1/3	ethernet1/4	558	vsys1
⊞	07/08 11:29:00	z1	z2			44823	42573	6	ftp-data	rules6-1	ethernet1/3	ethernet1/4	277874	vsys1
⊞	07/08 11:29:10	z1	z2			60162	47273	6	ftp-data	rules6-1	ethernet1/3	ethernet1/4	580	vsys1
⊞	07/08 11:29:10	z1	z2			45751	6013	6	ftp-data	rules6-1	ethernet1/3	ethernet1/4	560	vsys1
⊞	07/08 11:29:00	z1	z2			52923	42559	6	ftp-data	rules6-1	ethernet1/3	ethernet1/4	111119	vsys1
⊞	07/08 11:29:12	z1	z2			45772	8348	6	ftp-data	rules6-clone-with-group	ethernet1/3	ethernet1/4	785	vsys1
⊞	07/08 11:29:10	z1	z2			39762	61408	6	ftp-data	rules6-1	ethernet1/3	ethernet1/4	554	vsys1
⊞	07/08 11:29:06	z1	z2			53948	56596	6	ftp-data	rules6-1	ethernet1/3	ethernet1/4	792	vsys1
⊞	07/08 11:28:11	z1	z2			38185	42186	6	ftp-data	rules6-1	ethernet1/3	ethernet1/4	3243	vsys1

STEP 9 | Affichez l'historique des mises à niveau logicielles sur le pare-feu.

1. Connectez-vous à l'interface du pare-feu.
2. Allez à **Device (Périphérique)** > **Summary (Résumé)** > **Software (Logiciel)** et cliquez sur**Device History (Historique du périphérique)**.

Mettre à niveau une paire de pare-feux haute disponibilité

Consultez les PAN-OS 11.0 Release Notes (notes de publication de PAN-OS 10.1), puis utilisez la procédure suivante pour mettre à niveau une paire de pare-feu dans une configuration à haute disponibilité (HA). Cette procédure s'applique aussi bien aux configurations actives/passives qu'actives/actives.

Pour éviter les temps d'arrêt lors de la mise à niveau des pare-feu qui sont en configuration de disponibilité élevée, mettre à jour un pair HA à la fois : Pour les pare-feu actifs/actifs, l'homologue que vous mettez à niveau en premier n'a pas d'importance (même si cette procédure explique comment mettre à niveau l'homologue primaire actif en premier, dans un souci de simplicité). Pour les pare-feu actifs/passifs, vous devez d'abord suspendre (basculer) et mettre à niveau le pair actif (principal). Après avoir mis à niveau le pair principal, vous devez annuler la suspension du pair principal pour le ramener à un état fonctionnel (passif). Ensuite, vous devez suspendre le pair passif (secondaire) pour rendre le pair principal actif à nouveau. Une fois le pair principal actif et le pair secondaire suspendu, vous pouvez poursuivre la mise à niveau. Afin d'éviter un basculement lors de la mise à niveau des homologues HA, assurez-vous que la préemption est désactivée avant de poursuivre la mise à niveau. Vous devez uniquement désactiver la préemption sur un homologue de la paire.

Lorsque vous mettez à niveau des pare-feu HA sur plusieurs versions PAN-OS de fonctionnalités, vous devez mettre à niveau chaque pair HA vers la même version PAN-OS de fonctionnalités sur votre chemin de mise à niveau avant de continuer. Par exemple, vous mettez à niveau les pairs HA de PAN-OS 10.0 vers PAN-OS 11.0. Vous devez mettre à niveau les deux pairs HA vers PAN-OS 10.1 avant de pouvoir continuer la mise à niveau vers la version PAN-OS 11.0 cible. Lorsque les pairs HA sont espacés de deux versions de fonctionnalités ou plus, le pare-feu avec l'ancienne version installée entre dans un état `suspended (suspendu)` avec le message `Peer versiion too old (Peer version trop ancienne)`.

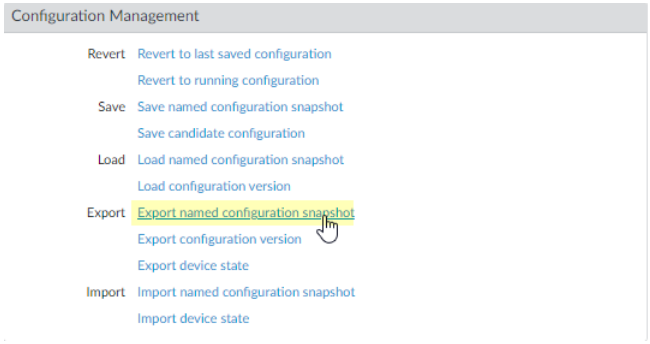
Pour éviter tout impact sur le trafic, procédez à la mise à niveau pendant l'intervalle d'interruption. Assurez-vous que les pare-feu sont branchés à une source d'alimentation fiable. La perte de courant au cours d'une mise à niveau peut rendre les pare-feu inutilisables.

STEP 1 | Faites une sauvegarde du fichier de configuration actuel.

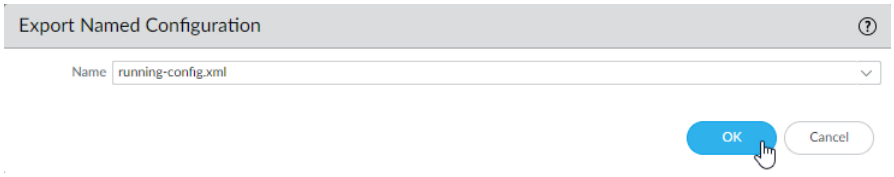
Bien que le pare-feu crée automatiquement une sauvegarde de la configuration, il est recommandé de créer et de stocker une sauvegarde externe avant de procéder à la mise à niveau.

Effectuez ces étapes sur chaque pare-feu dans la paire :

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Operations (Opérations)**, puis cliquez sur **Export named configuration snapshot (Exporter l'instantané de configuration nommé)**.



2. Sélectionnez le fichier XML contenant la configuration actuelle (par exemple, **running-config.xml**), puis cliquez sur **OK** pour exporter le fichier de configuration.



3. Enregistrez le fichier exporté dans un emplacement externe au pare-feu. Vous pouvez utiliser cette sauvegarde pour restaurer la configuration en cas de problème pendant la mise à niveau.

STEP 2 | Sélectionnez **Device (Périphérique)** > **Support (Assistance)** et **Generate Tech Support File (Générer un fichier de support technique)**.

Cliquez sur **Yes (Oui)** lorsque vous êtes invité à générer le fichier de support technique.

STEP 3 | Assurez-vous que chaque pare-feu dans la paire HA exécute la dernière version du contenu.

Consultez les Release Notes (Notes de publication) pour la version de contenu minimale que vous devez installer pour une version de PAN-OS 11.0. Assurez-vous de suivre le Meilleures pratiques pour les mises à jour du contenu de menace et des applications.

1. Sélectionnez **Device (Périphérique)** > **Dynamic Updates (Mise à jour dynamiques)** et vérifiez les **Applications** ou **Applications and Threats (Applications et menaces)** pour déterminer la mise à jour qui est actuellement installée.

VERSION	FILE NAME	FEATURES	TYPE	SIZE	SHA256	RELEASE DATE	DOWNLOA...	CURRENTLY INSTALLED	ACTION	DOCUMENTAT...
Applications and Threats	**Last checked:** 2020/07/08 01:02:02 PDT	**Schedule:** Every Wednesday at 01:02 (Download only)								
8287-6151	panupv2-all-contents-8287-6151	Apps, Threats	Full	56 MB	36315eff...	2020/06/26 17:34:56 PDT		✓		Release Notes
8287-6152	panupv2-all-contents-8287-6152	Apps, Threats	Full	56 MB	dced5c69...	2020/06/29 11:55:44 PDT	✓ previously		Revert Review Policies Review Apps	Release Notes
8287-6153	panupv2-all-contents-8287-6153	Apps, Threats	Full	56 MB	14af053b...	2020/06/29 17:15:33 PDT			Download	Release Notes
8287-6154	panupv2-all-contents-8287-6154	Apps, Threats	Full	56 MB	c872552f...	2020/06/30 16:14:19 PDT			Download	Release Notes
8287-6155	panupv2-all-contents-8287-6155	Apps, Threats	Full	56 MB	3f0fcb9a6...	2020/06/30 19:09:11 PDT			Download Review Policies Review Apps	Release Notes
8288-6157	panupv2-all-contents-8288-6157	Apps, Threats	Full	56 MB	54f355a1...	2020/07/01 17:00:41 PDT			Download	Release Notes
8288-6158	panupv2-all-contents-8288-6158	Apps, Threats	Full	56 MB	db9e5a8f...	2020/07/01 18:15:46 PDT			Download	Release Notes
8288-6159	panupv2-all-contents-8288-6159	Apps, Threats	Full	56 MB	b6863c96...	2020/07/02 11:55:30 PDT			Download	Release Notes

2. Si le pare-feu n'exécute pas la version du contenu requise minimum ou une version supérieure requise pour PAN-OS, cliquez sur **Check Now (Vérifier maintenant)** pour consulter la liste des mises à jour disponibles.
3. Trouvez et **téléchargez** la version du contenu souhaitée.

   Après avoir téléchargé avec succès un fichier de mise à jour du contenu, le lien dans la colonne Action passe de **Télécharger** à **Installer** pour cette version du contenu.
4. **Installez** la mise à jour. Vous devez installer la mise à jour sur les deux homologues.

STEP 4 | Déterminer le chemin de mise à niveau vers PAN-OS 11.0.

Vous ne pouvez pas sauter l'installation de versions de fonctions dans le chemin de la version PAN-OS en cours vers PAN-OS 11.0.

Consultez Liste de contrôle de mise à niveau de PAN-OS, les problèmes connus et les modifications apportées au comportement par défaut dans les Release Notes (notes de version) et Considérations de mise à niveau/rétrogradation pour chaque version par laquelle vous passez dans le cadre de votre chemin de mise à niveau.

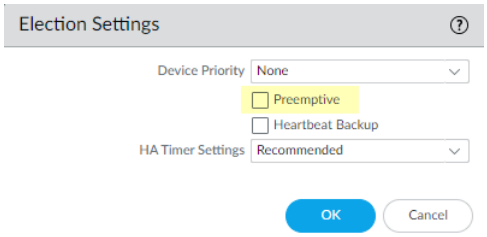
STEP 5 | (Best Practices (Meilleures pratiques)) Si vous utilisez Cortex Data Lake (CDL), install the device certificate (installez le certificat du périphérique) sur chaque homologue HA.

Le pare-feu passe automatiquement à l'utilisation du certificat du périphérique pour l'authentification avec l'ingestion de CDL et les points de terminaison d'interrogation lors de la mise à niveau vers PAN-OS 11.0.

Si vous n'installez pas le certificat de périphérique avant la mise à niveau vers PAN-OS 11.0, le pare-feu continue d'utiliser les certificats de service de journalisation existants pour l'authentification.

STEP 6 | Désactivez la préemption sur le premier homologue de chaque paire. Vous devez uniquement désactiver ce paramètre sur un pare-feu dans la paire HA, mais assurez-vous que la validation est réussie avant de continuer la mise à niveau.

1. Sélectionnez **Device (Périphérique)** > **High Availability (Haute disponibilité)** et modifiez les **Election Settings (Paramètres de sélection)**.
2. si cette option est activée, désactivez (effacez) le **Preemptive (paramètre préemptif)** et cliquez sur **OK**.



3. **Commit (Validez)** la modification.

STEP 7 | Suspendez l’homologue Primaire HA pour forcer un basculement.

(Pare-feux actifs/passifs) Pour les pare-feux dans une configuration HA active/passive, suspendez et mettez à niveau le pair HA actif en premier.

(Pare-feux actifs/actifs) Pour les pare-feux dans une configuration HA active/active, suspendez et mettez à niveau d'abord le pair HA actif-primaire.

1. Sélectionnez **Device (Périphérique)** > **High Availability (Haute disponibilité)** > **Operational Commands (Commandes opérationnelles)**, puis cliquez sur le lien **Suspend local device (Suspendre le périphérique local)**.
2. Dans le coin inférieur droit, vérifiez que l'état est `suspended (suspendu)`.

   Le basculement résultant devrait faire passer le pair HA secondaire à l'état `actif`.

   Le basculement résultant vérifie que le basculement HA fonctionne correctement avant votre mise à niveau.

STEP 8 | Installez PAN-OS 11.0 sur le pair HA suspendu.

1. Pour le premier homologue HA, sélectionnez **Device (Périphérique)** > **Software (Logiciel)** et cliquez sur **Check Now (Vérifier maintenant)** pour les dernières mises à jour.

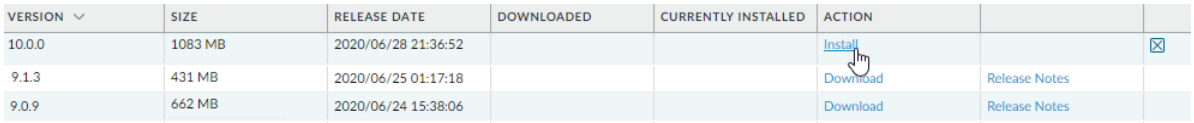
   Seules les versions de la prochaine version PAN-OS disponible sont affichées. Par exemple, si PAN-OS 11.0 est installé sur le pare-feu, seules les versions PAN-OS 11.0 sont affichées.

2. Localisez et **Download (téléchargez)** PAN-OS 11.0.0.

   Si votre pare-feu ne possède pas d'accès Internet depuis le port de gestion, vous pouvez télécharger l'image logicielle depuis le portail d'assistance Palo Alto Networks*, puis le* ***charger*** *manuellement sur votre pare-feu.*

   Si votre pare-feu a accès à Internet et que vous rencontrez une erreur de téléchargement de fichier, cliquez à nouveau sur ***Check Now (Vérifier maintenant)*** *pour actualiser la liste des images PAN-OS.*

3. Après avoir téléchargé l'image (ou après avoir chargé l'image pour une mise à niveau manuelle), **installez** l'image.



4. Une fois l'installation terminée, redémarrez en utilisant l'une des méthodes suivantes :

   - Si vous êtes invité à redémarrer, cliquez sur **Yes (Oui)**.
   - Si vous n'êtes pas invité à redémarrer, sélectionnez **Device (Périphérique)** > **Configuration** > **Operations (Opérations)** et **Reboot Device (Redémarrez le périphérique)**.

5. Une fois le périphérique terminé de redémarrer, affichez le widget Haute disponibilité sur le **Dashboard (tableau de bord)** et vérifiez que le périphérique que vous venez de mettre à niveau est synchronisé avec le pair.

STEP 9 | Restaurez la fonctionnalité HA au pair HA principal.

1. Accédez à l'interface Web du pare-feu, sélectionnez **Device (Dispositif)** > **High Availability (Haute Disponibilité)** > **Operational Commands (Commandes opérationnelles)**, et **Make local device functional (Activez le périphérique local pour la haute disponibilité)**.
2. Dans le coin inférieur droit, vérifiez que l'état est `Passif`. Pour les pare-feu dans une configuration active/active, vérifiez que l'état est `Active (Actif)`.
3. Attendez que la configuration de l'homologue HA en cours se synchronise.

   Dans **Dashboard (tableau de bord)**, surveillez l'état de la configuration d'exécution dans le widget Haute disponibilité.

STEP 10 | Sur l’homologue HA secondaire, suspendez l’homologue HA.

1. Sélectionnez **Device (Périphérique)** > **High Availability (Haute disponibilité)** > **Operational Commands (Commandes opérationnelles)**, puis cliquez sur le lien **Suspend local device (Suspendre le périphérique local)**.
2. Dans le coin inférieur droit, vérifiez que l'état est `suspended (suspendu)`.

   Le basculement qui en résulte devrait provoquer la transition de l’homologue primaire HA vers l’état `active (actif)`.

STEP 11 | Installez PAN-OS 11.0 sur l’homologue HA secondaire.

1. Pour le deuxième homologue, sélectionnez **Device (Périphérique)** > **Software (Logiciel)** et cliquez sur **Check Now (Vérifier maintenant)** pour les dernières mises à jour.
2. Localisez et **Download (téléchargez)** PAN-OS 11.0.0.
3. Une fois que vous avez téléchargé l’image, **installez**-la.
4. Une fois l’installation terminée, redémarrez en utilisant l’une des méthodes suivantes :
   - Si vous êtes invité à redémarrer, cliquez sur **Yes (Oui)**.
   - Si vous n’êtes pas invité à redémarrer, sélectionnez **Device (Périphérique)** > **Configuration** > **Operations (Opérations)** et **Reboot Device (Redémarrez le périphérique)**.

STEP 12 | Restaurez la fonctionnalité HA à l’homologue HA secondaire.

1. Accédez à l'interface Web du pare-feu, sélectionnez **Device (Dispositif)** > **High Availability (Haute Disponibilité)** > **Operational Commands (Commandes opérationnelles)**, et **Make local device functional (Activez le périphérique local pour la haute disponibilité)**.
2. Dans le coin inférieur droit, vérifiez que l'état est `Passif`. Pour les pare-feu dans une configuration active/active, vérifiez que l'état est `Active (Actif)`.
3. Attendez que la configuration de l’homologue HA en cours se synchronise.

   Dans le **Dasbhoard (tableau de bord)**, surveillez le widget de haute disponibilité de l'état Exécution de la configuration.

STEP 13 | Réactiver la préemption sur l’homologue HA où il a été désactivé à l'étape précédente.

1. Sélectionnez **Device (Périphérique)** > **High Availability (Haute disponibilité)** et modifiez les **Election Settings (Paramètres de sélection)**.
2. Activez (cochez) le paramètre **Préemptif** et cliquez sur **OK**.
3. **Commit (Validez)** la modification.

STEP 14 | Régénérez ou réimportez tous les certificats pour respecter le niveau de sécurité OpenSSL 2.

Lors de la mise à niveau vers PAN-OS 11.0, tous les certificats doivent répondre aux exigences minimales suivantes :

- RSA 2048 bits ou supérieur, ou ECDSA 256 bits ou supérieur
- Digest de SHA256 ou supérieur

Consultez le Guide de l’administrateur PAN-OS ou le Guide de l’administrateur de Panorama pour plus d’informations sur la régénération ou la réimportation de vos certificats.

STEP 15 | Vérifiez que les deux homologues font passer le trafic comme prévu.

Dans une configuration active/passive, seul l'homologue actif doit faire passer le trafic ; les deux homologues doivent faire passer le trafic dans une configuration active/active.

Exécutez les commandes CLI suivantes pour confirmer la réussite de la mise à niveau :

- (Homologues actifs uniquement) Pour vérifier que les homologues actifs font passer le trafic, exécutez la commande **`show session all (Montrer toutes les sessions)`** command.
- Pour vérifier la synchronisation des sessions, exécutez la **`show high-availability interface ha2`** et assurez-vous que les compteurs d'interface matérielle de la table du processeur augmentent comme suit :
  - Dans une configuration active/passive, seul l'homologue actif affiche les paquets transmis ; l'homologue passif affiche uniquement les paquets reçus.

    Si vous avez activé HA2 keep-alive (Maintien HA2), les compteurs d'interface matérielle sur l'homologue passif affichent à la fois les paquets de transmission et de réception. Cela se produit car HA2 keep-alive (Maintien HA2) est bidirectionnel, ce qui signifie que les deux homologues transmettent des paquets HA2 keep-alive (Maintien HA2).
  - Dans la configuration active/active, les paquets reçus et les paquets transmis s'affichent sur les deux homologues.

Mettre à niveau le pare-feu vers PAN-OS 11.0 à partir de Panorama

Déployez des mises à jour de contenu et mettez à niveau PAN-OS pour les pare-feu gérés à partir du serveur d'administration Panorama™.

- Mettre à niveau les pare-feu lorsque Panorama est connecté à Internet
- Mettre à niveau les pare-feu lorsque Panorama n'est pas connecté à Internet
- Mettre à niveau un pare-feu ZTP

Mettre à niveau les pare-feu lorsque Panorama est connecté à Internet

Passez en revue les PAN-OS 11.0 Release Notes (notes de publication de PAN-OS 11.0) puis utilisez la procédure suivante pour mettre à niveau les pare-feux que vous gérez avec Panorama. Cette procédure s'applique aux pare-feu autonomes et aux pare-feu déployés dans une configuration à haute disponibilité (HA).

Lorsque vous mettez à niveau des pare-feu HA sur plusieurs versions PAN-OS de fonctionnalités, vous devez mettre à niveau chaque pair HA vers la même version PAN-OS de fonctionnalités sur votre chemin de mise à niveau avant de continuer. Par exemple, vous mettez à niveau les pairs HA de PAN-OS 10.0 vers PAN-OS 11.0. Vous devez mettre à niveau les deux homologues HA vers PAN-OS 10.1 avant de pouvoir continuer la mise à niveau vers la version PAN-OS 11.0 cible. Lorsque les pairs HA sont espacés de deux versions de fonctionnalités ou plus, le pare-feu avec l'ancienne version installée entre dans un état `suspended (suspendu)` avec le message `Peer version too old (Peer version trop ancienne)`.

Si Panorama ne parvient pas à se connecter directement au serveur de mises à jour, suivez la procédure Mettre à niveau les pare-feu lorsque Panorama n'est pas connecté à Internet *afin de pouvoir télécharger manuellement des images dans Panorama, puis les distribuer les images sur le pare-feu.*

La nouvelle fonctionnalité Ignorer la mise à niveau des versions logicielles vous permet d'ignorer jusqu'à trois versions lors du déploiement de mises à niveau des appareils Panorama sur PAN-OS 11.0 vers des pare-feux sur PAN-OS 10.1 ou versions ultérieures.

Avant de faire la mise-à-jour du pare-feu sur Panorama, vous devez :

- Assurez-vous que Panorama exécute la même version ou une version ultérieure de PAN-OS que celle utilisée pour la mise à niveau. Vous devez mettre à niveau Panorama et ses Log Collectors (Collecteurs de journaux) vers la version 11.0 avant de mettre à niveau les pare-feu gérés vers cette version. Lorsque vous mettez à niveau les collecteurs de journaux vers la version 11.0, vous devez mettre à niveau tous les collecteurs de journaux en même temps en raison des modifications de l'infrastructure de journalisation.
- Assurez-vous que les pare-feu sont branchés à une source d'alimentation fiable. La perte de courant au cours d'une mise à niveau peut rendre les pare-feu inutilisables.
- Décidez si vous souhaitez rester en mode hérité si le périphérique virtuel Panorama est en mode hérité lors de la mise à niveau vers PAN-OS 11.0. Le mode hérité n'est pas pris en charge pour un nouveau déploiement de périphérique virtuel Panorama exécutant PAN-OS 9.1 ou une version ultérieure. Si

vous mettez à niveau le périphérique virtuel Panorama de PAN-OS 9.0 ou d'une version antérieure vers PAN-OS 11.0, Palo Alto Networks recommande de revoir les Setup Prerequisites for the Panorama Virtual Appliance (Conditions préalables à la configuration du périphérique virtuel Panorama) et de passer en Panorama mode (mode Panorama) ou en Management Only mode (mode Gestion uniquement) en fonction de vos besoins.

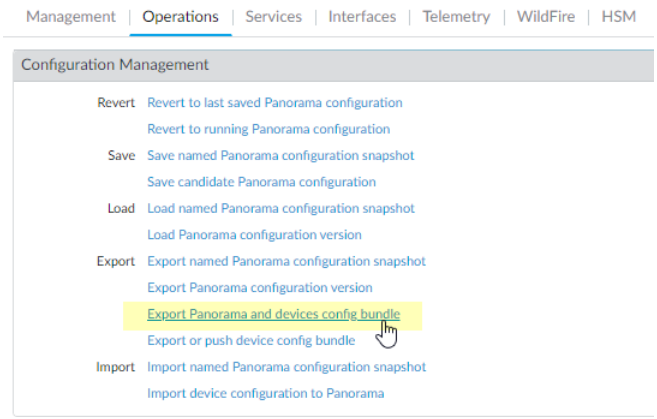
Si vous souhaitez conserver le périphérique virtuel Panorama en mode hérité, increase CPUs and memory (augmentez les processeurs et la mémoire) alloués au périphérique virtuel Panorama à un minimum de 16 processeurs et 16 Go de mémoire pour réussir la mise à niveau vers PAN-OS 11.0. Consultez les Setup Prerequisites for the Panorama Virtual Appliance (conditions préalables à l'installation du périphérique virtuel Panorama) pour plus d'informations.

STEP 1 | Connectez-vous à l'interface Web Panorama.

STEP 2 | Effectuez une copie de sauvegarde du fichier de configuration actuel sur chaque pare-feu géré que vous envisagez de mettre à niveau.

Bien que le pare-feu crée automatiquement une sauvegarde de la configuration, il est recommandé de créer et de stocker une sauvegarde externe avant de procéder à la mise à niveau.

1. Sélectionnez **Panorama** > **Setup (Configuration)** > **Operations (Opérations)** et cliquez sur**Export Panorama and devices config bundle (Exporter la solution de configuration de Panorama et des périphériques)** pour générer et exporter la dernière la sauvegarde de configuration de Panorama et celle de chaque appareil géré.



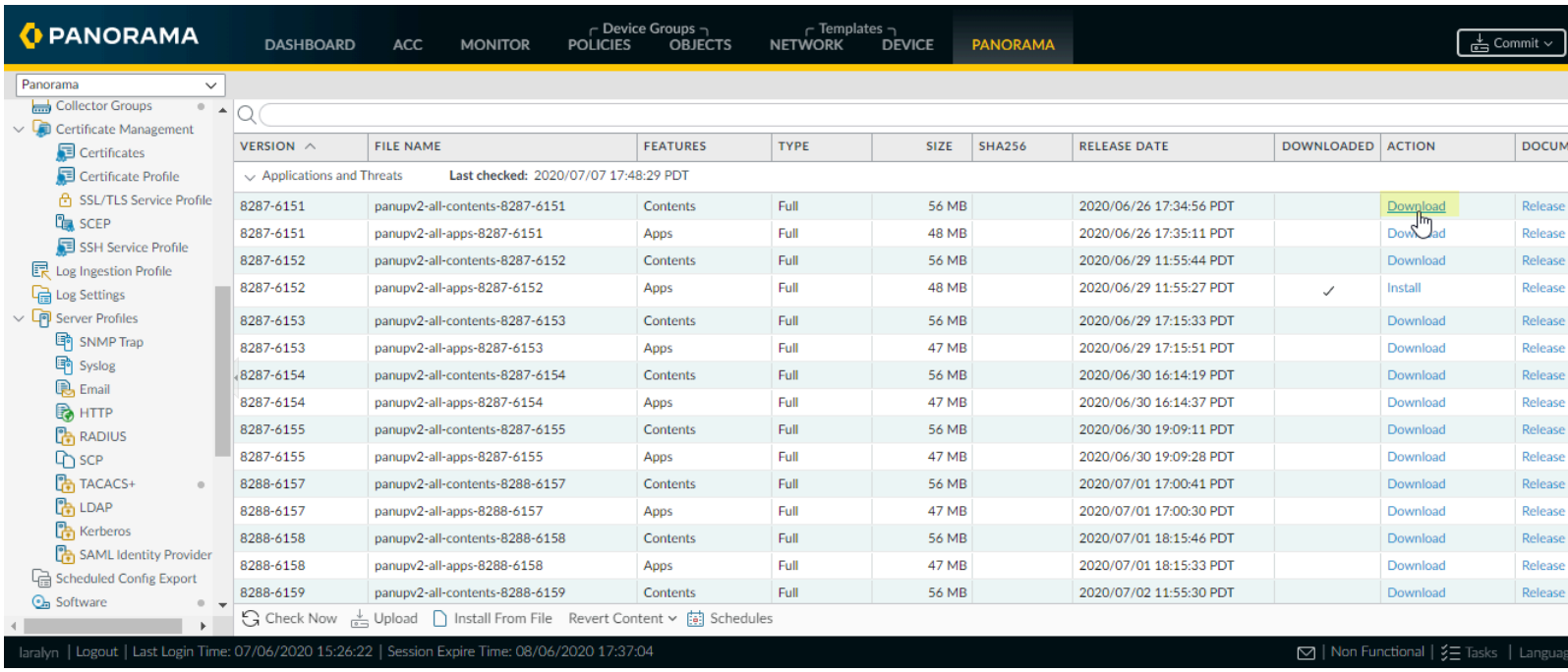
2. Enregistrez le fichier exporté dans un emplacement externe au pare-feu. Vous pouvez utiliser cette sauvegarde pour restaurer la configuration en cas de problème pendant la mise à niveau.

STEP 3 | Installez la dernière mise à jour de contenu.

Consultez les Release Notes (Notes de publication) de la version minimale de contenu que vous devez installer pour PAN-OS 11.0. Assurez-vous de suivre les Meilleures pratiques pour les mises à jour du contenu de menace et des applications lors du déploiement des mises à jour de contenu sur Panorama et les pare-feu gérés.

1. Sélectionnez **Panorama** > **Device Deployment (Déploiement de périphériques)** > **Dynamic Updates (Mises à jour dynamiques)** et **Check Now (Vérifiez maintenant)** pour obtenir les

dernières mises à jour. Si une mise à jour est disponible, la colonne Action affiche un lien **Download (Télécharger)**.



2. Cliquez sur **Install (Installer)** et sélectionnez les pare-feux sur lesquels vous voulez installer la mise à jour. Si vous mettez à niveau des pare-feu HA, vous devez mettre à jour le contenu des deux homologues.
3. Cliquez sur **OK**.

STEP 4 | Déterminer le chemin de mise à niveau vers PAN-OS 11.0..

Passez en revue la PAN-OS Upgrade Checklist (liste de vérification de mise à jour PAN-OS)*, les problèmes connus et les modifications du comportement par défaut dans les* Release Notes (Notes de version) *et les* upgrade/downgrade considerations (considérations de mise à niveau vers une version supérieure ou antérieure) *pour chaque version à travers laquelle vous passez dans le cadre de votre chemin de mise à niveau.*

Si vous mettez à niveau plusieurs pare-feu, rationalisez le processus en déterminant les chemins de mise à niveau de tous les pare-feu avant de commencer à télécharger des images.

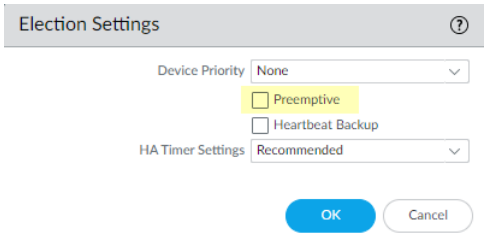
STEP 5 | (Best Practices (Meilleures pratiques)) Si vous utilisez Cortex Data Lake (CDL), install the device certificate (installez le certificat du périphérique).

Le pare-feu passe automatiquement à l'utilisation du certificat du périphérique pour l'authentification avec l'ingestion de CDL et les points de terminaison d'interrogation lors de la mise à niveau vers PAN-OS 11.0.

Si vous n'installez pas le certificat de périphérique avant la mise à niveau vers PAN-OS 11.0, le pare-feu continue d'utiliser les certificats de service de journalisation existants pour l'authentification.

STEP 6 | (HA firewall upgrades only) Si vous mettez à niveau des pare-feu faisant partie d'une paire haute disponibilité, désactivez la préemption. Vous devez uniquement désactiver ce paramètre sur un pare-feu dans chaque paire haute disponibilité.

1. Sélectionnez **Device (Périphérique)** > **High Availability (Haute disponibilité)** et modifiez les **Election Settings (Paramètres de sélection)**.
2. si cette option est activée, désactivez (effacez) le **Preemptive (paramètre préemptif)** et cliquez sur **OK**.



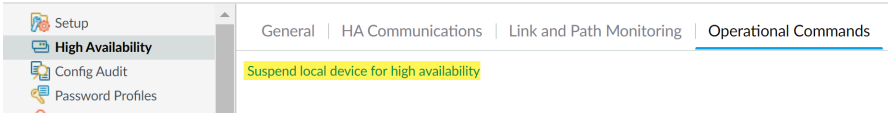
3. **Commit (Validez)** la modification. Assurez que la validation est un succès avant de procéder à la mise-à-jour.

STEP 7 | (HA firewall upgrades only (Mises à niveau du pare-feu HA uniquement)) Suspendez l'homologue HA principal pour forcer un basculement.

(Pare-feux actifs/passifs) Pour les pare-feux dans une configuration HA active/passive, suspendez et mettez à niveau le pair HA actif en premier.

(Pare-feux actifs/actifs) Pour les pare-feux dans une configuration HA active/active, suspendez et mettez à niveau d'abord le pair HA actif-primaire.

1. Log in to the firewall web interface (Connectez-vous à l'interface Web du pare-feu) principal actif de l'homologue HA du pare-feu.
2. Sélectionnez **Device (Équipement)** > **High Availability (Haute disponibilité)** > **Operational Commands (Commandes opérationnelles)**, puis cliquez sur le lien **Suspend local device (Suspendre le périphérique local)**.



3. Dans le coin inférieur droit, vérifiez que l'état est `suspended (suspendu)`.

   Le basculement qui en résulte doit entraîner la transition de l'homologue HA passif secondaire vers l'état `actif` .

   Le basculement résultant vérifie que le basculement HA fonctionne correctement avant la mise à niveau.

STEP 8 | (Facultatif) Mettez à niveau vos pare-feu gérés vers PAN-OS 10.1.

La fonctionnalité de mise à niveau de version logicielle ignore prend en charge les pare-feu gérés exécutant PAN-OS 10.1 ou versions ultérieures. Si vos pare-feu gérés sont sur PAN-OS 10.0 ou une version antérieure, commencez par effectuer une mise à niveau vers PAN-OS 10.1 ou une version ultérieure.

STEP 9 | (Optional (Facultatif)) **Export (Exportez)** le fichier vers un serveur SCP configuré.

Dans PAN-OS 11.0, les serveurs SCP sont disponibles en tant que source de téléchargement lors du déploiement de mises à niveau vers des pare-feu gérés. Exportez le fichier avant de télécharger le logiciel et les images de contenu à l'étape suivante.

STEP 10 | Validez et téléchargez les versions logicielles et de contenu requises pour la version cible.

Dans cette étape, vous pouvez afficher et télécharger les images logicielles et de contenu intermédiaires requises pour effectuer la mise à niveau vers PAN-OS 11.0.

Le téléchargement de logiciels et d'images de contenu à l'aide du téléchargement multi-images est facultatif. Vous pouvez toujours télécharger des images une à la fois.

1. Cliquez sur **Panorama** > **Device Deployment** > **Software** > **Action** > **Validate**.
2. Affichez les versions intermédiaires du logiciel et du contenu que vous devez télécharger.
3. Sélectionnez les pare-feux que vous souhaitez mettre à niveau et cliquez sur **Deploy (Déployer)**.
4. Sélectionnez une source de téléchargement et cliquez sur **Télécharger**.

STEP 11 | Installez PAN-OS 11.0.0 sur les pare-feux.

*(SD-WAN only (SD-WAN uniquement)) Pour conserver un état précis de vos liaisons SD-WAN, vous devez mettre à niveau vos pare-feu de concentrateur vers PAN-OS 11.0 avant de mettre à niveau vos pare-feu de succursale. La mise à jour des pare-feux de branche avant les pare-feux de plate-forme peut entraîner une mauvaise surveillance des données (**Panorama** > **SD-WAN** > **Monitoring (Surveillance)**) et les liens SD-WAN peuvent être affichés comme étant `down (en panne)` de façon erronée.*

1. Cliquez sur **Install (Installer)** dans la colonne Action correspondant aux modèles de pare-feu que vous souhaitez mettre à niveau. Par exemple, si vous souhaitez mettre à niveau vos pare-feux PA-220, cliquez sur **Install (installer)** dans la ligne correspondant à PanOS_220-11.0.0.
2. Dans la boîte de dialogue Déployer le fichier logiciel, sélectionnez tous les pare-feu que vous souhaitez mettre à niveau.

   (HA firewall upgrades only (Mises à niveau du pare-feu HA uniquement)) Pour réduire les temps d'arrêt, sélectionnez un seul homologue dans chaque paire HA. Pour les paires actives / passives, sélectionnez l'homologue passif; pour les paires actives / actives, sélectionnez l'homologue actif-secondaire.
3. (Mises à niveau des pare-feu HA uniquement) Assurez-vous que le **Group HA Peers (Groupe de paire HA)** n'est pas sélectionné.
4. Sélectionnez **Reboot device after install (Redémarrer le périphérique après l'installation)**.
5. Pour débuter la mise à jour, cliquez sur **OK**.
6. Une fois l'installation terminée, redémarrez en utilisant l'une des méthodes suivantes :
   - Si vous êtes invité à redémarrer, cliquez sur **Yes (Oui)**.
   - Si vous n'êtes pas invité à redémarrer, sélectionnez **Device (Périphérique)** > **Configuration** > **Operations (Opérations)** et **Reboot Device (Redémarrez le périphérique)**.
7. Après que le pare-feu a terminé le redémarrage, sélectionnez **Panorama** > **Managed Devices (Périphériques gérés)** et vérifiez que la version du logiciel est 11.0.0 pour les pare-feu que vous

avez mis à niveau. Vérifiez également que le statut HA de tous les pare-feu passifs mis à niveau est toujours passif.

STEP 12 | (HA firewall upgrades only (Mises à niveau du pare-feu HA uniquement)) Restaurez la fonctionnalité HA sur l'homologue HA principal.

1. Log in to the firewall web interface (Connectez-vous à l'interface Web) du pare-feu principal suspendu de l'homologue HA du pare-feu.
2. SélectionnezDevice (Appareil) > High Availability (Haute disponibilité) > Operational Commands (Commandes opérationnelles) et Make local device functional for high availability (Activez le périphérique local pour la haute disponibilité).
3. Dans le coin inférieur droit, vérifiez que l'état est `Passive (Passif)`. Pour les pare-feu dans une configuration active/active, vérifiez que l'état est `Active (Actif)`.
4. Attendez que la configuration de l'homologue HA en cours se synchronise.

   Dans **Dashboard (tableau de bord)**, surveillez l'état de la configuration d'exécution dans le widget Haute disponibilité.

STEP 13 | (HA firewall upgrades only (Mises à niveau du pare-feu HA uniquement)) Suspendez l'homologue HA secondaire pour forcer un basculement vers l'homologue HA principal.

1. Log in to the firewall web interface (Connectez-vous à l'interface Web) du pare-feu secondaire actif de l'homologue HA du pare-feu.
2. Sélectionnez **Device (Équipement)** > **High Availability (Haute disponibilité)** > **Operational Commands (Commandes opérationnelles)**, puis cliquez sur le lien **Suspend local device (Suspendre le périphérique local)**.
3. Dans le coin inférieur droit, vérifiez que l'état est `suspended (suspendu)`.

   Le basculement qui en résulte doit entraîner la transition de l'homologue HA passif principal vers l'état `actif` .

   Le basculement résultant vérifie que le basculement HA fonctionne correctement avant la mise à niveau.

STEP 14 | (Mise à niveau des pare-feu HA uniquement) Mettez à niveau le deuxième pair HA dans chaque paire HA.

1. Dans l'interface Web de Panorama, sélectionnez **Logiciel** > **de déploiement de** > **périphériques Panorama**.
2. Cliquez sur **Install (Installer)** dans la colonne Action correspondant aux modèles de HA que vous souhaitez mettre à niveau.
3. Dans la boîte de dialogue Déployer le fichier logiciel, sélectionnez tous les pare-feu que vous souhaitez mettre à niveau. Cette fois, sélectionnez uniquement les homologues des pare-feu HA que vous venez de mettre à jour.
4. Assurez-vous que le **Group HA Peers (Groupe de paire HA)** n'est pas sélectionné.
5. Sélectionnez **Reboot device after install (Redémarrer le périphérique après l'installation)**.
6. Pour débuter la mise à jour, cliquez sur **OK**.
7. Une fois l'installation terminée, redémarrez en utilisant l'une des méthodes suivantes :
   - Si vous êtes invité à redémarrer, cliquez sur **Yes (Oui)**.
   - Si vous n'êtes pas invité à redémarrer, sélectionnez **Device (Périphérique)** > **Configuration** > **Operations (Opérations)** et **Reboot Device (Redémarrez le périphérique)**.

STEP 15 | (HA firewall upgrades only (Mises à niveau du pare-feu HA uniquement) Restaurez la fonctionnalité HA sur l'homologue HA secondaire.

1. Log in to the firewall web interface (Connectez-vous à l'interface Web) du pare-feu de l'homologue HA du pare-feu secondaire suspendu.
2. Sélectionnez**Device (Appareil)** > **High Availability (Haute disponibilité)** > **Operational Commands (Commandes opérationnelles)** et **Make local device functional for high availability (Activez le périphérique local pour la haute disponibilité)**.
3. Dans le coin inférieur droit, vérifiez que l'état est `Passive (Passif)`. Pour les pare-feu dans une configuration active/active, vérifiez que l'état est `Active (Actif)`.
4. Attendez que la configuration de l'homologue HA en cours se synchronise.

   Dans **Dashboard (tableau de bord)**, surveillez l'état de la configuration d'exécution dans le widget Haute disponibilité.

STEP 16 | (mode FIPS-CC uniquement) Mettre à niveau Panorama et les périphériques gérés en mode FIPS-CC.

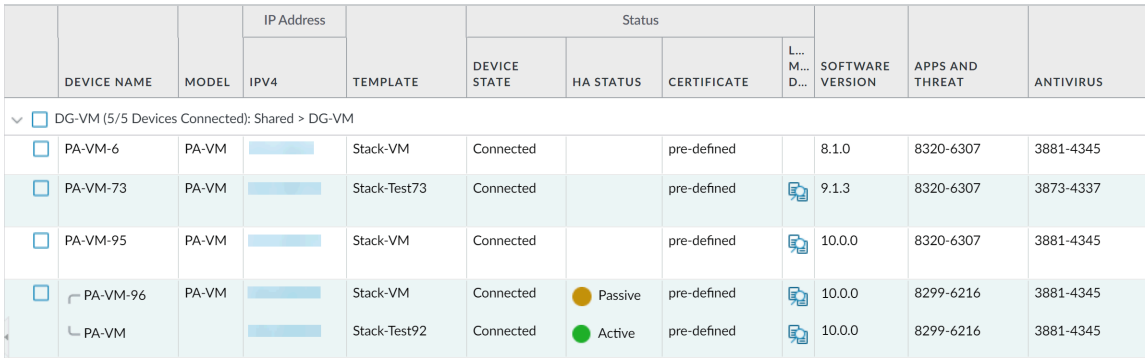
La mise à niveau d'un pare-feu géré en mode FIPS-CC nécessite que vous réinitialisiez l'état de la connexion sécurisée si vous avez ajouté le collecteur de journaux dédié à la gestion Panorama alors que le pare-feu géré exécutait une version de PAN-OS 11.0.

Vous n'avez pas besoin de réintégrer le pare-feu géré ajouté à la gestion Panorama lorsque le pare-feu géré exécutait PAN-OS 10.0 ou une version antérieure.

STEP 17 | Vérifiez la version du logiciel et du contenu qui s'exécute sur chaque pare-feu géré.

1. Sur Panorama, sélectionnez **Panorama** > **Managed Devices (Périphériques gérés)**.
2. Localisez les pare-feu et examinez les versions de contenu et logicielles dans le tableau.

   Pour les pare-feu HA, vous pouvez également vérifier que l'état HA de chaque homologue est conforme aux attentes.



	DEVICE NAME	MODEL	IP Address IPV4	TEMPLATE	Status DEVICE STATE	HA STATUS	CERTIFICATE	L... M... D...	SOFTWARE VERSION	APPS AND THREAT	ANTIVIRUS
	DG-VM (5/5 Devices Connected): Shared > DG-VM										
	PA-VM-6	PA-VM		Stack-VM	Connected		pre-defined		8.1.0	8320-6307	3881-4345
	PA-VM-73	PA-VM		Stack-Test73	Connected		pre-defined		9.1.3	8320-6307	3873-4337
	PA-VM-95	PA-VM		Stack-VM	Connected		pre-defined		10.0.0	8320-6307	3881-4345
	PA-VM-96	PA-VM		Stack-VM	Connected	Passive	pre-defined		10.0.0	8299-6216	3881-4345
	PA-VM			Stack-Test92	Connected	Active	pre-defined		10.0.0	8299-6216	3881-4345

STEP 18 | (Mises à niveau des pare-feu HA uniquement)Si vous avez désactivé la préemption sur l'un de vos pare-feu haute disponibilité avant de procéder à la mise à niveau, modifiez les **Election Settings (Paramètres d'élection)** (**Device (Périphérique)** > **High Availability (Haute disponibilité)**) et réactivez le paramètre **Preemptive (Préemptif)** pour ce pare-feu, puis **Commit (Validez)** le changement.

STEP 19 | Sur Panorama web interface (interface Web de Panorama), transférez l'ensemble de la configuration gérée de Panorama vers vos pare-feu gérés.

Cette étape est nécessaire pour activer la validation sélective et la diffusion des modifications de configuration des groupes de périphériques et des piles de modèles de Panorama vers vos pare-feu gérés.

Cela est nécessaire pour appliquer avec succès les modifications de configuration aux pare-feu multi-vsys gérés par Panorama après une mise à niveau réussie vers PAN-OS 11.0 à partir de PAN-OS 10.1 ou d'une version antérieure. Pour plus d'informations, consultez la modification du comportement par défaut des objets de configuration partagés pour les pare-feu multi-vsys gérés par Panorama.

1. Sélectionnez **Commit (valider)** > **Push to Devices (Appliquer aux périphériques)**.
2. **Push (Appliquer)**.

STEP 20 | Régénérez ou réimportez tous les certificats pour respecter le niveau de sécurité OpenSSL 2.

Lors de la mise à niveau vers PAN-OS 10.2 ou version ultérieure, tous les certificats doivent répondre aux exigences minimales suivantes. Ignorez cette étape si vous effectuez une mise à niveau à partir de PAN-OS 10.2 et que vous avez déjà régénéré ou réimporté vos certificats.

- RSA 2048 bits ou supérieur, ou ECDSA 256 bits ou supérieur
- Digest de SHA256 ou supérieur

Consultez le Guide de l'administrateur PAN-OS ou le Guide de l'administrateur de Panorama pour plus d'informations sur la régénération ou la réimportation de vos certificats.

STEP 21 | Affichez l'historique des mises à niveau logicielles du pare-feu.

1. Connectez-vous à l'interface Panorama.
2. Accédez à **Panorama** > **Managed Devices (appareils gérés)** > **Summary (Résumé)** et cliquez sur **Device History (Historique des appareils)**.

Mettre à niveau les pare-feu lorsque Panorama n'est pas connecté à Internet

Pour une liste des mises à jour de logiciels et de contenu que vous pouvez installer sur des pare-feu, voir Mises à jour prises en charge.

La nouvelle fonctionnalité Ignorer la mise à niveau des versions logicielles vous permet d'ignorer jusqu'à trois versions lors du déploiement de mises à niveau des appareils Panorama sur PAN-OS 11.0 vers des pare-feux sur PAN-OS 10.1 ou versions ultérieures.

STEP 1 | Avant de mettre à niveau des pare-feu gérés, assurez-vous que vous exécutez PAN-OS 11.0 sur le serveur d'administration Panorama et les collecteurs de journaux.

Palo Alto Networks® recommande vivement que Panorama et les collecteurs de journaux exécutent la même version du logiciel Panorama et que Panorama, les collecteurs de journaux et tous les pare-feu gérés exécutent la même version de contenu.

Pour les détails de compatibilité de logiciels et de contenus importants, voir Compatibilité des versions de Panorama, des collecteurs de journaux, des pare-feu et de WildFire.

Panorama doit exécuter la même version de logiciel (ou une version ultérieure) que les pare-feu, mais doit avoir la même version de contenu ou une version antérieure :

- **Version du logiciel** : si votre serveur de gestion Panorama ou les collecteurs de journaux n'exécutent pas déjà la même version de logiciel ou une version ultérieure que la version à laquelle vous souhaitez mettre à jour les pare-feu, vous devez installer la même version ou une version ultérieure sur Panorama, puis sur les collecteurs de journaux (voir Installer les mises à jour de contenu et logicielles pour Panorama) avant de mettre à jour les pare-feu.
- **Version du contenu** : pour les versions de publication de contenu, vous devez vous assurer que tous les pare-feu exécutent la dernière version de contenu ou, au minimum, qu'ils exécutent une version ultérieure de Panorama et des collecteurs de journaux ; sinon, mettez à jour les pare-feu gérés, puis mettez à niveau les collecteurs de journaux lorsque Panorama n'est pas connecté à Internet avant de mettre à jour la version du contenu sur le serveur de gestion Panorama (voir Installer les mises à jour de contenu et logicielles pour Panorama).

Pour vérifier les versions de logiciel et de contenu :

- **Serveur de gestion Panorama** : connectez-vous à l'interface Web Panorama et accédez aux paramètres General Information (Informations générales) (**Dashboard (Tableau de bord)**).
- **Collecteurs de journaux** : connectez-vous à l'ILC de chaque collecteur de journaux et exécutez la commande **`show system info`**.

STEP 2 | Effectuez une copie de sauvegarde du fichier de configuration actuel sur chaque pare-feu géré que vous envisagez de mettre à niveau.

Bien que le pare-feu crée automatiquement une sauvegarde de la configuration, il est recommandé de créer et de stocker une sauvegarde externe avant de procéder à la mise à niveau.

1. **Export Panorama and devices config bundle (Exporter la solution de configuration des périphériques et de Panorama)** (**Panorama** > **Setup (Configuration)** > **Operations (Opérations)**) pour générer et exporter la dernière la sauvegarde de configuration de Panorama et celle de chaque appareil géré.
2. Enregistrez le fichier exporté dans un emplacement externe au pare-feu. Vous pouvez utiliser cette sauvegarde pour restaurer la configuration en cas de problème pendant la mise à niveau.

STEP 3 | Déterminez les mises à jour de contenu à installer. Consultez les Notes de version pour la version de contenu minimale que vous devez installer pour une version de PAN-OS®.

Palo Alto Networks recommande fortement que Panorama, les collecteurs de journaux et tous les pare-feu gérés exécutent la même version de contenu.

Pour chaque mise à jour de contenu, déterminez si vous avez besoin de mises à jour et quelles mises à jour de contenu doivent être téléchargées à la prochaine étape.

Assurez-vous que Panorama exécute la même version de contenu, mais pas une version ultérieure à celle exécutée sur les pare-feu gérés et les collecteurs de journaux.

STEP 4 | Determine the software upgrade path (Déterminez le chemin de mise à niveau logicielle) pour les pare-feux que vous avez l'intention de mettre à jour vers Panorama 11.0.

Connectez-vous à Panorama, sélectionnez **Panorama** > **Managed Collectors (Collecteurs gérés)**, et notez la version du logiciel actuel des pare-feu que vous souhaitez mettre à niveau.

Consultez Liste de contrôle de mise à niveau de PAN-OS, *les problèmes connus et les modifications apportées au comportement par défaut dans les* Release Notes (notes de version) *et* Considérations de mise à niveau/rétrogradation *pour chaque version par laquelle vous passez dans le cadre de votre chemin de mise à niveau.*

STEP 5 | (Facultatif) Mettez à niveau vos pare-feu gérés vers PAN-OS 10.1.

La fonctionnalité de mise à niveau de version logicielle ignore prend en charge les pare-feu gérés exécutant PAN-OS 10.1 ou versions ultérieures. Si vos pare-feu gérés sont sur PAN-OS 10.0 ou une version antérieure, commencez par effectuer une mise à niveau vers PAN-OS 10.1 ou une version ultérieure.

STEP 6 | Effectuez un contrôle de validation de la version.

Dans cette étape, vous pouvez afficher les images logicielles et de contenu intermédiaires requises pour effectuer la mise à niveau vers la version 11.0.

1. Sélectionnez **Panorama** > **Device Deployment (Déploiement de périphérique)** > **Software (Logiciel)** > **Action** > **Validate (Valider)**.
2. Affichez les versions intermédiaires du logiciel et du contenu que vous devez télécharger.

STEP 7 | Téléchargez les mises à jour de contenu et logicielles sur un hôte qui peut se connecter et charger les fichiers sur Panorama ou un serveur SCP configuré via SCP ou HTTPS.

Par défaut, vous pouvez charger un maximum de deux mises à jour logicielles ou de contenu de chaque type vers un appareil Panorama. Si vous téléchargez une troisième mise à jour du même type, Panorama supprimera la mise à jour de la première version de ce type. Si vous devez télécharger plus de deux mises à jour logicielles ou mises à jour de contenu d'un seul type, utilisez la commande CLI **`set max-num-images count <number>`** pour augmenter le nombre maximum d'images que Panorama peut stocker.

1. Utilisez un hôte avec accès à Internet pour ouvrir une session sur le site Web d'assistance client de Palo Alto Networks.
2. Téléchargez les mises à jour de contenu :
   1. Cliquez **Dynamic Updates (Mises à jour dynamique)** dans la section Ressources.
   2. **Download (Téléchargez)** la dernière version de contenu (ou, au minimum, la même version ou une version ultérieure que celle que vous installerez ou exécuterez sur le serveur de gestion Panorama) et enregistrez le fichier sur l'hôte ; répétez pour chaque type de contenu que vous devez mettre à jour.
3. Télécharger les mises à jour logicielles :
   1. Retour à la page principale du site de Support Clients de Palo Alto Networks et cliquez sur **Software Updates (Mises à jour de logiciel)** dans la section Ressources.
   2. Consultez la colonne Télécharger pour déterminer les versions à installer. Le nom des packages de mise à jour indique le modèle. Par exemple, pour mettre à niveau un pare-feu PA-220 et PA-5260 vers PAN-OS 11.0.0, téléchargez les images `PanOS_200-11.0.0`, `PanOS_3000-11.0.0`, et `PanOS_5000-11.0.0`.

      *Vous pouvez rapidement localiser des images PAN-OS spécifiques en sélectionnant **PAN-OS for the PA (PAN-OS pour le PA)**-<series/model> depuis le menu déroulant **Filter By (Filtrer par)**.*
4. Cliquez sur le nom du fichier approprié et enregistrez le fichier sur l'hôte.

STEP 8 | Téléchargez les versions intermédiaires du logiciel et la dernière version du contenu.

Sur PAN-OS 11.0, vous pouvez télécharger plusieurs versions intermédiaires à l'aide de la fonctionnalité de téléchargement multi-images.

1. Sélectionnez les pare-feu que vous souhaitez mettre à niveau (**Required Deployments (Déploiements requis)** > **Deploy (Déployer)**).
2. Sélectionnez une source de téléchargement et cliquez sur **Télécharger**.

STEP 9 | Installez les mises à jour de contenu sur les pare-feu gérés.

Vous devez installer les mises à jour de contenu avant les mises à jour logicielles.

Installez d'abord les mises à jour des applications ou des applications et menaces, puis installez toutes les autres mises à jour (Antivirus, WildFire® ou Filtrage d'URL) au besoin, une à la fois et dans n'importe quel ordre.

1. Sélectionnez **Panorama (Panorama)** > **Device Deployment (Déploiement du périphérique)** > **Dynamic Updates (Mises à jour dynamiques)**.
2. Cliquez sur **Upload (Charger)**, sélectionnez le **Type** de mise à jour, **Browse (Rechercher)** le fichier de mise à jour de contenu approprié, puis cliquez sur **OK**.
3. Cliquez sur **Install From File (Installer depuis le fichier)**, sélectionnez le **Type** de mise à jour et sélectionnez le **File Name (Nom du fichier)** de la mise à jour de contenu que vous venez de charger.
4. Sélectionnez les collecteurs de journaux sur lesquels installer la mise à jour.
5. Cliquez sur **OK** pour démarrer l'installation.
6. Répétez ces étapes pour chaque mise à jour de contenu.

STEP 10 | (Pare-feu servant de portails GlobalProtect™ uniquement) Chargez et activez une mise à jour du logiciel de l'agent / application GlobalProtect sur les pare-feu.

Vous activez la mise à jour sur les pare-feu, afin que les utilisateurs puissent les télécharger sur leurs points de terminaison (systèmes client).

1. Utilisez un hôte avec accès à Internet pour ouvrir une session sur le site Web d'assistance client de Palo Alto Networks.
2. Téléchargez la mise à jour du logiciel de l'agent / application GlobalProtect appropriée.
3. Sur Panorama, sélectionnez **Panorama** > **Device Deployment (Déploiement de périphériques)** > **GlobalProtect Client (Client GlobalProtect)**.
4. Cliquez sur **Upload (Charger)**, **Browse (Rechercher)** la mise à jour du logiciel de l'agent / application GlobalProtect appropriée sur l'hôte pour lequel vous avez téléchargé le fichier, puis cliquez sur **OK**.
5. Cliquez sur **Activate from File (Activer depuis le fichier)** et sélectionnez le **File Name (Nom du fichier)** de la mise à jour de l'agent / application GlobalProtect que vous venez de charger.

   Vous ne pouvez activer qu'une seule version du logiciel de l'agent / application à la fois. Si vous activez une nouvelle version mais que certains agents nécessitent une version antérieure, vous devrez réactiver à nouveau la version antérieure pour que ces agents téléchargent la mise à jour précédente.
6. Sélectionnez les pare-feu sur lesquels installer la mise à jour.
7. Cliquez sur **OK** pour l'activer.

STEP 11 | Installez PAN-OS 11.0.

Pour éviter les pannes lors de mise à jour du logiciel sur le pare-feu haute disponibilité (HD), mettez à jour un homologue HD à la fois.

Pour les pare-feu actifs / actifs, l'homologue que vous mettez à jour en premier n'a pas d'importance.

Pour les pare-feu actifs / passifs, vous devez d'abord mettre à jour l'homologue passif, suspendre l'homologue actif (basculement), mettre à jour l'homologue actif, puis ramener l'homologue actif à un état fonctionnel (retour arrière).

*(SD-WAN only (SD-WAN uniquement)) Pour conserver un état précis de vos liaisons SD-WAN, vous devez mettre à niveau vos pare-feu de concentrateur vers PAN-OS 11.0 avant de mettre à niveau vos pare-feu de succursale. La mise à jour des pare-feux de branche avant les pare-feux de plate-forme peut entraîner une mauvaise surveillance des données (**Panorama** > **SD-WAN** > **Monitoring (Surveillance)**) et les liens SD-WAN peuvent être affichés comme étant `down (en panne)` de façon erronée.*

1. Effectuez les étapes qui s'appliquent à la configuration de votre pare-feu pour installer la mise à jour logicielle de PAN-OS que vous venez de charger.
   - **Pare-feu non-HD** : cliquez sur **Install (Installer)** dans la colonne Action, sélectionnez tous les pare-feu que vous mettez à niveau, sélectionnez **Reboot device after install (Redémarrer le périphérique après l'installation)**, puis cliquez sur **OK**.
   - **Pare-feu HD actifs / actifs :**
     1. Confirmez que le paramètre de préemption est désactivé sur le premier homologue que vous avez l'intention de mettre à niveau (**Device (Périphérique)** > **High Availability (Haute Disponibilité)** > Election Settings (Paramètres d'élection)). Si activés, modifiez les **Election Settings (Paramètres d'élection)** et désactivez le paramètre **Preemptive (Préemptif)**, puis **Commit (Validez)** votre modification. Vous devez uniquement désactiver ce paramètre sur un pare-feu dans chaque paire haute disponibilité, mais assurez-vous que la validation est réussie avant de continuer.
     2. Cliquez sur **Install (Installer)**, désactivez **Group HA Peers (Regrouper les homologues HD)**, sélectionnez un homologue HD, sélectionnez **Reboot device after install (Redémarrer le périphérique après l'installation)**, puis cliquez sur **OK**. Attendez que le pare-feu termine le redémarrage avant de poursuivre.
     3. Cliquez sur **Install (Installer)**,désactivez **Group HA Peers (Regrouper les homologues HD)**, sélectionnez l'homologue HD que vous n'avez pas mis à jour à l'étape précédente, sélectionnez **Reboot device after install (Redémarrer le périphérique après l'installation)**, puis cliquez sur **OK**.
   - **Pare-feu HA actifs/passifs**: dans cet exemple, le pare-feu actif est nommé fw1 et le pare-feu passif est nommé fw2 :
     1. Vérifiez que le paramètre de préemption est désactivé sur le premier homologue que vous souhaitez mettre à niveau (**Device (Appareil)** > **High Availability (Haute disponibilité)** > Election Settings (Paramètres de choix). Si activés, modifiez les **Election Settings**

(Paramètres d'élection) et désactivez le paramètre **Preemptive (Préemptif)**, puis **Commit (Validez)** votre modification. Vous devez uniquement désactiver ce paramètre sur un pare-feu dans chaque paire haute disponibilité, mais assurez-vous que la validation est réussie avant de continuer.

2. Cliquez sur **Install (Installer)** dans la colonne Action pour la mise à jour appropriée, désactivez (effacez) **Group HA Peers (Regrouper les homologues HA)**, select fw2, **Reboot device after install (Redémarrer le périphérique après installation)**, et cliquez sur **OK**. Attendez que fw2 termine le redémarrage avant de poursuivre.
3. Après le redémarrage de fw2, vérifiez sur fw1 (**Dashboard (Tableau de bord)** > High Availability (Haute disponibilité)) que fw2 est toujours l'homologue passif (l'état du pare-feu local est `active (actif)` et l'homologue fw2 est `passive (passif)`).
4. Accédez à fw1 et **Suspend local device (Suspendre le périphérique local)** (**Device (Périphérique)** > **High Availability (Haute disponibilité)** > **Operational Commands (Commandes opérationnelles)**).
5. Accédez à fw2 (**Dashboard (Tableau de bord)** > High Availability (Haute disponibilité)) et vérifiez que l'état du pare-feu local est `active (actif)` et que l'homologue est `suspended (suspendu)`.
6. Accédez à Panorama, sélectionnez **Panorama** > **Device Deployment (Déploiement de périphériques)** > **Software (Logiciel)**, cliquez sur **Install (Installer)** dans la colonne Action de la version appropriée, désactivez

   Group HA Peers (Regrouper les homologues HD)**, sélectionnez fw1, Reboot device after install (Redémarrer le périphérique après l'installation), puis cliquez sur OK. Attendez que fw1 termine le redémarrage avant de poursuivre.**
7. Accédez à fw1 (**Device (Périphérique)** > **High Availability (haute disponibilité)** > **Operational Commands (Commandes opérationnelles)**), cliquez sur **Make local device functional (Rendre l'appareil local fonctionnel)**, et attendez deux minutes avant de continuer.
8. Sur fw1 (**Dashboard (Tableau de bord)** > High Availability (Haute disponibilité)), vérifiez que l'état du pare-feu local est `passive (passif)` et que l'homologue (fw2) est `active (actif)`.

STEP 12 | (mode FIPS-CC uniquement) Mettre à niveau Panorama et les périphériques gérés en mode FIPS-CC.

La mise à niveau d'un pare-feu géré en mode FIPS-CC nécessite que vous réinitialisiez l'état de la connexion sécurisée si vous avez ajouté le collecteur de journaux dédié à la gestion Panorama alors que le pare-feu géré exécutait une version de PAN-OS 11.0.

Vous n'avez pas besoin de réintégrer le pare-feu géré ajouté à la gestion Panorama lorsque le pare-feu géré exécutait PAN-OS 10.0 ou une version antérieure.

STEP 13 | Vérifiez que le logiciel et/ou les versions de mise à jour de contenu sont installés sur chaque pare-feu géré.

1. Sélectionnez **Panorama** > **Managed Devices (Périphériques gérés)**.
2. Localisez le pare-feu et examinez les valeurs dans les colonnes de la Version du logiciel, applications et menace, Antivirus, filtrage d'URL et Client GlobalProtect.

STEP 14 | Si vous avez désactivé la préemption sur l'un de vos pare-feu HD avant de procéder à la mise à niveau, modifiez les **Election Settings (Paramètres d'élection)** (**Device (Périphérique)** > **High Availability (Haute disponibilité)**) et réactivez le paramètre **Préemptif** pour ce pare-feu.

STEP 15 | Sur Panorama web interface (interface Web de Panorama), transférez l'ensemble de la configuration gérée de Panorama vers vos pare-feu gérés.

Cette étape est nécessaire pour activer la validation sélective et la diffusion des modifications de configuration des groupes de périphériques et des piles de modèles de Panorama vers vos pare-feu gérés.

Cela est nécessaire pour appliquer avec succès les modifications de configuration aux pare-feu multi-vsys gérés par Panorama après une mise à niveau réussie vers PAN-OS 11.0. Pour plus d'informations, consultez la modification du comportement par défaut des objets de configuration partagés pour les pare-feu multi-vsys gérés par Panorama.

1. Sélectionnez **Commit (valider)** > **Push to Devices (Appliquer aux périphériques)**.
2. **Push (Appliquer)**.

STEP 16 | Régénérez ou réimportez tous les certificats pour respecter le niveau de sécurité OpenSSL 2.

Lors de la mise à niveau vers PAN-OS 11.0, tous les certificats doivent répondre aux exigences minimales suivantes :

- RSA 2048 bits ou supérieur, ou ECDSA 256 bits ou supérieur
- Digest de SHA256 ou supérieur

Consultez le Guide de l'administrateur PAN-OS ou le Guide de l'administrateur de Panorama pour plus d'informations sur la régénération ou la réimportation de vos certificats.

STEP 17 | Affichez l'historique des mises à niveau logicielles du pare-feu.

1. Connectez-vous à l'interface Panorama.
2. Accédez à **Panorama** > **Managed Devices (appareils gérés)** > **Summary (Résumé)** et cliquez sur **Device History (Historique des appareils)**.

Mettre à niveau un pare-feu ZTP

Après avoir ajouté avec succès un pare-feu ZTP au serveur de gestion Panorama™, configurez la version PAN-OS cible du pare-feu ZTP. Panorama vérifie si la version du PAN-OS installée sur le pare-feu ZTP est postérieure ou égale à la version du PAN-OS cible configurée après sa première connexion réussie à Panorama. Si la version PAN-OS installée sur le pare-feu ZTP est antérieure à la version PAN-OS cible, alors le pare-feu ZTP entre dans un cycle de mise à jour jusqu'à ce que la version PAN-OS cible soit installée.

STEP 1 | Log in to the Panorama Web Interface (Connectez-vous à l'interface Web Panorama) en tant qu'administrateur.

STEP 2 | Add a ZTP Firewall to Panorama (Ajouter un pare-feu ZTP à Panorama).

STEP 3 | Sélectionnez **Panorama** > **Device Deployment (Déploiement de périphériques)** > **Updates (Mises à jour)** et **Check Now (Vérifiez maintenant)** pour obtenir les dernières mises à jour PAN-OS.

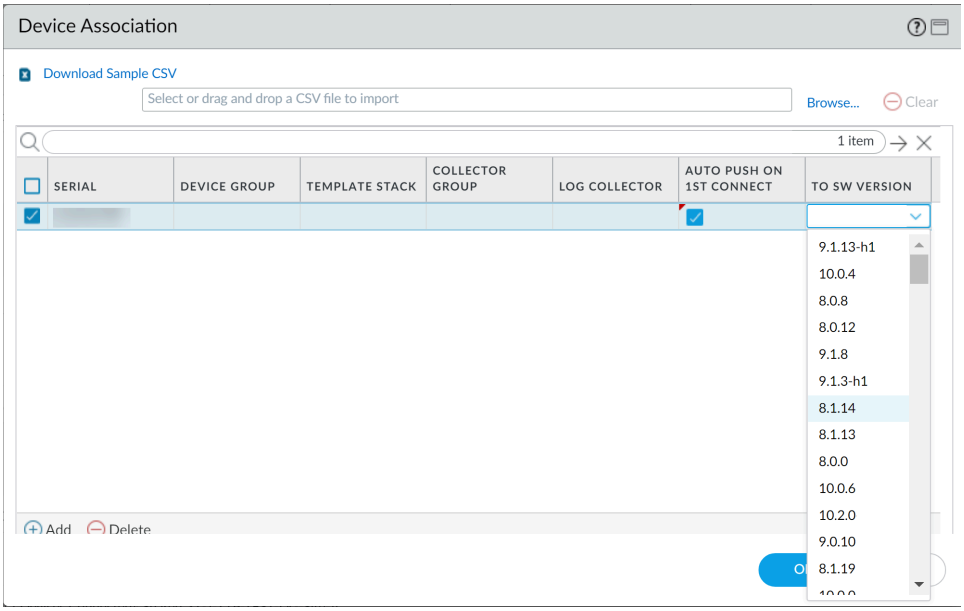
STEP 4 | Sélectionnez **Panorama** > **Managed Devices (Appareils gérés)** > **Summary (Résumé)** et sélectionnez un ou plusieurs pare-feux ZTP.

STEP 5 | **Réassocier** le(s) pare-feu(x) ZTP sélectionné(s).

STEP 6 | Cochez (activez) **Auto Push on 1st Connect (application automatique lors de la 1ère connexion)**.

STEP 7 | Dans la colonne **To SW Version (Vers la version SW)**, sélectionnez la version PAN-OS cible pour le pare-feu ZTP.

STEP 8 | Cliquez sur **OK** pour enregistrer votre configuration.



STEP 9 | Sélectionnez **Commit (Valider)** et **Commit to Panorama (Validez sur Panorama)**.

STEP 10 | Mettez le pare-feu ZTP sous tension.

Lorsque le pare-feu ZTP se connecte à Panorama pour la première fois, il passe automatiquement à la version PAN-OS que vous avez sélectionnée.

- **Panorama running PAN-OS 11.0.0 (Panorama exécutant PAN-OS 11.0.0)** — Si vous mettez à niveau des pare-feu gérés sur des versions majeures ou de maintenance de PAN-OS, les versions intermédiaires de PAN-OS sur votre chemin de mise à niveau sont installées en premier avant que la version cible de PAN-OS ne soit installée.

  Par exemple, vous avez configuré la cible **Version SW** pour le pare-feu géré en tant que PAN-OS 11.0.0 et le pare-feu exécute PAN-OS 10.1. Lors de la première connexion à Panorama, PAN-OS 10.2.0 est installé sur le pare-feu géré en premier. Après l'installation réussie de PAN-OS 10.2.0, le pare-feu est automatiquement mis à niveau vers la version PAN-OS 11.0.0 cible.
- **Panorama running PAN-OS 11.0.1 and later releases (Panorama exécutant PAN-OS 11.0.1 et versions ultérieures)** – Si vous mettez à niveau des pare-feux gérés à travers les versions majeures ou de maintenance PAN-OS, les versions majeures PAN-OS intermédiaires sur votre chemin de

mise à niveau sont installées et la version majeure PAN-OS de base est téléchargée avant que la version de maintenance PAN-OS cible ne soit installée.

Par exemple, vous avez configuré la cible **Version SW** pour le pare-feu géré en tant que PAN-OS 11.0.1 et le pare-feu exécute PAN-OS 10.0. Lors de la première connexion à Panorama, PAN-OS 10.1.0 et PAN-OS 10.2.0 sont installés sur le pare-feu géré. Après le redémarrage du pare-feu géré, PAN-OS 11.0.0 est téléchargé, puis le pare-feu s'installe automatiquement sur la version PAN-OS 11.0.1 cible.

STEP 11 | Vérifiez la mise à jour du logiciel de pare-feu ZTP.

1. Connectez-vous à l'interface Web Panorama.
2. Sélectionnez **Panorama** > **Managed Devices (Appareils gérés)** > **Summary (Résumé)** et naviguez vers le(s) pare-feu(x) ZTP.
3. Vérifiez que la colonne **Software Version (Version du logiciel)** affiche la bonne version PAN-OS cible.

STEP 12 | Pour toutes les futures mises à niveau de PAN-OS, voir Mettre à niveau le pare-feu vers PAN-OS 11.0 à partir de Panorama.

Rétrograder PAN-OS

La façon dont vous rétrogradez un pare-feu à partir de PAN-OS 11.0 dépend de si vous rétrogradez vers une version de fonctionnalité précédente (où le premier ou le deuxième chiffre de la version PAN-OS change, par exemple, de 9.1.2 à 9.0.8 ou de 9.0.3 à 8.1.14) ou si vous rétrogradez vers une version de maintenance dans la même version de fonctionnalité (où le troisième chiffre de la version de version change, par exemple, de 8.1.2 à 8.1.0). Lorsque vous passez d'une version de fonctionnalité à une version de fonctionnalité antérieure, vous pouvez migrer la configuration de la version ultérieure pour prendre en charge les nouvelles fonctionnalités. Pour migrer la configuration de PAN-OS 11.0 vers une version antérieure de PAN-OS, restaurez d'abord la configuration de la version de fonctionnalité vers laquelle vous effectuez une rétrogradation. Vous n'avez pas besoin de restaurer la configuration lorsque vous passez d'une version de maintenance à une autre au sein de la même version de fonctionnalité.

- Rétrograder un pare-feu vers une version de maintenance précédente
- Rétrograder un pare-feu vers une version de fonctionnalité précédente
- Rétrograder un agent Windows

Passez toujours à une configuration qui correspond à la version du logiciel. Des versions et des configurations logicielles inégalées peuvent entraîner des échecs de rétrogradation ou forcer le système en mode maintenance. Cela s'applique uniquement à une rétrogradation d'une fonctionnalité à une autre (par exemple de 9.0.0 à 8.1.3), pas aux rétrogradations vers des versions de maintenance au sein de la même version de fonctionnalité (par exemple, de 8.1.3 à 8.1.1).

Si vous rencontrez un problème avec une rétrogradation, vous devrez peut-être entrer en mode maintenance et réinitialiser l'appareil aux paramètres d'usine par défaut, puis restaurer la configuration à partir du fichier de configuration d'origine qui a été exporté avant la mise à niveau.

Rétrograder un pare-feu vers une version de maintenance précédente

Étant donné que les versions de maintenance n'introduisent pas de nouvelles fonctionnalités, vous pouvez revenir à une version de maintenance précédente dans la même version de fonctionnalité sans avoir à restaurer la configuration précédente. Une version de maintenance est une version dans laquelle le troisième chiffre de la version de la version change, par exemple une rétrogradation de 8.1.6 à 8.1.4 est considérée comme une rétrogradation de la version de maintenance car seul le troisième chiffre de la version de la version est différent.

Utilisez la procédure suivante pour revenir à une version de maintenance précédente dans la même version de fonctionnalité.

STEP 1 | Faites une sauvegarde du fichier de configuration actuel.

Bien que le pare-feu crée automatiquement une sauvegarde de la configuration, il convient d'effectuer une copie de sauvegarde avant de rétrograder et de l'enregistrer en externe.

1. Cliquez sur **Export named configuration snapshot (Exporter l'instantané de configuration nommé)** (**Device (Périphérique)** > **Setup (Configuration)** > **Operations (Opération)**).
2. Sélectionnez le fichier XML contenant la configuration actuelle (par exemple, **running-config.xml**), puis cliquez sur **OK** pour exporter le fichier de configuration.
3. Enregistrez le fichier exporté dans un emplacement externe au pare-feu. Vous pouvez utiliser cette sauvegarde pour restaurer la configuration en cas de problème pendant la rétrogradation.

STEP 2 | Installez l'image de la version de maintenance précédente.

Si votre pare-feu n'a pas accès à Internet à partir du port de gestion, vous pouvez télécharger la mise à jour du logiciel à partir du Palo Alto Networks Support Portal (portail d'assistance de Palo Alto Networks)*. Vous pouvez ensuite procéder au* ***Upload (téléchargement)*** *manuellement sur votre pare-feu.*

1. Cliquez sur **Check Now (Vérifier maintenant)** (**Device (Périphérique)** > **Software (Logiciel)**) pour vérifier les images disponibles.
2. Localisez l'image vers laquelle vous souhaitez procéder à la rétrogradation. Si l'image n'est pas déjà téléchargée, cliquez sur **Download (Télécharger)** pour la télécharger.
3. Une fois le téléchargement terminé, cliquez sur **Install (Installer)** pour installer l'image.
4. Une fois l'installation terminée, redémarrez en utilisant l'une des méthodes suivantes :
   - Si vous êtes invité à redémarrer, cliquez sur **Yes (Oui)**.
   - Si vous n'êtes pas invité à redémarrer, accédez à Device Operations (Opérations de périphérique) (**Device (Périphérique)** > **Setup (Configuration)** > **Operations (Opérations)**) et cliquez sur **Reboot Device (Redémarrer le périphérique)**.

Rétrograder un pare-feu vers une version de fonctionnalité précédente

Utilisez le processus suivant pour restaurer la configuration qui était en cours d'exécution avant la mise à niveau vers une autre version de fonctionnalité. Toutes les modifications apportées depuis la mise à niveau seront perdues. Il est donc important de sauvegarder votre configuration actuelle afin de pouvoir restaurer ces modifications lorsque vous reviendrez à la nouvelle version de la fonctionnalité. Passez en revue le Considérations de mise à niveau/rétrogradation avant de rétrograder un pare-feu vers une version précédente de fonctionnalité.

Pour passer de PAN-OS 11.0 à une version antérieure de PAN-OS, vous devez télécharger et installer PAN-OS 10.1.3 ou une version ultérieure de PAN-OS 11.0 avant de pouvoir continuer sur votre chemin de rétrogradation vers votre version cible de PAN-OS. La rétrogradation de PAN-OS 11.0 échoue si vous tentez de rétrograder vers PAN-OS 10.1.2 ou une version antérieure de PAN-OS 11.0.

Utilisez la procédure suivante pour procéder à la rétrogradation vers une version antérieure de la fonctionnalité.

STEP 1 | Faites une sauvegarde du fichier de configuration actuel.

Bien que le pare-feu crée automatiquement une sauvegarde de la configuration, il convient d'effectuer une copie de sauvegarde avant de mettre à niveau et de l'enregistrer en externe.

1. Cliquez sur **Export named configuration snapshot (Exporter l'instantané de configuration nommé)** (**Device (Périphérique)** > **Setup (Configuration)** > **Operations (Opération)**).
2. Sélectionnez le fichier XML contenant la configuration actuelle (par exemple, **running-config.xml**), puis cliquez sur **OK** pour exporter le fichier de configuration.
3. Enregistrez le fichier exporté dans un emplacement externe au pare-feu. Vous pouvez utiliser cette sauvegarde pour restaurer la configuration en cas de problème pendant la rétrogradation.

STEP 2 | Installez l'image de la version de fonctionnalité précédente.

Des versions de sauvegarde automatique sont créées lors de la mise à niveau vers une nouvelle version.

1. Cliquez sur **Check Now (Vérifier maintenant)** (**Device (Périphérique)** > **Software (Logiciel)**) pour vérifier les images disponibles.
2. Installer PAN-OS 10.1.

   La mise à niveau de PAN-OS 11.0 vers une version de fonctionnalité précédente nécessite que vous passiez d'abord à PAN-OS 10.1.3 ou version ultérieure de PAN-OS 11.0. Après avoir réussi la mise à niveau vers la version PAN-OS 10.1.3 ou ultérieure de PAN-OS 11.0, vous pouvez continuer la mise à niveau vers votre version PAN-OS cible.

   1. Recherchez et **Download (téléchargez)** l'image PAN-OS 11.0.
   2. **Installez** l'image PAN-OS 11.0.
3. Localisez l'image PAN-OS cible vers laquelle vous souhaitez rétrograder. Si l'image n'est pas déjà téléchargée, cliquez sur **Download (Télécharger)** pour la télécharger.
4. Une fois le téléchargement terminé, cliquez sur **Install (Installer)** pour installer l'image.
5. Cliquez sur **Select a Config File for Downgrading (Sélectionner un fichier de configuration pour la rétrogradation)** pour sélectionner le fichier que le pare-feu chargera après le redémarrage du périphérique. Dans la plupart des cas, vous devez sélectionner la configuration qui a été enregistrée automatiquement lors de la mise à niveau à partir de la version vers laquelle vous effectuez maintenant la rétrogradation. Par exemple, si vous exécutez PAN-OS 11.0 et que vous procédez à une rétrogradation vers PAN-OS 10.2.2, sélectionnez `autosave-10.2.2`.
6. Une fois l'installation terminée, redémarrez en utilisant l'une des méthodes suivantes :
   - Si vous êtes invité à redémarrer, cliquez sur **Yes (Oui)**.
   - Si vous n'êtes pas invité à redémarrer, accédez à Device Operations (Opérations de périphérique) (**Device (Périphérique)** > **Configuration** > **Operations (Opérations)**) et cliquez sur **Reboot Device (Redémarrer le périphérique)**.

Rétrograder un agent Windows

Après avoir désinstallé l'agent d'ID utilisateur Windows PAN-OS 11.0, effectuez les étapes suivantes avant d'installer une version antérieure de l'agent.

STEP 1 | Ouvrez le menu Démarrer de Windows et sélectionnez **Administrative Tools (Outils d'administration)**.

STEP 2 | Sélectionnez **Computer Management (Gestion de l'ordinateur)** > **Services and Applications (services et applications)** > **Services** et double-cliquez sur **User-ID Agent (Agent de l'ID de l'utilisateur).**

STEP 3 | Sélectionnez **Log on (Connexion)**, sélectionnez **This account (Ce compte)** et spécifiez le nom d'utilisateur pour le compte de l'agent User-ID.

STEP 4 | Saisissez le **Password (Mot de passe)** et **Confirm Password (Confirmez le mot de passe)**.

STEP 5 | Cliquez sur **OK** pour enregistrer vos modifications.

Dépannez votre mise à niveau PAN-OS

Pour dépanner votre mise à niveau PAN-OS, utilisez le tableau suivant pour examiner les problèmes possibles et comment les résoudre.

Symptôme	Résolution
La licence de garantie du logiciel a expiré.	À partir de la CLI, supprimez la clé de licence expirée : 1. Entrez **`delete licence key (supprimer la clé de licence)<software license key>`**. 2. Entrez **`delete license key Software_Warranty<expiredate>.key`**.
Les dernières versions du logiciel PAN-OS n'étaient pas disponibles.	Vous ne pouvez voir que les versions logicielles qui sont une version de fonctionnalité avant la version installée actuelle. Par exemple, si une version 8.1 est installée, seules les versions 9.0 seront disponibles. Pour voir les versions 9.1, vous devez d'abord effectuer une mise à niveau vers la version 9.0.
La vérification des mises à jour dynamiques a échoué.	Ce problème se produit en raison d'une erreur de connectivité réseau. Voir l'article de la base de connaissances Dynamic Updates Display Error After Clicking On Check Now Button (Erreur d'affichage des mises à jour dynamiques après avoir cliqué sur le bouton Vérifier maintenant).
Aucun certificat d'appareil valide n'a été trouvé.	Dans PAN-OS 9.1.3 et les versions ultérieures, un certificat de périphérique doit être installé si vous utilisez un service cloud de Palo Alto Networks. Pour installer le certificat d'appareil : 1. Ouvrez une session dans le portail de support client. 2. Sélectionnez **Generate OTP (Générer OTP)** (**Assets (Actifs)** > **Device Certificates (Certificats des appareils)**). 3. Pour le **Device Type (Type de périphérique)**, sélectionnez **Generate OTP for Next-Gen Firewalls (Générer un OTP pour les pare-feux nouvelle génération)**. 4. Sélectionnez votre numéro de série du périphérique PAN-OS.

Symptôme	Résolution
	5. **Generate OTP (Générer OTP)** et copiez le Mot de passe à usage unique. 6. Connectez-vous au pare-feu en tant qu'utilisateur administrateur. 7. Sélectionnez **Device Certificate (certificat du périphérique)** (**Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** > **Device (Périphérique)** > **Certificate (Certificat)** et **Get Certificate (Obtenir un certificat)**. 8. Collez l'OTP et cliquez sur **OK.**
Le fichier image du logiciel n'a pas pu être chargé sur le gestionnaire de logiciels en raison d'une erreur d'authentification de l'image.	Pour mettre à jour la liste des images logicielles, cliquez sur **Check Now (Vérifier maintenant)**. Cela établit une nouvelle connexion au serveur de mise à jour.
La version du plug-in VMware NSX n'était pas compatible avec la nouvelle version du logiciel.	Le plug-in VMware NSX a été automatiquement installé lors de la mise à niveau vers la version 8.0. Si vous n'utilisez pas le plugin, vous pouvez le désinstaller.
Le temps de redémarrage après la mise à niveau vers PAN-OS 9.1 était plus long que prévu.	Mettez à niveau vers la version de publication du contenu des applications et des menaces 8221 ou une version ultérieure. Pour plus d'informations sur les versions minimales de logiciel et de contenu, voir <xref to 11.0 Associated Software and Content Versions>.
L'appareil n'a pas pris en charge même lorsque les licences sont actives.	Dans **Device (Périphérique)** > **Software (Logiciel)**, cliquez sur **Check Now (Vérifier maintenant)**. Cela met à jour les informations de licence sur le pare-feu en établissant une nouvelle connexion au serveur de mise à jour. Si cela ne fonctionne pas à partir de l'interface Web, utilisez la **`request system software check (vérification du logiciel système de demande)`**.
Le pare-feu n'avait pas d'adresse DHCP attribuée par le serveur DHCP.	Configurez une règle de politique de sécurité autorisant le trafic du serveur DHCP du FAI vers les réseaux internes.

Symptôme	Résolution
Le pare-feu démarre en permanence en mode maintenance.	Dans l’interface de ligne de commande,Accédez au Maintenance Recovery Tool (Outil de récupération après maintenance ; MRT) Dans la fenêtre MRT, sélectionnez **Continue (Continuer)** > **Disk image (image du disque)**. Sélectionnez soit **Reinstall (Réinstaller)** <current version>ou **Revert to (Revenir à)**<previous version>. Une fois l'opération de restauration ou de réinstallation terminée, sélectionnez **Reboot (Redémarrer)**.
Dans une configuration HA, le pare-feu passe en état suspendu après la mise à niveau du pare-feu homologue avec une erreur indiquant que le pare-feu est trop ancien.	La mise à niveau d'un pare-feu vers une version qui précède plusieurs versions majeures entraînera une panne du réseau. Vous devez mettre à niveau les deux pare-feux une seule version majeure à l'avance avant de passer à la prochaine version majeure. Rétrogradez le pare-feu homologue vers la version à laquelle le pare-feu suspendu s'est arrêté.

Mise à niveau du pare-feu VM-Series

Mettre à niveau le logiciel PAN-OS de la série VM (autonome)

Passez en revue les nouvelles fonctionnalités, les problèmes résolus et les problèmes connus, puis utilisez la procédure suivante pour mettre à niveau un pare-feu qui n'est pas dans une configuration HA.

Pour éviter tout impact sur le trafic, procédez à la mise à niveau pendant l'intervalle d'interruption. Assurez-vous que le pare-feu est branché à une source d'alimentation fiable. La perte de courant au cours d'une mise à niveau peut rendre ls pare-feu inutilisable.

STEP 1 | Vérifiez que suffisamment de ressources matérielles sont disponibles pour le pare-feu VM-Series.

Reportez-vous à la Configuration système requise pour VM-Series pour voir les nouvelles exigences de ressources applicables à chaque modèle VM-Series. Allouez des ressources matérielles supplémentaires avant de poursuivre le processus de mise à niveau. Le processus d'allocation de ressources matérielles supplémentaires diffère selon chaque hyperviseur.

Si le pare-feu VM-Series ne dispose pas des ressources requises pour le modèle, sa capacité par défaut correspond à la capacité associée au VM-50.

STEP 2 | Dans l'interface Web, sélectionnez **Device (Périphérique)** > **Licenses (Licences)** et vérifiez que vous disposez de la licence correcte pour le pare-feu VM-Series et qu'elle est activée.

Sur le pare-feu VM-Series version autonome, accédez à **Device (Périphérique)** > **Support** et vérifiez que vous avez activé la licence de support.

STEP 3 | Faites une sauvegarde du fichier de configuration actuel.

Bien que le pare-feu crée automatiquement une sauvegarde de la configuration, il est recommandé de créer et de stocker une sauvegarde externe avant de procéder à la mise à niveau.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Operations (Opérations)**, puis cliquez sur **Export named configuration snapshot (Exporter l'instantané de configuration nommé)**.
2. Sélectionnez le fichier XML contenant la configuration actuelle (par exemple, **running-config.xml**), puis cliquez sur **OK** pour exporter le fichier de configuration.
3. Enregistrez le fichier exporté dans un emplacement externe au pare-feu. Vous pouvez utiliser cette sauvegarde pour restaurer la configuration en cas de problème pendant la mise à niveau.

STEP 4 | Si vous avez activé User-ID, après la mise à niveau, le pare-feu efface les mappages nom d'utilisateur/adresse IP et de groupe, afin que ces champs puissent être complétés avec les attributs

depuis les sources User-ID. Pour estimer le temps nécessaire pour que votre environnement complète à nouveau les mappages, exécutez les commandes CLI suivantes sur le pare-feu.

- Pour les mappages nom d'utilisateur/adresse IP :
  - **`show user user-id-agent state all`**
  - **`show user server-monitor state all`**
- Pour les mappages de groupe : **`show user group-mapping statistics`**

STEP 5 | Assurez-vous que le pare-feu exécute la dernière version du contenu.

1. Sélectionnez **Device (Périphérique)** > **Dynamic Updates (Mise à jour dynamiques)** et vérifiez les **Applications** ou **Applications and Threats (Applications et menaces)** pour déterminer la mise à jour qui est actuellement installée.
2. Si le pare-feu n'exécute pas la dernière version du contenu requise ou une version supérieure requise pour PAN-OS, cliquez sur **Check Now (Vérifier maintenant)** pour consulter la liste des mises à jour disponibles.
3. Trouvez et **téléchargez** la version du contenu souhaitée.

   Après avoir téléchargé avec succès un fichier de mise à jour du contenu, le lien dans la colonne Action passe de **Télécharger** à **Installer** pour cette version du contenu.
4. **Installez** la mise à jour.

STEP 6 | Mise à niveau du plug-in VM-Series.

1. Avant de procéder à la mise à niveau, consultez les dernières notes de version pour savoir si un nouveau plug-in VM-Series affecte votre environnement.

   Par exemple, supposons qu'une nouvelle version de plug-in VM-Series n'inclue que les fonctionnalités AWS. Pour tirer parti des nouvelles fonctionnalités, vous devez mettre à jour le plug-in sur vos instances de pare-feu VM-Series sur AWS.

   N'installez aucune mise à niveau qui ne s'applique pas à votre environnement.
2. Connectez-vous au pare-feu VM-Series et consultez le tableau de bord pour afficher la version du plug-in.
3. Sélectionnez **Device (Périphérique)** > **Plugins (Plug-ins)** pour savoir la version du plug-in. Utilisez **Check Now** (Vérifier maintenant) pour rechercher des mises à jour.
4. Sélectionnez la version du plug-in et cliquez sur **Install (Installer)** dans la colonne Action pour installer le plug-in.

STEP 7 | Mettez à jour PAN-OS.

Si votre pare-feu ne possède pas d'accès Internet depuis le port de gestion, vous pouvez télécharger l'image logicielle depuis le portail d'assistance client Palo Alto Networks*, puis le* ***charger*** *manuellement sur votre pare-feu.*

1. Sélectionnez **Device (Périphérique)** > **Software (Logiciel)** et cliquez sur **Check Now (Vérifier maintenant)** pour afficher les dernières mises à jour PAN-OS.
2. Trouvez et **téléchargez** la version du PAN-OS cible.
3. Après avoir téléchargé l'image (ou après avoir chargé l'image pour une mise à niveau manuelle), **installez** l'image.
4. Une fois l'installation terminée, redémarrez en utilisant l'une des méthodes suivantes :
   - Si vous êtes invité à redémarrer, cliquez sur **Yes (Oui)**.
   - Si vous n'êtes pas invité à redémarrer, sélectionnez **Device (Périphérique)** > **Configuration** > **Operations (Opérations)** et cliquez sur **Reboot Device (Redémarrer le périphérique)**.

   Le pare-feu efface alors les mappages User-ID, puis se connecte aux sources User-ID pour remplir à nouveau les mappages.
5. Si vous avez activé User-ID, utilisez les commandes CLI suivantes pour vérifier que le pare-feu a rempli à nouveau les mappages adresse IP/nom d'utilisateur et de groupe avant d'autoriser le trafic.
   - `show user ip-user-mapping all`
   - `show user group list`
6. Si vous mettez à niveau vers une version XFR pour la première fois, répétez cette étape pour mettre à niveau vers la version XFR correspondante.

STEP 8 | Vérifiez que le pare-feu fait passer le trafic.

Sélectionnez **Monitor (Surveiller)** > **Session Browser (Navigateur de session)** et vérifiez que vous voyez de nouvelles sessions.

Mise à niveau du logiciel PAN-OS VM-Series (paire HA)

Utilisez la procédure suivante pour mettre à jour une paire de pare-feu dans une configuration de haute disponibilité (High Availability - HA). Cette procédure s'applique aussi bien aux configurations actives/passives qu'actives/actives.

Pour éviter les temps d'arrêt lors de la mise à niveau des pare-feu qui sont en configuration de disponibilité élevée, mettre à jour un pair HA à la fois : Pour les pare-feu actifs/actifs, l'homologue que vous mettez à niveau en premier n'a pas d'importance (même si cette procédure explique comment mettre à niveau l'homologue secondaire actif en premier, dans un souci de simplicité). Pour les pare-feu actifs / passifs, vous devez d'abord mettre à niveau l'homologue passif, suspendre l'homologue actif (basculement), mettre à jour l'homologue actif, puis ramener cet homologue à un état fonctionnel (retour arrière). Afin d'éviter un basculement lors de la mise à niveau des homologues HA, assurez-vous que la préemption est désactivée avant de poursuivre la mise à niveau. Vous devez uniquement désactiver la préemption sur un homologue de la paire.

Pour éviter tout impact sur le trafic, procédez à la mise à niveau pendant l'intervalle d'interruption. Assurez-vous que les pare-feu sont branchés à une source d'alimentation fiable. La perte de courant au cours d'une mise à niveau peut rendre les pare-feu inutilisables.

STEP 1 | Vérifiez que suffisamment de ressources matérielles sont disponibles pour le pare-feu VM-Series.

Reportez-vous à la Configuration système requise pour VM-Series pour voir les nouvelles exigences de ressources applicables à chaque modèle VM-Series. Allouez des ressources matérielles supplémentaires avant de poursuivre le processus de mise à niveau. Le processus d'allocation de ressources matérielles supplémentaires diffère selon chaque hyperviseur.

Si le pare-feu VM-Series ne dispose pas des ressources requises pour le modèle, sa capacité par défaut correspond à la capacité associée au VM-50.

STEP 2 | Dans l'interface Web, sélectionnez **Device (Périphérique)** > **Licenses (Licences)** et vérifiez que vous disposez de la licence correcte pour le pare-feu VM-Series et qu'elle est activée.

Sur le pare-feu VM-Series version autonome, accédez à **Device (Périphérique)** > **Support** et vérifiez que vous avez activé la licence de support.

STEP 3 | Faites une sauvegarde du fichier de configuration actuel.

Bien que le pare-feu crée automatiquement une sauvegarde de la configuration, il est recommandé de créer et de stocker une sauvegarde externe avant de procéder à la mise à niveau.

Effectuez ces étapes sur chaque pare-feu dans la paire :

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Operations (Opérations)**, puis cliquez sur **Export named configuration snapshot (Exporter l'instantané de configuration nommé)**.
2. Sélectionnez le fichier XML contenant la configuration actuelle (par exemple, **running-config.xml**), puis cliquez sur **OK** pour exporter le fichier de configuration.
3. Enregistrez le fichier exporté dans un emplacement externe au pare-feu. Vous pouvez utiliser cette sauvegarde pour restaurer la configuration en cas de problème pendant la mise à niveau.

STEP 4 | Si vous avez activé User-ID, après la mise à niveau, le pare-feu efface les mappages nom d'utilisateur/adresse IP et de groupe, afin que ces champs puissent être complétés avec les attributs depuis les sources User-ID. Pour estimer le temps nécessaire pour que votre environnement complète à nouveau les mappages, exécutez les commandes CLI suivantes sur le pare-feu.

- Pour les mappages nom d'utilisateur/adresse IP :
  - **`show user user-id-agent state all`**
  - **`show user server-monitor state all`**
- Pour les mappages de groupe : **`show user group-mapping statistics`**

STEP 5 | Assurez-vous que chaque pare-feu dans la paire HA exécute la dernière version du contenu.

Consultez les Release Notes (Notes de publication) de la version minimale de contenu que vous devez installer pour une version de PAN-OS 11.0. Assurez-vous de suivre les meilleures pratiques pour les mises à jour du contenu de menace et des applications.

1. Sélectionnez **Device (Périphérique)** > **Dynamic Updates (Mise à jour dynamiques)** et vérifiez les **Applications** ou **Applications and Threats (Applications et menaces)** pour déterminer la mise à jour qui est actuellement installée.
2. Si les pare-feu n'exécutent pas la dernière version du contenu requise ou une version supérieure requise pour la version logicielle que vous installez, cliquez sur **Check Now (Vérifier maintenant)** pour consulter la liste des mises à jour disponibles.
3. Trouvez et **téléchargez** la version du contenu souhaitée.

   Après avoir téléchargé avec succès un fichier de mise à jour du contenu, le lien dans la colonne Action passe de **Télécharger** à **Installer** pour cette version du contenu.
4. **Installez** la mise à jour. Vous devez installer la mise à jour sur les deux homologues.

STEP 6 | Mise à niveau du plug-in VM-Series.

1. Avant de procéder à la mise à niveau, consultez les dernières notes de version pour savoir si un nouveau plug-in VM-Series affecte votre environnement.

   Par exemple, supposons qu'une nouvelle version de plug-in VM-Series n'inclue que les fonctionnalités AWS. Pour tirer parti des nouvelles fonctionnalités, vous devez mettre à jour le plug-in sur vos instances de pare-feu VM-Series sur AWS.

   N'installez aucune mise à niveau qui ne s'applique pas à votre environnement.

2. Connectez-vous au pare-feu VM-Series et consultez le tableau de bord pour afficher la version du plug-in.
3. Sélectionnez **Device (Périphérique)** > **Plugins (Plug-ins)** pour savoir la version du plug-in. Utilisez **Check Now** (Vérifier maintenant) pour rechercher des mises à jour.
4. Sélectionnez la version du plug-in et cliquez sur **Install (Installer)** dans la colonne Action pour installer le plug-in.

   Lors de l'installation de la fiche sur les pare-feu VM-Series d'une paire HA, installez la fiche sur le pair passif avant le pair actif. Après avoir installé le plug-in sur l'homologue passif, il passera à un état non fonctionnel. L'installation du plug-in sur l'homologue actif renvoie l'homologue passif à un état fonctionnel.

STEP 7 | Désactivez la préemption sur le premier homologue de chaque paire. Vous devez uniquement désactiver ce paramètre sur un pare-feu dans la paire HA, mais assurez-vous que la validation est réussie avant de continuer la mise à niveau.

1. Sélectionnez **Device (Périphérique)** > **High Availability (Haute disponibilité)** et modifiez les **Election Settings (Paramètres de sélection)**.
2. si cette option est activée, désactivez (effacez) le **Preemptive (paramètre préemptif)** et cliquez sur **OK**.
3. **Commit (Validez)** la modification.

STEP 8 | Installez la version du logiciel PAN-OS sur le premier homologue.

Afin de réduire l'interruption dans une configuration active/passive, mettez à niveau l'homologue passif en premier. Pour une configuration active/active, mettez à niveau l'homologue secondaire en

premier. Si vous utilisez une configuration active/active, nous vous conseillons en guise de bonne pratique de mettre à niveau les deux homologues lors du même intervalle de maintenance.

Si vous souhaitez vérifier que l'HA fonctionne correctement avant la mise à niveau, mettez à niveau l'homologue actif dans une configuration active/passive en premier afin de vous assurer que le basculement se déroule parfaitement.

1. Pour le premier homologue, sélectionnez **Device (Périphérique)** > **Software (Logiciel)** et cliquez sur **Check Now (Vérifier maintenant)** pour les dernières mises à jour.
2. Trouvez et **téléchargez** la version du PAN-OS cible.

   Si votre pare-feu ne possède pas d'accès Internet depuis le port de gestion, vous pouvez télécharger l'image logicielle depuis le portail d'assistance Palo Alto Networks*, puis le* ***charger*** *manuellement sur votre pare-feu.*
3. Après avoir téléchargé l'image (ou après avoir chargé l'image pour une mise à niveau manuelle), **installez** l'image.
4. Une fois l'installation terminée, redémarrez en utilisant l'une des méthodes suivantes :
   - Si vous êtes invité à redémarrer, cliquez sur **Yes (Oui)**.
   - Si vous n'êtes pas invité à redémarrer, sélectionnez **Device (Périphérique)** > **Configuration** > **Operations (Opérations)** et **Reboot Device (Redémarrez le périphérique)**.
5. Une fois que le périphérique a terminé le redémarrage, consultez le widget Haute disponibilité sur le **Dashboard (Tableau de bord)** et vérifiez que le périphérique que vous venez de mettre à jour est toujours l'homologue passif ou actif-secondaire dans la configuration HA.

STEP 9 | Installez la version du logiciel PAN-OS sur le deuxième homologue.

1. (Configurations actives/passives uniquement) Suspendez l'homologue actif afin que l'HA bascule vers l'homologue que vous venez de mettre à jour.
   1. Pour l'homologue actif, sélectionnez **Device (Équipement)** > **High Availability (Haute disponibilité)** > **Operational Commands (Commandes opérationnelles)**, puis cliquez sur le lien **Suspend local device (Suspendre le périphérique local)**.
   2. Consultez le widget High Availability (haute disponibilité - HA) sur le **Dashboard (Tableau de bord)** et vérifiez que l'état passe à **Passive (Passif)**.
   3. Vérifiez que l'autre homologue est actif et fait passer le trafic (**Monitor (Surveiller)** > **Session Browser (Navigateur de session)**).
2. Pour le deuxième homologue, sélectionnez **Device (Périphérique)** > **Software (Logiciel)** et cliquez sur **Check Now (Vérifier maintenant)** pour les dernières mises à jour.
3. Trouvez et **téléchargez** la version du PAN-OS cible.
4. Une fois que vous avez téléchargé l'image, **installez**-la.
5. Une fois l'installation terminée, redémarrez en utilisant l'une des méthodes suivantes :
   - Si vous êtes invité à redémarrer, cliquez sur **Yes (Oui)**.
   - Si vous n'êtes pas invité à redémarrer, sélectionnez **Device (Périphérique)** > **Configuration** > **Operations (Opérations)** et **Reboot Device (Redémarrez le périphérique)**.
6. (Configurations actives/passives uniquement) À partir de la CLI de l'homologue que vous venez de mettre à niveau, exécutez la commande suivante pour rendre le pare-feu de nouveau fonctionnel :

   ```
   request high-availability state functional (demande de fonctionnement d'état de haute disponibilité)
   ```


STEP 10 | Vérifiez que les deux homologues font passer le trafic comme prévu.

Dans une configuration active/passive, seul l'homologue actif doit faire passer le trafic ; les deux homologues doivent faire passer le trafic dans une configuration active/active.

Exécutez les commandes CLI suivantes pour confirmer la réussite de la mise à niveau :

- (Homologues actifs uniquement) Pour vérifier que les homologues actifs font passer le trafic, exécutez la commande **`show session all (Montrer toutes les sessions)`** command.
- Pour vérifier la synchronisation des sessions, exécutez la **`show high-availability interface ha2`** et assurez-vous que les compteurs d'interface matérielle de la table du processeur augmentent comme suit :
  - Dans une configuration active/passive, seul l'homologue actif affiche les paquets transmis ; l'homologue passif affiche uniquement les paquets reçus.

    Si vous avez activé HA2 keep-alive (Maintien HA2), les compteurs d'interface matérielle sur l'homologue passif affichent à la fois les paquets de transmission et de réception. Cela se produit car HA2 keep-alive (Maintien HA2) est bidirectionnel, ce qui signifie que les deux homologues transmettent des paquets HA2 keep-alive (Maintien HA2).
  - Dans la configuration active/active, les paquets reçus et les paquets transmis s'affichent sur les deux homologues.

STEP 11 | Si vous avez désactivé la préemption avant la mise à niveau, vous pouvez maintenant la réactiver.

1. Sélectionnez **Device (Périphérique)** > **High Availability (Haute disponibilité)** et modifiez les **Election Settings (Paramètres de sélection)**.
2. Sélectionnez **Preemptive (Préemptif)** et cliquez sur **OK**.
3. **Commit (Validez)** la modification.

Mise à niveau du logiciel VM-Series PAN-OS à l'aide de Panorama

Utilisez la procédure suivante pour mettre à niveau les pare-feu que vous gérez avec Panorama. Cette procédure s'applique aux pare-feu autonomes et aux pare-feu déployés dans une configuration à haute disponibilité (HA).

Si Panorama ne parvient pas à se connecter directement au serveur de mises à jour, suivez la procédure pour déployer des mises à jour des pare-feu lorsque Panorama n'est pas connecté à Internet *afin de pouvoir télécharger manuellement des images dans Panorama, puis les distribuer les images sur le pare-feu.*

Avant de faire la mise-à-jour du pare-feu sur Panorama, vous devez :

- Assurez-vous que Panorama exécute la même version ou une version ultérieure de PAN-OS que celle utilisée pour la mise à niveau. Vous devez mettre à niveau Panorama et ses Log Collectors (Collecteurs de journaux) vers la version 9.1 avant de mettre à niveau les pare-feu gérés vers cette version. Lorsque vous mettez à niveau les collecteurs de journaux vers la version 9.1, vous devez mettre à niveau tous les collecteurs de journaux en même temps en raison des modifications de l'infrastructure de journalisation.
- Prévoyez un intervalle de maintenance prolongée, qui peut durer six heures, pour la mise à niveau de Panorama vers la version 9.1. Cette version comprend des modifications importantes au niveau de l'infrastructure, ce qui signifie que la mise à niveau de Panorama prendra plus de temps que pour les versions précédentes.
- Assurez-vous que les pare-feu sont branchés à une source d'alimentation fiable. La perte de courant au cours d'une mise à niveau peut rendre les pare-feu inutilisables.

STEP 1 | Après avoir mis Panorama à niveau, validez et appliquez la configuration aux pare-feu que vous prévoyez de mettre à niveau.

STEP 2 | Vérifiez que suffisamment de ressources matérielles sont disponibles pour le pare-feu VM-Series.

Reportez-vous à la Configuration système requise pour VM-Series pour voir les nouvelles exigences de ressources applicables à chaque modèle VM-Series. Allouez des ressources matérielles supplémentaires avant de poursuivre le processus de mise à niveau. Le processus d'allocation de ressources matérielles supplémentaires diffère selon chaque hyperviseur.

Si le pare-feu VM-Series ne dispose pas des ressources requises pour le modèle, sa capacité par défaut correspond à la capacité associée au VM-50.

STEP 3 | Dans l'interface Web, sélectionnez **Device (Périphérique)** > **Licenses (Licences)** et vérifiez que vous disposez de la licence correcte pour le pare-feu VM-Series et qu'elle est activée.

Sur le pare-feu VM-Series version autonome, accédez à **Device (Périphérique)** > **Support** et vérifiez que vous avez activé la licence de support.

STEP 4 | Effectuez une copie de sauvegarde du fichier de configuration actuel sur chaque pare-feu géré que vous envisagez de mettre à niveau.

Bien que le pare-feu crée automatiquement une sauvegarde de la configuration, il est recommandé de créer et de stocker une sauvegarde externe avant de procéder à la mise à niveau.

1. À partir de l'interface web de Panorama, sélectionnez **Panorama** > **Setup (Configuration)** > **Operations (Opérations)** et cliquez sur **Export Panorama and devices config bundle (Exporter le groupe de configuration des périphériques et de Panorama)** pour générer et exporter la dernière sauvegarde de configuration de Panorama et de chaque appareil géré.
2. Enregistrez le fichier exporté dans un emplacement externe au pare-feu. Vous pouvez utiliser cette sauvegarde pour restaurer la configuration en cas de problème pendant la mise à niveau.

STEP 5 | Mettez à jour la version de contenu sur les pare-feu que vous prévoyez de mettre à niveau.

Consultez les Release Notes (Notes de publication) de la version minimale de contenu que vous devez installer pour PAN-OS 11.0. Assurez-vous que vous utilisez les meilleures pratiques pour les mises à jour d'applications et de menaces lorsque vous déployez des mises à jour de Panorama et des pare-feu que vous gérez.

1. Sélectionnez **Panorama** > **Device Deployment (Déploiement de périphériques)** > **Dynamic Updates (Mises à jour dynamiques)** et **Check Now (Vérifiez maintenant)** pour obtenir les dernières mises à jour. Si une mise à jour est disponible, la colonne Action affiche un lien **Download (Télécharger)**.
2. Si elle n'est pas déjà installée, **Download (Téléchargez)** la dernière version du contenu.
3. Cliquez sur **Install (Installer)** et sélectionnez les pare-feu sur lesquels vous voulez installer la mise à jour et cliquez sur **OK**. Si vous mettez à niveau des pare-feu HA, vous devez mettre à jour le contenu des deux homologues.

STEP 6 | (Mises à niveau du pare-feu HA uniquement) Si vous mettez à niveau des pare-feu faisant partie d'une paire haute disponibilité, désactivez la préemption. Vous devez uniquement désactiver ce paramètre sur un pare-feu dans chaque paire haute disponibilité.

1. Sélectionnez **Device (Périphérique)** > **High Availability (Haute disponibilité)** et modifiez les **Election Settings (Paramètres de sélection)**.
2. si cette option est activée, désactivez (effacez) le **Preemptive (paramètre préemptif)** et cliquez sur **OK**.
3. **Commit (Validez)** la modification. Assurez que la validation est un succès avant de procéder à la mise-à-jour.

STEP 7 | Téléchargez l'image de version cible de PAN-OS.

1. Sélectionnez **Panorama** > **Device Deployment (Déploiement de périphériques)** > **Software (Logiciel)** et **Check Now (Vérifiez maintenant)** pour obtenir les dernières versions.
2. **Download (Téléchargez)** le(s) fichier(s) spécifique du pare-feu pour la version finale vers laquelle vous effectuez la mise à niveau. Vous devez télécharger un fichier d'installation distinct pour chaque modèle de pare-feu (ou série de pare-feu) que vous avez l'intention de mettre à niveau.

STEP 8 | Installer la mise à jour logicielle PAN-OS sur les pare-feu.

1. Cliquez sur **Install (Installer)** dans la colonne Action correspondant aux modèles de pare-feu que vous souhaitez mettre à niveau.
2. Dans la boîte de dialogue Déployer le fichier logiciel, sélectionnez tous les pare-feu que vous souhaitez mettre à niveau. Pour réduire les temps d'arrêt, sélectionnez uniquement un pair dans chaque paire HA. Pour les paires actives / passives, sélectionnez l'homologue passif; pour les paires actives / actives, sélectionnez l'homologue actif-secondaire.
3. (Mises à niveau des pare-feu HA uniquement) Assurez-vous que le **Group HA Peers (Groupe d’homologues HA)** n’est pas sélectionné.
4. Sélectionnez **Reboot device after install (Redémarrer le périphérique après l’installation)**.
5. Pour débuter la mise à jour, cliquez sur **OK**.
6. Une fois l’installation terminée, redémarrez en utilisant l’une des méthodes suivantes :
   - Si vous êtes invité à redémarrer, cliquez sur **Yes (Oui)**.
   - Si vous n’êtes pas invité à redémarrer, sélectionnez **Device (Périphérique)** > **Configuration** > **Operations (Opérations)** et **Reboot Device (Redémarrez le périphérique)**.
7. Après que le pare-feu a terminé le redémarrage, sélectionnez **Panorama** > **Managed Devices (Périphériques gérés)** et vérifiez que la version du logiciel est 9.1.0 pour les pare-feux que vous avez mis à niveau. Vérifiez également que le statut HA de tous les pare-feu passifs mis à niveau est toujours passif.

STEP 9 | (Mise à niveau des pare-feu HA uniquement) Mettez à niveau le deuxième pair HA dans chaque paire HA.

1. (Mises à niveau active/passive uniquement) Suspendez le périphérique actif dans chaque paire active / passive que vous mettez à niveau.
   1. Basculez le contexte vers le pare-feu actif.
   2. Dans le widget de haute disponibilité sur le **Dashboard (Tableau de bord)**, vérifiez que l'état du pare-feu **Local** est **Active (Actif)** et que le **Peer (Homologue)** est **Passive (Passif)**).
   3. Sélectionnez **Device (Périphérique)** > **High Availability (Haute disponibilité)** > **Operational Commands (Commandes opérationnelles)** > **Suspend local device (Suspendre le périphérique local)**.
   4. Revenez au widget Haute disponibilité sur le **Dashboard (Tableau de bord)** et vérifiez que **Local** est passé à **Passive (Passif)** et que **Peer (Homologue)** est passé à **Active (Actif)**.
2. Retournez sur Panorama et sélectionnez **Panorama** > **Device Deployment (Déploiement de périphériques)** > **Software (Logiciel)**.
3. Cliquez sur **Install (Installer)** dans la colonne Action correspondant aux modèles de HA que vous souhaitez mettre à niveau.
4. Dans la boîte de dialogue Déployer le fichier logiciel, sélectionnez tous les pare-feu que vous souhaitez mettre à niveau. Cette fois, sélectionnez uniquement les homologues des pare-feu HA que vous venez de mettre à jour.
5. Assurez-vous que le **Group HA Peers (Groupe de paire HA)** n'est pas sélectionné.
6. Sélectionnez **Reboot device after install (Redémarrer le périphérique après l'installation)**.
7. Pour débuter la mise à jour, cliquez sur **OK**.
8. Une fois l'installation terminée, redémarrez en utilisant l'une des méthodes suivantes :
   - Si vous êtes invité à redémarrer, cliquez sur **Yes (Oui)**.
   - Si vous n'êtes pas invité à redémarrer, sélectionnez **Device (Périphérique)** > **Configuration** > **Operations (Opérations)** et **Reboot Device (Redémarrez le périphérique)**.
9. (Mises à niveau active/passive uniquement) À partir de la CLI de l'homologue que vous venez de mettre à niveau, exécutez la commande suivante pour rendre le pare-feu de nouveau fonctionnel :

   ```
   request high-availability state functional
   ```

STEP 10 | (Mise à niveau PAN-OS XFR uniquement) Mettez à niveau le premier homologue et le deuxième vers PAN-OS XFR en répétant l'étape 8 et l'étape 9.

STEP 11 | Vérifiez la version du logiciel et du contenu qui s'exécute sur chaque pare-feu géré.

1. Sur Panorama, sélectionnez **Panorama** > **Managed Devices (Périphériques gérés)**.
2. Localisez les pare-feu et examinez les versions de contenu et logicielles dans le tableau.

   Pour les pare-feu HA, vous pouvez également vérifier que l'état HA de chaque homologue est conforme aux attentes.

STEP 12 | (Mises à niveau des pare-feu HA uniquement)Si vous avez désactivé la préemption sur l'un de vos pare-feu haute disponibilité avant de procéder à la mise à niveau, modifiez les **Election Settings (Paramètres d'élection)** (**Device (Périphérique)** > **High Availability (Haute disponibilité)**)

et réactivez le paramètre **Preemptive (Préemptif)** pour ce pare-feu, puis **Commit (Validez)** le changement.

Mise à niveau de la version du logiciel PAN-OS (VM-Series pour NSX)

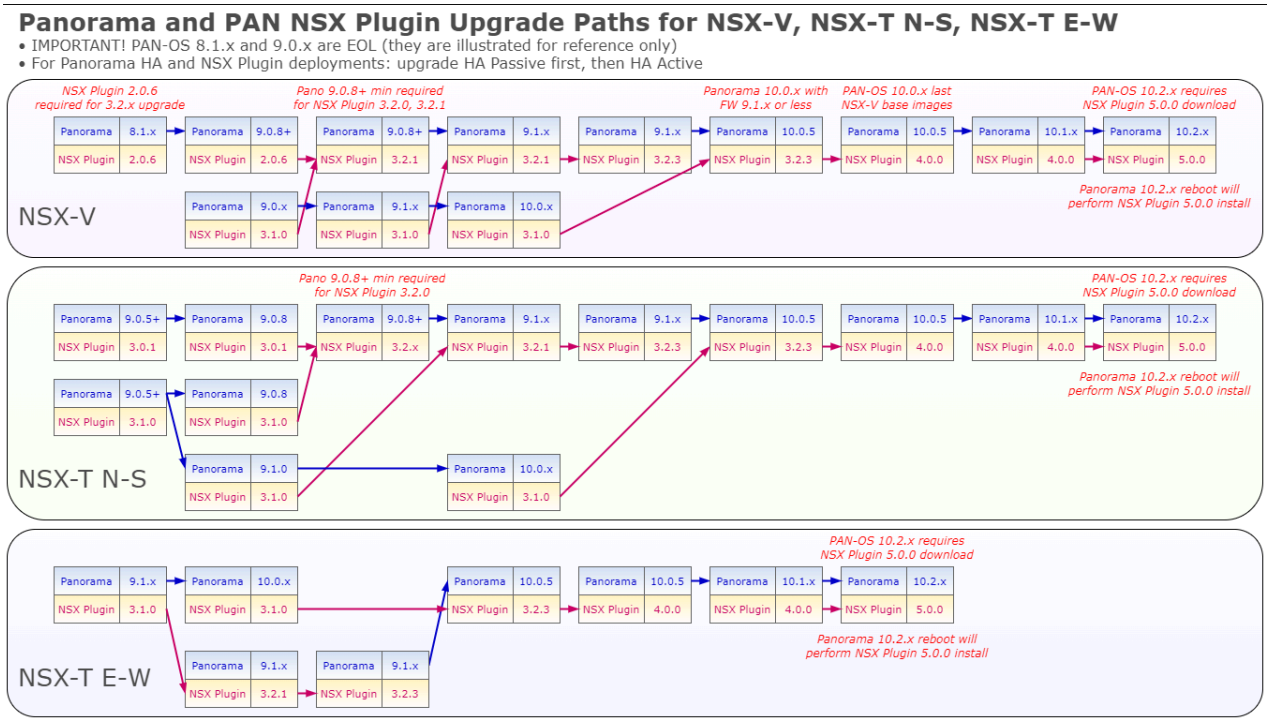
Choisissez la méthode de mise à niveau qui convient le mieux à votre déploiement.

- Upgrade the VM-Series for NSX During a Maintenance Window (Mettre à niveau le VM-Series pour NSX pendant une fenêtre de maintenance) :utilisez cette option pour mettre à niveau le pare-feu VM-Series pendant une fenêtre de maintenance sans modifier l'URL OVF dans la définition de service.
- Upgrade the VM-Series for NSX without disrupting traffic (Mettre à niveau le VM-Series pour NSX sans perturber le trafic) : utilisez cette option pour mettre à niveau le pare-feu VM-Series sans interrompre le service aux VM invitées ou changer l'URL OVF dans la définition du service.

Le graphique suivant montre les combinaisons actuellement prises en charge de Panorama et du plug-in Panorama pour VMware NSX, ainsi que les procédures de mise à niveau que vous devez suivre pour une mise à niveau réussie.

- Chaque case ci-dessous représente une combinaison prise en charge.
- Lorsque vous mettez à niveau le plug-in Panorama pour NSX ou Panorama dans une paire HA, mettez d'abord à niveau l'homologue Panorama passif, puis l'homologue HA actif.

Avant de mettre à niveau votre VM-Series pour le déploiement de VMware NSX, passez en revue les procédures de mise à niveau indiquées ci-dessous pour comprendre les étapes de mise à niveau permettant de parvenir à la combinaison de plug-in et de PAN-OS qui convient le mieux à votre environnement.



Mise à niveau de la VM-series pour le NSX durant une fenêtre de maintenance

Pour le pare-feu VM-Series Édition NSX, utilisez Panorama pour mettre à niveau la version logicielle sur les pare-feu.

STEP 1 | Passez en revue VM-Series pour les procédures de mise à niveau de VMware NSX.

STEP 2 | Allouez des ressources matérielles supplémentaires à votre pare-feu VM-Series.

Vérifiez que suffisamment de ressources matérielles sont disponibles pour le pare-feu VM-Series. Reportez-vous à Configuration système requise pour VM-Series pour voir les nouvelles exigences de ressources pour chaque modèle VM-Series. Allouez des ressources matérielles supplémentaires

avant de poursuivre le processus de mise à niveau. Le processus d'attribution de ressources matérielles supplémentaires diffère sur chaque hyperviseur.

STEP 3 | Effectuez une copie de sauvegarde du fichier de configuration actuel sur chaque pare-feu géré que vous envisagez de mettre à niveau.

Bien que le pare-feu crée automatiquement une sauvegarde de la configuration, il convient d'effectuer une copie de sauvegarde avant de mettre à niveau et de l'enregistrer en externe.

1. Sélectionnez **Device (Appareil)** > **Setup (Configuration)** > **Operations (Opérations)**, puis cliquez sur **Export Panorama and devices config bundle (Exporter la solution de configuration des appareils et de Panorama)**. Cette option est utilisée pour générer et exporter manuellement la dernière version de la sauvegarde de configuration de Panorama et celle de chaque périphérique géré.
2. Enregistrez le fichier exporté dans un emplacement externe au pare-feu. Vous pouvez utiliser cette sauvegarde pour restaurer la configuration en cas de problème pendant la mise à niveau.

STEP 4 | Consultez les notes de publication afin de vérifier la version de contenu requise pour la version de PAN-OS.

Les pare-feu dont vous envisagez une mise à niveau doivent exécuter la version de contenu requise pour la version de PAN-OS.

1. Sélectionnez **Panorama** > **Device Deployment (Déploiement d'appareils)** > **Dynamic Updates (Mises à jour dynamiques)**.
2. Recherchez les dernières mises à jour. Cliquez sur Check Now (Vérifier maintenant) (situé dans le coin inférieur gauche de la fenêtre) pour vérifier les dernières mises à jour. Le lien dans la colonne Action indique si une mise à jour est disponible. Si une version est disponible, le lien **Download (Télécharger)** s'affiche.
3. Cliquez sur **Télécharger (Télécharger)** pour télécharger la version sélectionnée. Une fois le téléchargement terminé, le lien se trouvant dans la colonne **Action** passe de **Télécharger (Télécharger)** à **Install (Installer)**.
4. Cliquez sur **Install (Installer)** et sélectionnez les périphériques sur lesquels vous voulez installer la mise à jour. Une fois l'installation terminée, une coche s'affiche dans la colonne **Currently Installed (Actuellement installé)**.

STEP 5 | Déployez les mises à jour logicielles sur les pare-feu sélectionnés.

*Si vos périphériques sont configurés en HA, veillez à décocher la case **Group HA Peers (Regrouper les homologues HA)** et mettez à niveau un homologue HA à la fois.*

1. Sélectionnez **Panorama** > **Device Deployment (Déploiement d'appareils)** > **Software (Logiciel)**.
2. Recherchez les dernières mises à jour. Cliquez sur **Check Now (Vérifier maintenant)** (situé dans le coin inférieur gauche de la fenêtre) pour vérifier les dernières mises à jour. Le lien dans la colonne **Action** indique si une mise à jour est disponible.
3. Consultez le **File Name (Nom de fichier)** et cliquez sur **Télécharger (Télécharger)**. Vérifiez que les versions de logiciel que vous téléchargez correspondent à celles des modèles de pare-feu

déployés sur votre réseau. Une fois le téléchargement terminé, le lien se trouvant dans la colonne **Action** passe de **Télécharger (Télécharger)** à **Install (Installer)**.

4. Cliquez sur **Install (Installer)** et sélectionnez les périphériques sur lesquels vous voulez installer la version de logiciel.
5. Sélectionnez **Reboot device after install (Redémarrer après l'installation)**, puis cliquez sur **OK**.
6. Si vous disposez de périphériques configurés en HA, décochez la case **Group HA Peers (Regrouper les homologues HA)** et mettez à niveau un homologue HA à la fois.

STEP 6 | Vérifiez la version logicielle et de contenu exécutée sur chaque périphérique géré.

1. Sélectionnez **Panorama** > **Managed Devices (Appareils gérés)**.
2. Localisez le(s) périphérique(s) et examinez les versions de contenu et de logiciel sur le tableau.

Mise à niveau de la VM-series pour le NSX sans perturber le flux

Utilisez la procédure suivante pour mettre à niveau la version PAN-OS des pare-feu de la série VM dans votre environnement VMware NSX. Cette procédure vous permet d'effectuer la mise à niveau PAN-OS sans perturber le trafic en migrant des MV vers différents hôtes ESXi.

STEP 1 | Passez en revue VM-Series pour les procédures de mise à niveau de VMware NSX.

STEP 2 | Effectuez une copie de sauvegarde du fichier de configuration actuel sur chaque pare-feu géré que vous envisagez de mettre à niveau.

Bien que le pare-feu crée automatiquement une sauvegarde de la configuration, il convient d'effectuer une copie de sauvegarde avant de mettre à niveau et de l'enregistrer en externe.

1. Sélectionnez **Device (Appareil)** > **Setup (Configuration)** > **Operations (Opérations)**, puis cliquez sur **Export Panorama and devices config bundle (Exporter la solution de configuration des appareils et de Panorama)**. Cette option est utilisée pour générer et exporter manuellement la dernière version de la sauvegarde de configuration de Panorama et celle de chaque périphérique géré.
2. Enregistrez le fichier exporté dans un emplacement externe au pare-feu. Vous pouvez utiliser cette sauvegarde pour restaurer la configuration en cas de problème pendant la mise à niveau.

STEP 3 | Consultez les notes de publication afin de vérifier la version de contenu requise pour la version de PAN-OS.

Les pare-feu dont vous envisagez une mise à niveau doivent exécuter la version de contenu requise pour la version de PAN-OS.

1. Sélectionnez **Panorama** > **Device Deployment (Déploiement d'appareils)** > **Dynamic Updates (Mises à jour dynamiques)**.
2. Recherchez les dernières mises à jour. Cliquez sur Check Now (Vérifier maintenant) (situé dans le coin inférieur gauche de la fenêtre) pour vérifier les dernières mises à jour. Le lien dans la

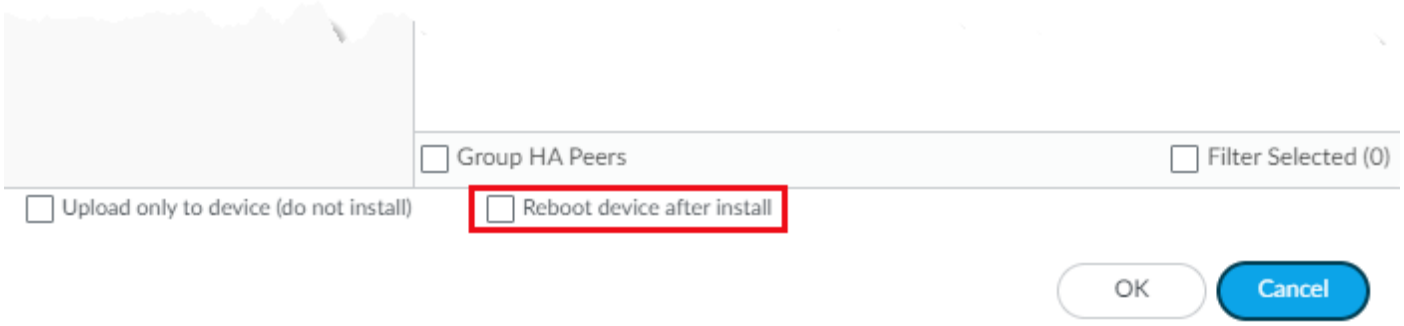
colonne Action indique si une mise à jour est disponible. Si une version est disponible, le lien **Download (Télécharger)** s'affiche.

3. Cliquez sur **Télécharger (Télécharger)** pour télécharger la version sélectionnée. Une fois le téléchargement terminé, le lien se trouvant dans la colonne **Action** passe de **Télécharger (Télécharger)** à **Install (Installer)**.
4. Cliquez sur **Install (Installer)** et sélectionnez les périphériques sur lesquels vous voulez installer la mise à jour. Une fois l'installation terminée, une coche s'affiche dans la colonne **Currently Installed (Actuellement installé)**.

STEP 4 | Téléchargez l'image PAN-OS sur tous les pare-feu de la série VM dans l'amas.

1. Connectez-vous à Panorama.
2. Sélectionnez **Panorama** > **Device Deployment (Déploiement d'appareils)** > **Software (Logiciel)**.
3. Cliquez sur **Refresh (Actualiser)** pour afficher la dernière version du logiciel et consultez les **Release Notes (Notes de publication)** pour obtenir la description des modifications de la version et le chemin de migration pour installer le logiciel.
4. Cliquez sur **Download (Télécharger)** pour obtenir le logiciel, puis sur **Install (Installer)**.

   Ne pas redémarrer les pare-feu de la série VM après avoir installé la nouvelle image logicielle.
5. Sélectionnez les appareils gérés à mettre à niveau.
6. Cochez la case **Reboot device after install (Redémarrer le dispositif après l'installation)**



7. Cliquez sur **OK**.

STEP 5 | Mettre à niveau le pare-feu de la série VM sur le premier hôte ESXi du groupe.

1. Connectez-vous à vCenter.
2. Sélectionnez **Hosts and Clusters (Hôtes et grappes)**.
3. Cliquez à droite sur l'hôte et sélectionnez **Maintenance Mode (Mode de maintenance)** > **Enter Maintenance Mode (Entrer mode de maintenance)**.
4. Migrer (automatiquement ou manuellement) toutes les MV, sauf le pare-feu de la série VM, hors de l'hôte.
5. Mettez le pare-feu VM-Series hors tension. Cela devrait se faire automatiquement au moment d'entrer en mode maintenance sur l'hôte.
6. (Facultatif) Attribuez des UCT ou une mémoire supplémentaires au pare-feu de la série VM avant de poursuivre le processus de mise à niveau.

   Vérifiez que suffisamment de ressources matérielles sont disponibles pour le pare-feu VM-Series. Reportez-vous à Modèles VM-Series pour voir les nouvelles exigences de ressources pour chaque modèle VM-Series.
7. Clique de droite sur l'hôte et sélectionnez **Maintenance Mode (Mode de maintenance)** > **Enter Maintenance Mode (Entrer mode de maintenance)**. La sortie du mode de maintenance entraîne l'alimentation du NSX ESX Agent Manager (EAM) sur le pare-feu de la série VM. Le pare-feu redémarre avec la nouvelle version PAN-OS.
8. Transférer (automatiquement ou manuellement) toutes les MV à l'hôte initial.

STEP 6 | Répétez ce processus pour chaque pare-feu de série VM sur chaque hôte ESXi.

STEP 7 | Vérifiez la version logicielle et de contenu exécutée sur chaque périphérique géré.

1. Sélectionnez **Panorama** > **Managed Devices (Appareils gérés)**.
2. Localisez le(s) périphérique(s) et examinez les versions de contenu et de logiciel sur le tableau.

Mise à niveau du modèle VM-Series

Le processus de licence du pare-feu VM-Series utilise l'UUID et l'ID de processeur pour générer un numéro de série unique pour chaque pare-feu VM-Series. Par conséquent, lorsque vous générez une licence, celle-ci est mappée à une instance spécifique du pare-feu VM-Series et ne peut être modifiée.

Suivez les instructions de cette section si vous :

- migrez depuis une licence d'évaluation vers une licence de production ;
- mettez à niveau le modèle pour en augmenter la capacité. Par exemple, vous souhaitez effectuer une mise à niveau depuis le modèle VM-100 vers le modèle VM-300.

- *mettez à niveau la capacité, ce qui redémarre certains processus critiques sur le pare-feu. Une configuration HA est recommandée pour minimiser les interruptions de service. Pour mettre à niveau la capacité sur une paire HA, reportez-vous à la section* Mise à niveau du modèle VM-Series d'une paire HA.
- *dans un déploiement de cloud privé ou public, si votre pare-feu est sous licence avec l'option BYOL, vous devez* désactiver votre VM *avant de modifier le type d'instance ou le type de VM. La mise à niveau du modèle ou de l'instance modifie l'UUID et l'ID du processeur, vous devez donc appliquer la licence lorsque le .*

STEP 1 | Allouez des ressources matérielles supplémentaires à votre pare-feu VM-Series.

Avant d'initier la mise à niveau de capacité, vous devez vérifier que le pare-feu VM-Series dispose de suffisamment de ressources matérielles pour prendre en charge la nouvelle capacité. Le processus d'attribution de ressources matérielles supplémentaires diffère sur chaque hyperviseur.

Pour vérifier la configuration matérielle requise pour votre nouveau modèle VM-Series, reportez-vous à la section Modèles VM-Series.

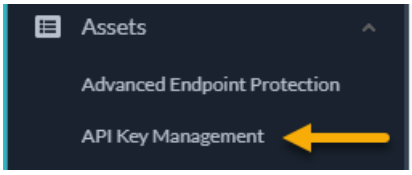
Bien que la mise à niveau de la capacité ne nécessite pas de redémarrage du pare-feu VM-Series, vous devez mettre la machine virtuelle hors tension pour modifier l'allocation matérielle.

STEP 2 | Récupérez la clé API de licence à partir du portail de support client.

1. Ouvrez une session dans le portail de support client.

   Assurez-vous que vous utilisez le même compte que vous avez utilisé pour enregistrer la licence initiale.

2. Dans le menu de gauche, sélectionnez **Assets (Ressources)** > **API Key Management (Gestion de clé API)**.
3. Copiez la clé API.



STEP 3 | Sur le pare-feu, utilisez la CLI pour installer la clé API copiée à l'étape précédente.


```
request license api-key set key <key>
```

STEP 4 | (Si vous avez accès à Internet) Autorisez le pare-feu à **Verify Update Server identity (Vérifier l'identité du serveur de mise à jour)** dans **Device (Périphérique)** > **Setup (Configuration)** > **Service**.

STEP 5 | **Commit (Validez)** vos modifications. Assurez-vous d'avoir un utilisateur configuré au niveau local sur le pare-feu. Les utilisateurs transmis sur Panorama peuvent ne pas être disponibles après la désactivation si la configuration dépasse la limite d'objets PA-VM sans licence.

STEP 6 | Mettez à niveau la capacité.

Sélectionnez **Device (Appareil)** > **Licenses (Licences)** > **Upgrade VM Capacity (Mettre à jour la fonctionnalité VM)**, puis activez vos licences et vos abonnements de l'une des manières suivantes :

- (internet) **Retrieve license keys from license server (Récupérer les clés de licence auprès du serveur de licences)** : utilisez cette option si vous avez activé votre licence sur le portail de support client.
- (internet) **Use an authorization code (Utiliser un code d'autorisation)** : utilisez cette option pour mettre à niveau la capacité de VM-Series à l'aide d'un code d'autorisation pour les licences qui n'ont pas été précédemment activées sur le portail de support. Lorsque vous y êtes invité, saisissez le **Authorization Code (Code d'autorisation)**, puis cliquez sur **OK (OK)**.
- (aucune connexion internet) **Manually upload license key (Charger manuellement la clé de licence)** : utilisez cette option si votre pare-feu ne dispose d'aucune connectivité au portail de support client. Depuis un ordinateur avec accès à Internet, connectez-vous au CSP, téléchargez un fichier de clé de licence, transférez-le sur un ordinateur du même réseau que le pare-feu et téléchargez-le sur le pare-feu.

STEP 7 | Vérifiez que votre pare-feu est correctement mis sous licence.

Sur la page **Device (Périphérique)** > **Licenses (Licences)**, vérifiez que la licence a été activée avec succès.

Mise à niveau du modèle VM-Series d'une paire HA

La mise à niveau du pare-feu VM-Series vous permet d'augmenter la capacité du pare-feu. La capacité est définie en fonction du nombre de sessions, règles, zones de sécurité, objets d'adresse, tunnels IPSec VPN et SSL VPN que le pare-feu VM-Series peut gérer. Le modèle VM-Series fonctionne sous licence. Lorsque vous appliquez la nouvelle licence de capacité sur le pare-feu VM-Series, le numéro de modèle et les fonctionnalités associées y sont implémentés.

Vérifiez la configuration système requise pour VM-Series pour votre modèle de pare-feu avant de procéder à la mise à niveau. Si votre pare-feu dispose de moins de 5,5 Go de mémoire, la capacité (nombre de sessions, règles, zones de sécurité, objets d'adresse, etc.) sur le pare-feu sera limitée à celle du VM-50 Lite.

Ce processus est similaire à celui de la mise à niveau d'une paire de pare-feu matériels dans une configuration haute disponibilité. Pendant le processus de mise à niveau de la capacité, la synchronisation de la session se poursuit, si vous l'avez activée. Pour éviter les temps d'arrêt lors de la mise à niveau des pare-feu qui sont en configuration de disponibilité élevée, mettre à jour un pair HA à la fois.

Ne modifiez pas la configuration des pare-feu pendant le processus de mise à niveau. Au cours du processus de mise à niveau, la synchronisation de la configuration est automatiquement désactivée lorsqu'une non-correspondance de capacité est détectée. Elle est ensuite réactivée lorsque les deux homologues HA présentent des licences de capacité correspondantes.

Si les pare-feu de la paire HA présentent des versions logicielles majeures différentes (telles que 9.1 et 9.0) et des capacités différentes, les deux périphériques entreront dans l'état HA suspendu. Par conséquent, il est recommandé de vous assurer que les deux pare-feu exécutent la même version de PAN-OS avant de mettre à niveau la capacité.

STEP 1 | Mettez à niveau la licence de capacité sur le pare-feu passif.

Suivez la procédure de mise à niveau du modèle VM-Series.

Le nouveau modèle VM-Series s'affiche sur le tableau de bord après le redémarrage de certains processus sur cet homologue passif. Cet homologue mis à niveau est maintenant un état non fonctionnel en raison de l'incompatibilité de capacité avec son homologue actif.

Si vous avez activé la synchronisation des sessions, vérifiez que les sessions sont synchronisées entre les homologues HA avant de passer à l'étape suivante. Pour vérifier la synchronisation des sessions, exécutez la **`show high-availability interface ha2`** et assurez-vous que les compteurs d'interface matérielle de la table du processeur augmentent comme suit :

- Dans une configuration active/passive, seul l'homologue actif affiche les paquets transmis et le périphérique passif affiche uniquement les paquets reçus.

  Si vous avez activé HA2 keep-alive (Maintien HA2), les compteurs d'interface matérielle sur l'homologue passif affichent à la fois les paquets de transmission et de réception. Cela se produit

car HA2 keep-alive (Maintien HA2) est bidirectionnel, ce qui signifie que les deux homologues transmettent des paquets HA2 keep-alive (Maintien HA2).

- Dans la configuration active/active, les paquets reçus et les paquets transmis s'affichent sur les deux homologues.

STEP 2 | Mettez à niveau la licence de capacité sur le pare-feu actif.

Suivez la procédure pour mettre à niveau le modèle VM-Series.

Le nouveau modèle VM-Series s'affiche sur le tableau de bord après le redémarrage des processus critiques. Le pare-feu passif devient actif et cet homologue (pare-feu précédemment actif) passe de l'état initial à l'homologue passif dans la paire HA.

Rétrograder un pare-feu VM-Series vers une version antérieure

Utilisez le processus suivant pour restaurer la configuration qui était en cours d'exécution avant la mise à niveau vers une autre version de fonctionnalité. Toutes les modifications apportées depuis la mise à niveau seront perdues. Il est donc important de sauvegarder votre configuration actuelle afin de pouvoir restaurer ces modifications lorsque vous reviendrez à la nouvelle version.

Utilisez la procédure suivante pour procéder à la rétrogradation vers une version antérieure.

STEP 1 | Faites une sauvegarde du fichier de configuration actuel.

Bien que le pare-feu crée automatiquement une sauvegarde de la configuration, il convient d'effectuer une copie de sauvegarde avant de mettre à niveau et de l'enregistrer en externe.

1. Cliquez sur **Export named configuration snapshot (Exporter l'instantané de configuration nommé)** (**Device (Périphérique)** > **Setup (Configuration)** > **Operations (Opération)**).
2. Sélectionnez le fichier XML contenant la configuration actuelle (par exemple, **running-config.xml**), puis cliquez sur **OK** pour exporter le fichier de configuration.
3. Enregistrez le fichier exporté dans un emplacement externe au pare-feu. Vous pouvez utiliser cette sauvegarde pour restaurer la configuration en cas de problème pendant la rétrogradation.

STEP 2 | Installez l'image de la version de fonctionnalité précédente.

Des versions de sauvegarde automatique sont créées lors de la mise à niveau vers une nouvelle version.

1. Cliquez sur **Check Now (Vérifier maintenant)** (**Device (Périphérique)** > **Software (Logiciel)**) pour vérifier les images disponibles.
2. Localisez l'image vers laquelle vous souhaitez procéder à la rétrogradation. Si l'image n'est pas déjà téléchargée, cliquez sur **Download (Télécharger)** pour la télécharger.
3. Une fois le téléchargement terminé, cliquez sur **Install (Installer)** pour installer l'image.
4. Cliquez sur **Select a Config File for Downgrading (Sélectionner un fichier de configuration pour la rétrogradation)** pour sélectionner le fichier que le pare-feu chargera après le redémarrage du périphérique. Dans la plupart des cas, vous devez sélectionner la configuration qui a été enregistrée automatiquement lors de la mise à niveau à partir de la version vers laquelle vous effectuez maintenant la rétrogradation. Par exemple, si vous exécutez PAN-OS 9.1 et que vous procédez à une rétrogradation vers PAN-OS 9.0.3, sélectionnez `autosave-9.0.3`.
5. Une fois l'installation terminée, redémarrez en utilisant l'une des méthodes suivantes :
   - Si vous êtes invité à redémarrer, cliquez sur **Yes (Oui)**.
   - Si vous n'êtes pas invité à redémarrer, accédez à Device Operations (Opérations de périphérique) (**Device (Périphérique)** > **Configuration** > **Operations (Opérations)**) et cliquez sur **Reboot Device (Redémarrer le périphérique)**.

Mettre à niveau les plugins Panorama

Considérations relatives à la mise à niveau/rétrogradation des plug-ins Panorama

Le tableau suivant répertorie les nouvelles fonctionnalités qui ont un impact sur la mise à niveau ou la rétrogradation. Assurez-vous de bien comprendre les considérations de mise à niveau/rétrogradation avant de procéder à une mise à niveau ou à une rétrogradation à partir d'une version PAN-OS 11.0. Pour plus d'informations sur les versions PAN-OS 11.0, reportez-vous aux PAN-OS 11.0 Release Notes (notes de version PAN-OS 10.1).

Table 1: Considérations relatives à la mise à niveau/rétrogradation des plug-ins Panorama

Fonctionnalité	Considérations relatives à la mise à niveau	Considérations de rétrogradation
Les plug-ins Panorama • Plug-in AWS • Plug-in Azure • Plug-in Kubernetes • Plug-in de licence de pare-feu logiciel • Plugin PAN-OS SD-WAN • Plugin convertisseur de signatures IPS • ZTP Plugin • Plugin Enterprise DLP • Plugin Openconfig • Plugin GCP • Plugin Cisco ACI • Plugin Nutanix • Plugin VCenter	Avant d'effectuer la mise à niveau vers PAN-OS 11.0, vous devez télécharger la version du plug-in Panorama prise en charge sur PAN-OS 11.0 pour tous les plug-ins installés sur Panorama. Cela est nécessaire pour réussir la mise à niveau vers PAN-OS 11.0. Consultez Compatibility Matrix (matrice de compatibilité) pour plus d'informations.	Pour rétrograder à partir de PAN-OS 11.0, vous devez télécharger la version du plug-in Panorama prise en charge sur PAN-OS 10.2 et versions antérieures pour tous les plug-ins installés sur Panorama. Consultez la Panorama Plugins Compatibility Matrix (matrice de compatibilité des plugins Panorama) pour plus d'informations.
	(Enterprise DLP) Après la mise à niveau de Panorama vers PAN-OS 10.2, vous devez installer la version `8520` du contenu Application and Threats sur tous les pare-feu gérés exécutant PAN-OS 11.0 ou une version antérieure. Cela est nécessaire pour transmettre avec succès les modifications de configuration aux pare-feux gérés à l'aide de DLP Enterprise que vous n'avez pas mis à niveau vers PAN-OS 10.2.	
	(Enterprise DLP) Loading a Panorama configuration backup (chargement d'une sauvegarde de configuration Panorama) qui contient la configuration DLP d'entreprise partagée supprime le filtre d'exclusion d'application	

Fonctionnalité	Considérations relatives à la mise à niveau	Considérations de rétrogradation
	partagée requis pour analyser le trafic non basé sur des fichiers.	
	(SD-WAN)Le plug-in Panorama pour SD-WAN 2.2 et versions antérieures n'est pas pris en charge dans PAN-OS 11.0. La mise à niveau d'un serveur d'administration Panorama vers PAN-OS 11.0 lorsque le plug-in Panorama pour SD-WAN 2.2 ou version antérieure est installé entraîne le masquage du plug-in SD-WAN dans l'interface Web Panorama ou la suppression de la configuration SD-WAN. Dans les deux cas, vous ne pouvez pas installer une nouvelle version du plug-in SD-WAN ou désinstaller le plug-in SD-WAN.	
PAN-OS SD-WAN	Après une mise à niveau réussie de Panorama vers PAN-OS 11.0 et du plug-in Panorama de SD-WAN version 2.0.0 vers SD-WAN version 3.0, vous devez effacer le cache SD-WAN sur Panorama pour les déploiements SD-WAN existants uniquement. L'effacement du cache SD-WAN ne supprime aucune configuration SD-WAN existante, mais supprime les conventions de dénomination d'adresse IP, de tunnel et de passerelle pour le nouveau format introduit dans le plug-in Panorama pour SD-WAN version 3.0. Pour les nouveaux déploiements de SD-WAN, vous n'avez pas besoin d'effacer le cache SD-WAN sur Panorama si vous installez le plug-in Panorama pour SD-WAN version 3.0 sur Panorama après la mise à niveau vers PAN-OS 11.0.	Aucun.

Fonctionnalité	Considérations relatives à la mise à niveau	Considérations de rétrogradation
	1. Connectez-vous à l'CLI de Panorama. 2. Videz le cache SD-WAN sur Panorama. `admin> debug plugins sd_wan drop-config-cache all`	

Mettre à niveau le plug-in Enterprise DLP

Mettez à jour la version installée du plug-in Entreprise Data Loss Prevention (prévention des pertes de données - DLP) sur votre serveur de gestion Panorama™.

Consultez la matrice de compatibilité du plug-in Palo Alto Networks Panorama et passez en revue la version minimale du PAN-OS requise pour votre version cible du plug-in Enterprise DLP.

STEP 1 | Connectez-vous à l'interface Web Panorama.

STEP 2 | Mettez à niveau la version du plug-in Enterprise DLP sur Panorama.

Si Panorama est en configuration High Availability (haute disponibilité - HA), répétez cette étape sur l'homologue HA de Panorama.

1. Sélectionnez **Panorama** > **Plugins** et **Check now (vérifiez maintenant)** la dernière version du plugin `dlp` .
2. **Download (Téléchargez)** et **Install (Installez)** la dernière version du plugin Enterprise DLP.
3. Une fois la nouvelle version du plug-in installée, affichez le **Dashboard (tableau de bord)** de Panorama et vérifiez dans le widget Informations générales que la version `DLP du plug-in` affiche la version du plug-in DLP Enterprise vers laquelle vous avez effectué la mise à niveau.

STEP 3 | (Upgrade to 4.0.0 only (Mise à niveau vers la version 4.0.0 uniquement)) Edit the Enterprise DLP data filtering settings (Modifiez les paramètres de filtrage des données Enterprise DLP) pour réduire la **Max File Size (taille maximale du fichier)** à 20 Mo ou moins.

Ceci est nécessaire lors de la mise à niveau du plug-in Panorama pour Enterprise DLP 3.0.3 ou versions ultérieures vers Enterprise DLP 4.0.0 car cette version du plug-in ne prend pas en charge large file size inspection (l'inspection de la taille des fichiers volumineux).

Mettre à niveau le plugiciel (plug-in) Panorama Interconnect

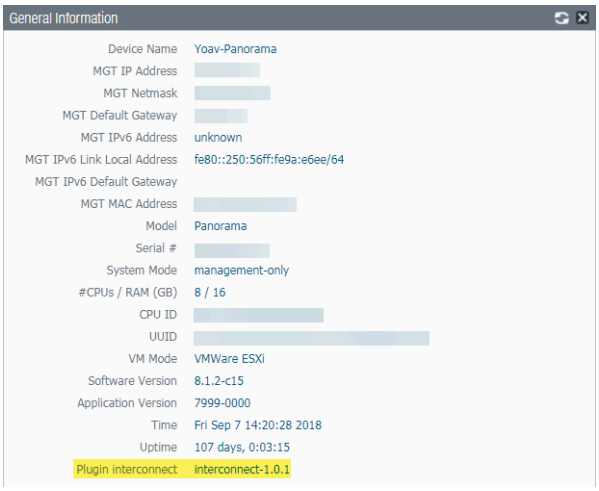
Utilisez la procédure suivante pour mettre à niveau le plugiciel Panorama™ Interconnect sur le contrôleur Panorama et les nœuds Panorama. Lors de la mise à niveau du plugiciel Panorama Interconnect, vous devez procéder à la mise à niveau du contrôleur Panorama avant de faire passer les nœuds Panorama à la même version de plugiciel de le contrôleur. La nouvelle version du plugiciel que vous avez téléchargée et installée sur le nœud Panorama doit correspondre à la version du plugiciel que vous avez installée sur le contrôleur Panorama pour vous assurer que le contrôleur Panorama et les nœuds Panorama sélectionnés demeurent synchronisés.

S'il s'agit de la première fois que vous installez le plug-in, consultez Set up the Panorama Interconnect Plugin (Configurer le plug-in d'interconnexion Panorama).

STEP 1 | Log in to the Panorama web interface (Connectez-vous à l'interface Web Panorama) du contrôleur Panorama.

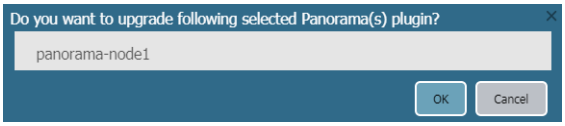
STEP 2 | Mettez à niveau le plugiciel Panorama Interconnect sur le contrôleur Panorama.

1. Sélectionnez **Panorama** > **Plugins (Plugiciels)**, puis cherchez **`Interconnect`**.
2. **Download (Téléchargez)**, puis **Install (Installez)** la nouvelle version du plugiciel Panorama Interconnect. Une invite vous avise que l'installation est terminée.
3. Vérifiez que le **Dashboard (Tableau de bord)** affiche la version nouvellement installée du plugiciel Interconnect.

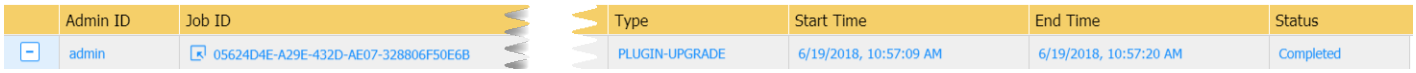


STEP 3 | Mettez à niveau le plugiciel Panorama Interconnect sur le nœud Panorama.

1. Sélectionnez **Panorama** > **Interconnect** > **Panorama Nodes (Nœuds Panorama)**, sélectionnez un ou plusieurs nœuds Panorama, puis **Upgrade Plugin (Mettre le plugiciel à niveau)**.
2. Vérifiez les nœuds Panorama sélectionnés, puis cliquez sur **OK** pour commencer la mise à niveau du plugiciel.



3. Attendez que la tâche de mise à niveau du plugiciel soit `Completed`. Cliquez sur **Panorama** > **Interconnect** > **Tasks (Tâches)** pour voir la progression du travail.



4. Une fois la mise à niveau terminée, sélectionnez **Panorama** > **Interconnect** > **Panorama Nodes (Nœuds Panorama)** pour vérifier que la version du **Plugin (Plugiciel)** est la bonne pour les nœuds Panorama sélectionnés.

Mise à niveau du plug-in SD-WAN

Mettez à niveau la version du plug-in SD-WAN installée sur votre serveur de gestion Panorama™ et sur vos pare-feu qui utilisent SD-WAN.

Consultez la matrice de compatibilité des plug-ins Panorama de Palo Alto Networks et passez en revue la version minimale de PAN-OS requise pour votre version de plug-in SD-WAN cible.

STEP 1 | Connectez-vous à l'interface Web Panorama.

STEP 2 | Mettez à niveau la version du plug-in SD-WAN sur Panorama.

Si Panorama est en configuration High Availability (haute disponibilité - HA), répétez cette étape sur l'homologue HA de Panorama.

1. Sélectionnez **Panorama** > **Plugins** et **Check Now (Vérifier maintenant)** pour passer à la version la plus récente du plugin **`sd_wan`**.
2. **Download (Téléchargez)** et **Install (Installez)** la dernière version du plugin SD-WAN.

STEP 3 | Une fois la nouvelle version du plug-in installée avec succès, affichez le **Tableau de bord** Panorama et dans le widget Informations générales, vérifiez que le `plug-in SD-WAN` affiche la version du plug-in SD-WAN vers laquelle vous avez effectué la mise à niveau.

Commandes CLI pour la mise à niveau

Utiliser les commandes CLI pour les tâches de mise à niveau

Utilisez les commandes CLI suivantes pour effectuer les tâches de mise à niveau.

Si vous souhaitez...	Utilisez ...
Check the current versions of the firewall (Vérifiez les versions actuelles du pare-feu)	
• Vérifiez la version actuelle du logiciel et du contenu du pare-feu.	`show system info`
Access the available dynamic updates and upgrade the content version of the firewall (Accédez aux mises à jour dynamiques disponibles et mettez à niveau la version de contenu du pare-feu)	
• Vérifiez les versions de contenu disponibles des mises à jour dynamiques directement à partir des serveurs de Palo Alto Networks.	`request content upgrade check (demander une vérification de mise à niveau du contenu)`
• Vérifiez les versions de contenu disponibles des mises à jour dynamiques directement depuis le pare-feu.	`request content upgrade info (demander des informations sur la mise à niveau du contenu)`
• Téléchargez la version du contenu directement sur le pare-feu.	`request content upgrade download (Demander le téléchargement de la mise à niveau du contenu) <content version>`
• Installer la version du contenu.	

Si vous souhaitez...	Utilisez ...
	request content upgrade install (Demander l’installation de la mise à niveau du contenu) <content version>
Access the available software versions and upgrade the firewall (Accéder aux versions logicielles disponibles et mettre à niveau le pare-feu)	
• Vérifiez les versions logicielles disponibles en téléchargement.	request system software info (demander des informations sur le logiciel système)
• Vérifiez les versions disponibles chargées sur le pare-feu.	request system software check (request system software check)
• Téléchargez une version spécifique du logiciel.	request system software download version (demander le téléchargement du logiciel système version 10.2)<version>
• Vérifiez l'état d'une tâche de téléchargement spécifique.	Afficher l’ID de tâche <jobid>
• Installez le logiciel téléchargé.	

Si vous souhaitez...	Utilisez ...
	`request system software install version 10.1.0 (demander l'installation du logiciel système version 10.2.0)`
• Redémarrez le pare-feu.	`request restart system`

Accédez aux correctifs logiciels disponibles pour le pare-feu :

La fonctionnalité de correctif est actuellement proposée en mode aperçu. La prise en charge complète n'est pas disponible avec cette fonctionnalité.

Si vous souhaitez...	Utilisez ...
• Vérifiez les correctifs logiciels disponibles au téléchargement.	`request system patch check (demander une vérification des correctifs système)`
• Vérifiez les correctifs disponibles pour la version du pare-feu actuellement installée.	`request system patch info (demander des informations sur le correctif système)`
• Téléchargez une version de correctif spécifique.	`request system patch download version (demander la version de téléchargement du correctif système) <version>`

Si vous souhaitez...	Utilisez ...
• Consultez des informations plus détaillées pour une version de correctif spécifique.	`request system patch info version (demander la version des informations sur les correctifs système) <version>`
• Installez le correctif téléchargé.	`request system patch install version (demander la version d’installation du correctif système) <version>`
• Appliquez le correctif installé.	`request system patch apply (demander un correctif système Appliquer)`

API pour la mise à niveau

Utiliser l'API pour les tâches de mise à niveau

Utilisez les commandes CLI suivantes pour effectuer les tâches de mise à niveau.

Si vous souhaitez...	Utilisez ...
Check the current versions of the firewall (Vérifiez les versions actuelles du pare-feu)	
• Vérifiez la version actuelle du logiciel et du contenu du pare-feu.	**https://firewall/api/?type=op&cmd=<request><system><software><chec check></software></system>**
Access the available dynamic updates and upgrade the content version of the firewall (Accédez aux mises à jour dynamiques disponibles et mettez à niveau la version de contenu du pare-feu)	
• Vérifiez les versions de contenu disponibles des mises à jour dynamiques directement à partir des serveurs de Palo Alto Networks.	**https://firewall/api/?type=op&cmd=<request><content><upgrade><chec check></upgrade></content></request>**
• Vérifiez les versions de contenu disponibles des mises à jour dynamiques directement depuis le pare-feu.	**https://firewall/api/?type=op&cmd=<request><content><upgrade><info info></upgrade></content></request>**
• Téléchargez la dernière version du contenu directement sur le pare-feu.	**https://firewall/api/?type=op&cmd=<request><content><upgrade><down latest></download></upgrade></content></request>**
• Téléchargez une version de contenu spécifique directement sur le pare-feu.	**https://firewall/api/?type=op&cmd=<request><content><upgrade><down le nom spécifique du fichier ici<file></download></upgrade></content></request>**
• Installer la version du contenu.	**https://firewall/api/?type=op&cmd=<request><content><upgrade><inst <content version></version></install></upgrade></content></request>**
Access the available software versions and upgrade the firewall (Accéder aux versions logicielles disponibles et mettre à niveau le pare-feu)	

Si vous souhaitez...	Utilisez ...
• Vérifiez les versions logicielles disponibles en téléchargement.	`https://firewall/api/?type=op&cmd=<request><system><software><info info></software></system></request>`
• Vérifiez les versions disponibles chargées sur le pare-feu.	`https://firewall/api/?type=op&cmd=<request><system><software><chec check></software></system></request>`
• Téléchargez une version spécifique du logiciel.	`https://firewall/api/?type=op&cmd=request><system><software><downl version></download></software></system></request>`
• Vérifiez l'état d'une tâche de téléchargement spécifique.	`https://firewall/api/?type=op&cmd=<show><jobs></jobs></show>`
• Installez le logiciel téléchargé.	`https://firewall/api/?type=op&cmd=<request><system><software><inst version></install></software></system></request>`
• Redémarrez le pare-feu.	`https://firewall/api/?type=op&cmd=<request><restart><system></system></restart></request>`

