




Mises à jour

Ce chapitre explique comment effectuer des mises à jour de contenu.



Important Pour mettre à niveau des périphériques gérés, voir [Guide de mise à niveau de Cisco Secure Firewall Threat Defense pour le centre de gestion Firewall livré dans le nuage](#).

Dans Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), choisissez **System**() > **Product Upgrades** pour accéder à la page de mise à niveau de Threat Defense. Vous pouvez également accéder à cette page à partir de **Devices** (périphériques) – **Mise à niveau**.

- [À propos des mises à jour du système, à la page 1](#)
- [Lignes directrices et limites des mises à jour du système, à la page 3](#)
- [Mettre à jour la base de données sur les vulnérabilités \(VDB\), à la page 4](#)
- [Mettre à jour la base de données de géolocalisation \(GeoDB\), à la page 5](#)
- [Mettre à jour les règles de prévention des intrusions, à la page 7](#)

À propos des mises à jour du système

Utilisez centre de gestion pour mettre à niveau le logiciel système pour les périphériques qu'il gère. Vous pouvez également mettre à jour diverses bases de données et flux qui fournissent des services avancés.

Si le centre de gestion dispose d'un accès Internet, le système peut souvent obtenir des mises à jour directement auprès de Cisco. Nous vous recommandons de planifier ou d'activer des mises à jour automatiques de contenu dans la mesure du possible. Certaines mises à jour sont activées automatiquement lors de la configuration initiale ou lorsque vous activez la fonctionnalité associée. Vous devez planifier vous-même les autres mises à jour. Après la configuration initiale, nous vous recommandons de passer en revue toutes les mises à jour automatiques et de les modifier si nécessaire.

Tableau 1 : Mises à jour et mises à niveau

Composant	Description	Détails
Logiciel système	<p>Les versions logicielles <i>principales</i> contiennent de nouvelles fonctions, fonctionnalités et améliorations. Elles peuvent comporter des modifications d'infrastructure ou d'architecture.</p> <p>Les versions de <i>maintenance</i> contiennent des correctifs généraux de bogues et de sécurité. Les changements de comportement sont rares et sont liés à ces correctifs.</p> <p><i>Les correctifs</i> sont des mises à jour sur demande limitées aux correctifs critiques et urgents.</p> <p><i>Les correctifs</i> peuvent résoudre des problèmes spécifiques de clients.</p>	<p>Téléchargement direct : sélectionnez certains correctifs et versions de maintenance uniquement, généralement quelque temps après que la version soit disponible pour le téléchargement manuel. La durée du délai dépend du type de version, de l'adoption de la version et d'autres facteurs. Les téléchargements à la demande et planifiés sont pris en charge.</p> <p>Planifier l'installation : correctifs et versions de maintenance uniquement, en tant que tâche planifiée.</p> <p>Désinstaller : Uniquement les correctifs.</p> <p>Revenir en arrière : versions majeures et de maintenance uniquement.</p> <p>Nouvelle image : versions majeures et de maintenance uniquement.</p> <p>Voir : Guide de mise à niveau de Cisco Secure Firewall Threat Defense pour le centre de gestion Firewall livré dans le nuage</p>
Base de données relative aux vulnérabilités (VDB)	La base de données sur les vulnérabilités de Cisco (VDB) est une base de données contenant les vulnérabilités connues auxquelles les hôtes peuvent être sensibles, ainsi que les empreintes digitales pour les systèmes d'exploitation, les clients et les applications. Le système utilise la VDB pour déterminer si un hôte particulier augmente le risque de compromission.	<p>Téléchargement direct : oui.</p> <p>Planifier : Oui, en tant que tâche planifiée.</p> <p>Désinstallation : À partir de la version VDB 357, vous pouvez installer n'importe quelle VDB dès la version de référence pour centre de gestion.</p> <p>Voir : Mettre à jour la base de données sur les vulnérabilités (VDB), à la page 4</p>
Base de données de géolocalisation (GeoDB)	La base de données de géolocalisation Cisco (GeoDB) est une base de données de données géographiques et de connexion associées à des adresses IP routables.	<p>Téléchargement direct : oui.</p> <p>Planification : Oui, à partir de sa propre page de mise à jour</p> <p>Désinstaller : non</p> <p>Voir : Mettre à jour la base de données de géolocalisation (GeoDB), à la page 5</p>
Règles de prévention des intrusions (SRU/LSP)	<p>Les mises à jour des règles de prévention des intrusions fournissent des règles de prévention des intrusions et des règles de préprocesseur nouvelles et mises à jour, des états modifiés pour les règles existantes et des paramètres de politique de prévention des intrusions par défaut modifiés.</p> <p>Les mises à jour de règles peuvent également supprimer des règles, fournir de nouvelles catégories de règles et variables par défaut, et modifier les valeurs des variables par défaut.</p>	<p>Téléchargement direct : oui.</p> <p>Planification : Oui, à partir de sa propre page de mise à jour.</p> <p>Désinstaller : non</p> <p>Voir : Mettre à jour les règles de prévention des intrusions, à la page 7</p>

Composant	Description	Détails
Flux de renseignements sur la sécurité	Les flux de Security Intelligence (renseignements sur la sécurité) sont des ensembles d'adresses IP, de noms de domaine et d'URL que vous pouvez utiliser pour filtrer rapidement le trafic qui correspond à une entrée.	<p>Téléchargement direct : oui.</p> <p>Planification : Oui, à partir du gestionnaire d'objets.</p> <p>Désinstaller : non</p> <p>Voir : Guide de configuration Cisco Secure Firewall Management Center Device</p>
Catégories d'URL et réputations	Le filtrage d'URL vous permet de contrôler l'accès aux sites Web en fonction de la classification générale de l'URL (catégorie) et du niveau de risque (réputation).	<p>Téléchargement direct : oui.</p> <p>Planifier : Oui, lorsque vous configurez les intégrations ou les services en nuage, ou en tant que tâche planifiée.</p> <p>Désinstaller : non</p> <p>Voir : Guide de configuration Cisco Secure Firewall Management Center Device</p>

Lignes directrices et limites des mises à jour du système

Avant de procéder à la mise à jour

Avant de mettre à jour un composant de votre déploiement (y compris les règles de prévention des intrusions, VDB ou GeoDB), lisez les notes de version ou l'avis qui accompagne la mise à jour. Ceux-ci fournissent des informations critiques et spécifiques aux versions, notamment sur la compatibilité, les conditions préalables, les nouvelles fonctionnalités, les changements de comportement et les avertissements.

Mises à jour planifiées

Le système planifie les tâches, y compris les mises à jour, en UTC. Cela signifie que le moment où ils se produisent localement dépend de la date et de votre emplacement spécifique. En outre, étant donné que les mises à jour sont planifiées en UTC, elles ne s'ajustent pas à l'heure avancée, à l'heure avancée ou à tout ajustement saisonnière que vous pourriez observer dans votre région. Si vous êtes concerné, les mises à jour planifiées ont lieu une heure « plus tard » en été qu'en hiver, en fonction de l'heure locale.



Important Nous vous recommandons *fortement* de consulter les mises à jour planifiées pour vous assurer qu'elles se produisent quand vous le souhaitez.

Directives sur la bande passante

Pour mettre à niveau le logiciel système ou effectuer une vérification de l'état de préparation, l'ensemble de mise à niveau doit se trouver sur le périphérique. La taille des paquets de mise à niveau varie. Assurez-vous de disposer de la bande passante pour effectuer un transfert de données volumineux vers vos périphériques gérés. Consultez les [Directives relatives au téléchargement de données du centre de gestion Cisco Firepower Management Center vers des périphériques gérés](#) (Note technique de dépannage).

Mettre à jour la base de données sur les vulnérabilités (VDB).

La base de données sur les vulnérabilités de Cisco (VDB) est une base de données contenant les vulnérabilités connues auxquelles les hôtes peuvent être sensibles, ainsi que les empreintes digitales pour les systèmes d'exploitation, les clients et les applications. Le système utilise la VDB pour déterminer si un hôte particulier augmente le risque de compromission.

Cisco publie des mises à jour périodiques de la VDB. Le temps nécessaire pour la mise à jour de la VDB et de ses mappages sur centre de gestion dépend du nombre d'hôtes dans votre cartographie du réseau. En règle générale, divisez le nombre d'hôtes par 1 000 pour déterminer le nombre approximatif de minutes pour effectuer la mise à jour.

La configuration initiale de centre de gestion télécharge et installe automatiquement la dernière VDB de Cisco sous forme d'opération unique. Elle planifie également une tâche hebdomadaire pour télécharger les dernières mises à jour logicielles disponibles, qui comprennent la dernière base de données de vulnérabilités (VDB). Nous vous recommandons de passer en revue cette tâche hebdomadaire et de l'ajuster si nécessaire. Vous pouvez éventuellement planifier une nouvelle tâche hebdomadaire pour mettre à jour la VDB et déployer les configurations. Pour plus de renseignements, consultez [Automatisation de la mise à jour de la base de données sur les vulnérabilités \(VDB\)](#).

Pour VDB 343 et versions ultérieures, toutes les informations sur les détecteurs d'applications sont accessibles par l'intermédiaire [des Détecteurs d'applications de Cisco Secure Firewall](#). Ce site comprend une base de données interrogeable de détecteurs d'applications. Les notes de version fournissent des renseignements sur les changements pour une version particulière de VDB.

Planifier la mise à jour de la VDB

Nous vous recommandons de planifier des mises à jour régulières de la VDB. Consultez [Automatisation de la mise à jour de la base de données sur les vulnérabilités \(VDB\)](#).

Mettre à jour manuellement la VDB

Cette procédure permet de mettre à jour manuellement la VDB. À partir de la VDB 357, vous pouvez installer n'importe quelle VDB aussi ancienne que la VDB de référence pour centre de gestion.



Mise en garde

N'effectuez pas de tâches liées aux vulnérabilités mappées pendant la mise à jour de la VDB. Même si le centre de messages n'affiche aucune progression pendant plusieurs minutes ou indique que la mise à jour a échoué, ne redémarrez pas la mise à jour. Communiquez plutôt avec Centre d'assistance technique Cisco (TAC).

Dans la plupart des cas, le premier déploiement après une mise à jour de la VDB redémarre le processus Snort, interrompant l'inspection du trafic. Le système vous avertit lorsque cela se produira (les détecteurs d'applications mis à jour et les empreintes du système d'exploitation nécessitent un redémarrage, ce qui n'est pas le cas des informations de vulnérabilité). Le fait que le trafic soit interrompu ou qu'il passe sans autre inspection pendant cette interruption dépend de la manière dont l'appareil ciblé gère le trafic. Pour plus de renseignements, consultez [Comportement du trafic au redémarrage de Snort](#).

Avant de commencer

Si votre centre de gestion ne peut pas accéder au Site d'assistance et de téléchargement Cisco, obtenez vous-même la mise à jour : <https://www.cisco.com/go/firepower-software>. Choisissez n'importe quel modèle de centre de gestion, puis accédez à la page *Mises à jour de la couverture et du contenu*.

Procédure

- Étape 1** Choisissez **System** (⚙️) > **Mises à jour** > **Mises à jour de produits**.
- Étape 2** Choisissez comment vous souhaitez obtenir la VDB sur votre centre de gestion.
- Téléchargement direct : cliquez sur le bouton **Télécharger les mises à jour**.
 - Téléversement manuel : cliquez sur **Upload Update** (téléverser la mise à jour), puis **Choose File** (choisissez le fichier) et accédez à la VDB. Après avoir choisi le fichier, cliquez sur **Upload** (Téléverser).
- Étape 3** Installez la VDB.
- À côté de la mise à jour de la base de données sur les vulnérabilités et les empreintes que vous souhaitez installer, cliquez sur l'icône **Installer** (pour une VDB plus récente) ou sur l'icône **Restaurer** (pour une VDB plus ancienne).
 - Choisissez votre centre de gestion.
 - Cliquez sur **Install** (Installer).
- Surveillez la progression de la mise à jour dans le centre de messages. Une fois la mise à jour terminée, le système utilise les nouvelles informations de vulnérabilité. Cependant, vous devez effectuer le déploiement pour que les détecteurs d'applications et les empreintes du système d'exploitation mis à jour prennent effet.
- Étape 4** Vérifiez la mise à jour réussie.
-

Prochaine étape

- Déployer les changements de configuration.
- Si vous avez basé vos configurations sur des vulnérabilités, des détecteurs d'applications ou des empreintes digitales qui ne sont plus disponibles, examinez ces configurations pour vous assurer que vous gérez le trafic comme prévu. De plus, gardez à l'esprit qu'une tâche planifiée pour mettre à jour la VDB peut annuler une restauration. Pour éviter cela, modifiez la tâche planifiée ou supprimez tous les nouveaux paquets de VDB.

Mettre à jour la base de données de géolocalisation (GeoDB)

La base de données de géolocalisation (GeoDB) est une base de données que vous pouvez utiliser pour afficher et filtrer le trafic en fonction de l'emplacement géographique. Nous publions des mises à jour périodiques de la GeoDB, et vous devez la mettre régulièrement à jour pour avoir des renseignements exacts de géolocalisation.

Vous pouvez consulter votre version actuelle sur **System** (⚙️) > **Mises à jour du contenu** > **Mises à jour de la géolocalisation**.



Remarque Dans le cadre de la configuration initiale, le système planifie des mises à jour quotidiennes des règles de prévention des intrusions. Nous vous recommandons de passer en revue cette tâche et d'apporter des modifications au besoin, comme décrit dans la section [Planifier les mises à jour de GeoDB, à la page 6](#).

Une mise à jour de GeoDB remplace toute version précédente et prend effet immédiatement. Le centre de gestion met automatiquement à jour ses périphériques gérés. Vous n'avez pas besoin de procéder à un redéploiement.

Bien qu'une mise à jour de GeoDB n'interrompe aucune autre fonction du système (y compris la collecte continue d'informations de géolocalisation), la mise à jour consomme des ressources système pendant qu'elle se termine. Tenez compte de ces éléments lors de la planification de vos mises à jour.

Planifier les mises à jour de GeoDB

Dans le cadre de la configuration initiale, le système planifie des mises à jour quotidiennes des règles de prévention des intrusions. Nous vous recommandons de passer en revue cette tâche et d'apporter des modifications au besoin, comme décrit dans la section cette procédure.

Avant de commencer

Assurez-vous que le centre de gestion peut accéder à Site d'assistance et de téléchargement Cisco.

Procédure

-
- Étape 1** Choisissez **System** (⚙) > **Mises à jour** > **Mises à jour de la géolocalisation**.
 - Étape 2** Sous **Mises à jour récurrentes de la géolocalisation**, cochez **Activer les mises à jour hebdomadaires récurrentes...**
 - Étape 3** Spécifiez l'**heure de début de la mise à jour**.
 - Étape 4** Cliquez sur **Save** (enregistrer).
-

Mettre à jour manuellement la base de données GeoDB

Utilisez cette procédure pour effectuer une mise à jour de GeoDB à la demande.

Avant de commencer

Si le centre de gestion ne peut pas accéder à Site d'assistance et de téléchargement Cisco, obtenez vous-même la mise à jour : <https://www.cisco.com/go/firepower-software>. Choisissez n'importe quel modèle de centre de gestion, puis accédez à la page *Mises à jour de la couverture et du contenu*. Téléchargez l'ensemble de codes pays.

Procédure

-
- Étape 1** Choisissez **System** (⚙) > **Mises à jour du contenu** > **Mises à jour de la géolocalisation**.

- Étape 2** Sous **Mise à jour unique de la géolocalisation**, choisissez comment vous souhaitez mettre à jour la base de données GeoDB.
- Téléchargement direct : choisissez **Télécharger et installer...**
 - Chargement manuel : Choisissez **Téléverser et installer...**, puis cliquez sur **Choisissez un fichier** et accédez à l'ensemble de codes pays que vous avez téléchargé plus tôt.
- Étape 3** Cliquez sur **Import (Importer)**.
Surveillez la progression de la mise à jour dans le centre de messages.
- Étape 4** Vérifiez la mise à jour réussie.
La page de mise à jour de GeoDB affiche la version actuelle.
-

Mettre à jour les règles de prévention des intrusions

À mesure que de nouvelles vulnérabilités sont connues, Talos Intelligence Group publie des mises à jour des règles de prévention des intrusions. Ces mises à jour affectent les règles de prévention des intrusions, les règles de préprocesseur et les politiques qui utilisent les règles. Les mises à jour des règles de prévention des intrusions sont cumulatives, et Cisco vous recommande de toujours importer la dernière mise à jour. Vous ne pouvez pas importer une mise à jour de règle de prévention des intrusions qui correspond à la version des règles actuellement installées ou qui est antérieure à celle-ci.

Une mise à jour d'une règle de prévention des intrusions peut fournir les éléments suivants :

- **Règles et états de règles nouvelles et modifiées** : les mises à jour de règles fournissent des règles de préprocesseur et de prévention des intrusions nouvelles et mises à jour. Pour les nouvelles règles, l'état des règles peut être différent dans chaque politique de prévention des intrusions fournie par le système. Par exemple, une nouvelle règle peut être activée dans la politique de prévention des intrusions de la sécurité avant la connectivité et désactivée dans la politique de prévention des intrusions de la connectivité avant la sécurité. Les mises à jour de règles peuvent également modifier l'état par défaut des règles existantes ou les supprimer complètement.
- **Nouvelles catégories de règles** : les mises à jour des règles peuvent inclure de nouvelles catégories, qui sont toujours ajoutées.
- **Préprocesseur et paramètres avancés modifiés** : les mises à jour des règles peuvent modifier les paramètres avancés dans les politiques de prévention des intrusions fournies par le système et les paramètres de préprocesseur dans les politiques d'analyse de réseau fournies par le système. Elles peuvent également mettre à jour les valeurs par défaut des options de prétraitement avancé et de rendement dans vos politiques de contrôle d'accès.
- **Variables nouvelles et modifiées** : Les mises à jour de règles peuvent modifier les valeurs par défaut des variables par défaut existantes, mais ne remplacent pas vos modifications. De nouvelles variables sont toujours ajoutées.

Comprendre quand les règles de prévention des intrusions sont mises à jour et modifient les politiques

Les mises à jour des règles de prévention des intrusions peuvent avoir une incidence sur les politiques d'analyse de réseau personnalisées et fournies par le système, ainsi que sur toutes les politiques de contrôle d'accès :

- **fourni par le système** : les modifications apportées par le système aux politiques d'analyse de réseau et de prévention des intrusions fournies par le système, ainsi que les modifications apportées aux paramètres de contrôle d'accès avancé prennent effet automatiquement lorsque vous redéployez les politiques après la mise à jour.
- **personnalisée** : Étant donné que chaque politique d'analyse de réseau et de prévention des intrusions personnalisée utilise une politique fournie par le système comme base ou comme base éventuelle d'une chaîne de politiques, les mises à jour de règles peuvent affecter les politiques d'analyses de réseau et de prévention des intrusions personnalisées. Cependant, vous pouvez empêcher les mises à jour de règles d'effectuer automatiquement ces modifications. Cela vous permet de mettre à jour les politiques de base fournies par le système manuellement, selon un calendrier indépendant des importations des mises à jour de règles. Quel que soit votre choix (mis en œuvre sur la base d'une politique personnalisée), les mises à jour des politiques fournies par le système ne remplacent **pas** les paramètres que vous avez personnalisés.

Notez que l'importation d'une mise à jour de règle ignore toutes les modifications en cache apportées aux politiques d'analyse de réseau et de prévention des intrusions. Pour votre commodité, la page Rule Updates (mises à jour des règles) répertorie les politiques avec les modifications mises en cache et les utilisateurs qui ont apporté ces modifications.

Déploiement des mises à jour des règles de prévention des intrusions

Pour que les modifications apportées par une mise à jour d'une règle de prévention des intrusions prennent effet, vous devez redéployer les configurations. Lors de l'importation d'une mise à jour de règle, vous pouvez configurer le système pour le redéployer automatiquement sur les périphériques concernés. Cette approche est particulièrement utile si vous permettez à la mise à jour de la règle de prévention des intrusions de modifier les politiques de base en matière de prévention des intrusions fournies par le système.



Mise en garde

Bien qu'une mise à jour de règle en elle-même ne redémarre pas le processus Snort lorsque vous le déployez, d'autres modifications que vous avez apportées peuvent le faire. Le redémarrage de Snort interrompt brièvement le flux de trafic et l'inspection sur tous les périphériques, y compris ceux qui sont configurés pour la haute disponibilité et l'évolutivité. Les configurations de l'interface déterminent si le trafic chute ou s'il passe sans inspection pendant l'interruption. Lorsque vous déployez sans redémarrer Snort, les demandes de ressources peuvent entraîner l'abandon d'un petit nombre de paquets sans inspection.

Mises à jour des règles de prévention des intrusions récurrentes

Vous pouvez importer des mises à jour de règles quotidiennes, hebdomadaires ou mensuelles à l'aide de la page Rule Updates (Mises à jour de règles).

Les sous-tâches applicables à l'importation des mises à jour de la règle de prévention des intrusions se produisent dans l'ordre suivant : téléchargement, installation, mise à jour de la politique de base et déploiement de la configuration. Lorsqu'une sous-tâche est terminée, la sous-tâche suivante commence.

À l'heure planifiée, le système installe la mise à jour de règle et déploie la configuration modifiée comme vous l'avez spécifié à l'étape précédente. Vous pouvez vous déconnecter ou utiliser l'interface Web pour effectuer d'autres tâches avant ou pendant l'importation. Lorsqu'il est accédé pendant une importation, le journal de mise à jour des règles affiche un **État rouge** (🔴), et vous pouvez visualiser les messages au fur et à mesure qu'ils arrivent dans la vue détaillée du journal de mise à jour des règles. Selon la taille et le contenu de la mise à jour des règles, plusieurs minutes peuvent s'écouler avant que les messages d'état ne s'affichent.

Dans le cadre de la configuration initiale, le système planifie des mises à jour quotidiennes des règles de prévention des intrusions. Nous vous recommandons de passer en revue cette tâche et d'apporter des modifications au besoin, comme décrit dans la section [Planifier les mises à jour des règles de prévention des intrusions](#), à la page 9.

Importation des règles de prévention des intrusions locales

Une règle de prévention des intrusions locale est une règle de texte standard personnalisée que vous importez à partir d'un ordinateur local en tant que fichier texte brut avec encodage ASCII ou UTF-8. Vous pouvez créer des règles locales en suivant les instructions du manuel de l'utilisateur Snort, disponible à l'adresse <http://www.snort.org>.

Planifier les mises à jour des règles de prévention des intrusions

Dans le cadre de la configuration initiale, le système planifie des mises à jour quotidiennes des règles de prévention des intrusions. Nous vous recommandons de passer en revue cette tâche et d'apporter des modifications au besoin, comme décrit dans la section cette procédure.

Avant de commencer

- Assurez-vous que votre processus de mise à jour des règles de prévention des intrusions est conforme à vos politiques de sécurité.
- Examinez l'effet de la mise à jour sur le flux de trafic et l'inspection en raison des contraintes de bande passante et des redémarrages Snort. Nous vous recommandons d'effectuer les mises à jour dans une fenêtre de maintenance.

Procédure

-
- | | |
|----------------|---|
| Étape 1 | Choisissez System (⚙) > Mises à jour > Mises à jour de règles . |
| Étape 2 | Sous Recurring Rule Update Imports (importations récurrentes de mises à jour de règles), cochez Enable Recurring Rule Update Importations (activer les importations récurrentes de mises à jour de règles). |
| Étape 3 | Précisez la fréquence d'importation et l'heure de début. |
| Étape 4 | (Facultatif) Cochez la case Réappliquer toutes les politiques... pour les déployer après chaque mise à jour. |
| Étape 5 | Cliquez sur Save (enregistrer). |
-

Mettre à jour manuellement les règles de prévention des intrusions

Utilisez cette procédure pour effectuer une mise à jour des règles de prévention des intrusions à la demande.

Avant de commencer

- Assurez-vous que votre processus de mise à jour des règles de prévention des intrusions est conforme à vos politiques de sécurité.

- Examinez l'effet de la mise à jour sur le flux de trafic et l'inspection en raison des contraintes de bande passante et des redémarrages Snort. Nous vous recommandons d'effectuer les mises à jour dans une fenêtre de maintenance.
- Si centre de gestion ne peut pas accéder à Site d'assistance et de téléchargement Cisco, obtenez vous-même la mise à jour : <https://www.cisco.com/go/firepower-software>. Choisissez n'importe quel modèle de centre de gestion, puis accédez à la page *Mises à jour de la couverture et du contenu*.

Procédure

- Étape 1** Choisissez **System** (⚙) > **Mises à jour** > **Mises à jour de règles**.
- Étape 2** Sous **One-Time Rule Update/Rules Import**(Importation de règles/Mise à jour unique de règles), choisissez comment vous souhaitez mettre à jour les règles de prévention des intrusions.
- Téléchargement direct : choisissez **Télécharger la mise à jour de la nouvelle règle...**
 - Chargement manuel : choisissez **Rule Update or text Rule file...** (Mise à jour de la règle ou fichier texte de la règle.), puis cliquez sur **Choose File** (Choisir un fichier) et accédez à la mise à jour de la règle de prévention des intrusions.
- Étape 3** (Facultatif) Cochez la case **Reapply all policies...** (Réappliquer toutes les politiques...) pour les déployer après la mise à jour.
- Étape 4** Cliquez sur **Import (Importer)**.
Surveillez la progression de la mise à jour dans le centre de messages. Même si le centre de messages n'affiche aucune progression pendant plusieurs minutes ou indique que la mise à jour a échoué, ne redémarrez pas la mise à jour. Communiquez plutôt avec Centre d'assistance technique Cisco (TAC).
- Étape 5** Vérifiez la mise à jour réussie.
-

Prochaine étape

Si vous n'avez pas effectué le déploiement dans le cadre de la mise à jour, déployez maintenant.

Importer les règles de prévention des intrusions locales

Cette procédure vous permet d'importer des règles de prévention des intrusions locales. Les règles de prévention des intrusions importées apparaissent dans la catégorie de règle locale à l'état désactivé. Vous pouvez effectuer cette tâche dans n'importe quel domaine.

Avant de commencer

- Assurez-vous que votre fichier de règles local suit les directives décrites dans [Bonnes pratiques pour l'importation des règles de prévention des intrusions locales](#), à la page 11.
- Assurez-vous que votre processus d'importation des règles de prévention des intrusions locales est conforme à vos politiques de sécurité.

- Examinez l'effet de l'importation sur le flux de trafic et l'inspection en raison des contraintes de bande passante et des redémarrages Snort. Nous vous recommandons de planifier les mises à jour des règles pendant les périodes de maintenance.

Procédure

- Étape 1** Choisissez **System** (⚙) > **Mises à jour** > **Mises à jour de règles**.
- Étape 2** (Facultatif) Supprimez les règles locales existantes.
- Cliquez sur **Delete All Local Rules**, puis confirmez que vous souhaitez déplacer toutes les règles de prévention des intrusions créées et importées vers le dossier supprimé.
- Étape 3** Sous **One-Time Rule Update/Rules Import**(Importation de règles/Mise à jour de règles uniques), choisissez **Rule update or text rule file to upload and install** (Mise à jour de la règle ou fichier texte de la règle à téléverser et à installer), puis cliquez sur **Choose File** (sélectionner un fichier) et recherchez votre fichier de règles local.
- Étape 4** Cliquez sur **Import (Importer)**.
- Vous pouvez surveiller la progression de l'importation dans le centre de messages. Même si le centre de messages n'affiche aucune progression pendant plusieurs minutes ou indique que la mise à jour a échoué, ne redémarrez pas l'importation. Communiquez plutôt avec Centre d'assistance technique Cisco (TAC).
-

Prochaine étape

- Modifiez les politiques de prévention des intrusions et activez les règles que vous avez importées.
- Déployer les changements de configuration.

Bonnes pratiques pour l'importation des règles de prévention des intrusions locales

Respectez les consignes suivantes lors de l'importation d'un fichier de règles local :

- L'utilitaire d'importation de règles exige que toutes les règles personnalisées soient importées dans un fichier texte brut codé en ASCII ou UTF-8.
- Le nom du fichier texte peut inclure des caractères alphanumériques, des espaces et aucun caractère spécial à part un trait de soulignement (_), un point (.) et un tiret (-).
- Le système importe les règles locales précédées d'un seul caractère dièse (#), mais elles sont marquées comme supprimées.
- Le système importe les règles locales précédées d'un seul dièse (#) et n'importe pas les règles locales précédées de deux dièses (##).
- Les règles ne peuvent contenir aucun caractère État.
- Vous n'avez pas besoin de préciser d'ID de générateur (GID) lors de l'importation d'une règle locale. Si vous le faites, spécifiez uniquement le GID 1 pour une règle de texte standard.
- Lors de l'importation d'une règle pour la première fois, ne spécifiez *pas* de ID de Snort (SID) ou de numéro de révision. Cela évite les conflits avec les SID d'autres règles, y compris les règles supprimées.

Le système attribue automatiquement à la règle le prochain SID de règle personnalisée disponible, égal ou supérieur à 1000000, et un numéro de révision 1.

Si vous devez importer des règles avec un SID, celui-ci peut être n'importe quel nombre unique ou supérieur à 1 000 000.

- Lors de l'importation d'une version mise à jour d'une règle locale que vous avez importée précédemment, ou lors de la restauration d'une règle locale que vous avez supprimée, vous *devez* inclure le SID attribué par le système et un numéro de révision supérieur au numéro de révision actuel. Vous pouvez déterminer le numéro de révision d'une règle actuelle ou supprimée en modifiant la règle.



Remarque

Le système incrémente automatiquement le numéro de révision lorsque vous supprimez une règle locale; Il s'agit d'un périphérique qui vous permet de rétablir les règles locales. Toutes les règles locales supprimées sont déplacées de la catégorie de règles locales vers la catégorie de règles supprimée.

- Importez les règles locales sur le centre de gestion principal dans une paire à haute disponibilité pour éviter les problèmes de numérotation SID.
- L'importation échoue si une règle contient l'un des éléments suivants :
 - Un SID supérieur à 2147483647.
 - Une liste de ports source ou de destination qui comporte plus de 64 caractères.
- La validation de la politique échoue si vous activez une règle locale importée qui utilise le mot-clé de `threshold` (seuil) déconseillé en combinaison avec la fonction de seuillage des incidents d'intrusion dans une politique de prévention des intrusions.
- Toutes les règles locales importées sont automatiquement enregistrées dans la catégorie de règles locales.
- Le système définit toujours les règles locales que vous importez à l'état de règle désactivée. Vous devez définir manuellement l'état des règles locales avant de pouvoir les utiliser dans votre politique de prévention des intrusions.

Afficher les journaux de mise à jour des règles de prévention des intrusions

Le système génère des journaux des mises à jour et des importations de règles, classées par horodatage et utilisateur et selon la réussite ou l'échec de chaque mise à jour. Ces journaux contiennent des informations d'importation détaillées sur l'ensemble des règles et des composants mis à jour; voir [Détails des journaux de mise à jour des règles de prévention des intrusions, à la page 13](#). Utilisez cette procédure pour afficher les journaux d'importation de règles. Notez que la suppression d'un journal des importations ne supprime pas les objets importés.

Procédure

- Étape 1** Choisissez **System** (⚙) > **Mises à jour** > **Mises à jour de règles**.
- Étape 2** Cliquez sur **Rule Update Log** (Journal de la mises à jour des règles).

Étape 3 (Facultatif) Affichez les détails d'une mise à jour de règle en cliquant sur **Afficher** (🔍) à côté du fichier journal.

Détails des journaux de mise à jour des règles de prévention des intrusions



Astuces

Vous pouvez effectuer une recherche dans toute la base de données du journal d'importation de mise à jour des règles, même lorsque vous lancez une recherche, en cliquant sur **Rechercher** dans la barre d'outils dans la vue détaillée du journal d'importation de mise à jour des règles, de sorte que seuls les enregistrements d'un fichier d'importation soient affichés. Assurez-vous de définir vos contraintes de temps pour inclure tous les objets que vous souhaitez inclure dans la recherche.

Tableau 2 : Détails des journaux de mise à jour des règles de prévention des intrusions

Champ	Description
Action	<p>Une indication que l'une des situations suivantes s'est produite pour le type d'objet :</p> <ul style="list-style-type: none"> • Nouveau (pour une règle, c'est la première fois qu'elle est stockée sur cet appareil) • Modifié (dans le cas d'un composant de mise à jour de règle ou d'une règle, le composant de mise à jour de la règle a été modifié ou la règle porte un numéro de révision plus élevé et les mêmes GID et SID) • Collision (pour un composant ou une règle de mise à jour de règle, l'importation a été ignorée, car sa révision est en conflit avec un composant ou une règle existante sur le périphérique) • Supprimé (pour les règles, la règle a été supprimée de la mise à jour de la règle) • Activé (pour une modification de mise à jour de règle, un préprocesseur, une règle ou une autre fonctionnalité a été activé dans une politique par défaut fournie avec le système) • Désactivé (pour les règles, la règle a été désactivée dans une politique par défaut fournie avec le système) • Abandonner (pour les règles, la règle a été définie comme Abandon et Générer des événements dans une politique par défaut fournie avec le système) • Error (pour une mise à jour de règle ou un fichier de règles local, l'importation a échoué) • Appliquer (l'option Réappliquer toutes les politiques après la fin de l'importation de la mise à jour de la règle a été activée pour l'importation)
Action par défaut	L'action par défaut définie par la mise à jour de la règle. Lorsque le type d'objet importé est Rule (règle), l'action par défaut est Ignorer, Alerter ou Abandonner. Pour tous les autres types d'objets importés, il n'y a pas d'action par défaut.
Détails	Une chaîne unique pour le composant ou la règle. Pour les règles, GID, SID et numéro de révision précédente d'une règle modifiée, affichés comme précédemment (GID:SID:Rev). Ce champ est vide pour une règle qui n'a pas changé.
Domaine	Domaine dont les politiques de prévention des intrusions peuvent utiliser la règle mise à jour. Les politiques de prévention des intrusions dans les domaines descendants peuvent également utiliser la règle. Ce champ n'est présent que dans un déploiement multidomaine.

Champ	Description
GID	L'ID de générateur pour une règle. Par exemple, 1 (règle de texte standard, domaine global ou GID existant) ou 3 (règle d'objet partagé).
Nom	Le nom de l'objet importé, qui, pour les règles, correspond au champ de message de la règle et pour les composants de mise à jour de la règle est le nom du composant.
Politique	Pour les règles importées, ce champ affiche <code>ALL</code> (Toutes). Cela signifie que la règle a été importée avec succès et qu'elle peut être activée dans toutes les politiques de prévention des intrusions par défaut appropriées. Pour les autres types d'objets importés, ce champ est vide.
Rév.	Le numéro de révision d'une règle.
Mise à jour des règles	Nom du fichier de mise à jour des règles.
SID	Le SID pour une règle.
Durée	L'heure et la date de début de l'importation.
Type	Le type d'objet importé, qui peut être l'un des types suivants : <ul style="list-style-type: none"> composant de mise à jour de règles (un composant importé tel qu'un ensemble de règles ou un ensemble de politiques) Rule (pour règles, une règle nouvelle ou mise à jour) la politique s'applique (l'option Réappliquer toutes les politiques après la fin de l'importation de la mise à jour de la règle a été activée pour l'importation)
Nombre	Le nombre (1) de chaque enregistrement. Le champ Nombre apparaît dans une vue de tableau lorsque la table est limitée, et la vue détaillée du journal de mise à jour des règles est limitée par défaut aux enregistrements de mise à jour de règles. Il n'est pas possible de rechercher ce champ.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d'incohérence, la version anglaise du présent contenu prévaudra.