Migrer de Snort 2 vers Snort 3

À partir de la version 7.0, Snort 3 est la plateforme d'inspection par défaut des nouveaux déploiements FTD avec FMC. Si vous utilisez toujours la plateforme d'inspection Snort 2, optez dès à présent pour Snort 3 afin de bénéficier d'une détection et de performances améliorées.

Plateforme d'inspection Snort 3

Snort 3 est le moteur d'inspection par défaut pour les périphériques Cisco Firepower Threat Defense nouvellement enregistrés, avec les versions 7.0 ou ultérieures. Cependant, pour les périphériques Cisco Firepower Threat Defense de versions antérieures, Snort 2 est le moteur d'inspection par défaut. Lorsque vous mettez à niveau un périphérique géré Cisco Firepower Threat Defense vers la version 7.0 ou une version ultérieure, le moteur d'inspection reste sur Snort 2. Pour utiliser Snort 3 dans les Cisco Firepower Threat Defense mis à niveau à partir de la version 7.0 ou des versions ultérieures, vous devez l'activer explicitement. Lorsque Snort 3 est activé comme moteur d'inspection du périphérique , la version Snort 3 de la politique de prévention des intrusions qui est appliquée au périphérique (par les politiques de contrôle d'accès) est activée et appliquée à tout le trafic passant par le périphérique.

Vous pouvez changer de version de Snort au besoin. Les règles de prévention des intrusions Snort 2 et Snort 3 sont mappées et le mappage est fourni par le système. Cependant, vous pourriez ne pas trouver de mappage individuel de toutes les règles de prévention des intrusions dans Snort 2 et Snort 3. Si vous modifiez l'action de règle pour une règle dans Snort 2, cette modification n'est pas conservée si vous passez à Snort 3 sans synchroniser Snort 2 avec Snort 3. Pour plus d'informations sur la synchronisation, voir Synchroniser les règles de Snort 2 avec celles de Snort 3 , à la page 7.

Snort 2 par rapport à Snort 3

L'architecture de Snort 3 a été repensée pour inspecter plus de trafic avec des ressources équivalentes par rapport à Snort 2. Snort 3 permet une insertion simplifiée et flexible des analyseurs de trafic. Snort 3 fournit

également une nouvelle syntaxe de règles qui facilite l'écriture de règles et rend visibles les équivalents des règles d'objets partagés.

Le tableau ci-dessous répertorie les différences entre les versions Snort 2 et Snort 3 en termes de capacités du moteur d'inspection.

Fonctionnalités	Snort 2	Snort 3
Fils de paquets	Un par processus	N'importe quel nombre par processus
Utilisation de la mémoire de configuration	Nombre de processus * *x* Go	*x* Go au total; plus de mémoire disponible pour les paquets
Rechargement de la configuration	Plus lent	Plus rapide; un fil peut être épinglé à des cœurs distincts
Syntaxe des règles	Incohérent et nécessite des échappements de ligne	Système uniforme avec espaces aléatoires
Commentaire sur la règle	Commentaires seulement	les marques #, #begin et #end; Le style de langage C

Référence supplémentaire : Différences entre Snort 2 et Snort 3 dans Firepower

Conditions préalables pour les politiques d'analyse de réseau et de prévention des intrusions

Pour permettre au moteur d'inspection Snort de traiter le trafic pour l'analyse des intrusions et des programmes malveillants, la licence IPS doit être activée pour le périphérique FTD.

Vous devez être un utilisateur administrateur pour gérer l'analyse de réseau et les politiques de prévention des intrusions et effectuer les tâches de migration.

Comment migrer de Snort 2 vers Snort 3

La migration de Snort 2 vers Snort 3 nécessite de basculer le moteur d'inspection du périphérique Cisco Firepower Threat Defense de Snort 2 à Snort 3.

Selon vos besoins, les tâches pour terminer la migration de votre périphérique de Snort 2 vers Snort 3 sont énumérées dans le tableau suivant :

Étape	Tâche	Liens vers les procédures
1	Activer Snort 3	• Activer Snort 3 sur un périphérique individuel, à la page 3 • Activer Snort 3 sur plusieurs périphériques, à la page 4

Étape	Tâche	Liens vers les procédures
2	Convertir les règles personnalisées de Snort 2 en Snort 3	• Convertir toutes les règles personnalisées Snort 2 de toutes les politiques de prévention des intrusions en Snort 3, à la page 5 • Convertir les règles personnalisées Snort 2 d'une politique de prévention des intrusions unique en Snort 3, à la page 6
3	Synchroniser les règles de Snort 2 avec celles de Snort 3	Synchroniser les règles de Snort 2 avec celles de Snort 3 , à la page 7

Conditions préalables à la migration de Snort 2 vers Snort 3

Voici les conditions préalables recommandées que vous devez prendre en compte avant de migrer votre périphérique de Snort 2 vers Snort 3.

- Avoir une connaissance pratique de Snort. Pour en savoir plus sur l'architecture de Snort 3, consultez la section Adoption de Snort 3.
- Sauvegardez le centre de gestion. Reportez-vous à la section Sauvegarder le centre de gestion.
- Sauvegardez votre politique de prévention des intrusions. Voir Exportation des configurations.
- Copiez votre politique de prévention des intrusions. Pour ce faire, vous pouvez utiliser une politique existante comme politique de base pour créer une copie de votre politique de prévention des intrusions. Dans la page **Intrusion Policies** (Politiques de prévention des intrusions), cliquez sur **Create Policy** (créer une politique) et choisissez une politique de prévention des intrusions existante dans la liste déroulante **Base Policy** (Politique de base).

Activer Snort 3 sur un périphérique individuel

Important Pendant le processus de déploiement, il peut y avoir une perte de trafic momentanée car le moteur d'inspection actuel doit être arrêté.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **Device Management (gestion des appareils)**.

Étape 2 Cliquez sur le périphérique pour accéder à sa page d'accueil.

Remarque
Le périphérique est marqué comme Snort 2 ou Snort 3, ce qui affiche la version actuelle sur le périphérique.

Étape 3 Cliquez sur l'onglet **Device** (appareil).

Étape 4 Dans la section Inspection Engine (moteur d'inspection), cliquez sur **Mettre à niveau**.

Remarque
Si vous souhaitez désactiver Snort 3, cliquez sur **Revert to Snort 2** (Restaurer Snort 2) dans la section Inspection Engine (moteur d'inspection).

Étape 5 Cliquez sur **Yes** (Oui).

Prochaine étape

Déployez les modifications sur le périphérique. Consultez, Déployer les modifications de configuration, à la page 8.

Le système convertit vos configurations de politiques au cours du processus de déploiement pour les rendre compatibles avec la version sélectionnée de Snort.

Activer Snort 3 sur plusieurs périphériques

Pour activer Snort 3 sur plusieurs périphériques, assurez-vous que tous les périphériques Cisco Firepower Threat Defense requis utilisent la version 7.0 ou une version ultérieure.

Important Pendant le processus de déploiement, il peut y avoir une perte de trafic momentanée car le moteur d'inspection actuel doit être arrêté.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **Device Management (gestion des appareils)**.

Étape 2 Sélectionnez tous les périphériques sur lesquels vous souhaitez activer ou désactiver Snort 3.

Remarque
Les périphériques sont marqués comme Snort 2 ou Snort 3 et affichent la version actuelle sur le périphérique.

Étape 3 Cliquez sur la liste déroulante **Select Bulk Action** (sélectionner une action en bloc) et choisissez **Upgrade to Snort 3**(mettre à niveau vers Snort 3).

Remarque
Pour désactiver Snort 3, cliquez sur **Downgrade to Snort 2** (Rétrograder vers Snort 2).

Étape 4 Cliquez sur **Yes** (Oui).

Prochaine étape

Déployez les modifications sur le périphérique. Consultez, Déployer les modifications de configuration, à la page 8.

Le système convertit vos configurations de politiques au cours du processus de déploiement pour les rendre compatibles avec la version sélectionnée de Snort.

Convertir les règles IPS personnalisées de Snort 2 en Snort 3

Si vous utilisez un ensemble de règles d'un fournisseur tiers, communiquez avec ce fournisseur pour confirmer que ses règles ont été converties avec succès vers Snort 3 ou pour obtenir un ensemble de règles de remplacement écrit de manière native pour Snort 3. Si vous avez des règles personnalisées que vous avez écrites vous-même, familiarisez-vous avec la rédaction des règles de Snort 3 avant la conversion, afin de pouvoir mettre à jour vos règles et optimiser la détection de Snort 3 après la conversion. Consultez les liens ci-dessous pour en savoir plus sur l'écriture de règles dans Snort 3.

- https://blog.snort.org/2020/08/how-rules-are-improving-in-snort-3.html
- https://blog.snort.org/2020/10/talos-transition-to-snort-3.html

Vous pouvez consulter d'autres blogs à l'adresse https: // blog.snort.org/ pour en savoir plus sur les règles Snort 3.

Consultez les procédures suivantes pour convertir les règles Snort 2 en règles Snort 3 à l'aide de l'outil fourni par le système.

- Convertir toutes les règles personnalisées Snort 2 de toutes les politiques de prévention des intrusions en Snort 3, à la page 5
- Convertir les règles personnalisées Snort 2 d'une politique de prévention des intrusions unique en Snort 3, à la page 6

Important Les paramètres de politique d'analyse de réseau (NAP) de Snort 2 *ne peuvent pas* être copiés dans Snort 3 automatiquement. Les paramètres de Politique d'analyse de réseau (NAP) doivent être répliqués manuellement dans Snort 3.

Convertir toutes les règles personnalisées Snort 2 de toutes les politiques de prévention des intrusions en Snort 3

Procédure

Étape 1 Choisissez **Objects (Objets)** > **Intrusion Rules (Règles de prévention des intrusions)**.

Étape 2 Cliquez sur l'onglet **Snort 3 All Rules (toutes les règles Snort 3)**.

Étape 3 Assurez-vous que **Toutes les règles** est sélectionné dans le volet gauche.

Étape 4 Cliquez sur la liste déroulante **Tasks** (Tâches) et sélectionnez :

- (Convertir et importer) (Convertir les règles de Snort 2 et les importer) : pour convertir automatiquement toutes les règles personnalisées Snort 2 dans toutes les politiques de prévention des intrusions vers Snort 3 et les importer dans FMC en tant que règles personnalisées Snort 3.
- (Convertir et télécharger) (Convertir les règles Snort 2 et les télécharger) : pour convertir automatiquement toutes les règles personnalisées de Snort 2 pour toutes les politiques de prévention des intrusions vers Snort 3 et les télécharger dans votre système local.

Étape 5 Cliquez sur **OK**.

Remarque

- Si vous avez sélectionné **Convert and import** à l'étape précédente, alors toutes les règles converties sont enregistrées dans un nouveau groupe de règles **All Snort 2 Converted Global** sous **Local Rules** (Règles locales).
- Si vous avez sélectionné **Convert and download** à l'étape précédente, enregistrez le fichier de règles localement. Vous pouvez consulter les règles converties dans le fichier téléchargé et les téléverser ultérieurement en suivant les étapes décrites dans Ajouter des règles personnalisées aux groupes de règles.

Reportez-vous à la vidéo Conversion des règles Snort 2 en règles Snort 3 pour obtenir de l'aide et des renseignements supplémentaires.

Prochaine étape

Déployez les modifications de configuration; voir Déployer les modifications de configuration, à la page 8.

Convertir les règles personnalisées Snort 2 d'une politique de prévention des intrusions unique en Snort 3

Procédure

Étape 1 Choisissez **Policies (Politiques)** > **Access Control heading (En-tête Contrôle d'accès)** > **Intrusion**.

Étape 2 Dans l'onglet **Intrusion Policies** (politiques de prévention des intrusions), cliquez sur **Show Snort 3 Sync status** (Afficher l'état de la synchronisation Snort).

Étape 3 Cliquez sur l'icône **Sync Désynchronisation de Snort** ( ) de la politique de prévention des intrusions.

Remarque
Si les versions Snort 2 et Snort 3 de la politique de prévention des intrusions sont synchronisées, l'icône **Sync** est de couleur verte**Versions Snort synchronisées** ( ). Cela indique qu'il n'y a aucune règle personnalisée à convertir.

Étape 4 Lisez le résumé et cliquez sur l'onglet **Règles personnalisées**.

Étape 5 Choisissez :

- **Importer les règles converties dans cette politique** : pour convertir les règles personnalisées de Snort 2 de la politique de prévention des intrusions vers Snort 3 et les importer dans FMC en tant que règles personnalisées de Snort 3.
- **Télécharger les règles converties** : pour convertir les règles personnalisées Snort 2 de la politique de prévention des intrusions vers Snort 3 et les télécharger dans votre système local. Vous pouvez consulter les règles converties dans le fichier téléchargé, puis téléverser le fichier ultérieurement en cliquant sur l'icône de chargement.

Étape 6 Cliquez sur **Re-Sync** (Resynchroniser).

Prochaine étape

Déployez les modifications de configuration; voir Déployer les modifications de configuration, à la page 8.

Afficher le mappage de politique de base Snort 2 et Snort 3

Procédure

Étape 1 Choisissez **Policies (Politiques)** > **Access Control heading (En-tête Contrôle d'accès)** > **Intrusion**.

Étape 2 Assurez-vous que l'onglet **Intrusion Policies** (Politiques de prévention des intrusions) est sélectionné.

Étape 3 Cliquez sur **IPS Mapping** (Mappage IPS).

Étape 4 Dans la boîte de dialogue **IPS Policy Mapping** (Mappage de politique IPS), cliquez sur **View Mappings** (Afficher les mappages) pour afficher le mappage de la politique de prévention des intrusions de Snort 3 à Snort 2.

Étape 5 Cliquez sur **OK**.

Synchroniser les règles de Snort 2 avec celles de Snort 3

Pour s'assurer que les paramètres et les règles personnalisées de la version Snort 2 sont conservés et transférés dans Snort 3, FMC fournit la fonctionnalité de synchronisation. La synchronisation aide les paramètres de règles de Snort 2 à remplacer les règles et les paramètres de règles personnalisées, que vous avez peut-être modifiés et ajoutés au cours des derniers mois ou années, pour être répliqués sur la version Snort 3. Cet utilitaire sert à synchroniser la configuration de la politique de Snort 2 avec la version de Snort 3 pour commencer avec une couverture semblable.

Si FMC est mis à niveau de la version 6.7 ou antérieure vers la version 7.0 ou ultérieure, le système synchronise la configuration. S'il s'agit d'une nouvelle version 7.0 ou d'une version ultérieure, vous pouvez effectuer une mise à niveau vers une version ultérieure FMC. Le système ne synchronisera aucun contenu pendant la mise à niveau.

Avant de mettre à niveau un appareil vers Snort 3, si des modifications sont apportées à la version de Snort 2, vous pouvez vous servir de cet utilitaire afin d'obtenir la dernière synchronisation de la version de Snort 2 vers la version de Snort 3 et ainsi commencer avec une couverture semblable.

Remarque Après le passage vers Snort 3, il est recommandé de gérer la version Snort 3 de la politique de façon indépendante et de ne pas utiliser cet utilitaire comme fonctionnement normal.

Important

- Seuls les remplacements de règles Snort 2 et les règles personnalisées sont copiés dans Snort 3 et non le contraire. Il se peut que vous ne trouviez pas de mappage individuel de toutes les règles de prévention des intrusions dans Snort 2 et Snort 3 Vos modifications apportées aux actions liées aux règles pour les règles qui existent dans les deux versions sont synchronisées lorsque vous effectuez la procédure suivante.
- La synchronisation *ne migre pas* les paramètres de seuil et de suppression des règles personnalisées ou fournies par le système de Snort 2 vers Snort 3.

Procédure

Étape 1 Choisissez **Policies (Politiques)** > **Access Control heading (En-tête Contrôle d'accès)** > **Intrusion**.

Étape 2 Assurez-vous que l'onglet **Intrusion Policies** (Politiques de prévention des intrusions) est sélectionné.

Étape 3 Cliquez sur **Afficher l'état de synchronisation de Snort 3**

Étape 4 Déterminez la politique de prévention des intrusions désynchronisée.

Étape 5 Cliquez sur l'icône **Sync Désynchronisation de Snort** ( ).

Remarque
Si les versions Snort 2 et Snort 3 de la politique de prévention des intrusions sont synchronisées, l'icône **Sync** est de couleur verte**Versions Snort synchronisées** ( ).

Étape 6 Lisez le résumé et téléchargez-en une copie si nécessaire.

Étape 7 Cliquez sur **Re-Sync** (Resynchroniser).

Remarque

- Les paramètres synchronisés ne seront applicables sur le moteur de prévention des intrusions Snort 3 que s'ils sont appliqués sur un périphérique et après un déploiement réussi.
- Les règles personnalisées Snort 2 peuvent être converties vers Snort 3 à l'aide de l'outil fourni par le système. Si vous avez des règles personnalisées Snort 2, cliquez sur l'onglet Règles personnalisées et suivez les instructions à l'écran pour convertir les règles. Pour en savoir plus, consultez Convertir les règles personnalisées Snort 2 d'une politique de prévention des intrusions unique en Snort 3, à la page 6.

Prochaine étape

Déployez les modifications de configuration; voir Déployer les modifications de configuration, à la page 8.

Déployer les modifications de configuration

Après avoir modifié les configurations, déployez-les sur les appareils ciblés.

Remarque Cette rubrique couvre les étapes de base du déploiement des modifications de configuration. Nous vous recommandons *fortement* de consulter la rubrique sur le *déploiement des modifications de configuration* dans la dernière version du *Guide de configuration de Cisco Firepower Management Center* pour comprendre les conditions préalables et les conséquences du déploiement des modifications avant de poursuivre les étapes.

Mise en garde Lorsque vous déployez, les demandes de ressources peuvent entraîner l'abandon un petit nombre de paquets sans inspection. En outre, le déploiement de certaines configurations redémarre le processus Snort, qui interrompt l'inspection du trafic. Pendant cette interruption, la diminution de trafic ou son passage sans inspection dépend de la façon dont l'appareil cible gère le trafic.

Procédure

Étape 1 Dans la barre de menus Cisco Firepower Management Center, cliquez sur **Deploy** (déployer) puis sélectionnez **Deployment** (déploiement).

La page de GUI répertorie les périphériques dont les configurations sont obsolètes et dont l'état est en **attente**.

- La colonne **Modified By** (modifié par) répertorie les utilisateurs qui ont modifié les politiques ou les objets. En développant la liste des appareils, vous pouvez afficher les utilisateurs qui ont modifié les politiques par rapport à chaque liste de politiques.

  Remarque
  Les noms d'utilisateur ne sont pas fournis pour les politiques et objets supprimés.

- La colonne **Inspect Interruption** (inspecter l'interruption) indique si une interruption de l'inspection du trafic peut se produire dans le périphérique pendant le déploiement.

  Si cette colonne est vide pour un périphérique, cela signifie qu'il n'y aura pas d'interruption de l'inspection du trafic sur ce périphérique pendant le déploiement.

- La colonne **Last Modified Time** (heure de la dernière modification) indique la dernière fois que vous avez modifié la configuration.
- La colonne **Preview** (aperçu) vous permet de prévisualiser les modifications pour le prochain déploiement.
- La colonne **Status** (état) indique l'état de chaque déploiement.

Étape 2 Définissez et choisissez les appareils sur lesquels vous souhaitez déployer les modifications de configuration.

- Search (rechercher) : Faites une recherche par nom, type, domaine, groupe ou état du périphérique dans le champ de recherche.
- Expand (développer) : Cliquez sur **Flèche Développer** ( ) pour afficher les modifications de configuration propres au périphérique à déployer.

  Lorsque vous cochez une case à côté d'un périphérique, toutes les modifications apportées au périphérique et répertoriées sous ce dernier sont transmises pour déploiement. Cependant, vous pouvez utiliser **Sélection de politique** ( ) pour sélectionner des politiques ou des configurations spécifiques à déployer tout en conservant les modifications restantes sans les déployer.

  Remarque
  - Lorsque l'état de la colonne **Inspect Interruption** (interruption de l'inspection) indique (**Yes** (oui)) que le déploiement interrompra l'inspection, et peut-être le trafic, sur un appareil Cisco Firepower Threat Defense, la liste étendue indique les configurations particulières causant l'interruption avec **Inspecter l'interruption** ( ).

- Lorsque des changements sont apportés aux groupes d'interface, aux zones de sécurité ou aux objets, les appareils touchés sont affichés comme étant périmés sur FMC. Pour vous assurer que ces modifications prennent effet, les politiques relatives à ces groupes d'interface, zones de sécurité ou objets doivent également être déployées avec les modifications. Les politiques concernées sont indiquées comme étant obsolètes sur la page **Prévisualisation** de FMC.

Étape 3 Cliquez sur **Deploy** (déployer).

Étape 4 Si le système détecte des erreurs ou des avertissements dans les modifications à déployer, il les affiche dans la fenêtre **Validation Messages** (messages de validation). Pour afficher tous les détails, cliquez sur l'icône en forme de flèche avant les avertissements ou les erreurs.

Vous avez les choix suivants :

- Deploy (déployer) : Continuer le déploiement sans résoudre les conditions de mise en garde. Vous ne pouvez pas continuer si le système détecte des erreurs.
- Close (fermer) : Quitter sans déployer. Vous devrez résoudre les conditions d'erreur et de mise en garde, puis réessayer de déployer la configuration.

Prochaine étape

Pendant le déploiement, en cas d'échec du déploiement pour quelque raison que ce soit, il est possible que l'échec influe sur le trafic. Cependant, cela dépend de certaines conditions. S'il y a certains changements de configuration dans le déploiement, l'échec du déploiement peut entraîner une interruption du trafic. Pour en savoir plus, consultez la rubrique sur le déploiement des modifications de la dernière version du *Guide de configuration de Cisco Firepower Management Center* .

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.

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.

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.