



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 Firewall Threat Defense avec Firewall Management Center. Snort 3 est requis dans la version 7.7 ou ultérieure. 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.

La mise à niveau de Firewall Threat Defense vers les versions 7.2 à 7.6 met également à niveau les périphériques Snort 2 éligibles vers Snort 3. Pour les périphériques qui ne sont pas éligibles, car ils utilisent des politiques de prévention des intrusions ou d'analyse de réseau personnalisées, procédez à une mise à niveau manuelle vers Snort 3, comme décrit ici.

Bien qu'il soit possible de rétablir des périphériques individuels, cette action est déconseillée. La mise à niveau de Firewall Threat Defense vers la version 7.7 ou ultérieure est bloquée pour les périphériques Snort 2.

- [Plateforme d'inspection Snort 3, à la page 1](#)
- [Snort 2 par rapport à Snort 3, à la page 2](#)
- [Migration de Snort 2 vers Snort 3, à la page 2](#)
- [Afficher le mappage de politique de base Snort 2 et Snort 3, à la page 7](#)
- [Synchroniser les règles de Snort 2 avec celles de Snort 3, à la page 8](#)
- [Déploiement des modifications de configuration, à la page 10](#)
- [Exemples de migration, à la page 12](#)

Plateforme d'inspection Snort 3

Snort 3 est un moteur d'inspection de réseau qui

- sert de moteur d'inspection par défaut pour les périphériques Firewall Threat Defense nouvellement enregistrés sur la version 7.0 ou ultérieure,
- nécessite une activation explicite après la mise à niveau des périphériques Firewall Threat Defense vers la version 7.0 ou une version ultérieure, et
- active la version Snort 3 de la politique de prévention des intrusions, qui est appliquée par le biais des politiques de contrôle d'accès, pour tout le trafic passant par le périphérique.

Pour les périphériques Firewall Threat Defense sur la version 6.x ou toute version antérieure, Snort 2 est le moteur d'inspection par défaut.

Commutation de version et mappage de règles

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 8.

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](#)

Migration de Snort 2 vers Snort 3

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

process_summary

Selon vos besoins, passez par les étapes énumérées dans le flux de travail pour terminer la migration de votre périphérique de Snort 2 vers Snort 3.

process_workflow

Voici les étapes de la migration de Snort 2 vers Snort 3 :

1. Activez Snort 3 sur le périphérique.
 - [Activer Snort 3 sur un périphérique individuel, à la page 3](#)
 - [Activer Snort 3 sur plusieurs périphériques, à la page 4](#)
2. Convertissez 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. Synchronisez les règles de Snort 2 avec celles de Snort 3.
 - [Synchroniser les règles de Snort 2 avec celles de Snort 3, à la page 8](#)

Conditions préalables à la migration de Snort 2 vers Snort 3

Tenez compte des conditions préalables recommandées avant de migrer votre appareil de Snort 2 à 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

Activez Snort 3 sur un périphérique individuel pour profiter de fonctionnalités de sécurité renforcées.

Utilisez cette procédure lorsque vous devez mettre à niveau un périphérique spécifique du moteur d'inspection Snort 2 à Snort 3. Le système convertit vos configurations de politiques au cours du processus de déploiement pour les rendre compatibles avec la version sélectionnée de Snort.



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 (périphériques)** > **Device Management (gestion des périphériques)**.

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 [Déploiement des modifications de configuration, à la page 10](#).

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

Cette tâche permet à Snort 3 sur plusieurs périphériques de fournir des capacités de détection d'intrusion améliorées.

Pour activer Snort 3 sur plusieurs périphériques, assurez-vous que tous les périphériques Firewall 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 (périphériques) > Device Management (gestion des périphériques)**.

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).
- Étape 4** Cliquez sur **Yes** (Oui).

Prochaine étape

Déployez les modifications sur le périphérique. Consultez [Déploiement des modifications de configuration](#), à la page 10.

Convertir les règles IPS personnalisées de Snort 2 en Snort 3

La conversion des règles IPS personnalisées Snort 2 au format Snort 3 est un processus de migration qui modifie les règles du système de prévention des intrusions personnalisées du format Snort 2 au format Snort 3.

Exigences de conversion et ressources

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.

Convertissez les règles personnalisées Snort 2 existantes au format Snort 3 mis à jour pour assurer la compatibilité avec les systèmes de détection d'intrusion actuels.

Cette tâche migre les règles personnalisées Snort 2 existantes vers le format Snort 3, vous permettant de conserver vos configurations de règles personnalisées lors de la mise à niveau vers le dernier moteur de détection d'intrusion. Vous pouvez soit importer les règles converties directement, soit les télécharger pour les consulter avant de les importer.

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) **Convert Snort 2 rules and import** (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 Firewall Management Center en tant que règles personnalisées Snort 3.
 - (Convertir et télécharger) **Convert Snort 2 Rules and download** (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

Déployer les modifications de configuration. Consultez [Déploiement des modifications de configuration](#), à la page 10.

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

Convertissez les règles personnalisées Snort 2 dans une politique de prévention des intrusions au format Snort 3 pour maintenir la compatibilité avec les environnements Snort 3.

Lors de la migration vers Snort 3, les règles personnalisées Snort 2 existantes doivent être converties pour conserver leurs fonctionnalités. Cette tâche vous permet de convertir des règles personnalisées pour une politique de prévention des intrusions spécifique.

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 bleue **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 **Custom Rules** (Règles personnalisées).

Étape 5 Choisissez :

- **Import converted rules to this policy** (Importer les règles converties dans cette politique) : pour convertir les règles personnalisées Snort 2 de la politique de prévention des intrusions vers Snort 3 et les importer dans Firewall Management Center en tant que règles personnalisées Snort 3.
- **Download converted rules** (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

Déployer les modifications de configuration. Consultez [Déploiement des modifications de configuration, à la page 10](#).

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

Cette tâche vous permet d'afficher le mappage entre les politiques de prévention des intrusions Snort 3 et Snort 2.



Remarque Snort 2 n'est pas pris en charge sur Threat Defense, version 7.7. Pour en savoir plus sur les fonctionnalités de Snort 2 qui sont prises en charge dans les versions antérieures à 7.7, consultez le guide [Firewall Management Center](#) correspondant à votre version Firewall Threat Defense.

Procédure

-
- Étape 1** Choisissez **Politiques (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

Cette tâche permet de s'assurer que les paramètres de remplacement de règles Snort 2 et les règles personnalisées sont répliqués sur Snort 3, vous permettant de commencer avec une couverture similaire lors de la transition entre les versions.

Pour s'assurer que les paramètres et les règles personnalisées de la version Snort 2 sont conservés et transférés dans Snort 3, Firewall Management Center 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.



Remarque Snort 2 n'est pas pris en charge sur Threat Defense, version 7.7. Pour en savoir plus sur les fonctionnalités de Snort 2 qui sont prises en charge dans les versions antérieures à 7.7, consultez le guide [Firewall Management Center](#) correspondant à votre version Firewall Threat Defense.

Si Firewall Management Center 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 Firewall Management Center. 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 Lorsque vous passez à Snort 3, gérez la version Snort 3 de la politique de manière indépendante. N'utilisez pas cet utilitaire comme une opération normale.

**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 bleue **Versions Snort synchronisées** (→).

- Étape 6** Lisez le résumé. Téléchargez une copie du résumé, au besoin.
- 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 Custom Rules (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

Déployer les modifications de configuration. Consultez [Déploiement des modifications de configuration](#), à la page 10.

Déploiement des modifications de configuration

Déployez les modifications de configuration pour vous assurer que les modifications apportées aux configurations des périphériques prennent effet sur les périphériques concernés.

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 vous reporter à la rubrique sur le *déploiement des modifications de configuration* dans la dernière version du [Guide de configuration des appareils du système de gestion de Cisco Secure Firewall](#) pour comprendre les conditions préalables et les conséquences du déploiement des modifications avant de procéder aux étapes.



Mise en garde

Lorsque vous déployez, les demandes de ressources peuvent entraîner l'abandon d'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 Firewall 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.

- Recherche : recherchez par nom, type, domaine, groupe ou état du périphérique dans le champ de recherche.
- Développer : cliquez sur **Flèche Développer** (►) pour afficher les modifications de configuration propres au périphérique à déployer.

Si vous cochez une case à côté d'un périphérique, toutes les modifications apportées à ce périphérique et répertoriées pour le périphérique sont incluses dans le 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 Firewall 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 Firewall Management Center. 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 Firewall Management Center.

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 :

- Déployer : continuer le déploiement sans résoudre les conditions de mise en garde. Vous ne pouvez pas continuer si le système détecte des erreurs.
- Fermer : quitter sans déployer. Vous devrez résoudre les conditions d'erreur et de mise en garde, puis réessayer de déployer la configuration.

Les modifications de configuration sont déployées sur les périphériques sélectionnés et prennent effet en fonction des paramètres de déploiement.

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 Déployer les modifications de configuration dans la dernière version du [Guide de configuration des appareils du système de gestion de Cisco Secure Firewall](#).

Exemples de migration

Migrer de Snort 2 vers Snort 3

Migration de Snort 2 vers Snort 3

- implique la conversion et l'adaptation des règles Snort 2 à la syntaxe de la règle Snort 3,
- optimise les règles pour améliorer la détection et les performances, et
- permet aux entreprises de tirer parti des fonctionnalités et des capacités améliorées de Snort 3.

Les entreprises dont les périphériques de protection contre les menaces sont gérés par le centre de gestion de pare-feu Cisco Secure Firewall Management Center peuvent choisir une approche de déploiement hybride lors de la migration de Snort 2 à Snort 3. Cette approche permet une transition graduelle et réduit les perturbations potentielles, le cas échéant.

Avantages de la migration vers Snort 3

Snort 3 fournit

- **Enhanced protocol support** (Prise en charge améliorée des protocoles) : Snort 3 offre une prise en charge améliorée des protocoles, vous permettant de détecter et de superviser les menaces sur un large éventail de protocoles modernes, y compris le trafic chiffré.
- **Streamlined rule management** (Gestion simplifiée des règles) : Snort 3 offre un langage de règles et un système de gestion de règles plus convivial, ce qui permet de créer, de modifier et de gérer efficacement les règles.
- **Improved performance** (Performances améliorées) : Snort 3 a été optimisé pour gérer des volumes de trafic plus élevés plus efficacement, ce qui garantit une détection rapide des menaces et réduit le risque de goulot d'étranglement des performances.

Exemple de scénario d'entreprise

Cet exemple de scénario d'entreprise est une situation illustrative qui

- montre comment les entreprises évaluent les migrations des moteurs d'inspection de sécurité des réseaux,
- affiche les rôles et les motivations des analystes de sécurité et des administrateurs réseau dans les décisions en matière de technologie, et
- met en évidence les avantages de la mise à niveau des solutions de surveillance de sécurité existantes vers les solutions de surveillance de sécurité modernes.

Scénario de migration organisationnelle

Alice travaille en tant qu'analyste en sécurité dans une grande organisation qui s'appuie fortement sur le moteur d'inspection Snort pour superviser et protéger son infrastructure réseau. L'organisation utilise Snort version 2 depuis plusieurs années, mais elle a rencontré des limites et des défis.

Bob, l'administrateur réseau, envisage de migrer de Snort 2 à Snort 3 pour résoudre ces problèmes et améliorer les capacités de sécurité du réseau de son organisation.

Cette migration améliorera également la supervision de la sécurité du réseau, améliorera les performances et simplifiera la gestion des règles.

Bonnes pratiques pour la migration de Snort 2 à Snort 3

Suivez ces bonnes pratiques lors de la migration de Snort 2 vers Snort 3 pour assurer l'intégrité des données et maintenir la couverture de sécurité.

- Sauvegardez votre politique de prévention des intrusions avant d'effectuer la migration. Consultez la tâche Exporter les configurations dans le [Guide d'administration de Cisco Secure Firewall Management Center de Cisco Secure Firewall Management Center](#).
- Avant de mettre à niveau un périphérique vers Snort 3, si des modifications sont apportées dans Snort 2, utilisez l'utilitaire de synchronisation pour inclure la dernière synchronisation de Snort 2 à Snort 3 afin de pouvoir commencer avec une couverture similaire. Consultez [Synchroniser les règles de Snort 2 avec celles de Snort 3](#), à la page 8.
- Les règles personnalisées Snort 2 ne sont pas automatiquement converties en Snort 3 et doivent être migrées manuellement. Consultez [Convertir les règles IPS personnalisées de Snort 2 en Snort 3](#), à la page 5.
- La synchronisation ne migre pas les règles Snort 2 avec des seuils ou des suppressions. Ces règles doivent être créées à nouveau dans Snort 3.

Préalables pour la migration

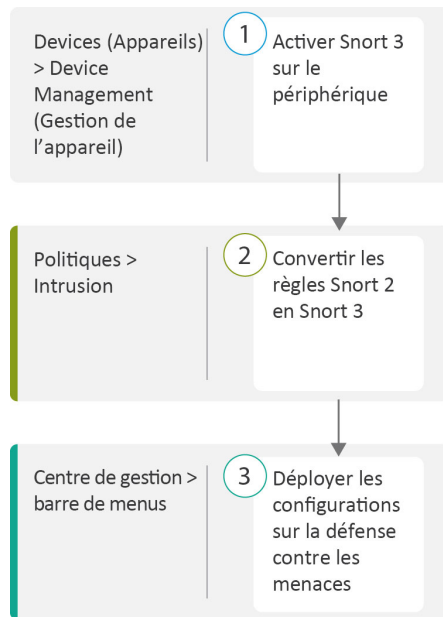
Remplissez ces conditions préalables avant de commencer le processus de migration pour assurer l'état de préparation du système et la protection des données.

- 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](#).

Flux de travail de migration de bout en bout

process_summary

Selon vos besoins, passez par les étapes énumérées dans le flux de travail pour terminer la migration de votre périphérique de Snort 2 vers Snort 3.

process_workflow

Voici les étapes de la migration de Snort 2 vers Snort 3 :

1. Activez Snort 3 sur le périphérique. Consultez [Activer Snort 3 sur le périphérique de protection contre les menaces, à la page 14](#).
2. Convertir les règles Snort 2 en Snort 3. Consultez [Convertir les règles Snort 2 d'une politique de prévention des intrusions unique en Snort 3, à la page 15](#).
3. Déployez la configuration. Consultez [Déploiement des modifications de configuration, à la page 10](#).

Activer Snort 3 sur le périphérique de protection contre les menaces

Activez Snort 3 sur votre périphérique de protection contre les menaces pour améliorer les capacités de sécurité.

Utilisez cette procédure pour effectuer une mise à niveau de Snort 2 à Snort 3 sur votre périphérique de protection contre les menaces.

**Attention**

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 (périphériques) > Device Management (gestion des périphériques) . |
| Étape 2 | Cliquez sur le périphérique pour accéder à sa page d'accueil. |
| Étape 3 | Cliquez sur l'onglet Device (appareil). |
| Étape 4 | Dans la section Inspection Engine (Moteur d'inspection), cliquez sur Inspection Engine (Mise à niveau). |

Inspection Engine

Inspection Engine:

Snort 2

Before you upgrade, read and understand the Snort 3 configuration guide for your version: <https://www.cisco.com/go/fmc-snort3>. Pay special attention to feature limitations and migration instructions. Although upgrading to Snort 3 is designed for minimal impact, features do not map exactly. Custom intrusion rules are not automatically migrated during upgrade but **options** are available to migrate. Careful planning and preparation can help you make sure that traffic is handled as expected.

Upgrading to Snort 3 also deploys configuration changes to affected devices. This briefly interrupts traffic flow and inspection on all devices, including those configured for high availability/scalability. Interface configurations determine whether traffic drops or passes without inspection during the interruption. For details, see the [Snort Restart Traffic Behavior](#) section in the online help.

Upgrade to Snort3 should be done during a maintenance window.

Étape 5

Cliquez sur **Yes** (Oui).

Prochaine étape

Déployez les modifications sur le périphérique. Consultez [Déploiement des modifications de configuration, à la page 10](#).

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 Snort 2 d'une politique de prévention des intrusions unique en Snort 3

Cette tâche synchronise et convertit les règles de politique de prévention des intrusions Snort 2 au format Snort 3, en veillant à ce que les règles personnalisées, les seuils et les suppressions soient correctement migrés pour maintenir l'efficacité de la politique de sécurité lors de l'utilisation des moteurs Snort 3.

Lorsque les politiques de prévention des intrusions affichent un indicateur de flèche orange, les versions Snort 2 et Snort 3 ne sont pas synchronisées. Le processus de synchronisation utilise l'outil snort2Lua pour convertir les règles et peut nécessiter une intervention manuelle pour les règles, les seuils et les suppressions personnalisés qui ne peuvent pas être migrés automatiquement.

Before you begin

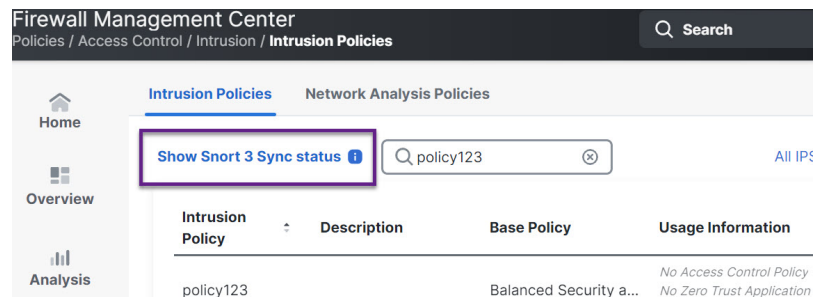
Suivez ces étapes pour convertir les règles Snort 2 d'une politique de prévention des intrusions unique en Snort 3 :

Procédure

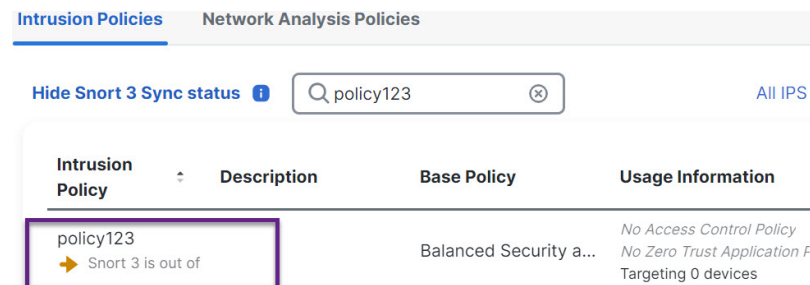
Étape 1

Choisissez **Politiques (Politiques)** > **Access Control heading (En-tête Contrôle d'accès)** > **Intrusion** > **Intrusion Policies (Politiques de prévention des intrusions)**.

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



Si votre politique affiche une flèche orange, cela indique que les versions Snort 2 et Snort 3 de la politique de prévention des intrusions ne sont pas synchronisées.



- b) Cliquez sur la flèche orange.

La page **Snort 2 to Snort 3 Sync Summary** (Résumé de la synchronisation Snort 2 to Snort 3) montre que la synchronisation de Snort 2 à Snort 3 est en attente.

Snort 2 to Snort 3 Sync Summary ?

This is a utility to synchronize Snort 2 policy configuration with Snort 3 version to start with a similar coverage.

- Snort 3 policy configuration is synced from Snort 2 version by the system when Firewall Management Center is upgraded from pre-7.0 version.
- Before upgrading a device to Snort 3, if changes are made in Snort 2 version, you can use this utility to have the latest synchronization from Snort 2 version to Snort 3 version so that you start with similar coverage.

Note: After moving to Snort 3, it is recommended that you manage the Snort 3 version of the policy independently and do not use this utility as a regular operation.

[Click here](#) to learn more.

Policy Name: policy123

➔ Snort 3 and Snort 2 Sync Pending 2025-01-10 03:49:25 EST

Used by: No Access Control Policy | No Device

Re-Sync

Close

- c) Cliquez sur **Re-Sync** (Resynchroniser) pour lancer la synchronisation.



Remarque

Lorsque vous cliquez sur **Re-Sync** (Resynchroniser), l'outil snort2Lua convertit les règles de Snort 2 en Snort 3.

La section **Summary Details** (Détails du résumé) répertorie les règles qui ont été migrées ou ignorées. Dans notre cas d'utilisation, il y a 76 règles Snort 2 personnalisées, 17 règles avec seuils et 15 règles avec suppression qui ont été ignorées pendant le processus de synchronisation. Pour migrer les règles personnalisées, passez à l'étape suivante.

Policy Name: _Intrusion_Policy_1

➔ Snort 3 is partially in sync with Snort 2. 2023-08-01 05:42:52 EDT

Used by: 1 Access Control Policy | 0 Devices (Snort 2), 1 Devices (Snort 3)

Summary Details

Rule Overrides

● Based on Talos rule-mapping 18639 Snort 2 rule action overrides migrated to 18635 Snort 3 rules.

▲ Rules migration skipped for 17 rules with threshold, 15 rules with suppression, as sync of Suppression and Threshold setting(s) are not supported.

▲ Rules migration skipped for 76 custom rules, as sync of Custom Rule setting(s) are not supported. You can manually convert the Snort 2 custom rules to Snort 3 using the snort2Lua tool.

[Download Summary Details](#)

Overridden

Advanced

Custom Rules

The custom rules are not auto-converted to the Snort 3 version, as Snort 3 rules are written differently compared to Snort 2 rules. Use one of the following options to convert the custom rules manually:

Pour migrer des règles avec des seuils et des suppressions, passez à l'étape 6.

Policy Name: **_Intrusion_Policy_1**

➔ **Snort 3 is partially in sync with Snort 2.** 2023-08-01 05:42:52 EDT

Used by: 1 Access Control Policy | 0 Devices (Snort 2), 1 Devices (Snort 3)

Summary Details

Rule Overrides

● Based on Talos rule-mapping 18639 Snort 2 rule action overrides migrated to 18635 Snort 3 rules.

▲ Rules migration skipped for 17 rules with threshold, 15 rules with suppression, as sync of Suppression and Threshold setting(s) are not supported.

▲ Rules migration skipped for 76 custom rules, as sync of Custom Rule setting(s) are not supported. You can manually convert the Snort 2 custom rules to Snort 3 using the snort2Lua tool.

[Download Summary Details](#)

Overridden

Advanced

Custom Rules

The custom rules are not auto-converted to the Snort 3 version, as Snort 3 rules are written differently compared to Snort 2 rules. Use one of the following options to convert the custom rules manually:

Étape 2

Pour migrer les 76 règles personnalisées, effectuez l'une des étapes suivantes :

- Dans l'onglet **Custom Rules** (Règles personnalisées), cliquez sur l'icône **Import** (Importer) pour convertir et charger automatiquement les règles locales dans la version Snort 3 de la politique.

Overridden

Advanced

Custom Rules

Convert the rules and auto-import them to the Snort 3 version of the policy 

OR

Download converted rules  You can upload the file after you have reviewed the converted rules 

Un message de confirmation s'affiche une fois les règles importées.

- Choisissez **Objects (Objets) > Intrusion Rules (Règles de prévention des intrusions)** et cliquez sur **Snort 3 All Rules** (Toutes les règles).
 1. Cliquez sur **Local Rules** (Règles locales) dans le volet de gauche pour vérifier si des règles ont été migrées. Remarquez qu'aucune règle personnalisée de Snort 2 n'a été migrée.
 2. Dans la liste déroulante **Tasks** (Tâches), choisissez **Convert Snort 2 rules and import** (Convertir les règles Snort 2 et les importer).

< Intrusion Policy

All Rules

> Local Rules(1 group)

> MITRE(1 group)

> Rule Categories(9 groups)

All Rules

All rules assigned to current intrusion policy

Rule Actions

1 ☒ | 51,056 rules

☐

GID:SID

Info

>

☐

133:3

(dce_smb)...

3. Cliquez sur **OK**.

Snort 2 All Rules

Snort 3 All Rules

< Intrusion Policy

Back To Top

All Rules

All rules assigned to current intrusion policy irrespective of rule group

Rule Actions

Search by CVE, SID, Reference Info, or Rule Message

Tasks

49,218 rules

☐

GID:SID

Info

Rule Action

Assigned Groups

Alert Configuration

>

☐

112:1

(arp_spoof) unicast ARP request

Disable (Default)

Protocol/Builtins

None

>

☐

105:3

(back_office) Back Office server traffic detec...

Disable (Default)

Protocol/Builtins

None

Local Rules (2 groups)

All Snort 2 Converted Global

Intrusion_Policy_1_custom_rules

Browser (6 groups)

Server (9 groups)

Policy (4 groups)

Indicator (4 groups)

The custom rules were successfully imported

Un groupe de règles nommé **All Snort 2 Converted Global** (Tous les éléments Snort 2 convertis - Global) est maintenant créé sous **Local Rules** (Règles locales) dans le volet de gauche.

Remarquez que les 76 règles personnalisées ont été migrées, comme le montre la figure suivante.

< Intrusion Policy

Back To Top

All Rules

Local Rules / Intrusion_Policy_1_custom_rules

Description

Group created for custom rules enabled in snort 2 version

Rule Actions

Search by CVE, SID, Reference Info, or Rule Message

Tasks

76 rules

☐

GID:SID

Info

Rule Action

Assigned Groups

Alert Configuration

>

☐

2000:1000143

http://mischa5xix2mrhd.onion/MZ2MMJ_2

Alert (Default)

All Snort 2 Converted...

None

>

☐

2000:1000139

CERT-In MALWARE THREAT EXCHANGE (CM...

Alert (Default)

All Snort 2 Converted...

None

Local Rules (2 groups)

All Snort 2 Converted Global

Intrusion_Policy_1_custom_rules

Browser (6 groups)

Server (9 groups)

Policy (4 groups)

Indicator (4 groups)

The custom rules were successfully imported

Vous pouvez également sélectionner **Convert Snort 2 rules and download** (Convertir les règles Snort 2 et les télécharger) à l'étape précédente pour enregistrer le fichier de règles localement. Vous pouvez consulter les règles converties dans le fichier téléchargé, puis les charger ultérieurement à l'aide de l'option **Upload Snort 3 rules** (Charger les règles Snort 3).

Étape 3 Cliquez sur le lien **Download Summary Details** (Télécharger les détails du résumé) pour télécharger les règles au format .txt.

Il s'agit d'un exemple du résumé qui s'affiche.

Exemple :

```
"id": "00505691-15DC-0ed3-0000-004294988561",
"name": "_Intrusion_Policy_1",
"type": "IntrusionPolicy",
"syncStatus": {
  "source": {
    "id": "bdce2d6a-1ebe-11ee-8e88-220032eb1fb5",
    "type": "IntrusionPolicy"
  },
  "status": "WARN",
  "description": "Migration is partially successful. Some of the rules are not copied to
Snort3.",
  "timestamp": 1690883954814,
  "lastUser": {
    "name": "admin"
  },
  "details": [
    {
      "type": "Summary",
      "status": "INFO",
      "description": "Based on Talos rule-mapping 18639 Snort 2 rule action overrides
migrated to 18635 Snort 3 rules."
    },
    {
      "id":
"1:1000156=alert,1:1000114=alert,1:1000160=alert,1:1000135=alert,1:1000115=alert,1:1000118=alert,

1:1000092=alert,1:1000139=alert,1:1000123=alert,1:1000159=alert,1:1000149=disabled,1:1000167=alert,

1:1000133=alert,1:1000095=alert,1:1000143=alert,1:1000106=alert,1:1000153=alert,1:1000097=alert,1:1000141=alert,

1:1000148=alert,1:1000090=alert,1:1000119=alert,1:1000112=alert,1:1000138=alert,1:1000128=alert,1:1000132=alert,

1:1000134=alert,1:1000145=disabled,1:1000110=disabled,1:1000107=alert,1:1000163=alert,1:1000124=alert,1:1000125=alert,

1:1000094=alert,1:1000113=disabled,1:1000147=alert,1:1000161=alert,1:1000105=disabled,1:1000140=alert,1:1000111=alert,

1:1000102=alert,1:1000129=disabled,1:1000108=alert,1:1000144=disabled,1:1000088=alert,1:1000091=alert,1:1000131=alert,

1:1000157=alert,1:1000120=alert,1:1000126=alert,1:1000165=alert,1:1000146=alert,1:1000162=alert,1:1000116=alert,1:1000142=alert,

1:1000170=disabled,1:1000169=alert,1:1000104=alert,1:1000099=disabled,1:1000171=alert,1:1000093=alert,1:1000087=alert,1:1000100=alert,

1:1000137=alert,1:1000158=alert,1:1000103=alert,1:1000098=alert,1:1000127=disabled,1:1000130=alert,1:1000164=alert,1:1000089=alert,

1:1000109=alert,1:1000136=alert,1:1000117=alert,1:1000166=alert,1:1000168=alert",
      "type": "PolicyInfo",
      "description": "Corresponding Snort 2 policy overridden custom (local) rules."
    }
  ]
}
```

```

    "type": "AssignedDevices",
    "status": "INFO",
    "description": "Snort3:0 , Snort2:0"
  },
  {
    "id": "122:6",
    "type": "Threshold",
    "status": "ERROR",
    "description": "PSNG_TCP_FILTERED_DECOY_PORTSCAN"
  },
  {
    "id": "122:15",
    "type": "Threshold",
    "status": "ERROR",
    "description": "PSNG_IP_PORTSWEEP_FILTERED"
  },
  {
    "id": "122:1",
    "type": "Threshold",
    "status": "ERROR",
    "description": "PSNG_TCP_PORTSCAN"
  },
},

```

- Étape 4** Cliquez sur **Close** (Fermer) pour fermer la boîte de dialogue **Sync Summary** (Résumé de la synchronisation).
- Étape 5** Pour vérifier les règles ayant l'état : ERREUR, choisissez **Policies (Politiques) > Access Control heading (En-tête Contrôle d'accès) > Intrusion** et cliquez sur la version **Snort 2** de la politique de prévention des intrusions.
- Étape 6** Sous **Policy Information** (Informations sur la politique), cliquez sur **Rules** (Règles) et filtrez la règle. Par exemple, saisissez **PSNG_TCP_PORTSCAN** dans le champ **Filter** (Filtre) pour trouver la règle.
- Étape 7** Cliquez sur **Show Details** (Afficher les détails) pour afficher la version détaillée de la règle.
- Étape 8** Créez à nouveau la règle dans Snort 3 en utilisant les directives de règle Snort 3 et enregistrez le fichier en tant que fichier .txt ou .rules. Pour en savoir plus, consultez www.snort3.org.
- Étape 9** Chargez la règle personnalisée que vous venez de créer localement dans la liste de toutes les règles Snort 3. Voir [Ajouter des règles personnalisées aux groupes de règles](#).

Prochaine étape

Déployer les modifications de configuration. Consultez [Déploiement des modifications de configuration](#), à la page 10.

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.