Gestion du système

Les rubriques suivantes expliquent comment effectuer les tâches de gestion du système telles que la mise à jour des bases de données du système ainsi que la sauvegarde et la restauration du système.

Installation des mises à jour logicielles

Vous pouvez installer les mises à jour des bases de données du système et du logiciel système. Les rubriques suivantes expliquent comment installer ces mises à jour.

Mise à jour des bases de données système et des flux

Le système utilise plusieurs bases de données et flux de Security Intelligence pour fournir des services avancés. Cisco fournit des mises à jour de ces bases de données et de ces flux afin que vos politiques de sécurité utilisent les dernières informations disponibles.

Aperçu des mises à jour de la base de données du système et des flux

FTD utilise les bases de données et les flux suivants pour fournir des services avancés.

Règles d'intrusion

À mesure que de nouvelles vulnérabilités sont découvertes, Cisco Talos Intelligence Group (Talos) publie des mises à jour de règles de prévention des intrusions que vous pouvez importer. 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 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. 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.

Pour que les modifications apportées par une mise à jour de règles de prévention des intrusions prennent effet, vous devez redéployer les configurations.

Les mises à jour de règles peuvent être volumineuses; importez-les pendant les périodes de faible utilisation du réseau. Sur les réseaux lents, une tentative de mise à jour peut échouer et vous devrez réessayer.

Base de données de géolocalisation (GeoDB)

La base de données de géolocalisation Cisco (GeoDB) est une base de données de données géographiques (pays, ville, coordonnées, etc.) associées à des adresses IP routables.

Les mises à jour de GeoDB fournissent des renseignements à jour sur les emplacements physiques que votre système peut associer aux adresses IP routables détectées. Vous pouvez utiliser les données de géolocalisation comme condition dans les règles de contrôle d'accès.

Le temps nécessaire pour mettre à jour la base de données GeoDB dépend de votre appareil ; l'installation prend habituellement entre 30 et 40 minutes. 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.

Base de données relative aux vulnérabilités (VDB)

La base de données sur les vulnérabilités de Cisco (VDB) est une base de données des vulnérabilités connues auxquelles les hôtes peuvent être exposés, ainsi que des empreintes pour les systèmes d'exploitation, les clients et les applications. Le système de pare-feu corrèle ces empreintes avec les vulnérabilités pour vous aider à déterminer si un hôte particulier augmente le risque de compromission du réseau. Cisco Talos Intelligence Group (Talos) publie des mises à jour périodiques de la VDB.

Le temps nécessaire pour mettre à jour la VDB et ses mappages de vulnérabilités dépend du nombre d'hôtes dans votre cartographie du réseau. Vous pouvez planifier la mise à jour pendant les périodes de faible utilisation du système afin de minimiser l'impact de tout temps d'arrêt. En règle générale, divisez le nombre d'hôtes de votre réseau par 1 000 pour déterminer le nombre approximatif de minutes nécessaires pour effectuer la mise à jour.

Après avoir mis à jour la VDB, vous devez redéployer les configurations pour que les détecteurs d'applications et les empreintes de systèmes d'exploitation mis à jour prennent effet.

Flux de renseignements sur la sécurité Cisco Talos Intelligence Group (Talos)

Talos donne accès à des flux de renseignements régulièrement mis à jour à utiliser dans les politiques de Security Intelligence. Les sites qui représentent des menaces de sécurité, comme les programmes malveillants, les pourriels, les réseaux de zombies et l'hameçonnage peuvent apparaître et disparaître plus rapidement que vous ne pouvez mettre à jour et déployer des configurations personnalisées. Ces flux contiennent des adresses et des URL pour les menaces connues. Lorsque le système met à jour un flux, il n'est pas nécessaire de le redéployer. Les nouvelles listes sont utilisées pour évaluer les connexions ultérieures.

Base de données de catégorie/réputation d'URL

Le système obtient la base de données de catégorie URL et de réputation auprès de Cisco Collective Security Intelligence (CSI). Si vous configurez des règles de contrôle d'accès avec filtrage d'URL sur la base de la catégorie et de la réputation, les URL demandées sont comparées à cette base de données. Vous pouvez configurer les mises à jour de base de données et d'autres préférences de filtrage d'URL dans **System Settings (Paramètres du système)** > **URL Filtering Preferences (Préférences de filtrage**

d'URL). Vous ne pouvez pas gérer les mises à jour de la base de données de catégorie/réputation d'URL de la même manière que les mises à jour des autres bases de données du système.

Mise à jour des bases de données du système.

Vous pouvez récupérer manuellement et appliquer les mises à jour de la base de données du système selon votre commodité. Les mises à jour sont récupérées à partir du site d'assistance de Cisco. Ainsi, il doit y avoir un chemin d'accès à l'Internet à partir de l'adresse de gestion du système.

Sinon, vous pouvez récupérer vous-même les paquets de mise à jour sur Internet, puis les charger à partir de votre ordinateur. Cette méthode est principalement destinée aux réseaux isolés, où il n'y a pas de chemin d'accès à Internet pour récupérer les mises à jour de Cisco. Téléchargez les mises à jour à partir de software.cisco.com à partir des mêmes dossiers où vous téléchargeriez les mises à niveau logicielles système.

Remarque En mai 2022, nous avons scindé la base de données GeoDB en deux ensembles : un ensemble de codes de pays qui mappe les adresses IP aux pays/continents, et un ensemble d'adresses IP qui contient des données contextuelles supplémentaires associées aux adresses IP routables. Le FDM n'a pas utilisé et n'a jamais utilisé les informations contenues dans le paquet IP. Cette séparation permet d'économiser beaucoup d'espace disque dans les déploiements FTD gérés localement. Si vous obtenez vous-même la base de données GeoDB de Cisco, assurez-vous d'obtenir le paquet du code de pays, qui porte le même nom de fichier que l'ancien paquet tout-en-un : Cisco_GEODB_Update-*date-build*.

Vous pouvez également configurer un calendrier régulier pour récupérer et appliquer les mises à jour de la base de données. Étant donné que ces mises à jour peuvent être volumineuses, planifiez-les pour les périodes de faible activité du réseau.

Remarque Lorsqu'une mise à jour d'une base de données est en cours, vous pourriez trouver que l'interface utilisateur est lente pour répondre à vos actions.

Avant de commencer

Pour éviter toute incidence potentielle sur les modifications en attente, déployez la configuration sur le périphérique avant de mettre à jour manuellement ces bases de données.

Sachez que les mises à jour de VDB et de catégories d'URL peuvent supprimer des applications ou des catégories. Vous devez mettre à jour toutes les règles de contrôle d'accès ou de déchiffrement SSL qui utilisent ces éléments obsolètes avant de pouvoir déployer les modifications.

Procédure

Étape 1 Cliquez sur **Device (périphérique)**, puis cliquez sur **View Configuration** (Afficher la configuration) dans le résumé des mises à jour.

Cela ouvre la page Updates (Mises à jour). Les renseignements sur la page affichent la version actuelle de chaque base de données ainsi que la date et l'heure de la dernière mise à jour de chaque base de données.

Étape 2 Pour mettre à jour manuellement une base de données, cliquez sur l'une des options suivantes dans la section de cette base de données :

- **Update from Cloud** (Mettre à jour à partir du cloud) : pour que FDM récupère le package de mise à jour auprès de Cisco. Il s'agit de la méthode la plus simple et de la plus fiable, mais il doit y avoir un chemin d'accès à Internet pour l'utiliser.
- **(flèche vers le bas)** > ***option*** : pour sélectionner le package de mise à jour à partir de votre poste de travail ou d'un lecteur connecté à votre poste de travail. L'option sera l'une des suivantes :
  - **Select File** (Sélectionner un fichier) : sélectionnez un ensemble VDB ou de géolocalisation.
  - **Update to Newer Version** (Mettre à jour vers une version plus récente) : sélectionnez un ensemble de règles de prévention des intrusions qui est plus récent que celui actuellement installé.
  - **Downgrade to Older Version** (Rétrograder à une version antérieure) : sélectionnez un ensemble de règles de prévention des intrusions plus ancien que celui actuellement installé.

Les mises à jour de règles et de VDB nécessitent un déploiement de configuration pour les rendre actives. Lorsque vous effectuez une mise à jour à partir du Cloud, il vous est demandé si vous souhaitez procéder au déploiement maintenant ; cliquez sur **Yes** (Oui). Si vous cliquez sur **No** (Non), n'oubliez pas de lancer une tâche de déploiement dès que vous le pouvez.

Si vous chargez votre propre fichier, vous devez toujours déployer les modifications manuellement.

Remarque
Lors du chargement manuel d'un ensemble de règles de prévention des intrusions, assurez-vous de charger le type de package approprié pour votre version Snort, SRU pour Snort 2, LSP pour Snort 3. Vous pouvez charger un package pour la version Snort non active, mais elle ne sera activée que si vous changez de version. Pour en savoir plus sur le changement de version de Snort, consultez Commutation entre Snort 2 et Snort 3.

Étape 3 (Facultatif) Pour configurer une planification de mise à jour régulière de la base de données :

a) Cliquez sur le lien **Configure** (Configurer) dans la section de la base de données souhaitée. S'il existe déjà un calendrier, cliquez sur **Edit** (Modifier).

Les calendriers de mise à jour des bases de données sont distincts. Vous devez définir les planifications séparément.

b) Spécifiez l'heure de début de la mise à jour :

- La fréquence de la mise à jour (quotidienne, hebdomadaire ou mensuelle).
- Pour les mises à jour hebdomadaires ou mensuelles, les jours de la semaine ou du mois pendant lesquels vous souhaitez que la mise à jour se produise.
- L'heure à laquelle vous souhaitez que la mise à jour commence. L'heure que vous précisez est ajustée selon l'heure avancée. Elle sera reculée ou avancée à chaque changement d'heure dans votre région. Vous devez modifier le calendrier au moment du changement d'heure si vous souhaitez conserver cette heure tout au long de l'année.

c) Pour les mises à jour de règles ou de VDB, cochez la case **Automatically Deploy the Update** (déployer automatiquement la mise à jour) si vous souhaitez que le système déploie la configuration chaque fois que la base de données est mise à jour.

La mise à jour n'est effective que lorsqu'elle est déployée. Le déploiement automatique déploie également toutes les autres modifications de configuration qui ne sont pas encore déployées.

d) Cliquez sur **Save** (enregistrer).

Remarque
Si vous souhaitez supprimer une planification récurrente, cliquez sur le lien **Edit** (Modifier) pour ouvrir la boîte de dialogue de planification, puis cliquez sur le bouton **Remove** (Supprimer).

Mise à jour des flux de renseignements de sécurité

Cisco Talos Intelligence Group (Talos) fournit un accès à des flux de renseignements de sécurité régulièrement mis à jour. Les sites qui représentent des menaces de sécurité, comme les programmes malveillants, les pourriels, les réseaux de zombies et l'hameçonnage peuvent apparaître et disparaître plus rapidement que vous ne pouvez mettre à jour et déployer des configurations personnalisées. Lorsque le système met à jour un flux, il n'est pas nécessaire de le redéployer. Les nouvelles listes sont utilisées pour évaluer les connexions ultérieures.

Si vous souhaitez contrôler strictement quand le système met à jour un flux à partir d'Internet, vous pouvez désactiver les mises à jour automatiques pour ce flux. Cependant, les mises à jour automatiques assurent l'obtention des données pertinentes les plus à jour.

Procédure

Étape 1 Cliquez sur **Device (Périphérique)**, puis cliquez sur **View Configuration (Afficher la configuration)** dans le résumé Updates (Mises à jour).

Cela ouvre la page Updates (Mises à jour). Les renseignements sur la page affichent la version actuelle des **Security Intelligence Feeds** (Flux de renseignements de sécurité) ainsi que la date et l'heure de la dernière mise à jour des flux.

Étape 2 Pour mettre à jour manuellement les flux, cliquez sur **Update Now** (Mettre à jour maintenant) dans le groupe **Security Intelligence Feeds (Flux de renseignements de sécurité).**.

Si vous mettez à jour manuellement les flux sur une unité dans un groupe à haute disponibilité, vous devez également les mettre à jour manuellement sur l'autre unité pour assurer la cohérence.

Étape 3 (Facultatif) Pour configurer une fréquence de mise à jour régulière :

a) Cliquez sur le lien **Configure** (Configurer) dans la section des flux Cisco. S'il existe déjà un calendrier, cliquez sur **Edit** (Modifier).

b) Sélectionnez la fréquence de mise à jour souhaitée.

La valeur par défaut est **Hourly (Toutes les heures)**. Vous pouvez également définir une mise à jour **Daily (Journalière)** (précisez l'heure du jour) ou une mise à jour **Weekly** (Hebdomadaire) (sélectionnez les jours de la semaine et l'heure du jour). L'heure que vous précisez est ajustée selon l'heure avancée. Elle sera reculée ou avancée à chaque changement d'heure dans votre région. Vous devez modifier le calendrier au moment du changement d'heure si vous souhaitez conserver cette heure tout au long de l'année.

Cliquez sur **Delete** (Supprimer) pour empêcher les mises à jour automatiques.

c) Cliquez sur **OK**.

Mise à niveau FTD

Utilisez cette procédure pour mettre à niveau un périphérique autonome FTD. Si vous devez mettre à jour FXOS, faites-le en premier. Pour mettre à niveau la défense contre les menaces haute disponibilité, voir au niveau de la haute disponibilité FTD.

Mise en garde Le trafic est abandonné pendant la mise à niveau. Même si le système semble inactif ou ne répond pas, ne le redémarrez pas ou ne l'éteignez pas manuellement pendant la mise à niveau. vous pourriez rendre le système inutilisé et nécessiter une réinitialisation. Vous pouvez annuler manuellement les mises à niveau majeures ou de maintenance en cours ou qui ont échoué, et réessayer les mises à niveau qui ont échoué. Si les problèmes persistent, communiquez avec Centre d'assistance technique Cisco (TAC).

Pour en savoir plus sur ces problèmes et d'autres que vous pouvez rencontrer pendant la mise à niveau, consultez Dépannage de des mises à niveau de la protection contre les menaces, à la page 10.

Avant de commencer

Remplissez la liste de contrôle avant la mise à niveau. Vérifiez que votre déploiement est intègre et communique correctement.

Astuces La liste de contrôle avant la mise à niveau comprend la planification (en commençant par la lecture du Cisco Firepower Notes de mise à jour), la création de sauvegardes, l'obtention des paquets de mise à niveau et l'exécution des mises à niveau associées (comme FXOS pour Firepower 4100/9300). Elle comprend également la vérification des modifications de configuration nécessaires, de la préparation, de la vérification de l'espace disque et de la vérification des tâches en cours d'exécution et planifiées. Pour des instructions détaillées de mise à niveau, y compris la liste de contrôle avant la mise à niveau, consultez le http://www.cisco.com/go/ftd-quick pour votre version.

Procédure

Étape 1 Sélectionnez **Device** (périphérique), puis cliquez sur **View Configuration** (afficher la configuration) dans le volet des mises à jour (Updates).
Le volet de mise à niveau du système indique la version du logiciel en cours d'exécution et tout paquet de mise à niveau que vous avez déjà téléversé.

Étape 2 Téléverser le paquet de mise à niveau

Vous ne pouvez téléverser qu'un seul paquet. Si vous téléversez un nouveau fichier, il remplace l'ancien fichier. Assurez-vous que le paquet convient à votre version cible et au modèle de périphérique. Cliquez sur **Parcourir** ou sur **Remplacer le fichier** pour commencer le téléversement.

Une fois le téléversement terminé, le système affiche une boîte de dialogue de confirmation. Avant de cliquer sur **OK**, sélectionnez éventuellement **Exécuter la mise à niveau Immédiatement** pour et choisissez les options de restauration et la mise à niveau maintenant. Si vous effectuez une mise à niveau maintenant, il est particulièrement important d'avoir complété autant que possible la liste de contrôles avant mise à niveau (voir l'étape suivante).

Étape 3 Effectuer les vérifications finales préalables à la mise à niveau, y compris la vérification de l'état de préparation.

Consultez la liste de contrôles avant mise à niveau. Assurez-vous d'avoir effectué toutes les tâches pertinentes, en particulier les vérifications finales. Si vous n'exécutez pas la vérification de la préparation manuellement, elle s'exécute lorsque vous lancez la mise à niveau. Si la vérification échoue, la mise à niveau est annulée. Pour en savoir plus, consultez Exécution d'une vérification de l'état de préparation aux mises à niveau, à la page 7.

Étape 4 Cliquez sur **Upgrade Now** (Installer > Mettre à niveau maintenant) pour lancer le processus d'installation de la mise à niveau.

a) Choisissez les options de restauration.

Vous pouvez **Annuler automatiquement en cas d'échec de la mise à niveau et revenir à la version précédente**. Lorsque cette option est activée, le périphérique revient automatiquement à son état d'avant la mise à niveau en cas d'échec de celle-ci qu'elle soit majeure ou de maintenance. Désactivez cette option si vous souhaitez pouvoir annuler ou réessayer manuellement une mise à niveau qui a échoué.

b) Cliquez sur **Continuer** pour mettre à niveau et redémarrer le périphérique.

Vous êtes automatiquement déconnecté et dirigé vers une page d'état où vous pouvez surveiller la mise à niveau jusqu'à ce que le périphérique redémarre. La page comprend également une option pour annuler l'installation en cours. Si vous avez désactivé la restauration automatique et que la mise à niveau échoue, vous pouvez annuler manuellement ou tenter de nouveau la mise à niveau.

Le trafic est abandonné pendant la mise à niveau. Pour ISA 3000 uniquement, si vous avez configuré le contournement matériel pour une panne de courant, le trafic est abandonné pendant la mise à niveau, mais transmis sans inspection pendant que le périphérique termine son redémarrage après la mise à niveau.

Étape 5 Reconnectez-vous quand vous le pouvez et vérifiez la réussite de la mise à niveau.

La page Device Summary (sommaire du périphérique) affiche la version du logiciel actuellement exécutée.

Étape 6 Effectuer les tâches postérieures à la mise à niveau.

a) Mettez à jour les bases de données du système. Si les mises à jour automatiques ne sont pas configurées pour les règles de prévention des intrusions, VDB et GeoDB, mettez-les à jour maintenant.
b) Apportez toutes les modifications de configuration requises après la mise à niveau.
c) Déployez.

Exécution d'une vérification de l'état de préparation aux mises à niveau

Avant d'installer une mise à niveau, le système exécute une vérification de préparation pour s'assurer que la mise à niveau est valide pour le système et pour examiner les autres facteurs qui peuvent empêcher la réussite de la mise à niveau. Si la vérification de préparation échoue, vous devez résoudre les problèmes avant de relancer l'installation. Si la vérification a échoué, vous serez informé de l'échec la prochaine fois que vous tenterez l'installation, et vous aurez la possibilité de forcer l'installation si vous le souhaitez.

Vous pouvez également exécuter manuellement le test de préparation avant de lancer la mise à niveau, comme le décrit cette procédure.

Avant de commencer

Chargez l'ensemble de mises à niveau que vous souhaitez vérifier.

Procédure

Étape 1 Sélectionnez **Device** (périphérique), puis cliquez sur **View Configuration** (afficher la configuration) dans le résumé des mises à jour (Updates).

La section **System Upgrade** (mise à niveau du système) affiche la version du logiciel en cours d'exécution et toute mise à jour que vous avez déjà téléchargée.

Étape 2 Consultez la section **Readiness Check** (vérification de l'état de préparation).

- Si la vérification de mise à niveau n'a pas encore été effectuée, cliquez sur le lien **Run Upgrade Readiness Check** (exécuter la vérification de l'état préparation aux mises à niveau). La progression de la vérification s'affiche dans cette zone. Le processus devrait prendre environ 20 secondes.
- Si la vérification de mise à niveau a déjà été exécutée, cette section indique si la vérification s'est soldée par une réussite ou un échec. En cas d'échec, cliquez sur **See Details** pour consulter plus d'information au sujet de la vérification de l'état de préparation. Après avoir résolu les problèmes, relancez la vérification.

Étape 3 Si la vérification de l'état de préparation conduit à un échec, vous devez résoudre les problèmes avant d'installer la mise à niveau. Les informations détaillées comprennent de l'aide pour résoudre les problèmes signalés. À la suite d'un script d'échec, cliquez sur le lien **Show Recovery Message** (afficher le message de récupération) pour afficher les informations.

Voici quelques problèmes courants :

- Incompatibilité de la version de FXOS - Sur les systèmes où vous installez les mises à niveau de FXOS séparément, comme le Firepower 4100/9300, un paquet de mise à niveau peut nécessiter une version minimale de FXOS différente de la version du logiciel FTD que vous exécutez actuellement. Dans ce cas, vous devez d'abord mettre à niveau FXOS avant de pouvoir mettre à niveau le logiciel FTD.
- Modèle de périphérique non pris en charge : l'ensemble de mise à niveau ne peut pas être installé sur ce périphérique. Vous avez peut-être téléchargé le mauvais paquet, ou l'appareil est un ancien modèle qui n'est tout simplement plus pris en charge par la nouvelle version du logiciel FTD. Veuillez vérifier la compatibilité de l'appareil et télécharger un ensemble pris en charge, s'il en existe un.
- Espace disque insuffisant : Si l'espace disponible est insuffisant, essayez de supprimer les fichiers inutiles, comme les sauvegardes du système. Supprimez uniquement les fichiers que vous avez créés.

Surveillance des mises à niveau de FTD

Lorsque vous lancez la mise à niveau de FTD, vous êtes automatiquement déconnecté et dirigé vers une page d'état où vous pouvez surveiller la progression globale de la mise à niveau. La page comprend également une option pour annuler l'installation en cours. Si vous avez désactivé la restauration automatique et que la mise à niveau échoue, la page vous permet d'annuler manuellement ou de tenter de nouveau la mise à niveau.

Vous pouvez également vous connecter en SSH au périphérique et utiliser l'interface de ligne de commande : **show upgrade status**. Ajoutez le mot-clé **continuous** pour afficher les entrées de journal telles qu'elles sont créées et **detail** pour afficher des informations détaillées. Ajoutez les deux mots-clés pour obtenir des informations détaillées en continu.

Une fois la mise à niveau terminée, vous perdez l'accès à la page d'état et à l'interface de ligne de commande lorsque le périphérique redémarre.

Annulation ou nouvelle tentative des FTD mises à niveau

Utilisez la page d'état de la mise à niveau ou l'interface de ligne de commande pour annuler manuellement les mises à niveau majeures ou de maintenance qui ont échoué ou en cours, et pour réessayer les mises à niveau qui ont échoué :

- Page d'état de mise à niveau : cliquez sur **Annuler la mise à niveau** pour annuler une mise à niveau en cours. Si la mise à niveau échoue, vous pouvez cliquer sur **Annuler la mise à niveau** pour arrêter la tâche et revenir à l'état du périphérique avant la mise à niveau, ou cliquer sur **Continuer** pour réessayer la mise à niveau.
- CLI : Utilisez la commande **upgrade cancel** pour annuler une mise à niveau en cours. Si la mise à niveau échoue, vous pouvez utiliser **upgrade cancel** pour arrêter la tâche et revenir à l'état du périphérique avant la mise à niveau, ou utiliser **upgrade retry** pour réessayer la mise à niveau.

Remarque Par défaut, FTD revient automatiquement à son état d'avant la mise à niveau en cas d'échec de cette dernière (« auto-cancel ») (Annulation automatique). Pour pouvoir annuler manuellement ou réessayer une mise à niveau ayant échoué, désactivez l'option d'annulation automatique lorsque vous lancez la mise à niveau. Dans un déploiement à haute disponibilité, l'annulation automatique s'applique à chaque périphérique individuellement. Autrement dit, si la mise à niveau échoue sur un périphérique, seul ce périphérique est rétabli.

Ces options ne sont pas prises en charge pour les correctifs. Pour en savoir plus sur la reprise d'une mise à niveau réussie, consultez Rétablissement FTD en cours..., à la page 9.

Rétablissement FTD en cours...

Si une mise à niveau majeure ou de maintenance réussit, mais que le système ne fonctionne pas comme prévu, vous pouvez revenir en arrière. Le rétablissement de FTD ramène le logiciel à l'état qu'il avait avant la dernière mise à niveau majeure ou de maintenance; les modifications de configuration ultérieures à la mise à niveau ne sont pas conservées. Le rétablissement après l'application d'un correctif supprime également les correctifs. Notez que vous ne pouvez pas annuler des correctifs ou des correctifs rapides individuels.

La procédure suivante explique comment restaurer à partir de FDM. Si vous ne pouvez pas accéder à FDM, vous pouvez revenir à la ligne de commande FTD dans une session SSH en utilisant la commande **upgrade revert**. Vous pouvez utiliser la commande **show upgrade revert-info** pour voir à quelle version le système retournera.

Avant de commencer

Si l'unité fait partie d'une paire à haute disponibilité, vous devez rétablir les deux unités. Idéalement, lancez la restauration sur les deux unités en même temps afin que la configuration puisse être restaurée sans problème de basculement. Ouvrez des sessions avec les deux unités et vérifiez que le rétablissement est possible sur chacune, puis démarrez les processus. Notez que le trafic sera interrompu pendant la restauration, donc effectuez-la si possible en dehors des heures ouvrables.

Pour les châssis Firepower 4100/9300, les versions principales FTD ont une version FXOS associée spécialement qualifiée et recommandée. Cela signifie qu'après avoir rétabli le logiciel FTD, vous exécutez peut-être une version non recommandée de FXOS (trop récente). Bien que les nouvelles versions de FXOS soient rétrocompatibles avec les anciennes versions de FTD, nous effectuons des tests avancés des combinaisons recommandées. Vous ne pouvez pas passer à une version antérieure de FXOS, donc si vous vous trouvez dans cette situation et que vous souhaitez exécuter une combinaison recommandée, vous devrez recréer l'image du périphérique.

Procédure

Étape 1 Sélectionnez **Device** (périphérique), puis cliquez sur **View Configuration** (afficher la configuration) dans le résumé des mises à jour **(Updates)**.

Étape 2 Dans la section **System Upgrade** (mise à niveau du système), cliquez sur le lien **Revert Upgrade** (annuler la mise à niveau).

Une boîte de dialogue de confirmation s'affiche et affiche la version actuelle et la version à laquelle le système sera restauré. Si aucune version n'est disponible pour la restauration, il n'y a pas de lien **Annuler la mise à niveau**.

Étape 3 Si la version cible vous convient (et qu'une version est disponible), cliquez sur **Revert** (Restaurer).

Après avoir effectué le retour en arrière, vous devez réenregistrer le périphérique auprès du Smart Software Manager.

Dépannage de des mises à niveau de la protection contre les menaces

Ces problèmes peuvent se produire lorsque vous mettez à niveau un périphérique, qu'il soit autonome ou au sein d'une paire à haute disponibilité. Pour résoudre les problèmes spécifiques aux mises à niveau à haute disponibilité, consultez Dépannage des mises à niveau de Threat Defense haute disponibilité.

Erreurs relatives au paquet de mise à niveau

Pour trouver le bon paquet de mise à niveau, sélectionnez ou recherchez votre modèle sur Site d'assistance et de téléchargement Cisco, puis accédez à la page de téléchargement du logiciel pour la version appropriée. Les paquets de mise à niveau disponibles sont répertoriés avec les paquets d'installation, les correctifs rapides et les autres téléchargements applicables. Les noms des fichiers de paquet de mise à niveau reflètent la plateforme, le type de paquet (mise à niveau, correctif, correctif), la version du logiciel et la version.

Les paquets de mise à niveau à partir de la version 6.2.1+ sont signés et se terminent par .sh.REL.tar. Ne décompressez pas les paquets de mise à niveau signés. Ne renommez pas les paquets de mise à niveau et ne les transférez pas par courriel.

Impossible d'atteindre le périphérique pendant la mise à niveau.

Les périphériques arrêtent de transmettre le trafic pendant la mise à niveau ou en cas d'échec de la mise à niveau. Avant d'effectuer la mise à niveau, assurez-vous que le trafic en provenance de votre emplacement n'a pas à traverser le périphérique lui-même pour accéder à l'interface de gestion du périphérique .

Le périphérique semble inactif ou ne répond pas pendant la mise à niveau.

Vous pouvez annuler manuellement les mises à niveau majeures et de maintenance en cours ; voir Annulation ou nouvelle tentative des FTD mises à niveau, à la page 9. Si le périphérique ne répond pas ou si vous ne pouvez pas annuler la mise à niveau, communiquez avec Centre d'assistance technique Cisco (TAC).

⚠

Mise en garde Même si le système semble inactif, ne le redémarrez pas ou ne l'éteignez *pas* manuellement pendant la mise à niveau. Vous risquez de mettre le système dans un état inutilisable et de nécessiter une nouvelle image.

La mise à niveau a réussi, mais le système ne fonctionne pas comme vous le souhaitez.

Tout d'abord, assurez-vous que les informations en cache sont actualisées. N'actualisez pas simplement la fenêtre du navigateur pour vous reconnecter. Supprimez plutôt tout chemin « supplémentaire » de l'URL et reconnectez-vous à la page d'accueil; par exemple, http://threat-defense.exemple.com/.

Si les problèmes persistent et que vous devez revenir à une version majeure ou de maintenance antérieure, vous pourrez peut-être effectuer une restauration ; voir Rétablissement FTD en cours..., à la page 9. Si vous ne pouvez pas revenir en arrière, vous devez recréer l'image.

Échec de la mise à niveau.

Lorsque vous lancez une mise à niveau majeure ou de maintenance, utilisez l'option **Automatically cancel on upgrade failure... (Annuler automatiquement en cas d'échec de la mise à niveau...)** Option d'annulation automatique pour choisir ce qui se passe en cas d'échec de la mise à niveau, comme suit :

- Annulation automatique activée (par défaut) : si la mise à niveau échoue, la mise à niveau est annulée et le périphérique revient automatiquement à l'état qu'il avait avant la mise à niveau. Corrigez les problèmes et réessayez.
- Annulation automatique désactivée : si la mise à niveau échoue, le périphérique reste tel qu'il est. Corrigez les problèmes et réessayez immédiatement, ou annulez manuellement la mise à niveau et réessayez ultérieurement.

Pour en savoir plus, consultez Annulation ou nouvelle tentative des FTD mises à niveau, à la page 9. Si vous ne pouvez pas réessayer ou annuler, ou si les problèmes persistent, communiquez avec Centre d'assistance technique Cisco (TAC).

Recréation d'image du périphérique

La recréation d'image d'un périphérique implique l'effacement de la configuration du périphérique et l'installation d'une nouvelle image logicielle. L'intention de la recréation d'image est d'avoir une installation propre avec une configuration d'usine par défaut.

Vous devriez recréer l'image du périphérique dans les circonstances suivantes :

- Vous souhaitez convertir le système du logiciel ASA au logiciel FTD. Vous ne pouvez pas mettre à niveau un périphérique exécutant une image ASA vers un périphérique exécutant une image FTD.
- Le périphérique exécute une image antérieure à la version 6.1.0, et vous souhaitez effectuer une mise à niveau vers la version 6.1 ou une image ultérieure et configurer le périphérique à l'aide de l'option FDM. Vous ne pouvez pas utiliser le FMC pour mettre à niveau un périphérique antérieur à la version 6.1, puis passer à la gestion locale.

- Le périphérique ne fonctionne pas correctement et toutes les tentatives de correction de la configuration ont échoué.

Pour en savoir plus sur la réinitialisation d'un appareil, consultez *Réinitialiser l'appareil de protection contre les menaces Cisco ASA ou Threat Defense* ou le guide de *démarrage rapide de la défense contre les menaces* pour votre modèle d'appareil. Ces guides sont disponibles sur http://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-guides-list.html.

Sauvegarde et restauration du système

Vous pouvez sauvegarder la configuration du système afin de pouvoir restaurer le périphérique si la configuration est corrompue en raison d'une mauvaise configuration ultérieure ou d'un incident physique.

Vous pouvez restaurer une sauvegarde sur un périphérique de remplacement uniquement si les deux périphériques sont du même modèle et exécutent la même version du logiciel (y compris le numéro de build, pas seulement la même version mineure). N'utilisez pas le processus de sauvegarde et de restauration pour copier des configurations entre des périphériques. Un fichier de sauvegarde contient des informations qui identifient de manière unique un périphérique et ne peuvent pas être partagées.

Remarque La sauvegarde n'inclut pas la configuration de l'adresse IP de gestion. Ainsi, lorsque vous récupérez un fichier de sauvegarde, l'adresse de gestion n'est pas remplacée à partir de la copie de sauvegarde. Cela garantit que toutes les modifications que vous avez apportées à l'adresse sont conservées et permet également de restaurer la configuration sur un périphérique différent sur un segment de réseau différent. La sauvegarde ne comprend pas non plus les informations de licence ou d'enregistrement dans le nuage, de sorte que tout état de licence ou d'enregistrement dans le nuage qui existe au moment de la restauration est conservé.

Les sauvegardes comprennent la configuration uniquement, et non le logiciel système. Si vous devez recréer complètement l'image du périphérique, vous devez réinstaller le logiciel, puis vous pouvez charger une sauvegarde et récupérer la configuration.

La base de données de configuration est verrouillée pendant la sauvegarde. Vous ne pouvez pas apporter de modifications à la configuration pendant une sauvegarde, bien que vous puissiez afficher les politiques, les tableaux de bord, etc. Pendant une restauration, le système est complètement indisponible.

Le tableau de la page Backup and Restore (Sauvegarde et restauration) répertorie toutes les copies de sauvegarde existantes qui sont disponibles sur le système, y compris le nom de fichier de la sauvegarde, la date et l'heure de sa création et la taille du fichier. Le type de sauvegarde (manuelle, planifiée ou récurrente) dépend de la façon dont vous avez demandé au système de créer cette copie de sauvegarde.

Astuces Les copies de sauvegarde sont créées sur le système lui-même. Vous devez télécharger manuellement les copies de sauvegarde et les stocker sur des serveurs sécurisés pour vous assurer d'avoir les copies de sauvegarde dont vous avez besoin pour la reprise sur sinistre. Le système conserve jusqu'à 3 copies de sauvegarde sur le périphérique. Les nouvelles sauvegardes remplacent la sauvegarde la plus ancienne.

Les rubriques suivantes expliquent comment gérer les opérations de sauvegarde et de restauration.

Sauvegarder le système immédiatement

Vous pouvez démarrer une sauvegarde quand vous le souhaitez.

Procédure

Étape 1 Cliquez sur **Device (périphérique)**, puis sur **View Configuration** (Afficher la configuration) dans le résumé de la sauvegarde et de la restauration.

Cela ouvre la page de sauvegarde et de restauration. Le tableau répertorie toutes les copies de sauvegarde existantes qui sont disponibles sur le système.

Étape 2 Cliquez sur **Manual Backup (Sauvegarde manuelle)** > **Back Up Now (Sauvegarder maintenant)**.

Étape 3 Entrez un nom pour la sauvegarde et, facultativement, une description.

Si vous décidez que vous souhaitez effectuer la sauvegarde à une date ultérieure plutôt qu'immédiate, vous pouvez cliquer sur **Schedule** (Planifier) à la place.

Étape 4 (Facultatif) Sélectionnez l'option **Encrypt File** (chiffrer le fichier) pour chiffrer le fichier de sauvegarde.

Si vous sélectionnez l'option, vous devez entrer le **mot de passe** qui sera nécessaire pour restaurer le fichier de sauvegarde (et **confirmer le mot de passe**).

Étape 5 (ISA 3000 uniquement.) Sélectionnez l'**emplacement des fichiers de sauvegarde**.

Vous pouvez créer la sauvegarde sur le **disque dur local** ou sur la **carte SD**. L'intérêt de l'utilisation de la carte SD est que vous pouvez l'utiliser pour récupérer la configuration sur un périphérique de remplacement.

Étape 6 Cliquez sur **Back Up Now** (Sauvegarder maintenant).

Le système démarre le processus de sauvegarde. Une fois la sauvegarde complétée, le fichier de sauvegarde s'affichera dans le tableau. Vous pouvez ensuite télécharger la copie de sauvegarde sur votre système et la stocker ailleurs, si vous le souhaitez.

Vous pouvez quitter la page de sauvegarde et de restauration après avoir lancé la sauvegarde. Cependant, le système sera probablement lent et vous devriez envisager de suspendre votre travail pour permettre à la sauvegarde de se terminer.

En outre, le système acquerra des verrous sur la base de données de configuration pendant une partie ou toute la sauvegarde, ce qui peut vous empêcher d'apporter des modifications pendant la durée du processus de sauvegarde.

Sauvegarder le système à une heure planifiée

Vous pouvez configurer une sauvegarde planifiée pour sauvegarder le système à une date et à une heure futures spécifiques. Une sauvegarde planifiée est une occurrence unique. Si vous souhaitez créer un calendrier de sauvegarde pour créer régulièrement des sauvegardes, configurez une sauvegarde récurrente au lieu d'une sauvegarde planifiée.

Remarque Si vous souhaitez supprimer la planification pour une sauvegarde future, modifiez la planification et cliquez sur **Remove** (Supprimer).

Procédure

Étape 1 Cliquez sur **Device (périphérique)**, puis sur **View Configuration** (Afficher la configuration) dans le résumé Backup and Restore (Sauvegarde et restauration).

Étape 2 Cliquez sur **Scheduled Backup (Sauvegarde planifiée)** > **Schedule a Backup (Planifier une sauvegarde)**.

Si vous avez déjà une sauvegarde planifiée, cliquez sur **Scheduled Backup (Sauvegarde planifiée)** > **Edit (Modifier)**.

Étape 3 Entrez un nom pour la sauvegarde et, facultativement, une description.

Étape 4 Sélectionnez la date et l'heure de la sauvegarde.

Étape 5 (Facultatif) Sélectionnez l'option **Encrypt File** (chiffrer le fichier) pour chiffrer le fichier de sauvegarde.

Si vous sélectionnez l'option, vous devez entrer le **mot de passe** qui sera nécessaire pour restaurer le fichier de sauvegarde (et **confirmer le mot de passe**).

Étape 6 (ISA 3000 uniquement.) Sélectionnez l'**emplacement des fichiers de sauvegarde**.

Vous pouvez créer la sauvegarde sur le **disque dur local** ou sur la **carte SD**. L'intérêt de l'utilisation de la carte SD est que vous pouvez l'utiliser pour récupérer la configuration sur un périphérique de remplacement.

Étape 7 Cliquez sur **Schedule** (Planifier).

Lorsque la date et l'heure sélectionnées arrivent, le système effectue une sauvegarde. Une fois terminée, la copie de sauvegarde est répertoriée dans le tableau des sauvegardes.

Configuration d'une planification de sauvegarde récurrente

Vous pouvez configurer une sauvegarde récurrente pour sauvegarder le système à des intervalles réguliers. Par exemple, vous pourriez effectuer une sauvegarde tous les vendredis à minuit. Un calendrier de sauvegardes récurrentes vous permet de vous assurer que vous avez toujours un ensemble de sauvegardes récentes.

Remarque Si vous souhaitez supprimer une planification récurrente, modifiez la planification et cliquez sur **Remove** (Supprimer).

Procédure

Étape 1 Cliquez sur **Device (périphérique)**, puis sur **View Configuratio**n (Afficher la configuration) dans le résumé Backup and Restore (Sauvegarde et restauration).

Étape 2 Cliquez sur **Recurring Backup (Sauvegarde récurrente)** > **Configure (Configurer)**.

Si vous avez déjà configuré une sauvegarde récurrente, cliquez sur **Recurring Backup (Sauvegarde récurrente)** > **Edit (Modifier)**.

Étape 3 Entrez un nom pour la sauvegarde et, facultativement, une description.

Étape 4 Sélectionnez la **Frequency** (Fréquence) et le calendrier associé :

- **Daily** (Quotidien) : sélectionnez l'heure. Une sauvegarde est effectuée chaque jour à l'heure planifiée.
- **Weekly** (Hebdomadaire) : sélectionnez les jours de la semaine et l'heure. Une sauvegarde est effectuée chaque jour que vous sélectionnez à l'heure planifiée. Par exemple, vous pouvez planifier des sauvegardes chaque lundi, mercredi et vendredi à 23 h 00 (11 PM).
- **Monthly** (Mensuel) : sélectionnez les jours du mois et l'heure. Une sauvegarde est effectuée chaque jour que vous sélectionnez à l'heure planifiée. Par exemple, vous pouvez planifier des sauvegardes les 1er (1), 15e (15) et 28e (28) jours du mois à 23 h 00 (11 p.m.).

L'heure que vous précisez est ajustée selon l'heure avancée. Elle sera reculée ou avancée à chaque changement d'heure dans votre région. Vous devez modifier le calendrier au moment du changement d'heure si vous souhaitez conserver cette heure tout au long de l'année.

Étape 5 (Facultatif) Sélectionnez l'option **Encrypt File** (chiffrer le fichier) pour chiffrer le fichier de sauvegarde.

Si vous sélectionnez l'option, vous devez entrer le **mot de passe** qui sera nécessaire pour restaurer le fichier de sauvegarde (et **confirmer le mot de passe**).

Étape 6 (ISA 3000 uniquement.) Sélectionnez l'**emplacement des fichiers de sauvegarde**.

Vous pouvez créer la sauvegarde sur le **disque dur local** ou sur la **carte SD**. L'intérêt de l'utilisation de la carte SD est que vous pouvez l'utiliser pour récupérer la configuration sur un périphérique de remplacement.

Étape 7 Cliquez sur **Save** (enregistrer).

Lorsque les dates et heures sélectionnées arrivent, le système effectue une sauvegarde. Une fois terminée, la copie de sauvegarde est répertoriée dans le tableau des sauvegardes.

La planification récurrente continue d'effectuer des sauvegardes jusqu'à ce que vous la changiez ou la supprimiez.

Restauration d'une sauvegarde

Vous pouvez restaurer les sauvegardes au besoin tant que le périphérique exécute la même version du logiciel (y compris le numéro de build) que celle qu'il exécutait au moment où vous avez effectué la sauvegarde. Vous pouvez restaurer une sauvegarde sur un périphérique de remplacement uniquement si les deux périphériques sont du même modèle et exécutent la même version du logiciel (y compris le numéro de build).

Cependant, vous ne pouvez pas restaurer une sauvegarde si le périphérique fait partie d'un pair à haute disponibilité. Vous devez d'abord interrompre la haute disponibilité à partir de la page **Device (périphérique)** > **High Availability (haute disponibilité)**, puis vous pourrez restaurer la sauvegarde. Si la sauvegarde comprend la configuration à haute disponibilité, le périphérique rejoindra le groupe à haute disponibilité. Ne restaurez pas la même sauvegarde sur les deux unités, car elles deviendraient alors toutes les deux actives. Au lieu de cela, restaurez la sauvegarde sur l'unité que vous souhaitez rendre active en premier, puis restaurez la sauvegarde équivalente sur l'autre unité.

Si la copie de sauvegarde que vous souhaitez restaurer ne se trouve pas déjà sur le périphérique, vous devez d'abord téléverser la sauvegarde avant de la restaurer.

Pendant une restauration, le système est complètement indisponible.

Remarque La sauvegarde n'inclut pas la configuration de l'adresse IP de gestion. Ainsi, lorsque vous récupérez un fichier de sauvegarde, l'adresse de gestion n'est pas remplacée par la copie de sauvegarde. Cela permet de préserver toutes les modifications que vous avez apportées à l'adresse et rend également possible la restauration de la configuration sur un périphérique différent, sur un segment de réseau différent. La sauvegarde ne comprend pas non plus les renseignements de licence ou d'enregistrement dans le nuage; l'état de licence ou d'enregistrement dans le nuage qui existe au moment de la restauration est donc conservé.

Avant de commencer

Si vous restaurez une sauvegarde sur un système différent, par exemple lors du remplacement d'un périphérique, la meilleure pratique consiste d'abord à enregistrer le périphérique et à activer les licences facultatives requises par les fonctionnalités configurées dans le fichier de sauvegarde. Le fichier de sauvegarde ne comprend pas les renseignements sur les licences ni sur les services dans le nuage. Ainsi, les modifications de licences ou les enregistrements dans le nuage que vous effectuez avant la restauration sont conservés.

Procédure

Étape 1 Cliquez sur **Device (périphérique)**, puis sur **View Configuration** (Afficher la configuration) dans le résumé Backup and Restore (Sauvegarde et restauration).

Cela ouvre la page Backup and Restore (Sauvegarde et restauration). Le tableau répertorie toutes les copies de sauvegarde existantes qui sont disponibles sur le système.

Étape 2 Si la copie de sauvegarde que vous souhaitez restaurer ne figure pas dans la liste des sauvegardes disponibles, cliquez sur **Upload (Charger)** > **Browse (Parcourir)** et chargez la copie de sauvegarde.

Étape 3 Cliquez sur l'icône de restauration ( ) pour le fichier.

Vous êtes invité à confirmer la restauration. Par défaut, la copie de sauvegarde sera supprimée après la restauration, mais vous pouvez sélectionner **Do not remove the backup after restoring** (Ne pas supprimer la sauvegarde après la restauration) pour la conserver avant de poursuivre la restauration.

Si le fichier de sauvegarde a été chiffré, vous devez saisir le **Password (mot de passe)** requis pour ouvrir le fichier et le déchiffrer.

Le système redémarrera une fois la restauration terminée.

Remarque
Après le redémarrage, le système vérifie automatiquement les mises à jour de Vulnerability Database (base de données relative aux vulnérabilités) (VDB), de Geolocation (Géolocalisation) et de la base de données Rules (Règles), et les télécharge au besoin. Comme ces mises à jour peuvent être volumineuses, la tentative initiale peut échouer. Veuillez vérifier la liste des tâches et, si un téléchargement échoue, téléchargez manuellement une mise à jour, comme décrit dans Mise à jour des bases de données du système., à la page 3 Le système redéploie également les politiques. Tout déploiement ultérieur échouera tant que la mise à jour n'aura pas été effectuée avec succès.

Étape 4 Si nécessaire, cliquez sur **Device (Périphérique)** > **Smart License (Licence Smart)** > **View Configuration (Afficher la configuration)**, réenregistrez le périphérique et réactivez les licences facultatives requises.

La sauvegarde n'inclut pas les informations de licence ni d'enregistrement dans le nuage. Ainsi, si vous restaurez une sauvegarde sur un nouveau système, par exemple lors du remplacement d'un périphérique, et que le système est en mode d'évaluation, vous devez l'enregistrer et activer les licences dont vous avez besoin. Si vous avez enregistré le périphérique et activé les licences avant la restauration, aucune modification supplémentaire n'est requise.

Si vous restaurez simplement une sauvegarde précédente sur le même système, vous ne devriez pas avoir à apporter de modifications aux licences ou à l'enregistrement dans le nuage. Cependant, vérifiez que toutes les licences facultatives nécessaires sont activées, car la sauvegarde pourrait inclure des fonctionnalités nécessitant des licences que vous avez désactivées après la création de la sauvegarde.

Remplacement d'un périphérique ISA 3000

L'ISA 3000 dispose d'une carte SD que vous pouvez retirer et insérer dans un autre périphérique ISA 3000. Si vous créez des sauvegardes de système sur la carte SD, vous pouvez utiliser cette fonction pour remplacer facilement un périphérique. Il suffit de retirer la carte SD du périphérique défaillant et de l'insérer dans le nouveau périphérique. Les sauvegardes sont alors disponibles pour restauration.

Pour vous assurer d'avoir les sauvegardes nécessaires, configurez la tâche de sauvegarde pour créer la sauvegarde sur la carte SD.

Gestion des fichiers de sauvegarde

Lorsque vous créez de nouvelles sauvegardes, les fichiers de sauvegarde sont répertoriés sur la page Backup and Restore (Sauvegarde et restauration). Les copies de sauvegarde ne sont pas conservées indéfiniment : lorsque l'utilisation de l'espace disque sur le périphérique atteint le seuil maximal, les anciennes copies de sauvegarde sont supprimées pour faire place aux plus récentes. En outre, lorsque vous installez une mise à niveau autre qu'un correctif rapide, tous les fichiers de sauvegarde sont supprimés. Ainsi, vous devez gérer régulièrement les fichiers de sauvegarde pour vous assurer d'avoir les copies de sauvegarde spécifiques que vous souhaitez conserver.

Vous pouvez effectuer les opérations suivantes pour gérer vos copies de sauvegarde :

- Télécharger des fichiers vers un stockage sécurisé : pour télécharger un fichier de sauvegarde sur votre poste de travail, cliquez sur l'icône de téléchargement () en regard du fichier. Vous pouvez ensuite déplacer le fichier vers votre stockage sécurisé.
- Charger un fichier de sauvegarde dans le système : si vous souhaitez restaurer une copie de sauvegarde qui n'est plus disponible sur le périphérique, cliquez sur **Upload (Charger)** > **Browse File (Parcourir le fichier)**, puis chargez-le depuis votre poste de travail. Vous pouvez ensuite le restaurer.

Remarque Les fichiers chargés peuvent être renommés pour correspondre au nom de fichier d'origine. De plus, s'il y a déjà plus de 3 copies de sauvegarde sur le système, la plus ancienne sera supprimée pour faire de l'espace pour le fichier téléchargé. Vous ne pouvez pas téléverser de fichiers qui ont été créés par une ancienne version de logiciel.

- Restaurer une sauvegarde : pour restaurer une copie de sauvegarde, cliquez sur l'icône de restauration () pour le fichier. Le système n'est pas disponible pendant la restauration et redémarrera une fois la restauration terminée. Vous devez déployer la configuration une fois que le système est opérationnel.
- Supprimer un fichier de sauvegarde : si vous ne souhaitez plus effectuer de sauvegarde en particulier, cliquez sur l'icône de suppression () pour le fichier. Vous êtes invité à confirmer la suppression. Une fois supprimé, vous ne pouvez pas récupérer le fichier de sauvegarde.

Audit et gestion du changement

Vous pouvez afficher les informations d'état sur les événements du système et les actions que les utilisateurs ont effectuées. Ces informations peuvent vous aider à effectuer l'audit du système et à vous assurer qu'il est géré correctement.

Cliquez sur **Device (Périphérique)** > **Device Administration (Administration du périphérique)** > **Audit Log (Journal d'audit)** pour voir le journal d'audit. En outre, vous pouvez trouver des renseignements sur la gestion du système en cliquant sur les boutons de l'icône **Task List** (Liste des tâches) ou **Deployment** (Déploiement) dans le coin supérieur droit.

Les rubriques suivantes couvrent certains des concepts et tâches principaux d'audit du système et de gestion des changements.

Événements d'audit

Le journal d'audit peut inclure les types d'événements suivants :

Événement de mise à jour du flux personnalisé, échec de la mise à jour du flux personnalisé

Ces événements indiquent une mise à jour réussie ou un échec d'un flux de Security Intelligence personnalisé. Les détails comprennent qui a lancé la mise à jour et des renseignements sur le flux qui a été mis à jour.

Événement du résumé de l'importation du fichier de règles personnalisées

Ces événements indiquent que vous avez importé un fichier qui contient une ou plusieurs règles de prévention des intrusions personnalisées. L'événement comprend un résumé du nombre de règles ajoutées, mises à jour et supprimées, ainsi qu'une vue sur les différences qui affiche les détails des règles importées.

Deployment Completed (Déploiement terminé), Deployment Failed (Échec du déploiement) : *job name* (nom de la tâche) ou *entity name* (nom d'entité)

Ces événements indiquent une tâche de déploiement terminée ou échouée. Les détails comprennent qui a lancé la tâche et des informations sur l'entité de tâche. Les tâches ayant échoué comprennent le message d'erreur lié à la défaillance.

Les détails comprennent également un onglet **Differences View (Affichage des différences)**, qui affiche les modifications qui ont été déployées sur le périphérique dans la tâche. Il s'agit de la combinaison de tous les événements de modification d'entité pour les entités déployées.

Pour filtrer en fonction de ces événements, cliquez simplement sur le filtre prédéfini **Deployment History** (Historique de déploiement). Notez que le type d'événement pour ces événements est un événement de déploiement, vous ne pouvez pas filtrer en fonction des événements terminés ou échoués uniquement.

Le nom de l'événement comprend le nom de la tâche défini par l'utilisateur (si vous en configurez un), ou « Utilisateur (*nom d'utilisateur*) déployé pour le déploiement ». Il existe également des tâches « Device Setup Automatic Deployment (Déploiement automatique de la configuration du périphérique) » et « Device Setup Automatic Deployment (Final Step) (Déploiement automatique de la configuration du périphérique – dernière étape) » qui se produisent pendant l'assistant de configuration du périphérique.

Entity Created (Entité créée), Entity Updated (Entité mise à jour), Entity Deleted (Entité supprimée) : *nom d'entité* (*type d'entité*)

Ces événements indiquent qu'une modification a été apportée à l'entité ou à l'objet identifié. Les détails de l'entité comprennent qui a effectué la modification, ainsi que le nom, le type et l'ID de l'entité. Vous pouvez filtrer en fonction de ces éléments. Les détails comprennent également un onglet **Differences View** (Affichage des différences), qui affiche les modifications apportées à l'objet.

Événement d'action à haute disponibilité

Ces événements sont liés à des actions sur la configuration à haute disponibilité, soit des actions que vous avez lancées, soit des actions que le système a lancées. HA Action Event (Événement d'action HA) est le type d'événement, mais les noms d'événements sont l'un des suivants :

- **HA Suspended** (HA suspendue) : vous avez suspendu intentionnellement la haute disponibilité sur le système.
- **HA Resumed** (HA reprise) : vous avez repris intentionnellement la haute disponibilité sur le système.
- **HA Reset** (HA réinitialisée) : vous avez réinitialisé intentionnellement la haute disponibilité sur le système.
- **HA Failover: Unit Switched Modes** (Basculement HA : unité ayant changé de mode) : vous avez changé de mode intentionnellement ou le système a basculé en raison de violations des mesures d'intégrité. Le message indique que l'homologue actif est devenu en veille ou que l'homologue en veille est devenu actif.

High Availability Sync Completed (Synchronisation de la haute disponibilité terminée)

L'unité active a synchronisé la configuration avec l'unité en veille. L'événement comprend les informations de modification pour la version précédente par rapport à la version synchronisée.

Liste des interfaces analysée

Cet événement indique que vous avez recherché des modifications dans l'inventaire des interfaces.

Modifications en attente annulées

Cet événement indique que vous avez supprimé toutes les modifications en attente. Toutes les modifications indiquées dans les événements Entity Created (Entité créée), Entity Updated (Entité mise à jour) et Entity Deleted (Entité supprimée), entre cet événement et l'événement Deployment Completed (Déploiement terminé), sont supprimées, et l'état des objets concernés est rétabli à la dernière version déployée.

Événement de mise à jour des règles

Lors de l'exécution de Snort 3, cet événement de l'entité LSPUpdateServer affiche des informations détaillées sur les règles de prévention des intrusions qui ont été ajoutées, supprimées ou modifiées lors du téléchargement et de l'installation d'un nouvel ensemble de règles de prévention des intrusions. L'événement est limité à 100 règles, donc si plus de 100 sont ajoutées, supprimées ou modifiées, l'événement ne contiendra pas d'informations complètes. Cet événement ne s'affiche pas pour les mises à jour de Snort 2.

Task Started (Tâche démarrée), Task Completed (Tâche terminée), Task Failed (Tâche échouée)

Les événements de tâche indiquent le début et la fin d'une tâche lancée par le système ou un utilisateur. Ces deux événements sont regroupés en une seule tâche dans la liste des tâches, que vous pouvez voir en cliquant sur le bouton **Task List** (Liste des tâches) dans le coin supérieur droit.

Les tâches comprennent des actions telles que les tâches de déploiement et les mises à jour manuelles ou planifiées de la base de données. Tout élément dans la liste des tâches correspondra à deux événements de tâche dans le journal d'audit, une indication du début de la tâche et un achèvement réussi ou un échec.

User Logged In (Utilisateur connecté), User Logged Out (Utilisateur déconnecté) : ***nom d'utilisateur***

Ces événements affichent l'heure et l'adresse IP source de l'utilisateur qui se connecte et se déconnecte de FDM. L'événement Déconnexion de l'utilisateur se produit à la fois pour les déconnexions actives et les déconnexions automatiques en raison du dépassement du temps d'inactivité.

Ces événements ne sont pas liés aux utilisateurs de VPN d'accès à distance qui établissent des connexions avec le périphérique. Ils n'incluent pas non plus la connexion et la déconnexion à l'interface de ligne de commande du périphérique.

Visualisation et analyse du journal d'audit

Le journal d'audit comprend des informations sur les événements lancés par le système et par l'utilisateur, tels que les tâches de déploiement, les mises à jour de la base de données et les connexions/déconnexions de FDM.

Pour obtenir une explication des types d'événement que vous pouvez voir dans le journal, consultez Événements d'audit, à la page 18.

Procédure

Étape 1 Cliquez sur **Device (Périphérique)**, puis sur le lien **Device Administration (Administration du périphérique)** > **View Configuration (Afficher la configuration)**.

Étape 2 Cliquez sur **Audit Log** (Journal d'audit) dans la table des matières s'il n'est pas déjà sélectionné.

Les événements sont regroupés par date et, dans une journée, par heure, la date et l'heure les plus récentes en haut de la liste. Au départ, chaque événement est réduit, de sorte que vous ne voyez que l'heure, le nom de l'événement, l'utilisateur qui a lancé l'événement et l'adresse IP source de l'utilisateur. « Système » pour l'utilisateur et l'adresse IP signifie que le périphérique lui-même a lancé l'événement.

Vous pouvez effectuer les opérations suivantes :

- Cliquez sur > à côté du nom de l'événement pour l'ouvrir et voir les détails de l'événement. Cliquez à nouveau sur l'icône pour fermer l'événement. De nombreux événements ont une liste simple d'attributs d'événement, tels que le type d'événement, le nom d'utilisateur, l'adresse IP source, etc. Cependant, les événements d'entité et de déploiement ont deux onglets :
  - **Summary** (Résumé) affiche les attributs de base de l'événement.
  - **Differences View** (Affichage des différences) affiche une comparaison de la configuration « déployée » existante avec les modifications apportées dans le cadre de l'événement. Pour les tâches de déploiement, cet affichage peut être long et nécessiter un défilement. Il résume toutes les

différences par rapport aux modifications d'événements d'entité qui ont fait partie de la tâche de déploiement.

- Sélectionnez une plage temporelle différente dans la liste déroulante à droite du champ de filtre. La valeur par défaut est d'afficher les événements des 2 dernières semaines, mais vous pouvez modifier cela pour les dernières 24 heures, 7 jours, mois ou 6 mois. Cliquez sur **Custom** (Personnalisé) pour spécifier une plage exacte en saisissant la date et l'heure de début et de fin.
- Cliquez sur n'importe quel lien dans le journal pour ajouter un filtre de recherche pour cet élément. La liste est mise à jour de sorte que seuls les événements qui comprennent l'élément sont affichés. Vous pouvez également simplement cliquer dans la zone **Filter** (Filtre) et créer un filtre directement. Il existe des filtres prédéfinis sous la zone de filtre, sur lesquels vous pouvez cliquer pour charger les critères de filtrage correspondants. Pour des informations détaillées sur le filtrage des événements, consultez Filtrage du journal d'audit, à la page 21.
- Rechargez la page du navigateur pour actualiser le journal avec les derniers événements.

Filtrage du journal d'audit

Vous pouvez appliquer un filtre au journal d'audit pour restreindre votre affichage à certains types de messages uniquement. Chaque élément du filtre doit correspondre exactement et entièrement. Par exemple, « User = admin » (Utilisateur = admin) n'affiche que les événements déclenchés par l'utilisateur nommé **admin**.

Vous pouvez utiliser les techniques suivantes, seules ou en combinaison, pour créer un filtre. La liste est automatiquement mise à jour chaque fois que vous ajoutez un élément de filtre.

Cliquez sur Predefined Filter (Filtre prédéfini).

Sous le champ **Filter** (Filtre) se trouvent les filtres prédéfinis. Cliquez simplement sur un lien pour charger le filtre. Vous êtes invité à confirmer. Si un filtre est déjà appliqué, il est remplacé ; il n'est pas complété.

Cliquer sur les éléments en surbrillance

La façon la plus simple de créer un filtre est de cliquer sur les éléments dans le tableau de journaux ou les détails des événements qui contiennent les valeurs sur lesquelles vous avez l'intention de filtrer. Cliquez sur un élément pour mettre à jour le champ **Filter** (Filtre) avec un élément correctement formaté pour cette combinaison de valeur et d'élément. Cependant, l'utilisation de cette technique nécessite que la liste d'événements existante contienne les valeurs souhaitées.

Si vous pouvez ajouter un élément de filtre pour un élément, l'élément est souligné lorsque vous passez le curseur dessus et vous voyez la commande **Click to Add to Filter** (Cliquer pour ajouter au filtre).

Sélection d'éléments atomiques

Vous pouvez également créer un filtre en cliquant dans le champ **Filter** (Filtre) et en sélectionnant l'élément atomique souhaité dans la liste déroulante, en saisissant la valeur de correspondance après le signe égal, puis en appuyant sur Enter (Entrée). Vous pouvez filtrer en fonction des éléments suivants. Notez que tous les éléments ne sont pas pertinents pour chaque type d'événement.

- **Event Type** (Type d'événement) : il s'agit généralement, mais pas toujours, du même élément que le nom de l'événement (sans qualificatifs variables comme le nom d'entité ou l'utilisateur). Pour les événements de déploiement, le type d'événement est Deployment Event (Événement de

déploiement). Pour obtenir une explication des types d'événements, consultez Événements d'audit, à la page 18.

- **User** (Utilisateur) : le nom de l'utilisateur qui a initié l'événement. L'utilisateur du système est écrit en majuscules : SYSTEM.
- **Source IP (IP source)** : l'adresse IP à partir de laquelle l'utilisateur a initié l'événement. L'adresse IP source des événements initiés par le système est SYSTEM.
- **Entity ID** (ID d'entité) : l'UUID de l'entité ou de l'objet, qui est une longue chaîne illisible, telle que 8e7021b4-2e1e-11e8-9e5d-0fc002c5f931. Normalement, pour utiliser ce filtre, vous devez soit cliquer sur un ID d'entité dans les détails d'un événement, soit récupérer l'ID nécessaire par le biais d'un appel GET pertinent utilisant l'API REST.
- **Entity Name** (Nom d'entité) : le nom de l'entité ou de l'objet. Pour les entités créées par l'utilisateur, il s'agit généralement du nom que vous avez donné à l'objet, par exemple, InsideNetwork pour un objet réseau. Pour les entités générées par le système ou, dans certains cas, les entités définies par l'utilisateur, il s'agit d'un nom prédéfini mais intelligible, par exemple, « Déploiement déclenché par l'utilisateur (admin) » pour les tâches de déploiement que vous ne nommez pas explicitement.
- **Entity Type** (Type d'entité) : le type d'entité ou d'objet. Il s'agit de noms prédéfinis, mais intelligibles, comme Network Object (Objet réseau). Vous pouvez trouver des types d'entités dans l'explorateur d'API en examinant le modèle d'objet pertinent pour la valeur de « type ». Les types d'API sont normalement tous en minuscules sans espaces. Si vous les saisissez exactement comme indiqué dans le modèle, la chaîne passe à un format plus lisible lorsque vous appuyez sur Entrée. La saisie dans l'un ou l'autre des formats fonctionne. Pour ouvrir l'explorateur d'API, cliquez sur le bouton more options (plus d'options) (⋮) et choisissez **API Explorer** (Explorateur d'API).

Règles pour les filtres de journal d'audit complexes

Lors de la création d'un filtre complexe qui contient plus d'un élément atomique, gardez les règles suivantes à l'esprit :

- Les éléments du même type ont une relation OU entre toutes les valeurs de ce type. Par exemple, l'inclusion de « User = admin » et « User = SYSTEM » correspond aux événements qui ont été lancés par l'un ou l'autre des utilisateurs.
- Les éléments de différents types ont une relation ET. Par exemple, inclure « Type d'événement = Entité mise à jour » et « Utilisateur = SYSTEM » affiche uniquement les événements pour lesquels le système a mis à jour une entité plutôt qu'un utilisateur actif.
- Vous ne pouvez pas utiliser de caractères génériques, d'expressions régulières, de correspondances partielles ou de correspondances de chaîne de texte simples.

Examen du déploiement et de l'historique des modifications d'entité

Les événements de déploiement et d'entité comprennent un onglet **Differences View** (Affichage des différences) dans les détails de l'événement. Cet onglet affiche une comparaison codée par couleur de l'ancienne configuration avec les modifications.

- Pour les tâches de déploiement, il s'agit d'une comparaison de la configuration exécutée sur le périphérique avant le déploiement avec les modifications effectivement déployées.

- Pour les événements d'entité, il s'agit des modifications de configuration apportées à la version précédente de l'objet. La version précédente peut être la version actuellement présente sur le périphérique, ou il peut s'agir d'un changement apporté à un objet qui n'a pas encore été déployé.

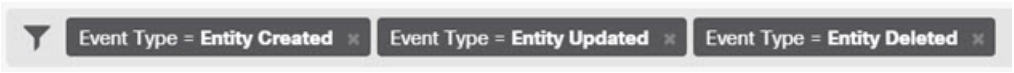
Procédure

Étape 1 Cliquez sur **Device (Périphérique)**, puis sur le lien **Device Administration (Administration du périphérique)** > **View Configuration (Afficher la configuration)**.

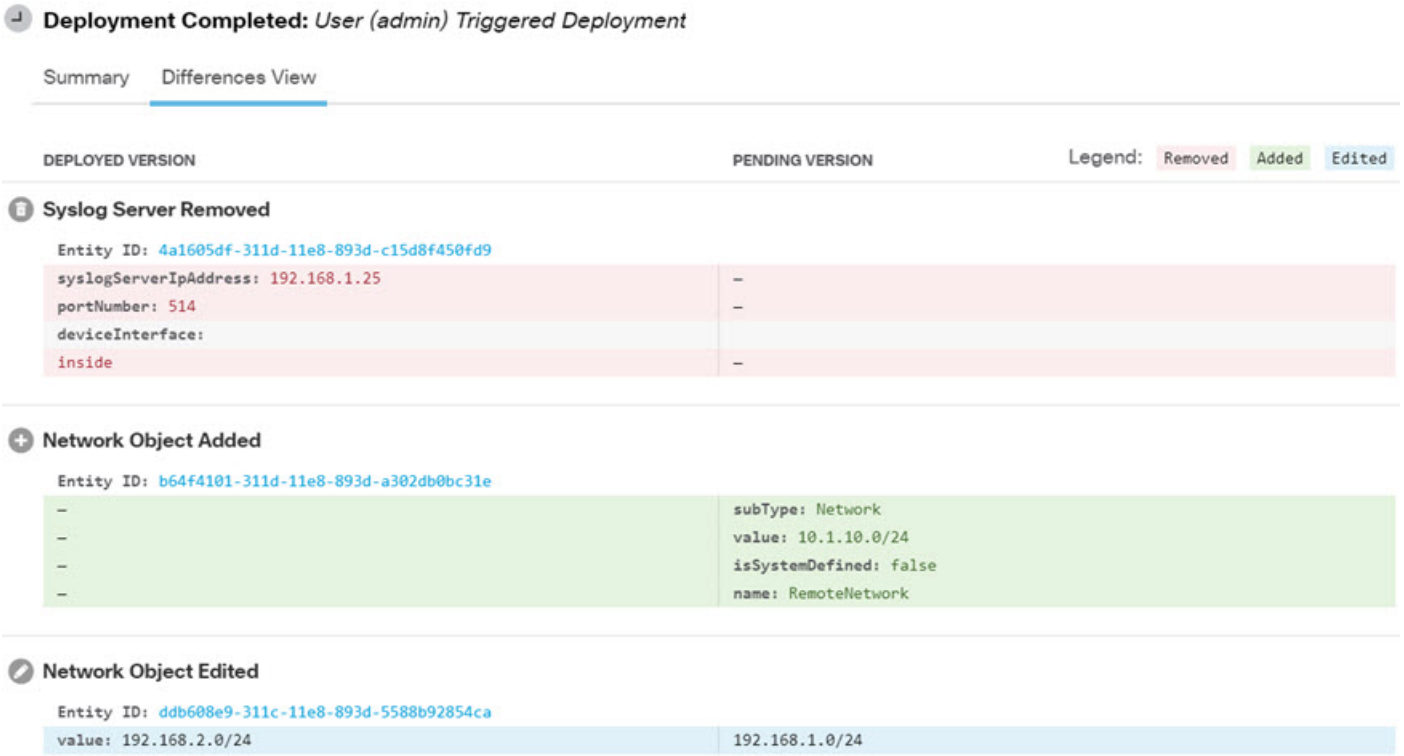
Étape 2 Cliquez sur **Audit Log** (Journal d'audit) dans la table des matières s'il n'est pas déjà sélectionné.

Étape 3 (Facultatif) Filtrer les messages :

- Événements de déploiement : cliquez sur le filtre prédéfini **Deployment History** (Historique de déploiement) dans la zone de filtre.
- Événements de modification d'entité : créez manuellement un filtre à l'aide de l'élément Event Type (Type d'événement) pour le type de modification qui vous intéresse. Pour voir toutes les modifications d'entités, incluez trois spécifications pour l'entité créée, l'entité mise à jour et l'entité supprimée. Le filtre ressemblerait à ce qui suit :



Étape 4 Ouvrez l'événement et cliquez sur l'onglet **Differences View** (Affichage des différences).



Les modifications sont codées par couleur et l'en-tête indique le type d'objet et s'il a été ajouté (Created (Créé)), supprimé (Deleted (Supprimé)) ou modifié (Updated (Mis à jour)). Les objets modifiés affichent uniquement les attributs qui ont été modifiés ou supprimés de l'objet. Dans les tâches de déploiement, il existe des en-têtes distincts pour chaque entité modifiée. L'en-tête indique le type d'entité de l'objet.

Annuler toutes les modifications en attente

Si vous n'êtes pas satisfait d'un ensemble de modifications de configuration qui n'ont pas encore été déployées, vous pouvez annuler toutes les modifications en attente. Ainsi, toutes les fonctionnalités sont restaurées à l'état qui existe sur le périphérique. Vous pouvez ensuite recommencer avec vos modifications de configuration.

Procédure

Étape 1 Cliquez sur l'icône **Deploy Changes** (déployer les modifications) dans le coin supérieur droit de la page Web.

L'icône est mise en évidence avec un point lorsqu'il y a des modifications en attente.

Étape 2 Cliquez sur **More Options (Plus d'options)** > **Discard All (Ignorer tout)**.

Étape 3 Cliquez sur **OK** dans la boîte de dialogue de confirmation.

Le système annule les modifications, et vous verrez un message indiquant qu'il n'y a aucune modification en attente une fois le processus terminé. Le système ajoute un événement Modifications en attente ignorées au journal d'audit.

Exporter la configuration du périphérique.

Téléchargez une copie de la configuration actuellement déployée au format JSON. Vous pouvez utiliser le fichier à des fins d'archivage ou de conservation des données. Toutes les données sensibles, telles que les mots de passe et les clés secrètes, sont masquées.

Vous ne pouvez pas importer le fichier dans cet appareil ou dans un autre appareil. Cette fonction ne remplace pas la sauvegarde du système.

Vous devez avoir effectué au moins une tâche de déploiement réussie avant de pouvoir télécharger la configuration.

Procédure

Étape 1 Choisissez **Device** (Périphérique), puis cliquez sur **View Configuration** (Afficher la configuration) dans le groupe **Device Administration** (Administration du périphérique).

Étape 2 Cliquez sur **Download Configuration** (Télécharger la configuration) dans la table des matières.

Étape 3 Cliquez sur **Get Device Configuration** (Obtenir la configuration du périphérique) pour lancer une tâche qui crée le fichier.

Si vous avez déjà créé un fichier, vous verrez un bouton de téléchargement et le message **File is ready to download** (Le fichier est prêt à être téléchargé), avec la date de création du fichier.

Selon la taille de la configuration, la génération du fichier peut prendre plusieurs minutes. Vérifiez la liste des tâches ou le journal d'audit, ou revenez à cette page périodiquement, jusqu'à ce que la tâche d'exportation de la configuration soit terminée et que le fichier soit généré.

Étape 4 Lorsque le fichier est généré, revenez à cette page et cliquez sur le bouton **Download the Configuration File** (Télécharger le fichier de configuration) ( ) pour enregistrer le fichier sur votre poste de travail.

Gestion de FDM et accès des utilisateurs FTD

Vous pouvez configurer une source d'authentification et d'autorisation externe pour que les utilisateurs puissent se connecter à FTD (accès HTTPS). Vous pouvez utiliser un serveur externe en plus ou à la place de la base de données des utilisateurs locaux et de l'utilisateur **admin** défini par le système. Notez que vous ne pouvez pas créer de comptes utilisateurs locaux supplémentaires pour l'accès FDM.

Bien que vous puissiez avoir plusieurs comptes d'utilisateurs FDM externes qui peuvent modifier la configuration, ces modifications ne sont pas suivies par utilisateur. Lorsqu'un utilisateur déploie des changements, les modifications effectuées par tous les utilisateurs sont déployées. Il n'y a aucun verrouillage : c'est-à-dire que plus d'un utilisateur peut tenter de mettre à jour le même objet en même temps, ce qui entraînera l'enregistrement d'un changement par un seul utilisateur. Vous ne pouvez pas non plus ignorer les modifications en fonction de l'utilisateur.

Vous pouvez avoir cinq sessions utilisateur simultanées. Si un sixième utilisateur se connecte, la session utilisateur la plus ancienne est automatiquement déconnectée. Il y a également un délai d'inactivité qui déconnecte les utilisateurs inactifs après 20 minutes.

Vous pouvez également configurer l'authentification et l'autorisation externes pour l'accès SSH à l'interface de ligne de commande Cisco Firepower Threat Defense. La base de données locale est toujours vérifiée avant d'utiliser la source externe. Vous pouvez donc créer des utilisateurs locaux supplémentaires pour un accès sécurisé. Ne créez pas d'utilisateurs en double dans la source locale et externe. À l'exception de l'utilisateur admin **admin**, il n'y a pas de croisement entre l'interface de ligne de commande et les utilisateurs FDM : les comptes d'utilisateurs sont complètement séparés.

Remarque Lorsque vous utilisez des serveurs externes, vous pouvez contrôler l'accès par utilisateur au niveau des sous-ensembles de vos périphériques en configurant des groupes de serveurs AAA distincts ou en créant des politiques d'authentification et d'autorisation dans les serveurs AAA qui permettent à l'utilisateur d'accéder uniquement à certaines adresses IP du périphériqueCisco Firepower Threat Defense.

Les rubriques suivantes expliquent comment configurer et gérer l'accès utilisateur FDM et l'accès utilisateur de l'interface de ligne de commande.

Configuration de l'autorisation externe (AAA) pour les utilisateurs HTTPS FDM

Vous pouvez fournir un accès HTTPS à FDM à partir d'un serveur AAA externe. En activant l'authentification et l'autorisation AAA, vous pouvez fournir différents niveaux de droits d'accès et ne pas demander à chaque utilisateur de se connecter avec le compte **admin** local.

Ces utilisateurs externes sont également autorisés pour l'API FTD et l'API Explorer.

Vous pouvez fournir un contrôle d'accès basé sur les rôles (RBAC) en configurant l'autorisation pour les utilisateurs de gestion dans le serveur AAA. Les niveaux varient selon le type de serveur. Lorsqu'un utilisateur se connecte à FDM, le nom d'utilisateur et le rôle sont affichés dans le coin supérieur droit de la page. Après avoir configuré les comptes correctement sur le serveur AAA, vous pouvez l'activer pour un accès administratif en utilisant cette procédure.

Autorisation utilisateur RADIUS

Pour fournir un contrôle d'accès basé sur les rôles, mettez à jour les comptes d'utilisateurs sur votre serveur RADIUS pour définir l'attribut **cisco-av-pair** (dans ISE, mais l'attribut est écrit Cisco-AVPair dans RADIUS gratuit; vérifiez votre système pour vérifier si l'écriture est correcte). Cet attribut doit être défini correctement sur un compte utilisateur, sinon l'utilisateur se voit refuser l'accès à l'API REST.FDM Voici les valeurs suivantes prises en charge pour l'attribut **cisco-av-pair** :

- **fdm.userrole.authority.admin** fournit un accès administrateur complet. Ces utilisateurs peuvent effectuer toutes les actions que l'utilisateur **admin** local peut effectuer.
- **fdm.userrole.authority.rw** fournit un accès en lecture-écriture. Ces utilisateurs peuvent faire tout ce qu'un utilisateur en lecture seule peut faire, ainsi que modifier et déployer la configuration. Les seules restrictions concernent les actions critiques pour le système, qui comprennent l'installation des mises à niveau, la création et la restauration de sauvegardes, l'affichage du journal d'audit et la déconnexion d'autres utilisateurs.FDM
- **fdm.userrole.authority.ro** fournit un accès en lecture seule. Ces utilisateurs peuvent afficher les tableaux de bord et la configuration, mais ne peuvent apporter aucune modification. Si l'utilisateur tente d'apporter une modification, le message d'erreur explique que cela est causé par un manque d'autorisation.

Procédure

Étape 1 Cliquez sur **Device** (dispositif), puis cliquez sur le lien **System Settings** > **Management Access**.

Si vous êtes déjà dans la page des paramètres système (System Settings), cliquez simplement sur **Management Access List** (liste d'accès de gestion) dans la table des matières.

Étape 2 Cliquez sur l'onglet **AAA Configuration** s'il n'est pas déjà sélectionné.

Étape 3 Configurez les options (**HTTPS Connection (Connexion HTTPS)**) :

- **Server Group for Management/REST API** (Groupe de serveurs pour la gestion/l'API REST) : sélectionnez le groupe de serveurs RADIUS (pour l'authentification/autorisation externe) ou la base de données d'utilisateurs locaux (LocalIdentitySource) que vous souhaitez utiliser comme source d'authentification principale.

  Si le groupe de serveurs n'existe pas encore, cliquez sur le lien pour créer un nouveau groupe et créez-le maintenant. Pour RADIUS, vous devrez également créer des objets de serveur RADIUS pour chaque serveur, afin de les ajouter au groupe, mais vous pouvez le faire tout en définissant le groupe de serveurs. Pour en savoir plus sur RADIUS, consultez Serveurs et groupes RADIUS.

- **Authentication with LOCAL** (Authentification avec LOCAL) (RADIUS uniquement.) : si vous sélectionnez un groupe de serveurs RADIUS externes, vous pouvez spécifier comment utiliser la source d'identité locale, qui contient le compte utilisateur local **admin**. Sélectionnez l'une des options suivantes :
  - **Before External Server** (Avant le serveur externe) : le système vérifie d'abord le nom d'utilisateur et le mot de passe par rapport à la source locale.
  - **After External Server** (Après le serveur externe) : la source locale est vérifiée uniquement si la source externe n'est pas disponible ou si le compte d'utilisateur n'a pas été trouvé dans la source externe.
  - **Never** (Jamais) : (non recommandé.) La source locale n'est jamais utilisée, vous ne pouvez donc pas vous connecter en tant qu'utilisateur admin.

    Mise en garde
    Si vous sélectionnez **Never** (Jamais), vous ne pourrez pas vous connecter au FDM en utilisant le compte **admin**. Vous serez verrouillé hors du système si le serveur AAA devient indisponible ou si vous configurez mal les comptes dans le serveur AAA.

Étape 4 Cliquez sur **Save** (enregistrer).

Configuration de l'autorisation externe (AAA) pour les utilisateurs de l'interface de commande (SSH) FTD

Vous pouvez fournir un accès SSH à l'interface de ligne de commande FTD à partir d'un serveur RADIUS externe. En activant l'authentification et l'autorisation RADIUS, vous pouvez fournir différents niveaux de droits d'accès à partir d'une source d'authentification unique, plutôt que de définir des comptes d'utilisateurs locaux distincts sur chaque appareil.

Ces utilisateurs externes SSH ne sont **pas** autorisés pour l'API FTD et l'API Explorer. Le mécanisme que vous utilisez pour définir l'autorisation SSH est différent de celui requis pour l'accès HTTPS. Cependant, vous pouvez configurer le même utilisateur RADIUS avec les critères d'authentification SSH et HTTPS, de sorte qu'un utilisateur donné puisse accéder au système via les deux protocoles.

Pour fournir un contrôle d'accès basé sur les rôles (RBAC) pour l'accès SSH, mettez à jour les comptes d'utilisateur sur votre serveur RADIUS pour définir l'attribut de type de service (**Service-Type**). Cet attribut doit être défini sur un compte utilisateur, sinon l'utilisateur se voit refuser l'accès SSH au périphérique. Voici les valeurs suivantes prises en charge pour l'attribut **Service-Type** :

- **Administratif (6)** : Fournit une autorisation d'accès de **configuration** au niveau de l'interface de ligne de commande. Ces utilisateurs peuvent utiliser toutes les commandes de l'interface de ligne de commande.
- **NAS Prompt (7)** ou tout autre niveau que 6 : Fournit une autorisation d'accès de **base** au niveau de l'interface de ligne de commande. Ces utilisateurs peuvent utiliser des commandes de lecture seule, comme les commandes **show**, à des fins de surveillance et de dépannage.

Après avoir configuré les comptes correctement sur le serveur RADIUS, vous pouvez l'activer pour un accès administratif SSH à l'aide de cette procédure.

Remarque Ne créez pas d'utilisateurs en double dans la source locale et externe. Si vous créez des noms d'utilisateur en double, assurez-vous qu'ils ont les mêmes droits d'autorisation. Vous ne pouvez pas vous connecter en utilisant le mot de passe de la version externe du compte d'utilisateur lorsque les droits d'autorisation diffèrent dans le compte d'utilisateur local; vous pouvez vous connecter en utilisant uniquement le mot de passe local. Si les droits sont identiques, le mot de passe que vous utilisez détermine si vous êtes connecté en tant qu'utilisateur externe ou local, en supposant que les mots de passe sont différents. Même si la base de données locale est vérifiée en premier, si un nom d'utilisateur existe dans la base de données locale mais que le mot de passe est incorrect, le serveur externe est vérifié, et si le mot de passe est correct pour la source externe, la connexion réussira.

Avant de commencer

Veuillez informer les utilisateurs définis en externe du comportement suivant afin de définir correctement les attentes :

- La première fois qu'un utilisateur externe se connecte, le FTD crée les structures requises mais ne peut pas créer simultanément la séance de l'utilisateur. L'utilisateur doit simplement s'authentifier à nouveau pour démarrer la session. L'utilisateur verra un message semblable au suivant : « New external username identified. Please log in again to start a session. » (Vos privilèges d'autorisation ont changé. Veuillez vous reconnecter pour lancer une session.)
- De même, si l'autorisation de l'utilisateur (définie dans le type de service) a été modifiée depuis la dernière connexion, l'utilisateur devra s'authentifier de nouveau. L'utilisateur verra un message semblable au suivant : « Your authorization privilege has changed. Please log in again to start a session. » (Vos privilèges d'autorisation ont changé. Veuillez vous reconnecter pour lancer une session.)

Procédure

Étape 1 Cliquez sur **Device** (dispositif), puis cliquez sur le lien **System Settings** > **Management Access**.

Si vous êtes déjà dans la page des paramètres système (System Settings), cliquez simplement sur **Management Access List** (liste d'accès de gestion) dans la table des matières.

Étape 2 Cliquez sur l'onglet **AAA Configuration** s'il n'est pas déjà sélectionné.

Étape 3 Configurez les options de connexion SSH (**SSH Connection**) :

- **Server Group** (groupe de serveurs) : Sélectionnez le groupe de serveurs RADIUS ou la base de données d'utilisateurs locaux (LocalIdentitySource) que vous souhaitez utiliser comme source d'authentification principale. Vous devez sélectionner un groupe de serveurs RADIUS pour utiliser une autorisation externe.

  Si le groupe de serveurs n'existe pas encore, cliquez sur le lien **Create New RADIUS Server Group** pour créer immédiatement un nouveau groupe de serveurs RADIUS. Vous devrez également créer des objets de serveur RADIUS pour chaque serveur, afin de les ajouter au groupe, mais vous pouvez le faire tout en définissant le groupe de serveurs. Pour en savoir plus sur RADIUS, consultez Serveurs et groupes RADIUS.

  Notez que les connexions SSH utilisent uniquement les deux premiers serveurs du groupe. Si vous utilisez un groupe comptant trois serveurs ou plus, les serveurs supplémentaires ne seront jamais essayés. En

outre, les attributs de groupe **Dead Time** (temps mort) et **Maximum Failed Attempts** (nombre maximal de tentatives échouées) ne sont pas utilisés.

- **Authentification with LOCAL** : Si vous sélectionnez un groupe de serveurs externes, vous pouvez spécifier comment utiliser la source d'identité locale. Pour l'accès SSH, la base de données locale est toujours vérifiée avant le serveur externe.

Étape 4 Cliquez sur **Save** (enregistrer).

Gérer les sessions des utilisateurs FDM

Choisissez **Monitoring (Surveillance)** > **Sessions** pour afficher la liste des utilisateurs actuellement connectés à FDM. La liste indique la durée de connexion de chaque utilisateur pour la session actuelle.

Si le même nom d'utilisateur apparaît plus d'une fois, cela signifie que l'utilisateur a ouvert des sessions à partir d'adresses source différentes. Les sessions sont suivies séparément en fonction du nom d'utilisateur et de l'adresse source, chaque session ayant son propre horodatage unique.

Le système permet 5 sessions utilisateur simultanées. Si un sixième utilisateur se connecte, la session utilisateur la plus ancienne est automatiquement déconnectée. En outre, les utilisateurs inactifs sont automatiquement déconnectés après 20 minutes d'inactivité.

Si l'utilisateur FDM saisit le mauvais mot de passe et ne parvient pas à se connecter lors de 3 tentatives consécutives, le compte de l'utilisateur est verrouillé pendant 5 minutes. L'utilisateur doit attendre avant de réessayer de se connecter. Il n'y a aucun moyen de déverrouiller le compte d'utilisateur FDM, ni d'ajuster le nombre de tentatives ou le délai de verrouillage. (Notez que pour les utilisateurs SSH, vous pouvez ajuster ces paramètres et déverrouiller le compte.)

Si nécessaire, vous pouvez mettre fin à une session utilisateur en cliquant sur l'icône de suppression ( ) de la session. Si vous supprimez votre propre session, vous êtes également déconnecté. Il n'y a pas de période de verrouillage si vous mettez fin à une session : l'utilisateur peut se connecter immédiatement.

Activation de l'accès FDM sur une unité de secours à haute disponibilité pour les utilisateurs externes

Si vous configurez l'autorisation extérieure pour les utilisateurs FDM, ces utilisateurs peuvent se connecter à l'unité active et en veille d'une paire à haute disponibilité. Cependant, la connexion réussie à l'unité de secours pour la première fois nécessite quelques étapes supplémentaires par rapport à la connexion à l'unité active.

Après qu'un utilisateur externe se soit connecté à l'unité active pour la première fois, le système crée un objet qui définit l'utilisateur et les droits d'accès de l'utilisateur. Un utilisateur administrateur ou en lecture-écriture doit ensuite déployer la configuration à partir de l'unité active pour que l'objet utilisateur s'affiche sur l'unité de secours.

Ce n'est qu'après l'achèvement réussi du déploiement et de la synchronisation de la configuration que l'utilisateur externe peut se connecter à l'unité de secours.

Les utilisateurs administrateurs et de lecture-écriture peuvent déployer les modifications après s'être connectés à l'unité active. Cependant, les utilisateurs en lecture seule ne peuvent pas déployer la configuration et doivent demander à un utilisateur disposant des droits appropriés de déployer la configuration.

Création de comptes d'utilisateur locaux pour l'interface de ligne de commande de FTD

Vous pouvez créer des utilisateurs pour l'accès à l'interface de ligne de commande sur les appareils Cisco Firepower Threat Defense. Ces comptes ne permettent pas l'accès à l'application de gestion, mais à l'interface de ligne de commande uniquement. L'interface de ligne de commande est utile pour le dépannage et la surveillance.

Vous ne pouvez pas créer de comptes utilisateur locaux sur plusieurs appareils à la fois. Chaque périphérique possède son propre ensemble de comptes utilisateur uniques d'interface de ligne de commande.

Procédure

Étape 1 Connectez-vous à l'interface de ligne de commande de l'appareil en utilisant un compte avec des privilèges de configuration.

Le compte d'utilisateur admin dispose des privilèges requis, mais tout compte doté de privilèges de configuration fonctionnera. Vous pouvez utiliser une session SSH ou le port de console.

Pour certains modèles d'appareils, le port de console vous place dans l'interface de ligne de commande FXOS. Utilisez la commande **connect ftd** pour accéder à l'interface de ligne de commande Cisco Firepower Threat Defense.

Étape 2 Créez un compte utilisateur.

configure user add *username* (nom d'utilisateur) {**basic** | **config**}

Vous pouvez définir l'utilisateur avec les niveaux de privilège suivants :

- **config** : Donne accès à la configuration utilisateur. Cela donne à l'utilisateur tous les droits d'administrateur sur toutes les commandes.
- **basic** : Donne à l'utilisateur un accès de base. Cela ne permet pas à l'utilisateur d'entrer des commandes de configuration.

Exemple :

Dans l'exemple suivant, un compte d'utilisateur nommé joecool est ajouté avec des droits d'accès de configuration. Le mot de passe ne s'affiche pas lorsque vous le saisissez.

```
> configure user add joecool config
Enter new password for user joecool: newpassword
Confirm new password for user joecool: newpassword
> show user
Login              UID   Auth Access  Enabled Reset    Exp Warn  Str Lock Max
admin             1000  Local Config  Enabled    No  Never  N/A  Dis   No N/A
joecool           1001  Local Config  Enabled    No  Never  N/A  Dis   No   5
```

Remarque

Dites aux utilisateurs qu'ils peuvent changer leur mot de passe à l'aide de la commande **configure password**.

Étape 3 (Facultatif) Ajustez les caractéristiques du compte pour satisfaire à vos exigences de sécurité.

Vous pouvez utiliser les commandes suivantes pour modifier le comportement par défaut du compte.

- **configure user aging** *nom d'utilisateur max_days warn_days*

  Définit une date d'expiration pour le mot de passe de l'utilisateur. Précisez le nombre maximal de jours de la période de validité du mot de passe, suivi du nombre de jours de préavis (c.-à-d. le moment auquel l'utilisateur sera averti de l'expiration prochaine). Les deux valeurs sont comprises entre 1 et 9999, mais le nombre de jours de préavis doit être inférieur au nombre de jours de la période de validité maximale. Lorsque vous créez le compte, le mot de passe ne comporte aucune date d'échéance.

- **configure user forcereset** *username (nom d'utilisateur)*

  Force l'utilisateur à modifier le mot de passe lors de la prochaine connexion.

- **configure user maxfailedlogins** *username number (numéro d'utilisateur)*

  Définit le nombre maximal de connexions échouées consécutives que vous autoriserez avant de verrouiller le compte (de 1 à 9999). Utilisez la commande **configure user unlock** pour déverrouiller des comptes. La valeur par défaut pour les nouveaux comptes est cinq échecs consécutifs de connexion.

- **configure user minpasswdlen** *username number (numéro d'utilisateur)*

  Définit une longueur de mot de passe minimale, qui peut aller de 1 à 127.

- **configure user strengthcheck** *username (nom d'utilisateur)* {**enable** | **disable**}

  Active ou désactive la vérification de la force du mot de passe, qui contraint un utilisateur à répondre à des critères de mot de passe spécifiques lors de la modification de son mot de passe. Lorsque le mot de passe d'un utilisateur expire ou si la commande **configure user forcereset** est utilisée, cette exigence est automatiquement activée lors de la prochaine connexion de l'utilisateur.

Étape 4 Gérez les comptes utilisateur au besoin.

Il arrive que des comptes soient verrouillés ou que vous deviez supprimer des comptes ou résoudre d'autres problèmes. Utilisez les commandes suivantes pour gérer les comptes d'utilisateur dans le système.

- **configure user access** *username (nom d'utilisateur)* {**basic** | **config**}

  Modifie les privilèges d'un compte d'utilisateur.

- **configure user delete** *username (nom d'utilisateur)*

  Supprime le compte spécifié.

- **configure user disable** *username (nom d'utilisateur)*

  Désactive le compte spécifié sans le supprimer. L'utilisateur ne peut pas se connecter tant que vous n'avez pas activé le compte.

- **configure user enable** *username (nom d'utilisateur)*

  Active le compte spécifié.

- **configure user password** *username (nom d'utilisateur)*

  Modifie le mot de passe de l'utilisateur spécifié. Les utilisateurs doivent normalement modifier leur propre mot de passe à l'aide de la commande **configure password**.

- **configure user unlock** *username (nom d'utilisateur)*

Déverrouille un compte d'utilisateur qui a été verrouillé en raison du nombre maximal de tentatives de connexion échouées consécutives.

Redémarrage ou arrêt du système

Si nécessaire, vous pouvez redémarrer ou arrêter le système.

En plus de la procédure ci-dessous, vous pouvez également effectuer ces tâches par le biais d'une session SSH ou de la console CLI FDM en utilisant les commandes **reboot** ou **shutdown**.

Remarque L'ISA 3000 ne prend pas en charge l'arrêt; vous pouvez uniquement redémarrer le système.

Procédure

Étape 1 Cliquez sur **Device** (périphérique), puis cliquez sur le lien **System Settings (paramètres système)** > **Reboot/Shutdown (redémarrage/arrêt)**.

Si vous êtes déjà dans la page des paramètres système, cliquez simplement sur **Reboot/Shutdown** (redémarrage/arrêt) dans la table des matières.

Étape 2 Cliquez sur le bouton qui effectue la fonction dont vous avez besoin.

- **Reboot** (Redémarrer) : si vous pensez que le système ne fonctionne pas correctement et que d'autres tentatives pour résoudre le problème ont échoué, vous pouvez redémarrer le périphérique. En outre, il peut y avoir quelques procédures qui vous demanderont de redémarrer le périphérique pour recharger le logiciel système.
- **Reboot** (Redémarrer) : mettez le système hors tension de manière contrôlée. Utilisez l'arrêt lorsque vous avez l'intention de retirer le périphérique du réseau, par exemple pour le remplacer. Après avoir éteint le périphérique, vous pouvez le rallumer uniquement à partir du commutateur marche/arrêt du matériel.

Étape 3 Attendez que l'action soit terminée.

Si vous disposez d'une connexion de console au pare-feu, surveillez les notifications du système lorsque le pare-feu s'éteint. La notification suivante s'affichera :

```
System is stopped.
It is safe to power off now.
Do you want to reboot instead? [y/N]
```

Vous ne pouvez pas effectuer d'autres actions dans FDM ou l'interface de ligne de commande pendant le redémarrage ou l'arrêt du système.

Pendant le redémarrage, la page FDM devrait être actualisée une fois le redémarrage terminé et vous mener à la page de connexion. Si vous essayez d'actualiser la page avant la fin du redémarrage, le navigateur Web peut renvoyer des erreurs 503 ou 404, en fonction de l'état opérationnel du serveur Web FDM à ce moment-là.

Pour l'arrêt, le système ne pourra pas répondre du tout et vous obtiendrez des erreurs 404. Il s'agit du résultat attendu, car vous éteignez complètement le système.

Dépannage du système

Les rubriques suivantes traitent de certaines tâches et fonctionnalités de résolution de problèmes au niveau du système. Pour en savoir plus sur le dépannage d'une fonction en particulier, comme le contrôle d'accès, consultez le chapitre correspondant.

Envoi de requêtes ping pour tester la connectivité

La commande ping est un outil simple qui vous permet de déterminer si une adresse particulière est active et répond. Cela signifie que la connectivité de base fonctionne. Cependant, d'autres politiques exécutées sur un périphérique peuvent empêcher des types de trafic spécifiques de passer par un périphérique. Vous pouvez l'utiliser **ping** en ouvrant la console d'interface de ligne de commande ou en vous connectant à l'interface de ligne de commande du périphérique.

Remarque Comme le système dispose de plusieurs interfaces, vous pouvez contrôler l'interface utilisée pour envoyer un ping à une adresse. Vous devez vous assurer que vous utilisez la bonne commande, afin de tester la connectivité qui compte. Par exemple, le système doit pouvoir atteindre le serveur de licences Cisco par l'intermédiaire de l'interface de gestion virtuelle . Vous devez donc utiliser la commande **ping system** pour tester la connexion. Si vous utilisez **ping**, vous testez si une adresse peut être atteinte par l'intermédiaire des interfaces de données, ce qui pourrait ne pas vous donner le même résultat.

Le ping normal utilise des paquets ICMP pour tester la connexion. Si votre réseau interdit ICMP, vous pouvez utiliser un ping TCP à la place (pour les pings d'interface de données uniquement).

Vous pouvez envoyer un ping à une adresse IP ou à un nom de domaine complet (FQDN). Pour qu'un ping fonctionne sur un nom de domaine complet, les serveurs DNS configurés pour les interfaces de gestion ou de données doivent renvoyer avec succès une adresse IP. Vous devez configurer séparément les serveurs DNS pour les interfaces de gestion et de données. Si vous n'avez pas configuré de serveurs DNS pour une interface spécifique, utilisez la commande **dig** pour rechercher l'adresse IP d'un nom de domaine complet donné.

Voici les principales options pour envoyer des pings aux adresses réseau.

Ping d'une adresse par l'intermédiaire de l'interface de gestion virtuelle

Utilisez la commande **ping system**.

ping system *host*

L'hôte peut être une adresse IP ou un nom de domaine complet (FQDN), tel que www.exemple.com. Contrairement aux pings via les interfaces de données, il n'y a pas de nombre par défaut pour les pings système. Le ping continue jusqu'à ce que vous l'arrêtiez à l'aide de Ctrl+C. Par exemple :

```
> ping system www.cisco.com
PING origin-www.cisco.COM (72.163.4.161) 56(84) bytes of data.
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=1 ttl=242 time=10.6 ms
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=2 ttl=242 time=8.13 ms
```

```
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=3 ttl=242 time=8.51 ms
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=4 ttl=242 time=8.40 ms
^C
--- origin-www.cisco.COM ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 8.139/8.927/10.650/1.003 ms
>
```

Ping d’une adresse par l’intermédiaire d’une interface de données à l’aide de la table de routage

Utilisez la commande **ping**. Sans préciser d’interface, vous testez si le système peut trouver de manière générique une voie de routage vers l’hôte. Comme il s’agit de la façon dont le système achemine normalement le trafic, c’est généralement ce que vous souhaitez tester.

ping *host*

Par exemple :

```
> ping 171.69.38.1
Sending 5, 100-byte ICMP Echos to 171.69.38.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

Remarque Vous pouvez préciser le délai d’expiration, le nombre de répétitions, la taille des paquets et même le modèle de données à envoyer. Utilisez l’indicateur d’aide « ? » dans la console d’interface en ligne de commande pour voir les options disponibles.

Ping d’une adresse par l’intermédiaire d’une interface de données spécifique

Utilisez la commande **ping interface** *if_name* si vous souhaitez tester la connectivité par l’intermédiaire d’une interface de données spécifique. Vous pouvez également spécifier l’interface de diagnostic en utilisant cette commande, mais pas l’interface de gestion virtuelle.

ping interface *if_name hôte*

Par exemple :

```
> ping interface inside 171.69.38.1
Sending 5, 100-byte ICMP Echos to 171.69.38.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

Ping d'une adresse par l'intermédiaire d'une interface de données à l'aide du ping TCP

Utilisez la commande **ping tcp**. Un ping TCP envoie des paquets SYN et considère l’envoi ping comme réussi si la destination envoie un paquet SYN-ACK.

ping tcp [**interface** *if_name*] *hôte port*

Vous devez préciser l’hôte et le port TCP.

Vous pouvez éventuellement préciser l’interface, qui est l’interface source du ping, et non l’interface par laquelle envoyer les ping. Ce type de ping utilise toujours la table de routage.

Un ping TCP envoie des paquets SYN et considère l’envoi ping comme réussi si la destination envoie un paquet SYN-ACK. Par exemple :

```
> ping tcp 10.0.0.1 21
Type escape sequence to abort.
No source specified. Pinging from identity interface.
Sending 5 TCP SYN requests to 10.0.0.1 port 21
from 10.0.0.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Remarque Vous pouvez également préciser le délai d'expiration, le nombre de répétitions et l'adresse source du ping TCP. Utilisez l'indicateur d'aide « ? » dans la console d'interface en ligne de commande pour voir les options disponibles.

Suivi des routes vers les hôtes

Si vous éprouvez des problèmes pour envoyer le trafic vers une adresse IP, vous pouvez retracer la route vers l'hôte pour déterminer s'il y a un problème sur le chemin du réseau. Un traceroute fonctionne par envoi de paquets UDP sur un port non valide, ou d'échos ICMPv6, vers une destination. Les routeurs le long du chemin vers la destination répondent avec un message ICMP Time Exceeded et signalent cette erreur à traceroute. Chaque nœud reçoit trois paquets, ce qui vous donne trois possibilités par nœud d'obtenir un résultat informatif. Vous pouvez l'utiliser **traceroute** en ouvrant la console d'interface de ligne de commande ou en vous connectant à l'interface de ligne de commande du périphérique.

Remarque Il existe des commandes distinctes pour tracer un routage par l'intermédiaire d'une interface de données (**traceroute**) ou par l'interface de gestion virtuelle (**traceroute system**). Assurez-vous d'utiliser la bonne commande.

Le tableau suivant décrit le résultat possible par paquet, comme affiché dans la sortie.

Output Symbol (Icône de sortie)	Description
*	Aucune réponse n'a été reçue pour la sonde dans le délai d'expiration.
nn msec	Pour chaque nœud, le temps aller-retour (en millisecondes) pour le nombre spécifié de sondes.
!N.	Réseau inaccessible ICMP
!H	Hôte inaccessible ICMP
!P	Protocole inaccessible ICMP
!A	Administrativement interdit ICMP
?	Erreur ICMP inconnue.

Suivi d'un routage par le biais de l'interface de gestion virtuelle

Utilisez la commande **traceroute system**.

traceroute system *destination*

L'hôte peut être une adresse IPv4/IPv6 ou un nom de domaine complet (FQDN), tel que www.exemple.com. Par exemple :

```
> traceroute system www.example.com
traceroute to www.example.com (172.163.4.161), 30 hops max, 60 byte packets
 1  192.168.0.254 (192.168.0.254)  0.213 ms  0.310 ms  0.328 ms
 2  10.88.127.1 (10.88.127.1)  0.677 ms  0.739 ms  0.899 ms
 3  lab-gw1.example.com (10.89.128.25)  0.638 ms  0.856 ms  0.864 ms
 4  04-bb-gw1.example.com (10.152.240.65)  1.169 ms  1.355 ms  1.409 ms
 5  wan-gw1.example.com (10.152.240.33)  0.712 ms  0.722 ms  0.790 ms
 6  wag-gw1.example.com (10.152.240.73)  13.868 ms  10.760 ms  11.187 ms
 7  rbb-gw2.example.com (172.30.4.85)  7.202 ms  7.301 ms  7.101 ms
 8  rbb-gw1.example.com (172.30.4.77)  8.162 ms  8.225 ms  8.373 ms
 9  sbb-gw1.example.com (172.16.16.210)  7.396 ms  7.548 ms  7.653 ms
10  corp-gw2.example.com (172.16.16.58)  7.413 ms  7.310 ms  7.431 ms
11  dmzbb-gw2.example.com (172.16.0.78)  7.835 ms  7.705 ms  7.702 ms
12  dmzdcc-gw2.example.com (172.16.0.190)  8.126 ms  8.193 ms  11.559 ms
13  dcz05n-gw1.example.com (172.16.2.106)  11.729 ms  11.728 ms  11.939 ms
14  www1.example.com (172.16.4.161)  11.645 ms  7.958 ms  7.936 ms
```

Suivi d'un routage par le biais d'une interface de données

Utilisez la commande **traceroute**.

traceroute *destination*

L'hôte peut être une adresse IPv4 ou IPv6 ou un nom de domaine complet (FQDN), tel que www.exemple.com, si vous configurez les serveurs DNS pour les interfaces de données. Si vous n'avez pas configuré de serveurs DNS pour une interface spécifique, utilisez la commande **dig** pour rechercher l'adresse IP d'un nom de domaine complet donné. Par exemple :

```
> traceroute 209.165.200.225
Tracing the route to 209.165.200.225
 1  10.83.194.1 0 msec 10 msec 0 msec
 2  10.83.193.65 0 msec 0 msec 0 msec
 3  10.88.193.101 0 msec 10 msec 0 msec
 4  10.88.193.97 0 msec 0 msec 10 msec
 5  10.88.239.9 0 msec 10 msec 0 msec
 6  10.88.238.65 10 msec 10 msec 0 msec
 7 172.16.7.221 70 msec 70 msec 80 msec
 8 209.165.200.225 70 msec 70 msec 70 msec
```

Remarque Vous pouvez préciser le délai d'expiration, la durée de vie, le nombre de paquets par nœud et même l'adresse IP ou l'interface à utiliser comme source du traceroute. Utilisez l'indicateur d'aide, ?, dans l'interface de ligne de commande pour voir les options disponibles.

Faire apparaître le périphérique sur les Traceroutes

Par défaut, le périphérique FTD n'apparaît pas sur les Traceroutes en tant que saut. Pour l'afficher, vous devez décrémenter la durée de vie des paquets qui passent par le périphérique et augmenter la limite de débit pour les messages ICMP unreachable. Pour ce faire, vous devez créer un objet FlexConfig qui configure la règle de politique de service requise et d'autres options.

Pour une description détaillée des politiques de service et des classes de trafic, consultez le *guide de configuration des pare-feu Cisco ASA Series* accessible à l'adresse https://www.cisco.com/c/en/us/support/security/asa-firepower-services/products-installation-and-configuration-guides-list.html.

Remarque Si vous décrémentez la durée de vie, les paquets avec une TTL de 1 seront abandonnés, mais une connexion sera ouverte pour la session en supposant que la connexion pourrait contenir des paquets avec une TTL plus élevée. Notez que certains paquets, comme les paquets Hello d'OSPF, sont envoyés avec une TTL = 1, donc la décrémentation de la durée de vie peut avoir des conséquences inattendues. Gardez ces considérations à l'esprit lorsque vous définissez votre classe de trafic.

Procédure

Étape 1 Cliquez sur **View Configuration** (Afficher la configuration) dans **Device (Périphérique)** > **Advanced Configuration (Configuration avancée)**.

Étape 2 Cliquez sur **FlexConfig** > **FlexConfig Objects (Objets FlexConfig)** dans la table des matières de configuration avancée.

Étape 3 Créez l'objet pour décrémenter le TTL.

a) Cliquez sur le bouton **+** pour créer un nouvel objet.

b) Entrez un nom pour l'objet. Par exemple, **Décrémenter_TTL**.

c) Dans l'éditeur **Template** (Modèle), saisissez les lignes suivantes, y compris les indentations.

```
icmp unreachable rate-limit 50 burst-size 1
policy-map global_policy
 class class-default
  set connection decrement-ttl
```

d) Dans l'éditeur **Negate Template** (Modèle d'annulation), saisissez les lignes nécessaires pour annuler cette configuration.

Tout comme vous devez inclure les commandes parentes pour entrer dans le sous-mode approprié pour une commande afin de l'activer, vous devez également inclure ces commandes dans le modèle de négation.

Le modèle d'annulation sera appliqué si vous supprimez cet objet de la politique FlexConfig (après l'avoir déployé avec succès), et également lors d'un déploiement infructueux (pour réinitialiser la configuration à son état précédent).

Ainsi, pour cet exemple, le modèle de négation serait le suivant :

```
no icmp unreachable rate-limit 50 burst-size 1
policy-map global_policy
 class class-default
```

```
no set connection decrement-ttl
```

e) Cliquez sur **OK** pour enregistrer l'objet.

Étape 4 Ajoutez les objets à la politique FlexConfig.

Seuls les objets sélectionnés dans la politique FlexConfig sont déployés.

a) Cliquez sur **FlexConfig Policy** (Politique FlexConfig) dans la table des matières.
b) Cliquez sur **+** dans la liste des groupes.
c) Sélectionnez l'objet Dement_TTL et cliquez sur **OK**.

L'aperçu doit être mis à jour avec les commandes du modèle. Vérifiez que vous voyez les commandes attendues.

d) Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant déployer la politique.

Dépannage du protocole NTP

Le système dépend d'une heure précise et constante pour fonctionner correctement et pour s'assurer que les événements et les autres points de données sont traités avec exactitude. Vous devez configurer au moins un, mais idéalement trois, serveurs NTP (Network Time Protocol) pour que le système dispose toujours d'informations horaires fiables.

Le diagramme récapitulatif de la connexion du périphérique (cliquez sur **Device** (Périphérique) dans le menu principal) affiche l'état de la connexion au serveur NTP. Si l'état est jaune ou orange, un problème de connexion existe avec les serveurs configurés. Si le problème de connexion persiste (et qu'il ne s'agit pas simplement d'un problème momentané), essayez ce qui suit.

- Tout d'abord, assurez-vous qu'au moins trois serveurs NTP sont configurés dans **Device (Périphérique)** > **System Settings (Paramètres système)** > **NTP**. Bien qu'il ne s'agisse pas d'une exigence, la fiabilité est considérablement améliorée si vous avez au moins trois serveurs NTP.
- Assurez-vous qu'il existe un chemin réseau entre l'adresse IP de l'interface de gestion (définie dans **Device (Périphérique)** > **System Settings (Paramètres système)** > **Management Interface (Interface de gestion)**) et les serveurs NTP.
  - Si la passerelle de l'interface de gestion correspond aux interfaces de données, vous pouvez configurer des routes statiques vers les serveurs NTP dans **Device (Périphérique)** > **Routing (Routage)** si la route par défaut n'est pas adéquate.
  - Si vous définissez une passerelle d'interface de gestion explicite, connectez-vous à l'interface CLI du périphérique et utilisez la commande **ping system** pour vérifier s'il existe un chemin réseau vers chaque serveur NTP.
- Connectez-vous à l'interface CLI du périphérique et vérifiez l'état des serveurs NTP à l'aide des commandes suivantes.
  - **show ntp** : cette commande affiche des informations de base sur les serveurs NTP et leur disponibilité. Cependant, l'état de connectivité dans le FDM utilise des informations supplémentaires pour indiquer l'état, de sorte qu'il peut y avoir une incohérence dans ce que cette commande affiche et ce que

montre le diagramme d'état de connectivité. Vous pouvez également émettre cette commande à partir de la console d'interface de ligne de commande.

- **system support ntp** : cette commande comprend la sortie de **show ntp** plus la sortie de la commande NTP standard **ntpq**, qui est documentée avec le protocole NTP. Utilisez cette commande si vous devez confirmer la synchronisation NTP.

  Recherchez la section « Résultats de « ntpq -pn ». Par exemple, vous pourriez voir quelque chose comme ce qui suit :

```
Results of 'ntpq -pn'
remote                   : +216.229.0.50
refid                    : 129.7.1.66
st                       : 2
t                        : u
when                     : 704
poll                     : 1024
reach                    : 377
delay                    : 90.455
offset                   : 2.954
jitter                   : 2.473
```

  Dans cet exemple, le signe plus (+) avant l'adresse du serveur NTP indique qu'il s'agit d'un candidat potentiel. Un astérisque ici, *, indique l'homologue de la source de temps actuelle.

  Le démon NTP (NTPD) utilise une fenêtre glissante de huit échantillons pour chacun des homologues et en sélectionne un, puis la sélection de l'horloge détermine les vraies sources et les fausses. NTPD détermine ensuite la distance aller-retour (le décalage d'un candidat ne doit pas dépasser la moitié du retard aller-retour). Si des retards de connexion, une perte de paquets ou des problèmes de serveur entraînent le rejet d'un ou de tous les candidats, vous verrez de longs retards dans la synchronisation. L'ajustement se produit également sur une très longue période : les erreurs de décalage d'horloge et d'oscillateur doivent être résolues par l'algorithme de correction d'horloge, ce qui peut prendre des heures.

Remarque Si le refid est .LOCL., cela indique que l'homologue est une horloge locale non asservie, c'est-à-dire qu'il utilise son horloge locale uniquement pour définir l'heure. Le FDM marque toujours la connexion NTP en jaune (non synchronisée) si l'homologue sélectionné est .LOCL. Normalement, le protocole NTP ne sélectionne pas un candidat .LOCL. si un meilleur est disponible, c'est pourquoi vous devez configurer au moins trois serveurs.

Dépannage du DNS pour l'interface de gestion

Vous devez configurer au moins un serveur DNS pour l'utilisation par l'interface de gestion. Le serveur est nécessaire pour les connexions en nuage aux services tels que les licences Smart, les mises à jour de bases de données (comme GeoDB, règles et VDB) et toute autre activité nécessitant une résolution du nom de domaine.

La configuration d'un serveur DNS est plutôt simple. Il suffit d'entrer les adresses IP des serveurs DNS que vous utilisez lors de la configuration initiale de l'appareil. Vous pourrez les modifier ultérieurement dans la page **Device (périphérique)** > **System Settings (paramètres système)** > **DNS Server (serveur DNS)**.

Cependant, le système peut ne pas résoudre les noms de domaine complets (FQDN) en raison de problèmes de connectivité réseau ou du serveur DNS lui-même. Si vous constatez que le système ne peut pas utiliser vos serveurs DNS, envisagez les actions suivantes pour cerner et résoudre le problème. Vous pouvez aussi consulter Dépannage des problèmes généraux de DNS.

Procédure

Étape 1 Déterminez si vous avez un problème.

a) Utilisez SSH pour vous connecter à l'interface de ligne de commande de l'appareil.

b) Entrez **ping system www.cisco.com**. Si vous obtenez un message « unknown host » (hôte inconnu) comme le suivant, le système ne pourra pas résoudre le nom de domaine. Si le message ping réussit, alors vous avez terminé : le DNS fonctionne. (Appuyez sur Ctrl + C pour arrêter le message ping.)

```
> ping system www.cisco.com
ping: unknown host www.cisco.com
```

Remarque
Il est essentiel d'inclure le mot-clé **system** dans la commande **ping**. Le mot-clé **system** envoie le message ping via l'adresse IP de gestion, qui est la seule interface qui utilise le serveur DNS de gestion. L'envoi d'un message ping www.cisco.com est également une bonne option, car vous avez besoin d'une voie de routage vers ce serveur pour les licences Smart et les mises à jour.

Étape 2 Vérifiez la configuration de l'interface de gestion.

a) Cliquez sur **Device (périphérique)** > **System Settings (paramètres système)** > **Management Interface (interface de gestion)**, puis vérifiez les points suivants. Si vous apportez des modifications, les modifications sont appliquées immédiatement lorsque vous cliquez sur **Save** (enregistrer). Si vous modifiez l'adresse de gestion, vous devrez vous reconnecter et ouvrir une nouvelle session.

- L'adresse IP de la passerelle est correcte pour le réseau de gestion. Si vous utilisez les interfaces de données comme passerelle, les étapes suivantes vérifieront cette configuration.
- Si vous n'utilisez pas les interfaces de données comme passerelle, vérifiez que l'adresse IP de gestion (ou le masque de sous-réseau) et l'adresse IP de la passerelle se trouvent sur le même sous-réseau.

b) Cliquez sur **Device (périphérique)** > **System Settings (paramètres système)** > **DNS Server (serveur DNS)** et vérifiez que les bons serveurs DNS sont configurés.

Si vous déployez le périphérique sur votre périphérie réseau, votre fournisseur de services peut avoir des exigences spécifiques concernant le serveur DNS que vous pouvez utiliser.

c) Si vous utilisez les interfaces de données comme passerelle, vérifiez que vous disposez des voies de routage requises.

Vous avez besoin d'une voie de routage par défaut pour 0.0.0.0. Vous pourriez avoir besoin de voies de routage supplémentaire si le serveur DNS n'est pas disponible par la passerelle pour le routage par défaut. Fondamentalement, il y a deux types de situations :

- Si vous utilisez DHCP pour obtenir une adresse pour l'interface extérieure, et que vous avez sélectionné l'option **Obtain Default Route using DHCP (obtenir la route par défaut à l'aide de DHCP)**, la route par défaut n'est pas visible dans le FDM. À partir de SSH, entrez **show route** et vérifiez qu'il existe une voie de routage pour 0.0.0.0. Puisque c'est la configuration par défaut pour l'interface

externe, il s'agit d'une situation probable. (allez à **Device (appareil)** > **Interfaces)** pour voir la configuration de l'interface extérieure.)

- Si vous utilisez une adresse IP statique sur l'interface externe ou si vous n'obtenez pas la voie de routage par défaut de DHCP, ouvrez **Device (périphérique)** > **Routing (routage)**. Vérifiez que la bonne passerelle est utilisée pour la voie de routage par défaut.

Si le serveur DNS ne peut pas être atteint par la voie de routage par défaut, vous devez définir une voie de routage statique vers celui-ci sur la page **Routing** (routage). Notez que vous ne devez pas ajouter de voies de routage pour les réseaux directement connectés, c.-à-d. Les réseaux qui sont connectés directement à l'une des interfaces de données du système, car le système peut assurer le routage vers ces réseaux automatiquement.

Vérifiez également qu'il n'y a aucune voie de routage statique qui dirige le trafic vers le serveur par la mauvaise interface.

d) Si le bouton de déploiement indique des modifications non déployées, déployez-les maintenant et attendez la fin du déploiement.

e) Effectuez un nouveau test sur **ping system www.cisco.com**. Si vous rencontrez toujours des problèmes, passez à l'étape suivante.

Étape 3 Dans la session SSH, entrez **dig www.cisco.com**.

- Si **dig** indique qu'il a obtenu une réponse du serveur DNS, mais que le serveur n'a pas pu trouver le nom, cela signifie que DNS est configuré correctement, mais que le serveur DNS que vous utilisez n'a pas d'adresse pour le nom de domaine complet. Cette erreur est indiquée par l'état de NXDOMAIN. La réponse ressemblerait à ceci :

```
> dig www.cisco.com

; <<>> DiG 9.11.4 <<>> www.cisco.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 43246
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
; COOKIE: 78b1c6b2b3ef5b689fc2f65260db9e9b36a7d9fefb301943 (good)
;; QUESTION SECTION:
;www.cisco.com.                 IN      A

;; AUTHORITY SECTION:
.                       3600    IN      SOA     a.root-servers.net.
nstld.verisign-grs.com. 2021062901 1800 900 604800 86400

;; Query time: 13 msec
;; SERVER: 10.163.47.11#53(10.163.47.11)
;; WHEN: Tue Jun 29 22:28:43 UTC 2021
;; MSG SIZE  rcvd: 145
```

Résolution : Dans ce cas, vous devez configurer un serveur DNS différent ou obtenir celui que vous avez mis à jour pour qu'il puisse résoudre les noms de domaine complets dont vous avez besoin. Collaborez avec votre administrateur réseau ou votre fournisseur de services Internet pour obtenir l'adresse IP d'un serveur DNS qui fonctionnera pour votre réseau.

- Si la commande échoue, c'est que le système ne peut pas atteindre vos serveurs DNS, ou que tous les serveurs DNS sont en panne et ne répondent pas (ce qui est moins probable). Passez à l'étape suivante.

Étape 4 Utilisez la commande **traceroute system** *DNS_server_ip_address* pour tracer la voie de routage vers le serveur DNS.

Par exemple, si le serveur DNS est 10.100.10.1, entrez :

```
> traceroute system 10.100.10.1
```

Voici les résultats possibles :

- L'opération traceroute s'achève en parvenant au serveur DNS. Dans ce cas, en fait, il y a une voie de routage vers le serveur DNS et le système peut l'atteindre. Ainsi, il n'y a aucun problème de routage. Cependant, pour une raison ou une autre, les demandes DNS vers ce serveur ne reçoivent pas de réponse.

  Résolution: il est possible qu'un routeur ou un pare-feu bloque le trafic UDP/53, qui est le port utilisé pour le DNS. Vous pouvez essayer un serveur DNS sur un chemin réseau différent. Il s'agit d'un problème difficile à résoudre, car vous devrez déterminer quel nœud bloque le trafic et travailler avec l'administrateur système pour modifier les règles d'accès.

- L'opération traceroute ne peut pas atteindre ne serait-ce qu'un seul nœud, ce qui ressemblerait à ceci :

  ```
  > traceroute system 10.100.10.1
  traceroute to 10.100.10.1 (10.100.10.1), 30 hops max, 60 byte packets
   1  * * *
   2  * * *
   3  * * *
  (and so forth)
  ```

  Résolution : dans ce cas, le problème de routage est au niveau du système. Essayez de faire un **ping system** pour l'adresse IP de la passerelle. Revérifiez la configuration de l'interface de gestion comme indiqué dans les étapes précédentes et assurez-vous que les passerelles et les voies de routage requises sont configurées.

- L'opération traceroute traverse quelques nœuds avant de parvenir à un point où elle ne peut plus résoudre la voie de routage, ce qui ressemblerait à ceci :

  ```
  > traceroute system 10.100.10.1
  traceroute to 10.100.10.1 (10.100.10.1), 30 hops max, 60 byte packets
   1  192.168.0.254 (192.168.0.254)  0.475 ms  0.532 ms  0.542 ms
   2  10.88.127.1 (10.88.127.1)  0.803 ms  1.434 ms  1.443 ms
   3  site04-lab-gw1.example.com (10.89.128.25)  1.390 ms  1.399 ms  1.435 ms
   4  * * *
   5  * * *
   6  * * *
  ```

  Résolution : Dans ce cas, le routage est interrompu au dernier nœud. Vous devrez peut-être travailler avec l'administrateur système pour obtenir l'installation des voies de routage correctes dans ce nœud. Cependant, s'il n'y a intentionnellement aucune voie de routage vers le serveur DNS par le biais du nœud, vous devez modifier votre passerelle ou créer votre propre voie de routage statique pour orienter le trafic vers un routeur qui peut l'acheminer jusqu'au serveur DNS.

Analyse de l'utilisation du processeur et de la mémoire

Pour afficher les informations au niveau du système concernant l'utilisation du processeur et de la mémoire, sélectionnez **Monitoring (Surveillance)** > **System (Système)** et recherchez les graphiques à barres du processeur et de la mémoire. Ces graphiques affichent les informations collectées par l'interface de ligne de commande à l'aide des commandes **show cpu system** et **show memory system**.

Si vous ouvrez la console d'interface de ligne de commande ou vous connectez à celle-ci, vous pouvez utiliser des versions supplémentaires de ces commandes pour afficher d'autres informations. En règle générale, vous ne consulterez ces renseignements que si vous avez des problèmes persistants d'utilisation ou sous la demande du centre d'assistance technique de Cisco (TAC). Une grande partie des renseignements détaillés sont complexes et nécessitent une explication par le TAC.

Voici quelques points saillants de ce que vous pouvez examiner. Vous pouvez trouver des informations plus détaillées sur ces commandes dans Référence de commande Cisco Firepower Threat Defense à l'adresse http://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense.html.

- **show cpu** affiche l'utilisation du processeur du plan de données.
- **show cpu core** affiche l'utilisation de chaque cœur de CPU séparément.
- **show cpu detailed** affiche l'utilisation supplémentaire de la CPU par cœur et globale du plan de données.
- **show memory** affiche l'utilisation de la mémoire du plan de données.

Remarque Certains mots-clés (non mentionnés ci-dessus) nécessitent que vous configuriez d'abord le profilage ou d'autres fonctionnalités à l'aide des commandes **cpu** ou **memory**. Utilisez ces fonctionnalités uniquement selon les directives du TAC.

Afficher les journaux des événements

Le système consigne les informations pour une grande variété d'actions. Vous pouvez utiliser la commande **system support view-files** pour ouvrir un journal système. Utilisez cette commande lorsque vous travaillez avec le centre d'assistance technique de Cisco (TAC) afin qu'il puisse vous aider à interpréter le résultat et pour sélectionner le journal approprié à afficher.

La commande présente un menu pour sélectionner un journal. Utilisez les commandes suivantes pour naviguer dans l'assistant :

- Pour passer à un sous-répertoire, saisissez le nom du répertoire et appuyez sur Enter (Entrée).
- Pour sélectionner un fichier à afficher, saisissez **s** à l'invite. Vous êtes invité à saisir un nom. Vous devez saisir le nom complet, en respectant la casse. La liste des fichiers vous indique la taille du journal, que vous pouvez prendre en compte avant d'ouvrir des journaux très volumineux.
- Appuyez sur la barre d'espace lorsque vous voyez --More (Plus)-- pour afficher la page suivante d'entrées de journal ; appuyez sur Enter (Entrée) pour n'afficher que l'entrée suivante. Lorsque vous atteignez la fin du journal, vous accédez au menu principal. La ligne --Plus-- vous affiche la taille du journal et la partie que vous avez affichée. **Utilisez les touches Ctrl + C pour fermer le journal et quitter la commande si vous ne souhaitez pas effectuer de page dans l'ensemble du journal.**

- Tapez **b** pour monter d'un niveau dans la structure jusqu'au menu.

Si vous souhaitez laisser le journal ouvert afin de pouvoir voir les nouveaux messages à mesure qu'ils sont ajoutés, utilisez la commande **tail-logs** au lieu de **system support view-files**.

L'exemple suivant montre comment afficher le fichier cisco/audit.log, qui suit les tentatives de connexion au système. La liste des fichiers commence par les répertoires en haut, puis une liste de fichiers dans le répertoire actuel.

```
> system support view-files

===View Logs===

============================
Directory: /ngfw/var/log
----------sub-dirs----------
cisco
mojo
removed_packages
setup
connector
sf
scripts
packages
removed_scripts
httpd
-----------files------------
2016-10-14 18:12:04.514783 | 5371       | SMART_STATUS_sda.log
2016-10-14 18:12:04.524783 | 353        | SMART_STATUS_sdb.log
2016-10-11 21:32:23.848733 | 326517     | action_queue.log
2016-10-06 16:00:56.620019 | 1018       | br1.down.log

<list abbreviated>


([b] to go back or [s] to select a file to view, [Ctrl+C] to exit)
Type a sub-dir name to list its contents: cisco

============================
Directory: /ngfw/var/log/cisco
-----------files------------
2017-02-13 22:44:42.394907 | 472        | audit.log
2017-02-13 23:40:30.858198 | 903615     | ev_stats.log.0
2017-02-09 18:14:26.870361 | 0          | ev_stats.log.0.lck
2017-02-13 05:24:00.682601 | 1024338    | ev_stats.log.1
2017-02-12 08:41:00.478103 | 1024338    | ev_stats.log.2
2017-02-11 11:58:00.260805 | 1024218    | ev_stats.log.3
2017-02-09 18:12:13.828607 | 95848      | firstboot.ngfw-onbox.log
2017-02-13 23:40:00.240359 | 6523160    | ngfw-onbox.log

([b] to go back or [s] to select a file to view, [Ctrl+C] to exit)
Type a sub-dir name to list its contents: s

Type the name of the file to view ([b] to go back, [Ctrl+C] to exit)
> audit.log
2017-02-09 18:59:26 - SubSystem:LOGIN, User:admin, IP:10.24.42.205, Message:Login successful,

2017-02-13 17:59:28 - SubSystem:LOGIN, User:admin, IP:10.24.111.72, Message:Login successful,

2017-02-13 22:44:36 - SubSystem:LOGIN, User:admin, IP:10.24.111.72, Message:Login failed,
2017-02-13 22:44:42 - SubSystem:LOGIN, User:admin, IP:10.24.111.72, Message:Login successful,
```

```
2017-02-13 22:44:42 - SubSystem:LOGIN, User:admin, IP:10.24.111.72, Message:Unlocked account.,

<remaining log truncated>
```

Création d'un fichier de dépannage

Le personnel du centre d'assistance technique de Cisco (TAC) peut vous demander de fournir des informations sur le journal du système lorsque vous soumettez un rapport de problème. Ces renseignements les aident à diagnostiquer le problème. Vous n'avez pas besoin d'envoyer de fichier de diagnostic, sauf si vous y êtes invité.

La procédure suivante explique comment créer et télécharger le fichier de diagnostic.

Procédure

Étape 1 Cliquez sur **Device (périphérique)**.

Étape 2 Sous **Troubleshooting** (Dépannage), cliquez sur **Request File to be Created** (Demander la création du fichier) ou **Re-Request File to be Created** (Redemander la création du fichier) (si vous en avez créé un auparavant).

Le système commence à générer le fichier de diagnostic. Vous pouvez accéder à d'autres pages et revenir ici pour vérifier l'état. Lorsque le fichier est prêt, la date et l'heure de la création du fichier s'affichent ainsi qu'un bouton de téléchargement.

Étape 3 Lorsque le fichier est prêt, cliquez sur le bouton de téléchargement.

Le fichier est téléchargé sur votre ordinateur à l'aide de la méthode de téléchargement standard de votre navigateur.

Tâches de gestion peu courantes

Les rubriques suivantes traitent d'actions que vous n'effectuerez pas souvent, si jamais. Toutes ces actions entraînent l'effacement de la configuration de votre appareil. Assurez-vous que le périphérique ne fournit pas actuellement de services essentiels à un réseau de production avant d'apporter ces modifications.

Modification du mode de pare-feu :

Le pare-feu FTD peut fonctionner en mode routé ou transparent. Un pare-feu en mode routé est un saut routé et agit comme une passerelle par défaut pour les hôtes qui se connectent à l'un de ses sous-réseaux filtrés. Un pare-feu transparent, en revanche, est un pare-feu de couche 2 qui agit comme une « présence sur le réseau câblé » ou un « pare-feu furtif », et qui n'est pas considéré comme un saut de routeur vers les appareils connectés.

Le FDM local prend en charge uniquement le mode routé. Si, toutefois, vous devez exécuter le périphérique en mode transparent, vous pouvez modifier le mode de pare-feu et commencer à gérer le périphérique avec le FMC. Inversement, vous pouvez convertir un périphérique en mode transparent en mode routé, puis vous

avez la possibilité de le configurer avec le gestionnaire local (vous pouvez également gérer les périphériques en mode routé à l'aide de FMC).

Indépendamment de la gestion locale ou à distance, vous devez utiliser l'interface de ligne de commande du périphérique pour modifier le mode.

La procédure suivante explique comment modifier le mode lors de l'utilisation du gestionnaire local ou lorsque vous prévoyez d'utiliser le gestionnaire local.

Mise en garde Le changement de mode de pare-feu efface la configuration du périphérique et ramène le système à la configuration par défaut. Cependant, l'adresse IP de gestion et le nom d'hôte sont conservés.

Avant de commencer

Si vous effectuez une conversion en mode transparent, installez FMC avant de modifier le mode de pare-feu.

Si vous avez activé des licences de fonctionnalités, vous devez les désactiver dans le FDM avant de supprimer le gestionnaire local et de passer à la gestion à distance. Sinon, ces licences restent attribuées au périphérique dans Cisco Smart Software Manager. Consultez Activation ou désactivation des licences facultatives.

Si le périphérique est configuré pour la haute disponibilité, vous devez d'abord rompre la configuration de haute disponibilité à l'aide du gestionnaire de périphériques (si possible) ou de la commande **configure high-availability disable**. Idéalement, interrompez la haute disponibilité à partir de l'unité active.

Procédure

Étape 1 Utilisez un client SSH pour ouvrir une connexion à **l'adresse IP de gestion** et vous connecter à l'interface de ligne de commande du périphérique avec un nom d'utilisateur qui dispose d'un accès à l'interface de ligne de commande de configuration. Par exemple, le nom d'utilisateur **admin**.

Il est important que vous suiviez ce processus lorsque vous êtes connecté à l'adresse IP de gestion. Lorsque vous utilisez FDM, vous avez la possibilité de gérer le périphérique au moyen de l'adresse IP d'une interface de données. Cependant, vous devez utiliser le port physique de gestion et l'adresse IP de gestion pour administrer le périphérique à distance.

Si vous ne pouvez pas vous connecter à l'adresse IP de gestion, adressez-vous aux points suivants :

- Vérifiez que le port physique de gestion est câblé à un réseau fonctionnel.
- Assurez-vous que l'adresse IP de gestion et la passerelle sont configurées pour le réseau de gestion. À partir de FDM, configurez l'adresse et la passerelle dans **Device (Périphérique)** > **System Settings (Paramètres du système)** > **Management Interface (Interface de gestion)**. (Dans l'interface de ligne de commande, utilisez la commande **configure network ipv4/ipv6 manual**.)

  Remarque
  Assurez-vous d'utiliser une passerelle externe pour l'adresse IP de gestion. Vous ne pouvez pas utiliser les interfaces de données comme passerelle lors de l'utilisation d'un gestionnaire distant.

Étape 2 Pour changer le mode de routé à transparent et utiliser la gestion à distance :

a) Désactivez la gestion locale et passez en mode sans gestionnaire.

Vous ne pouvez pas modifier le mode de pare-feu lorsqu'il y a un gestionnaire actif. Utilisez la commande **configure manager delete** pour supprimer le gestionnaire.

```
> configure manager delete
If you enabled any feature licenses, you must disable them in
Firepower Device Manager before deleting the local manager.
Otherwise, those licenses remain assigned to the device in
Cisco Smart Software Manager.
Do you want to continue[yes/no] yes
Deleting task list
Manager successfully deleted.

>
> show managers
No managers configured.
```

b) Changez le mode de pare-feu en mode transparent.

configure firewall transparent

Exemple :

```
> configure firewall transparent
This will destroy the current interface configurations,
are you sure that you want to proceed? [y/N] y
The firewall mode was changed successfully.
```

c) Configurez le gestionnaire à distance.

configure manager add {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE** } *regkey* [*nat_id*]

Lieu :

- {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} spécifie le nom d'hôte DNS ou l'adresse IP (IPv4 ou IPv6) du FMC qui gère ce périphérique. Si FMC n'est pas directement adressable, utilisez **DONTRESOLVE**. Si vous utilisez **DONTRESOLVE**, un *nat_id* est requis.
- *regkey* est la clé d'enregistrement alphanumérique unique nécessaire pour enregistrer un périphérique dans le FMC.
- *nat_id* est une chaîne alphanumérique facultative utilisée lors du processus d'enregistrement entre le FMC et le périphérique. Elle est requise si le nom d'hôte (hostname) est défini sur DONTRESOLVE.

Par exemple, pour utiliser le gestionnaire à l'adresse 192.168.0.123 avec la clé d'enregistrement **secret**, saisissez ce qui suit :

```
> configure manager add 192.168.0.123 secret
Manager successfully configured.
Please make note of reg_key as this will be required while adding
Device in FMC.

> show managers
Host                    : 192.168.0.123
Registration Key        : ****
Registration            : pending
RPC Status              :
```

d) Connectez-vous à FMC et ajoutez le périphérique.

Consultez l'aide en ligne de FMC pour connaître les étapes détaillées.

Étape 3 Pour changer le mode de transparent à routé et convertir à la gestion locale :

a) Annulez l'enregistrement du périphérique du FMC.

b) Accédez à l'interface de ligne de commande Cisco Firepower Threat Defense du périphérique, de préférence à partir du port de console.

Étant donné que la modification du mode efface votre configuration, l'adresse IP de gestion reviendra à sa valeur par défaut, de sorte que vous risquez de perdre une connexion SSH avec l'adresse IP de gestion après avoir changé de mode.

c) Modifiez le mode de pare-feu en mode routé.

configure firewall routed

Exemple :

```
> configure firewall routed
This will destroy the current interface configurations,
are you sure that you want to proceed? [y/N] y
The firewall mode was changed successfully.
```

d) Activez le gestionnaire local.

configure manager local

Par exemple :

```
> configure manager local
Deleting task list

> show managers
Managed locally.
```

Vous pouvez maintenant utiliser un navigateur Web pour ouvrir le gestionnaire local à l'adresse **https://***management-IP-address*.

Réinitialiser la configuration

Vous pouvez réinitialiser la configuration système aux valeurs d'usine par défaut si vous souhaitez recommencer. Bien que vous ne puissiez pas réinitialiser directement la configuration, la suppression et l'ajout du gestionnaire effacent la configuration.

Si votre intention est d'effacer la configuration puis de récupérer une sauvegarde, assurez-vous d'avoir déjà téléchargé la copie de sauvegarde que vous souhaitez restaurer. Vous devrez la charger après la réinitialisation du système pour pouvoir la restaurer.

Avant de commencer

Si vous avez activé des licences de fonctionnalités, vous devez les désactiver dans le FDM avant de supprimer le gestionnaire local. Sinon, ces licences restent attribuées au périphérique dans Cisco Smart Software Manager. Consultez Activation ou désactivation des licences facultatives.

Si l'appareil est configuré pour la haute disponibilité, vous devez d'abord interrompre la configuration à haute disponibilité à l'aide de FDM (si possible) ou de la commande **configure high-availability disable**. Idéalement, interrompez la haute disponibilité à partir de l'unité active.

Procédure

Étape 1 Utilisez un client SSH pour ouvrir une connexion à l'adresse IP de gestion et vous connecter à l'interface de ligne de commande du périphérique avec un nom d'utilisateur qui dispose d'un accès à l'interface de ligne de commande de configuration. Par exemple, le nom d'utilisateur **admin**.

Étape 2 Utilisez la commande **configure manager delete** pour supprimer le gestionnaire.

```
> configure manager delete
If you enabled any feature licenses, you must disable them in
Device Manager before deleting the local manager.
Otherwise, those licenses remain assigned to the device in Cisco
Smart Software Manager.
Do you want to continue[yes/no] yes
Deleting task list
Manager successfully deleted.

>
> show managers
No managers configured.
```

Étape 3 Configurez le gestionnaire local.

configure manager local

Par exemple :

```
> configure manager local
Deleting task list

> show managers
Managed locally.
```

Vous pouvez maintenant utiliser un navigateur Web pour ouvrir le gestionnaire local à l'adresse **https://***management-IP-address*. En effaçant la configuration, vous serez invité à terminer l'assistant de configuration du périphérique.

Échange à chaud d'un SSD sur Cisco Secure Firewall

Si vous avez deux disques SSD, ils forment un RAID lorsque vous démarrez. Vous pouvez effectuer les tâches suivantes au niveau de l'interface de ligne de commande FTD lorsque le pare-feu est sous tension :

- Échangez à chaud un des disques SSD : si un disque SSD est défectueux, vous pouvez le remplacer. Notez que si vous n'avez qu'un seul disque SSD, vous ne pouvez pas le retirer tant que le pare-feu est sous tension.
- Retirez un des disques SSD : si vous avez deux disques SSD, vous pouvez en retirer un.

- Ajouter un deuxième SSD : si vous avez un deuxième SSD, vous pouvez en ajouter un deuxième et former un RAID.

Mise en garde Ne retirez pas physiquement un SSD sans l'avoir supprimé du RAID en suivant cette procédure. Vous pourriez entraîner des pertes de données.

Procédure

Étape 1 Retirez l'un des disques SSD.

a) Retirez le SSD du RAID.

configure raid remove-secure local-disk {**1** | **2**}

Le mot-clé **remove-secure** supprime le SSD du RAID, désactive la fonction de disque à chiffrement automatique et effectue un effacement sécurisé du SSD. Si vous souhaitez uniquement retirer le SSD du RAID et conserver les données intègres, vous pouvez utiliser le mot-clé **remove**.

Exemple :

```
> configure raid remove-secure local-disk 2
```

b) Surveiller l'état RAID jusqu'à ce que SSD ne s'affiche plus dans l'inventaire.

show raid

Une fois le SSD retiré du RAID, l'**exploitabilité** et **l'état du lecteur** s'affichent comme **dégradés**. Le deuxième lecteur ne sera plus répertorié en tant que disque membre.

Exemple :

```
> show raid
Virtual Drive
ID:                     1
Size (MB):              858306
Operability:            operable
Presence:               equipped
Lifecycle:              available
Drive State:            optimal
Type:                   raid
Level:                  raid1
Max Disks:              2
Meta Version:           1.0
Array State:            active
Sync Action:            idle
Sync Completed:         unknown
Degraded:               0
Sync Speed:             none

RAID member Disk:
Device Name:            nvme0n1
Disk State:             in-sync
Disk Slot:              1
Read Errors:            0
Recovery Start:         none
```

```
Bad Blocks:
Unacknowledged Bad Blocks:

Device Name:                nvme1n1
Disk State:                 in-sync
Disk Slot:                  2
Read Errors:                0
Recovery Start:             none
Bad Blocks:
Unacknowledged Bad Blocks:

> show raid
Virtual Drive
ID:                         1
Size (MB):                  858306
Operability:                degraded
Presence:                   equipped
Lifecycle:                  available
Drive State:                degraded
Type:                       raid
Level:                      raid1
Max Disks:                  2
Meta Version:               1.0
Array State:                active
Sync Action:                idle
Sync Completed:             unknown
Degraded:                   1
Sync Speed:                 none

RAID member Disk:
Device Name:                nvme0n1
Disk State:                 in-sync
Disk Slot:                  1
Read Errors:                0
Recovery Start:             none
Bad Blocks:
Unacknowledged Bad Blocks:
```

c) Retirez physiquement le disque SSD du châssis.

Étape 2 Ajouter un disque SSD.

a) Ajoutez physiquement le SSD dans le logement vide.

b) Ajoutez le SSD au RAID.

configure raid add local-disk {**1** | **2**}

La synchronisation du nouveau SSD avec le RAID peut prendre plusieurs heures, pendant laquelle le pare-feu est complètement opérationnel. Vous pouvez même redémarrer et la synchronisation se poursuivra après la mise sous tension. Utilisez la commande **show raid** pour afficher l'état.

Si vous installez un disque SSD qui a été utilisé précédemment sur un autre système et qui est toujours verrouillé, saisissez la commande suivante :

configure raid add local-disk {**1** | **2**} *psid*

Le *psid* est imprimé sur l'étiquette fixée à l'arrière du disque SSD. Sinon, vous pouvez redémarrer le système et le SSD sera formaté et ajouté au RAID.

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.