Sauvegarde et restauration

À propos de la sauvegarde et de la restauration

La reprise après sinistre est un élément essentiel de tout plan de maintenance de système. Dans le cadre de votre plan de reprise après sinistre, nous vous recommandons d'effectuer des sauvegardes périodiques dans un emplacement distant sécurisé.

Sauvegardes à la demande

Vous pouvez effectuer des sauvegardes sur demande pour de plusieurs périphériques Cisco Secure Firewall Threat Defense dans CDO.

Pour en savoir plus, consultez Sauvegarder les périphériques gérés, à la page 7.

Sauvegardes planifiées

Vous pouvez utiliser le planificateur sur CDO pour automatiser les sauvegardes. Vous pouvez également planifier des sauvegardes de périphérique à distance à partir de CDO.

Le processus de configuration de CDO planifie des sauvegardes hebdomadaires de configuration uniquement, à stocker localement. Les sauvegardes ne remplacent pas les sauvegardes complètes hors site. Une fois la configuration initiale terminée, vous devez passer en revue vos tâches planifiées et les ajuster en fonction des besoins de votre organisation.

Pour en savoir plus, consultez Sauvegarder les périphériques gérés, à la page 7.

Stockage des fichiers de sauvegarde

Lorsque vous sauvegardez un appareil, Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) stocke les fichiers de sauvegarde dans son stockage sécurisé en nuage.

Pour en savoir plus, consultez Sauvegarder les périphériques gérés, à la page 7.

Périphériques restaurés gérés

Vous devez utiliser la CLI défense contre les menaces pour restaurer le périphérique défense contre les menaces .

Pour en savoir plus, consultez Restaurer les périphériques gérés par CDO, à la page 8.

Qu'est-ce qui est sauvegardé?

Les sauvegardes de périphérique sont toujours de configuration uniquement.

Qu'est-ce qui est restauré?

La restauration de configurations écrase *toutes* les configurations sauvegardées.

Assurez-vous de comprendre et de planifier les éléments suivants :

- Vous ne pouvez pas restaurer ce qui n'est pas sauvegardé.
- Le processus de restauration défense contre les menaces supprime les certificats VPN et toutes les configurations VPN des périphériques défense contre les menaces , y compris les certificats ajoutés après la sauvegarde. Après avoir restauré un périphérique défense contre les menaces , vous devez ajouter/réinscrire tous les certificats VPN et redéployer le périphérique.

Configuration requise pour la sauvegarde et la restauration

La sauvegarde et la restauration ont les exigences suivantes :

Exigences du modèle : sauvegarde

Vous pouvez sauvegarder :

- Périphériques autonomes Défense contre les menaces, instances natives, instances de conteneur, paires de haute disponibilité et grappes
- Défense contre les menaces virtuelles pour les périphériques VMware, qu'ils soient autonomes ou paires à haute disponibilité, et les grappes

La sauvegarde n'est *pas* prise en charge pour :

- Implémentations Défense contre les menaces virtuelles *autres que* VMware

Si vous devez remplacer un périphérique où la sauvegarde et la restauration ne sont pas prises en charge, vous devez recréer manuellement les configurations propres au périphérique.

Exigences du modèle : restaurer

Le périphérique géré de remplacement doit être du même modèle que celui que vous remplacez, avec le même nombre de modules de réseau et le même type et le même nombre d'interfaces physiques.

Exigence de la version

Comme première étape de toute sauvegarde, notez le niveau de correctif. Pour restaurer une sauvegarde, l'ancien et le nouvel appareil doivent exécuter la même version de pare-feu, y compris les correctifs.

Exigences de licence

Traiter les préoccupations relatives à l'octroi de licences ou aux droits dépendants comme décrit dans les pratiques et procédures exemplaires. Si vous remarquez des conflits de licences, communiquez avec le TAC de Cisco.

Directives et limites relatives à la sauvegarde et à la restauration

La sauvegarde et la restauration doivent respecter les directives et les limites suivantes.

Mise en garde Les utilisateurs avec un accès au niveau de l'interface de ligne de commande peuvent accéder à l'interface shell Linux avec la commande **expert**, ce qui peut présenter un risque pour la sécurité. Pour des raisons de sécurité du système, nous vous recommandons fortement :

- De n'utiliser l'interface Shell Linux que sous la supervision du centre d'assistance technique Cisco TAC ou lorsque la documentation de l'utilisateur du pare-feu et de CDO le demande explicitement.
- De restreindre la liste des utilisateurs avec accès à l'interpréteur de commandes shell Linux.
- De ne pas ajouter d'utilisateurs directement dans l'interface Shell Linux; d'utiliser uniquement les procédures décrites dans ce chapitre.

La sauvegarde et la restauration sont destinées à la reprise après sinistre ou à l'autorisation de retour de matériel

La sauvegarde et la restauration sont principalement destinées aux scénarios d'autorisation de retour de matériel (ARM). Avant de commencer le processus de restauration d'un appareil physique défectueux ou en panne, communiquez avec nous pour obtenir le matériel de remplacement.

La sauvegarde et la restauration ne consistent pas en une importation ou une exportation de configuration

Un fichier de sauvegarde contient des informations qui identifient de manière unique un périphérique et ne peuvent pas être partagées. N'utilisez pas le processus de sauvegarde et de restauration pour copier des configurations entre des périphériques ou des périphériques, ou comme moyen d'enregistrer des configurations tout en testant de nouvelles. Utilisez plutôt la fonction d'importation/exportation.

Par exemple, les sauvegardes de périphérique défense contre les menaces comprennent l'adresse IP de gestion du périphérique et toutes les informations dont le périphérique a besoin pour se connecter à son CDO de gestion. Ne restaurez pas de sauvegarde FTD sur un périphérique géré par un autre gestionnaire; Le périphérique restauré tente de se connecter au gestionnaire spécifié dans la sauvegarde.

La restauration est individuelle et locale

Vous restaurez les périphériques Threat Defense individuellement et localement. Cela signifie :

- Vous ne pouvez pas effectuer de restauration par lots sur des périphériques à haute disponibilité (HA). Les procédures de restauration décrites dans ce guide expliquent comment effectuer une restauration dans un environnement de haute disponibilité.

- Vous ne pouvez pas utiliser CDO pour restaurer un périphérique. Pour les périphériques défense contre les menaces , vous devez utiliser l'interface de ligne de commande défense contre les menaces , à l'exception de l'ISA 3000 zero-touch restore (restauration sans intervention), qui utilise une carte SD et le bouton de réinitialisation.
- Vous ne pouvez pas utiliser un compte d'utilisateur centre de gestion pour vous connecter et restaurer l'un de ses périphériques gérés. Les périphériques centre de gestion et défense contre les menaces possèdent leurs propres comptes utilisateur.

Bonnes pratiques pour la sauvegarde et la restauration

La sauvegarde et la restauration respectent les bonnes pratiques suivantes.

Quand effectuer la sauvegarde?

Nous vous recommandons d'effectuer la sauvegarde pendant une fenêtre de maintenance ou pendant toute autre période de faible utilisation.

Vous devez effectuer une sauvegarde dans les situations suivantes :

- Sauvegardes régulières .

  Dans le cadre de votre plan de reprise après sinistre, nous vous recommandons d'effectuer des sauvegardes périodiques.

- Avant la mise à niveau ou la recréation d'image.

  En cas d'échec majeur d'une mise à niveau, vous devrez peut-être effectuer une réinitialisation et une restauration. La recréation d'image rétablit la plupart des paramètres aux valeurs par défaut, y compris le mot de passe système. Si vous avez une sauvegarde récente, vous pouvez revenir aux opérations normales plus rapidement.

- Après la mise à niveau.

  Assurez-vous de sauvegarder le périphérique après la mise à niveau, afin d'avoir une sauvegarde de périphérique nouvellement mise à niveau.

Maintien de la sécurité du fichier de sauvegarde

Les fichiers de sauvegarde sont stockés en tant que fichiers d'archive non chiffrés (.tar); ils doivent être stockés dans un référentiel sécurisé.

Les clés privées dans les objets PKI, qui représentent les certificats de clé publique, et les paires de clés privées nécessaires à la prise en charge de votre déploiement sont déchiffrées avant d'être sauvegardées. Les clés sont rechiffrées avec une clé générée aléatoirement lorsque vous restaurez la sauvegarde.

Le fichier de sauvegarde doit être stocké en toute sécurité.

Sauvegarde et restauration dans les déploiements Défense contre les menaces à haute disponibilité

Dans un déploiement défense contre les menaces à haute disponibilité, vous devez :

- Sauvegarder la paire de périphériques à partir de Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), mais restaurer individuellement et localement à partir de la CLI défense contre les menaces .

Le processus de sauvegarde produit des fichiers de sauvegarde uniques pour les périphériques défense contre les menaces à haute disponibilité. Ne restaurez pas un homologue à haute disponibilité avec le fichier de sauvegarde d'un autre homologue. Un fichier de sauvegarde contient des informations qui identifient de manière unique un périphérique et ne peuvent pas être partagées.

Le rôle d'un périphérique défense contre les menaces à haute disponibilité est indiqué dans le nom de son fichier de sauvegarde. Lorsque vous effectuez une restauration, veillez à choisir le fichier de sauvegarde approprié : principal ou secondaire.

- Ne suspendez *pas* et n'interrompez pas la haute disponibilité avant d'effectuer la restauration.

  Le maintien de la configuration à haute disponibilité garantit que les périphériques de remplacement peuvent facilement se reconnecter après la restauration. Notez que vous devrez reprendre la synchronisation à haute disponibilité pour que cela se produise.

- N'exécutez *pas* la commande CLI de restauration sur les deux homologues en même temps.

  En supposant que vos sauvegardes soient réussies, vous pouvez remplacer l'un des homologues ou les deux dans une paire à haute disponibilité. Toutes les tâches de remplacement physique que vous pouvez effectuer simultanément : déploiement, changement de rack, etc. Cependant, n'exécutez *pas* la commande de restauration sur le deuxième périphérique tant que le processus de restauration n'est pas terminé pour le premier périphérique, y compris le redémarrage.

Sauvegarde et restauration dans les déploiements en grappe Défense contre les menaces

Dans le déploiement de la mise en grappe défense contre les menaces , vous devez :

- Sauvegardez l'ensemble de la grappe à partir de Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), mais restaurez les nœuds individuellement et localement à partir de l'interface de commande en ligne de Threat Defense.

  Le processus de sauvegarde produit un fichier tar qui comprend des fichiers de sauvegarde uniques pour chaque nœud de la grappe. Ne restaurez pas un nœud avec le fichier de sauvegarde d'un autre nœud. Un fichier de sauvegarde contient des informations qui identifient de manière unique un périphérique et ne peuvent pas être partagés.

  Le rôle du nœud est indiqué dans le nom de son fichier de sauvegarde. Lorsque vous effectuez une restauration, veillez à choisir le fichier de sauvegarde approprié : control ou data (contrôle ou données).

  Vous ne pouvez pas sauvegarder des nœuds individuels. Si un nœud de données ne parvient pas à la sauvegarde, le centre de gestion sauvegarde quand même tous les autres nœuds. Si le nœud de contrôle ne parvient pas à être sauvegardé, la sauvegarde est annulée.

- Tous les nœuds qui font partie de la grappe doivent être enregistrés dans le centre de gestion pour que la sauvegarde réussisse.

- Ne suspendez *pas* et n'interrompez pas la mise en grappe avant d'avoir effectué la restauration. Le maintien de la configuration de la grappe garantit que les périphériques de remplacement peuvent facilement se reconnecter après la restauration.

- N'exécutez *pas* la commande CLI **restore** sur plusieurs nœuds en même temps. Nous vous recommandons de restaurer d'abord le nœud de contrôle et d'espérer qu'il rejoigne la grappe avant de restaurer des nœuds de données.

  En supposant que vos sauvegardes soient réussies, vous pouvez remplacer plusieurs nœuds de la grappe. Toutes les tâches de remplacement physique que vous pouvez effectuer simultanément : le démontage,

le remplacement du bâti, etc. Cependant, n'exécutez *pas* la commande **restore** sur un nœud supplémentaire jusqu'à ce que le processus de restauration pour le nœud précédent soit terminé, y compris le redémarrage.

Avant la restauration

Avant la restauration, vous devez :

- Annuler les modifications de licence.

  Annulez les modifications de licence effectuées depuis que vous avez effectué la sauvegarde.

  Sinon, vous risquez d'avoir des conflits de licence ou des droits orphelins après la restauration. Cependant, ne vous désinscrivez *pas* de Cisco Smart Software Manager (CSSM). Si vous vous désinscrivez du CSSM, vous devez vous désinscrire à nouveau après la restauration, puis vous réinscrire.

  Une fois la restauration terminée, reconfigurez les licences. Si vous remarquez des conflits de licences ou des droits orphelins, communiquez avec le TAC de Cisco.

- Débranchez les périphériques défectueux.

  Déconnectez l'interface de gestion et pour les périphériques, les interfaces de données.

  La restauration d'un périphérique défense contre les menaces définit l'adresse IP de gestion du périphérique de remplacement selon l'adresse IP de gestion de l'ancien périphérique. Pour éviter les conflits d'adresses IP, déconnectez l'ancien périphérique du réseau de gestion avant de restaurer la sauvegarde sur le périphérique de remplacement.

- N'annulez *pas* l'enregistrement des périphériques gérés.

  Que vous restaurez un périphérique géré, ne désactivez pas l'enregistrement de périphériques auprès de CDO, même si vous déconnectez physiquement un appareil du réseau.

  Si vous vous désinscrivez, vous devez refaire certaines configurations de périphériques, telles que les mappages de zone de sécurité à interface. Après la restauration, CDO et les périphériques devraient commencer à communiquer normalement.

- Recréer l'image.

  Dans un scénario d'autorisation de retour de matériel, le périphérique de remplacement arrive configuré avec les paramètres d'usine par défaut. Toutefois, si le périphérique de remplacement est déjà configuré, nous vous recommandons d'effectuer une réinitialisation. La recréation d'image rétablit la plupart des paramètres aux valeurs par défaut, y compris le mot de passe système. Vous pouvez uniquement effectuer une réinitialisation vers les versions principales, vous devrez donc peut-être appliquer les correctifs après la réinitialisation.

  Si vous n'effectuez pas la réinitialisation, gardez à l'esprit que les incidents d'intrusion CDO et les listes de fichiers sont fusionnés au lieu d'être remplacés.

Après la restauration

Après la restauration, vous devez :

- Reconfigurer tout ce qui n'a pas été restauré.

  Cela peut inclure la reconfiguration des paramètres de licences, de stockage à distance et de certificat du serveur de journaux d'audit. Vous devez également rajouter/réinscrire les certificats VPN défense contre les menaces qui ont échoué.

- Déployez.

  Après avoir restauré un périphérique, procédez au déploiement sur celui-ci. Vous *devez* déployer. Si le ou les périphériques ne sont pas marqués comme obsolètes, forcez le déploiement à partir de la page Device Management (gestion des périphériques).

Sauvegarder les périphériques gérés

Vous pouvez effectuer des sauvegardes à la demande ou planifiées pour les périphériques Cisco Secure Firewall Threat Defense pris en charge en utilisant Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) sans profil de sauvegarde.

Pour en savoir plus, consultez Sauvegarder un périphérique Défense contre les menaces à partir de Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), à la page 7.

Renseignements connexes

Sauvegarder un périphérique Défense contre les menaces à partir de Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)

Utilisez cette procédure pour effectuer une sauvegarde à la demande de l'un des périphériques suivants :

- Défense contre les menaces : périphériques physiques, autonomes, à haute disponibilité ou en grappe
- Défense contre les menaces virtuelles : VMware, autonome, haute disponibilité ou en grappe

La sauvegarde et la restauration ne sont pas prises en charge pour d'autres plateformes ou configurations.

Avant de commencer

Vous devez lire et comprendre les exigences, les directives, les limites et les bonnes pratiques. Ne sautez aucune étape et ne négligez pas les problèmes de sécurité. Une planification et une préparation rigoureuses peuvent vous aider à éviter les erreurs.

- Configuration requise pour la sauvegarde et la restauration, à la page 2
- Directives et limites relatives à la sauvegarde et à la restauration, à la page 3
- Bonnes pratiques pour la sauvegarde et la restauration, à la page 4

⚠

Mise en garde Les utilisateurs avec un accès au niveau de l'interface de ligne de commande peuvent accéder à l'interface shell Linux avec la commande **expert**, ce qui peut présenter un risque pour la sécurité. Pour des raisons de sécurité du système, nous vous recommandons fortement :

- De n'utiliser l'interface Shell Linux que sous la supervision du centre d'assistance technique Cisco TAC ou lorsque la documentation de l'utilisateur du pare-feu et de CDO le demande explicitement.
- De restreindre la liste des utilisateurs avec accès à l'interpréteur de commandes shell Linux.
- De ne pas ajouter d'utilisateurs directement dans l'interface Shell Linux; d'utiliser uniquement les procédures décrites dans ce chapitre.

Procédure

Étape 1 Connectez-vous à CDO.

Étape 2 Dans le menu CDO, naviguez sur **Outils et services** > **Centre de gestion du pare-feu** pour ouvrir la page des **services**.

Étape 3 Sélectionnez **FMC en nuage** et dans le volet **Actions**, cliquez sur **Monitoring** (surveillance) pour accéder à l'interface utilisateur Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage).

Étape 4 Sélectionnez **Système** (⚙), puis naviguez dans les **Outils** > **sauvegarde/restauration**.

Étape 5 Cliquez sur **Sauvegarde des appareils gérés**

Étape 6 Sélectionnez un ou plusieurs périphériques défense contre les menaces dans **Périphériques gérés**.

Pour la mise en grappe, choisissez la grappe. Vous ne pouvez pas effectuer de sauvegardes sur des nœuds individuels.

Étape 7 Cliquez sur **Start Backup** (démarrer la sauvegarde) pour démarrer la sauvegarde à la demande.

Étape 8 Surveillez la progression sous **Tasks** (Tâches) dans le volet **Notifications**.

Restaurer les périphériques gérés par CDO

Pour les périphériques défense contre les menaces , vous devez utiliser la CLI défense contre les menaces pour restaurer à partir d'une sauvegarde. Vous ne pouvez pas utiliser centre de gestion pour restaurer un périphérique.

Renseignements connexes

Restaurer un périphérique Défense contre les menaces

La sauvegarde et la restauration Défense contre les menaces sont destinées aux automatisations de retour de matériel (ARM). La restauration des configurations remplace *toutes les* configurations du périphérique, y compris l'adresse IP de gestion. Elle redémarre également le périphérique.

En cas de défaillance matérielle, cette procédure décrit comment remplacer un périphérique pare-feu, qu'il soit autonome ou dans une paire à haute disponibilité. Cela suppose que vous ayez accès à une sauvegarde réussie du ou des périphériques que vous remplacez.

Dans un déploiement défense contre les menaces à haute disponibilité, vous pouvez utiliser cette procédure pour remplacer l'un des homologues ou les deux. Pour remplacer les deux, effectuez toutes les étapes sur les deux périphériques simultanément, à l'exception de la commande CLI de restauration elle-même. Vous ne pouvez pas remplacer un périphérique défense contre les menaces à haute disponibilité sans une sauvegarde réussie.

Remarque Ne vous désinscrivez *pas* du CDO, même lorsque vous déconnectez un périphérique du réseau. Dans un déploiement défense contre les menaces à haute disponibilité, ne suspendez *pas* ou n'interrompez pas la haute disponibilité. Le maintien de ces liaisons garantit que les périphériques de remplacement peuvent se reconnecter automatiquement après une restauration.

Avant de commencer

Vous devez lire et comprendre les exigences, les directives, les limites et les bonnes pratiques. Ne sautez aucune étape et ne négligez pas les problèmes de sécurité. Une planification et une préparation rigoureuses peuvent vous aider à éviter les erreurs.

- Configuration requise pour la sauvegarde et la restauration, à la page 2
- Directives et limites relatives à la sauvegarde et à la restauration, à la page 3
- Bonnes pratiques pour la sauvegarde et la restauration, à la page 4

Procédure

Étape 1 Communiquez avec Centre d'assistance technique Cisco (TAC) pour remplacer le matériel.

Obtenir un modèle identique, avec le même nombre de modules de réseau et le même type et le même nombre d'interfaces physiques. Vous pouvez commencer le processus d'autorisation de retour de matériel (ARM) à partir du Portail de retours Cisco.

Étape 2 Accédez à **System(⚙)** > **Tools (Outils)** > **Backup/Restore (Sauvegarde/Restauration)**.

Étape 3 Localisez une sauvegarde réussie du périphérique défectueux à partir de **Sauvegardes de périphériques** sous **Gestion des sauvegardes**.

Utilisez le **téléchargement** qui télécharge le ou les fichiers de sauvegarde dans votre stockage local ou **Exporte les liens de sauvegarde** qui génère une URL pour télécharger la sauvegarde et l'exporter vers un fichier CSV qui est téléchargé. Utilisez l'URL pour télécharger la sauvegarde dans un emplacement sécurisé. Notez que l'URL n'est valide que six heures, après quoi vous devez exporter à nouveau pour obtenir une autre URL.

Dans un déploiement défense contre les menaces à haute disponibilité, vous sauvegardez la paire en tant qu'unité, mais le processus de sauvegarde produit des fichiers de sauvegarde uniques pour chaque périphérique de la paire. Le rôle du périphérique est indiqué dans le nom du fichier de sauvegarde.

Si la seule copie de la sauvegarde se trouve sur le périphérique défectueux, copiez-la ailleurs maintenant. Si vous recréez l'image du périphérique, la sauvegarde sera effacée. Si quelque chose se passe mal, vous ne pourrez peut-être pas récupérer la sauvegarde.

Le périphérique de remplacement aura besoin de la sauvegarde, mais peut la récupérer avec la commande de copie sécurisée (SCP) pendant le processus de restauration. Nous vous recommandons de placer la sauvegarde dans un endroit accessible par SCP sur le périphérique de remplacement. Vous pouvez également copier la sauvegarde sur le périphérique de remplacement lui-même.

Étape 4 Retirez (retirez du châssis) le périphérique défectueux et déconnectez toutes les interfaces. Dans les déploiements à haute disponibilité Threat Defense, cela inclut la liaison de basculement.

Consultez les guides d'installation du matériel et de démarrage correspondant à votre modèle : Cisco Firepower NGFW :Guides d'installation et de mise à niveau.

Remarque Ne vous désinscrivez pas du centre de gestion, même lorsque vous déconnectez un périphérique du réseau. Dans les déploiements de haute disponibilité de défense contre les menaces, ne pas suspendre ou interrompre la haute disponibilité. Le maintien de ces liaisons garantit que les périphériques de remplacement peuvent se reconnecter automatiquement après la restauration.

Étape 5 Installez le périphérique de remplacement et connectez-le au réseau de gestion.

Connectez le périphérique à l'alimentation et l'interface de gestion au réseau de gestion. Dans les déploiements défense contre les menaces à haute disponibilité, connectez la liaison de basculement. Cependant, ne connectez *pas* les interfaces de données.

Consultez le guide d'installation du matériel correspondant à votre modèle : Cisco Firepower NGFW : Guides d'installation et de mise à niveau.

Étape 6 (Facultatif) Recréez l'image du périphérique de remplacement.

Dans un scénario d'autorisation de retour de matériel, le périphérique de remplacement arrivera configuré avec les paramètres d'usine. Si le périphérique de remplacement n'exécute pas la même version principale que le périphérique défectueux, nous vous recommandons d'effectuer une réinitialisation de l'image.

Consultez le Guide pour recréer l'image de Cisco Secure Firewall ASA et Cisco Threat Defense

Étape 7 Effectuez la configuration initiale sur le périphérique de remplacement.

Accédez à l'interface de ligne de commande défense contre les menaces en tant qu'utilisateur admin. Vous pouvez utiliser la console ou SSH pour récupérer l'adresse IP de l'interface de gestion par défaut (192.168.45.45). Un assistant d'installation vous invite à configurer l'adresse IP de gestion, la passerelle et d'autres paramètres réseau de base.

Consultez les rubriques de configuration initiale dans le guide de démarrage correspondant à votre modèle : Cisco Firepower NGFW : Guides d'installation et de mise à niveau.

Remarque Si vous devez appliquer le correctif sur le périphérique de remplacement, démarrez le processus d'enregistrement du centre de gestion comme décrit dans le guide de démarrage. Si vous n'avez *pas* besoin d'appliquer le correctif, ne l'enregistrez pas.

Étape 8 Vérifiez que le périphérique de remplacement exécute la même version du logiciel du pare-feu, correctifs compris, que le périphérique défectueux.

Le périphérique existant ne doit pas être supprimé du centre de gestion. Le périphérique de remplacement ne doit pas être géré par le réseau physique et le nouveau matériel ainsi que le correctif de remplacement défense contre les menaces doivent avoir la même version. L'interface de ligne de commande défense contre les menaces n'a pas de commande de mise à niveau. Pour appliquer un correctif :

a) À partir de l'interface Web du centre de gestion, terminez le processus d'enregistrement du périphérique : voir *Add a Device to Management Center (ajouter un périphérique au centre de gestion) dans le*Guide de configuration des périphériques de Cisco Secure Firewall Management Center.

   Créez une nouvelle politique d'autorité de certification et utilisez l'action par défaut de « découverte du réseau ». Laisser cette politique telle quelle; n'ajoutez aucune fonctionnalité ni modification. Ceci est utilisé pour enregistrer le périphérique et déployer une politique sans fonctionnalités, de sorte que vous n'avez pas besoin de licences. Vous pourrez alors appliquer un correctif au périphérique. Une fois la sauvegarde restaurée, les licences et la politique devraient être restaurées dans l'état attendu.

b) Appliquer les correctifs au périphérique : Guide de mise à niveau de Cisco Firewall Management Center.

c) Annulez l'enregistrement du périphérique nouvellement corrigé du centre de gestion : voir *Delete a Device from the Management Center* (Supprimer un périphérique du centre de gestion) dans le Guide de configuration des périphériques de Cisco Secure Firewall Management Center.

   Si vous n'annulez pas l'enregistrement, un périphérique virtuel sera enregistré auprès du centre de gestion après que le processus de restauration ait restauré votre « ancien » périphérique.

Étape 9 Assurez-vous que le périphérique de remplacement a accès au fichier de sauvegarde.

Le processus de restauration peut récupérer la sauvegarde avec le protocole SCP. Nous vous recommandons donc de la placer dans un endroit accessible. Vous pouvez également copier manuellement la sauvegarde sur le périphérique de remplacement, dans le répertoire `/var/sf/backup`.

Étape 10 À partir de l'interface de ligne de commande de FTD, restaurez la sauvegarde.

Accédez à l'interface de ligne de commande défense contre les menaces en tant qu'utilisateur admin. Vous pouvez utiliser la console ou accéder à SSH sur la nouvelle interface de gestion (adresse IP ou nom d'hôte). Gardez à l'esprit que le processus de restauration modifiera cette adresse IP.

Pour procéder à la restauration :

- Avec SCP : **restore remote-manager-backup location scp-hostname username filepath backup tar-file**
- À partir du périphérique local : **restore remote-manager-backup backup tar-file**

Étape 11 Connectez-vous à CDO et attendez que les périphériques se connectent.

Lorsque la restauration est terminée, le périphérique vous déconnecte de l'interface de ligne de commande, redémarre et se connecte automatiquement à CDO. À ce moment-là, l'appareil devrait sembler obsolète.

À ce moment-là, l'appareil devrait sembler obsolète.

Étape 12 Avant de procéder au déploiement, effectuez toutes les tâches après la restauration et résolvez les problèmes post-restauration :

- Résoudre les conflits de licences ou les droits parentaux. Communiquer avec le centre d'assistance technique Cisco (TAC).
- Reprendre la synchronisation
- Ajoutez de nouveau ou réinscrivez tous les certificats VPN. Le processus de restauration supprime les certificats VPN des périphériques FTD, y compris les certificats ajoutés après la sauvegarde.

Étape 13 Déployez des configurations.

Vous devez effectuer le déploiement. Si un périphérique restauré n'est pas marqué comme obsolète, forcez le déploiement à partir de la page Device Management (gestion des périphériques).

Étape 14 Connectez les interfaces de données du périphérique.

Consultez le guide d'installation du matériel correspondant à votre modèle : Cisco Secure Firewall Threat Defense : Guides d'installation et de mise à niveau.

Restaurer Défense contre les menaces à partir d'une sauvegarde Défense contre les menaces

Utilisez cette procédure pour remplacer un périphérique défense contre les menaces virtuelles défectueux ou en panne pour VMware.

Dans les déploiements de défense contre les menaces haute disponibilité et les déploiements en grappe, vous pouvez utiliser cette procédure pour remplacer tous les homologues. Pour tout remplacer, effectuez toutes les étapes sur tous les périphériques simultanément, à l'exception de la commande CLI **restore** (restaurer) elle-même.

Remarque Ne vous désinscrivez *pas* du centre de gestion, même lorsque vous déconnectez un périphérique du réseau. Dans les déploiements de défense contre les menaces haute disponibilité et les déploiements en grappe, ne *pas* suspendre ni interrompre la haute disponibilité en grappes. Le maintien de l'enregistrement garantit que les périphériques de remplacement peuvent se reconnecter automatiquement après la restauration.

Avant de commencer

Vous devez lire et comprendre les exigences, les directives, les limites et les bonnes pratiques. Ne sautez aucune étape et ne négligez pas les problèmes de sécurité. Une planification et une préparation rigoureuses peuvent vous aider à éviter les erreurs.

- Configuration requise pour la sauvegarde et la restauration, à la page 2
- Directives et limites relatives à la sauvegarde et à la restauration, à la page 3
- Bonnes pratiques pour la sauvegarde et la restauration, à la page 4

Procédure

Étape 1 Accédez à **System(⚙) > Tools (Outils) > Backup/Restore (Sauvegarde/Restauration)**.

Étape 2 Localisez une sauvegarde réussie du périphérique défectueux à partir de **Sauvegardes de périphériques** sous **Gestion des sauvegardes**.

Pour la mise en grappe, les fichiers de sauvegarde de nœud sont regroupés dans un seul fichier compressé pour la grappe (*cluster_name.timestamp***.tar.gz**). Avant de pouvoir restaurer des nœuds, vous devez extraire les fichiers de sauvegarde de nœud individuel (*node_name***_control_***timestamp***.tar** ou *node_name***_data_***timestamp***.tar**).

Utilisez le **téléchargement** qui télécharge le ou les fichiers de sauvegarde dans votre stockage local ou **Exporte les liens de sauvegarde** qui génère une URL pour télécharger la sauvegarde et l'exporter vers un fichier CSV qui est téléchargé. Utilisez l'URL pour télécharger la sauvegarde dans un emplacement sécurisé. Notez que l'URL n'est valide que six heures, après quoi vous devez exporter à nouveau pour obtenir une autre URL.

Dans les déploiements de défense contre les menaces haute disponibilité, vous sauvegardez la paire en tant qu'unité, mais le processus de sauvegarde produit des fichiers de sauvegarde uniques pour chaque périphérique de la paire. Le rôle du périphérique est indiqué dans le nom du fichier de sauvegarde.

Si la seule copie de la sauvegarde se trouve sur le périphérique défectueux, copiez-la ailleurs maintenant. Si vous recréez l'image du périphérique, la sauvegarde sera effacée. Si quelque chose se passe mal, vous ne pourrez peut-être pas récupérer la sauvegarde.

Le périphérique de remplacement a besoin de la sauvegarde, mais peut la récupérer avec le protocole SCP pendant le processus de restauration. Nous vous recommandons de placer la sauvegarde dans un endroit accessible par SCP sur le périphérique de remplacement. Vous pouvez également copier la sauvegarde sur le périphérique de remplacement lui-même.

Étape 3 Retirez le périphérique défectueux.

Arrêtez, mettez hors tension et supprimez la machine virtuelle. Pour connaître les procédures, consultez la documentation de votre environnement virtuel.

Étape 4 Déployer un périphérique de remplacement

Reportez-vous au Guide de démarrage (GD) de Cisco Firepower Threat Defense Virtual pour VMware

Étape 5 Effectuez la configuration initiale sur le périphérique de remplacement.

Utilisez la console VMware pour accéder à l'interface de ligne de commande défense contre les menaces virtuelles en tant qu'utilisateur admin. Un assistant d'installation vous invite à configurer l'adresse IP de gestion, la passerelle et d'autres paramètres réseau de base.

Ne définissez pas la même adresse IP de gestion que celle du périphérique défectueux. Cela peut provoquer des problèmes si vous devez enregistrer le périphérique pour lui appliquer un correctif. Le processus de restauration réinitialisera correctement l'adresse IP de gestion.

Voir les rubriques relatives à la configuration de l'interface de ligne de commande dans le : Guide de démarrage (GD) de Cisco Firepower Threat Defense Virtual pour VMware

Étape 6 Vérifiez que le périphérique de remplacement exécute la même version du logiciel du pare-feu, correctifs compris, que le périphérique défectueux.

Assurez-vous que le périphérique existant ne doit pas être supprimé du CDO. Le périphérique de remplacement ne doit pas être géré à partir du réseau physique, et le nouveau matériel ainsi que le correctif défense contre les menaces virtuelles de remplacement doivent avoir la même version. L'interface de ligne de commande défense contre les menaces virtuelles n'a pas de commande de mise à niveau. Pour appliquer un correctif :

1. Terminer le processus d'enregistrement de défense contre les menaces virtuelles dans CDO.
2. Appliquez les correctifs au périphérique défense contre les menaces virtuelles.
3. Annulez l'enregistrement du périphérique nouvellement appliqué de CDO.

Étape 7 Assurez-vous que le périphérique de remplacement a accès au fichier de sauvegarde.

Le processus de restauration peut récupérer la sauvegarde avec le protocole SCP. Nous vous recommandons donc de la placer dans un endroit accessible. Vous pouvez également copier manuellement la sauvegarde sur

le périphérique de remplacement, dans le répertoire `/var/sf/backup`. Pour les grappes, assurez-vous d'extraire le fichier de sauvegarde de nœud individuel du lot de la grappe principale.

Étape 8 À partir de la CLI défense contre les menaces , restaurez la sauvegarde.

Accédez à l'interface de ligne de commande défense contre les menaces virtuelles en tant qu'utilisateur admin. Vous pouvez utiliser la console ou accéder à SSH sur la nouvelle interface de gestion (adresse IP ou nom d'hôte). Gardez à l'esprit que le processus de restauration modifiera cette adresse IP.

Pour procéder à la restauration :

- Avec SCP : **restore remote-manager-backup location scp-hostname username filepath backup tar-file**
- À partir du périphérique local : **restore remote-manager-backup backup tar-file**

Dans les déploiements défense contre les menaces à haute disponibilité et les déploiements en grappe, assurez-vous de choisir le fichier de sauvegarde approprié : principal ou secondaire, ou contrôle ou données. Le rôle est indiqué dans le nom du fichier de sauvegarde. Si vous restaurez tous les périphériques, faites-le dans l'ordre. N'exécutez pas la commande de **restore** sur le périphérique suivant avant la fin du processus de restauration pour le premier périphérique, y compris le redémarrage.

Étape 9 Connectez-vous à CDO et attendez que les périphériques se connectent.

Lorsque la restauration est terminée, le périphérique vous déconnecte de l'interface de ligne de commande, redémarre et se connecte automatiquement à CDO. À ce moment-là, l'appareil devrait sembler obsolète.

À ce moment-là, l'appareil devrait sembler obsolète.

Étape 10 Avant de procéder au déploiement, effectuez toutes les tâches après la restauration et résolvez les problèmes post-restauration :

- Résoudre les conflits de licences ou les droits parentaux. Communiquer avec le centre d'assistance technique Cisco (TAC).
- Reprendre la synchronisation
- Ajoutez de nouveau ou réinscrivez tous les certificats VPN. Le processus de restauration supprime les certificats VPN des périphériques défense contre les menaces virtuelles, y compris les certificats ajoutés après la sauvegarde.

Étape 11 Déployez des configurations.

Vous devez effectuer le déploiement. Si un périphérique restauré n'est pas marqué comme obsolète, forcez le déploiement à partir de la page Device Management (gestion des périphériques).

Étape 12 Connectez les interfaces de données du périphérique.

Consultez le guide d'installation du matériel correspondant à votre modèle : Cisco Secure Firewall Threat Defense : Guides d'installation et de mise à niveau.

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.