Intégrer un FTD au Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)

Lisez les renseignements suivants pour connaître les conditions préalables et les procédures d'intégration.

Présentation de l'intégration

Passez en revue les scénarios d'utilisation suivants et les versions de logiciels prises en charge qui sont compatibles avec la gestion de Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage).

Périphériques Défense contre les menaces actuellement gérés par Géré par FDM

Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) prend actuellement en charge les scénarios de périphérique suivants pour l'intégration :

Vous pouvez uniquement intégrer un périphérique défense contre les menaces qui est géré par Géré par FDM.

- Les périphériques doivent exécuter la version 7.0.3 ou 7.2.0, ou une version ultérieure. Pour voir toutes les versions prises en charge et la compatibilité des produits, consultez le Guide de compatibilité Cisco Secure Firewall Threat Defense pour plus d'informations.
- Un périphérique configuré pour la gestion locale doit être géré par le gestionnaire d'appareil. L'appareil peut être connecté ou non avant l'intégration. Pour les périphériques qui ne sont pas connectés, vous pouvez intégrer le périphérique à l'aide du Préparation d'un appareil avec un provisionnement à faible intervention humaine.

Remarque Si vous intégrez un appareil Géré par FDM à Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), vous ne pouvez plus gérer le périphérique avec le gestionnaire d'appareil.

- Un périphérique géré par un centre de gestion de pare-feu local.

  Si vous avez déjà un périphérique défense contre les menaces géré par un centre de gestion de pare-feu local, vous pouvez le faire migrer pour la gestion dans le nuage. Consultez la section Migration de Cisco Secure Firewall Threat Defense vers le nuage pour en savoir plus.

Périphériques Défense contre les menaces actuellement gérés par Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)

Les scénarios suivants se produisent lorsque vous déplacez ou migrez un périphérique vers Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) :

- Si vous supprimez un périphérique d'un centre de gestion de pare-feu local ou gestionnaire d'appareil Cisco Secure Firewall Threat Defense pour l'intégrer à Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), le changement de gestionnaires efface toutes les politiques configurées à l'aide de centre de gestion de pare-feu local.
- Si vous **migrez** un périphérique d'un centre de gestion de pare-feu local vers Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), le périphérique conserve la majorité de vos politiques précédemment configurées.

Remarque Si vous ne savez pas si votre périphérique est déjà géré par un autre gestionnaire, utilisez la commande `show managers` dans la CLI du périphérique.

Méthodes d'intégration

Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) prend en charge les méthodes d'intégration suivantes :

- Intégrer un périphérique avec une clé d'enregistrement de ligne de commande : intégrer un périphérique avec une clé d'enregistrement. L'assistant de configuration initiale du périphérique est achevé sur le périphérique.
- Préparation d'un appareil avec un provisionnement à faible intervention humaine : intégrer un nouveau périphérique sortant d'usine lorsque l'assistant de configuration initiale du périphérique n'a **pas** été exécuté sur ce dernier. Notez que cette méthode prend uniquement en charge les périphériques Firepower 1000, Firepower 2100ou Secure Firewall 3100.

Remarque La version 7.0.3 ne prend pas en charge le provisionnement à faible intervention.

- Intégrer un périphérique avec un numéro de série (numéro de série) : intégrer un appareil qui a déjà été configuré initialement avec son numéro de série. Notez que cette méthode prend uniquement en charge les périphériques Firepower 1000, Firepower 2100ou Secure Firewall 3100.

Remarque La version 7.0.3 ne prend pas en charge l'intégration avec un numéro de série.

Conditions préalables à l'intégration d'un périphérique à Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)

Limites et exigences de l'intégration

Gardez à l'esprit les limites suivantes lors de l'intégration d'un périphérique sur Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) :

- Les périphériques **doivent** exécuter la version 7.0.3, ou la version 7.2, ou une version ultérieure. Nous vous recommandons **fortement** d'utiliser la version 7.2 ou une version ultérieure.
- Vous n'avez pas besoin d'un SDC local ou virtuel pour intégrer votre appareil.
- Vous pouvez migrer une paire à haute disponibilité gérée par un Centre de gestion de pare-feu local en suivant le processus Migration du FTD vers le Firewall Management Center en nuage. Confirmez que les deux homologues sont dans un état intègre avant la migration.
- Seuls les périphériques configurés pour la gestion locale et gérés par un gestionnaire d'appareil peuvent être intégrés avec le numéro de série et les méthodes de provisionnement à faible intervention.
- Si le périphérique est géré par un centre de gestion de pare-feu local, vous pouvez soit intégrer le périphérique à Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), soit le faire migrer. La migration conserve les politiques et les objets existants, tandis que l'intégration du périphérique supprime la plupart des politiques et tous les objets. Consultez la section Migration du FTD vers le Firewall Management Center en nuage pour de plus amples renseignements.
- Si votre appareil est actuellement géré par un gestionnaire d'appareil, désenregistrez toutes vos licences Smart avant d'intégrer le périphérique. Même si vous changez de gestion de périphériques, Cisco Smart Software Manager conserve les licences Smart.
- Si vous avez déjà intégré un appareil qui était géré par gestionnaire d'appareil et que vous avez supprimé le périphérique de CDO avec l'intention de le réintégrer pour la gestion dans le nuage, vous **devez** enregistrer gestionnaire d'appareil dans le nuage Security Services Exchange après avoir supprimé le périphérique. Reportez-vous au chapitre « Accès aux services de sécurité Exchange » du *Guide d'intégration de Firepower et Cisco SecureX Threat Response.*

Astuces L'intégration d'un périphérique à Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) supprime toutes les politiques et la plupart des objets configurés par le gestionnaire précédent. Si votre périphérique est actuellement géré par un centre de gestion de pare-feu local, il est possible de migrer le périphérique et de conserver vos politiques et vos objets. Consultez la section Migration du FTD vers le Firewall Management Center en nuage pour de plus amples renseignements.

Exigences en matière de réseau

Avant d'intégrer un périphérique, assurez-vous que les ports suivants ont un accès externe et sortant. Confirmez que les ports suivants du périphérique sont autorisés. Si les ports de communication sont bloqués derrière un pare-feu, l'intégration du périphérique peut échouer.

Remarque Vous ne pouvez pas configurer ces ports dans l'interface utilisateur CDO. Vous devez activer ces ports via le protocole SSH du périphérique.

Tableau 1 : Configuration de ports requise pour l'appareil

Port	Protocole/Fonctionnalité	Détails
443/tcp	HTTPS	Envoyez et recevez des données d'Internet
443	HTTPS	Communiquez avec le nuage AMP (public ou privé)
8305/tcp	Communications concernant les périphériques	Communiquez en toute sécurité entre les périphériques d'un déploiement

Interfaces de gestion et de données

Assurez-vous que votre périphérique est correctement configuré avec une interface de gestion ou de données.

Pour configurer une interface de gestion ou de données sur votre périphérique, consultez Terminer la configuration initiale d'un périphérique Cisco Secure Firewall Threat Defense à l'aide de l'interface de ligne de commande.

Intégrer un périphérique avec une clé d'enregistrement de ligne de commande

Utilisez la procédure ci-dessous pour intégrer un appareil à Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) avec une clé d'enregistrement d'interface de ligne de commande.

Remarque Si votre appareil est actuellement géré par un centre de gestion de pare-feu local, l'intégration du périphérique échouera. Vous pouvez soit supprimer le périphérique de centre de gestion de pare-feu local et l'intégrer en tant que nouveau périphérique sans politique ni objet, ou vous pouvez migrer le périphérique et conserver les politiques et les objets existants. Consultez la section Migration de FTD vers le centre de gestion de pare-feu en nuage pour de plus amples renseignements.

Important Vous pouvez créer un périphérique logique autonome défense contre les menaces géré par CDO à l'aide du gestionnaire de châssis Cisco Secure Firewall ou de l'interface de ligne de commande de FXOS.

Avant de commencer

Avant d'intégrer un appareil, assurez-vous d'effectuer les tâches suivantes :

- Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) est activé pour votre détenteur.
- Confirmez que la configuration de l'interface de ligne de commande du périphérique est terminée. Consultez Terminer la configuration initiale d'un périphérique Cisco Secure Firewall Threat Defense à l'aide de l'interface de ligne de commande pour obtenir de plus amples renseignements.
- Passez en revue les conditions préalables et les limites avant d'intégrer le périphérique. Consultez les Conditions préalables à l'intégration d'un périphérique dans Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) dans Gérer Cisco Firewall Threat Defense avec Cisco Cloud-Delivered Firewall Management Center dans Cisco Defense Orchestrator
- L'appareil peut être configuré pour la gestion locale avec Cisco Secure Firewall device manager ou pour la gestion à distance avec Cisco Secure Firewall Management Center.

Remarque Si vous souhaitez que le périphérique conserve la gestion à partir du Cisco Secure Firewall device manager, sélectionnez **FDM** et consultez Intégrer un périphérique Géré par FDM exécutant la version du logiciel 6.6+ à l'aide d'une clé d'enregistrement pour de plus amples renseignements.

- Le périphérique doit exécuter la version 7.0.3, ou 7.2.0, ou une version ultérieure.
- Vous avez réinitialisé le mot de passe SSH du périphérique dans le cadre du processus de démarrage. Si vous ne réinitialisez pas le mot de passe SSH, CDO recommande d'utiliser la méthode Préparation d'un appareil avec un provisionnement à faible intervention humaine, à la page 7

Procédure

Étape 1 Connectez-vous à CDO.

Étape 2 Dans le volet de navigation, cliquez sur **Inventory** (inventaire), puis sur le bouton bleu Plus.

Étape 3 Cliquez sur la fenêtre **FTD**.

Étape 4 Sous **Management Mode** (Mode de gestion), assurez-vous que **FTD** est sélectionné. En sélectionnant **FTD** sous **Management Mode**, vous ne pourrez pas gérer le périphérique à l'aide de la plateforme de gestion précédente. Toutes les configurations de politiques existantes, à l'exception des configurations d'interface, seront réinitialisées. Vous devez reconfigurer les politiques après avoir intégré le périphérique.

Remarque Si vous utilisez la licence d'évaluation de 90 jours, le nombre de jours restants est indiqué sous les options basculer **FTD** et **FDM**. Cliquez sur le lien **Manage Subscription License** (Gérer la licence d'abonnement) pour choisir une licence d'abonnement complet. Voir Types de licences pour périphériques gérés pour de plus amples renseignements.

Étape 5 Sélectionnez **Use CLI Registration Key (Utiliser la clé d'enregistrement de l'interface de ligne de commande)** comme méthode de préparation.

Étape 6 Saisissez un nom pour le périphérique dans le champ **Nom du périphérique** et cliquez sur **Suivant**.

Étape 7 À l'étape d'affectation de politique, utilisez le menu déroulant pour sélectionner une politique de contrôle d'accès à déployer une fois que le périphérique est intégré. Si vous n'avez pas configuré de politique, sélectionnez la **politique de contrôle d'accès par défaut**.

Étape 8 Précisez si le périphérique que vous intégrez est un périphérique physique ou virtuel. Si vous intégrez un appareil virtuel, vous devez sélectionner le niveau de performance du périphérique dans le menu déroulant.

Étape 9 Sélectionnez les licences d'abonnement que vous souhaitez appliquer au périphérique. Cliquez sur **Next** (suivant).

Étape 10 CDO génère une commande avec la clé d'enregistrement. Connectez-vous au périphérique que vous êtes en train d'intégrer à l'aide de SSH. Connectez-vous en tant qu'« admin » ou en tant qu'utilisateur doté de privilèges d'administrateur équivalents et collez la clé d'enregistrement complète telle quelle dans l'interface de ligne de commande du périphérique .

Remarque : Pour les périphériques Firepower 1000, Firepower 2100, ISA 3000 et défense contre les menaces virtuelles, ouvrez une connexion SSH avec le périphérique et connectez-vous en tant `qu'administrateur`. Copiez la commande d'enregistrement complète et collez-la dans l'interface CLI du périphérique à l'invite. Dans l'interface de ligne de commande, saisissez **Y** (Oui) pour terminer l'enregistrement. Si votre périphérique était auparavant géré par gestionnaire d'appareil, saisissez **Yes** (oui) pour confirmer la soumission.

Étape 11 Cliquez sur **Next** (suivant) dans l'assistant d'intégration CDO.

Étape 12 (Facultatif) Ajoutez des étiquettes à votre appareil pour trier et filtrer la page **d'inventaire**. Saisissez une étiquette et sélectionnez le bouton bleu Plus. Les étiquettes sont appliquées au périphérique après son intégration à CDO.

Prochaine étape

Une fois le périphérique synchronisé, sélectionnez le périphérique que vous venez d'intégrer dans la page **Inventaire** et sélectionnez l'une des options répertoriées dans le volet **Gestion des périphériques** situé à droite. Nous vous recommandons fortement d'effectuer les actions suivantes :

- Si vous ne l'avez pas encore fait, créez une politique de contrôle d'accès personnalisée pour adapter la sécurité à votre environnement. Consultez la présentation du contrôle d'accès dans le document *Gestion de Firewall Threat Defense avec CiscoFirewall Management Center en nuage dans Cisco Defense Orchestrator* pour obtenir de plus amples renseignements.
- Activez Cisco Security Analytics and Logging (SAL) pour afficher les événements dans le tableau de bord CDO **ou** enregistrez le périphérique sur un Cisco Secure Firewall Management Center pour des analyses de sécurité. Pour obtenir de plus amples renseignements sur Cisco Security Analytics and

Logging, consultez le guide *Gestion de Firewall Threat Defense avec Cisco Firewall Management Center en nuage dans Cisco Defense Orchestrator*.

Préparation d'un appareil avec un provisionnement à faible intervention humaine

Seuls les périphériques Firepower 1000, Firepower 2100 et Secure Firewall 3100 peuvent être intégrés avec la méthode de provisionnement à faible intervention.

Avant de commencer

Confirmez que les étapes suivantes ont été achevées avant l'intégration :

- Vous avez un détenteur CDO. Si ce n'est pas le cas, consultez Demander un détenteur CDO pour de plus amples renseignements.
- Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) est activé pour votre détenteur.
- Le périphérique vient d'être installé, mais n'a jamais été connecté par l'interface de ligne de commande du périphérique, centre de gestionou gestionnaire d'appareil.
- Le périphérique exécute la version 7.2 ou ultérieure. La version 7.0.3 ne prend **pas** en charge le provisionnement à faible intervention.

Procédure

Étape 1 Connectez-vous à CDO.

Étape 2 Dans le volet de navigation, cliquez sur **Inventory** (inventaire), puis sur le bouton bleu Plus.

Étape 3 Cliquez sur la fenêtre **FTD**.

Étape 4 Sous **Management Mode** (Mode de gestion), assurez-vous que **FTD** est sélectionné. En sélectionnant **FTD** sous **Management Mode**, vous ne pourrez pas gérer le périphérique à l'aide de la plateforme de gestion précédente. Toutes les configurations de politiques existantes, à l'exception des configurations d'interface, seront réinitialisées. Vous devez reconfigurer les politiques après avoir intégré le périphérique.

Remarque Si vous utilisez la licence d'évaluation de 90 jours, le nombre de jours restants est indiqué sous les options basculer **FTD** et **FDM**. Cliquez sur le lien **Manage Subscription License** (Gérer la licence d'abonnement) pour choisir une licence d'abonnement complet. Voir Types de licences pour périphériques gérés pour de plus amples renseignements.

Étape 5 Saisissez le **Device Serial Number** (Numéro de série du périphérique) et le **Device Name** (Nom du périphérique). Sélectionnez **Next** (suivant).

Étape 6 Réinitialisation du mot de passe Sélectionnez l'option **Oui, ce nouvel appareil n'a jamais été connecté ou configuré pour un gestionnaire**.

Si votre appareil a déjà été enregistré auprès d'un gestionnaire ou est **toujours** enregistré auprès d'un gestionnaire, consultez Intégrer un périphérique avec un numéro de série, à la page 8.

Étape 7 Cliquez sur **Next** (suivant).

Étape 8 À l'étape d'affectation de politique, utilisez le menu déroulant pour sélectionner une politique de contrôle d'accès à déployer une fois que le périphérique est intégré. Si vous n'avez pas configuré de politique, sélectionnez la **politique de contrôle d'accès par défaut**.

Étape 9 Sélectionnez les licences d'abonnement que vous souhaitez appliquer au périphérique. Cliquez sur **Next** (suivant).

Prochaine étape

Une fois le périphérique synchronisé, sélectionnez le périphérique que vous venez d'intégrer dans la page **Inventaire** et sélectionnez l'une des options répertoriées dans le volet **Gestion des périphériques** situé à droite. Nous vous recommandons fortement d'effectuer les actions suivantes :

- Si vous ne l'avez pas encore fait, créez une politique de contrôle d'accès personnalisée pour adapter la sécurité à votre environnement. Consultez la présentation du contrôle d'accès dans le document *Gestion de Firewall Threat Defense avec CiscoFirewall Management Center en nuage dans Cisco Defense Orchestrator* pour obtenir de plus amples renseignements.
- Activez Cisco Security Analytics and Logging (SAL) pour afficher les événements dans le tableau de bord CDO **ou** enregistrez le périphérique sur un Cisco Secure Firewall Management Center pour des analyses de sécurité. Pour obtenir de plus amples renseignements sur Cisco Security Analytics and Logging, consultez le guide *Gestion de Firewall Threat Defense avec Cisco Firewall Management Center en nuage dans Cisco Defense Orchestrator*.

Intégrer un périphérique avec un numéro de série

Seuls les périphériques Firepower 1000, Firepower 2100 et Secure Firewall 3100 peuvent être intégrés avec la méthode d'intégration par numéro de série.

Avant de commencer

Assurez-vous que les étapes suivantes sont effectuées avant l'intégration :

- Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) est activé pour votre détenteur.
- Confirmez que la configuration de l'interface de ligne de commande du périphérique est terminée. Consultez Terminer la configuration initiale d'un périphérique Cisco Secure Firewall Threat Defense à l'aide de l'interface de ligne de commande pour obtenir de plus amples renseignements.
- Passez en revue les conditions préalables et les limites avant d'intégrer le périphérique. Consultez les Conditions préalables à l'intégration d'un périphérique dans Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) dans Gérer Cisco Firewall Threat Defense avec Cisco Cloud-Delivered Firewall Management Center dans Cisco Defense Orchestrator
- Annulez l'enregistrement de toutes les licences Smart existantes que le périphérique a peut-être activées avant l'intégration.
- Vérifiez que le périphérique est configuré pour la gestion locale et qu'il est actuellement géré par Cisco Secure Firewall device manager.
- Le périphérique exécute les versions 7.2 ou ultérieures. La version 7.0.3 ne prend **pas** en charge l'intégration avec des numéros de série.

Procédure

Étape 1 Dans l'interface utilisateur Cisco Secure Firewall device manager, allez à **System Settings (paramètres systèmes)** > **Cloud Services (services en nuage Cisco)** et sélectionnez l'option **Auto-enroll with Tenancy from Cisco Defense Orchestrator** (inscription automatique avec localisation de détention à partir de Cisco Defense Orchestrator) et cliquez sur **Register** (Enregistrer).

Étape 2 Connectez-vous à CDO.

Étape 3 Dans le volet de navigation, cliquez sur **Inventory** (inventaire), puis sur le bouton bleu Plus.

Étape 4 Cliquez sur la fenêtre **FTD**.

Étape 5 Sous **Management Mode** (Mode de gestion), assurez-vous que **FTD** est sélectionné. En sélectionnant **FTD** sous **Management Mode**, vous ne pourrez pas gérer le périphérique à l'aide de la plateforme de gestion précédente. Toutes les configurations de politiques existantes, à l'exception des configurations d'interface, seront réinitialisées. Vous devez reconfigurer les politiques après avoir intégré le périphérique.

Remarque Si vous utilisez la licence d'évaluation de 90 jours, le nombre de jours restants est indiqué sous les options basculer **FTD** et **FDM**. Cliquez sur le lien **Manage Subscription License** (Gérer la licence d'abonnement) pour choisir une licence d'abonnement complet. Voir Types de licences pour périphériques gérés pour de plus amples renseignements.

Étape 6 Sélectionnez **Use Serial Number** (Utiliser le numéro de série).

Étape 7 Saisissez le **Device Serial Number** (Numéro de série du périphérique) et le **Device Name** (Nom du périphérique). Cliquez sur **Next** (suivant).

Étape 8 Réinitialisation du mot de passe Sélectionnez **No, this device has been logged into and configured for a manager** (Non, ce périphérique a été connecté et configuré pour un gestionnaire.). Cela signifie que le périphérique a déjà été enregistré sur un gestionnaire d'appareil et que le mot de passe par défaut a été modifié dans le cadre de cette configuration.

Si votre appareil est neuf et n'a jamais été configuré pour un gestionnaire, consultez Préparation d'un appareil avec un provisionnement à faible intervention humaine, à la page 7.

Étape 9 Cliquez sur **Next** (suivant).

Étape 10 À l'étape d'affectation de politique, utilisez le menu déroulant pour sélectionner une politique de contrôle d'accès à déployer une fois que le périphérique est intégré. Si vous n'avez pas configuré de politique, sélectionnez la **politique de contrôle d'accès par défaut**.

Étape 11 Sélectionnez les licences d'abonnement que vous souhaitez appliquer au périphérique. Cliquez sur **Next** (suivant).

Prochaine étape

Une fois le périphérique synchronisé, sélectionnez le périphérique que vous venez d'intégrer dans la page **Inventaire** et sélectionnez l'une des options répertoriées dans le volet **Gestion des périphériques** situé à droite. Nous vous recommandons fortement d'effectuer les actions suivantes :

- Si vous ne l'avez pas encore fait, créez une politique de contrôle d'accès personnalisée pour adapter la sécurité à votre environnement. Consultez la présentation du contrôle d'accès dans le document *Gestion de Firewall Threat Defense avec CiscoFirewall Management Center en nuage dans Cisco Defense Orchestrator* pour obtenir de plus amples renseignements.

- Activez Cisco Security Analytics and Logging (SAL) pour afficher les événements dans le tableau de bord CDO **ou** enregistrez le périphérique sur un Cisco Secure Firewall Management Center pour des analyses de sécurité. Pour obtenir de plus amples renseignements sur Cisco Security Analytics and Logging, consultez le guide *Gestion de Firewall Threat Defense avec Cisco Firewall Management Center en nuage dans Cisco Defense Orchestrator*.

Déployer un périphérique Threat Defense avec AWS

Utilisez la procédure suivante pour intégrer et provisionner provisoirement le pare-feu d'un périphérique défense contre les menaces qui est associé à un VPC AWS qui doit être géré par Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage).

Avant de commencer

Confirmez que les conditions préalables suivantes sont remplies avant de générer un défense contre les menaces virtuel et de le déployer dans un environnement AWS :

- La fonctionnalité Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) doit être activée et associée à votre client hébergé.
- Un VPC AWS doit déjà être intégré pour CDO. Pour en savoir plus, consultez Intégrer un VPC AWS.

Procédure

Étape 1 Connectez-vous à CDO.

Étape 2 Dans le volet de navigation, cliquez sur **Inventory** (inventaire), puis sur le bouton bleu Plus.

Étape 3 Sélectionnez la vignette **FTD**.

Étape 4 Sous **Management Mode** (Mode de gestion), assurez-vous que **FTD** est sélectionné.

Étape 5 Sélectionnez **Utiliser AWS VPC** comme méthode de préparation. Si aucun VPC AWS n'est déjà intégré, vous pouvez cliquer sur le lien fourni à partir de cette étape et intégrer l'environnement virtuel.

Étape 6 Sélectionnez la **zone de disponibilité** dans le menu déroulant. Sélectionnez la zone où se trouve le nuage défense contre les menaces , et non l'endroit où se trouve votre ordinateur local.

Étape 7 Sélectionnez le sous-réseau de l'interface de gestion avec l'une des options suivantes :

- **Utiliser les sous-réseaux existants** : développez les menus déroulants et sélectionnez les sous-réseaux appropriés pour les sous-réseaux de l'interface de gestion, de l'interface interne et de l'interface externe.
- **Créer de nouveaux sous-réseaux** : Ajoutez un ensemble d'interfaces de sous-réseau que le périphérique utilisera une fois intégré. Cisco Defense Orchestrator crée automatiquement ces sous-réseaux et les applique au VPC AWS dans le cadre de la procédure d'intégration.

Notez que l'interface de dépistage utilisera la même interface que l'interface de gestion.

Étape 8 Cliquez sur **Select** (Sélectionner) pour affecter les sous-réseaux. Cliquez sur **Next** (suivant).

Étape 9 Saisissez un nom pour le périphérique dans le champ **Nom du périphérique** et cliquez sur **Suivant**.

Étape 10 À l'étape d'affectation de politique, utilisez le menu déroulant pour sélectionner une politique de contrôle d'accès à déployer une fois que le périphérique est intégré. Si vous n'avez pas configuré de politique, sélectionnez la **politique de contrôle d'accès par défaut**.

Étape 11 Sélectionnez les **licences d'abonnement** que vous souhaitez appliquer au périphérique. Vous devez avoir au moins la licence URL sélectionnée pour les périphériques défense contre les menaces virtuels.

Prochaine étape

Il peut s'écouler quelques minutes avant que le périphérique n'apparaisse dans la page d**Inventaire** de CDO, car il ne peut pas se synchroniser tant que CDO n'a pas déployé avec succès la formation du nuage, initialisé les connexions du périphérique et établi la communication avec le périphérique virtuel et l'environnement du VPC AWS .

Si nécessaire, vous pouvez modifier la sélection du niveau de performance du périphérique virtuel défense contre les menaces après l'intégration à l'aide de l'interface utilisateur Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage).

Déployer un périphérique Défense contre les menaces avec un réseau virtuel Azure

Il s'agit d'un processus en deux parties qui comprend l'intégration d'un compte de réseau virtuel Azure à CDO, ainsi que la génération d'un défense contre les menaces virtuel et son déploiement sur votre réseau virtuel Azure. Lisez attentivement les conditions préalables et les procédures suivantes.

Intégrer un environnement de réseau virtuel Azure

Utilisez la procédure suivante pour intégrer un réseau virtuel Azure pour la gestion Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) :

Avant de commencer

Vous devez avoir effectué les éléments suivants avant cette procédure d'intégration :

- Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) est activé pour votre détenteur.
- Vous devez avoir au moins un groupe de ressources disponible dans votre compte Azure avec une instance de réseau virtuel Azure vide. Si vous n'avez pas de groupe de ressources pour héberger le périphérique virtuel, créez-en un avec le portail Azure. Consultez **Gérer les groupes de ressources Azure à l'aide du guide du portail Azure** de Microsoft Azure pour en savoir plus.
- Votre groupe de ressources dans le portail Azure doit avoir un réseau virtuel créé pour le périphérique virtuel. Si vous n'en avez pas, créez-en un dans le portail Azure. Consultez le guide de démarrage rapide du portail Azure sur le guide de démarrage rapide **Création d'un réseau virtuel à l'aide du portail Azure** de Microsoft Azure pour en savoir plus.
- Vous **devez** enregistrer Cisco Defense Orchestrator dans votre compte Microsoft pour assurer le succès de la communication entre Azure et CDO. Consultez la section « Démarrage rapide : enregistrer une application auprès de la plateforme d'identité de Microsoft » de la documentation du produit Azure pour en savoir plus.
- Vous **devez** attribuer un rôle intégré, ou créer un rôle personnalisé, dans l'environnement Azure et lui attribuer un membre ou un groupe qui accédera à Azure et CDO. Consultez la section « Rôle personnalisé Azure » ou la section « Rôles personnalisés Azure » de la documentation du produit Azure pour en savoir plus.

- Vous **devez** activer toutes les autorisations suivantes dans l'environnement Azure pour communiquer avec CDO et l'intégrer avec succès :

```
"Microsoft.Network/virtualNetworks/write"
« Microsoft.Network/virtualNetworks/join/action »
« Microsoft.Network/virtualNetworks/Subnets/read »
« Microsoft.Network/virtualNetworks/Subnets/write »
« Microsoft.Network/virtualNetworks/Subnets/prepareNetworkPlicies/action »
« Microsoft.Network/networkSecurityGroups/read »
« Microsoft.Network/networkSecurityGroups/write »
« Microsoft.Network/networkSecurityGroups/join/action »
« Microsoft.Network/networkSecurityGroups/securityRules/write »
« Microsoft.Network/networkSecurityGroups/securityRules/read »
« Microsoft.Network/networkSecurityGroups/securityRules/delete »
« Microsoft.Storage/storageAccounts/write »
« Microsoft.Storage/storageAccounts/read »
« Microsoft.Resources/deployments/write »
« Microsoft.Resources/deployments/read »
« Microsoft.Network/publicIPAddresses/read »
« Microsoft.Network/publicIPAddresses/write »
« Microsoft.Network/routeTables/read »
« Microsoft.Network/routeTables/write »
« Microsoft.Network/networkInterfaces/read »
« Microsoft.Network/networkInterfaces/write »
« Microsoft.Compute/virtualMachines/write »
« Microsoft.Resources/deployments/operationstatuses/read »
« Microsoft.Resources/Subscriptions/resourcegroups/deployments/operationstatuses/read »
« Microsoft.Network/routeTables/join/action »
« Microsoft.Network/virtualNetworks/Subnets/join/action »
« Microsoft.Network/publicIPAddresses/join/action »
« Microsoft.Network/networkInterfaces/join/action »
« Microsoft.Compute/virtualMachines/read »
« Microsoft.Resources/Subscriptions/resourceGroups/write »
« Microsoft.Resources/Subscriptions/resourceGroups/delete »
```

Procédure

Étape 1 Passez en revue les conditions préalables indiquées ci-dessus. Vous devez enregistrer CDO sur votre compte Microsoft, créer un rôle d'utilisateur et activer toutes les autorisations applicables avant d'intégrer un environnement virtuel.

Étape 2 Connectez-vous à CDO.

Étape 3 Dans le volet de navigation, cliquez sur **Inventory** (inventaire), puis sur le bouton bleu Plus.

Étape 4 Sélectionnez la vignette de **réseau virtuel Azure**.

Étape 5 Saisissez les informations d'authentification suivantes pour continuer avec l'assistant d'intégration, puis cliquez sur **Next**(suivant) :

- **Identifiant du détenteur Azure (ID d'annuaire)** : un ID d'annuaire est un identifiant unique pour le détenteur dans le monde des services en nuage de Microsoft. Il n'y a qu'un seul ID d'annuaire par détenteur. Pour le trouver, connectez-vous au portail Azure, accédez à **Azure Services** > **Azure Active Directory** et localisez l'ID du détenteur indiqué sur cette page.

- **ID de client (ID d'application)** : Un ID d'application est un identifiant unique attribué à CDO par Azure AD lors de l'enregistrement de l'application. Pour le trouver, connectez-vous au portail Azure, accédez à **Services Azure** > **Azure Active Directory** > **Inscriptions d'applications**, et affichez l'ID de l'application dans la liste des applications. S'il n'y a pas d'ID d'application pour CDO, cliquez sur **New Registrations** (Nouvelles inscriptions) pour en créer un pour cette procédure d'intégration.
- **Secret client** : vous devez demander manuellement une clé secrète client, bien que le portail Azure génère automatiquement une chaîne unique pour protéger votre détenteur. Pour la trouver, connectez-vous au portail Azure, accédez à **Services Azure** > **Azure Active Directory** > **Inscriptions d'applications**, puis développez l'application pour CDO. Dans le panneau de gauche, cliquez sur **Certificates et clés secrètes**. S'il n'y a pas de clé secrète, cliquez sur **New client secret** pour en créer une. Copiez la rubrique **Valeur** de cette procédure d'intégration, et non la rubrique ID de la clé secrète.
- **ID d'abonnement** : un abonnement est un contrat basé sur l'utilisation des services infonuagiques de Microsoft. dans ce cas, Azure VNet. L'ID d'abonnement est le code unique associé entre le détenteur et ce service en nuage particulier. Pour le trouver, connectez-vous au portail Azure et accédez à **Services Azure** > **Abonnements**. Si aucun abonnement n'est disponible pour CDO, cliquez sur **Add** (ajouter) pour en créer un.

Étape 6 Dans l'assistant d'intégration CDO, utilisez le menu déroulant pour sélectionner le **réseau virtuel Azure** que vous souhaitez intégrer.

Étape 7 Saisissez le **Device Name** (nom du périphérique), puis cliquez sur **Next** (suivant). Ce nom de périphérique est le nom sous lequel le réseau virtuel Azure s'affiche dans la page Inventory (inventaire).

Étape 8 (Facultatif) Ajoutez des étiquettes à votre appareil pour trier et filtrer la page **d'inventaire**. Saisissez une étiquette et sélectionnez le bouton bleu Plus. Les étiquettes sont appliquées au périphérique après son intégration à CDO.

Prochaine étape

Intégrer un périphérique virtuel dans CDO avec cette instance de réseau virtuel Azure comme gestionnaire. Consultez la Intégrer un appareil Défense contre les menaces virtuelles au réseau virtuel Azure, à la page 13 pour de plus amples renseignements.

Intégrer un appareil Défense contre les menaces virtuelles au réseau virtuel Azure

Utilisez cette procédure pour provisionner et intégrer un défense contre les menaces virtuelles pour le réseau virtuel Azure géré par Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage).

L'environnement de réseau virtuel Azure ne peut prendre en charge qu'un défense contre les menaces virtuelles. Si vous avez l'intention d'intégrer plusieurs périphériques, vous devez avoir un réseau virtuel Azure distinct pour chacun de ces périphériques.

Avant de commencer

Vous devez avoir une instance de réseau virtuel Azure déjà intégrée pour CDO. Consultez Intégrer un environnement de réseau virtuel Azure , à la page 11 pour obtenir de plus amples renseignements.

Procédure

Étape 1 Connectez-vous à CDO.

Étape 2 Dans le volet de navigation, cliquez sur **Inventory** (inventaire), puis sur le bouton bleu Plus.

Étape 3 Cliquez sur la fenêtre **FTD**.

Étape 4 Sous **Management Mode** (Mode de gestion), assurez-vous que **FTD** est sélectionné.

Attention En sélectionnant **FTD** sous **Mode de gestion**, le périphérique sera reconfiguré pour utiliser Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) comme gestionnaire.

Étape 5 Cliquez sur **Deploy an FTD to a Cloud environment** (déploiement d'un FTD dans un environnement en nuage) comme méthode d'intégration.

Étape 6 (Facultatif) Si vous n'avez pas encore enregistré votre compte CDO dans un abonnement Azure, vous pouvez le faire maintenant. Cliquez sur le lien hypertexte pour lancer Azure Cloud Shell et collez le script fourni. Si vous avez déjà enregistré votre compte ou si vous venez de terminer l'exécution du script, cliquez sur **Next** (Suivant).

Étape 7 Utilisez le menu déroulant pour sélectionner le réseau virtuel Azure que vous avez précédemment intégré et cliquez sur **Next** (Suivant).

Étape 8 Confirmez les valeurs de sous-réseau suivantes pour le pare-feu. Vous pouvez également modifier manuellement les valeurs si des valeurs valides ne sont pas générées automatiquement. Cliquez sur **Next** (suivant).

- CIDR de sous-réseau de gestion
- CIDR de sous-réseau de dépistage
- CIDR de sous-réseau GigabitEthernet 0/0
- CIDR de sous-réseau GigabitEthernet 0/1

Étape 9 Saisissez un **Device Name** (Nom de périphérique). Ce nom est appliqué à défense contre les menaces virtuelles dans la page Inventory (Inventaire) et non à l'instance de réseau virtuel Azure.

Étape 10 À l'étape d'affectation de politique, utilisez le menu déroulant pour sélectionner une politique de contrôle d'accès à déployer une fois que le périphérique est intégré. Si vous n'avez pas configuré de politique, sélectionnez la **politique de contrôle d'accès par défaut**.

Étape 11 Sélectionnez les licences que vous souhaitez appliquer au périphérique. Vous **devez** sélectionner au moins essentiel comme licence de base pour ce périphérique. Cliquez sur **Next** (suivant).

Étape 12 Cliquez sur **Complete onboarding** (Terminer l'intégration). Cette dernière étape met fin à l'assistant d'intégration. L'intégration et la synchronisation complètes du périphérique peuvent prendre jusqu'à 20 minutes. Pour surveiller le processus de création, développez l'option de **flux de travail** du réseau virtuel Azure qui héberge le périphérique.

Prochaine étape

Une fois le périphérique synchronisé, sélectionnez le périphérique que vous venez d'intégrer dans la page **Inventaire** et sélectionnez l'une des options répertoriées dans le volet **Gestion des périphériques** situé à droite. Nous vous recommandons fortement d'effectuer les actions suivantes :

- Si vous ne l'avez pas encore fait, créez une politique de contrôle d'accès personnalisée pour adapter la sécurité à votre environnement. Consultez la présentation du contrôle d'accès dans le document *Gestion de Firewall Threat Defense avec CiscoFirewall Management Center en nuage dans Cisco Defense Orchestrator* pour obtenir de plus amples renseignements.

- Activez Cisco Security Analytics and Logging (SAL) pour afficher les événements dans le tableau de bord CDO **ou** enregistrez le périphérique sur un Cisco Secure Firewall Management Center pour des analyses de sécurité. Pour obtenir de plus amples renseignements sur Cisco Security Analytics and Logging, consultez le guide *Gestion de Firewall Threat Defense avec Cisco Firewall Management Center en nuage dans Cisco Defense Orchestrator*.

Déployer un périphérique Défense contre les menaces sur Google Cloud Platform

Déployez un périphérique défense contre les menaces sur votre compte Google Cloud Platform (GCP) pour protéger vos charges de travail Google Cloud. La politique de sécurité pour ce périphérique sera gérée sur votre Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage).

Pour une communication efficace entre Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) et GCP, vous devez d'abord avoir un compte GCP, un projet GCP et plusieurs réseaux établis. Une fois que vous avez défini les paramètres de la GCP, intégrez un périphérique défense contre les menaces à déployer sur la GCP.

Utilisez les procédures suivantes pour intégrer et déployer un périphérique défense contre les menaces sur GCP.

Créer des réseaux VPC pour GCP

Le déploiement de défense contre les menaces virtuel nécessite quatre réseaux que vous devez créer avant de déployer défense contre les menaces virtuel. Les réseaux sont les suivants :

- VPC de gestion pour le sous-réseau de gestion.
- VPC de dépistage ou sous-réseau de dépistage.
- VPC interne pour le sous-réseau interne.
- VPC externe pour le sous-réseau externe.

En outre, vous devrez peut-être configurer des tables de routage et des règles de pare-feu GCP pour permettre au trafic de circuler dans défense contre les menaces. Les tableaux de routage et les règles de pare-feu sont distincts de ceux configurés sur le défense contre les menaces virtuel lui-même. Nommez les tables de routage et les règles de pare-feu de la plateforme GCP en fonction du réseau et des fonctionnalités associés

Procédure

Étape 1 Dans la console GCP, choisissez **VPC networking** (réseaux VPC), puis cliquez sur **Create VPC Network** (créer un réseau VPC).

Étape 2 Dans le champ **Name** (nom), saisissez le nom souhaité.

Étape 3 Dans le mode de création de sous-réseau, cliquez sur **Personnalisé**.

Étape 4 Dans le champ **Name** (Nom) sous **New subnet** (nouveau sous-réseau), saisissez le nom souhaité.

Étape 5 Dans la liste déroulante **Region** (région), sélectionnez la région appropriée pour votre déploiement. Les quatre réseaux doivent se trouver dans la même région.

Étape 6 Dans le champ **IP address range** (plage d'adresses IP), saisissez le sous-réseau du premier réseau au format CIDR, par exemple 10.10.0.0/24.

Étape 7 Acceptez les valeurs par défaut de tous les autres paramètres, puis cliquez sur **Create** (Créer).

Étape 8 Répétez les étapes 1 à 7 pour créer les trois autres réseaux VPC.

Prochaine étape

Vous devrez peut-être créer des règles de pare-feu à appliquer à vos nouveaux réseaux VPC. Dans la console GCP, accédez à **Networking** > **VPC network** > **Firewall** (pare-feu de réseau VPC), puis cliquez sur **Create Firewall Rule** (créer une règle de pare-feu). Consultez la documentation de GCP pour plus d'informations.

Une fois que vos réseaux VPC GCP ont été finalisés, continuez à déployer le défense contre les menaces virtual.

Déployer un périphérique Défense contre les menaces sur Google Cloud Platform

Avant de commencer

Lorsque vous effectuez cette procédure, Cisco Defense Orchestrator crée le défense contre les menaces virtuelles dans le cadre de l'assistant d'intégration. Vous ne pouvez pas utiliser cette procédure avec un périphérique physique défense contre les menaces ou un périphérique déjà intégré à CDO.

Les conditions préalables suivantes doivent être respectées avant d'intégrer un défense contre les menaces actuellement associé à un environnement Google Cloud Platform (GCP) :

- Vous devez avoir activé Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) pour votre détenteur.
- Vous devez avoir un compte GCP et avoir déjà créé un projet. Consultez la documentation de GCP pour plus d'informations.
- Interfaces de gestion (2) : une utilisée pour connecter le défense contre les menaces virtuel au centre de gestion, la seconde utilisée pour les dépistages; ne peut pas être utilisé pour le trafic de transit.

  Interfaces de trafic (2) : utilisées pour connecter les défense contre les menaces virtuels aux hôtes internes et au réseau public. Consultez Créer des réseaux VPC pour GCP, à la page 15 pour obtenir de plus amples renseignements.
- Vous **devez** activer toutes les autorisations suivantes dans l'environnement GCP pour réussir à communiquer avec CDO et à l'intégrer :

```
deploymentmanager.deployments.create
deploymentmanager.deployments.get
compute.networks.list
```

Procédure

Étape 1 Connectez-vous à CDO.

Étape 2 Dans le volet de navigation, cliquez sur **Inventory** (inventaire), puis sur le bouton bleu (+) pour ajouter un périphérique.

Étape 3 Sélectionnez la vignette **FTD**.

Étape 4 Sous **Management Mode** (Mode de gestion), sélectionnez **FTD**.

Étape 5 Sélectionnez **Utiliser GCP VPC** comme méthode de préparation.

Étape 6 **SI** vous n'avez pas encore authentifié votre environnement GCP avec CDO avant ce stade, copiez la commande bash générée par CDO et exécutez-la sur votre environnement bash ou sur Google Cloud Shell pour authentifier votre compte GCP et permettre la communication entre les applications. **SI** vous avez déjà authentifié votre compte GCP, ignorez les étapes d'intégration du compte et cliquez sur **Next** (suivant).

Étape 7 Utilisez le menu déroulant pour sélectionner le projet GCP que vous souhaitez associer au périphérique que vous comptez intégrer. Si aucun projet n'est disponible immédiatement, cliquez sur **+ Lier un nouveau projet**. Si vous cliquez sur **+ Lier un nouveau projet**, procédez comme suit :

a) Saisissez l'ID du projet GCP lorsque vous y êtes invité. Localisez cette valeur dans l'interface utilisateur de GCP. Pour trouver l'ID de projet, consultez la documentation de la GCP.

b) **Téléverser le fichier d'authentification** Cliquez sur **Parcourir** et accédez à l'endroit où le fichier .JSON généré à partir du script à l'étape 1 de l'assistant d'intégration est stocké localement. Sélectionnez-le et cliquez sur **Save** (Enregistrer).

Étape 8 Cliquez sur **Next** (suivant).

Étape 9 Utilisez les menus déroulants pour sélectionner les paramètres suivants et cliquez sur **Next** (suivant) :

- **VPC interne**
- **Sous-réseau interne**
- **VPC externe**
- **Sous-réseau externe**
- **VPC de gestion**
- **Sous-réseau de gestion**
- **Réseau de dépistage**
- **Sous-réseau de dépistage**

Étape 10 Saisissez un nom pour le périphérique défense contre les menaces dans le champ **Nom du périphérique** et cliquez sur **Suivant**.

Étape 11 À l'étape d'affectation de politique, utilisez le menu déroulant pour sélectionner une politique de contrôle d'accès à déployer une fois que le périphérique est intégré. Si vous n'avez pas configuré de politique pour votre Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) associé au détenteur CDO, sélectionnez la **politique de contrôle d'accès par défaut**.

Étape 12 Sélectionnez les **licences d'abonnement** que vous souhaitez appliquer au périphérique. Vous devez avoir au moins la licence URL sélectionnée pour les périphériques de défense contre les menaces virtuels.

Étape 13 Cliquez sur **Terminer l'intégration**.

Prochaine étape

Accédez à la page **Inventory** (inventaire) pour afficher la progression de l'enregistrement du périphérique à cet endroit. Une fois le périphérique synchronisé, nous vous recommandons fortement d'effectuer le lancement croisé sur Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) et de personnaliser votre politique de contrôle d'accès et l'état du périphérique.

Intégrer une grappe Cisco Secure Firewall Threat Defense

Remarque Si vous devez supprimer une grappe, supprimez la grappe de la page Inventory (inventaire) CDO. (Consultez Supprimer des périphériques de Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), à la page 20 pour obtenir de plus amples renseignements.)

Le tableau suivant fournit des informations sur les modèles de périphérique qui prennent en charge l'intégration et la création de grappes sur Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) :

Plateformes Cisco Secure Firewall Threat Defense	Version minimale de Cisco Secure Firewall Threat Defense pour la gestion des grappes	Prend en charge la création de grappes à partir de Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)?
VMware, KVM	7.2.1	Oui
AWS, GCP	7.2.1	Non
Azure	7.3	Non
Secure Firewall 3100	7.2.1	Oui
Firepower 4100	7.0.6	Non
Secure Firewall 4200	7.4	Oui
Firepower 9300	7.0.6	Non

Avant de commencer

Lisez attentivement les limites suivantes :

- Les périphériquesFirepower 4100 et Firepower 9300 doivent être mis en grappe par le biais du périphérique gestionnaire de châssis.
- Les périphériquesSecure Firewall 3100, les environnements KVM et VMware doivent être mis en grappe par l'intermédiaire de l'interface utilisateur Cisco Secure Firewall Management Center.
- Les grappes d'environnements Azure, AWS et GCP doivent être créées dans leur propre environnement et intégrées à Cisco Secure Firewall Management Center.

Procédure

Étape 1 Connectez-vous à CDO.

Étape 2 Dans le volet de navigation, cliquez sur **Inventory** (inventaire), puis sur le bouton bleu Plus.

Étape 3 Cliquez sur la fenêtre **FTD**.

Étape 4 Sous **Management Mode** (Mode de gestion), assurez-vous que **FTD** est sélectionné. En sélectionnant **FTD** sous **Management Mode**, vous ne pourrez pas gérer le périphérique à l'aide de la plateforme de gestion précédente. Toutes les configurations de politiques existantes, à l'exception des configurations d'interface, seront réinitialisées. Vous devez reconfigurer les politiques après avoir intégré le périphérique.

Remarque Si vous utilisez la licence d'évaluation de 90 jours, le nombre de jours restants est indiqué sous les options basculer **FTD** et **FDM**. Cliquez sur le lien **Manage Subscription License** (Gérer la licence d'abonnement) pour choisir une licence d'abonnement complet. Voir Types de licences pour périphériques gérés pour de plus amples renseignements.

Étape 5 Sélectionnez **Utiliser la clé d'enregistrement de l'interface de ligne de commande**.

Étape 6 Saisissez un nom pour le périphérique dans le champ **Nom du périphérique** et cliquez sur **Suivant**.

Étape 7 À l'étape d'affectation de politique, utilisez le menu déroulant pour sélectionner une politique de contrôle d'accès à déployer une fois que le périphérique est intégré. Si vous n'avez pas configuré de politique, sélectionnez la **politique de contrôle d'accès par défaut**.

Étape 8 Précisez si le périphérique que vous intégrez est un périphérique physique ou virtuel. Si vous intégrez un appareil virtuel, vous devez sélectionner le niveau de performance du périphérique dans le menu déroulant.

Étape 9 Sélectionnez les licences d'abonnement que vous souhaitez appliquer au périphérique. Cliquez sur **Next** (suivant).

Étape 10 CDO génère une commande avec la clé d'enregistrement. Collez la clé d'enregistrement complète telle quelle dans l'interface de ligne de commande du périphérique.

Étape 11 (Facultatif) Ajoutez des étiquettes à votre appareil pour trier et filtrer la page **d'inventaire**. Saisissez une étiquette et sélectionnez le bouton bleu Plus. Les étiquettes sont appliquées au périphérique après son intégration à CDO.

Prochaine étape

Une fois le périphérique synchronisé, sélectionnez le périphérique que vous venez d'intégrer dans la page **Inventaire** et sélectionnez l'une des options répertoriées dans le volet **Gestion des périphériques** situé à droite. Nous vous recommandons fortement d'effectuer les actions suivantes :

- Si vous ne l'avez pas encore fait, créez une politique de contrôle d'accès personnalisée pour adapter la sécurité à votre environnement. Consultez la présentation du contrôle d'accès dans le document *Gestion de Firewall Threat Defense avec CiscoFirewall Management Center en nuage dans Cisco Defense Orchestrator* pour obtenir de plus amples renseignements.
- Activez Cisco Security Analytics and Logging (SAL) pour afficher les événements dans le tableau de bord CDO **ou** enregistrez le périphérique sur un Cisco Secure Firewall Management Center pour des analyses de sécurité. Pour obtenir de plus amples renseignements sur Cisco Security Analytics and Logging, consultez le guide *Gestion de Firewall Threat Defense avec Cisco Firewall Management Center en nuage dans Cisco Defense Orchestrator*.

Supprimer des périphériques de Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)

Bien que des périphériques puissent être enregistrés dans Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), CDO gère toujours l'enregistrement des périphériques. Vous devez supprimer le périphérique du tableau de bord CDO pour supprimer un périphérique de Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage).

Remarque CDO ne synchronise pas la suppression des périphériques associés à un environnement VPC AWS. Vous devez supprimer un périphérique directement à partir de l'interface utilisateur d'AWS VPC. Pour obtenir de plus amples renseignements, consultez la documentation d'AWS.

Procédure

Étape 1 Connectez-vous à CDO et cliquez sur **Inventory**(inventaire).

Étape 2 Localisez le périphérique que vous souhaitez supprimer en utilisant les filtres ou la barre de recherche. Sélectionnez-la pour que la ligne du périphérique soit mise en surbrillance. Si votre périphérique fait partie d'une paire à haute disponibilité, localisez et sélectionnez le périphérique actif.

Étape 3 Dans le volet Device Actions (Actions des périphériques) situé à droite, cliquez sur **Supprimer**.

Étape 4 Lorsque vous y êtes invité, sélectionnez **OK** pour confirmer la suppression du périphérique sélectionné. Cliquez sur **Annuler** pour garder le périphérique intégré.

À propos des Interfaces des périphériques

Interface de gestion

Lors de la configuration de votre appareil, vous devez préciser l'adresse IP à laquelle vous souhaitez vous connecter. Le trafic de gestion et d'événement va à cette adresse lors de l'enregistrement initial.

Remarque Dans certaines situations, le périphérique peut établir la connexion *initiale* sur une interface de gestion différente. les connexions ultérieures doivent utiliser l'interface de gestion avec l'adresse IP spécifiée.

Si le périphérique possède une interface d'événements seulement distincte, le périphérique géré envoie le trafic des événements suivants est envoyé à l'interface d'événements seulement si le réseau le permet. En outre, certains modèles de périphérique géré comprennent une interface de gestion supplémentaire que vous pouvez configurer pour le trafic d'événement uniquement.

Remarque Notez que si vous configurez une interface de données pour la gestion, vous ne pouvez pas utiliser des interfaces de gestion et d'événements distinctes.

Si le réseau de l'événement tombe en panne, le trafic d'événement revient aux interfaces de gestion normales sur le périphérique géré.

À propos des interfaces de données

Vous pouvez utiliser soit l'interface de gestion dédiée, soit une interface de données habituelle pour communiquer avec le périphérique. L'accès CDO sur une interface de données est utile si vous souhaitez gérer FTD à distance depuis l'interface externe ou si vous n'avez pas de réseau de gestion distinct. Le CDO prend en charge la haute disponibilité sur le FTD géré à distance à partir de l'interface de données.

L'accès à la gestion du FTD à partir d'une interface de données présente les limites suivantes :

- Vous ne pouvez activer l'accès du gestionnaire que sur une seule interface physique de données. Vous ne pouvez pas utiliser une sous-interface ou EtherChannel.
- Mode de pare-feu routé uniquement, en utilisant une interface routée.
- PPPoE n'est pas pris en charge. Si votre fournisseur de services Internet requiert PPPoE, vous devrez placer un routeur avec prise en charge PPPoE entre FTD et le modem WAN.
- L'interface doit être dans le VRF global seulement.
- SSH n'est pas activé par défaut pour les interfaces de données, vous devrez donc activer SSH ultérieurement avec CDO. Comme la passerelle de l'interface de gestion sera transformée en interfaces de données, vous ne pouvez pas non plus autoriser SSH vers l'interface de gestion à partir d'un réseau distant, sauf si vous ajoutez une route statique pour l'interface de gestion à l'aide de la commande **configure network static-routes**. Pour FTDv sur Amazon Web Services, un port de console n'est pas disponible, vous devez donc conserver votre accès SSH à l'interface de gestion : ajoutez une route statique pour la gestion avant de poursuivre votre configuration. Sinon, assurez-vous de terminer toute la configuration de l'interface de ligne de commande (y compris la commande **configure manager add**) avant de configurer l'interface de données .

Routages réseau sur les interfaces de gestion de périphériques

Les interfaces de gestion (y compris les interfaces d'événements uniquement) prennent uniquement en charge les routes statiques pour atteindre les réseaux distants. Lorsque vous configurez votre périphérique géré, le processus de configuration crée une route par défaut vers l'adresse IP de la passerelle que vous spécifiez. Vous ne pouvez pas supprimer cette voie de routage; vous pouvez uniquement modifier l'adresse de la passerelle.

Remarque Si vous configurez une interface de données pour la gestion au lieu d'utiliser l'interface de gestion dédiée, le trafic est acheminé sur le fond de panier (backplane) pour utiliser la table de routage des données. Les renseignements de cette section ne s'appliquent pas.

Au moins une voie de routage statique est recommandée par interface de gestion pour accéder aux réseaux distants. Nous vous recommandons de placer chaque interface sur un réseau distinct pour éviter les problèmes de routage potentiels, y compris les problèmes de routage d'autres périphériques vers le périphérique. Si vous ne rencontrez pas de problèmes avec les interfaces sur le même réseau, veillez à configurer correctement les routes statiques. Par exemple, management0 et management1 se trouvent sur le même réseau, mais les interfaces de gestion et d'événement de FTD se trouvent sur des réseaux différents. La passerelle est 192.168.45.1. Si vous souhaitez que management1 se connecte à l'interface d'événements uniquement de la gestion à l'adresse 10.6.6.1/24, vous pouvez créer une route statique pour 10.6.6.0/24 par l'intermédiaire de management1 avec la même passerelle que 192.168.45.1. Le trafic vers10.6.6.0/24 atteindra cette route avant la route par défaut. Par conséquent, management1 sera utilisé comme prévu.

Connexion à l'interface de ligne de commande (CLI) sur le périphérique

Vous pouvez vous connecter directement à l'interface de ligne de commande sur les périphériques défense contre les menaces . S'il s'agit de votre première connexion, terminez le processus de configuration initiale en utilisant l'utilisateur **admin** par défaut. voir Terminer la configuration initiale d'un périphérique Cisco Secure Firewall Threat Defense à l'aide de l'interface de ligne de commande.

Remarque Après qu'un utilisateur ait échoué à trois reprises à se connecter à l'interface de lige de commande au moyen de SSH, le périphérique met fin à la connexion SSH.

Avant de commencer

Créez des comptes d'utilisateur locaux qui peuvent se connecter à l'interface de ligne de commande à l'aide de la commande **configure user add**.

Procédure

Étape 1 Connectez-vous à l'interface de ligne de commande défense contre les menaces , à partir du port de console ou à l'aide de SSH.

Vous pouvez vous connecter en SSH à l'interface de gestion de l'appareil défense contre les menaces . Vous pouvez également vous connecter à l'adresse sur une interface de données si vous ouvrez l'interface pour les connexions SSH. L'accès SSH aux interfaces de données est désactivé par défaut. Consultez Secure Shell pour autoriser les connexions SSH à des interfaces de données spécifiques.

Pour les périphériques physiques, vous pouvez vous connecter directement au port de console du périphérique. Consultez le guide du matériel de votre appareil pour en savoir plus sur le câble de la console. Utilisez les paramètres de série suivants :

- 9 600 bauds
- 8 bits de données
- Pas de parité
- 1 bit d'arrêt

L'interface de ligne de commande sur le port de console est FXOS (à l'exception de l'ISA 3000, où il s'agit de l'interface de commande en ligne défense contre les menaces normale). Utilisez l'interface de ligne de

commande de défense contre les menaces pour la configuration de base, la surveillance et le dépannage normal du système. Consultez la documentation de FXOS pour obtenir des renseignements sur les commandes FXOS.

Étape 2 Connectez-vous avec le nom d'utilisateur et le mot de passe **d'administrateur**.

Exemple :

```
firepower login: admin
Password:
Last login: Thu May 16 14:01:03 UTC 2019 on ttyS0
Successful login attempts for user 'admin' : 1

firepower#
```

Étape 3 Si vous avez utilisé le port de console, accédez à l'interface de ligne de commande défense contre les menaces .

connect ftd

Remarque Cette étape ne s'applique pas à ISA 3000.

Exemple :

```
firepower# connect ftd
>
```

Étape 4 À l'invite de l'interface de ligne de commande (>), utilisez l'une des commandes autorisées par votre niveau d'accès à la ligne de commande.

Pour revenir à FXOS sur le port de console, saisissez **exit**.

Étape 5 (Facultatif) Si vous avez utilisé SSH, vous pouvez vous connecter à FXOS.

connect fxos

Pour revenir à l'interface de ligne de commande défense contre les menaces , saisissez **exit**.

Étape 6 (Facultatif) Accédez à l'interface de ligne de commande de dépistage :

system support diagnostic-cli

Utilisez cette interface de ligne de commande pour un dépannage avancé. Cette interface de ligne de commande comprend des commandes supplémentaires **show** et d'autres commandes.

Elle comporte deux sous-modes : le mode EXEC utilisateur et le mode EXEC privilégié. Davantage de commandes sont disponibles en mode EXEC privilégié. Pour passer en mode d'exécution privilégié, saisissez la commande **enable** ; appuyez sur Entrée sans saisir de mot de passe lorsque vous y êtes invité.

Exemple :

```
> system support diagnostic-cli
firepower> enable
Password:
firepower#
```

Pour revenir à l'interface de ligne de commande classique, tapez **Ctrl-a**, **d**.

Dépannage

Utilisez les scénarios suivants pour résoudre les problèmes d'intégration.

Résoudre les problèmes de connectivité de Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) avec TCP

Utilisez la procédure suivante pour dépanner la connectivité entre le Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) et un périphérique défense contre les menaces doté du port TCP 8305.

Procédure

Étape 1 Connectez-vous à CDO.

Étape 2 Accédez à **Outils et services** dans le panneau de gauche et sélectionnez **Firewall Management Center** pour ouvrir la page **Services**. Choisissez **Cloud-Delivered FMC** (FMC en nuage) et localisez le nom de domaine complet de Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)dans le coin supérieur droit.

Étape 3 Assurez-vous que l'état du périphérique défense contre les menaces dans CDO est en cours **d'intégration**. Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) ne répondra pas si le périphérique n'est pas en état d'intégration. Si l'intégration échoue, cliquez sur **Réessayer l'intégration**.

Étape 4 Connectez-vous au périphérique défense contre les menaces à l'aide de SSH.

Étape 5 Saisissez en mode expert avec la commande suivante :

```
> expert
admin@devicename:~$
```

Étape 6 Exécutez une prise de contact TCP :

```
admin@devicename:~$ nc -v xxxxxx.cdo.cisco.com 8305
Connection to xxxxxx.cdo.cisco.com 8305 port [tcp/*] succeeded!
^C (CTRL-C to exit netcat)
admin@devicename:~$.
```

Prochaine étape

S'il n'y a toujours pas de réponse de Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), il est possible que le port sortant TCP 8305 soit bloqué en amont de votre périphérique défense contre les menaces et que le chemin réseau devra être renforcé avant que votre défense contre les menaces puisse se connecter à Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage).

Dépannage de la connectivité du périphérique Défense contre les menaces

Testez la connectivité à Internet à partir du plan de gestion du périphérique défense contre les menaces :

Procédure

	Commande ou action	Objectif
Étape 1	Connectez-vous au périphérique défense contre les menaces à l'aide de SSH.	
Étape 2	Envoyez un ping à l'un des éléments suivants ou aux deux :	• system 208.67.222.222 • system cisco.com

Prochaine étape

Si l'un de ces tests échoue, il y a probablement un problème L1 à L3 et vous devrez vérifier votre configuration de mise en réseau de gestion (`show network`) (Afficher le réseau) et/ou un problème DNS.

Dépannage de la perte de connectivité de l'appareil après la mise à jour de Firewall Management Center en nuage

Un Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) reçoit une adresse IP dynamique lorsqu'il est ajouté à un détenteur CDO. Lorsque le centre de gestion est mis à jour, le centre de gestion reçoit une nouvelle adresse IP dynamique.

Si votre pare-feu inspecte le trafic sortant de votre périphérique de défense contre les menaces vers Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), vos règles de pare-feu doivent permettre au trafic de défense contre les menaces de circuler vers le nom de domaine complet et le port du centre de gestion plutôt que son adresse IP, sinon le centre de gestion pas en mesure de gérer votre périphérique de défense contre les menaces.

Par exemple, si votre règle de trafic réseau autorisant la gestion du trafic de votre appareil de défense contre les menaces vers Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) ressemble à ceci :

```
autoriser tout le trafic<my-threat-defense-ip-src> à 200.165.200.225
```

où 200.165.200.225 est l'adresse de gestion de Firewall Management Center en nuage, remplacez la règle Allow (autorisation) par ces deux règles Allow (autorisation), car les ports 443 et 8305 doivent être ouverts :

```
allow all traffic <my-threat-defense-ip-src > to <my-cdfFMC-FQDN>:443

allow all traffic <my-threat-defense-ip-src > to <my-cdfFMC-FQDN>:8305
```

Consultez la section « Exigences relatives au réseau » dans les Conditions préalables à l'intégration d'un périphérique au centre de gestion Firewall en nuage pour en savoir plus sur le port.

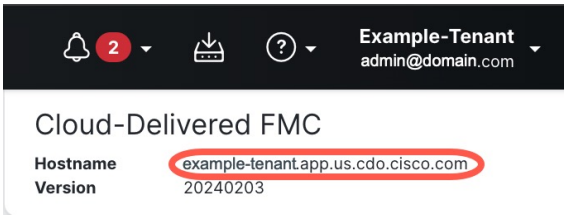
Où puis-je trouver le nom de domaine de mon Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)?

Où puis-je trouver le nom de domaine de mon Cisco Firewall Management Center fourni en nuage?

1. Connectez-vous à CDO.
2. Dans la barre de menu, accédez à **Outils et services > Firewall Management Center.**
3. Sélectionner Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) dans le tableau FMC.

4. Dans le coin supérieur droit de l'écran, vous verrez le nom d'hôte du centre de gestion. Il s'agit du FQDN (nom de domaine complet).

Illustration 1 : Nom de domaine complet du FMC en nuage (FQDN)



Dépannage de l'intégration d'un périphérique à Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) à l'aide de la clé d'enregistrement de la CLI

Erreur : le périphérique reste en attente de configuration après l'intégration

Lorsqu'un périphérique ne s'enregistre pas, l'état de connectivité du périphérique indique **Pending Setup**(configuration en attente) . Dans le panneau situé à droite, CDO affiche un message **Échec de l'enregistrement** ainsi qu'un bouton **Réessayer l'intégration** pour vous permettre immédiatement de réessayer d'intégrer le périphérique.

Si vous n'exécutez pas la commande du `gestionnaire de configuration` dans l'interface de ligne de commande du périphérique dans les 3 minutes suivant son intégration dans CDO, la tentative d'enregistrement du périphérique expire et entraîne un échec de l'enregistrement. Utilisez la procédure suivante pour résoudre le problème :

Procédure

Étape 1 Connectez-vous à CDO et accédez à la page **Inventaire**. Localisez le périphérique qui n'a pas pu s'enregistrer.

Étape 2 Dans le panneau situé à droite, localisez la fenêtre **Registration Failed** (échec de l'enregistrement). À côté de la clé d'enregistrement de l'interface de ligne de commande du périphérique, cliquez sur **Copy** (Copier). Cette action copie la clé CLI dans un presse-papiers local.

Étape 3 Ouvrez une connexion SSH avec le périphérique et connectez-vous en tant `qu'administrateur`.

Étape 4 Collez la clé d'enregistrement de l'interface de ligne de commande dans l'interface CLI du périphérique. Dans l'interface de ligne de commande, saisissez **Y** (Oui) pour terminer l'enregistrement. Si votre périphérique était auparavant géré par gestionnaire d'appareil, saisissez **Yes** (oui) pour confirmer la soumission.

Dépannage de l'intégration d'un appareil dans Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) utilisant le numéro de série

Le périphérique est inaccessible ou inatteignable

Si le périphérique est inaccessible pendant le processus d'intégration, ou à tout moment après l'intégration, CDO affiche l'état de la connectivité **Inaccessible**. L'appareil ne pourra pas s'intégrer complètement à CDO tant que le périphérique ne pourra pas se connecter. Les scénarios suivants peuvent en être la cause :

- Le périphérique n'est pas correctement câblé.
- Votre réseau peut nécessiter une adresse IP statique pour le périphérique.
- Votre réseau utilise un DNS personnalisé, ou un DNS externe bloque le réseau.
- Si votre périphérique est associé à la région européenne (https://defenseorchestrator.eu/), vous devrez peut-être activer l'authentification PPPoE. Pour les autres domaines, consultez les exigences du domaine.
- Le périphérique est peut-être bloqué par un pare-feu ou bloque de manière incorrecte un port pour la connectivité. Passez en revue le Exigences en matière de réseau, à la page 4 de périphérique et confirmez que les bons ports de sortie sont activés.

Erreur : numéro de série déjà demandé

L'appareil a été acheté auprès d'un fournisseur externe

Si le périphérique a été acheté auprès d'un fournisseur externe et que l'intégration échoue avec une erreur de **numéro de série déjà réclamé**, il est possible que le périphérique soit toujours associé au détenteur du fournisseur. Suivez les étapes suivantes pour réclamer le périphérique et son numéro de série :

1. Supprimez le périphérique de votre détenteur CDO.
2. Installez l'image FXOS sur le périphérique. Pour en apprendre davantage, consultez le chapitre « Procédures de recréation d'image » du guide de dépannage Cisco FXOS pour les périphériques Firepower 1000/21000 et Secure Firewall 3100 Firepower Threat Defense.
3. Connectez un ordinateur portable au port de console du périphérique.
4. Connectez-vous à l'interface de ligne de commande FXOS et connectez-vous en tant **qu'administrateur**.
5. Dans l'interface de ligne de commande de FXOS, connectez-vous à **local-mgmt** à l'aide de la commande `firepower # connect local-mgmt`.
6. Exécutez la commande `firepower(local-mgmt) # cloud deregister pour annuler l'enregistrement` du périphérique du détenteur en nuage.
7. Une fois l'enregistrement du périphérique réussi, l'interface de la CLI renvoie un message de réussite. Voici un exemple du message :

```
Example: firepower(local-mgmt) # cloud deregister Release Image Detected RESULT=success
 MESSAGE=SUCCESS 10, X-Flow-Id: 2b3c9e8b-76c3-4764-91e4-cfd9828e73f9
```

Remarque Si le périphérique n'a jamais été enregistré auprès d'un autre détenteur CDO, le message ci-dessus indique `RESULT=success MESSAGE=DEVICE_NOT_FOUND`.

8. Intégrez le périphérique à votre détenteur CDO avec son numéro de série. Consultez Intégrer un périphérique avec un numéro de série, à la page 8 pour obtenir de plus amples renseignements.

L'appareil est réclamé par un détenteur CDO dans une autre région

Le périphérique peut avoir été précédemment géré par une autre instance CDO dans une région différente et est toujours enregistré pour ce détenteur.

Si vous **avez** accès au détenteur auquel le périphérique est actuellement enregistré, utilisez la procédure suivante :

1. Supprimez le périphérique du détenteur CDO non valide.
2. Connectez-vous à l'interface utilisateur gestionnaire d'appareil du périphérique.
3. Accédez aux **Paramètres système** > **Services en nuage**.
4. Cliquez sur **Services en nuage** et sélectionnez **Désenregistrer les services en nuage** dans la liste déroulante.
5. Confirmez l'action et cliquez sur **Unregister** (Désenregistrer). Cette action génère un avertissement pour indiquer que le périphérique a été supprimé de CDO. Il s'agit du comportement attendu.
6. Connectez-vous au détenteur CDO dans la région appropriée et intégrez le périphérique. Consultez Intégrer un périphérique avec un numéro de série, à la page 8 pour obtenir de plus amples renseignements.
7. Accédez aux **Paramètres système** > **Services en nuage**.
8. Cliquez sur **Services en nuage** et sélectionnez **Désenregistrer les services en nuage** dans la liste déroulante.
9. Sélectionnez **Auto-enroll with Tenancy from Cisco Defense Orchestrator** (Inscription automatique avec Tenancy de Cisco Defense Orchestrator) et cliquez sur **Register** (Enregistrer). L'appareil est mappé au nouveau détenteur qui appartient à la nouvelle région et CDO intègre le périphérique.

Si vous **n'avez pas** accès au détenteur, utilisez la procédure ci-dessous :

1. Connectez-vous à l'interface de ligne de commande FXOS à partir du port de console et connectez-vous en tant **qu'administrateur**. Pour obtenir des renseignements sur la connexion à l'interface de ligne de commande de FXOS, consultez Accéder à l'interface de ligne de commande de FXOS).
2. Dans l'interface de ligne de commande de FXOS, connectez-vous à **local-mgmt** à l'aide de la commande `firepower # connect local-mgmt`.
3. Exécutez la commande `firepower(local-mgmt) # cloud deregister pour annuler l'enregistrement` du périphérique du détenteur en nuage.
4. Une fois l'enregistrement du périphérique réussi, l'interface de la CLI renvoie un message de réussite. Voici un exemple du message :

```
Example: firepower(local-mgmt) # cloud deregister Release Image Detected RESULT=success
 MESSAGE=SUCCESS 10, X-Flow-Id: 2b3c9e8b-76c3-4764-91e4-cfd9828e73f9
```

Remarque Si le périphérique n'a jamais été enregistré auprès d'un autre détenteur CDO, le message ci-dessus indique `RESULT=success MESSAGE=DEVICE_NOT_FOUND.`

5. Dans votre détenteur CDO, au domaine valide, intégrez le périphérique. Consultez Intégrer un périphérique avec un numéro de série, à la page 8 pour obtenir de plus amples renseignements.
6. Dans l'interface utilisateur gestionnaire d'appareil du périphérique , accédez à **Paramètres système** > **Cloud Services**.
7. Sélectionnez **Auto-enroll with Tenancy from Cisco Defense Orchestrator** (Inscription automatique avec Tenancy de Cisco Defense Orchestrator) et cliquez sur **Register** (Enregistrer). L'appareil est mappé au nouveau détenteur qui appartient à la nouvelle région et CDO intègre le périphérique.

Erreur : Erreur de demande

Si vous saisissez le mauvais numéro de série lors de l'intégration d'un appareil, CDO générera un état d'**erreur de réclamation**.

Remarque Pour confirmer que le périphérique est réclamé dans la bonne région dans CDO.

Résolvez ce problème avec la solution ci-dessous :

Procédure

Étape 1 Connectez-vous à CDO et accédez à la page **Inventaire**. Localisez le périphérique comportant l'erreur.

Étape 2 Sélectionnez le périphérique pour qu'il soit en surbrillance et **retirez** le périphérique de CDO.

Étape 3 Vérifiez les points suivants :

- Le périphérique est en ligne et peut se connecter à Internet.
- Le périphérique n'a pas déjà été intégré à votre instance CDO ou réclamé par un détenteur CDO dans une autre région.

Étape 4 Localisez le numéro de série du périphérique. Vous pouvez utiliser l'une des méthodes suivantes :

- Pour les modèles des séries 1000, 2100 et 3100, recherchez le numéro de série sur le périphérique physique.
- Ouvrez une connexion SSH avec le périphérique et saisissez la commande `show serial- number`.
- S'il s'agit actuellement d'un périphérique Géré par FDM, connectez-vous à l'interface utilisateur gestionnaire d'appareil et localisez le numéro de série sur la page des **services en nuage**.

Étape 5 Dans CDO, intégrez le périphérique avec le bon numéro de série. Consultez la Intégrer un périphérique avec un numéro de série, à la page 8 pour de plus amples renseignements.

Erreur : échec de la demande

Si le message **Erreur : échec de la demande** de l'état de la connectivité ou du message d'erreur s'affiche après une tentative d'intégration d'un appareil, les éléments suivants peuvent en être la cause :

- La plateforme Security Services Exchange peut connaître des problèmes temporaires qui entraînent une perte de connectivité.
- Le serveur CDO est peut-être en panne.

Suivez la procédure ci-dessous pour résoudre ce problème :

Procédure

Étape 1 Connectez-vous à CDO et accédez à la page **Inventaire**. Localisez le périphérique qui n'a pas pu s'enregistrer.

Étape 2 Sélectionnez le périphérique pour qu'il soit en surbrillance et **supprimez** le périphérique de votre détenteur CDO.

Étape 3 Attendez au moins 10 minutes avant de tenter de réintégrer le périphérique de votre détenteur CDO. Consultez Préparation d'un appareil avec un provisionnement à faible intervention humaine, à la page 7 pour obtenir de plus amples renseignements.

Prochaine étape

Si vous ne parvenez toujours pas à réclamer le périphérique, passez en revue le flux de travail du périphérique pour voir s'il y a un message d'erreur. Si tel est le cas,exportez le flux de travail et ouvrez une demande d'assistance pour résoudre le problème.

Erreur : Erreur de provisionnement

Le mot de passe du périphérique n'a pas été modifié

Si vous n'avez pas modifié le mot de passe par défaut du périphérique lors de la configuration de ce dernier pour la gestion à distance et que vous avez sélectionné l'option **Non, cet appareil a été connecté et configuré pour un gestionnaire** lors de l'intégration du périphérique à CDO, le périphérique générera un état de connectivité **Non provisionné** dans la page **Inventory** (Inventaire).

Utilisez la procédure suivante pour résoudre ce problème :

1. Connectez-vous à CDO et accédez à la page **Inventaire**.
2. Localisez et sélectionnez le périphérique avec l'état de connectivité **UnProvisioned** (non provisionné) afin qu'il soit mis en surbrillance.
3. Dans le volet situé à droite, recherchez la fenêtre de **modification du mot de passe**.
4. Cliquez sur **Change Password** (modifier le mot de passe) et saisissez un nouveau mot de passe pour votre périphérique. Cela remplace le mot de passe par défaut.

Cela peut prendre quelques minutes pour que le périphérique soit intégré et se synchronise complètement avec CDO.

Le mot de passe du périphérique a déjà été modifié

Si vous **avez vraiment** modifié le mot de passe par défaut du périphérique lors de la configuration du périphérique pour la gestion à distance et que vous avez sélectionné la commande **S'agit-il d'un nouveau périphérique qui n'a jamais été connecté ou configuré auparavant?** lors de l'intégration du périphérique sur CDO, CDO génère un état de connectivité **UnProvisioned** (non provisionné) dans la page **Inventory** (inventaire).

Utilisez la procédure suivante pour résoudre ce problème :

1. Connectez-vous à CDO et accédez à la page **Inventaire**.
2. Localisez et sélectionnez le périphérique avec l'état de connectivité **UnProvisioned** (non provisionné) afin qu'il soit mis en surbrillance.
3. Dans le volet situé à droite, localisez la fenêtre **Confirmer et continuer**.
4. Cliquez sur **Confirmer et continuer**. Cette action ignore le mot de passe qui a été fourni dans l'assistant d'intégration et rétablit le mot de passe par défaut pour le périphérique. CDO poursuit ensuite l'intégration de ce dernier.

Autres scénarios d'erreurs provisoires

Indépendamment de la configuration du mot de passe par défaut du périphérique , il est toujours possible qu'un appareil génère un état de connectivité **UnProvisioned** (non provisionné) pendant le processus d'intégration. Si vous confirmez que la sélection du mot de passe dans l'assistant d'intégration est correcte pour l'état du périphérique , envisagez les options suivantes pour résoudre le problème :

- Sélectionnez le périphérique pour qu'il soit mis en surbrillance. Dans la fenêtre située dans le volet droit de l'écran, cliquez sur **Retry** (réessayer) pour forcer CDO à réintégrer le périphérique avec les paramètres provisoires existants.
- Supprimez le périphérique de la page d'**inventaire** et tentez de réintégrer le périphérique.
- Dans l'interface utilisateur gestionnaire d'appareil du périphérique , accédez à **Paramètres système** > **Cloud Services**. Sélectionnez **Auto-enroll with Tenancy from Cisco Defense Orchestrator** (Inscription automatique avec Tenancy de Cisco Defense Orchestrator) et cliquez sur **Register** (Enregistrer).

Si vous ne parvenez toujours pas à réclamer le périphérique, passez en revue le flux de travail du périphérique pour voir s'il y a un message d'erreur. Si tel est le cas,exportez le flux de travail et ouvrez une demande d'assistance pour résoudre le problème.

Erreur : Erreur de provisionnement

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.