CSM 3.x : Ajouter des capteurs et des modules IDS à l'inventaire de Security Manager

Contenu

Introduction

Ce document fournit des informations sur la façon dont ajouter des capteurs et des modules de système de détection d'intrusion (ID) (inclut IDSM sur des Commutateurs de Catalyst 6500, NM-CIDS sur des Routeurs et AIP SSM sur l'ASA) dans le Cisco Security Manager (CSM).

Remarque: CSM 3.2 ne prend en charge pas IPS 6.2. Il est pris en charge dans CSM 3.3.

Conditions préalables

Conditions requises

Ce document suppose que des périphériques CSM et d'ID sont installés et fonctionnent correctement.

Composants utilisés

Les informations dans ce document sont basées sur le CSM 3.0.1.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Ajoutez les périphériques à l'inventaire de directeur de la sécurité

Quand vous ajoutez un périphérique au directeur de la sécurité, vous apportez une plage de l'information d'identification pour le périphérique, tel que son nom DNS et adresse IP. Après que vous ajoutiez le périphérique, il apparaît dans l'inventaire des périphériques de directeur de la sécurité. Vous pouvez gérer un périphérique dans le directeur de la sécurité seulement après que vous l'ajoutez à l'inventaire.

Vous pouvez ajouter des périphériques à l'inventaire de directeur de la sécurité avec ces méthodes :

- Ajoutez un périphérique du réseau.
- Ajoutez un nouveau périphérique qui n'est pas encore sur le réseau
- Ajoutez un ou plusieurs périphériques du périphérique et du référentiel de qualifications (DCR).
- Ajoutez un ou plusieurs périphériques à partir d'un fichier de configuration.

Remarque: Ce document se concentre sur la méthode : Ajoutez un nouveau périphérique qui n'est pas encore sur le réseau.

Étapes pour ajouter les ID capteur et modules

Employez la nouvelle option de périphérique d'ajouter afin d'ajouter un à un dispositif à l'inventaire de directeur de la sécurité. Vous pouvez utiliser cette option pour le pré-provisionnement. Vous pouvez créer le périphérique dans le système, assigner des stratégies au périphérique, et générer des fichiers de configuration avant que vous receviez le matériel de périphérique.

Quand vous recevez le matériel de périphérique, vous devez disposer les périphériques pour être géré par le directeur de la sécurité. Référez-vous à préparer les périphériques pour le directeur de la sécurité gérer le pour en savoir plus.

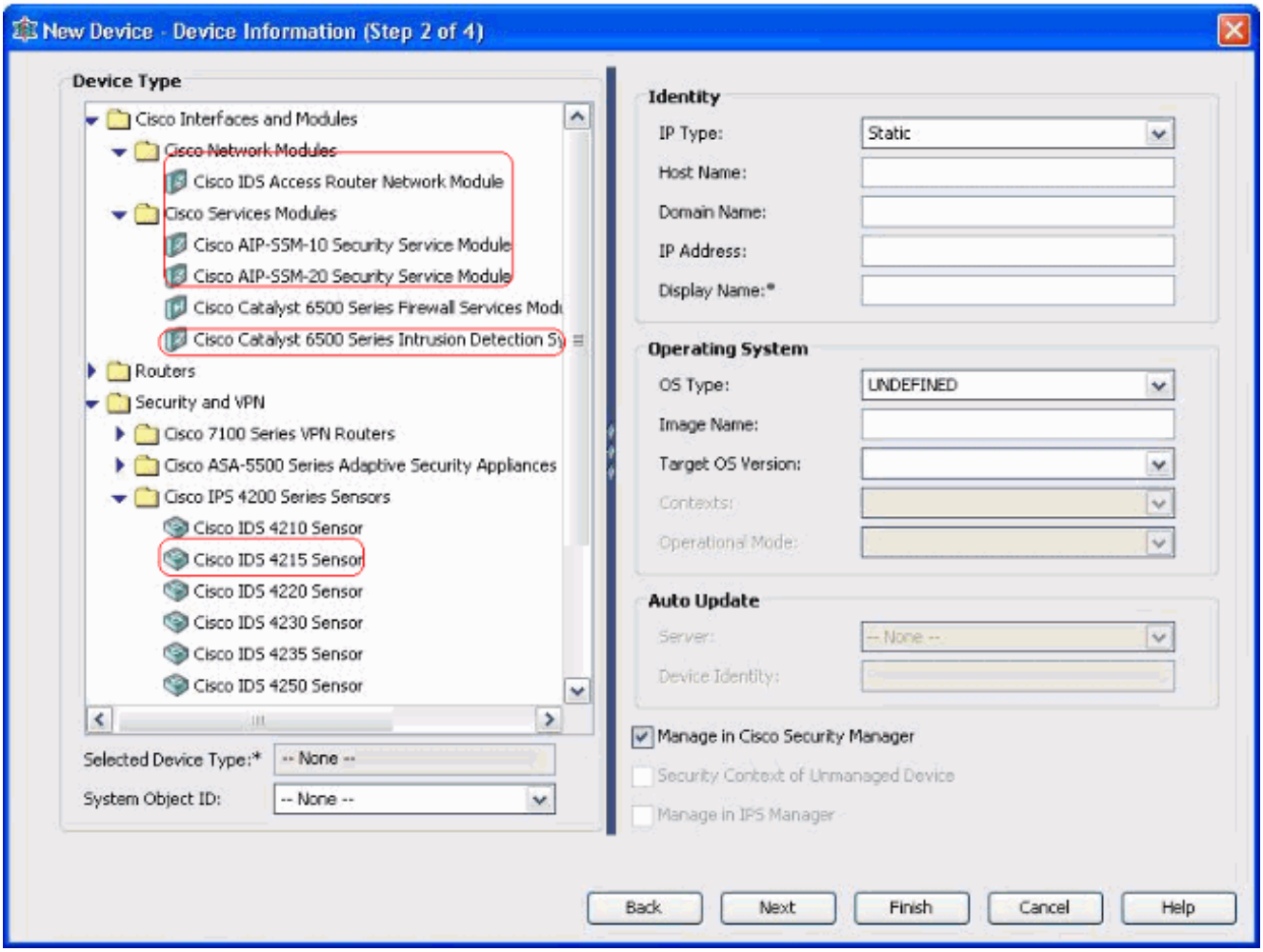
Cette procédure affiche comment ajouter de nouveaux ID capteur et modules :

1. Cliquez sur le bouton d'**affichage périphériques** dans la barre d'outils.La page de périphériques paraît.
2. Cliquez sur le bouton d'**ajouter** dans le sélecteur de périphérique.Le nouveau périphérique - Choisissez la page de méthode apparaît avec quatre options.
3. Choisissez **ajoutent le nouveau périphérique**, puis cliquent sur Next.Le nouveau périphérique - La page de l'information sur le périphérique paraît.
4. Écrivez l'information sur le périphérique dans les champs appropriés.Voyez l'information sur le périphérique de fourniture — Nouveau pour en savoir plus de section de périphérique.
5. Cliquez sur **Finish** (Terminer).Le système effectue des tâches de validation de périphérique :Si les données sont incorrectes, le système génère des messages d'erreur et affiche la page à laquelle l'erreur se produit avec une icône rouge d'erreur qui correspond à lui.Si les données sont correctes, le périphérique est ajouté à l'inventaire et il apparaît dans le sélecteur de périphérique.

Fournissant l'information sur le périphérique — Nouveau périphérique

Procédez comme suit :

1. Sélectionnez le type de périphérique pour le nouveau périphérique :Sélectionnez le répertoire supérieur de type de périphérique afin d'afficher les familles de périphérique pris en charge.Sélectionnez le répertoire de gamme de périphériques afin d'afficher les types de périphérique pris en charge.Sélectionnez les **Interfaces et modules Cisco > les Modules de réseau Cisco** afin d'ajouter le **Module de réseau pour routeur d'accès Cisco IDS**. De même, **Interfaces et modules Cisco > Modules de services Cisco** choisis afin d'ajouter les modules d'AIP SSM et IDSM affichés.Sélectionnez la **Sécurité et VPN > les Détecteurs de la gamme Cisco IPS 4200** afin d'ajouter le Détecteur Cisco IDS 4210 à l'inventaire CSM.



Sélectionnez le type de périphérique.**Remarque:** Après que vous ajoutiez un périphérique, vous ne pouvez pas changer le type de périphérique.Des object id de système pour ce type de périphérique sont affichés dans le domaine de SysObjectId. Le premier object id de système est sélectionné par défaut. Vous pouvez sélectionner un autre si nécessaire.

2. Écrivez les informations d'identité de périphérique, telles que le type IP (statique ou dynamique), l'adresse Internet, le nom de domaine, l'adresse IP, et le nom d'affichage.
3. Écrivez les informations du système d'exploitation de périphérique, telles que le type de SYSTÈME D'EXPLOITATION, le nom d'image, la version de système d'exploitation de cible, les contextes, et le mode opérationnel.
4. Le gisement automatique d'engine de mise à jour ou de CNS-configuration apparaît, qui dépend du type de périphérique que vous sélectionnez :Mise à jour automatique — Affiché

pour le Pare-feu PIX et les périphériques ASA.Engine de CNS-configuration — Affiché pour des Routeurs de Cisco IOS®.**Remarque:** Ce champ n'est pas en activité pour le Catalyst 6500/7600 et les périphériques FWSM.

5. Procédez comme suit :Mise à jour automatique — Cliquez sur la flèche pour afficher une liste de serveurs. Sélectionnez le serveur qui gère le périphérique. Si le serveur n'apparaît pas dans la liste, terminez-vous ces étapes :Cliquez sur la flèche, puis sélectionnez **+ ajoutez le serveur**… La boîte de dialogue Properties de serveur apparaît.Écrivez les informations dans les champs requis.Cliquez sur **OK**. Le nouveau serveur est ajouté à la liste de serveurs disponibles.Engine de CNS-configuration — Les informations différentes sont affichées, qui dépendent de si vous sélectionnez le type statique ou dynamique IP :**Statique** — Cliquez sur la flèche pour afficher une liste de Configurations Engine. Sélectionnez la Configuration Engine qui gère le périphérique. Si la Configuration Engine n'apparaît pas dans la liste, terminez-vous ces étapes :Cliquez sur la flèche, puis sélectionnez **+ ajoutez la Configuration Engine**… La boîte de dialogue Properties de Configuration Engine apparaît.Écrivez les informations dans les champs requis.Cliquez sur **OK**. La nouvelle Configuration Engine est ajoutée à la liste de Configurations Engine disponibles.**Dynamique** — Cliquez sur la flèche pour afficher une liste de serveurs. Sélectionnez le serveur qui gère le périphérique. Si le serveur n'apparaît pas dans la liste, terminez-vous ces étapes :Cliquez sur la flèche, puis sélectionnez **+ ajoutez le serveur**… La boîte de dialogue Properties de serveur apparaît.Écrivez les informations dans le champ requis.Cliquez sur **OK**. Le nouveau serveur est ajouté à la liste de serveurs disponibles.
6. Procédez comme suit :Afin de gérer le périphérique dans le directeur de la sécurité, cochez le **gérer dans la** case de **Cisco Security Manager**. Il s'agit de la configuration par défaut.Si la seule fonction du périphérique que vous ajoutez est de servir de point final VPN, décochent le **gérer dans la** case de **Cisco Security Manager**.Le directeur de la sécurité ne gèrera pas des configurations ou téléchargera ou téléchargera des configurations sur ce périphérique.
7. Cochez le contexte de sécurité de la case de périphérique de non pris en charge afin de gérer un contexte de sécurité, dont le périphérique de parent (Pare-feu PIX, ASA, ou FWSM) n'est pas géré par le directeur de la sécurité.Vous pouvez partitionner un Pare-feu PIX, une ASA, ou un FWSM dans de plusieurs Pare-feu de Sécurité, également connus sous le nom de contextes de sécurité. Chaque contexte est un système indépendant, avec sa propres configuration et stratégies. Vous pouvez gérer ces contextes autonomes dans le directeur de la sécurité, quoique le parent (Pare-feu PIX, ASA, ou FWSM) ne soit pas géré par le directeur de la sécurité.**Remarque:** Ce champ est en activité seulement si le périphérique que vous avez sélectionné dans le sélecteur de périphérique est un périphérique de Pare-feu, tel que le Pare-feu PIX, l'ASA, ou le FWSM, qui prend en charge le contexte de sécurité.
8. Cochez le **gérer dans la** case de **gestionnaire IPS** afin de gérer un routeur Cisco IOS dans le gestionnaire IPS.Ce champ est en activité seulement si vous sélectionniez un routeur Cisco IOS du sélecteur de périphérique.**Remarque:** Le gestionnaire IPS peut gérer les caractéristiques IPS seulement sur un routeur Cisco IOS qui a des capacités IPS. Le pour en savoir plus, voient la documentation IPS.Si vous cochez le gérer dans la case de gestionnaire IPS, vous devez cocher le gérer dans la case de Cisco Security Manager également.Si le périphérique sélectionné est des ID, ce champ n'est pas en activité. Cependant, la case est cochée parce que le gestionnaire IPS gère des capteurs d'ID.Si le périphérique sélectionné est Pare-feu PIX, ASA, ou FWSM, ce champ n'est pas en activité parce que le gestionnaire IPS ne gère pas ces types de périphérique.
9. Cliquez sur **Finish** (Terminer).Le système effectue des tâches de validation de périphérique :Si les données que vous avez saisies sont incorrectes, le système génère des messages

d'erreur et affiche la page où l'erreur se produit.Si les données que vous avez saisies sont correctes, le périphérique est ajouté à l'inventaire et il apparaît dans le sélecteur de périphérique.

Dépannez

Utilisez cette section pour dépanner votre configuration.

Messages d'erreur

Quand vous ajoutez l'IPS au CSM, le `périphérique non valide : N'a pas pu déduire le SysObjId pour le` message d'erreur de `type de plate-forme` apparaît.

Solution

Terminez-vous ces étapes afin de résoudre ce message d'erreur.

1. Arrêtez le service de démon CSM dans Windows, et puis choisissez les **fichiers de programme > le CSCOpx > la MDC > l'Athéna > le config > le répertoire**, où vous pouvez trouver `VMS-SysObjID.xml.`
2. Sur le système CSM, remplacez le fichier situé de l'original VMS-SysObjID.xml par défaut dans C:\Program Files\CSCOpx\MDC\athena\config\directory `par le` dernier `fichier` VMS-SysObjID.xml.
3. Redémarrez le service de gestionnaire de démon CSM (CRMDmgtd), et relancez pour ajouter ou découvrir les dispositifs affectés de nouveau.

Informations connexes

- Page de support de Cisco Security Manager
- Page de support de Detection System de Cisco Intrusion
- Support et documentation techniques - Cisco Systems