Directeur de la sécurité 4.3 : Problèmes communs et solutions IPS

Contenu

Introduction

Ce document décrit des problèmes courants et des solutions aux questions du Système de protection contre les intrusions Cisco (IPS) dans le Cisco Security Manager.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations dans ce document sont basées sur la version 4.3 de Cisco Security Manager.

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.

Produits connexes

Ce document décrit des problèmes courants produits dans le Cisco Security Manager 4.3. Tandis que ce document se concentre sur la version 4.3 de Cisco Security Manager, il est possible que les mêmes problèmes et solutions s'appliquent à d'autres versions aussi bien.

Ne peut pas se connecter à l'IPS

Problème

Vous pouvez plus ne se connecter à l'IPS par le Cisco Security Manager. Cependant, vous pouvez se connecter au Protocole Secure Shell (SSH) et au gestionnaire de périphériques IPS (IDM) du serveur de Cisco Security Manager.

Solution

Vérifiez que l'IPS utilise un certificat du courant X.509. Exécutez la commande de **show version à l'**IPS CLI afin de vérifier la version du certificat. Si le certificat a expiré, exécutez la commande de générer-**clé de tls** afin d'obtenir un nouveau certificat. Après que vous génériez la clé, importez le certificat IPS.

Capteur d'AIP SSM non identifié après mise à jour à 7.1(6)E4

Problème

Après que vous amélioriez votre module d'Advanced Inspection and Prevention Security Services Module de Cisco ASA (AIP SSM) à la version 7.1(6)E4 dans la version 4.3 de Cisco Security Manager, le Cisco Security Manager n'identifie pas le capteur d'AIP SSM.

Solution

Afin de résoudre ce problème, vous devez installer le Service Pack 1 de version 4.3 de Cisco Security Manager, ou le Service Pack 2, sur le serveur de Cisco Security Manager de sorte qu'il prenne en charge votre AIP SSM avec les 7.1 IPS de logiciel.

Signatures IPS pas automatiquement mises à jour au cours du

délai de grâce

Problème

Le Cisco Security Manager ne met pas à jour automatiquement votre événement de signatures IPS bien que votre IPS ait lieu toujours à l'intérieur du délai de grâce.

Solution

Le Cisco Security Manager ne met pas à jour des signatures automatiquement si le capteur a lieu au cours du délai de grâce. Afin de résoudre ce problème, choisissez les **outils > appliquent des mises à jour IPS** dans l'interface de Cisco Security Manager pour mettre à jour manuellement les signatures.

Grand nombre de demandes RADIUS aux périphériques IPS

Problème

Vous voyez un grand nombre de demandes RADIUS de Cisco Security Manager à vos périphériques IPS.

Solution

Cette question se produit quand le Cisco Security Manager vote rapidement les périphériques surveillés. Par défaut, les versions affectées de la caractéristique de surveillance d'événement (concours complet) sur le Cisco Security Manager peuvent tenter de voter les périphériques surveillés plusieurs fois par seconde. Si d'autres caractéristiques de surveillance de Cisco Security Manager (les santés et le moniteur de performances et/ou le gestionnaire d'état) sont activées, les balayages de périphérique supplémentaire se produisent.

Afin de résoudre ce problème, vous pouvez changer le temps d'attente par défaut (intervalle de sommeil). L'intervalle par défaut de sommeil entre les balayages de périphérique est placé à 250ms par défaut. Cette valeur peut être changée manuellement à une plus grande, plus raisonnable valeur. Afin de changer la valeur de temps d'attente, éditez le fichier communication.properties sur le serveur de Cisco Security Manager ; ce fichier se trouve au > < NMSROOT \ *MDC* \ concours complet \ config \ communication.properties.

Dans le fichier communication.properties, remplacez SLEEP_INTERVAL_SYNCH_CALLS=250WITH SLEEP_INTERVAL_SYNCH_CALLS=2000.

> **Note**: La valeur est spécifiée en quelques millisecondes (ms) ; donc, 2000 égalise à 2 secondes.

> **Attention** : Précaution d'usage quand vous éditez ce fichier. Les modifications à ceci fichier

autre que celui répertorié ci-dessus peuvent entraîner des effets non souhaités au Cisco Security Manager.

Après que vous changiez et sauvegardiez le fichier, assurez que toutes les applications cliente de Cisco Security Manager sont fermées, et puis redémarrent le service de gestionnaire de démon de Cisco Security Manager (CRMDmgtd).

Informations connexes

- Installation du Cisco Security Manager 4.3 et guide de mise à jour
- Support et documentation techniques - Cisco Systems