IPS 5.x et version ultérieure : Différentes méthodes de surveillance des événements

Contenu

Introduction

Ce document fournit de diverses méthodes pour surveiller les événements IPS.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations dans ce document sont basées sur IPS 5.x et plus tard.

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.

Méthodes de moniteur les événements IPS

Actuellement, il y a quatre options pour surveiller les capteurs :

1. Le Manager Express IPS (IME) est fourni par le téléchargement logiciel dans Cisco.com. Cette application peut s'abonner sécurisé au capteur IPS avec SDEE et récupérer les événements/logs qui ont été générés en raison de toutes les questions ou signatures qui se sont déclenchées en raison d'une correspondance.Le gestionnaire de périphériques IPS (IDM) s'appelle quand vous accédez au capteur directement par HTTPS.Visualisez la mémoire d'événement directement sur le capteur avec les outils de surveillance de surveillance IDM ou d'événement IME. IDM et IME sont les solutions non valides si vous devez enregistrer le long terme d'événements car le stock d'événement local du capteur est une mémoire tampon circulaire du Mo 30 et commence à l'overwite lui-même une fois les 30 que limite de Mo est atteint. Cette limite est non-configurable.
2. Utilisez un périphérique CS-MARS afin de par habitude tirer et corréler les événements du capteur. Le CS-MARS emploie le protocole SDEE afin d'établir une connexion sécurisée au capteur pour récupérer les événements et récupère de nouveaux événements toutes les quelques secondes.Entrez en contact avec votre pour en savoir plus de l'équipe chargée du compte/reseller/SE si vous êtes intéressé par la démonstration-ing le périphérique CS-MARS.Pour les périphériques 5.x et 6.x de Cisco IPS, TROUBLE des tractions les logs avec SDEE au-dessus de SSL. Par conséquent, le MARS doit avoir accès HTTPS au capteur. Afin de préparer le capteur, vous devez permettre le trafic HTTPS de la station de Gestion IDM/IME, et vous assurez que l'adresse IP du MARS est définie comme hôte permis sur le capteur.
```
sensor#conf t
 sensor(config)#service host
 sensor(config-hos)#network-settings
 sensor(config-hos-net)#access-list x.x.x.x/subnet_mask
 sensor(config-hos-net)#exit
 sensor(config-hos)#exit
 Apply Changes?[yes]:
 sensor(config)#
```
3. Surveillez les événements avec l'IEV. Le visualisateur d'événements d'ID est une application basée sur Java qui te permet de visualiser et gérer des alarmes pour jusqu'à cinq capteurs. Avec le visualisateur d'événements d'ID vous pouvez se connecter à et des alarmes de vue en temps réel ou dans des fichiers journal importés. Vous pouvez configurer des filtres et des vues pour vous aider à gérer les alarmes. Vous pouvez également importer et exporter des données d'événement pour l'analyse approfondie. Comme le MARS, IEV établit une connexion sécurisée au capteur et récupère des événements toutes les quelques secondes. L'IEV enregistre ces événements dans une base de données sur le serveur sur lequel IEV est installé. Le DB est inclus avec IEV et installé avec l'application. Clic IEV afin de télécharger.**Remarque:** La documentation pour IEV est trouvée par le menu Help après que vous l'installiez. Le readme contient les informations d'installation.
4. Configurez les signatures sur votre capteur pour avoir une action de demande-SNMP-**déroutement** et pour configurer le capteur pour envoyer les déroutements à un serveur SNMP. Vous pouvez alors utiliser ce serveur pour transmettre par relais les messages comme Syslog à un autre ordinateur.Le SNMP est un protocole de la couche applicative qui facilite l'échange des informations de Gestion entre les périphériques de réseau. Le SNMP permet à des administrateurs réseau de gérer des performances du réseau, découverte et de résoudre des problèmes de réseau, et le plan pour la croissance de réseau.Le SNMP est un protocole simple de demande/réponse. Le système d'administration de réseaux émet une demande, et les périphériques gérés renvoient des réponses. Ce comportement est mis en application avec l'utilisation d'une de quatre opérations de protocole :ObtenezGetNextPlacezDéroutementVous pouvez configurer le capteur pour surveiller par

SNMP. Le SNMP définit une méthode standard pour que les stations de Gestion de réseau surveillent les santés et le statut de beaucoup de types de périphériques, qui inclut des Commutateurs, des Routeurs, et des capteurs.

Informations connexes

- Détecteurs de la gamme Cisco IPS 4200
- Système de protection contre les intrusions Cisco
- Notes de terrain relatives aux produits de sécurité (détection y compris d'intrusion de CiscoSecure)
- Support et documentation techniques - Cisco Systems