IPS 5.x en hoger: Diverse bewakingsmethoden

Inhoud

Inleiding

Dit document biedt verschillende methoden om de IPS-gebeurtenissen te controleren.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op IPS 5.x en hoger.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Methoden voor het bewaken van de IPS-gebeurtenissen

Op dit moment zijn er vier opties voor het bewaken van de sensoren:

1. IPS Manager Express (IME) is beschikbaar van softwaredownloads in Cisco.com. Deze toepassing kan zich veilig op de IPS-sensor abonneren en de gebeurtenissen/logboeken ophalen die zijn gegenereerd als resultaat van problemen of handtekeningen die zijn

afgevuurd door een match.IPS Apparaatbeheer (IDM) wordt opgeroepen wanneer u de sensor rechtstreeks benadeelt via HTTPS.Bekijk de gebeurtenis-winkel rechtstreeks op de sensor met de gereedschappen voor bewaking van IDM of IME Event Monitoring. IDM en IME zijn geen geldige oplossingen als u de gebeurtenissen op lange termijn moet opslaan, aangezien de lokale eventopslag van de sensor een circulaire buffer van 30 MB is en zichzelf begint te overschrijden zodra de grens van 30 MB is bereikt. Deze limiet is niet aanpasbaar.

2. Gebruik een CS-MARS-apparaat om de gebeurtenissen van de sensor routinematig te trekken en te correleren. Het CS-MARS gebruikt het SDEE-protocol om een veilige verbinding met de sensor tot stand te brengen om de gebeurtenissen terug te halen en om elke paar seconden nieuwe gebeurtenissen te vinden.Neem voor meer informatie contact op met het accountteam/de wederverkoper/SE als u het CS-MARS-apparaat wilt demonteren.Voor Cisco IPS 5.x en 6.x apparaten trekt MARS de logbestanden met SDEE over SSL aan. Daarom moet MARS toegang hebben tot de sensor. Om de sensor voor te bereiden moet u HTTPS-verkeer vanuit het IDM/IME-beheerstation toestaan en ervoor zorgen dat het IP-adres van MARS wordt gedefinieerd als een toegestane host op de sensor.

```
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. Volg de gebeurtenissen bij het IEV. IDS Event Viewer is een op Java gebaseerde toepassing die u in staat stelt alarmen voor maximaal vijf sensoren te bekijken en te beheren. In het DIS Event Viewer kunt u in real-time of in geïmporteerde logbestanden verbinding maken met en alarmen weergeven. U kunt filters en weergaven configureren om u te helpen de alarmen te beheren. U kunt ook gegevens over gebeurtenissen importeren en exporteren voor verdere analyse. Zoals MARS, stipuleert IEV een veilige verbinding met de sensor en wint elke paar seconden gebeurtenissen terug. Het IEV slaat deze gebeurtenissen op in een database op de server waarop IEV is geïnstalleerd. De OB is opgenomen bij IEV en wordt samen met de aanvraag geïnstalleerd. Klik op IEV om het te downloaden.**Opmerking:** De documentatie voor IEV is te vinden in het Help -menu nadat u het hebt geïnstalleerd. Het leesprogramma bevat installatieinformatie.
4. Configureer de handtekeningen op uw sensor om een actie van **request-snmp-val** te hebben en stel de sensor in om de vallen naar een SNMP server te sturen. U kunt deze server dan gebruiken om de berichten als syslogs naar een andere machine door te geven.SNMP is een protocol op de toepassingslaag dat de uitwisseling van beheerinformatie tussen netwerkapparaten vergemakkelijkt. Met SNMP kunnen netwerkbeheerders netwerkprestaties beheren, netwerkproblemen identificeren en oplossen en netwerkgroei plannen.SNMP is een eenvoudig verzoek/responsprotocol. Het netwerk-beheersysteem geeft een verzoek uit, en de beheerde apparaten geven reacties terug. Dit gedrag wordt uitgevoerd met behulp van een van de vier protocoloperaties:StapVolgende verkrijgenInstellenTrapU kunt de sensor configureren voor controle door SNMP. SNMP definieert een standaardmanier voor netwerkbeheerstations om de status en status van veel soorten apparaten te bewaken, waaronder switches, routers en sensoren.

Gerelateerde informatie

- Cisco IPS 4200 Series sensoren
- Cisco-inbraakpreventiesysteem
- Security meldingen uit het veld (inclusief Cisco Secure Inbraakdetectie)
- Technische ondersteuning en documentatie – Cisco Systems