Connection-gebeurtenissen lijken te verdwijnen uit het FireSIGHT Management Center

Inhoud

Inleiding

In dit document wordt beschreven hoe u de oorzaak van de verbinding kunt bepalen en het probleem kunt oplossen wanneer er verbindingsgebeurtenissen uit het FireSIGHT Management Center verdwijnen nadat het systeem enkele dagen heeft gedraaid. Dit kan gebeuren vanwege de configuratie-instellingen van het beheercentrum.

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben van FireSIGHT Management Center.

Gebruikte componenten

De informatie in dit document is gebaseerd op deze hardware- en softwareversies:

- FireSIGHT Management Center
- Software versie 5.2 of 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.

Problemen oplossen

Stap 1: Bepaal het aantal opgeslagen gebeurtenissen

Om het aantal Connection Events te bepalen dat is opgeslagen op een FireSIGHT Management Center,

1. Kies **Analyse > Verbindingen > Tabelweergave van Verbindingsgebeurtenissen**.
2. Breid het tijdvenster uit tot een breed bereik dat alle huidige gebeurtenissen omvat, bijvoorbeeld 12 maanden.
3. Let op het totale aantal rijen aan de onderkant van de pagina. Klik op de laatste pagina en noteer de tijdstempel van de laatst beschikbare Connection Event.

Deze informatie geeft u een idee van hoeveel en hoe lang u in staat bent om Connection Events met uw huidige configuratie te behouden.

Stap 2: De vastlegging-optie bepalen

Bekijk welke verbindingen worden vastgelegd en waar in de flow die verbindingen worden vastgelegd. U dient de verbindingen te registreren in overeenstemming met de beveiligings- en nalevingsbehoeften van uw organisatie. Als uw doel is om het aantal gebeurtenissen dat u genereert te beperken, laat alleen vastlegging toe voor de regels die van cruciaal belang zijn voor uw analyse. Als u echter een brede weergave van uw netwerkverkeer wilt, kunt u vastlegging inschakelen voor aanvullende toegangscontroleregels of voor de standaardactie. U kunt Verbindingsvastlegging voor niet-essentieel verkeer uitschakelen om te helpen verbindingsgebeurtenissen voor een langere periode te behouden.

> **Tip**: Om de prestaties te optimaliseren, raadt Cisco u aan het begin of het einde van de verbinding, maar niet beide, te registreren.

> **Opmerking:** Voor één verbinding bevat de end-of-connection-gebeurtenis alle informatie in de start-of-connection-gebeurtenis, evenals informatie die tijdens de duur van de sessie is verzameld. Voor Regels Vertrouwen en toestaan wordt aangeraden dat End-of-Connection wordt gebruikt.

In dit schema worden de verschillende registratieopties voor elke regelactie beschreven:

Regel Actie of vastlegging optie	Log bij begin	Log aan einde
Trust (vertrouwen) Standaardactie: Trust (vertrouwen)	X	X
Allow (toestaan) Standaardactie: Inbraak	X	X
Standaardactie: Detectie Monitor (bewaken)		X (verplicht)
Block (blokkeren) Block with reset (blokkeren met reset)	X	
Standaardactie: Block (blokkeren) Interactive Block (interactief blokkeren)	X	X (indien overgeslagen)

Interactive Block with reset (interactief blokkeren met reset)	
Beveiligingsinformatie	X

Stap 3: De grootte van de verbindingsdatabase aanpassen

Verbindingsgebeurtenissen worden gesnoeid afhankelijk van de instelling Maximum Connection Events in het systeembeleid. Zo wijzigt u de instelling:

1. Kies **Systeem > Lokaal > Systeembeleid**.
2. Klik op het *potloodpictogram* om het momenteel toegepaste beleid te bewerken.
3. Kies **Database > Verbindingsdatabase > Maximum aantal verbindingsgebeurtenissen**.
4. Wijzig de waarde voor **Maximum Connection Events**.
5. Klik op **Beleid opslaan en Afsluiten** en **pas** het beleid vervolgens op uw apparatuur toe.

De maximale hoeveelheid Connection Events die kan worden opgeslagen, is afhankelijk van het Management Center model:

> **Opmerking:** De maximale gebeurtenislimiet wordt gedeeld tussen verbindingsgebeurtenissen en Security Intelligence-gebeurtenissen; de som van de ingestelde maxima voor de twee gebeurtenissen kan de maximale gebeurtenislimiet niet overschrijden.

Management Center-model	Maximum aantal gebeurtenissen
FS750, DC750	50 miljoen
FS1500, DC1500	100 miljoen
SF200	300 miljoen
FS3500, DC3500	500 miljoen
SF400	1 miljard
Virtuele applicatie	10 miljoen

> **Voorzichtig:** Een verhoging van de databaselimieten kan een negatief effect hebben op de prestaties van het apparaat. Om de prestaties te verbeteren, moet u gebeurtenislimieten aanpassen aan het aantal gebeurtenissen waarmee u regelmatig werkt.

Voor widgets die gebeurtenistellingen over een tijdbereik weergeven, het totale aantal gebeurtenissen mogelijk niet het aantal gebeurtenissen weergeven waarvoor gedetailleerde gegevens beschikbaar zijn in de gebeurtenisviewer. Dit komt voor omdat het systeem soms oudere gebeurtenisdetails snoeit om schijfruimte gebruik te beheren. Om het voorkomen van het snoeien van gebeurtenisdetail te minimaliseren, kunt u gebeurtenisregistreren verfijnen om slechts die gebeurtenissen te registreren die voor uw plaatsing het belangrijkst zijn.

Gerelateerde informatie

- Gebeurtenislimieten database configureren
- Technische ondersteuning en documentatie – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.