ASA Embedded Event Manager configuratievoorbeeld

Inhoud

Inleiding

In dit document wordt Embedded Event Manager (EEM) beschreven, een tool voor probleemoplossing die is toegevoegd aan Adaptieve security applicatie (ASA) versie 9.2(1). De functionaliteit is vergelijkbaar met Cisco IOS? gebaseerd EEM. Het is een krachtige manier om CLI-opdrachten te gebruiken op basis van ASA-gebeurtenissen (syslogs) en de uitvoer op te slaan. Dit document bevat een inleiding op het onderdeel en een aantal voorbeelden van EEM-applets.

Voorwaarden

Vereisten

Het gebruik van EEM vereist dat de ASA in één contextmodus is geconfigureerd.

Gebruikte componenten

De informatie in dit document is gebaseerd op ASA versie 9.2(1) of hoger.

Richtsnoeren en beperkingen

In dit deel zijn de richtsnoeren en beperkingen voor deze functie opgenomen.

Richtsnoeren voor Context

EEM wordt momenteel alleen ondersteund op ASA-firewalls die in één contextmodus werken. Firewalls in meerdere contextmodus zijn op dit moment niet ondersteund.

Richtlijnen voor firewallmodus

EEM wordt momenteel ondersteund in zowel routinematige als transparante firewallmodi.

Aanvullende richtsnoeren

- Terwijl het apparaat crasht, is de status van de ASA in het algemeen onbekend. Sommige opdrachten zijn mogelijk niet veilig om te starten wanneer de ASA in deze toestand verkeert.
- De naam van een evenementenbeheerapplicatie kan geen spaties bevatten.
- U kunt de parameters Geen gebeurtenis en Crashinfo gebeurtenis niet wijzigen.
- De prestaties kunnen worden beïnvloed doordat syslog-berichten naar het EEM worden gestuurd om te worden verwerkt.
- De standaardinvoer is **geen** uitvoer voor elke gebeurtenis Manager-toepassing. Om de standaardinvoer te wijzigen, moet u een andere uitvoerwaarde invoeren.
- Mogelijk is er slechts één uitvoeroptie gedefinieerd voor elke applicatie van de Event Manager.

Configureren

De opdracht **voor** de **toepassing** van de **gebeurtenis manager** maakt/bewerkt een applicatie die gebeurtenissen met handelingen en uitvoer verbindt. Het *<name>* is beperkt tot 32 tekens en kan geen spaties hebben. Dit voert een gebeurtenis Manager toe applet submode.

```
ASA(config)# [no] event manager applet
```

Er kan een **beschrijving** aan een applet worden toegevoegd. Dit is uitsluitend ter informatie. <*text*> is beperkt tot 256 tekens.

```
ASA(config-applet)# [no] description
```

Event Configuratie

Er kunnen meerdere gebeurtenissen worden toegevoegd aan een applet dat de applet activeert om de handelingen aan te halen die er op zijn ingesteld. Ze worden gedefinieerd met het trefwoord **voor** de **gebeurtenis**. Voor elke applet kunnen meerdere gebeurtenissen worden ingesteld.

Syslog Events

Het eerste type gebeurtenis dat wordt ondersteund is **syslog**. ASA gebruikt syslogID's om syslogs te identificeren die een applet activeren. Dit wordt voltooid door het sleutelwoord ID, dat een enkele syslog of een bereik kan zijn. Het optionele trefwoord geeft het aantal keer aan dat de syslogan moet voorkomen voordat de applet kan worden opgeroepen (standaard is 1). Het optionele **punt** sleutelwoord geeft de hoeveelheid tijd aan, in seconden, die de gebeurtenis moet plaatsvinden. De frequentie van de aanroeping van de applet wordt beperkt tot ten hoogste één keer de geconfigureerde periode. Een **optreden** van 5 met een **periode** van 30, betekent dat de syslog 5 keer binnen 30 seconden moet optreden voordat de gebeurtenis geactiveerd wordt. Als de slang 11 keer in 30 seconden voorkomt, wordt de applet slechts één keer geactiveerd. Een waarde van 0 voor **periode** betekent dat geen periode wordt gedefinieerd.

Er kunnen meerdere syslogs worden ingesteld, maar de bereiken kunnen niet overlapen.

```
ASA(config-applet)# [no] event syslog id
```

```
ASA(config-applet)# no event syslog id
```

De waarde *<n>* heeft een toegestaan bereik van 1 tot 4294967295. De waarde van de **periode** <seconden> heeft een toegestaan bereik van 0 tot 604800. Een 0 (nul) waarde betekent dat er geen periode is ingesteld.

voorbeeld SLOGgebeurtenissen

In dit voorbeeld neemt EEM actie wanneer het een geheugenbloktoestand detecteert. Als de

beschikbare 1550 byte-blokken uitgeput raken, worden de **blokken** bijeengebracht, met **1550-stort** en opgeslagen op de schijf. Dat doet hij tenminste elke 10 minuten.

```
event manager applet depletedblock
description "Take a snapshot of block output when it is depleted"
event syslog id 321007 period 600
action 1 cli command "show blocks pool 1550 dump"
output file rotate 10
```

Periodieke gebeurtenissen

EEM kan ook worden ingesteld om regelmatig een actie uit te voeren. Wanneer u een op timer gebaseerde gebeurtenis vormt, gebruik het **timer** sleutelwoord in de eventconfiguratie. Er zijn 3 opties op timer:

- absoluut - De eerste timer is een **absolute** timer die de applet één keer per dag op het opgegeven tijdstip activeert en automatisch opnieuw start.
  `ASA(config-applet)# **[no] event timer absolute time**`

  `ASA(config-applet)# **no event timer absolute**`
- aftellen - De tweede timer is een **afteltimer** die de applet eenmaal activeert en niet opnieuw start, tenzij verwijderd en opnieuw toegevoegd.
  `ASA(config-applet)# **[no] event timer countdown time**`

  `ASA(config-applet)# **no event timer countdown**`
- waakhond - De derde timer is een **waakhond**-timer die de applet eenmaal per geconfigureerde periode triggt en automatisch opnieuw start.
  `ASA(config-applet)# **[no] event timer watchdog time**`

  `ASA(config-applet)# **no event timer watchdog**`

Voorbeeld van periodieke gebeurtenissen

Bijvoorbeeld, deze gebeurtenis configuratie pings 192.168.1.100 elke 1 minuut. Dit kan worden gebruikt om er zeker van te zijn dat een VPN-tunnel ingeschakeld en gebruiksklaar is, zelfs tijdens perioden van onklaar verkeer. De timer voor de **horlogetimer** gebruikt om elke 60 seconden uit te voeren.

```
event manager applet period-event
description "Run a command once per minute"
event timer watchdog time 60
action 0 cli command "ping 192.168.1.100"
output none
```

In dit applet wordt de informatie over de toewijzing van geheugenblokken elk uur opgeslagen en wordt de uitvoer naar een roterende set logbestanden geschreven, omdat deze de waarde van een dag bevat. De timer voor de **waakhond** wordt elke 1 uur uitgevoerd.

```
event manager applet blockcheck
description "Log block usage"
event timer watchdog time 3600
output rotate 24
action 1 cli command "show blocks old"
```

Deze applets blokkeren de gegeven interface (Gig 0/0) tussen middernacht en 3 uur. Er wordt **absolute** timer gebruikt om één keer per dag uit te voeren.

```
event manager applet disableintf
description "Disable the interface at midnight"
event timer absolute time 0:00:00
output none
action 1 cli command "interface GigabitEthernet 0/0"
action 2 cli command "shutdown"
action 3 cli command "write memory"
!
event manager applet enableintf
description "Enable the interface at 3am"
event timer absolute time 3:00:00
output none
action 1 cli command "interface GigabitEthernet 0/0"
action 2 cli command "no shutdown"
action 3 cli command "write memory"
```

Handmatige gebeurtenis

Deze EEM-applets kunnen ook handmatig worden ingeroepen. Om dit te doen moet de applet **gebeurtenis geen** vormen. Voer de opdracht **voor** de **beheerder** in om een applet handmatig uit te voeren, gevolgd door de naam van de applet. Als het applet voor om het even welke gebeurtenis trigger mechanisme behalve "geen" is ingesteld, genereert de poging om het handmatig uit te voeren een fout. Met behulp van een van de voorgaande voorbeelden, "depletedblock", zie je:

```
ASA# event manager run depletedblock
ERROR: Applet not configured with 'event none'
```

Handmatig Event Voorbeeld

Handmatige gebeurtenissen kunnen op dezelfde manier als een macro worden gebruikt. Bijvoorbeeld, zou een handgebeurtenis kunnen worden gebruikt om een paar opdrachten in volgorde uit te voeren. In dit voorbeeld, redt het de configuratie, pings een gastheer, en ontruimt alle slangen.

```
event manager applet clean-up
event none
action 0 cli command "write mem"
action 1 cli command "ping 192.168.1.100"
action 2 cli command "clear shun"
output none
```

Crash Event

De gebeurtenis crashinformatie leidt tot een applet wanneer er een ongeluk op de ASA plaatsvindt. Ongeacht de waarde van de opdracht **uitvoeren**, worden de opdrachten in de **actie** gericht op het crashinformatie-bestand. De output wordt gegenereerd voordat het aandeel van de crashinformatie in **de** toontechnologie is gegenereerd.

> **Waarschuwing**: Wanneer de ASA crasht, is de status van het doosje over het algemeen onbekend. Sommige CLI-opdrachten zijn mogelijk niet veilig om te kunnen gebruiken wanneer de unit in deze toestand verkeert.

```
ASA(config-applet)# [no] event crashinfo
```

Activeringsconfiguratie

Als het apparaat is geactiveerd, worden de handelingen op het apparaat uitgevoerd. Elke **actie** heeft een verordening die wordt gebruikt om de volgorde van de acties te specificeren. Per applet kunnen meerdere acties worden ingesteld; maar elk voorschrift kan slechts eenmaal worden gebruikt . De opdrachten zijn typische CLI-opdrachten, zoals **showblokken**. De offertes worden ten zeerste aanbevolen, maar zijn niet vereist.

```
ASA(config-applet)# [no] action
```

```
ASA(config-applet)# no action
```

De waarde van de actie ID *<n>* heeft een bereik van 0 tot 4294967295. De waarde van de *<opdracht>*moet worden geciteerd, anders gebeurt er een fout als de opdracht uit meer dan één woord bestaat. De opdracht wordt uitgevoerd in configuratiemodus als een gebruiker met voorkeursniveau 15 (de hoogste). De opdracht aanvaardt geen input. als invoer wordt uitgeschakeld als de opdracht de optie **niet bevestigen** heeft. Dit dient te worden gebruikt omdat de opdrachten niet interactief worden verwerkt.

Uitvoerconfiguratie

De uitvoer van de acties kan naar een gespecificeerde locatie worden gericht via de uitvoeropdracht. Er kan slechts één uitvoerwaarde tegelijkertijd worden ingeschakeld. De standaardwaarde is **geen uitvoer**. Deze waarde wijst elke uitvoer van de actieopdrachten af.

```
ASA(config-applet)# [no] output none
```

De opdracht uitvoerconsole verstuurt de uitvoer van de actieopdrachten naar de console.

```
ASA(config-applet)# [no] output console
```

De opdracht Uitvoeren bestand leidt de uitvoer van de actieopdrachten naar bestanden. Er zijn vier opties die kunnen worden gebruikt. De **nieuwe** optie schrijft de uitvoer van de applet naar een nieuw bestand voor elke invocatie. De *bestandsnaam* heeft het formaat **eem-*<applet>*-*<timestamp>*.log**. Waar *<applet>* de naam van de applicatie is en *<timestamp>* is een gedateerd tijdstempel in het formaat van *YYYYYMMD-SHMS*.

```
ASA(config-applet)# [no] output file new
```

De optie **rotate** wordt gebruikt om een verzameling bestanden te maken die gedraaid zijn vergelijkbaar met het logrotatiemechanisme van Linux. Het bestandsindeling is **eem-*<applet>*-*<x>*.log**. Waar *<applet>* de naam van de applet is, en *<x>*is het bestandsnummer. Het laatste bestand wordt aangegeven door nummer 0 (nul) en het oudste bestand wordt aangegeven door het hoogste nummer (*<n>*-1). Wanneer een nieuw bestand moet worden geschreven, wordt het oudste bestand verwijderd en alle daaropvolgende bestanden worden genummerd voordat het 0ste bestand is geschreven.

```
ASA(config-applet)# [no] output file rotate
```

De rotatiewaarde *<n>* heeft een bereik van 2 tot 100.

De optie **overschrijven** wordt gebruikt om altijd de uitvoer van de actieopdracht naar één bestand te schrijven dat elke keer wordt ingekort.

```
ASA(config-applet)# [no] output file overwrite
```

De optie **toevoegen** wordt gebruikt om altijd de uitvoer van de actieopdracht naar één bestand te schrijven, maar dat bestand wordt elke keer toegevoegd.

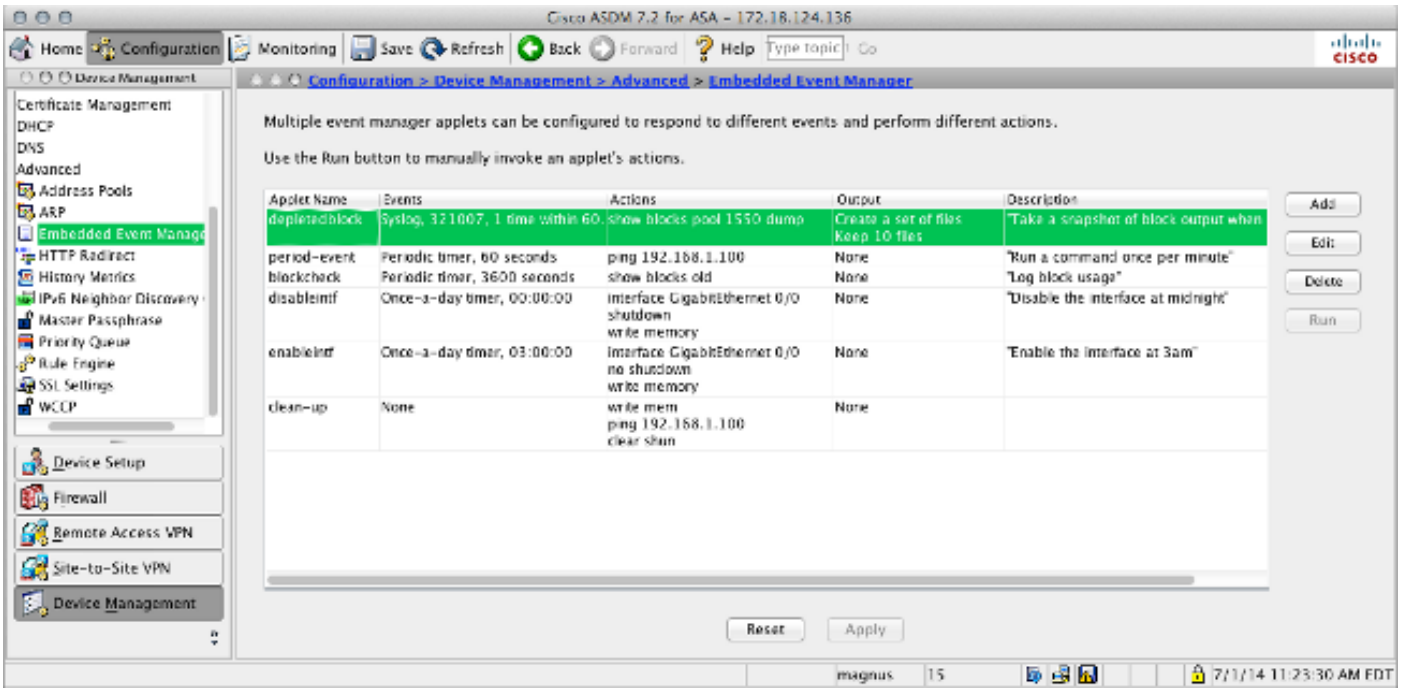
```
ASA(config-applet)# [no] output file append
```

Het *<filename>* argument is een lokale (te vergelijken met de ASA) bestandsnaam. De opdracht tot overschrijven kan ook **ftp** gebruiken:, **tftp:** en **smb :** gerichte bestanden.

ASDM-configuratie

EEM kan ook worden geconfigureerd vanuit ASDM. Kies **Configuratie > Apparaatbeheer > Geavanceerd > Ingesloten Event Manager**. In dit gedeelte van ASDM, kunt u uw EEM applets configureren met dezelfde parameters die eerder besproken zijn. Nadat u een applet hebt

gevormd, klik op **Toepassen** om de configuratie naar de ASA te duwen.



Verifiëren

Opdrachten in Exec-modus

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Al deze opdrachten worden in exec-modus gebruikt.

Deze opdracht toont de actieve configuratie van het eventbeheersysteem.

ASA# **show running-config event manager**

Deze opdracht voert een applicatie uit van een Event Manager die is ingesteld met **geen** gebeurtenis. Als u een applet draait dat niet is ingesteld met **gebeurtenis geen**, wordt er een fout gemeld.

ASA# **event manager run**

Deze opdracht geeft informatie over de geconfigureerde applets, die ook aantal hit's omvat, en het moment waarop de applet voor het laatst werd gebruiktASA# event manager applet period-event, hits 1, last 2014/07/01 10:51:52
last file none
event watchdog 60 secs, left 54 secs, hits 1, last 2014/07/01 10:51:52
action 0 cli command "ping 192.168.1.100", hits 1, last 2014/07/01 10:51:52Event Manager gebruikt de standaardtellers. Wegens beperkingen binnen deshow teller CLI, wordt het eem sleutelwoord gebruikt voor protocolfiltering.

ASA# show counters protocol eem De Output Interpreter Tool (alleen voor geregistreerde klanten) ondersteunt bepaalde opdrachten metshow. Gebruik de Output Interpreter Tool om een analyse te bekijken van de output van de opdracht show.

DebuggenVoer deze opdrachten in om de EEM te reinigen en de uitvoer weer te geven.Opmerking: Raadpleeg Important Information on Debug Commands (Belangrijke informatie over opdrachten met debug) voordat u opdrachten met debug opgeeft.

ASA# [no] debug event manager

ASA# show debug event managerProblemen oplossenEr is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie. Als het niet werkt zoals verwacht, gebruik de het debuggen en de verificatieronden in de vorige sectie om te bepalen of een fout is opgetreden.