Esempio di configurazione di ASA Embedded Event Manager

Sommario

Introduzione

In questo documento viene descritto Embedded Event Manager (EEM), uno strumento di risoluzione dei problemi aggiunto in Adaptive Security Appliance (ASA) versione 9.2(1). La funzionalità è simile a Cisco IOS? EEM. È un modo potente per eseguire i comandi CLI basati su eventi ASA (syslog) e salvare l'output. In questo documento viene fornita un'introduzione a questa funzionalità e ad alcune applet EEM di esempio.

Prerequisiti

Requisiti

Per utilizzare EEM, è necessario configurare l'ASA in modalità contesto singolo.

Componenti usati

Il riferimento delle informazioni contenute in questo documento è ASA versione 9.2(1) o successive.

Linee guida e limitazioni

In questa sezione sono riportate le linee guida e le limitazioni per questa funzionalità.

Linee guida per la modalità contesto

EEM è attualmente supportato solo sui firewall ASA in esecuzione in modalità contesto singolo. I firewall configurati in modalità contesto multiplo non sono attualmente supportati.

Linee guida per la modalità firewall

EEM è attualmente supportato in modalità firewall sia instradata che trasparente.

Linee guida aggiuntive

- Mentre l'unità si blocca, lo stato dell'ASA è generalmente sconosciuto. L'esecuzione di alcuni comandi potrebbe non essere sicura quando l'ASA è in questa condizione.
- Il nome di un'applet di gestione eventi non può contenere spazi.
- Non è possibile modificare i parametri degli eventi None e Crashinfo.
- Le prestazioni potrebbero risentirne perché i messaggi syslog vengono inviati all'EEM per l'elaborazione.
- L'output predefinito è **nessuno** per ciascuna applet di gestione eventi. Per modificare l'output predefinito, è necessario immettere un valore di output diverso.
- Per ogni applet di gestione eventi potrebbe essere definita una sola opzione di output.

Configurazione

Il comando **applet Gestione eventi** crea/modifica un'applet Gestione eventi, un processo che collega gli eventi alle azioni e all'output. Il valore di *<name>* è limitato a 32 caratteri e non può contenere spazi. In questo modo viene attivata la modalità secondaria di un'applet di Gestione eventi.

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

Èpossibile aggiungere una **descrizione** a un'applet. Questa operazione ha solo scopo informativo. <*text*> è limitato a 256 caratteri.

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

Configurazione evento

A un'applet possono essere aggiunti diversi eventi che attivano l'applet per richiamare le azioni configurate su di essa. Sono definiti con la parola chiave **event**. È possibile configurare più eventi per ogni applet.

Eventi Syslog

Il primo tipo di evento supportato è **syslog**. L'appliance ASA usa gli ID syslog per identificare i syslog che attivano un'applet. Questa operazione viene completata tramite la parola chiave id, che può essere un singolo syslog o un intervallo. La parola chiave **OCCUR** facoltativa indica il numero di occorrenze del syslog necessarie per richiamare l'applet (il valore predefinito è 1). La parola chiave facoltativa **period** indica la quantità di tempo, in secondi, in cui l'evento deve verificarsi. Limita la frequenza della chiamata dell'applet a non più di una volta il periodo configurato. Se **si verifica** il numero 5 con un **periodo** di 30, il syslog deve verificarsi 5 volte entro 30 secondi prima che l'evento venga attivato. Se il syslog si verifica 11 volte in 30 secondi, l'applet viene attivata una sola volta. Il valore 0 per **periodo** indica che non è definito alcun periodo.

Èpossibile configurare più syslog, ma gli intervalli non possono sovrapporsi.

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

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

Il valore **OCCURs** *<n>* ha un intervallo consentito compreso tra 1 e 4294967295. Il valore **period** <seconds> ha un intervallo consentito compreso tra 0 e 604800. Un valore 0 (zero) indica che non è configurato alcun periodo.

Esempio di eventi Syslog

In questo esempio, EEM interviene quando rileva una condizione di blocco di memoria insufficiente. Se i blocchi da 1550 byte disponibili si esauriscono, il **pool di blocchi show 1550**

viene raccolto e salvato sul disco. Lo fa, al massimo, una volta ogni 10 minuti.

```
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
```

Eventi periodici

EEM può inoltre essere configurato per eseguire un'azione periodicamente. Quando si configura un evento basato su timer, utilizzare la parola chiave **timer** nella configurazione degli eventi. Sono disponibili 3 opzioni basate sul timer:

- absolute - Il primo timer è un timer **assoluto** che attiva l'applet una volta al giorno all'ora specificata e si riavvia automaticamente.
  ```
  ASA(config-applet)# [no] event timer absolute time
  ```

  ```
  ASA(config-applet)# no event timer absolute
  ```
- conto alla rovescia - Il secondo timer è un timer di **conto alla rovescia** che attiva l'applet una volta e non si riavvia a meno che non venga rimosso e riaggiunto.
  ```
  ASA(config-applet)# [no] event timer countdown time
  ```

  ```
  ASA(config-applet)# no event timer countdown
  ```
- watchdog - Il terzo timer è un timer di **watchdog** che attiva l'applet una volta per periodo configurato e si riavvia automaticamente.
  ```
  ASA(config-applet)# [no] event timer watchdog time
  ```

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

Esempio di eventi periodici

Ad esempio, questa configurazione di evento esegue il ping 192.168.1.100 ogni 1 minuto. Questa opzione può essere utilizzata per garantire che un tunnel VPN sia mantenuto attivo e operativo anche nei periodi di traffico inattivo. Utilizza il timer **watchdog** per l'esecuzione ogni 60 secondi.

```
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
```

Questa applet registra le informazioni di allocazione dei blocchi di memoria ogni ora e scrive

l'output in un set rotante di file di registro, poiché conserva l'equivalente di un giorno di registri. Utilizza il timer **watchdog** per l'esecuzione ogni 1 ora.

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

Queste applet disabilitano l'interfaccia specificata (Gig 0/0) tra la mezzanotte e le 3 del mattino. Utilizza il timer **assoluto** per l'esecuzione una volta al giorno.

```
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"
```

Evento manuale

Queste applet EEM possono inoltre essere richiamate manualmente. A tale scopo, l'applet deve configurare l'**evento none (nessuno)**. Per eseguire manualmente un'applet, immettere il comando **run manager eventi** seguito dal nome dell'applet. Se l'applet è configurata per qualsiasi meccanismo di attivazione degli eventi a parte 'none', il tentativo di eseguirla manualmente genererà un errore. Utilizzando uno degli esempi precedenti, 'depletedblock', è possibile visualizzare:

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

Esempio di evento manuale

Gli eventi manuali possono essere utilizzati in modo simile a una macro. Ad esempio, è possibile utilizzare un evento manuale per eseguire alcuni comandi in ordine. In questo esempio viene salvata la configurazione, viene eseguito il ping di un host e vengono cancellati tutti gli shun.

```
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
```

Evento Crash

L'evento **crashinfo** attiva un'applet quando si verifica un arresto anomalo sull'appliance ASA. Indipendentemente dal valore del comando **output**, i comandi **action** vengono indirizzati al file crashinfo. L'output viene generato prima della parte **show tech** di crashinfo.

> **Avviso:** Quando l'appliance ASA si blocca, lo stato del dispositivo è in genere sconosciuto. Alcuni comandi CLI potrebbero non essere sicuri quando l'unità si trova in queste condizioni.

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

Configurazione azione

Quando l'applet viene attivata, vengono eseguite le azioni sull'applet. Ogni **azione** dispone di un ordinale utilizzato per specificare l'ordine delle azioni. È possibile configurare più azioni per applet. ma ogni ordinale può essere utilizzato una sola volta. I comandi sono comandi CLI standard, ad esempio **show block**. Le virgolette sono consigliate, ma non obbligatorie.

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

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

Il valore dell'identificatore di azione *<n>* è compreso tra 0 e 4294967295. Il valore di *<command>* deve essere racchiuso tra virgolette, altrimenti si verificherà un errore se il comando è composto da più parole. Il comando viene eseguito in modalità di configurazione come utente con il livello di privilegio 15 (il più alto). Il comando potrebbe non accettare input; as input verrà disattivato se un comando ha l'opzione **noconfirm**. Da utilizzare poiché i comandi non vengono elaborati in modo interattivo.

Configurazione di output

L'output delle azioni può essere indirizzato a una posizione specificata tramite il comando **output**. È possibile abilitare un solo valore di output alla volta. Il valore predefinito è **output none (nessuno)**. Questo valore elimina qualsiasi output dei comandi di azione.

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

Il comando **output console** invia l'output dei comandi di azione alla console.

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

Il comando **output file** indirizza l'output dei comandi di azione ai file. È possibile utilizzare quattro opzioni. La **nuova** opzione scrive l'output dell'applet in un nuovo file per ogni chiamata. Il *nome file*

ha il formato **eem-*<applet>*-*<timestamp>*.log**. Dove *<applet>* è il nome dell'applet e *<timestamp>* è un timestamp datato nel formato *AAAAMMGG-hhmmss*.

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

L'opzione **rotate** (rotazione) viene usata per creare un insieme di file ruotati in modo simile al meccanismo di rotazione log di Linux. Il formato del nome file è **eem-*<applet>*-*<x>*.log**. Dove *<applet>* è il nome dell'applet e *<x>* è il numero di file. Il file più recente è indicato dal numero 0 (zero), mentre il file meno recente è indicato dal numero più alto (*<n>*-1). Quando un nuovo file deve essere scritto, il file meno recente viene eliminato e tutti i file successivi vengono rinumerati prima della scrittura del file 0.

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

Il valore di rotazione *<n>* è compreso tra 2 e 100.

L'opzione **overwrite** viene utilizzata sempre per scrivere l'output del comando action in un singolo file che viene troncato ogni volta.

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

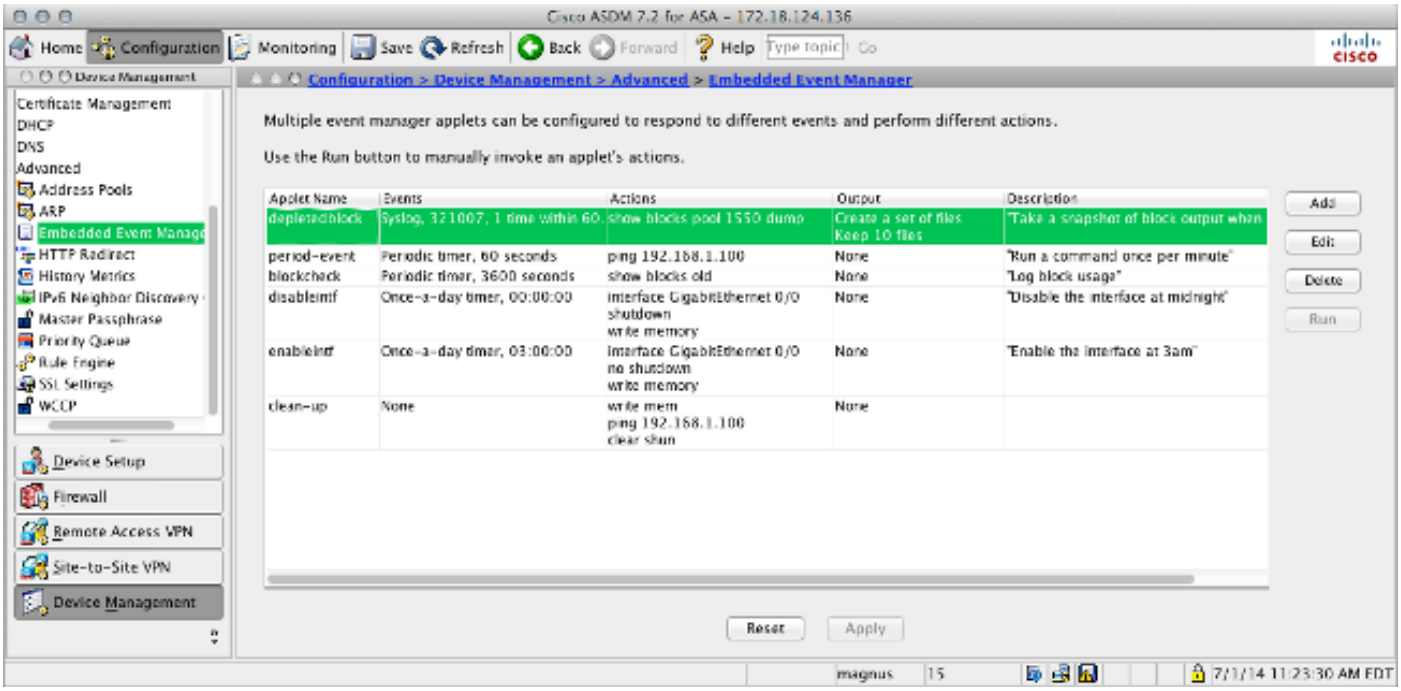
L'opzione **append** viene utilizzata sempre per scrivere l'output del comando action in un singolo file, ma tale file viene aggiunto a ogni volta.

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

L'argomento *<filename>* è un nome di file locale (dell'appliance ASA). Il comando overwrite può inoltre utilizzare **ftp**:, **tftp:** e **pmi:** file di destinazione.

Configurazione ASDM

EEM può essere configurato anche dall'interno di ASDM. Scegliere **Configurazione > Gestione dispositivi > Avanzate > Gestore eventi integrato**. In questa sezione di ASDM, è possibile configurare le applet EEM con gli stessi parametri descritti in precedenza. Dopo aver configurato un'applet, fare clic su **Apply** per eseguire il push della configurazione sull'appliance ASA.



Verifica

Comandi modalità di esecuzione

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Tutti questi comandi vengono utilizzati in modalità di esecuzione.

Questo comando mostra la configurazione corrente del sistema di gestione degli eventi.

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

Questo comando esegue un'applet di gestione eventi configurata con l'opzione **evento none**. Se si esegue un'applet che non è stata configurata con l'**evento none** (nessuno), viene segnalato un errore.

```
ASA# event manager run
```

Con questo comando vengono visualizzate informazioni sulle applet configurate, inclusi il numero di accessi e la data dell'ultimo richiamo dell'appletASA# 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 10:51:52Gestione eventi utilizza i contatori standard. A causa dei limiti della CLI delcontatore show, la parola chiave eem viene usata per filtrare il protocollo.

ASA# show counters protocol eem Lo strumento Output Interpreter (solo utenti registrati) supporta alcuni comandishow. Usare lo strumento Output Interpreter per visualizzare un'analisi

dell'output del comando show.

DebugImmettere questi comandi per eseguire il debug di EEM e visualizzare l'output.Nota: consultare le informazioni importanti sui comandi di debug prima di usare i comandi di debug.

```
ASA# [no] debug event manager
```

ASA# show debug event manager**Risoluzione dei problemi**Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione. Se non funziona come previsto, utilizzare i passaggi di debug e verifica elencati nella sezione precedente per determinare se si è verificato un errore.