La acción del evento reemplaza el troubleshooting

Introducción

Este documento describe los posibles problemas causados por la acción del evento reemplaza en el (IPS) del Cisco Intrusion Prevention System y ofrece las recomendaciones de ajustar y de resolver problemas su instalación.

> **Note**: La acción del evento reemplaza es medidas globales tomadas en las firmas basadas sobre un grado de riesgo. Como con cualquier configuración global, tome el gran cuidado con los cambios de configuración y las adiciones.

Problemas de la invalidación de la acción del evento

Descripción

La acción del evento reemplaza agrega las acciones adicionales a un evento de la firma cuando ese evento baja dentro de un rango especificado del grado de riesgo. La acción del evento del uso reemplaza cuidadosamente. Iif usted crea una invalidación con un rango ancho del grado de riesgo para un evento que se accione con frecuencia (las acciones especialmente específicas, costosas, tales como acciones del registro IP), usted puede ser que cause los problemas.

Impacto

Excesivo escribe al almacén del evento se asocian típicamente CPU elevada a la utilización y a la insensibilidad general del sensor a las herramientas del Acceso de administración tales como el comando line interface(cli) y el Cisco IPS Device Manager (IDM).

Acciones y descripciones del archivo del registro IP

Una descripción del archivo es una estructura de datos usada por un programa para conseguir una manija en un archivo; los descriptores bien conocidos son 0,1,2 para el estándar adentro, el estándar hacia fuera, y el error estándar. Se crea una descripción del archivo cuando un proceso abre un nuevo archivo o un socket.

Si usted crea una invalidación de la acción del evento para una acción del registro IP tal como registro-atacante-paquetes, registro-par-paquetes, o registro-víctima-paquetes, esto pudo agotar el pool de las descripciones del archivo; el funcionamiento total del sensor pudo ser negativamente afectado y el sensor puede no funcionar correctamente.

Las acciones del SNMP trap y la acción del evento reemplaza

Una firma que tiene solamente la sola acción del petición-SNMP-desvío también genera un evento alerta que se escriba al almacén del evento. Así pues, la despedida excesiva de la acción del Trap del Simple Network Management Protocol (SNMP) pudo también accionar los mismos problemas considerados con las acciones excesivas de la alerta de la producción.

Acciones para las firmas del motor del normalizador

No agregue ninguna acción que cause el almacén del evento escriba (por ejemplo la alerta, el petición-SNMP-desvío, o las registro-acciones de la producción) a las firmas del normalizador. Esto se aplica a los 1200-1330 ID de la firma del rango.

A excepción de los escenarios de Troubleshooting abreviados, usted no debe utilizar la acción del evento reemplaza para las firmas del motor del normalizador. Esto puede ser determinado problemático en:

- escenarios IP altamente hechos fragmentos (debido a las firmas 1200-range)
- (ooo) escenarios pesadamente fuera de servicio TCP (firmas 1300-range)

Por ejemplo, una invalidación de la acción del evento que causa una escritura al almacén del evento para cada paquete TCP del ooo puede causar los problemas del recurso y de la utilización.

La acción del evento reemplaza con el grado de riesgo de 0-100

Evite generalmente la acción del evento reemplaza con un grado de riesgo de 0-100 porque el grado bajo puede poner su sensor a riesgo del error en determinadas circunstancias.

De la meta de las firmas fuego componente a menudo para (y campo común) los tipos de tráfico aparentemente benignos. Las firmas de la meta buscan una combinación de una o más firmas componentes de la meta para accionar antes del padre que la firma de la meta enciende una alerta. Las firmas componentes de la meta, por abandono, no tienen ninguna acción asociada a ella; esto es intencional porque hacen juego con frecuencia en el tráfico común. Las firmas componentes de la meta tienen un grado de riesgo bajo predeterminado de 15. Para excluir la captura de estas coincidencias de la firma en una invalidación de la acción del evento, Cisco recomienda que usted no utiliza un grado de riesgo más bajo de 25 cuando usted crea una invalidación de la acción del evento; es decir, el grado de riesgo no debe estar debajo de 25-100.

Verifique la utilización IPS

Comandos

> **Note**: Utilice la herramienta de búsqueda de comandos (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección

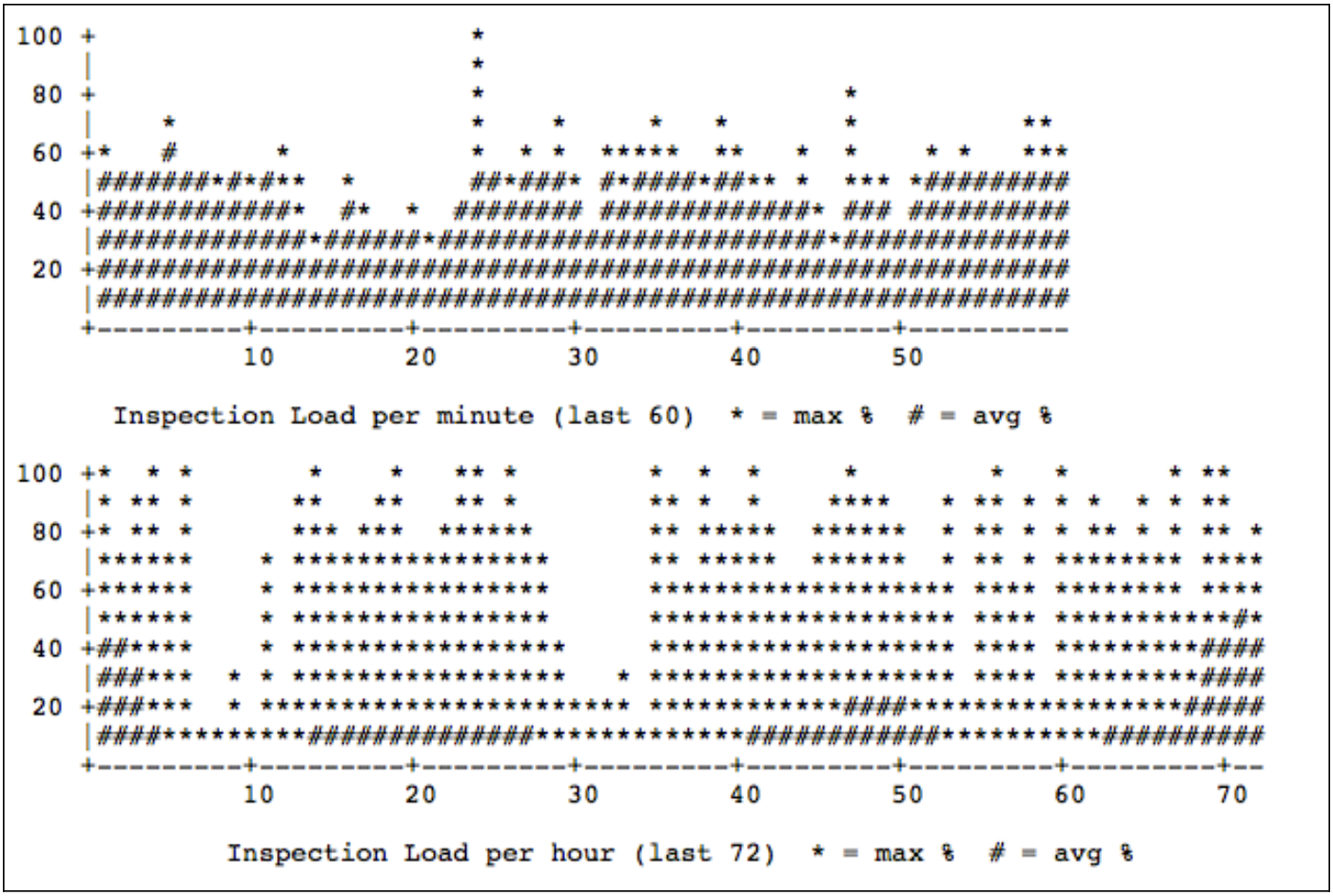
Ingrese el comando del virtual-**sensor de las estadísticas de la demostración** en el CLI para buscar el porcentaje de la carga del examen:

```
sensor# show statistics virtual-sensor | inc Load
Processing Load Percentage = 100
```

En las versiones 7.0(8)E4 y 7.1(6)E4 IPS, se ha agregado el comando de la examen-**carga de la demostración**:

```
sensor#  show inspection-load history
sensor 10:17:57 UTC Mon Apr 05 2013
```

Ésta es salida de ejemplo de ese comando:



Mismo un porcentaje de la mucha carga (el 90% o más alto) pudo indicar que hay eventos excesivos accionados por la acción del evento reemplaza. Refiera a abre una sesión la orden para confirmar más lejos esta posibilidad.

Registros

El indicador principal de la acción excesiva del evento reemplaza es almacén rápido del evento que envuelve, como se ve en este archivo de main.log del ejemplo:

```
sensor#  show inspection-load history
sensor 10:17:57 UTC Mon Apr 05 2013
```

El embalaje del almacén del evento que ocurre más a menudo de una vez una hora puede indicar generalmente un problema. En algunos escenarios, el embalaje es tan excesivo que puede ocurrir muchas veces dentro de un minuto. Hay muchas variables, tales como la capacidad de rendimiento general de la plataforma, considerar.

Troubleshooting

Determine qué tipo de evento, de tráfico, o de acción está causando el problema de la invalidación de la acción del evento. ¿Es una alerta de la producción, registro IP, firma del normalizador, o firma del componente de la meta?

- Si es una firma “habladora” y usted determina la firma crea los falsos positivos para los eventos, escriba un filtro de la acción del evento (EAF).
- Para el registro IP, Cisco le recomienda evita EAFs o utiliza EAFs con cautela y con una comprensión completa de los riesgos.
- Las firmas del normalizador y las firmas componentes de la meta no deben tener una acción alerta a excepción de los escenarios de Troubleshooting temporales.

Información Relacionada

- Configurar la acción del evento reemplaza
- Guías de configuración IPS
- Soporte Técnico y Documentación - Cisco Systems