Solucionar problemas de detección de inicios de sesión de interfaz de línea de comandos (CLI) excesivos de StarOS

Contenido

Introducción

Este documento describe cómo abordar el problema notificado por el sistema con respecto a los bajos recursos para la nueva sesión CLI.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- StarOs

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Problema

StarOs supervisa el número de sesiones CLI iniciadas para un administrador/operador/inspector

específico. Si el número de sesiones iniciadas es considerablemente mayor que el número de sesiones finalizadas, StarOs informa de que los recursos del sistema son bajos.

Cuando se intenta iniciar sesión, se muestra al usuario el siguiente mensaje de advertencia:

```
WARNING: system resources low:
NOTE: Creating an additional CLI session during a low resource state can
potentially cause service disruption.
To ignore the low resource condition and create a CLI session, enter "Y/y"
within 30 seconds:
```

Las razones de estas advertencias del sistema son las sesiones CLI excesivas que se producen en el nodo. A medida que se asignan los recursos de la CPU por tareas, el número de sesiones de CLI que pueden existir simultáneamente en un nodo de StarOS es limitado.

Cisco Prime u otros sistemas de administración de redes (NMS) recopilan periódicamente salidas de CLI de los nodos de StarOs, pero este problema se produce cuando la sesión de CLI no se cierra correctamente desde el lado de NMS. Como resultado, puede haber varias sesiones bloqueadas en un nodo de StarOs que consuman recursos de CPU.

Resolución de problemas

Cuando se produce esta situación, el sistema imprime este mensaje de evento en los registros.

Esto se puede ver mediante el comando **show logs :**

```
2017-Jul-12+11:01:07.786 [resmgr 14701 warning] [8/0/5990 <rmctrl:0> rmctrl_events.c:587]
[software internal system critical-info syslog] The resources needed for task cli/8028669 could
not be allocated to any active CPU.  Reason: CPU 8/0: insufficient unreserved memory (-22M
avail), mem: total: 4194304, used: 1262084, reclaimable: 0, unused_reserved: 2955429, available:
-23209, mem_size: 66560
```

El nodo StarOS genera una trampa **CLISessionStart** del protocolo simple de administración de red (SNMP) cuando se inicia una sesión CLI y una trampa **CLISessionEnd** cuando se detiene la sesión. En ambos casos se menciona al usuario específico involucrado.

Esto se puede ver ingresando el comando **show snmp trap history verbose** :

```
Tue Jul 11 18:35:22 2017 Internal trap notification 52 (CLISessionStart) user linuxcf privilege
level Security Administrator ttyname /dev/pts/21
el Secur
Wed Jul 12 10:53:17 2017 Internal trap notification 53 (CLISessionEnd) user linuxcf privilege
levity Administrator ttyname /dev/pts/21
```

> **Nota: Asegúrese de que esas trampas no estén suprimidas en el nodo con snmp trap suppress clisessend clisessstart**

Cómo detecta el problema el script

El script se utiliza para detectar esta situación analizando las trampas SNMP y el syslog a partir de la salida **show support details** (SSD) proporcionada.

El script realiza una búsqueda dentro de SSD e informa del problema cuando se cumplen estas condiciones:

Paso 1. Esta secuencia de comandos está contando el número de trampas SNMP **CLISessionStart** y **CLISessionEnd** en **show snmp trap history verbose**, y luego compara el número de sesiones iniciadas con las terminadas para un usuario específico. En caso de que haya un mayor número de sesiones iniciadas que un umbral predefinido de 40 ocurrencias, el script continúa con el paso 2.

Paso 2. El script pasa por **show logs** buscando la **advertencia** event id **resmgr 14701**.

Paso 3. La secuencia de comandos imprime el problema cuando coinciden los pasos anteriores.

Solución

Corto plazo

Recopile la lista de las sesiones de cli actualmente activas con el comando **show administrators session id**

```
[local]gw5# show administrators session id
Administrator/Operator Name    M Login Context      Remote Addr     Session ID
------------------------------ - ------------------ --------------- -----------
cisco                            local              10.149.4.25     5010152
cisco                            local              10.149.4.25     5010139
```

Fuerce las sesiones no deseadas por ID de sesión o por nombre con:

```
clear administrator session id
```

O bien

```
clear administrator name
```

A largo plazo

Corregir el comportamiento del usuario no conforme.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).