Troubleshoot StarOS Excessive Command Line Interface (CLI) Logins Detection

Contents

Introduction

This document describes how to address system reported problem regarding low resources for new CLI session.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- StarOs

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Problem

StarOs monitors number of started CLI sessions for specific administrator/operator/inspector, if number of session started is drastically higher then number of sessions ended, then StarOs reports warning that system resources are low.

The user is prompted with the following warning message when trying to logging in:

```
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:
```

Reasons for such system Warnings are excessive CLI sessions that are occurring on the node. As the CPU resources are assigned per tasks, the number of CLI session that can be simultaneously exist on a StarOS node is limited.

Cisco Prime or other Network Management Systems (NMS) periodically collect CLI outputs from StarOs nodes but this problem occurs when CLI session was not closed properly from NMS side. As a result, there can be multiple hanging session on a StarOs node consuming CPU resources.

Troubleshooting

When this situation occurs system prints this event message in the logs.

This can be seen by using the command **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
```

StarOS node generates Simple Network Management Protocol (SNMP) trap **CLISessionStart** when a CLI session is started and a **CLISessionEnd** trap when the session is stopped. In both cases the specific user involved is mentioned.

This can be seen by entering command **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
```

> **Note**: Please make sure those traps aren't suppressed on the node with **snmp trap suppress clisessend clisessstart**

How script detects the problem

Script is used to detect this situation analyzing SNMP traps and syslog from provided **show support details** (SSD) output.

The script preforms search inside SSD and reports the problem when these conditions are matched:

Step 1. This script is counting the number of SNMP traps **CLISessionStart** and **CLISessionEnd** in the **show snmp trap history verbose**, then comparing the number of session started versus the ones ended for specific user. In case the there is higher number of started sessions than a predefined threshold of 40 occurances then script continues with step 2.

Step 2. Script goes through **show logs** looking for event id **resmgr 14701 warning**.

Step 3. Script prints the problem when previous steps are matched.

Solution

Short term

Collect the list of the currently active cli sessions with the command **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
```

Force the unwanted sessions by session id or by name with:

```
clear administrator session id <id>
```

Or

```
clear administrator name <name>
```

Long term

Fix the behavior of the uncompliant user.