

Risoluzione dei problemi relativi al rilevamento di accessi CLI (Command Line Interface) eccessivi con StarOS

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Problema](#)

[Risoluzione dei problemi](#)

[Rilevamento del problema da parte dello script](#)

[Soluzione](#)

[A breve termine](#)

[A lungo termine](#)

Introduzione

Questo documento descrive come risolvere i problemi segnalati dal sistema relativi a risorse insufficienti per la nuova sessione CLI.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- StarOs

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Problema

StarOs controlla il numero di sessioni CLI avviate per amministratore/operatore/ispettore specifico, se il numero di sessioni avviate è notevolmente superiore al numero di sessioni terminate, StarOs

segnala che le risorse di sistema sono scarse.

Quando si tenta di eseguire l'accesso, viene visualizzato il seguente messaggio di avviso:

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:

I motivi di tali avvisi di sistema sono sessioni CLI eccessive che si verificano sul nodo. Poiché le risorse CPU vengono assegnate per attività, il numero di sessioni CLI che possono esistere contemporaneamente su un nodo StarOS è limitato.

Cisco Prime o altri sistemi di gestione della rete (NMS) raccolgono periodicamente gli output CLI dai nodi StarOs, ma questo problema si verifica quando la sessione CLI non è stata chiusa correttamente dal lato NMS. Di conseguenza, su un nodo StarOs possono essere presenti più sessioni sporgenti che utilizzano risorse CPU.

Risoluzione dei problemi

Quando si verifica questa situazione, il sistema stampa il messaggio di evento nei registri.

A tal fine, è possibile usare il 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
```

Il nodo StarOS genera una trap SNMP (Simple Network Management Protocol) **CLISessionStart** quando viene avviata una sessione CLI e una trap **CLISessionEnd** quando la sessione viene arrestata. In entrambi i casi viene indicato l'utente specifico coinvolto.

A tal fine, è possibile immettere il 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: assicurarsi che le trap non vengano eliminate nel nodo con l'opzione `snmp trap suppress clisessend clisessstart`

Rilevamento del problema da parte dello script

Lo script viene utilizzato per rilevare questa situazione analizzando le trap SNMP e il syslog dall'output **show support details** (SSD) fornito.

Lo script esegue la ricerca all'interno di SSD e segnala il problema quando vengono soddisfatte le

seguenti condizioni:

Passaggio 1. Questo script sta conteggiando il numero di trap SNMP **CLISessionStart** e **CLISessionEnd** nella **visualizzazione dettagliata della cronologia delle trap snmp**, quindi confrontando il numero di sessioni avviate con quelle terminate per un utente specifico. Se il numero di sessioni avviate è superiore alla soglia predefinita di 40 occorrenze, lo script continua con il passaggio 2.

Passaggio 2. Lo script esamina i **log di visualizzazione** per cercare l'ID evento **resmgr 14701 avviso**.

Passaggio 3. Lo script stampa il problema quando i passaggi precedenti corrispondono.

Soluzione

A breve termine

Raccogliere l'elenco delle sessioni CLI attualmente attive con il 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
```

Forzare le sessioni indesiderate in base all'ID sessione o al nome con:

```
clear administrator session id
```

O

```
clear administrator name
```

A lungo termine

Correggere il comportamento dell'utente non conforme.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).