VOSS Insights
Insights NetFlow System Function Validation Steps

Release 23.2

Jul 31, 2023

Legal Information

- Copyright © 2023 VisionOSS Limited.
  All rights reserved.
- This information is confidential. If received in error, it must be returned to VisionOSS ("VOSS"). Copyright in all documents originated by VOSS rests in VOSS. No portion may be reproduced by any process without prior written permission. VOSS does not guarantee that this document is technically correct or complete. VOSS accepts no liability for any loss (however caused) sustained as a result of any error or omission in the document.

DOCUMENT ID: 20230731130135

Contents

1 Overview 1

2 NetFlow Collector System Health Check 2

3 NetFlow Collector NetFlow Ingestion Count Increase Check 7

4 Dashboard Server System Status API check 14

5 Dashboard Server GUI Login - Interface Validation Check 16

6 Dashboard Server NetFlow Data Rendering Check 18

1. Overview

This guide outlines the steps for validating that the DS9 system is functioning properly from a service perspective, and that is it is receiving and processing NetFlow from the NetFlow source devices.

2. NetFlow Collector System Health Check

This procedure displays the output from the DS9 Collector internal Health Check, via the CLI **Administration** menu.

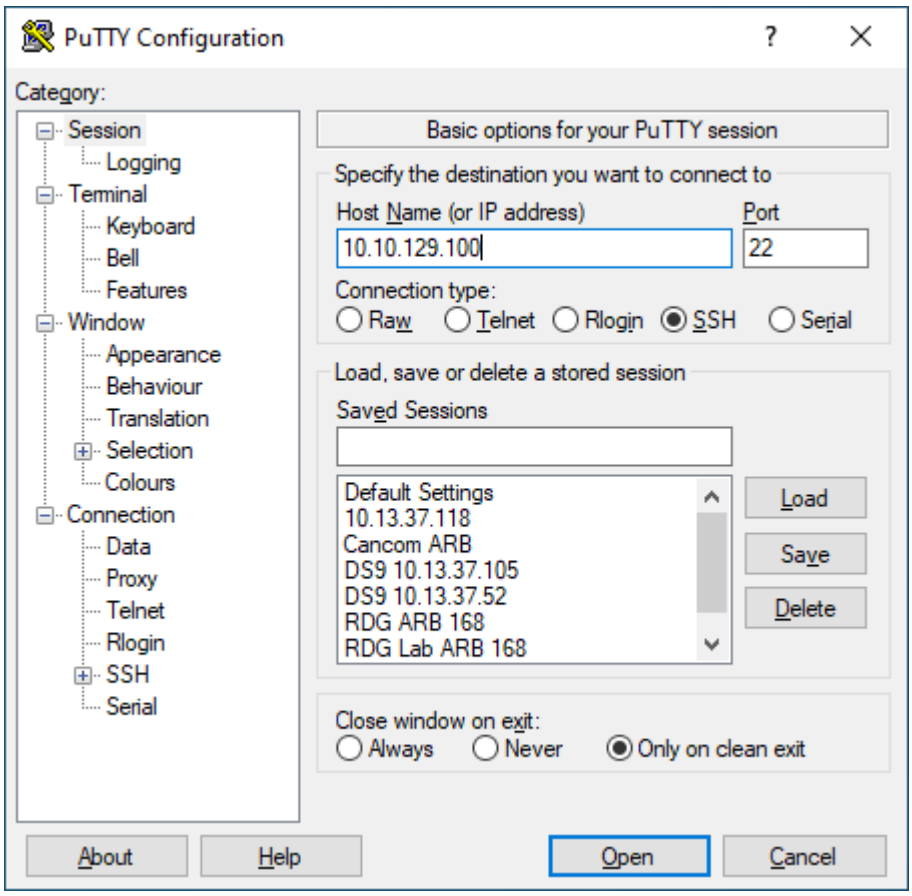
Note: If the displayed result is **Success**, the health check has validated that all services and processes are functioning properly.

If the displayed result is **Failure**, you will need to contact VOSS Support.

---

1. SSH to the DS9 system, and log in to the system using the DS9 CLI NetFlow Collector System Health Check **admin** credentials (username / password) to access the main **Administration** menu.

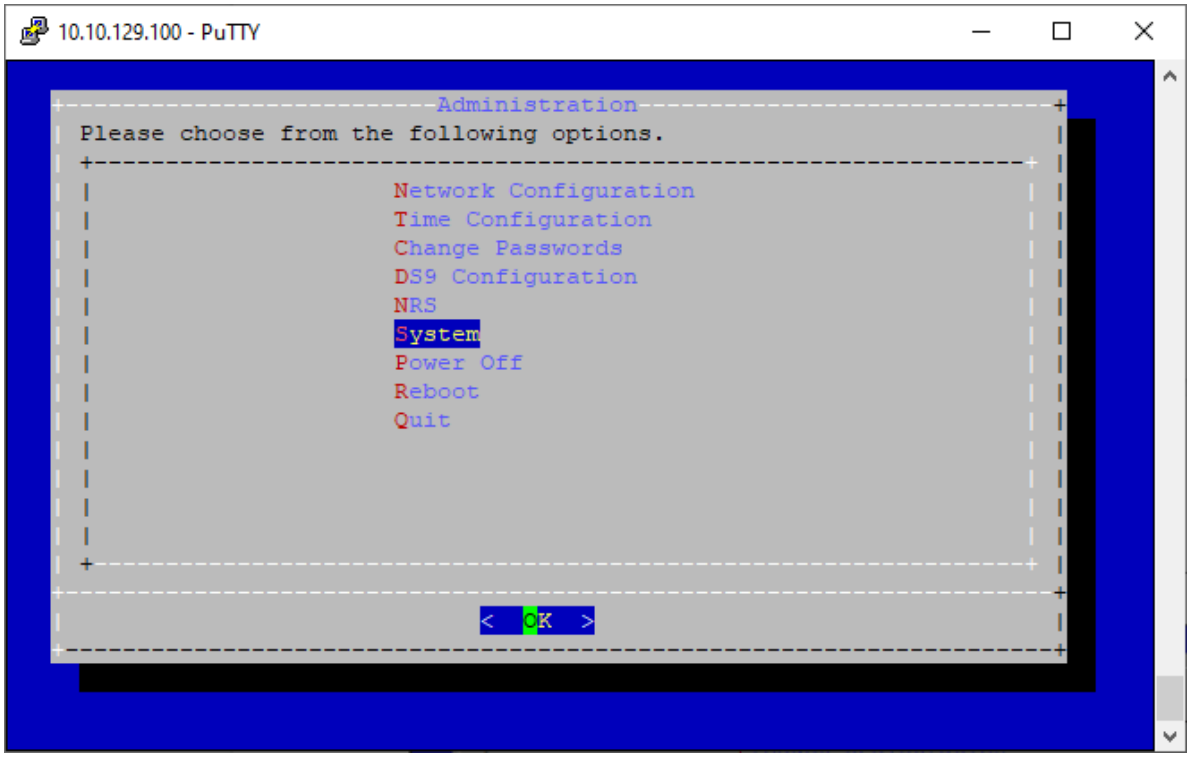
   Note: The image shows SSH connection example using Putty ssh client.



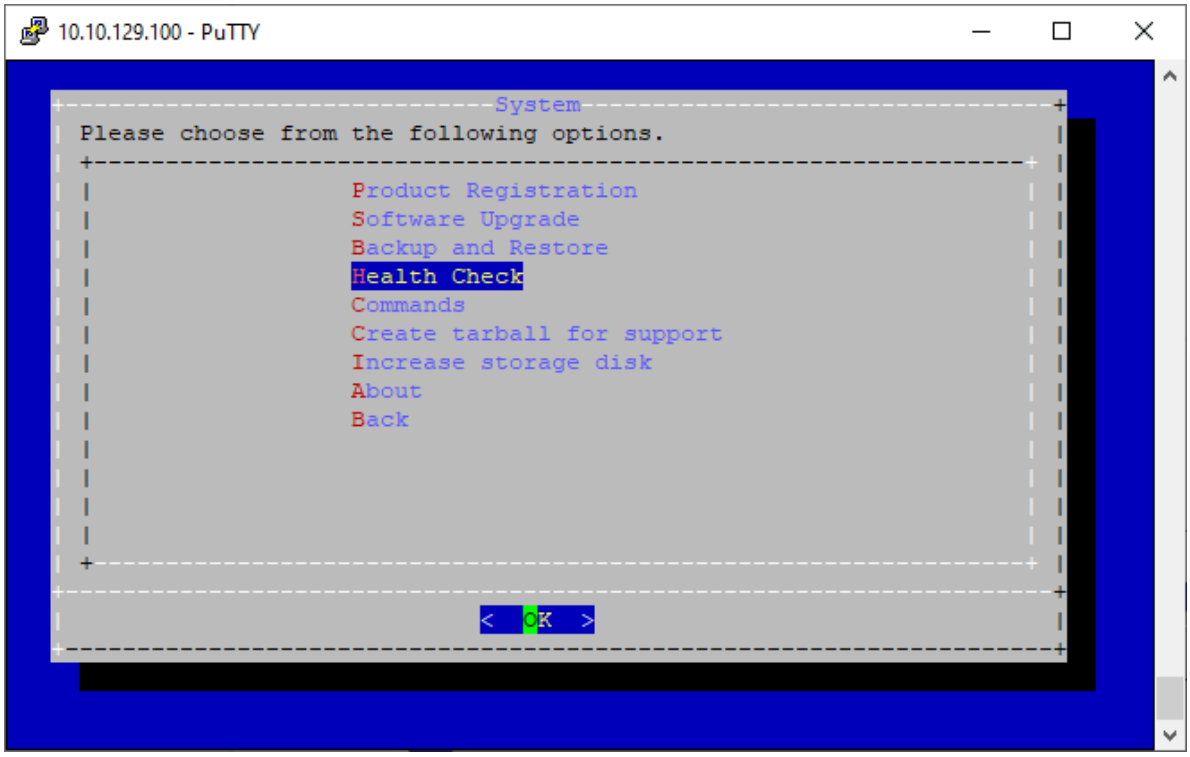
2. In the **Administration** menu, select **System**, then select **OK**, and press **<ENTER>**.

Note: Use the following keyboard keys to choose relevant options and to navigate through the CLI **Administration** menu: **<ARROW>**, **<TAB>**, **<ENTER>**

Copyright © 2023 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

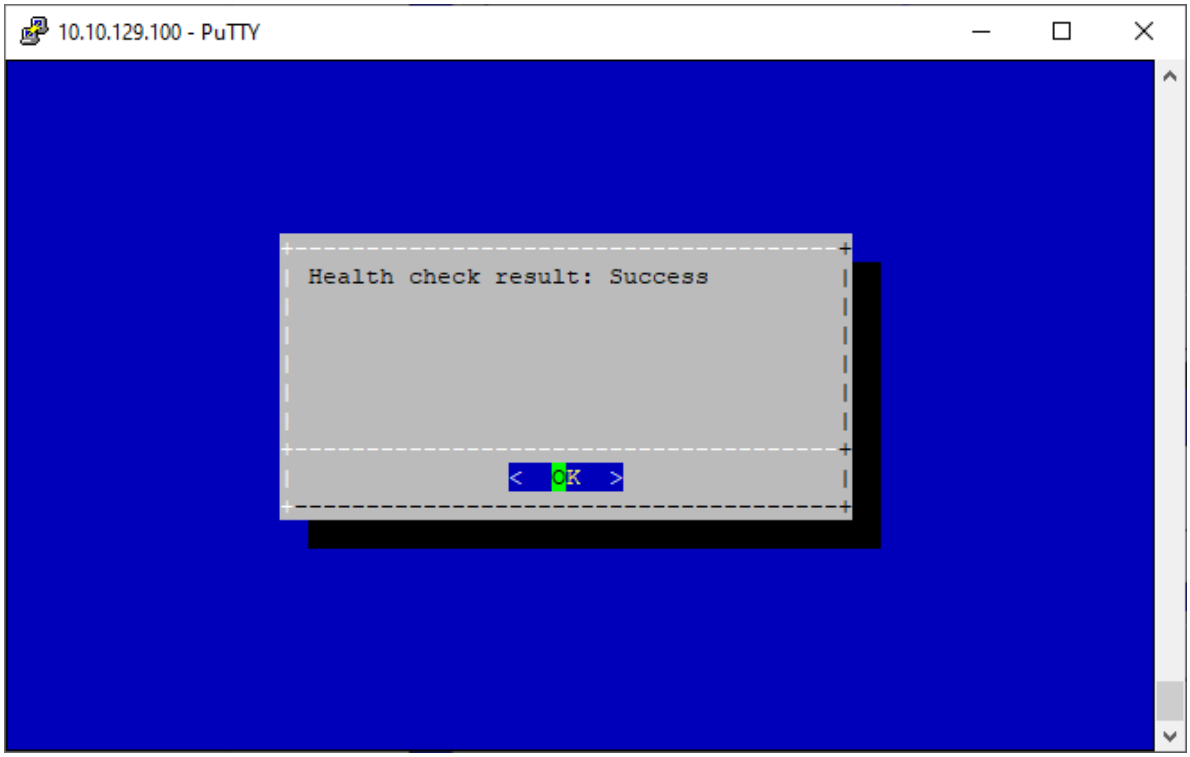


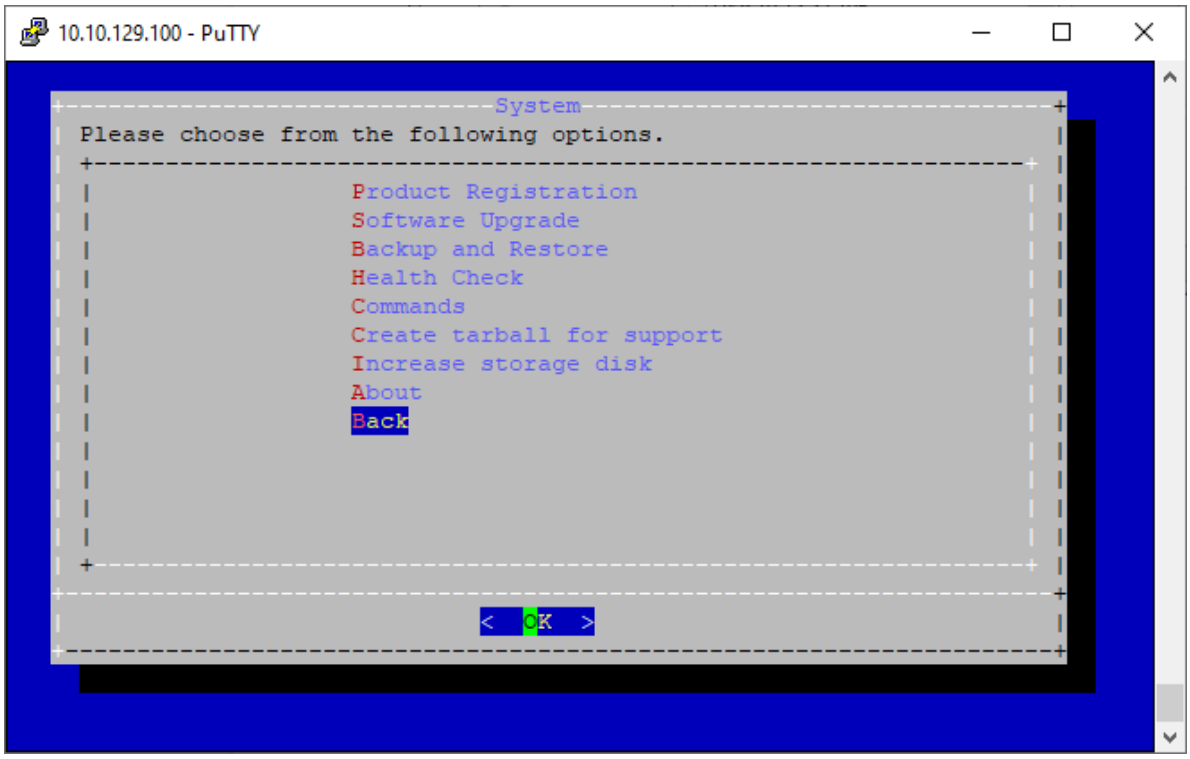
3. On the **System** page, select **Health Check**, then select **OK**, and press **<ENTER>**.



View the result, which should be **Success**. Select **OK**, and press **<ENTER>** to return to the **System** page.

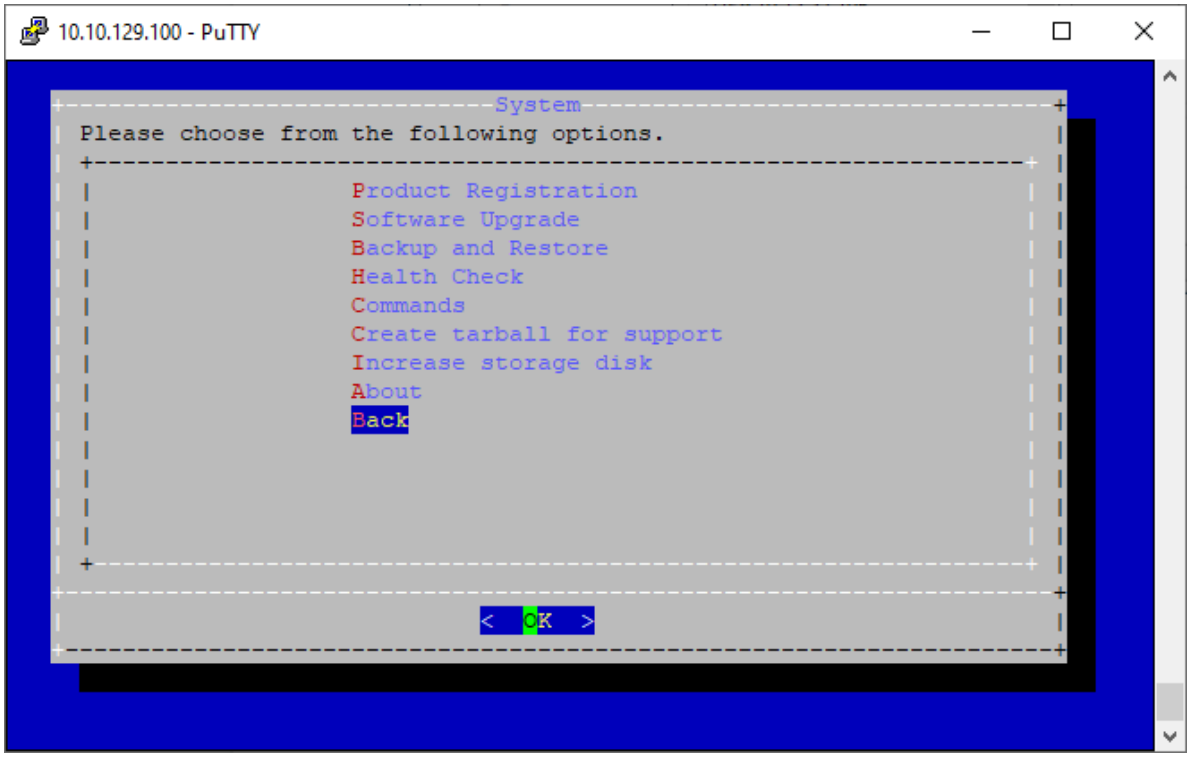
Copyright © 2023 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com





4. On the **System** page, select **Back**, select **OK**, and press **<ENTER>** to return to the main **Administration** menu.

Copyright © 2023 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com



5. In the **Administration** menu, select **Quit**, and press **<ENTER>** to disconnect from the system.

Copyright © 2023 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

3. NetFlow Collector NetFlow Ingestion Count Increase Check

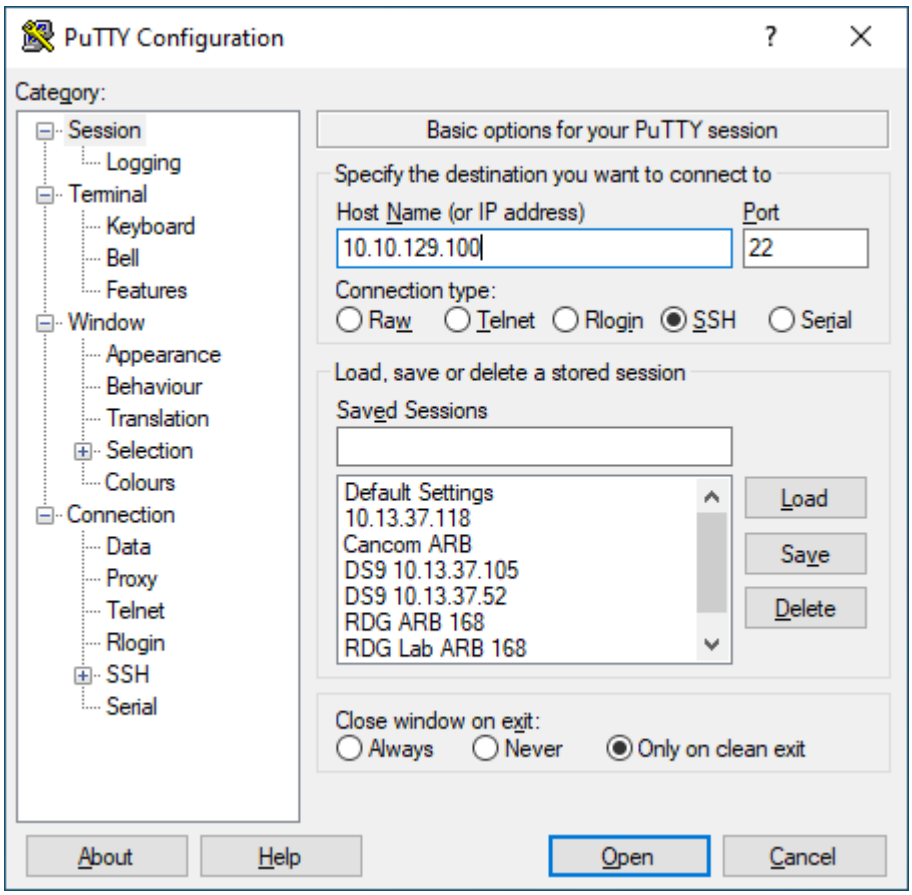
This procedure displays the output from the DS9 Collector NetFlow Count indicator via the CLI **Administration** menu.

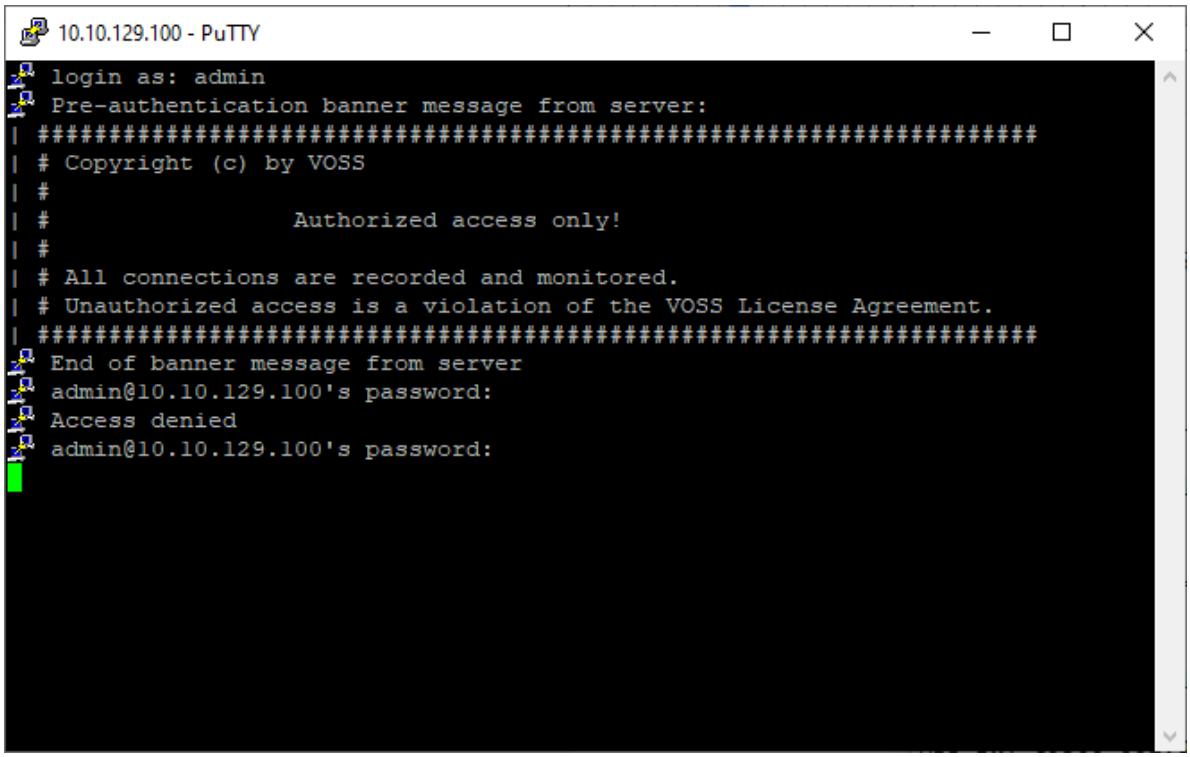
A count increase when comparing 2 count values generated in succession validates that all NetFlow ingestion and parsing services and processes are functioning properly, and that the database is functioning properly.

If the netflow count displays a value of **0** and the Health Check is showing **SUCCESS**, the system might not be receiving flow from the systems configured to send flow to the DS9. Validate that there are no firewalls impeding the netflow traffic to the DS9 before contacting VOSS support.

1. SSH to the system IP, and log in to the system using the CLI **admin** credential below to access the **Administration** menu.

   Note: The image shows SSH connection example using Putty ssh client.

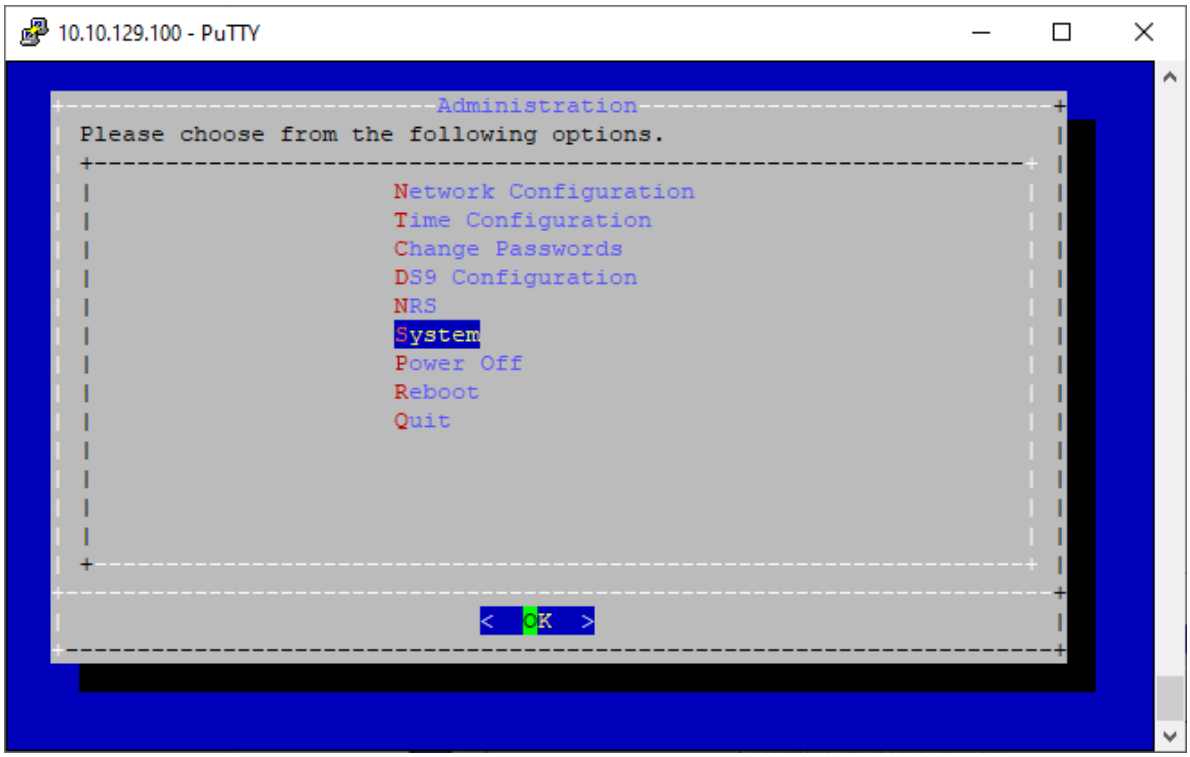




Copyright © 2023 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

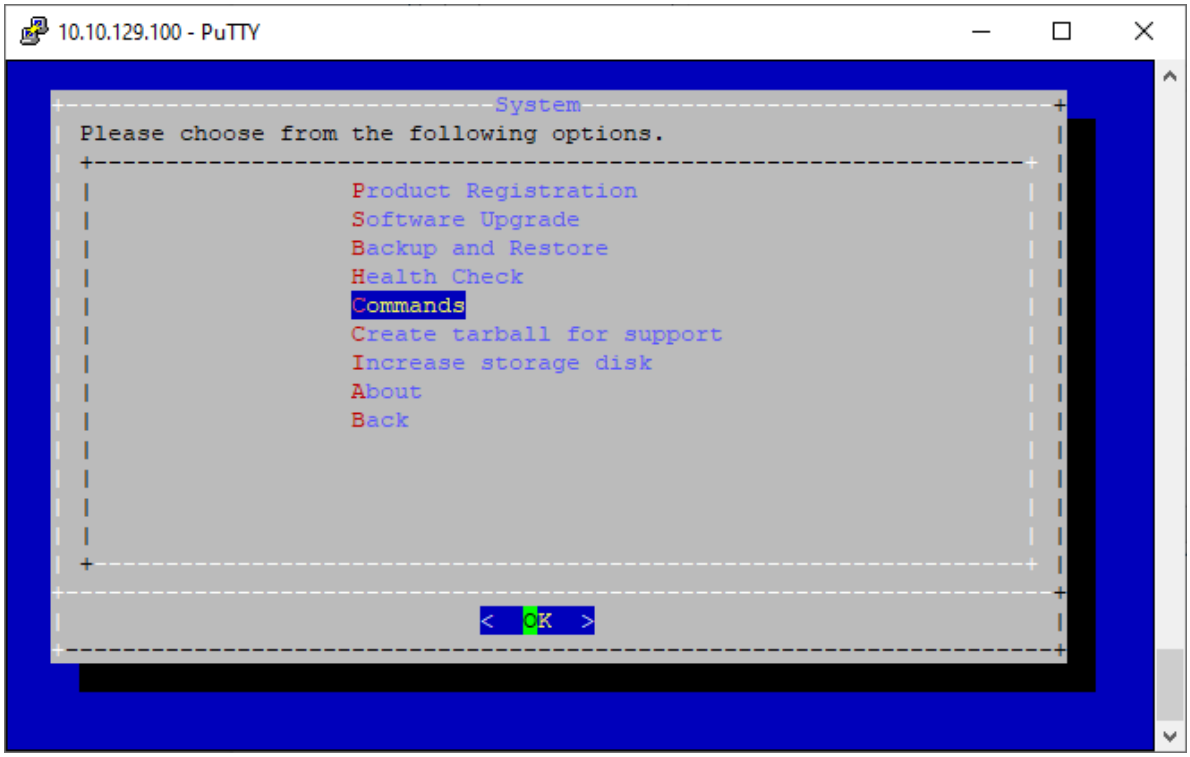
2. In the **Administration** menu, select **System**, then select **OK**, and press **<ENTER>**.

Note: Use the following keyboard keys to choose relevant options and to navigate through the CLI **Administration** menu: **<ARROW>**, **<TAB>**, **<ENTER>**

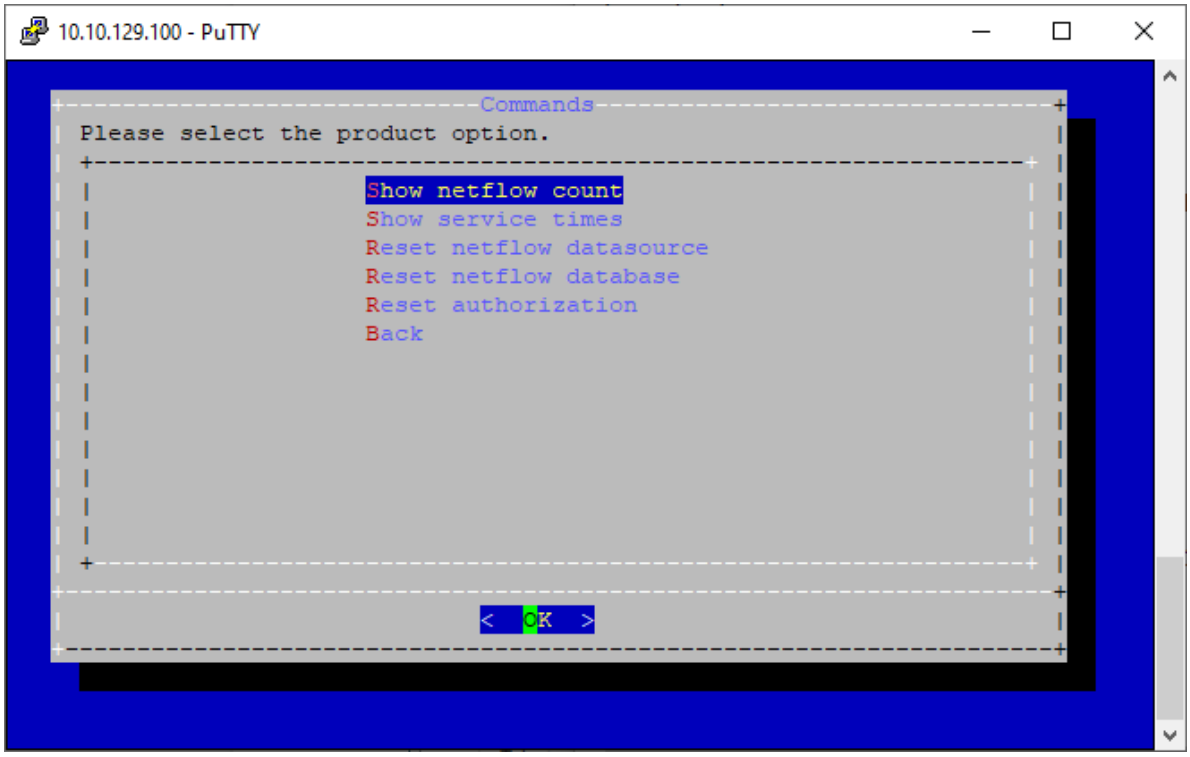


3. On the **System** page, select **Commands**, then select **OK**, and press **<ENTER>**.

Copyright © 2023 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

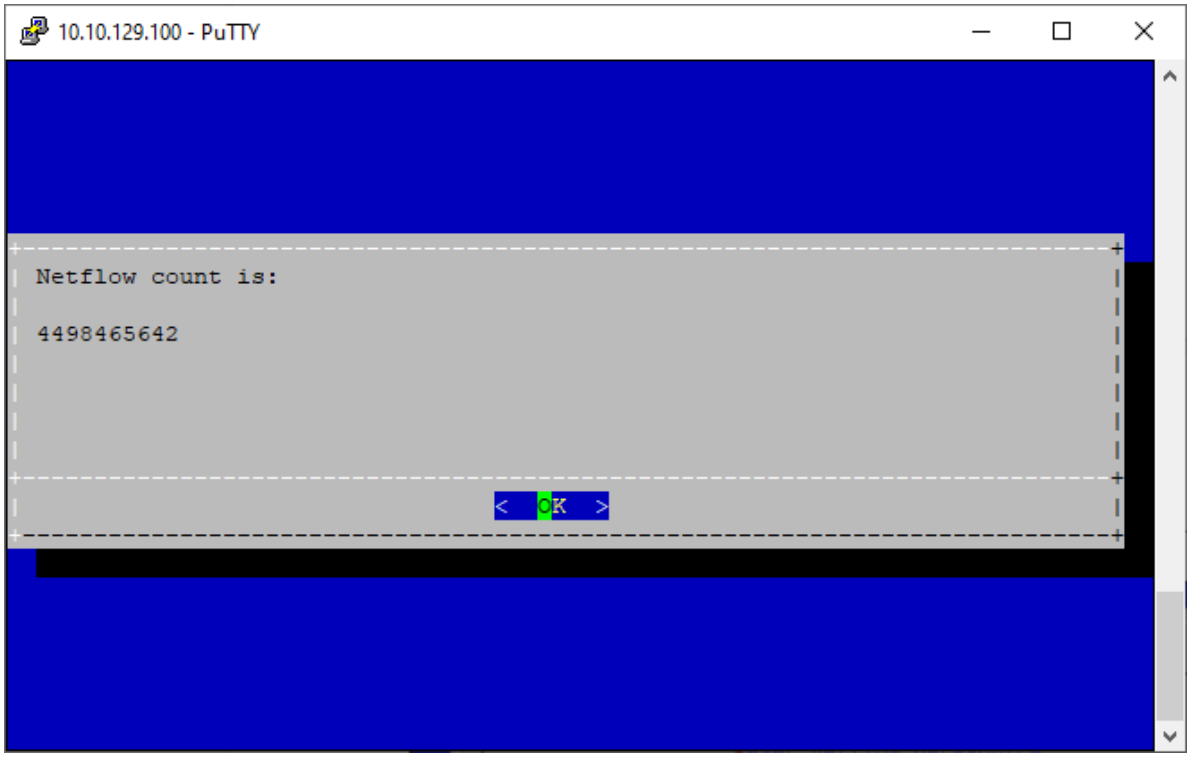


4. On the **Commands** page, select **Show netflow count**, then select **OK**, and press **<ENTER>**.

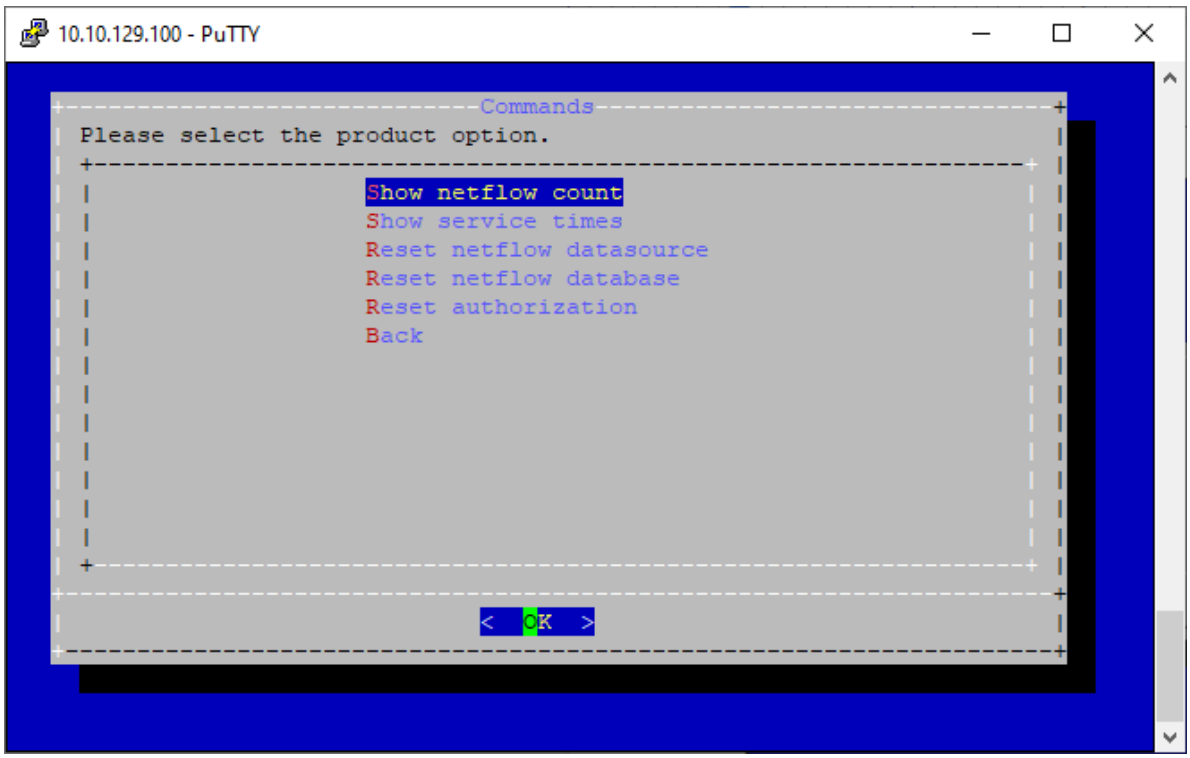


5. View the current count number.

Copyright © 2023 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com



6. Press **<ENTER>** to return to the **Commands** page.
7. On the **Commands** page, select **Show netflow count** again, then select **OK**, and press **<ENTER>**.

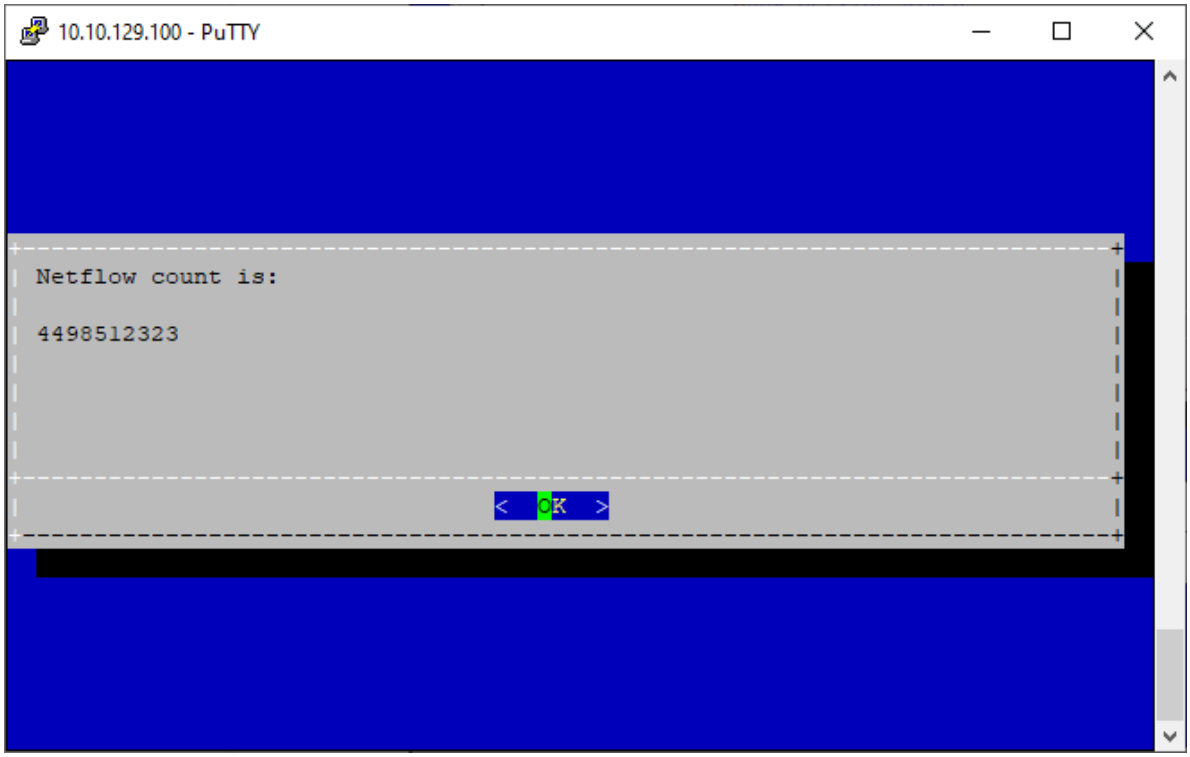


8. View the NetFlow data count number, which displays for the second time.

   The count number displays a larger number compared to the first count display. This count increase is

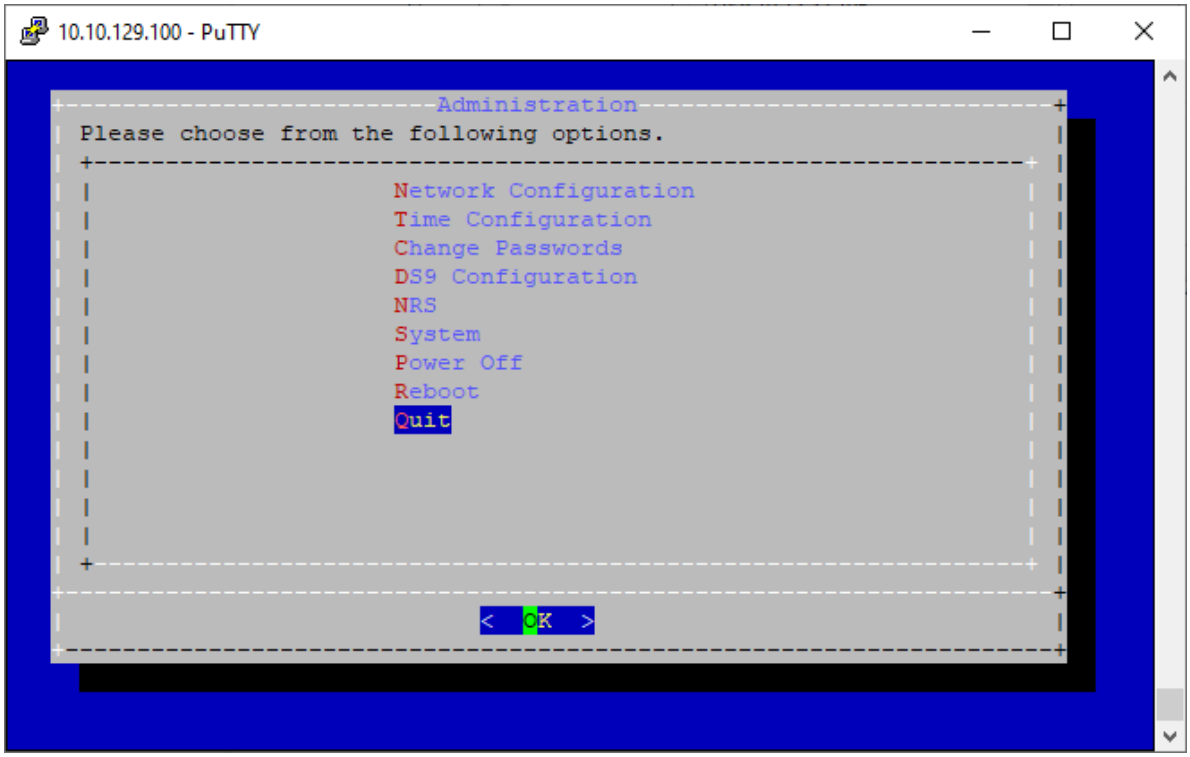
Copyright © 2023 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

validation that the incoming NetFlow packets are being ingested into the database and that the system processes are working properly.



9. To disconnect from the system:
    - Press **<ENTER>** to return to the **Commands** page.
    - On the **Commands** page, select **Back**, then select **OK**, and press **<ENTER>** to return to the **Administration** menu.
    - In the **Administration** menu, select **Quit**, then select **OK**, and press **<ENTER>**.

Copyright © 2023 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

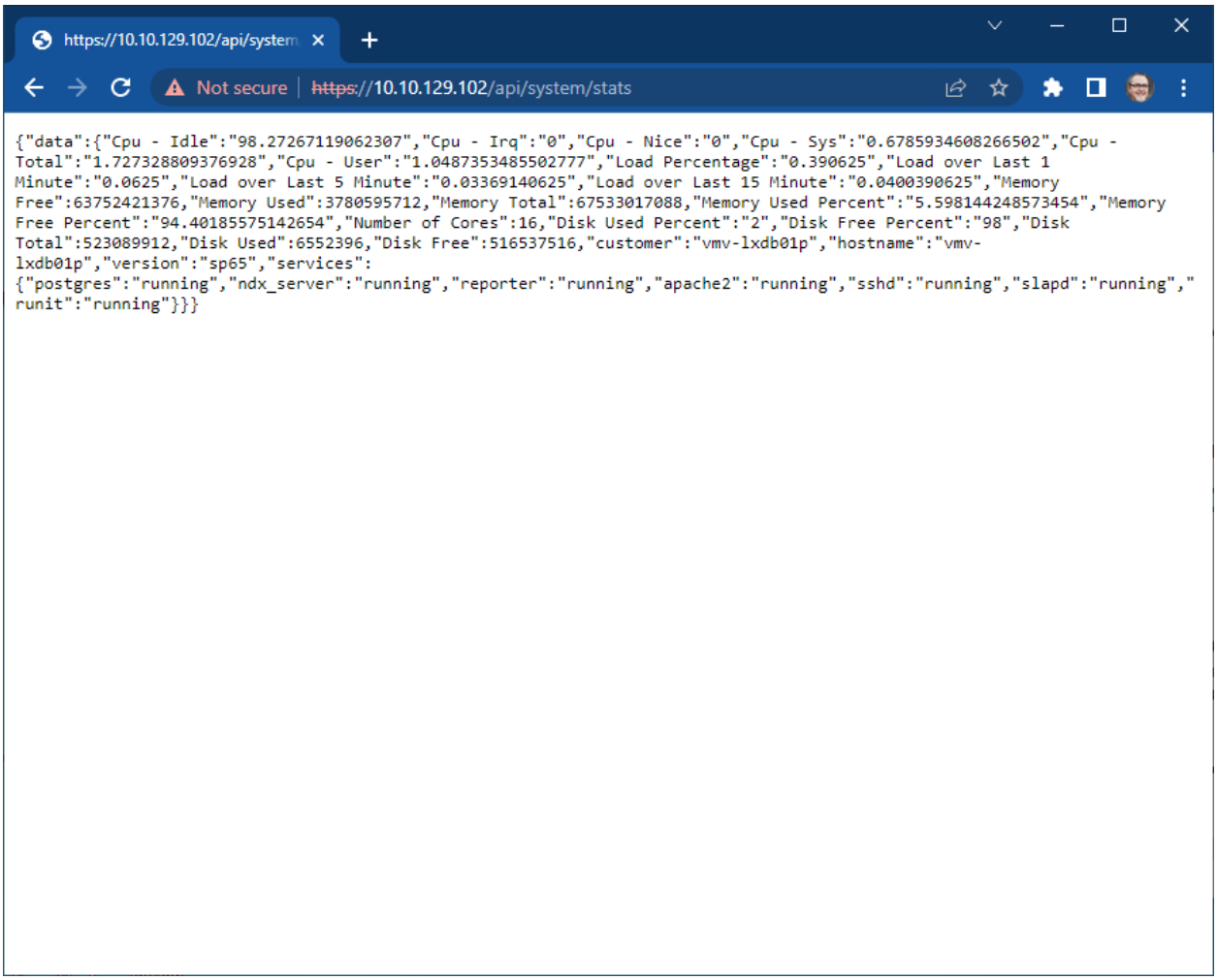


Copyright © 2023 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

4. Dashboard Server System Status API check

In a browser, navigate to the Dashboard System Status API, using a URL with the following format:

https://<IP address>/api/system/stats



API output text displays system utilization statistics (CPU, RAM, Disk) and process status. All service status results should display as “running” for proper system operation.

API text output:

```
{"data":
  {"Cpu - Idle":"98.27267119062307",
```

(continues on next page)

(continued from previous page)


```
  "Cpu - Irq":"0",
  "Cpu - Nice":"0",
  "Cpu - Sys":"0.6785934608266502",
  "Cpu - Total":"1.727328809376928",
  "Cpu - User":"1.0487353485502777",
  "Load Percentage":"0.390625",
  "Load over Last 1 Minute":"0.0625",
  "Load over Last 5 Minute":"0.03369140625",
  "Load over Last 15 Minute":"0.0400390625",
  "Memory Free":63752421376,
  "Memory Used":3780595712,
  "Memory Total":67533017088,
  "Memory Used Percent":"5.598144248573454",
  "Memory Free Percent":"94.40185575142654",
  "Number of Cores":16,
  "Disk Used Percent":"2",
  "Disk Free Percent":"98",
  "Disk Total":523089912,
  "Disk Used":6552396,
  "Disk Free":516537516,
  "customer":"vmv-lxdb01p",
  "hostname":"vmv-lxdb01p",
  "version":"sp65",
  "services":{"postgres":"running",
              "ndx_server":"running",
              "reporter":"running",
              "apache2":"running",
              "sshd":"running",
              "slapd":"running",
              "runit":"running"}}}
```


Copyright © 2023 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

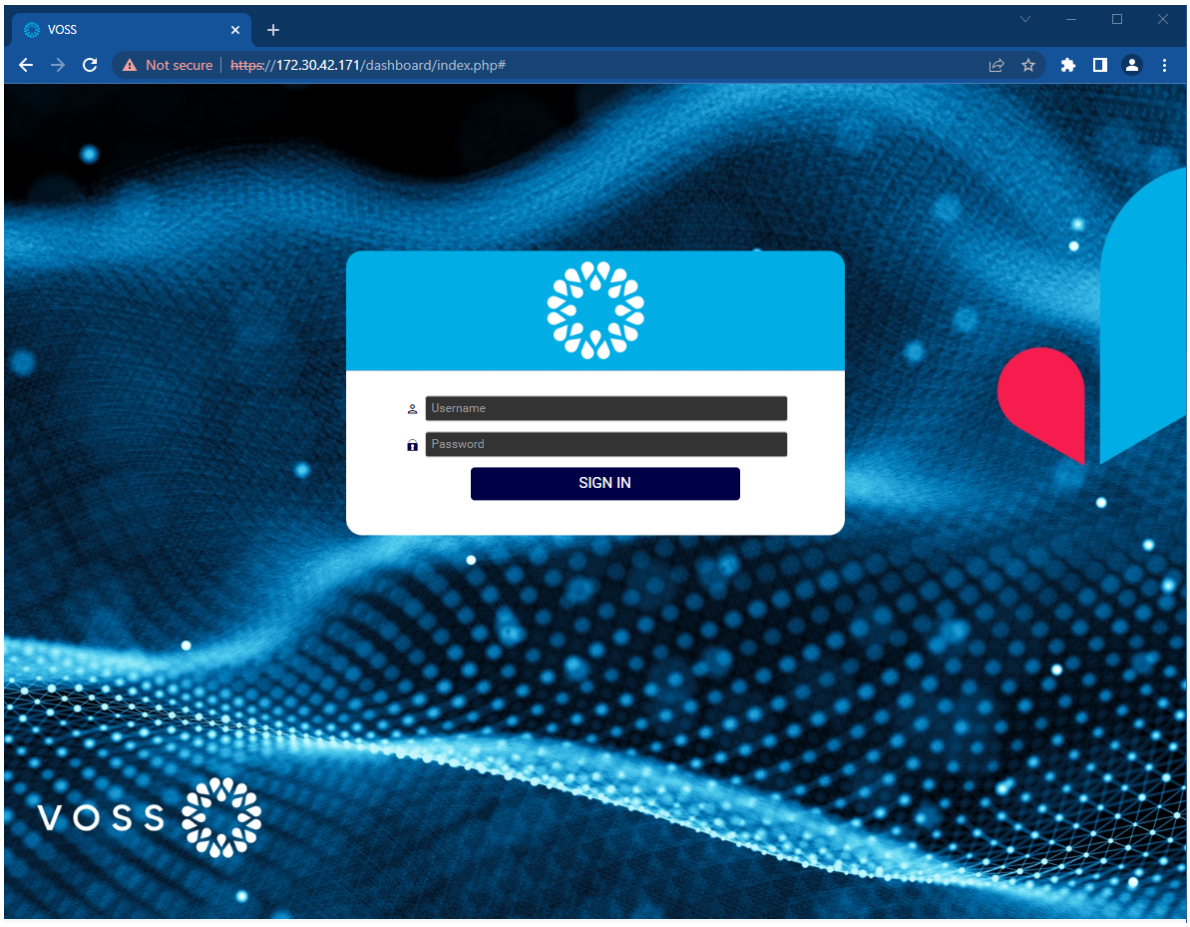
5. Dashboard Server GUI Login - Interface Validation Check

1. In a browser, navigate to the Dashboard GUI, using a URL with the following format:

   https://<IP address>

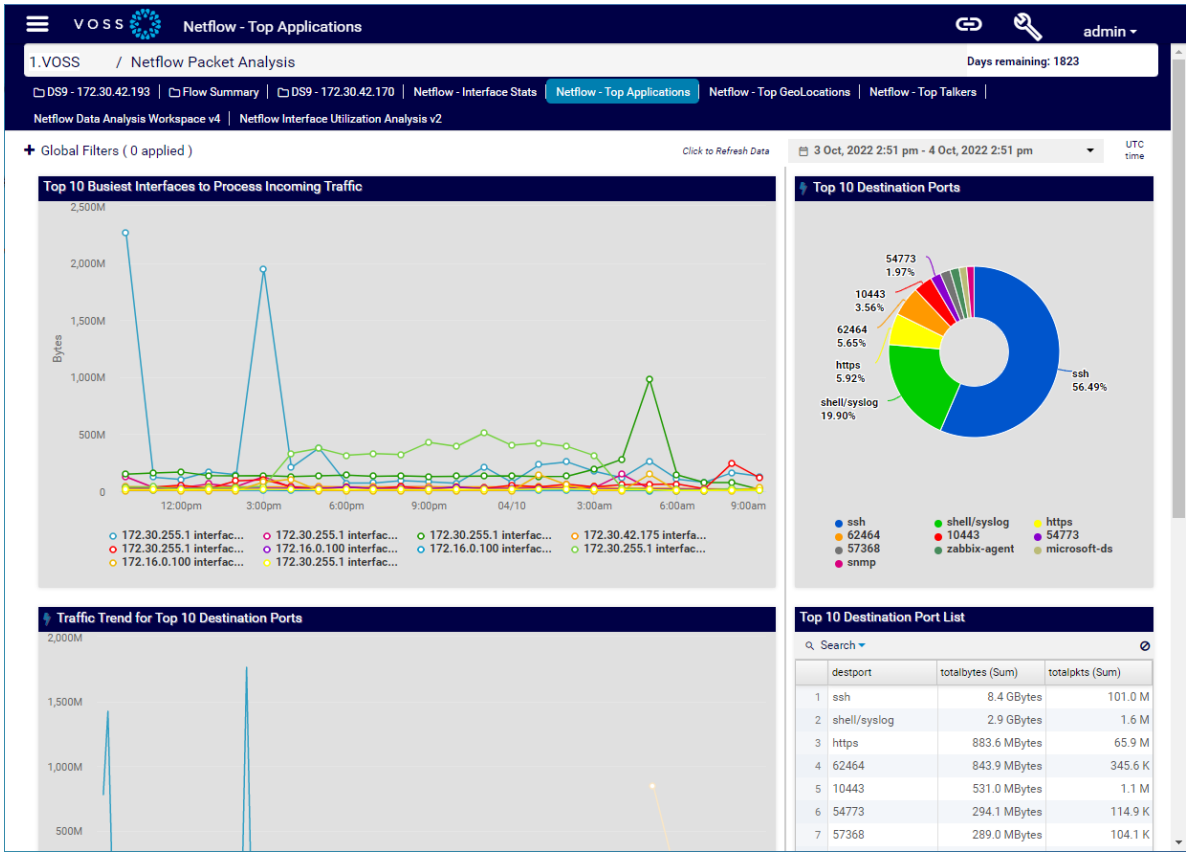
   If the log in page displays, this validates that the system is reachable and the Apache service is running.
2. Log in to the system using admin credentials (**admin** / **admin**).

   Successful authentication indicates that the system processes are running, and serving its GUI via Apache.



3. View the default Dashboard.

Data displayed in the dashboard validates GUI function and connectivity to the DS9 Collector system from the Dashboard system.



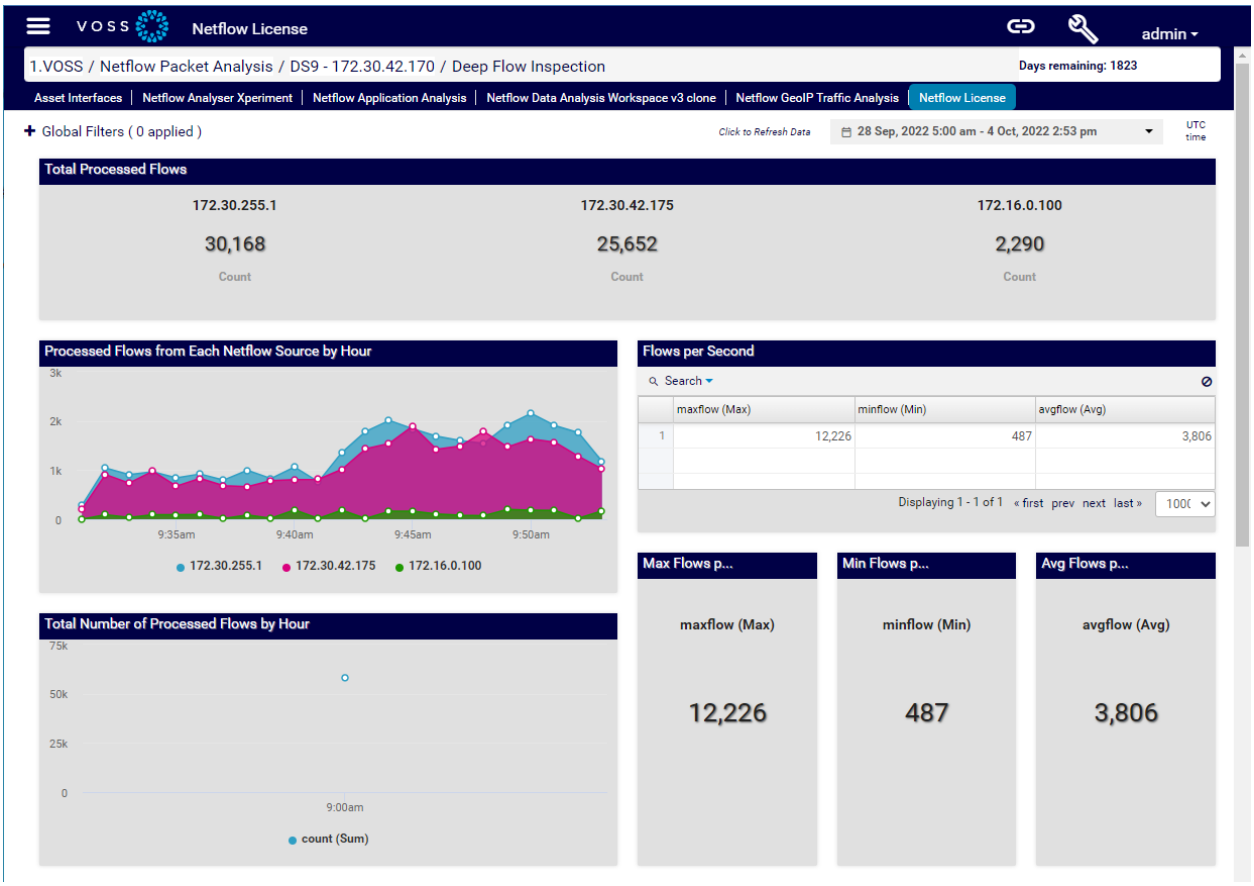
Copyright © 2023 VisionOSS Limited. All rights reserved. We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

6. Dashboard Server NetFlow Data Rendering Check

1. In a browser, connect to the Dashboard GUI, using a URL with the following format:

   https://<IP address>

2. Log in to the system using admin credentials (**admin** / **admin**).
3. In the **Deep Flow Inspection** folder, select the **NetFlow License** dashboard.
4. Set the time frame for the data to be viewed, to the 1 hour time frame.

   If you're able to see data rendered in the tables and graphs in the NetFlow License dashboard, system connectivity to the DS9 Collector databases is validated, as well as DS9 NetFlow data ingestion.

   If you're able to see data displaying in any dashboard in the NetFlow Packet Analysis and Deep Flow Inspection folders on the Dashboard application, then both systems are functioning properly.