Serviceability Diagnostics

Feature Summary and Revision History

Summary Data

Table 1: Summary Data

Applicable Products or Functional Area	PCF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Documentation	Not Applicable

Revision History

Table 2: Revision History

Revision Details	Release
First introduced.	2023.01.0

Feature Description

The Cisco Policy Control Function (PCF) doesn't offer capabilities for viewing the system of consolidated health such as Policy and Charging Rules Function (PCRF) Diagnostics. PCF relies significantly on numerous Kubernetes commands to determine the system of health.

PCF implements the diagnostics utility to provide the health check consolidated output of different critical services on the PCF namespace. Validates health of pods, services, and ingress points and produces a pass or fail health check status for each service.

The services for the health check:

- Rest-endpoint
- Engine
- Diameter
- Common Data Layer (CDL)
- ETCD
- Database (DB)
- Health check of the Splunk
- Active alarm report

Utility Details:

- Critical Pod Service Health Check and other Pods Check : When the status argument is "all", then all pods health check for previous mentioned services gets executed.
- CDL Pods Health Check:
  - When the status argument is "cdl" for the CDL pods health check, then the health check gets executed.
  - When the cdl-ep pods are up and running, then the geo sync functionality gets validated, and the execution status gets displayed.
- Database Pods Health Check:
  - When the status of the argument is "db" for the DB pod of the health check, then the health check gets executed.
  - When the pods are up, then the accessibility of the database gets performed.
- Health check of the Splunk
  - When the status of the argument is "splunk" for the health check of the Splunk, then the logging status gets executed and displays details on the console.
- Active alarm report
  - When the status argument input as "alert", then Active alert summary details get displays on the console.

Serviceability KPIs Diagnostics Implementation

Feature Summary and Revision History

Feature Description

The Cisco Policy Control Function (PCF) doesn't offer capabilities for viewing the messages packet counters at each critical application component. The PCF uses a Key Performance Indicators (KPIs) diagnostics utility to compute and determine the systems behavioral status at a specified time interval. The diagnostics utility also collects the counters from the component and helps to limiting down the issue to a particular area. The utility computes the appropriate KPI counters by querying the prometheus server.

The services to check the counters:

- Rest-endpoint
- Engine
- CDL

Advanced System Diagnostics with Comprehensive Service Monitoring

Table 3: Feature History

Feature Name	Release Information	Description
Enhancement for Service Diagnostics CLI Command	2025.02.0	This feature introduces advanced capabilities to the PCF system diagnostics command by incorporating additional service monitoring functionalities. It provides users with the ability to retrieve detailed information about network repository functions and LDAP server connections directly through the CLI: **pcf-system diagnostics status nrf/ldap** **Default Setting:** Disabled - Configuration required to enable

The Comprehensive CLI Enhancements for Service Diagnostics feature significantly expands the diagnostic capabilities of the PCF system by integrating detailed service monitoring functionalities into the existing **pcf-system diagnostics status** CLI command. The key aspects of this feature include:

- Advanced NRF (Network Repository Function) Monitoring:
  - rest-endpoint leader
  - Last registered NRF IP and connection timestamp
  - Previous NRF IP and connection timestamp
- Detailed LDAP (Lightweight Directory Access Protocol) Endpoint Analysis:
  - ldap-endpoint name
  - LDAP server connections IPs per endpoint

Display NRF Connectivity Diagnostics

The system diagnostics for NRF displays the rest-endpoint leader, last and previously registered NRF IP and connection timestamp.

Procedure

Step 1 Login to the Global Configuration mode.

Step 2 Enter the **pcf-system diagnostics status** with **nrf** to view the rest-endpoint leader, last and previously registered NRF IP and connection timestamp.

```
[unknown] pcf# pcf-system diagnostics status nrf
Fri Mar  7  15:38:32.283 UTC+00:00
diagnosticsInfo :
################## START Diagnostics #################
+-------------------------------------------------------------------------------------+
Rest-ep Leader : pcf-rest-ep-57ccc66f55-wp4mb
LastRegistered NRF :
URI:http://192.168.000.0:0000/nnrf-nfm/v1       TimeStamp:2025-03-07T15:37:19.065Z
PreviouslyRegistered NRF :
URI:http://192.168.000.0:0000/nnrf-nfm/v1       TimeStamp:2025-03-07T15:36:37.356Z
+-------------------------------------------------------------------------------------+
################## END Diagnostics ##################
```

Display LDAP Endpoint Analysis

The system diagnostics for LDAP endpoint displays the ldap-endpoint name and LDAP server connection IPs per endpoint.

Procedure

Step 1 Login to the Global Configuration mode.

Step 2 Enter the **pcf-system diagnostics status** with **ldap** to view the ldap-endpoint name and LDAP server connection IPs per endpoint.

```
[svi-cndp-tb8-s2/cluster2] pcf# pcf-system diagnostics status ldap
Wed Feb  19 07:50:28.533 UTC+00:00
diagnosticsInfo :
################## START Diagnostics #################
Ldap Connection Details:
+-------------------------------------------------------------------------------------------+
Ldap Endpoint Pod-name : ldap-pcf-cps-ldap-ep-68f5fb5c78-fsv6x
Server Address : 192.168.000.0#389        Connection Count : 5
Server Address : 192.168.000.0#489        Connection Count : 6
Server Address : 192.168.000.0#589        Connection Count : 7
+-------------------------------------------------------------------------------------------+
+-------------------------------------------------------------------------------------------+
Ldap Endpoint Pod-name : ldap-pcf-cps-ldap-ep-68f5fb5c78-zvl2l
Server Address : 192.168.000.0#389        Connection Count : 5
Server Address : 192.168.000.0#489        Connection Count : 6
Server Address : 192.168.000.0#589        Connection Count : 7
+-------------------------------------------------------------------------------------------+
################## END Diagnostics #################
```

KPI Counter for LDAP Connectivity

Here is the KPI counter for **ldapconnections_established** in system diagnostics:

```
ldapconnections_established_total{node_type="unknown",
server_address="192.168.105.150#390",pod_name="ldap-pcf-cluster2-cps-ldap-ep-7688dff8fb-j6xkk",
} 3.0
```

Feature History

Table 4: Feature History

Feature Name	Release Information	Description
TCP Dump	2025.04.0	You can now easily capture and manage network traffic data in PCF pods, improving troubleshooting and serviceability. This enhancement adds TCP dump support via the Opscenter CLI for key application pods (Rest, Diameter, LDAP, Engine). Users can run filtered tcpdump commands, set execution timeouts, and limit performance impact. Captured files are automatically transferred to a remote backup server using SCP or stored locally if no server is set. The system purges old files to prevent disk space issues, warns if usage exceeds thresholds, and limits parallel captures to three. Automatic cleanup removes files older than one hour. Command introduced: **pcf-system tcpdump { capture | clear }**— Used to capture or clear the tcp dump files. **Default Setting**: Disabled – Configuration Required

TCP Dump Functionality for Enhanced Serviceability

TCP dump is a command-line network packet analyzer that allows users to capture and display TCP/IP and other packets being transmitted or received over a network interface. This functionality helps users understand network behavior, diagnose issues, and monitor network activity.

In the context of PCF, tcpdump assists critical application pods in troubleshooting network, TCP, HTTP, and HTTP2-related issues.

Key Points during the Implementation of TCP Dump Functionality

Be aware of these key points while deploying TCP dump feature.

- It helps troubleshoot network issues effectively.
- It ensures minimal impact on ongoing calls during its execution by running as a low priority process.
- It automatically transfers captured files to a backup destination.
- It automatically purges old capture files to prevent disk space exhaustion.
- It offers filtering options to capture specific traffic, which avoids performance degradation.

Limitations of TCP Dump Functionality

Note these potential limitations when using TCP dump functionality for PCF system.

- PCF does not support multiple pod name as CLI input.
- The namespace information is not included in the captured pcap file.

How TCP Dump Functionality Works

Summary

The Opscenter CLI executes the tcpdump command within the target pod. The system runs tcpdump as a low priority process to minimize performance impact on the pod. When the utility captures data, it transfers the pcap files to a backup destination by default. If you do not configure a remote server, the command output shows the file name and path inside the target pod. The utility purges old pcap files automatically:

Workflow

These steps describe the stages for the TCP dump functionality:

1. Files are removed from the target pod after they are copied to the pcf-utilities pod.
2. If the Secure Copy Protocol (SCP) transfer to the remote server succeeds, the utility deletes files from the pcf-utilities pod.
3. If the SCP transfer to the remote server fails, files remain stored locally in the pcf-utilities pod. A cleanup scheduler, tcpdump_cleanup_scheduler.sh, runs every 20 seconds in the pcf-utilities pod. This scheduler removes tcpdump capture files older than one hour. The tcpdump-backup.cleanup-enabled configuration flag controls this process. This prevents disk space exhaustion. The utility throws proper errors if tcpdump execution fails.

Guidelines while Using TCP Dump Functionality

You can use the Opscenter command line interface (CLI) to run the tcpdump utility. The utility supports tcpdump for the following pods:

- Rest Endpoint
- Diameter Endpoint
- LDAP Endpoint

- Engine

To capture network traffic, use the pcf-system tcpdump capture CLI. This configuration requires you to specify the specific tcpdump command, pod name and includes a timeout. The command provides filtering options. You can filter traffic by protocol, port, source, or destination. These options help you capture only the necessary data.

Captured files follow a specific naming pattern, here is an example for file naming pattern: tcpdump_${TARGET_POD}_${TIMESTAMP}.pcap.

The utility checks local disk usage before execution:

Note

- If disk usage is below 80 percent, the utility continues normal operation.
- If disk usage is between 80 and 95 percent, the utility shows a warning and continues.
- If disk usage exceeds 95 percent, the utility shows a warning and blocks execution.

Restrictions while Using TCP Dump Functionality

The tcpdump functionality has the following restrictions

- A single tcpdump execution cannot exceed 100 seconds.
- The system limits parallel execution to a maximum of three simultaneous capture commands.
- For more than one capture operation, the maximum timeout is 90 seconds.
- The utility does not support multiple pod names as a single command line interface input.

Capture Network Traffic Using tcpdump Functionality in PCF System

Use this procedure to capture network traffic on a specific pod within the PCF system using the `tcpdump` functionality.

Before you begin

Ensure that you are connected to the Ops Center to execute the command.

Procedure

Step 1 To initiate network traffic capture, use the pcf-system tcpdump capture command along with its required parameters.

pcf-system tcpdump { capture | clear }

- **capture**: Captures the network traffic using tcpdump command in specified pod.
- **clear**: Clears all files from backup destination.

Step 2 Execute the exact command and enter the podname, and timeout value.

pcf-system tcpdump capture { command | podname | timeout }

- **command**: Specify the exact tcpdump command to run inside the pod.
- **podname**: Specify the name of the pod where tcpdump must be executed (supported Pods: pcf-rest-ep, diameter-ep, pcf-engine, pcf-ldapserver-ep).
- **timeout**: Specify the maximum duration for tcpdump execution in seconds. The maximum value for timeout duration is 100 seconds.

Configure tcpdump Backup Server details

Use this procedure to set up the details for backing up `tcpdump` files to an SCP server and configure automatic cleanup.

Before you begin

Ensure that you are connected to the Ops Center to execute the command.

Procedure

Step 1 Configure the SCP server details, backup path, and cleanup options for tcpdump files.

debug tcpdump-backup { scp-server-dest-backup-path *scp_server_dest_backup_path* **| scp-server-user-ip** *scp_server_user_ip* **| scp-server-user-name** *scp_server_user_name* **| scp-server-user-password** *scp_server_user_password* **| cleanup-enabled }**

- **scp-server-dest-backup-path** *scp_server_dest_backup_path*: Specify the destination path for backup files in SCP server.
- **scp-server-user-ip** *scp_server_user_ip*: Specify the host IP of SCP server.
- **scp-server-user-name** *scp_server_user_name*: Specify the username for SCP server authentication.
- **scp-server-user-password** *scp_server_user_password*: Specify the host password of SCP server.
- **cleanup-enabled** : Enables automatic cleanup of tcpdump files after successful transfer.

Step 2 Save and commit the configuration.