vDRA

Add Per Diameter Peer Connection TCP Statistics

Table 1: Summary Data

Applicable Product(s) or Functional Area	vDRA
Applicable Platform(s)	Not Applicable
Default Setting	Enabled - Always-on
Related Changes in This Release	Not Applicable
Related Documentation	Not Applicable

Table 2: Revision History

Revision Details	Release
First introduced	22.2.0

Feature Description

In CPS vDRA, you can monitor statistics for each physical interface using *link_state* KPI to figure out which interface is up or down at each Virtual Machine (VM). However, this does not provide more information about latency or any other errors on the network.

In CPS 22.2.0 and later releases, vDRA provides more information about the statistics of these network interfaces, which allows you to narrow down errors in peer connections on a particular interface.

Enabling the TCP statistics per diameter interface allows you to::

- Fetch the required network interface statistics during issues or troubleshooting.
- Receive information about dropped packets within any specific interfaces and determine if any peer connections went bad due to issues in physical interfaces.
- Monitor the network latency at regular intervals for the same purpose.
- Get get the information of these network interfaces by querying the Prometheus data stores.
- Get the same information over a time in Grafana for all the Prometheus data stores.
- Collect the SAR reports to check the network bandwidth over a time for the specific interfaces.

Benchmarking Zulu in DRA

Feature Summary and Revision History

Table 3: Summary Data

Applicable Product(s) or Functional Area	vDRA
Applicable Platform(s)	Not Applicable
Default Setting	Enabled - Always-on
Related Changes in This Release	Not Applicable
Related Documentation	Not Applicable

Table 4: Revision History

Revision Details	Release
First introduced	22.2.0

Feature Description

In the CPS 22.2.0 release, DRA supports both Zing and Zulu JVM software. Zing is the default software used in 22.2.0 release:

- **Enabling Zing and Zulu in DRA –** DRA supports both Zing and Zulu JVMs. While Zing is existing supported JVM, Zulu is added newly from 22.2.0 with limited qualification [Only FPAS]. User can chose

to enable either Zing or Zulu.. When Zulu is enabled, the following Zing related containers get terminated from DRA Worker and Director VMs:

- Haproxy-zvision
- Zvision

To enable Zulu/Zing through CLI, use the following commands:

- **dra jvm zulu enable** – Enables Zulu as default JVM.
- **dra jvm zing enable** – Enables Zing as default JVM.
- **show dra jvm** – Displays the default JVM service.

Note Zulu is qualified only in fPAS environment with SLA lock timeout disabled. For vPAS, it is not qualified and hence not recommended to enable in vPAS.

Deploy all VMs using Hypervisor

Feature Summary and Revision History

Table 5: Summary Data

Applicable Product(s) or Functional Area	vDRA
Applicable Platform(s)	Not Applicable
Feature Default	Enabled – Always-on
Related Changes in This Release	Not Applicable
Related Documentation	*CPS vDRA Installation Guide for VMware*

Revision History

Revision Details	Release
First introduced.	22.2.0

Feature Description

During ESXI upgrades, when VMs deployed in a single hypervisor are down, you can install all VMs from a particular blade using a single command **--hypervisor** flag with the hypervisor name.

CPS commands on vDRA can perform the following functionalities:

- Recognize a **--hypervisor** tag to fetch VM's that are tagged with the ESXIHOST value in their *vm.esxi.env* file.

- Recognize a **--addartifact** tag to perform operations on more than one artifact file. You can also use the **--hypervisor** tag on top of it to filter VMs.

Health Checks

Using the **--hypervisor** option that you can perform health check of docker engine and consul status of other VMs before making changes on the requested VM.

Configuration and Restrictions

Perform the health check only if the master VM is active. If there are no master VMs, then a prompt message appears indicating you to skip the health check and proceed to the next step because of master unavailability. You can choose Yes or No.

It is always recommended that you perform a manual check and consul status of docker engine, and other similar states of alternate VMs before proceeding with the deployments using *--hypervisor* option. Copy *cps.pem* keys that can be used for performing SSH to master VMs to `/data/deployer/envs` folder

For more information, see the *Deploy all VMs with or without a Hypervisor flag* section in the *CPS vDRA Installation Guide for VMware*.

Ensuring Equal Priority on Health Checks

Feature Summary and Revision History

Table 6: Summary Data

Applicable Product(s) or Functional Area	vDRA
Applicable Platform(s)	Not Applicable
Feature Default	Disabled – Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *CPS vDRA Administration Guide* • *CPS vDRA Operations Guide*

Revision History

Revision Details	Release
First introduced.	22.2.0

Feature Description

vDRA ensures that health checks for critical processes have equal priority to the monitored entity process using the **system-config get-cpu-priority** and **system-config set-cpu-priority** CLI commands.

For more information, see the CLI Commands section in the *CPS vDRA Operations Guide* and *DRA Health Checks* section in the *CPS vDRA Administration Guide*.

Fluentbit Log Forwarding without Authentication

Feature Summary and Revision History

Table 7: Summary Data

Applicable Product(s) or Functional Area	vDRA
Applicable Platform(s)	Not Applicable
Default Setting	Disabled- Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	*CPS vDRA Operations Guide*

Table 8: Revision History

Revision Details	Release
First introduced	22.2.0

Feature Description

In CPS 22.2 release, vDRA supports log forwarding to the external server in either of the 2 ways / or in both ways:

- **External fluentbit instance without authentication**: vDRA supports log forwarding to the external server without authentication through a CLI command. The **log-forward fluentbit external-forward** CLI can send the logs to another external server where fluentbit or fluentd is configured. This external server in turn forward logs to elasticsearch based on configuration provided by user at the external server.

Note The **log-forward fluentbit external-forward** CLI takes threshold input as IP and Port of the external server.

- **Elasticsearch with authentication**: Enables or disables log forwarding to elasticsearch.

Note Recommendation is to use any one of the above external forwarding only at a time and not to use both.

For more information, see the *CLI Commands* section in the *CPS vDRA Operations Guide*.

TLS Support for Diameter Encryption

Feature Summary and Revision History

Table 9: Summary Data

Applicable Product(s) or Functional Area	vDRA
Applicable Platform(s)	Not Applicable
Default Setting	Enabled – Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	Not Applicable

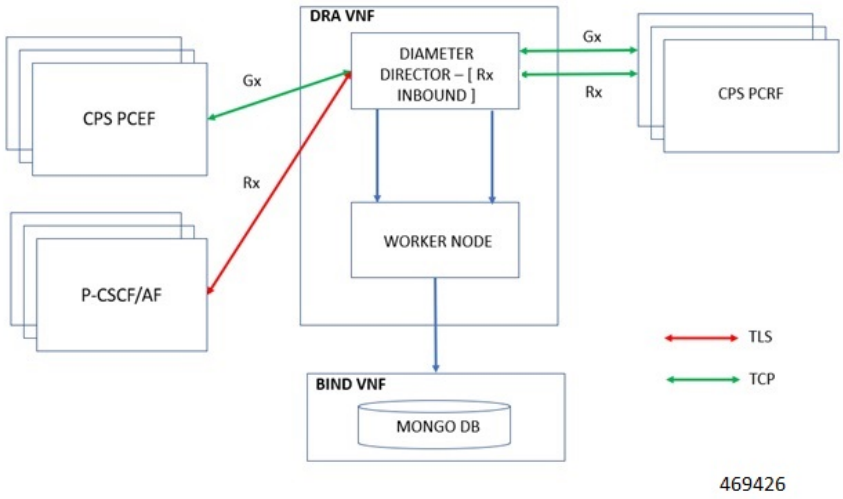
Table 10: Revision History

Revision Details	Release
First introduced	22.2.0

Feature Description

The vDRA supports a Transport Layer Security (TLS) secure channel for diameter peer connection. The following architecture describes TLS in DRA.

Figure 1: TLS in DRA



Following standards/functionalities are supported:

- Only compliant to RFC 6733 [Establishment of TLS connection before exchanging CER/CEA messages]
- Only Inbound configuration is supported for TLS.
- Only Rx protocol is supported with TLS.
- Certificate authentication is supported with the current feature:
  - Client CA certificate authentication is performed only using issuer-based authentication approach.
  - Supports certificate import option on server and user can generate their certificate.
  - Import certificate using CLI command is supported.
  - Third party certificates are required.

Following standards/functionalities are not supported:

- Other type of authentication to be treated as separate requirement.
- Backward compatibility support RFC 3588.
- Default certificate are not provided or packed in the ISO image.
- No other protocols other than Rx is supported for TLS.
- Outbound configurations for TLS.
- MTLS is not supported.
- Validation of TLS for vPAS.
- Inservice Certificate management.
- Certificate Expiry notification.

Before you Begin

- Ensure to input CA certificate to install and initiate the secured TLS connection in the Diameter application.
- Single CA certificate should be used for all TLS connection per site.

vDRA allows you to enable a connection as TLS in the Policy Builder and supports import of certificate through **dra-tls cert import <certificate file> <private file>** CLI command. For more information, see the *Enable TLS Option in the Policy Builder* and *Import Certificate through CLI* sections in the *CPS vDRA Configuration Guide*.

Configuration and Restrictions

Following are the configuration and restrictions:

- Install CA certificates through CLI before initiating the Stack from the Diameter PB configuration.
- Use the CLI command to place the java key store file to the desired location.
- Due to .pem files for certificate and private key support, place files in `/data/orchestrator/pemKey/` master VM.

- After completion of the certificate import, the new keystore file is placed in the `/etc/tls/certs/` folder in the diameter container.

  The keystore credentials will be encrypted and placed as part of application property file and it will be decrypted and used in the application

Improving Visibility on Relay Traffic Timeouts or Failures

Feature Summary and Revision History

Table 11: Summary Data

Applicable Product(s) or Functional Area	vDRA
Applicable Platform(s)	Not Applicable
Feature Default	Enabled – Always-on
Related Changes in This Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Revision Details	Release
First introduced.	22.2.0

Feature Description

vDRA allows you to differentiate failed requests and identify whether the failed calls are locally routed or relayed.

With this release, **site_id** parameter is added to the existing KPI parameters in Grafana.

- diameter_request_total
- diameter_request_timeout_total
- diameter_message_timeout_total

For more information, see the *Statistics/KPI Additions or Changes*.

IPv6 Address Zone Range Validation

Feature Summary and Revision History

Table 12: Summary Data

Applicable Product(s) or Functional Area	vDRA
Applicable Platform(s)	Not Applicable
Feature Default	Enabled – Always-on
Related Changes in This Release	Not Applicable
Related Documentation	• *CPS vDRA Operations Guide* • *CPS vDRA Administration Guide*

Revision History

Revision Details	Release
First introduced.	22.2.0

Feature Description

In CPS vDRA 22.2.0 and later releases, vDRA supports the IPv6 address validation in the IPv6 Range System ID Mapping CRD table and while configuring IPv6 zone ranges in the CLI.

Note During multi_table update, if any row gets failed due to conflict then entire Custom Reference Data (CRD) table is not updated. Displays a warning message after updating CRD successfully.

For more information see, the *CLI Commands* section in the *CPS vDRA Operations Guide* and *Regular Expression* parameter description in the *CPS vDRA Administration Guide.*

KPI Support to Account the Remote Peers Count

Feature Summary and Revision History

Table 13: Summary Data

Applicable Product(s) or Functional Area	vDRA
Applicable Platform(s)	Not Applicable
Default Setting	Enabled - Always-on

Related Changes in This Release	Not Applicable
Related Documentation	*CPS vDRA SNMP and Alarms Guide*

Table 14: Revision History

Revision Details	Release
First introduced	22.2.0

Feature description

In the CPS 22.2.0 and later releases, vDRA allows you to track a count of active peers (local and active according to the remote peer policy) that are known to a local site.

In Grafana, you can identify the *active_peer_count* KPI with *app_id* and *system_id* parameters in the Peer traffic monitor dashboard.

Configurations and Restrictions

You can configure Grafana and bulk statistics with the *active_peer_count* KPI.

Configure the *PEER_LIMIT_FOR_SITE_EXCEEDED* Alert with this KPI along with *peer_connection_status* to alert when total peers crossed the supported number per site.

For more information on alarms, see the *Sample Alert Rules Table* in the *CPS vDRA SNMP and Alarms Guide*.

Note While deriving a threshold, you can consider the remote policy.

Preventing a Repository from Corruption and Publishing a Corrupted repository

Table 15: Summary Data

Applicable Product(s) or Functional Area	vDRA
Applicable Platform(s)	Not Applicable
Default Setting	Disabled configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	*CPS vDRA Administration Guide* *CPS vDRA Operations Guide*

Table 16: Revision History

Revision Details	Release
First introduced	22.2.0

Feature Description

In the Policy Builder, during the import and publish process, if there is any invalid or incomplete data being imported it overwrites the current configuration in the SVN. During publishing there is a possibility that the imported data can corrupt the application cache. This can affect the traffic until the data is recovered.

To overcomme this issue, the CPS vDRA provides additional validation facility on the imported data before publishing. vDRA returns appropriate error messages if the import or publish is not successful due to any validation failure.

For more information , see the *Publish Configuration Changes* section in the *CPS vDRA Administration Guide* and the *dra policy-builder-must-plugins plugins-name* CLI section in the *CPS vDRA Operations Guide*.

Set Alarm Severity Based on Configurable Thresholds

Feature Summary and Revision History

Table 17: Summary Data

Applicable Product(s) or Functional Area	vDRA
Applicable Platform(s)	Not Applicable
Feature Default	Enabled – Always-on
Related Changes in This Release	Not Applicable
Related Documentation	*CPS vDRA SNMP and Alarms Guide*

Revision History

Revision Details	Release
First introduced.	22.2.0

Feature Description

In CPS 22.2.0 and later releases, vDRA allows you to:

- Configure thresholds parameter with threshold input as comma separated fields at the time of Alarm severity setup.

Note The **threshold** parameter is optional. This is because not all alerts will have different thresholds.

- Configure the following two type of alerts expression:
  - ascending threshold [HIGH_CPU_USAGE]
  - descending threshold [LOW_MEMORY]

For more information, the *Component Notifications* table and *Configure Different Thresholds* sections in the *CPS vDRA SNMP and Alarms Guide*.

User Audit Enhancements

Feature Summary and Revision History

Table 18: Summary Data

Applicable Product(s) or Functional Area	vDRA
Applicable Platform(s)	Not Applicable
Default Setting	Enabled - Always-on
Related Changes in This Release	Not Applicable
Related Documentation	Not Applicable

Table 19: Revision History

Revision Details	Release
First introduced	22.2.0

Feature Description

In the CPS 22.2.0 and later releases, in vDRA, User Audit feature supports the following functionalities:

- Tracks events that are related to user login or logout details in JSON format at the external server.
- Allows you to obtain information that is related to a login or logout for the user.
- Verifies if the action is triggered by the system or kernel or user.
- Allows you to forward them to the external server or Elasticsearch and filter information of these details with specific keywords, which can feed the data to the external tool in JSON format.
- Tracks events that are related to peer connections and tracks peer disconnects /admin disable details.