Ultra Cloud Core Common Data Layer, Release 1.6 - Release Change Reference

First Published: 2021-10-29

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

CONTENTS

CHAPTER 1

About this Guide

Note The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. While any existing biased terms are being substituted, exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

This RCR is applicable to the Common Data Layer (CDL). It provides information on new and modified features and behavior changes added in this release branch.

This Release Change Reference (RCR) describes new and modified feature and behavior change information for the applicable CDL release(s).

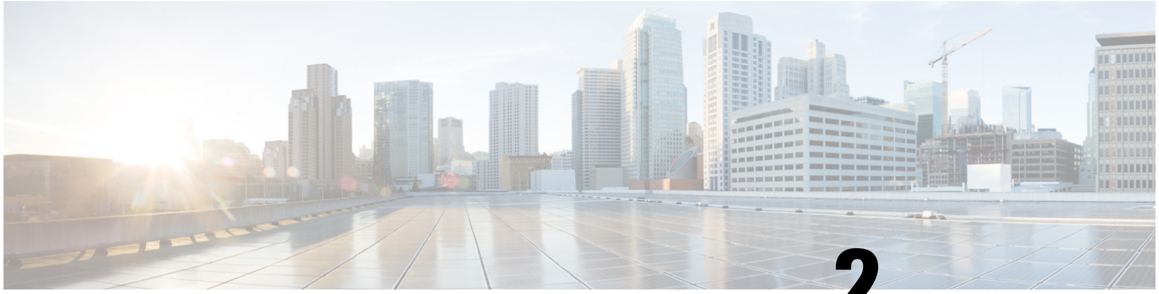
Conventions Used

The following tables describe the conventions used throughout this documentation.

Notice Type	**Description**
Information Note	Provides information about important features or instructions.
Caution	Alerts you of potential damage to a program, device, or system.
Warning	Alerts you of potential personal injury or fatality. May also alert you of potential electrical hazards.

Typeface Conventions	**Description**
Text represented as a `screen display`	This typeface represents displays that appear on your terminal screen, for example: `Login:`

Typeface Conventions	Description
Text represented as **commands**	This typeface represents commands that you enter, for example: **show ip access-list** This document always gives the full form of a command in lowercase letters. Commands are not case sensitive.
Text represented as a **command** *variable*	This typeface represents a variable that is part of a command, for example: **show card** *slot_number* *slot_number* is a variable representing the desired chassis slot number.
Text represented as menu or sub-menu names	This typeface represents menus and sub-menus that you access within a software application, for example: Click the **File** menu, then click **New**



CHAPTER 2

UCC CDL, Release 1.6 - Release Change Reference

Feature and Behavior Changes Quick Reference

Feature/Behavior Changes	Introduced/Modified
CDL IPv6 Support, on page 4	1.6
Enhancements in Kafka for CDL, on page 8	1.6
Index Overwrite Detection Prefix Key Label, on page 10	1.6
Local and Remote Site Version Conflict Notification, on page 11	1.6

Feature Defaults Quick Reference

The following table indicates what features are enabled or disabled by default.

Feature	Default
CDL IPv6 Support	Disabled – Configuration Required
Enhancements in Kafka for CDL	Disabled – Configuration Required
Index Overwrite Detection Prefix Key Label	Disabled – Configuration Required
Local and Remote Site Version Conflict Notification	Disabled – Configuration Required

CDL IPv6 Support

Feature Summary and Revision History

Summary Data

Applicable Product (s) or Functional Area	• KVM-based application deployment support • PCF 2021.04.0 and later
Applicable Platforms	Bare Metal, OpenStack, VMware
Feature Default Setting	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Revision Details	Release
First introduced.	CDL 1.6.0

Feature Description

In this release, the CDL supports IPv6, thus enabling the dual stack support for its endpoints in a GR enabled setup. Dual stack enables networking devices to be configured with both IPv4 and IPv6 addresses.

This feature provides the following functionality:

- IPv6 support for the CDL endpoints.
- IPv6 support for communicating between Mirror Maker and Kafka brokers.
- TLS support for CDL and Kafka IPv6 endpoints.

Note To get IPv6 support in CDL, the K8s cluster must support dual stack and it must be enabled in the cluster.

Configuring the IPv6 Support

To configure IPv6 support for CDL in a GR enabled setup, use the CLI commands or configuration in the following steps:

1. Expose the CDL IPv6 endpoint and connect to remote site IPv6 endpoint.

a. Enable CDL geo replication.

```
config
   cdl enable-geo-replication true
```

b. Configure the external IP address for CDL endpoints. In addition to the **endpoint external-ip**, configure the **endpoint external-ipv6** parameter too.

```
config
   cdl datastore session endpoint external-ipv6 IPv6_address
```

c. Configure the CDL endpoints for remote site.

```
config
   cdl remote-site system_id
      db-endpoint host IPv6_address
      db-endpoint port 8882
   exit
```

Note The IPv4 and IPv6 endpoints can be accessed over the same port (default value is 8882).

Note Currently, the CDL can connect to remote site endpoints using either IPv4 or IPv6, but not both. However, it can simultaneously expose both the IPv4 and IPv6 endpoints for the remote site to connect to either one of them.

2. Expose the CDL Kafka and connect to remote site Kafka over IPv6.

   a. Configure the external IP address and port for all Kafka replicas.

```
config
   cdl kafka external-ipv6 IPv6_address port_address
   exit
```

Note You must configure IPv6 for each broker separately. It is possible to simultaneously expose the Kafka brokers over IPv4 and IPv6, but the ports used must be different. Currently, the Kafka listeners do not support using the same port for different IP addresses.

   b. Configure the remote site Kafka configuration.

   Mirror Maker can connect to both local site and remote site Kafka brokers either over IPv4 and IPv6 or only one of them.

   Configure the remote kafka-server separately using the following CLI command:

```
config
   cdl remote-site system_id
      kafka-server IPv6_address port_address
   exit
```

3. (Optional step) Configure the SSL/TLS certificates to enable TLS support for both local and remote sites. These certificates help to establish a secure connection between the local and remote sites.

   Use the same configuration to configure the certificates on each site.

   a. Enable SSL for CDL endpoint.

   ```
   config
      cdl ssl-config enable true
   ```

   b. Configure the certificates.

   ```
   config
      cdl ssl-config certs external_ipv6_address
         ssl-key ssl_key
         ssl-crt ssl_crt
         ssl-ca ssl_ca
      exit
   ```

   NOTES:

   - **ssl-key** *ssl_key* - Specify the Private key of server.
   - **ssl-crt** *ssl_crt* - Specify the CA signed server certificate.
   - **ssl-ca** *ssl_ca* - Specify the Public CA certificate.

4. (Optional step) Configure the SSL/TLS certificates to enable TLS support for Kafka endpoints.

   a. Enable SSL for CDL endpoint.

   ```
   config
      cdl ssl-config enable true
   ```

   b. Enable SSL for Kafka endpoint.

   ```
   config
      cdl kafka ssl-settings enable-ssl true
      cdl kafka ssl-settings disable-host-name-verification true
   ```

   c. Configure the certificates for Kafka endpoints on both local and remote sites.

   ```
   config
      cdl ssl-config certs external_ipv6_address
         ssl-key ssl_key
         ssl-crt ssl_crt
         ssl-ca ssl_ca
      exit
   ```

   The following sample configuration is used to connect to remote site IPv6 TLS endpoints and IPv6/IPv4 TLS Kafka:

   Site-1 Configuration

   ```
   cdl remote-site 2
    db-endpoint host 2001:DB8:54ff:a4::139:250
    db-endpoint port 8882
    kafka-server 10.106.139:250 10092
    ssl-port 10094
    exit
   ```

```
 kafka-server 10.106.139:250 10093
 ssl-port 10095
 exit
 kafka-server 2001:DB8:54ff:a4::139:250 10096
 ssl-port 10098
 exit
 kafka-server 2001:DB8:54ff:a4::139:250 10097
 ssl-port 10099
 exit
exit
cdl ssl-config enable true
cdl ssl-config certs 2001:DB8:54ff:a4::139:250
    ssl-key  “<server-key>”
    ssl-crt  “<signed-certificate>”
    ssl-ca  “<ca-certificate>”
exit
cdl ssl-config certs 192.0.2.2
    ssl-key  “<server-key>”
    ssl-crt  “<signed-certificate>”
    ssl-ca  “<ca-certificate>”
exit
cdl ssl-config certs 192.0.2.1
    ssl-key  “<server-key>”
    ssl-crt  “<signed-certificate>”
    ssl-ca  “<ca-certificate>”
exit
cdl ssl-config certs 2001:DB8:54ff:a4::139:249
    ssl-key  “<server-key>”
    ssl-crt  “<signed-certificate>”
    ssl-ca  “<ca-certificate>”
exit
cdl datastore session
 geo-remote-site [ 2 ]
 endpoint external-ip 192.0.2.1 endpoint external-ipv6 2001:DB8:54ff:a4::139:249
exit
cdl kafka ssl-settings enable-ssl true
cdl kafka ssl-settings disable-host-name-verification true
cdl kafka external-ipv6 2001:DB8:54ff:a4::139:249 10096
 ssl-port 10098
exit
cdl kafka external-ipv6 2001:DB8:54ff:a4::139:249 10097
 ssl-port 10099
exit
cdl kafka external-ip 10.106.139.249 10092
 ssl-port 10094
exit
cdl kafka external-ip 10.106.139.249 10093
 ssl-port 10095
exit
```

Site-2 Configuration

```
cdl remote-site 1
 db-endpoint host 2001:DB8:54ff:a4::139:249
 db-endpoint port 8882
 kafka-server 10.106.139:249 10092
 ssl-port 10094
 exit
 kafka-server 10.106.139:249 10093
 ssl-port 10095
 exit
 kafka-server 2001:DB8:54ff:a4::139:249 10096
 ssl-port 10098
 exit
 kafka-server 2001:DB8:54ff:a4::139:249 10097
 ssl-port 10099
 exit
exit
cdl ssl-config enable true
cdl ssl-config certs 2001:DB8:54ff:a4::139:249
    ssl-key  “<server-key>”
    ssl-crt  “<signed-certificate>”
    ssl-ca  “<ca-certificate>”
exit
cdl ssl-config certs 192.0.2.1
    ssl-key  “<server-key>”
    ssl-crt  “<signed-certificate>”
    ssl-ca  “<ca-certificate>”
exit
cdl ssl-config certs 192.0.2.1
    ssl-key  “<server-key>”
    ssl-crt  “<signed-certificate>”
    ssl-ca  “<ca-certificate>”
exit
cdl ssl-config certs 2001:DB8:54ff:a4::139:250
    ssl-key  “<server-key>”
    ssl-crt  “<signed-certificate>”
    ssl-ca  “<ca-certificate>”
exit
cdl datastore session
 geo-remote-site [ 1 ]
 endpoint external-ip 192.0.2.1
 endpoint external-ipv6 2001:DB8:54ff:a4::139:250
exit
cdl kafka ssl-settings enable-ssl true
cdl kafka ssl-settings disable-host-name-verification true
cdl kafka external-ipv6 2001:DB8:54ff:a4::139:250 10096
 ssl-port 10098
exit
cdl kafka external-ipv6 2001:DB8:54ff:a4::139:250 10097
 ssl-port 10099
exit
cdl kafka external-ip 192.0.2.1 10092
 ssl-port 10094
exit
cdl kafka external-ip 192.0.2.1 10093
 ssl-port 10095
exit
```

Enhancements in Kafka for CDL

Feature Summary and Revision History

Summary Data

Applicable Product (s) or Functional Area	• KVM-based application deployment support • PCF 2021.04.0 and later
Applicable Platforms	Bare Metal, OpenStack, VMware

Feature Default Setting	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	*UCC CDL Configuration and Administration Guide*

Revision History

Revision Details	Release
First introduced.	CDL 1.6.0

Feature Description

In this release, the CDL supports enhancements in Kafka operations.

New CLI commands are introduced to support the following basic Kafka operations:

- List Kafka topics
- Describe Kafka topic(s)
- List Kafka consumer groups
- Describe Kafka consumer group(s)
- Reset Kafka consumer offset(dry-run/execute)

This feature also enables parallel pod management for Kafka and Zookeeper. As part of this particular enhancement, the CDL index can connect to Kafka before doing the remote index sync. This functionality ensures that the topics are created and Mirror Maker is ready to replicate messages from the remote site even before the gRPC sync starts.

Configuring the Kafka Enhancements

Configuring the Parallel Pod Management

To configure the parallel pod management for Kafka and Zookeeper, use the following CLI commands or configuration:

Kafka:

```
config
  cdl kafka enable-parallel-pod-management {true | false}
```

Zookeeper:

```
config
  cdl zookeeper enable-parallel-pod-management {true | false}
```

Index Overwrite Detection Prefix Key Label

Feature Summary and Revision History

Summary Data

Applicable Product (s) or Functional Area	• KVM-based application deployment support • PCF 2021.04.0 and later
Applicable Platforms	Bare Metal, OpenStack, VMware
Feature Default Setting	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	*UCC CDL Configuration and Administration Guide*

Revision History

Revision Details	**Release**
First introduced.	CDL 1.6.0

Feature Description

In this release, the CDL supports a new label, **prefix** for the following existing metrics:

- overwritten_index_records_deleted
- overwritten_index_records_skipped

Example:

```
metric: overwritten_index_records_deleted
    description: "Total number of records deleted due to overwritten/duplicate unique keys
 at index"
    sampleQuery: "overwritten_index_records_deleted"
    labels:
    -  label: errorCode
       description: "The errorCode in the DB response for deletion"
       example: "0, 502"
    -  label: sliceName
       description: "The name of the logical sliceName"
       example: "session"
    -  label: prefix
       description: "The unique key prefix pattern that detected the stale record"
       example: "uk1"
```

```
metric: overwritten_index_records_skipped
   description: "Total number of unprocessed stale records due to queue being full"
   sampleQuery: "overwritten_index_records_skipped"
```

```
labels:
-  label: action
   description: "action that was supposed to be performed for the stale record"
   example: "delete, notify"
-  label: sliceName
   description: "The name of the logical sliceName"
   example: "session"
-  label: prefix
   description: "The unique key prefix pattern that detected the stale record"
   example: "uk1"
```

Local and Remote Site Version Conflict Notification

Feature Summary and Revision History

Summary Data

Applicable Product (s) or Functional Area	• KVM-based application deployment support • PCF 2021.04.0 and later
Applicable Platforms	Bare Metal, OpenStack, VMware
Feature Default Setting	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Revision Details	**Release**
First introduced.	CDL 1.6.0

Feature Description

If the Update request is received for the same session on two different sites at the same time, the requests are successful locally, but while replicating to the remote site, a version conflict is detected. This leads to inconsistency of the data between the CDL sites. For all such version conflicts, this feature enables CDL to send the original session data and the request data along with the conflict notification toward the NF for appropriate conflict resolution.

Configuring the Site Version Conflict Notification

To enable this feature, use the following CLI commands or configuration:

```
config
   cdl datastore session slot notification include-conflict-data {true |
false}
```