Oracle® Enterprise Communications Broker

Release Notes

Release P-Cz4.2.0

F88126-01

July 2024

Oracle Enterprise Communications Broker Release Notes, Release P-Cz4.2.0

F88126-01

Contents

About This Guide

The Oracle Enterprise Communications Broker (Communications Broker) Release Notes provides the following information about the Communications Broker hardware and software.

- Specifications and requirements
- Upgrades and downgrades
- New features and enhancements
- Known issues, caveats, and limitations

Documentation Set

The following table describes the documentation set for the Communications Broker.

Document Name	Document Description
Release Notes	Contains information about the current release, including specifications, requirements, new features, enhancements, inherited features, known issues, caveats, and limitations.
Administrator's Guide	Describes how to deploy the system.
User's Guide	Describes how to configure SIP signaling management and how to tailor the system to specific needs.
Help system	Contains task-oriented topics for configuring, administering, maintaining, and troubleshooting the Communications Broker hardware and software.
SBC Family Security Guide	Provides information about security considerations and best practices from a network and application security perspective for the Session Border Controller family of products.

Related Documentation

The following table describes related documentation for the Communications Broker.

Document Name	Document Description
Installation and Platform Preparation Guide	Contains conceptual and procedural information for system provisioning, software installations, and upgrades.

Revision History

The following table lists changes to this document and the corresponding dates of publication.

Date	Description
July 2024	Content updates for Communications Broker Release 4.2.0.

My Oracle Support

My Oracle Support (https://support.oracle.com) is your initial point of contact for all product support and training needs. A representative at Customer Access Support (CAS) can assist you with My Oracle Support registration.

Call the CAS main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. When calling, make the selections in the sequence shown below on the Support telephone menu:

1. Select `2` for New Service Request.
2. Select `3` for Hardware, Networking, and Solaris Operating System Support.
3. Select one of the following options:
   - For technical issues such as creating a new Service Request (SR), select `1`.
   - For non-technical issues such as registration or assistance with My Oracle Support, select `2`.

You are connected to a live agent who can assist you with My Oracle Support registration and opening a support ticket.

My Oracle Support is available 24 hours a day, 7 days a week, 365 days a year.

Emergency Response

In the event of a critical service situation, emergency response is offered by the Customer Access Support (CAS) main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability
- Loss of the system's ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions
- Loss of access for maintenance or recovery operations
- Loss of the system ability to provide any required critical or major trouble notification

Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with Oracle.

Locate Product Documentation on the Oracle Help Center Site

Oracle Communications customer documentation is available on the web at the Oracle Help Center (OHC) site, http://docs.oracle.com. You do not have to register to access these documents. Viewing these files requires Adobe Acrobat Reader, which can be downloaded at http://www.adobe.com.

1. Access the Oracle Help Center site at http://docs.oracle.com.
2. Click **Industries**.
3. Under the Oracle Communications sub-header, click the **Oracle Communications documentation** link.
   The Communications Documentation page appears. Most products covered by these documentation sets appear under the headings "Network Session Delivery and Control Infrastructure" or "Platforms."
4. Click on your Product and then Release Number.
   A list of the entire documentation set for the selected product and release appears.
5. To download a file to your location, right-click the **PDF** link, select **Save target as** (or similar command based on your browser), and save to a local folder.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

1

Specifications and Requirements

Oracle recommends that you review the following information before installing the software.

Supported Platforms

The following platforms are supported in Oracle Enterprise Communications Broker - (will be referred to by it's short name - Communications Broker).

Platforms

For all the platforms listed here, you must install the Operating System and software from a USB memory device

- Oracle X9-2
- Oracle X8-2
- Go to My Oracle Support (MOS) at https://support.oracle.com to download the Operating System and software. See "Download Software from MOS."
- See the Software Installation information in the Oracle Enterprise Session Border Controller Installation and Platform Preparation Guide for installation instructions.

Image and Boot Loader Files

The Release 4.2.0 release uses the following ISO, image and boot loader files:

Table 1-1 Image and Bootloader Files

Component	Description
nnPCZ420-img.iso	ISO file
nnPCZ420.bz	Image file
nnPCZ420.boot	Boot loader
nnPCZ420-img-vm_kvm.tgz	Compressed image file including Communications Broker VNF for KVM virtual machines, Oracle Cloud Infrastructure (OCI), AWS EC2.
nnPCZ420-img-vm_vmware.ova	Open Virtualization Archive (.ova) distribution of the Communications Broker VNF for ESXi virtual machines.
nnPCZ420-img-vm_vhd.tgz	Compressed image file including Communications Broker for Azure, as well as the legal.txt file

Cores and Threads

The following list shows the recommended number of cores and the expected number of SIP threads per platform. Note that the number of SIP threads may vary, depending on the configuration of your deployment.

- VM—Recommended 8 cores. Yields 3 SIP threads.
- Oracle Servers X8-2, and X9-2 — Recommended 16 cores. Yields 9 SIP threads.

Memory

Oracle recommends at least 16G memory for all Communications Broker Release 4.2.0 deployments.

While the above presents standard recommendations, optimum Communications Broker resource sizing depends individual deployments. Oracle recommends that you work with consulting and/or sales teams to determine the best sizing for your deployment.

Supported Hypervisors

Supported Hypervisor for Private Virtual Infrastructures in Communications Broker Release 4.2.0:

- VMWare vSphere ESXi 7.0.
- KVM
- - Linux kernel version: 3.10.0-1127
  - Library: libvirt 4.5.0
  - API: QEMU 4.5.0
  - Hypervisor: QEMU 1.5.3

> **Note:**
>
> Starting with Communications Broker Release 4.2.0, X7-2 is not supported as a VMWare hypervisor.

Browser Requirements

Communications Broker Release 4.2.0 supports the following browser versions for navigating and configuring the GUI:

- Edge: 102.0.1245.30 and later
- Firefox 91.9.0esr and later
- Google Chrome (Recommended)—101.0.4951.67 and later

Download Software from MOS

When you want to get a software release or a patch from Oracle, go to My Oracle Support (MOS) and download it to your system or to a USB memory device.

- Establish an account with My Oracle Support.

The following procedure requires you to enter your MOS credentials to log on.

1. Go to https://support.oracle.com and log on.
2. Click the **Patches & Updates** tab.
3. On the Patch Search pane, click the **Search** tab.
4. On the Search dialog, do the following:
   a. Product is—Select a product from the drop-down list.

   b. Release is—Select a release from the drop-down list.

5. Click **Search**.
6. On the Patch Advanced Search Results page, click the patch that you want.

   The system displays information about the patch, and a dialog where you can open the Read Me file and download the software.
7. In the dialog, do the following:
   - Read Me—Click to see the build notes.
   - Download—Click to download the software.
8. Log off.

Platform Boot Loaders

The Communications Broker 4.2.0 platforms require a boot loader to load the operating system and software.

All Release 4.2.0 platforms require that the boot loader and the software image match per release. For example, if the software image file name is nnPCZ420.bz, use the corresponding boot loader file named nnPCZ420.boot.

You can install the boot loader file as /boot/bootloader on the target system. You can also upload the boot file from the Web GUI using the **Upgrade Software** option. When you plan to upgrade the system image, upgrade the boot loader before booting the new system image.

Upgrade Paths

The following in-service (hitless) upgrade and rollback paths are supported by the Communications Broker Release 4.2.0:

Table 1-2 Upgrade Paths

From Version	To Version
P-Cz4.1.0	P-Cz4.2.0
P-Cz4.0.0	P-Cz4.1.0
P-Cz3.3.0	P-Cz4.1.0
P-Cz3.3.0	P-Cz4.0.0

> **Note:**
>
> If you want to rollback or downgrade, ensure that you backup the configuration before performing the upgrade. After rollback, manually restore the saved backup.

All paths require that you meet recommended resource requirements before you upgrade. If necessary, upgrade to supported path versions prior to your upgrade.

When upgrading to Release 4.2.0 from a release older than the previous release, read all intermediate Release Notes documents for notification of incremental changes.

Co-product Support

The following products and features run in concert with the Oracle Enterprise Communications Broker for their respective solutions. Contact your Sales representative for further support and requirement details.

Oracle Communications Session Delivery Manager

Release 4.2.0 can inter-operate with the following versions of the Oracle Communications Session Delivery Manager:

- Enterprise Operations Monitor Release 5.1 and later versions
- FCAPS support from SDM 9.0.3

Schema Upgrade

Oracle Enterprise Communications Broker Release 4.2.0 requires a configuration schema upgrade after upgrading the software to Release 4.2.0. The system prompts you to upgrade the configuration schema the first time you log on as the administrator.

> **Important:**
>
> The upgrade configuration schema is performed when you log on to Communications Broker for the first time after completing an upgrade from a lower version to higher version. You will be prompted to update the config schema ONLY if your upgrade path is any one of the following:
>
> **Table 1-3 Schema Upgrade**
>
> | From | To |
> |---|---|
> | P-Cz 3.1.0 | P-Cz 3.3.0 |
> | P-Cz 3.2.0 | P-Cz 3.3.0 |
>
> If your upgrade path is P-CZ3.3.0 GA (or later releases) -> P-Cz-4.1.0 or P-CZ 4.2.0, you will NOT be prompted to update the config schema. It happens without user intervention.

LDAP Configuration

P-Cz-4.1.0 and later releases expose the RealmID parameter in the LDAP configuration. The configuration upgrade sets Realm ID to "ecb" for existing LDAP configurations.

> **Note:**
>
> Only the "ecb" realm can support LDAP.

ENUM Configuration

Communications Broker Release 4.1.0 exposes the RealmID parameter in the ENUM configuration. The configuration upgrade sets Realm ID to "ecb" for existing ENUM configurations. You can set the Realm ID, as needed, for newly added VLANs.

SPL Support

Communications Broker supports the following Session Plug-in Language (SPL) engines.

- C2.0.0
- C2.0.1
- C2.0.2
- C2.0.9
- C2.1.0
- C2.1.1
- C2.2.0
- C2.2.1
- C2.3.2
- C3.0.0
- C3.0.1
- C3.0.2
- C3.0.3
- C3.0.4
- C3.0.5
- C3.0.6
- C3.0.7
- P1.0.0
- P1.0.1
- C3.1.0
- C3.1.1
- C3.1.2
- C3.1.3
- C3.1.4
- C3.1.5
- C3.1.6
- C3.1.7
- C3.1.8
- C3.1.9
- C3.1.10

- C3.1.11
- C3.1.12
- C3.1.13
- C3.1.14
- C3.1.15
- C3.1.16
- C3.1.17
- C3.1.18
- C3.1.19
- C3.1.20
- C3.1.21

TLS Cipher Updates

Note the following changes to the DEFAULT cipher list.

Oracle recommends the following ciphers, and includes them in the DEFAULT cipher list:

1. TLS_AES_128_GCM_SHA256
2. TLS_AES_256_GCM_SHA384
3. TLS_CHACHA20_POLY1305_SHA256
4. TLS_AES_128_CCM_SHA256
5. TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
6. TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
7. TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
8. TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
9. TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
10. TLS_DHE_RSA_WITH_AES_128_GCM_SHA256

Oracle supports the following ciphers, but does not include them in the DEFAULT cipher list:

1. TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
2. TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
3. TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
4. TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
5. TLS_RSA_WITH_AES_256_CBC_SHA256
6. TLS_RSA_WITH_AES_256_GCM_SHA384
7. TLS_RSA_WITH_AES_128_CBC_SHA256
8. TLS_RSA_WITH_AES_128_CBC_SHA
9. TLS_RSA_WITH_AES_128_GCM_SHA256

Oracle supports the following ciphers for debugging purposes only:

1. TLS_RSA_WITH_NULL_SHA256

2. TLS_RSA_WITH_NULL_SHA
3. TLS_RSA_WITH_NULL_MD5

Oracle supports the following ciphers, but considers them not secure. They are not included in the DEFAULT cipher-list, but they are included when you set the **cipher-list** attribute to **ALL**. When you configure the **cipher-list** to **ALL**, the system provides a **verify-config** message warning you that you are using these insecure ciphers.

1. TLS_AES_128_CCM_8_SHA256 (demoted to weak in 9.3.0)
2. TLS_RSA_WITH_3DES_EDE_CBC_SHA
3. TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
4. TLS_DHE_RSA_WITH_AES_256_CBC_SHA
5. TLS_RSA_WITH_AES_256_CBC_SHA
6. TLS_DHE_RSA_WITH_AES_128_CBC_SHA

To configure TLS ciphers, use the **cipher-list** attribute in the **tls-profile** configuration element.

> **WARNING:**
>
> When you set **tls-version** to either **tlsv1** or **tlsv11** and you want to use ciphers that Oracle considers not secure, you must manually add them to the **cipher-list** attribute. TLS 1.0 and TLS 1.1 are not supported in this release.

> **WARNING:**
>
> TLS 1.0 and TLS 1.1 are not supported in the Communications Broker Release 4.2.0

Documentation Changes

The following information lists and describes the changes made to the documentation set for Oracle Enterprise Communications Broker Release 4.2.0.

Table 1-4 Documentation Updates

Feature	Description
Support for FQDN for LDAP configuration	Administrator Guide
Support for deployment on public cloud - AWS and Azure	Administrator Guide
OJET Uplift (15.1.3) and WebGUI enhancements	• User Guide • Administrator's Guide • Web Help

Table 1-4   (Cont.) Documentation Updates

Feature	Description
Naming abbreviation update	Documentation refers to the product as Oracle Enterprise Communications Broker in the first instance and later occurrences in the documentation is referred to as Communications Broker. • User Guide • Administrator's Guide • Web Help
REST API Support for dialing context	REST API for Communications Broker Release 4.2.0
REFER source agent routing	• User Guide • Administrator's Guide • Web Help

2

New Features in Communications Broker Release 4.2.0

The Communications Broker Release 4.2.0 delivers the following enhancements and new features to improve the functionality, look, and behavior of the software.

Table 2-1 New Features

Feature	Description
Support for FQDN for LDAP configuration	This feature allows Communications Broker to support FQDN LDAP server configuration. The FQDN is further resolved into an IP address. Communications Broker supports both A and SRV FQDN configurations. Communications Broker resolves the IP addresses using the default realm. The resolved IP addresses are used for identifying LDAP servers. This feature provides the flexibility of managing multiple LDAP servers based on LDAP load balancing for A Records, weights and priority for SRV Records. You can modify the LDAP servers where servers can be added or dropped. This makes it easy to support multiple LDAP servers across different LDAP configurations.
Support for deployment on public cloud - AWS and Azure	With Communications Broker Release 4.2.0 you can deploy Oracle Enterprise Communications Broker on the Azure and AWS environments.
OJET uplift (15.1.3), and Web GUI enhancements	The Communications Broker Release 4.2.0 user interface has been upgraded to OJET version 15.1.3 to provide an interactive and seamless user experience.
Naming abbreviation update for Communications Broker	As part of the organization-wide effort to use only the officially approved product names, the usage of the product name has been standardized across GUI, product documentation and Marketing collateral.
REST API Support for Communications Broker dialing context	This feature supports CRUD operations using REST API on the Dial Plan configuration which can be done easily and the response can be verified at the same time. Both Dialing Contexts and Dial Pattern can be viewed, modified, added or deleted using the REST commands. REST API integration is supported on enabling secure HTTPS, making it more reliable and secure to configure Dial Plan parameters.

Table 2-1 (Cont.) New Features

Feature	Description
REFER source agent routing on Communications Broker Release 4.2.0	This feature when enabled, sets the source agent of the INVITE that Communications Broker creates when terminating the REFER, to the agent that sent the REFER message and NOT to the agent from which the original call was received from. When you disable the refer-source-agent-routing, the look-up is based on the Source Agent of the Calling Party. However, the headers of the new INVITE do not change. The overall call flow remains similar, except for the modification of the Source Agent as described above.

3 Caveats, Resolved Issues, Known Issues

Oracle provides behavioral information that you need to know about the release in the form of caveats, known issues, and limitations. A caveat describes behavior that you might not expect, and explains why the system works in a certain way. A known issue describes temporarily incorrect or malfunctioning behavior, and often includes a workaround that you can use until Oracle corrects the behavior. A limitation describes a functional boundary or exclusion that might affect your deployment.

Caveats in Communications Broker Release 4.2.0

The following items provide key information about upgrading and downgrading with Oracle Enterprise Communications Broker Release 4.2.0:

Upgrade and Downgrade Caveats

Platform-Specific Downgrade Limitations

Do not attempt to downgrade Communications Broker to a release not supported by your platform. See the section Supported PlatformsSupported Platforms table for a matrix of platforms and supported releases.

Connection Failures with SSH/SFTP Clients

If you upgrade, and your older SSH or SFTP client stops working, check that the client supports the minimum ciphers required in the ssh-config element. The current default HMAC algorithm is `hmac-sha2-256`. The current key exchange algorithm is `diffie-hellman-group14-sha256`. If a verbose connection log of an SSH or SFTP client shows that it cannot agree on a cipher with the SBC, upgrade your client.

SSH Host Key Algorithms

Session Border Controller offers `rsa-sha2-512` as the default host key algorithm. SSH clients that offer only a `SHA1 hash` algorithm, such as `ssh-rsa`, are not supported; your SSH client must offer a `SHA2 hash` algorithm. If you see an error message: "no matching host key type found", upgrade your SSH client to one that supports SHA2 host key algorithms.

Diffie-Hellman Key Size

For TLS negotiations on SIP interfaces, the default Diffie-Hellman key size offered by the Communications Broker is 1024 bits. The key size is set in the `diffie-hellman-key-size` attribute in the tls-global configuration element. Increasing the key size by setting the key size to 2048 bits significantly decreases performance.

Default TLS Version

Releases prior to Communications Broker Release 4.1.0, do not support TLS1.3. Release Communications Broker does not support TLS 1.0 or TLS1.1. If you are downgrading from Communications Broker Release 4.2.0 to a release prior to Release 4.2.0, set your tls-version to compatibility.

Downgrade Caveat for NTP Configurations using an FQDN

If you create a realm-configuration for providing resolution of FQDNs for NTP servers using the wancom0 interface, Oracle recommends that you remove this wancom0 realm-config before downgrading to a version that does not support FQDNs for NTP servers.

If you retain this configuration, you will lose SSH and GUI access after the downgrade. To recover from this issue, use console access to remove the wancom0 realm-config. Also, remove the wancom0 **phy-interface** and **network-interface**. If you configure FQDN resolution for NTP servers through a media interface, you can downgrade to a version that does not support this resolution without removing the configuration.

During LDAP configuration, Address of the record and look-up queries are not available

SDM: In LDAP configuration, address of the record and look-up queries are not available.

Workaround: Configuration using the Web GUI and ACLI

LDAP SNMP Trap Support

LDAP SNMP traps are not supported in P-CZ 4.2.0. Communications Broker 4.2.0 does not generate any LDAP failures for the following OID failures:

- 1.3.6.1.4.1.9148.2.1.8.9 apSmgmtLDAPCap
- 1.3.6.1.4.1.9148.3.2.4.2.10 apSysMgmtLDAPServerStatusGroup
- 1.3.6.1.4.1.9148.3.2.4.3.15 apSysMgmtLDAPServerStatusNotificationsGroup

HA Limitation

HA switchover causes TCP/TLS ports to be reset. This terminates the TCP/TLS calls that were in progress on the formerly active Communications Broker. New call setup over TCP/TLS, however, is successful.

Logging Limitation

Setting Logging to DEBUG simultaneously with greater than 300k configuration degrades system performance. Be sure to set Logging to WARNING or NOTICE under this condition, and only use DEBUG when absolutely required.

LDAP Support

Only the default "ecb" network can support LDAP. Additional networks cannot.

Registrar Support

Only the default "ecb" network can act as the registrar. Additional networks cannot.

ECB Sync Compatibility

ECB Sync is supported only between nodes with the same configuration platforms. For example, X8-2 to X8-2, X9-2 to X9-2, VM to VM are supported. Both Communications Brokers participating in ECB Sync must have the same number of Cores.

Deprecated Ciphers

The system deprecates the following ciphers, adhering to recent OpenSSL changes intended to eliminate weak ciphers:

- All DES-CBC ciphers, including:
  - TLS_DHE_RSA_WITH_DES_CBC_SHA
  - TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA

Oracle recommends that you remove any prior version configuration that uses these ciphers, and that you do not configure a security profile with the expectation that these ciphers are available. Note also that TLS profiles using the **ALL** (default) value for the **cipher-list** parameter no longer use these ciphers.

> **Note:**
>
> The ACLI may still display these ciphers when you run **cipher-list ?**, but the system does not support them.

Resolved Issues

The following tables lists Resolved Issues.

The Resolved Issues table provides the Service Request ID number, a description of the issue, any workaround, when the issue occurred, and when Oracle fixed the issue.

Table 3-1 Resolved Issues

ID Number	Description	Fixed In
33842985	ECB GUI : Sorting is not working in Dialing contexts page.	PCz 4.1.0p2
35700038	ECB OCI VM: Registration Cache widget is not displaying registered entries.	PCz 4.1.0p2
35418244	Not able to see the child elements of CORPORATE, when we first open GEOGRAPHIC child elements.	PCz 4.1.0p1
35056106	Copy action not working on a few objects for a learned from remote entry.	PCZ 4.1.0p1
35316222	In existing file, LST entries are not syncing with Standby device.	PCZ4.1.0p1
35331882	SDM: The option NONE is not available under SNMP User Entry.	PCZ4.1.0p1
35380830/35238527	Intermittent reboot observed during save/activate.	PCZ4.1.0p1
35395958	Unable to GET/DELETE Communications Broker dialing context through REST API with name=value parameters.	PCZ4.1.0p1
33683448	Session timeout/ page unresponsiveness observed on tags load	PCZ4.0.0p2

Table 3-1 (Cont.) Resolved Issues

ID Number	Description	Fixed In
34266944	The sip-manipulation cfgrules modify screen is blank. Workaround: sip-manipulation->cfgrules can be configured using the ACLI.	PCZ4.0.0p1
32928940	When invalid values are configured in SA attributes, verify-config errors are not observed. Ensure your configuration values are valid.	PCZ4.0.0
35382471	SDM: Information message shows SBC instead of ECB.	SDM Release 9.0.3

Known Issues

The following tables lists Known Issues.

The Known Issue table includes issues that remain open. Issues from previous releases that do not appear here do not apply to this release. You can also find information about resolved issues in the Build Notes for this release.

Table 3-2 Known Issues

ID Number	Description	Workaround	Found In
34267309	No left-side Index/search in the browser for local Help files.	Not applicable	4.0.0
34935965	SDM: Able to provide the alphabets as input for the field ldap-servers from ldap-config	Valid inputs are configurable. The LDAP server attribute can be configured using the Web GUI	3.3.0
35430873	SDM: In Password policy, all attributes are displayed even admin security disabled.	None. Configuration will not take effect with Admin Security is disabled	4.1.0