Oracle® Enterprise Communications Broker

Release Notes

P-CZ3.0.0
F19864-02
August 2020

Oracle Enterprise Communications Broker Release Notes, P-CZ3.0.0

F19864-02

Contents

About This Guide

This guide provides the following information about the Oracle Enterprise Communications Broker (ECB) hardware and software.

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

Documentation Set

The following table describes the documentation set for the ECB.

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 ECB 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 ECB.

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
August 2018	• Initial Release

Date	Description
October 2018	• Updates the "Known Issues" section to reflect issues fixed in P-CZ3.0.0p1.
December 2018	• Adds the "Deprecated Ciphers" topic to the "Caveats" section.
January 2020	• Updates the "Known Issues" section to reflect updates in P-CZ3.0.0p6.
August 2020	• Updates the "Known Issues" section to reflect updates in P-CZ3.0.0p7 and P-CZ3.0.0p8.

1

Specifications and Requirements

Oracle recommends that you review the following information about PCZ3.0.0.

Supported Platforms

The following platforms and image files support the PCZ3.0.0 release. Note that the default number of cores for PCZ3.0.0 is different from previous releases.

Platforms

- Netra X3-2 — Ships with the Operating System and software installed.
- Netra X5-2 — Ships with the Operating System and software installed.
- Netra X7-2 — You must install the Operating System and software from a USB memory device.
  - Go to My Oracle Support (MOS) at https://support.oracle.com to download the Operating System and software. See "Download Software from MOS."
  - See "Software Installation - Oracle X7-2 Platforms" in the *Oracle Enterprise Session Border Controller Installation and Platform Preparation Guide* on https://docs.oracle.com/cd/E95619_01/index.htm for installation instructions.

Image and Boot Loader Files

The PCZ3.0.0 release uses the following image and boot loader files:

- Image—nnPCZ300.bz
- Boot loader—nnPCZ300.boot

Default Cores and Threads

The following list shows the default 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—Default 5 cores. Yields 3 SIP threads.
- Netra X3-2, Netra X5-2, and Netra X7-2—Default16 cores. Yields 9 SIP threads.

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 Oracle Enterprise Communications Broker (ECB) platforms require a boot loader to load the operating system and software.

All ECB platforms require that the boot loader and the software image match per release. For example, if the software image filename is nnPCZ300.bz, use the corresponding boot loader file named nnPCZ300.boot.

You must install the boot loader file as /boot/bootloader on the target system. When you plan to upgrade the system image, upgrade the boot loader before booting the new system image.

Boot Loader Requirements

All platforms require the Stage 3 boot loader that accompanies the Oracle Enterprise Communications Broker image file, as distributed. Install the boot loader according to the instructions in the *Oracle Enterprise Communications Broker Administrator's Guide*.

SPL Support

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

- C2.0.0
- C.2.0.1
- C2.0.2
- C2.0.9
- C2.1.0
- C3.0.0
- C3.0.1

- C3.0.2
- C3.0.3
- C3.0.4
- C3.0.5
- C3.0.7
- P1.0.0
- P1.0.1

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:

- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA384

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

- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

Oracle supports the following ciphers for debugging purposes only:

- TLS_RSA_WITH_NULL_SHA256 (debug only)
- TLS_RSA_WITH_NULL_SHA (debug only)
- TLS_RSA_WITH_NULL_MD5 (debug only)

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**. Note that they trigger **verify-config** error messages.

- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_3DES_EDE_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.

Upgrade and Downgrade Information

Upgrade Paths

The PCZ3.0.0 release supports the following upgrade paths:

- PCZ2.2.0 to PCZ3.0.0. Use the instructions in "Upgrade an HA Pair to PCZ3.0.0" to upgrade an HA pair.
- PCZ2.1.0 to PCZ2.2.0 to PCZ3.0.0

> **Note:**
>
> The PCZ3.0.0 release does not support an online upgrade from any PCZ2.x release. Oracle recommends that you perform such upgrades during a maintenance window.

Upgrade Caveats

Netra X3-2—You must upgrade the boot loader for PCZ3.0.0. See "Boot Loader Requirements" and "Image and Boot Loader Files."

Upgrade an HA Pair to PCZ3.0.0

All platforms—To upgrade an HA pair from PCZ2.2.0 to PCZ3.0.0, do the following:

1. Configure the PCZ3.0.0 boot parameters on both systems.
2. Reboot both systems, simultaneously.
3. Log on to the GUI of the active system and accept the change to update the schema.
4. Save and activate. The system creates a backup. Note its name for future reference, for example, if you need to downgrade.
5. Reboot the standby, again, to synchronize the HA pair.
6. Re-register all registered clients after the upgrade.
7. From the GUI, monitor the System Health widget to ensure that the systems remain in an HA pair with a health score of 100.

Downgrade to PCZ2.0.0

All platforms—To downgrade a system from PCZ3.0.0 to PCZ2.2.0, do the following:

1. Configure the boot parameters to boot PCZ2.2.0.

2. From the ACLI, run the **halt sysprep** command. This command clears all passwords from NVRAM and powers the system down.
3. Power up the system. Note that you must now use the default passwords.
4. Restore the PCZ2.2.0 configuration.
5. Save and activate.

> **Caution:**
>
> Be aware that the downgrade might reset the interface mapping to the factory defaults.

2
New Features

The PCZ3.0.0 release delivers numerous platform enhancements and library upgrades to improve the underlying Oracle Enterprise Communications Broker (ECB) software. This release contains no customer-facing features or enhancements other than those described in the "GUI Changes" and "Upgrade Information" topics in this guide.

3
GUI Changes

The PCZ3.0.0 release includes the following changes to the GUI.

Attribute Name Changes in session-agent Configuration

For PCZ3.0.0, Oracle changed the names of several attributes in the session-agent configuration. Updating the schema resolves the changes, but if you try to upload a .csv file of session-agents with the previous attribute names you will see errors. To avoid errors, update the column header names in your .csv file to match the new attribute names before you upload the .csv file. Note that the order of the attributes in session-agent configuration is different for PCZ3.0.0, but you do not need to re-order the attributes in your .csv file. The following table lists the attribute names prior to PCZ3.0.0 and the corresponding new names.

Prior to PCZ3.0.0	As of PCZ3.0.0
IP-address	ip-address
transport-protocol	transport-method
inbound-header-manipulation	in-manipulationid
outbound-header-manipulation	out-manipulationid
OPTIONS-ping-interval	ping-interval
enable-REFER-termination	refer-call-transfer
Send-NOTIFY-for-REFER-provisional-responses	refer-notify-provisional
enable-constraints	constraints
maximum-sessions	max-sessions
maximum-inbound-sessions	max-inbound-sessions
maximum-outbound-sessions	max-outbound-sessions
maximum-burst-rate	max-burst-rate
maximum-inbound-burst-rate	max-inbound-burst-rate
maximum-outbound-burst-rate	max-outbound-burst-rate
burst-rate-window-size	register-burst-window
maximum-sustain-rate	max-register-sustain-rate
maximum-inbound-sustain-rate	max-inbound-sustain-rate
maximum-outbound-sustain-rate	max-outbound-sustain-rate
sustained-rate-window-size	sustain-rate-window
SPL-options	spl-options

Cipher List Configuration

When you select **All** for the cipher list in the tls-profile configuration, the system displays a warning that the cipher list includes weak ciphers. For example:

```
Warning: tls-profile[sd] contains the following weak cipher(s):
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITHAES_256_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA.
```

You may need to adjust the cipher list according to your security requirements.

Denial of Services Configuration

The new architecture for PCZ3.0.0 supports Denial of Services (DoS) functionality designed to protect the system from overload. You no longer need to enable or set DoS parameters individually.

4
Caveats, Known Issues, and Limitations

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

The following items describe caveats in the P-CZ3.0.0 release.

ECB Sync Compatibility

ECB Sync is supported only between nodes with similar platforms. For example, a mix of X3/X5/X7 is supported, but not a VM and X7.

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

The user should remove any prior version configuration that used these ciphers, and not configure a security profile with the expectation that these ciphers are available. Note also that TLS profiles using the **ALL** (default) value to the **cipher-list** parameter no longer use these ciphers.

> **Note:**
>
> Your version of the ACLI may still print these ciphers when you run **cipher-list ?**. Despite printing them in ACLI output, the system does not support them within service operations.

Known Issues

The following table lists Known Issues and provides the Service Request ID number, a description of the issue, any workaround, when the issue occurred, and when Oracle fixed the issue. This table includes issues from previous releases that either remain open or are resolved in this release. 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.

ID Number	Description	Found In	Fixed In
31630190	ECB going out of service after upgrade from PCZ3.0.0p6 to PCZ3.0.0p7.	PCZ3.0.0p7	PCZ3.0.0p8
27240115	ECB Sync does not take effect. Workaround 1. Reboot the system.	PCZ2.2.0	PCZ3.0.0

ID Number	Description	Found In	Fixed In
No ID number	If you want to establish a High Availability pair that uses IP addresses other than the defaults, perform the following procedure. Use this procedure regardless of whether the ECBs run on virtual or physical systems. The IP addresses you use must be available and valid in your network. If not, you must directly connect the two ECBs before performing this procedure to establish the HA pair initially. Note • Primary default—169.254.1.1 • Secondary default —169.254.1.2 Procedure 1. Perform the standard HA setup with the **run setup** command, and allow both systems to come up in an HA pair. 2. From the GUI, go to General, General, High Availability and assign the IP addresses that you want to use to the Primary and Secondary ECBs. 3. Move the wancom1 connection to the network that you want to use. (Either the physical connection, or for VMs, change the vswitch used by the wancom1 interface.)	PCZ3.0.0	N/A

ID Number	Description	Found In	Fixed In
	4. Double reboot both systems, and they will come back up in an HA pair.		
28314178	When you turn on SIP debugging, you may see various unrelated messages displayed on the console. The messages do not prevent the ECB from generating logs, but they can make the console hard to use. Workaround: Use SSH when you turn on SIP debugging.	PCZ3.0.0	PCZ3.0.0p6

ID Number	Description	Found In	Fixed In
No ID number	If you see mapping errors after upgrading, for example errors about redundancy or media traffic, you may need to swap interface addresses. Workaround: Compare the MAC addresses on your Virtual Machine (VM) to those on your hardware. If the addresses are different, you need to swap interface addresses. Set the addresses on the hardware to match those from your VM. Use the **swap** command from the ECB command line. 1. Use SSH to access the command line prompt on the ECB. 2. From the ECB prompt type **sho interface mapping**, and press ENTER. The system displays its mappings. 3. Compare the mappings to your VM mappings. 4. Type **interface-mapping**, and press ENTER. 5. Type **swap <eth-if-name_1 eth-if-name_2>**, and press ENTER. Example: swap wancom0 s1p0 The system displays the interface mapping information after the swap and a warning that the change can	PCZ3.0.0	N/A

ID Number	Description	Found In	Fixed In
	affect services and requires a reboot. 6. At the Continue prompt, type **yes**, and press ENTER. 7. Exit the configuration. 8. Reboot the ECB.		
30576125	The ECB is reporting session limit inaccurately.	PCZ3.0.0	PCZ3.0.0p6

The following Known Issues have been found not to be present in this release. They are collected here for tracking purposes.

ID Number	Description	Found In	Fixed In
28207606	Registrations that expire at the producer are removed from the registration list. Removal happens when the registration of the endpoint is removed at the producer. The registration should be removed from the consumer the next time the two nodes sync registrations. Normal behavior on learned registrations is that an INVITE arriving at the consumer (learned the registration) is forwarded to the producer (of the registration). The producer then forwards the call to the registered endpoint. If the producer no longer has this registration, it will reject the call. Due to this defect, expired registrations are removed by the producer, but they are not removed by the consumer. The result is that the consumer continues to forward INVITES rather than rejecting them locally. At the producer, the expired registration is removed, and the call is rejected with a 4xx response. If the endpoint in question registers with a third ECB (node 3) that is also configured in the sync mesh, that registration is learned by the same consumer ECB. In this situation, both registrations exist in the learned registration database. One of those registrations is used to route a call. The	N/A	N/A

ID Number	Description	Found In	Fixed In
	behavior as to which registration is used is undefined. While the desired behavior is to send the call to node 3, the system may choose the stale registration and forward the call to node 2.		