Oracle® Corente Cloud Services Exchange

Release Notes for Release 9.4.3

E76015-05
May 2017

Oracle Legal Notices

Copyright © 2016, 2017, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Table of Contents

Preface v
1 New Features and Changes 1
1.1 What's New in Release 9.4.3 1
1.2 What's New in Release 9.4.2 1
1.3 What's New in Release 9.4.1 2
1.4 What's New in Release 9.4 4

Preface

This manual provides information on changes and new features for this release of Corente Cloud Services Exchange.

Related Documentation

The documentation for this product is available at:

http://www.oracle.com/technetwork/server-storage/corente/documentation/index.html

Feedback

Provide feedback about this documentation at:

http://www.oracle.com/goto/docfeedback

Conventions

Hyperlinks can be used to navigate through the guide or the procedures related to an overall activity, or to jump to a cross-referenced topic or Internet URL.

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

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.

Document Revision

Document generated on: 2017-05-01 (revision: 1222)

Chapter 1 New Features and Changes

Table of Contents

1.1 What's New in Release 9.4.3 1
1.2 What's New in Release 9.4.2 1
1.3 What's New in Release 9.4.1 2
1.4 What's New in Release 9.4 4

Find out what new features and changes are available for Corente Cloud Services Exchange.

1.1 What's New in Release 9.4.3

Corente Cloud Services Exchange Release 9.4.3 provides the following new features and changes:

Enhancement to include Internet Key Exchange (IKE) identifiers for third-party device partner configurations	As of this release, App Net Manager lets you set IKE identifiers in partner configurations for third-party devices that are used during authentication with Corente Services Gateways. App Net Manager now includes a **Partner IKE ID** section on the **Partners** tab of the **Location** window. This section is available only when you create partner configurations for third-party devices.
Support for IKE and IPSec tunnel lifetime configuration	Corente Cloud Services Exchange now lets you set the amount of time, in seconds, before IKE and IPSec tunnels timeout. If an IKE or IPSec tunnel between a third-party device and Corente Services Gateway reaches the timeout value, the third-party device must re-establish a secure connection with the Corente Services Gateway.
Performance improvements for IPSec packet encryption	As of this release Corente Services Gateways distribute processing for the encryption and decryption of IPSec packets across all available CPUs. This change can improve the performance of Corente Services Gateways by more than twice that of earlier releases. However, these performance improvements depend on your environment and system configuration. For optimal results, Corente Cloud Services Exchange recommends you install Corente Services Gateways on systems with no more than four CPUs. For more information, contact your Oracle Support representative.
Security patches and updates	This release of the Corente Services Gateway includes several security patches and software updates.

1.2 What's New in Release 9.4.2

Corente Cloud Services Exchange Release 9.4.2 provides the following new features and changes:

Support for arbitrary Internet Key Exchange (IKE) identifiers	As of this release, App Net Manager lets you define IKE identifiers that Corente Services Gateways use for authentication with third-party devices. App Net Manager provides a **Specified** field where you can define the IKE ID. This field is available in the **IKE ID** section on the **Partners** tab of the **Location** window. The **Specified** field is also available on

the **Add Location Partner** wizard when you create Location partners between a Corente Services Gateway and a third-party device. This field applies to Locations that you create from Release 9.4.2 or later.

Specified lets you define one of the following as the IKE ID:

- An IP address
- A string, that is prefixed with the at sign (@). App Net Manager does not send the at sign (@) as part of the IKE identity. For example, if you specify `@ExampleString01`, App Net Manager sends `ExampleString01` as the IKE identity.

Note

- The IKE ID is case sensitive and can contain a maximum of 255 ASCII alphanumeric characters including special characters, period or dot (.), hyphen or minus sign (-), and underscore (_). The IKE ID cannot contain embedded space characters.
- If you specify the IKE ID, the Peer ID type must be Domain Name on all third party devices. App Net Manager does not support other Peer ID types, such as Email Address, Firewall Identifier, or Key Identifier.

Improved handling of shared secrets	Corente Cloud Services Exchange now allows < and > characters in shared secrets.
Security patches and updates	This release of the Corente Services Gateway includes several security patches and software updates.

1.3 What's New in Release 9.4.1

Corente Cloud Services Exchange Release 9.4.1 provides the following new features and changes:

App Net Manager available from outside the Corente Services Gateway	As of this release, you can run App Net Manager from outside a Corente Services Gateway at `https://www.corente.com/appnet`.

Note

You can continue to access App Net Manager at `https://admin.corente.com/` if you currently do so. However, if you are installing a new instance of App Net Manager, you should access it at `https://www.corente.com/appnet`.

App Net Manager Lite is no longer supported	Because you no longer need to access App Net Manager from inside a Corente Services Gateway, App Net Manager Lite is not required.
Corente Services Gateway upgrade changes	This release changes how upgrades for Corente Services Gateway take place. When an upgrade for your Corente Services Gateway becomes

available, you receive a notification that the upgrade will automatically take place in the next available maintenance window after 60 days.

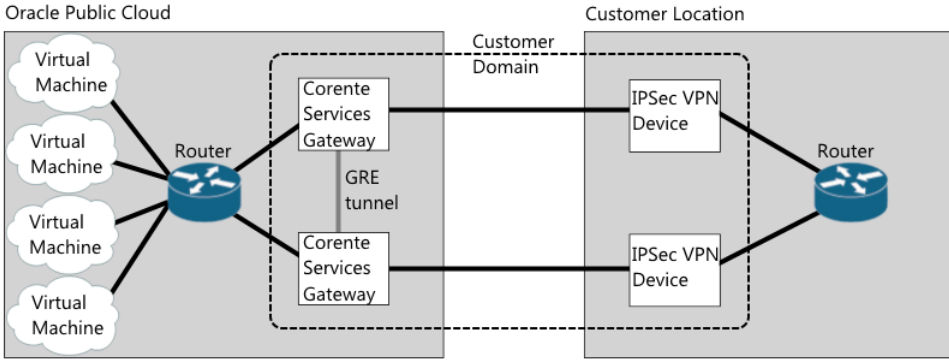
You can let the upgrade take place automatically during the maintenance window. Alternatively, you can schedule the upgrade to take place at a different time through App Net Manager or upgrade your Corente Services Gateway immediately.

Cloud failover configuration

If you use Corente Cloud Services Exchange in the Oracle Public Cloud environment and use a supported third-party VPN device configuration then the **Cloud Failover** section is available on the **Location** tab in App Net Manager.

The **Cloud Failover** section provides a **Failover Location Address** field where you can specify the LAN IP address of the Corente Services Gateway you plan to use as a failover location. In the event that the IPSec tunnel to the third-party device becomes unavailable, the Corente Services Gateway forwards packets to the failover location. The failover occurs within 30 seconds.

The following diagram illustrates the cloud failover configuration:



The preceding diagram shows two Corente Services Gateways that reside on the Oracle Public Cloud network and two third-party VPN devices that reside on the customer network. You configure the Corente Services Gateways and the third-party VPN devices on the same domain in App Net Manager. The two Corente Services Gateways are not partners. You partner each Corente Services Gateway with one of the third-party VPN devices.

In a cloud failover configuration, Corente Services Gateways:

- Must have an inline configuration.
- Must have the same LAN configuration. Although Corente Services Gateways do have different LAN IP addresses.
- Must have the same User Group configuration.

You must enable dead peer detection (DPD) for the third-party VPN devices and ensure that they have the same subnet configuration.

Dead peer detection with third-party devices

App Net Manager lets you use dead peer detection (DPD) with third-party devices.

Corente Services Gateway Virtual Environment edition (CVSG-VE) is now deprecated	As of this release, it is no longer possible to use Corente Services Gateway Virtual Environment edition.

Documentation changes	The following changes apply to the Corente Cloud Services Exchange documentation library as of Release 9.4.1:
	• *App Net Manager Help* is now available to assist you while using App Net Manager.
	• *Gateway Viewer Help* is now available to assist you while using Gateway Viewer.
	• The *Corente Services Gateway Deployment Guide* is now available to help you plan and install Corente Services Gateways.
	• The following books are no longer included in the Corente Cloud Services Exchange documentation library:
	  • *Corente Services Policy Definition and Provisioning Manual*
	  For details on defining and provisioning policies for Corente Services Gateways, see the *Corente Services Administration Guide*.
	  • *Corente Services Troubleshooting Guide*
	  For troubleshooting procedures, see the *Corente Services Administration Guide*.
	  • *Corente Services Remote Access User Guide*
	  For details on adding and configuring Mobile Users, see the *Corente Services Administration Guide*.
	  • *Corente Services Quick Start Installation and Setup Guide*
	  For instructions on how to install Corente Services Gateways, see the *Corente Services Gateway Deployment Guide*.
	  • *Corente Services Planning and Deployment Manual*
	  For planning information and instructions on how to install Corente Services Gateways, see the *Corente Services Gateway Deployment Guide*.
	  • *Corente Virtual Services Gateway – Virtual Environment Manual*

1.4 What's New in Release 9.4

Corente Cloud Services Exchange Release 9.4 provides the following new features and changes:

Retirement of 32-bit platform support for the Corente Services Gateway	The Corente Services Gateway software is now only available as a 64-bit package, and 32-bit gateways are no longer supported. You can no longer deploy a Corente Services Gateway on a 32-bit architecture machine.

Retirement of the SSL Client	The Corente SSL Client software is no longer available, and is no longer supported. Existing SSL Clients will no longer work and you will not be able to administer them. As an alternative, you can download and install one of the following: • Corente Client - A software-based IPSec remote access client for Windows platforms • Corente Mobile Client - For iOS or Android platforms
New implementation of the Corente Client	The Corente Client is a remote access client for Windows computers. For this release, the Corente Client has been implemented as a lightweight agent that uses the native IPSec functionality of the Windows operating system. Administration of the Corente Client has changed. The **Mobile User Administration** feature of App Net Manager is now used to manage Corente Client user accounts. In previous releases, the **Client Administration** feature of App Net Manager was used. The **Client Administration** feature is now reserved for managing legacy Corente Client user accounts. From this release, legacy Corente Client user accounts can no longer be created. The **Add Client** screen is no longer available. To upgrade from a previous version of the Corente Client, users must uninstall the current version first. They can then install version 9.4 of the client software. Users also need to download a new client configuration, created by the administrator. Previous versions of the Corente Client are still supported, but administrators are not able to create new Client accounts or download previous versions of the Corente Client software. On a computer with multiple users, each user can now have a separate Corente Client user account. Installation and operation of the Corente Client is the same as for previous releases. See the *Corente Services Remote Access User Guide* for more detailed information.
Windows 10 Client support	The Corente Client can now be installed and used on Windows 10 client devices.
Support for third-party devices	This release introduces support for third-party devices using native IPSec connections. A third-party device is a network device from an external manufacturer. For example, a Cisco router.
Support for GRE tunnels	This release introduces support for tunnels using the GRE (Generic Routing Encapsulation) protocol.
IPSec compression	Compression can now be enabled for IPSec connections through a Corente Services Gateway.

Improved integration with Oracle VM	After the installation of a Corente Services Gateway in a virtual environment, the gateway will reboot and configure itself automatically using Oracle VM Utilities.
Supported Oracle VM VirtualBox versions for Corente Services Gateway Virtual Environment edition	The Corente Services Gateway Virtual Environment edition (CVSG-VE) now supports Oracle VM VirtualBox version 5.0.6. Other versions of VirtualBox are not supported.
Corente Services Gateway console	A console window is now available, showing system and networking information for a Corente Services Gateway.
LDAP External Authentication changes	When you configure an LDAP server for external authentication on the User Remote Access tab for a location, you can specify either the DNS name or the IP address of the LDAP server. If you specify an IP address, you must now also specify the NetBIOS name of the LDAP server.
SNMP Monitoring Support	Monitoring using an SNMP (Simple Network Management Protocol) agent is now supported for servers running Windows 10 and Windows Server 2016.
Changes to software download locations	The locations where you download Corente software components have changed for this release, as follows: • Corente Services Gateway - Now available from the Oracle Software Delivery Cloud (https://edelivery.oracle.com) and My Oracle Support (https://support.oracle.com). • Corente Client - Now available from the Oracle Technology Network (OTN) web site at: http://www.oracle.com/technetwork/server-storage/corente/downloads/index.html
Documentation changes	The following changes to the Corente documentation set have been made for this release: • The *Corente Client User Guide* and *Mobile User Manual* have been combined, to form the *Remote Access User Guide*. • The *Planning Manual* and *Gateway Hardware Preparation and Deployment Manual* and have been combined, to form the *Planning and Deployment Manual*. • Planning and installation checklist documents have been incorporated into the relevant manual in the document set.