Oracle Private Cloud Appliance

Release Notes

F74805-38
August 2025

Oracle Private Cloud Appliance Release Notes,

F74805-38

Contents

Preface

3 Service Limits

4 Known Issues and Workarounds

Preface

This publication is part of the customer documentation set for Oracle Private Cloud Appliance Release 3.0. Note that the documentation follows the release numbering scheme of the appliance software, not the hardware on which it is installed. All Oracle Private Cloud Appliance product documentation is available at https://docs.oracle.com/en/engineered-systems/private-cloud-appliance/index.html.

Oracle Private Cloud Appliance Release 3.x is a flexible general purpose Infrastructure as a Service solution, engineered for optimal performance and compatibility with Oracle Cloud Infrastructure. It allows customers to consume the core cloud services from the safety of their own network, behind their own firewall.

Audience

This documentation is intended for owners, administrators and operators of Oracle Private Cloud Appliance. It provides architectural and technical background information about the engineered system components and services, as well as instructions for installation, administration, monitoring and usage.

Oracle Private Cloud Appliance has two strictly separated operating areas, known as enclaves. The Compute Enclave offers a practically identical experience to Oracle Cloud Infrastructure: It allows users to build, configure and manage cloud workloads using compute instances and their associated cloud resources. The Service Enclave is where privileged administrators configure and manage the appliance infrastructure that provides the foundation for the cloud environment. The target audiences of these enclaves are distinct groups of users and administrators. Each enclave also provides its own separate interfaces.

It is assumed that readers have experience with system administration, network and storage configuration, and are familiar with virtualization technologies. Depending on the types of workloads deployed on the system, it is advisable to have a general understanding of container orchestration, and UNIX and Microsoft Windows operating systems.

Feedback

Provide feedback about this documentation at https://www.oracle.com/goto/docfeedback.

Conventions

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.

Convention	Meaning
`monospace`	Monospace type indicates commands within a paragraph, code in examples, text that appears on the screen, or text that you enter.
$ prompt	The dollar sign ($) prompt indicates a command run as a non-root user.
# prompt	The pound sign (#) prompt indicates a command run as the `root` user.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at https://www.oracle.com/corporate/accessibility/.

Access to Oracle Support for Accessibility

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit https://www.oracle.com/corporate/accessibility/learning-support.html#support-tab.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

1

Accessibility and Oracle Private Cloud Appliance

Oracle is committed to making its products, services and supporting documentation accessible and usable to the disabled community. This chapter contains information about the status of Oracle Private Cloud Appliance in terms of compliance with the Americans with Disabilities Action (ADA) requirements.

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at https://www.oracle.com/corporate/accessibility/.

For information about the accessibility of the Oracle Help Center, see the Oracle Accessibility Conformance Report at https://www.oracle.com/corporate/accessibility/templates/t2-11535.html.

Oracle JET User Interface Accessibility Features

The Oracle Private Cloud Appliance user interface is built with Oracle JavaScript Extension Toolkit (JET) which is compliant with the Americans with Disabilities Action (ADA) requirements. For detailed accessibility information about JET, refer to Oracle JET and Accessibility.

Oracle Server X9-2 Accessibility Features

Oracle strives to make its products, services, and supporting documentation usable and accessible to the disabled community. To that end, products, services, and documentation include features that make the product accessible to users of assistive technology.

The accessibility features of Oracle Server X9-2 are detailed within the following product components:

- Oracle Server X9-2 hardware
- Oracle Integrated Lights Out Manager (ILOM)
- Oracle Hardware Management Pack
- BIOS

Oracle Server X9-2 Hardware Accessibility

Oracle Server X9-2 hardware has color-coded labels, component touch points, and status indicators (LEDs) that provide information about the system. These labels, touch points, and indicators can be inaccessible features for sight-impaired users. The product's HTML documentation provides context and descriptive text available to assistive technologies to aid in interpreting status and understanding the system.

You can also use the built-in Oracle Integrated Lights Out Manager (ILOM) to obtain information about the system. Oracle ILOM provides a browser-based user interface (UI) and a command-line interface (CLI) that support assistive technologies for real-time viewing of system status, indicator interpretation, and system configuration. For details, see Oracle Integrated Lights Out Manager Accessibility.

Oracle Integrated Lights Out Manager Accessibility

You can use the Oracle Integrated Lights Out Manager (ILOM) UI to monitor and manage the server hardware. The Oracle ILOMUI does not require a special accessibility mode; rather, its accessibility features are always available. The UI was developed using standard HTML and JavaScript and its features conform to accessibility guidelines.

To navigate a UI page and select items or enter commands, use standard keyboard inputs, such as the Tab key to go to a selection, or the up and down arrow keys to scroll through the page. You can use standard keyboard combinations to make menu selections.

For example, using the Oracle ILOM Open Problems UI page, you can identify faulted memory modules (DIMMs) or processors (CPUs) that would otherwise be identified by a lighted LED indicator on the motherboard. Likewise, you can use the Oracle ILOM UI to monitor the hardware power states that are also indicated by flashing LED indicators on the hardware.

The Oracle ILOM CLI is an alternative and equivalent way to access the Oracle ILOM UI features and functionality. Because the operating systems that run on the Oracle server hardware support assistive technologies to read the content of the screen, you can use the CLI as an equivalent means to access the color-based, mouse-based, and other visual-based utilities that are part of the UI. For example, you can use a keyboard to enter CLI commands to identify faulted hardware components, check system status, and monitor system health.

You can use the Oracle ILOM Remote Console Plus application to access both a text-based serial console and a graphics-based video console that enable you to remotely redirect host server system keyboard, video, mouse, and storage devices. Note, however, that the Oracle ILOM Java Remote Console Plus does not support scaling of the video frame within the Java application. You need to use assistive technology to enlarge or reduce the content in the Java Remote Console Plus display.

As an alternative method to using the BIOS Setup Utility to configure BIOS settings, Oracle ILOM provides a set of configurable properties that can help you manage the BIOS configuration parameters on an Oracle x86 server. Using Oracle ILOM, you can do the following:

- Back up a copy of the BIOS configuration parameters to an XML file using the Oracle ILOM UI.
- Edit the XML file using a standard XML editor. The BIOS XML tags correlate directly to the BIOS screen labels.
- Restore the XML file of the backed up or edited configuration parameters to BIOS.

The UI and CLI methods for using Oracle ILOM are described in the accessible HTML documentation for Oracle ILOM at https://www.oracle.com/goto/ilom/docs.

Oracle Hardware Management Pack Accessibility

Oracle Hardware Management Pack software is a set of CLI tools. Oracle Hardware Management Pack software does not include product-specific accessibility features. Using a keyboard, you can run the CLI tools as text commands from the operating system of a supported Oracle server. All output is text-based.

Additionally, most Oracle Hardware Management Pack tools support command output to a text log file or XML file, which can be used for text-to-speech conversion. Accessible man pages are available that describe the Hardware Management Pack tools on the system on which those tools are installed.

You can install and uninstall Oracle Hardware Management Pack by using text commands entered from the CLI. Assistive technology products such as screen readers, digital speech synthesizers, or magnifiers can be used to read the content of the screen.

Refer to the assistive technology product documentation for information about operating system and command-line interface support.

The CLI tools for using the software are described in the accessible HTML documentation for Hardware Management Pack at https://www.oracle.com/goto/ohmp/docs.

BIOS Accessibility

When viewing BIOS output from a terminal using the serial console redirection feature, some terminals do not support function key input. However, BIOS supports the mapping of function keys to Control key sequences when serial redirection is enabled. Descriptions of the function key to Control key sequence mappings are provided in the product documentation, typically within the server Service Manual. You can navigate the BIOS Setup Utility by using either a mouse or keyboard commands.

As an alternative method of configuring BIOS settings using the BIOS Setup Utility screens, Oracle ILOM provides a set of configurable properties that can help you manage the BIOS configuration parameters on an Oracle x86 server. For more information, see Oracle Integrated Lights Out Manager Accessibility.

2
Feature Updates

This section contains a list of the new features and changes to features that have been added to the Oracle Private Cloud Appliance software since its initial release. You can obtain the latest features and bug fixes by applying patches to your system. For more information, see the Oracle Private Cloud Appliance Patching Guide.

To check which components require upgrading or patching with a released software build, see My Oracle Support. Refer to the note with Doc ID 2907892.1. For information and recommendations about released builds, refer to the note with Doc ID 2906831.1.

Latest Features

> ⚠ **Caution**
>
> Prior to patching or upgrading to the latest release, ensure that all compute nodes are in the provisioned state.

Platform Images

New platform images are made available for Compute Enclave users through Private Cloud Appliance installation, upgrade, and patching.

The following platform images are delivered with this Private Cloud Appliance release:

Oracle Linux 9	`uln-pca-Oracle-Linux-9-2025.01.31_0.oci`
Oracle Linux 8	`uln-pca-Oracle-Linux-8-2025.01.31_0.oci`
Oracle Linux 7.9	`uln-pca-Oracle-Linux-7.9-2025.01.31_0.oci`
Oracle Solaris 11.4	`uln-pca-Oracle-Solaris-11-2025.02.04_0.oci`
Kubernetes Engine	`uln-pca-Oracle-Linux8-OKE-1.30.3-20250325.oci`
	`uln-pca-Oracle-Linux8-OKE-1.29.9-20250325.oci`
	`uln-pca-Oracle-Linux8-OKE-1.28.8-20250325.oci`

X11 Hardware Available

The Oracle Private Cloud Appliance X11 rack configuration is now available. This rack configuration is characterized by the use of Oracle Server X11 compute and management nodes, and the new Oracle ZFS Storage ZS11-2 node. Compared to the Oracle Private Cloud Appliance X10 rack configuration, the component order and cabling are slightly different.

Additionally, you can order Oracle Server X11 compute nodes as expansion nodes.

Compute Expansion Available

You can now expand your Oracle Private Cloud Appliance compute capacity by adding indvidual compute nodes to an existing rack, or adding an entire Compute Expansion rack.

When ordering individual compute expansion nodes, ensure you order nodes compatible with your exising system.

For information about Compute Expansion racks, see Optional Compute Expansion Rack in the "Oracle Private Cloud Appliance Installation Guide".

System Upgrade to Oracle Linux 8

This release of the appliance software migrates the core system components to Oracle Linux 8. This includes operating systems as well as the platform layer, container images, microservices, and so on. A new disk layout is applied to management nodes and compute nodes, which contributes to faster and more reliable future upgrades. The management cluster is torn down, and reconstructed from the upgraded components. For more information, see Full Management Cluster Migration to Oracle Linux 8 in the Oracle Private Cloud Appliance Upgrade Guide.

> **NOT_SUPPORTED**
>
> The minimum recommended appliance software version is now 3.0.2-b1261765. If your current version is older, see Upgrading from Earlier Software Versions. Version 3.0.2-b1261765 must be upgraded to version 3.0.2-b1392231 using ISO images. Migration to Oracle Linux 8 is not supported by ULN-based patching.

Enhanced Upgrade Workflow Orchestration

The appliance upgrade is now a fully integrated end-to-end process launched with a single command. Each individual component has its own process to maintain the granular nature of the upgrade, but all individual upgrade processes are orchestrated through a central workflow that runs all operations across the entire system, as prescribed by the upgrade plan.

The new unified full rack upgrade workflow is the preferred method, because it eliminates issues related to component order and timing of operations. Other upgrades of single components or groups of components remain possible, in case a workaround is required for an orchestration problem or a particular component requirement. More information, and instructions to use the new commands, can be found in the Oracle Private Cloud Appliance Upgrade Guide. See Performing a Full Rack Upgrade and Upgrading Components Individually.

For the enhanced workflow-driven approach, the Upgrader is integrated with the appliance job framework. You can query and drill down into its work requests and jobs from both the Service Web UI and Service CLI. The new full rack upgrade function also includes a convenient rack-wide health check. For more information, see Check Upgrade Readiness and Status.

Load Balancer Update

The internal foundations of the load balancer services are moving to a new implementation, which leads to minor differences in functionality. Administrators should verify the existing configuration of deployed load balancers before upgrading the appliance software. It might be necessary to reconfigure active load balancers to ensure a successful upgrade. For more information, see Load Balancer Functional Changes After Appliance Software Upgrade.

Kubernetes Engine

The following new features are added for Oracle Private Cloud Appliance Kubernetes Engine (OKE):

- Private Clusters. You can create a private cluster and use a Dynamic Routing Gateway to communicate with your on-premises IP address space, or use a Local Peering Gateway to communicate with instances in other VCNs. See "Public and Private Clusters" in the Creating OKE Network Resources chapter in the *Oracle Private Cloud Appliance Kubernetes Engine* user guide.
- VCN-Native Pod Networking. VCN-Native Pod Networking enables direct communication between pods in the control plane node pool worker nodes, and enables direct communication between worker node pods and other resources. The other resources can be in the same or different subnet and in the same or different compartment. See "VCN-Native Pod Networking" in the Creating OKE Network Resources chapter in the *Oracle Private Cloud Appliance Kubernetes Engine* user guide.
- Cluster Add-ons. Cluster add-ons are components that you can choose to deploy on a Kubernetes cluster. Cluster add-ons extend core Kubernetes functionality and improve cluster manageability and performance. This release offers the WebLogic Kubernetes Operator add-on, which supports running WebLogic Server and Fusion Middleware Infrastructure domains on Kubernetes. See Managing OKE Cluster Add-ons in the *Oracle Private Cloud Appliance Kubernetes Engine* user guide.
- Node Pool Creation. You can create a node pool when you create the cluster when you use the Compute Web UI. See "Creating an OKE Cluster" in the Creating and Managing OKE Clusters chapter in the *Oracle Private Cloud Appliance Kubernetes Engine* user guide.

Container Instances

Container Instances is a serverless compute service that enables you to quickly and easily run containers without managing any servers. Container Instances runs your containers on serverless compute optimized for container workloads that provides the same isolation as virtual machines.

A container instance is a minimal instance designed to run only what is needed for containers. Compute, networking, and storage resources are created as needed. A single user-specified container is started in the container instance.

For more information, see Container Instances in the *Oracle Private Cloud Appliance User Guide*.

Limit Service Expansion

Additional resource limits in more services can be viewed and set by Service Enclave administrators. In addition to the Service CLI, resource limits can be viewed and set by using the Service Web UI. See the Viewing and Setting Resource Limits chapter in the *Oracle Private Cloud Appliance Administrator Guide*.

New Flex Networking Commands

The Flex networking feature, formerly call Exadata Network, is introducing new commands in this release. The older Exadata commands will be deprecated in a future release. For more information, see Creating and Managing Flex Networks in the *Oracle Private Cloud Appliance Administrator Guide*.

New Flex Network Updates

- The limit for Flex networks allowed per port has changed from 8 to 32. There remains a rack limit of 128 Flex networks. See the Creating and Managing Flex Network section in the *Oracle Private Cloud Appliance Administrator Guide*.
- VRF-awareness is now supported.

Bugs Fixed in This Release

For a list of bugs fixed in each release, see Oracle Support Document 2906831.1 ([PCA 3.x] Private Cloud Appliance: Software Updates) can be found at: https://support.oracle.com/knowledge/Sun%20Microsystems/2906831_1.html.

Features Released in Software Version 3.0.2-b1325160 (March 2025)

> ⚠ **Caution**
>
> Prior to patching or upgrading to the latest release, ensure that all compute nodes are in the provisioned state.

Platform Images

New platform images are made available for Compute Enclave users through Private Cloud Appliance installation, upgrade, and patching.

The following platform images are delivered with this Private Cloud Appliance release:

Oracle Linux 9	`uln-pca-Oracle-Linux-9-2024.07.31_0.oci`
Oracle Linux 8	`uln-pca-Oracle-Linux-8-2024.07.31_0.oci`
Oracle Linux 7.9	`uln-pca-Oracle-Linux-7.9-2024.07.31_0.oci`
Oracle Solaris 11.4	`uln-pca-Oracle-Solaris-11-2024.08.26_0.oci`

Kubernetes Engine	`uln-pca-Oracle-Linux8-OKE-1.26.15-20240909.oci`
	`uln-pca-Oracle-Linux8-OKE-1.27.12-20240909.oci`
	`uln-pca-Oracle-Linux8-OKE-1.28.8-20240909.oci`

GPU Expansion

Add a GPU expansion rack to Private Cloud Appliance and build a scalable platform for AI and graphics intensive applications. The minimum expansion rack configuration contains a single GPU node with 4 NVIDIA L40S GPUs. More nodes can be installed after initial deployment. Two full racks, each with up to 6 GPU nodes, can be connected to the base rack.

When the racks are interconnected, GPU nodes become an integral part of the system and are managed like any other compute node. They are added to the same 3 fault domains, but the server families operate separately. Users must deploy compute instances with a dedicated shape to take advantage of the GPUs. These instances do not support live migration.

To learn about adding GPU capacity to a Private Cloud Appliance, see Optional GPU Expansion in the "Oracle Private Cloud Appliance Installation Guide".

New Disaster Recovery Service

A new disaster recovery (DR) service is introduced, with orchestration of DR operations built directly into the Service Enclave. This new implementation, also called the *Native DR Service*, requires a mutual, symmetrical peer connection between two Private Cloud Appliance systems, and uses a separate uplink from the spine switches. DR configurations and plans can be managed from the active or standby rack, and are automatically replicated to the peer system's DR service. If one of the peered systems goes down due to a site level incident, the failover operations defined in the DR plans are triggered from the standby system. Other DR plan operations can be run from either rack, because the peer connection allows both DR services to exchange data and instructions.

See Disaster Recovery in the Concepts Guide for an overview. A link to detailed information and instructions in the Administrator Guide is provided.

Existing installations can continue to use their first-generation disaster recovery configuration, orchestrated through Oracle Enterprise Manager with Oracle Site Guard. A path is provided to migrate existing configurations to the new Native DR Service.

New Limit Service

The Limit service enables you to view limits that are currently set for Private Cloud Appliance resources, and change those resource limits if the limit definition allows. See the Viewing and Setting Resource Limits chapter in the *Oracle Private Cloud Appliance Administrator Guide*.

Improved Upgrade and Patching Procedures

Both the Upgrade Guide and Patching Guide have been restructured to make it easier and clearer to follow the appropriate instructions based on active software version and target version. In the main instructional sections, it is assumed that the system is already at a minimum required version. For systems on earlier software versions, the procedures to get to the minimum required version are provided in a separate chapter. See Upgrading from Earlier Software Versions in the "Oracle Private Cloud Appliance Upgrade Guide".

Uplink Reference Topologies

The integration of a Private Cloud Appliance into the data center network can be challenging due to existing configurations and local requirements and standard practices. There are various ways to configure the uplinks, and Oracle provides assistance completing the relevant checklists in advance. To simplify and speed up the process, the Installation Guide provides examples of commonly used topologies, with switch configuration examples to guide network administrators in mapping their specific setup. See "Appliance Networking Reference Topologies".

Change to VM Console Port

As of this release, the VM console needs access to port 1443. In previous releases, port 443 was used for VM console access. For more information, see Port Matrix in *Oracle Private Cloud Appliance Security Guide*.

Kubernetes Engine

The following new features are added for Oracle Private Cloud Appliance Kubernetes Engine (OKE):

- Node Doctor. The Node Doctor utility helps you troubleshoot a cluster worker node that is not Active or Running. Node Doctor can identify potential problem areas and provide information to help you address those problem areas, and the utility can collect node system information into a support bundle to enable you to get help from Oracle Support. See Using Node Doctor to Troubleshoot Worker Node Issues in the *Oracle Private Cloud Appliance Kubernetes Engine* user guide.
- Node cycling. By default when you update a node pool, only new nodes that are added during this update or that are added later receive the updates. Node cycling enables you to replace existing nodes with new nodes that use updated settings. Node cycling performs

an in-place update of all existing nodes in the node pool to the latest specified configuration. New nodes are created, workloads moved onto them from existing nodes, current node pool updates applied, and the original nodes terminated. See Node Cycling an OKE Node Pool in the *Oracle Private Cloud Appliance Kubernetes Engine* user guide.

- Node labels. A node label is a key/value pair that enables you to target pods for scheduling on specific nodes or groups of nodes. See the OCI CLI procedure in Creating an OKE Worker Node Pool in the *Oracle Private Cloud Appliance Kubernetes Engine* user guide.
- Persistent storage. New ability to create high performance block volume storage and create file system storage by using the CSI (Container Storage Interface) plugin. See the Adding Storage for Containerized Applications chapter in the *Oracle Private Cloud Appliance Kubernetes Engine* user guide.

SR-IOV Support

Single root I/O virtualization (SR-IOV) technology enables virtual machines to achieve low latency and high throughput simultaneously on 1 or more physical links. This technology is ideal for low-latency workloads such as video streaming, real-time applications, and large or clustered databases. Hardware-assisted (SR-IOV) networking uses the VFIO driver framework.

See SR-IOV in the Concepts Guide for an overview. Configuration information is available at "Configuring SR-IOV for Virtual Networking" in the Networking section of the User Guide.

Dynamic Routing Gateways Limit Increase

As of this release, the limits for Dynamic Routing Gateways (DRG) have increased to 32 total DRGs across all tenancies, with up to 16 SR-IOV DRGs.

Flex Network Limit Increase

As of this release, the maximum number of flex networks per port is now 8 with a maximum of 32 flex networks per rack. The following restrictions apply:

- The relationship between flex networks and DRGs is 1:1.
- A flex network cannot share a DRG with another flex network.
- A flex network cannot share a DRG with one or more direct attach Exadata networks.

When upgrading to this release, if you have existing flex or Exadata networks that share a DRG with other flex networks for Exadata direct connect, they can no longer share a DRG. Each flex network must have its own DRG.

Bugs Fixed in This Release

For a list of bugs fixed in each release, see Oracle Support Document 2906831.1 ([PCA 3.x] Private Cloud Appliance: Software Updates) can be found at: https://support.oracle.com/knowledge/Sun%20Microsystems/2906831_1.html.

Features Released in Software Version 3.0.2-b1185392 (July 2024)

> ⚠ **Caution**
>
> Prior to patching or upgrading to the latest release, ensure that all compute nodes are in the provisioned state.

Platform Images

New platform images are made available for Compute Enclave users through Private Cloud Appliance installation, upgrade, and patching.

The following platform images are delivered with this Private Cloud Appliance release:

Oracle Linux 9	`uln-pca-Oracle-Linux-9-2024.05.29_0.oci`
Oracle Linux 8	`uln-pca-Oracle-Linux-8-2024.05.29_0.oci`
Oracle Linux 7.9	`uln-pca-Oracle-Linux-7.9-2024.05.29_0.oci`
Oracle Solaris 11.4	`uln-pca-Oracle-Solaris-11-2024.05.07_0.oci`
Kubernetes Engine	`uln-pca-Oracle-Linux8-OKE-1.26.6-20240611.oci`
	`uln-pca-Oracle-Linux8-OKE-1.27.7-20240602.oci`
	`uln-pca-Oracle-Linux8-OKE-1.28.3-20240602.oci`

Configurable Exadata Network Parameters to Support Additional Use Cases

Exadata Network ports (also referred to as flexNetwork ports) can now be used to connect to other network switches/routers, and ethernet based ZFSSA/3rd-party storage controllers. To facilitate the configuration, two new parameters are added to Exadata network creation: gateway (a valid IP address; the default is null) and speed (valid values are 10, 20, 25, 40, 50, and 100 Gbps). In addition, port ranges need to be set to valid values based on speed.

User Interface Enhancements

- The Compute Web UI has been enhanced to provide text search when selecting a compartment, making it easier to find a specific compartment.
- You can now view the current build information for the system in the Appliance Details page of the Service Web UI.
- The Compute Web UI and Service Web UI have updated their console theme to reflect the Oracle Redwood branding common in Oracle Cloud. This change is intended to bring the Oracle Private Cloud Appliance user experience inline with the Oracle Cloud user experience.

Upgrade Enhancements

The preparation phase of the upgrade and patching workflows has been redesigned to bring the Upgrader functionality of the latest release into the appliance at the earliest time possible.

Currently, preparation steps are performed through code within the active appliance software version. The new design allows Upgrader packages from the target software version to be installed first, so those preparation steps can be run using the latest software from the ISO image or ULN channels.

At this time, only the new design is implemented. The enhancements come into effect when the appliance software is upgraded or patched to a later version.

ULN Mirror for Appliance Patching on Oracle Linux 8

To comply with standard Oracle Linux 8 practice, and available packages on ULN, the procedure to set up the ULN mirror in the data center was updated. The specific instructions for Oracle Linux 8 are now centered around the `dnf reposync` command.

For detailed information, refer to the chapter "Configure Your Environment for Patching" in the Oracle Private Cloud Appliance Patching Guide.

OKE Worker Node Eviction

When you delete a node pool, delete a specified node, decrement the size of the node pool, or change the node pool nodes placement configuration, Oracle Private Cloud Appliance Kubernetes Engine (OKE) first cordons and drains the node. A node that is cordoned cannot have new pods placed on it. Existing pods on that node are not affected. When a node is drained, each pod's containers terminate gracefully and perform any necessary cleanup.

You can specify the maximum amount of time to allow for node eviction (eviction grace duration), up to 60 minutes.

Nodes are deleted after their pods are evicted or at the end of the eviction grace duration, even if not all pods are evicted.

This parameter can be set when the node pool is created, and it can be set or changed when you update the node pool, delete a specified node, or delete the node pool.

See Creating and Managing OKE Worker Node Pools in the *Oracle Private Cloud Appliance Kubernetes Engine* user guide.

Bugs Fixed in This Release

For a list of bugs fixed in this release, see Oracle Support Document 3037847.1 ([PCA 3.x] Private Cloud Appliance X9-2 and X10 release and updates (3.0.2-b1185392)) can be found at: https://support.oracle.com/epmos/faces/DocumentDisplay?id=3037847.1.

Features Released in Software Version 3.0.2-b1081557 (March 2024)

> ⚠ **Caution**
>
> Prior to patching or upgrading to the latest release, ensure that all compute nodes are in the provisioned state.

Platform Images

New platform images are made available for Compute Enclave users through Private Cloud Appliance installation, upgrade, and patching.

The following platform images are delivered with this Private Cloud Appliance release:

Oracle Linux 9	`uln-pca-Oracle-Linux-9-2023.09.26_0.oci`
Oracle Linux 8	`uln-pca-Oracle-Linux-8-2023.09.26_0.oci`
Oracle Linux 7.9	`uln-pca-Oracle-Linux-7.9-2023.09.26_0.oci`
Oracle Solaris 11.4	`uln-pca-Oracle-Solaris-11-2023.10.16_0.oci`
Kubernetes Engine	`uln-pca-Oracle-Linux8-OKE-1.26.6-20240210.oci`
	`uln-pca-Oracle-Linux8-OKE-1.27.7-20240209.oci`
	`uln-pca-Oracle-Linux8-OKE-1.28.3-20240210.oci`

Kubernetes Engine

Oracle Private Cloud Appliance Kubernetes Engine (OKE) is a scalable, highly available service that can be used to deploy any containerized application to the cloud. OKE uses Cluster API Provider (CAPI) and Cluster API Provider for Oracle Cloud Infrastructure (CAPOCI) to orchestrate the cluster on the Private Cloud Appliance. OKE uses Kubernetes, the open-source system for automating deployment, scaling, and management of containerized applications across clusters of hosts. Kubernetes groups the containers that make up an application into logical units called pods for easy management.

See the Oracle Private Cloud Appliance Kubernetes Engine user guide for information about how to configure the network, create an OKE cluster and node pool, expose containerized applications outside the appliance, and provide persistent storage for containerized applications. See the OKE Monitoring folder in Grafana for OKE dashboards.

Instance Principals

An instance principal is a compute instance that is authorized to perform actions on service resources. Applications running on an instance principal can call services and manage resources similar to the way Private Cloud Appliance users call services to manage resources. The instance is a principal actor just as a user is a principal actor. When you use instance principals, you do not need to configure user credentials or a configuration file on the instance to run applications that need to manage service resources.

To grant authorizations to an instance principal, include the instance as a member of a dynamic group. A dynamic group provides authorizations to instances just as a user group provides authorizations to users.

See "Configuring Instances for Calling Services" and "Creating and Managing Dynamic Groups" in the Identity and Access Management chapter of the *Oracle Private Cloud Appliance User Guide*.

Upgrade History and Enhancements

The upgrade history presents information from all upgrade and patch jobs in a categorized way, providing insight into which version upgrades have been performed, which jobs have been run for each of those upgrades, and from which source (ISO upgrade or ULN patch). Details include build versions, component versions before and after, job completion, success or failure, time stamps, and duration.

Oracle Integrated Lights Out Manager (ILOM) has been included in the upgrade or patch workflow of compute node and management node hosts, reducing the overall process duration and the number of reboots. The upgrade plan has also been refined and covers the Oracle Cloud Infrastructure images provided with Private Cloud Appliance.

An appliance software prerequisite version check is performed during the upgrade or patch preparation phase. The Upgrader service proceeds only if the running version passes this check, otherwise you must install the minimum required version first, before proceeding with the intended target version.

Upgrading or patching to this version of the appliance software also adds the *region registry*, which contains resources required for the operation of Kubernetes Engine.

All changes are reflected in the Oracle Private Cloud Appliance Upgrade Guide and Oracle Private Cloud Appliance Patching Guide.

ULN Mirror for Appliance Patching on Oracle Linux 8

The ULN mirror in the data center, which the appliance uses to retrieve new packages to patch components to the latest version, can now be configured on an Oracle Linux 8 server. For detailed information, refer to the chapter "Configure Your Environment for Patching" in the Oracle Private Cloud Appliance Patching Guide.

Backup Space Management

The Backup and Restore Service has been enhanced further to optimize storage space consumption on the ZFS Storage Appliance. When purging backups older than the retention period, the service also removes the large temporary files of previous MySQL database backups that are no longer required.

DRGv1+ Support

DRGv1+ provides VRF/VLAN-backed isolation for network traffic when using a DRG.

Bugs Fixed in This Release

For a list of bugs fixed in this release, see Oracle Support Document 3013714.1 ([PCA 3.x] Private Cloud Appliance X9-2 and X10 release and updates (3.0.2-b1081557)) can be found at: https://support.oracle.com/epmos/faces/DocumentDisplay?id=3013714.1.

Features Released in Software Version 3.0.2-b1001356 (December 2023)

X10 Rack Configuration

The Private Cloud Appliance X10 rack configuration ships from the factory with appliance software version 3.0.2-b1001356 or newer installed. This rack configuration is characterized by the use of Oracle Server X10 compute nodes (2U). Compared to the X9 rack configuration, the component order and cabling are slightly different. The storage and network infrastructure components are identical.

In terms of compute capacity, a 2U compute node is comparable to two 1U compute nodes. To deploy compute instances on the Oracle Server X10 compute nodes, you must select the *VM.PCAStandard.E5.Flex* shape, which offers adjustable CPUs, memory, and network bandwidth.

For more information about the X10 rack configuration, refer to the chapter Hardware Overview in the "Oracle Private Cloud Appliance Concepts Guide".

Platform Images

New platform images are made available for Compute Enclave users through Private Cloud Appliance installation, upgrade, and patching.

The following platform images are delivered with this Private Cloud Appliance release:

Oracle Linux 9	`uln-pca-Oracle-Linux-9-2023.08.31_0.oci`
Oracle Linux 8	`uln-pca-Oracle-Linux-8-2023.08.31_0.oci`
Oracle Linux 7.9	`uln-pca-Oracle-Linux-7.9-2023.08.31_0.oci`
Oracle Solaris 11.4	`uln-pca-Oracle-Solaris-11-2023.09.20_0.oci`

Network Load Balancer

A network load balancer provides automated layer 4 traffic distribution from one public or private entry point where incoming requests are received, to a set of backend servers in the virtual cloud network (VCN) where the requests are processed. For efficient resource management, you can attach a compute instance pool as a backend set.

Network load balancers and previously implemented (layer 7) application load balancers can coexist in your environment, and have shared resource configuration limits. The key difference is that the network load balancer operates at OSI network layer 4 and manages TCP traffic. It provides better performance but lacks the layer 7 routing intelligence. Distribution to the backend servers is controlled by a 5-tuple, 3-tuple, or 2-tuple hash policy. However, for architectural reasons these are mapped internally to a source IP hash, which ensures that a client's requests are all directed to the same backend server.

For information about layer 4 load balancing, see the chapter Network Load Balancing Overview of the *Oracle Private Cloud Appliance Concepts Guide*. Instructions to configure network load balancers can be found in the chapter Network Load Balancers of the *Oracle Private Cloud Appliance User Guide*

File System Service Improvements

File System Quota
You can set a space quota on a file system when you create the file system and when you update the file system. The quota includes the data in the file system and all snapshots created under the file system. You cannot set a quota smaller than the current usage of the file system.
For more information, see "Creating a File System" and "Updating a File System" in the *Oracle Private Cloud Appliance User Guide*.

File System High Performance Backing Store
By default, the backing store of a file system instance is the default pool of the attached ZFS Storage Appliance. You can specify that you want to use a high performance pool for the backing store. See `poolName` in "Creating a File System" in the *Oracle Private Cloud Appliance User Guide*.

Block Storage Volume Performance Option

By default, block volumes have Balanced performance. When you create block storage, you can optionally enable High performance. For a comparison of Balanced Performance and High Performance, see "Block Volume Performance Options" in the *Oracle Private Cloud Appliance Concepts Guide*.

Instance Pool Updates

Instance Pool Instance Attach and Detach
You can attach an existing instance to an instance pool or detach an instance that is attached to an instance pool.
When you detach an instance from a pool, you have the following choices:

- Regarding the detached instance, you can choose to terminate the instance or keep the instance as a standalone instance.
- Regarding the instance pool, you can choose to leave the pool as a smaller pool or create a new instance in the pool, using the instance configuration parameters for the pool.

For more information, see "Updating an Instance Pool" in the *Oracle Private Cloud Appliance User Guide*.

Instance Pool Soft Stop and Soft Reboot

When you use the Compute Web UI to stop or reboot an instance pool, by default soft stop or soft reboot is selected. A dialog enables you to stop or reboot all the instances in the pool immediately.

When you use the OCI CLI, you can specify `softstop` or `softreset`.

For more information, see "Stopping and Starting Instances in an Instance Pool" in the *Oracle Private Cloud Appliance User Guide*.

Compute Service Improvements

Instance Serial Console

To troubleshoot an instance that is not running, you can connect to the instance serial console as an alternative to using the instance VNC console. For more information, see "Remotely Troubleshooting an Instance by Using a Console Connection" in the *Oracle Private Cloud Appliance User Guide*.

Instance Configuration from an Existing Instance

In addition to creating an instance configuration by entering values in the Compute Web UI or in a file, you can create an instance configuration by using the configuration information from an existing compute instance. See "Working with Instance Configurations" in the *Oracle Private Cloud Appliance User Guide*.

More Bandwidth for Flexible Shape Instance Configurations

Maximum bandwidth for the VM.PCAStandard1.Flex shape is updated to more closely match the maximum bandwidth for fixed shapes. For 1-24 OCPUs, the maximum bandwidth is 24.6 Gbps. For 25-32 OCPUs, the maximum bandwidth is 1 Gbps per OCPU.

For the VM.PCAStandard.E5.Flex shape, maximum bandwidth for 1-24 OCPUs is 24.6 Gbps. Maximum bandwidth for 25-40 OCPUs is 1 Gbps per OCPU. Maximum bandwidth for 41-96 OCPUs is 40.0 Gbps.

IMDS Version 2 Endpoints

The Instance Metadata Service is available in two versions: version 1 and version 2. To increase the security of metadata requests, upgrade applications to use the IMDS version 2 endpoints.

New options are available in instance create and instance update to disable recognition of IMDSv1 endpoints. For more information, see "Retrieving Instance Metadata from Within the Instance" in the *Oracle Private Cloud Appliance User Guide*.

Features Released in Software Version 3.0.2-b925538 (August 2023)

Platform Images

New platform images are made available for Compute Enclave users through Private Cloud Appliance installation, upgrade, and patching.

The following platform images are delivered with this Private Cloud Appliance release:

Oracle Linux 9	`uln-pca-Oracle-Linux-9-2023.05.24_0.oci`
Oracle Linux 8	`uln-pca-Oracle-Linux-8-2023.05.24_0.oci`
Oracle Linux 7.9	`uln-pca-Oracle-Linux-7.9-2023.05.24_0.oci`
Oracle Solaris 11.4	`uln-pca-Oracle-Solaris-11-2023.04.18_0.oci`

New Kubernetes Version 1.25

In this release, the Kubernetes cluster hosted on the management nodes is upgraded to version 1.25, which implies that the environment goes through 5 full upgrade cycles. The Upgrader manages the entire process for you, but note that it takes at least 4 hours on a minimum appliance configuration, and up to 18 hours on a fully populated rack.

Streamlined Upgrade Process

Based on the upgrade plan, upgrade and patch operations for all components except firmware follow a prescribed order. All steps to prepare the upgrade environment must be completed before any upgrade or patch command can be run.

The upgrade plan logic has been improved to ensure that unnecessary component reboots are avoided, This shortens the overall upgrade or patch duration and minimizes the risk of failures, degraded performance, or downtime. In addition, the estimated durations listed in the upgrade plan are calculated more accurately, and the reboot and upgrade requirement indicators are more reliable.

Systems running appliance software version 3.0.1 need to be upgraded twice to reach the latest release. An intermediate upgrade to a version between 3.0.2-b776803 and 3.0.2-b892153 is required.

All changes are reflected in the Oracle Private Cloud Appliance Upgrade Guide and Oracle Private Cloud Appliance Patching Guide.

New Uplink Configuration Options

The data network uplinks (ports 1-4) from the appliance to the data center network can now be configured as a static routing connection without the use of vPC/MLAG for link aggregation. Data uplinks in active/active mode use the ECMP protocol; active/passive uplinks use VRRP.

The optional administration network uplink (port 5) now provides similar routing options as the data network. The administration network can be configured to use BGP-based dynamic routing. Static routing can now be configured without requiring vPC/MLAG for link aggregation. In active/active mode the uplink uses the ECMP protocol; an active/passive uplink uses VRRP.

See Configuring Oracle Private Cloud Appliance in the Oracle Private Cloud Appliance Installation Guide

DNS Mapping for Disaster Recovery

Custom CA certificates can now be used on systems that have been configured for disaster recovery. To allow the replication IP addresses to be resolved, pointer records must be added to the data center DNS configuration. These PTR records must map the ZFS Storage Appliance host names to the replication interface IPs of the remote system in the DR configuration. For more information and instructions, refer to the chapter Disaster Recovery in the Oracle Private Cloud Appliance Administrator Guide.

New Generation SSD

The Oracle Server X9-2 management and compute nodes use a pair of 240GB M.2 SATA hard drives as boot devices. As the current model is being phased out, a new generation has been qualified for Private Cloud Appliance. The new SSDs are functionally the same as the earlier model.

Features Released in Software Version 3.0.2-b892153 (July 2023)

Upgrade Enhancements

Both the upgrade and patching processes are now based on an *upgrade plan*, which is the result of a metadata comparison between the new version to be installed and the version currently running on the system. The upgrade plan ensures that components are only patched or upgraded if the latest version is newer. Overwriting an installed component with the same version can be forced, if necessary.

Every upgrade and patch command has a *verify-only* option. This can be used to test in advance for system health issues that would prevent the operation from completing successfully.

Patching or upgrading the operating system on the management nodes no longer requires the administrator to manually reassign the cluster primary role to another node in between operations. The code detects which node holds the primary role and automatically modifies the cluster configuration in the background.

User-friendly commands to retrieve IP addresses of nodes and their ILOMs have been added to the Service CLI.

The full management node cluster upgrade automatically runs the `upgradeOCIImages` command at the end. This updates the Oracle Cloud Infrastructure compute images across all tenancies.

All changes are reflected in the Oracle Private Cloud Appliance Upgrade Guide and Oracle Private Cloud Appliance Patching Guide.

Your Own CA Trust Chain

In the Oracle Private Cloud Appliance architecture, you can provide your own CA certificates which allows you to use your CA trust chain to access the rack's external interfaces.

> **Note**
>
> OpenSSH clients must be at least version openssh-clients-7.4p1 or later.

For instructions, see "Accessing External Interfaces with Your Certificate Authority Trust Chain" in the *Oracle Private Cloud Appliance Administrator Guide*.

Oracle Defined Volume Backup Policies

For scheduled (policy-based) backups of block volumes and boot volumes, you can select an Oracle defined policy to use as an alternative to defining your own policy. For descriptions of the Oracle defined backup policies, see "Volume Backups and Clones" in the Block Volume Storage Overview chapter in the *Oracle Private Cloud Appliance Concepts Guide*. For information about how to use these policies, see "Managing Backup Policies" in the Block Volume Storage chapter of the *Oracle Private Cloud Appliance User Guide*.

Platform Images

New platform images are made available for Compute Enclave users through Private Cloud Appliance installation, upgrade, and patching.

The following platform images are delivered with this Private Cloud Appliance release:

Oracle Linux 8	`uln-pca-Oracle-Linux-8-2022.08.29_0.oci`
Oracle Linux 7.9	`uln-pca-Oracle-Linux-7.9-2022.08.29_0.oci`
Oracle Solaris 11.4	`uln-pca-Oracle-Solaris-11-2023.04.18_0.oci`

Support for Oracle Exadata Multi-cluster VMs

Private Cloud Appliance now provides support for Oracle Exadata multi-cluster VMs. Note that when you are connecting more than one Oracle Exadata system to the Private Cloud Appliance rack, you must ensure that the configured IP address ranges do not overlap.

System Backup Service Updates

System backups that were created by running either a daily scheduled `brs` backup or a manual (`backup-now`) `brs` backup are retained for no more than 14 days.

After you upgrade the Private Cloud Appliance to this release and run either type of `brs` backup, all `brs` backups that were previously created and are older than 14 days are deleted.

ZFSSA manual snapshots are not deleted if they were not created by using any `brs` job, and their snapshot name is not in the following form (the `brs` snapshot naming convention):

`projectname/filesystemname_timestamp`

For more information, see "Backup and Restore" in the Appliance Administration Overview chapter of the *Oracle Private Cloud Appliance Concepts Guide* and the Backup and Restore chapter in the *Oracle Private Cloud Appliance Administrator Guide*.

Features Released in Software Version 3.0.2-b852928 (May 2023)

Load Balancer as a Service (Layer 7)

The Load Balancing service provides automated traffic distribution from one public or private entry point where incoming requests are received, to a set of backend servers in the virtual cloud network (VCN) where the requests are processed.

To efficiently manage compute resources associated with a load balancer, you can attach a compute instance pool to a load balancer backend set. Doing this adds each instance in the pool as a backend server in the backend set.

A load balancer manages TCP or HTTP traffic based on typical distribution policies like round-robin, least connections, or IP hash.

For optimal utilization of the backend resources, request routing on the listener side can be further refined by using multiple virtual host names and path route rules. Load balancers also provide configuration options for SSL traffic handling and session persistence.

For information about load balancing, see the Load Balancing Overview chapter of the *Oracle Private Cloud Appliance Concepts Guide*. Instructions to configure load balancers can be found in the chapter Load Balancing of the *Oracle Private Cloud Appliance User Guide*

Instance Pool Autoscaling

An instance pool defines a set of compute instances that is managed as a group. Autoscaling a pool enables you to use resources more effectively by stopping or removing instances when demand is lower and starting or adding instances when demand is higher.

For more information, see "Using Schedule-Based Autoscaling" in the section titled "Working with Instance Pools" in the *Oracle Private Cloud Appliance User Guide*.

You can use instance pool autoscaling along with load balancing by attaching an instance pool that has an autoscaling configuration to a load balancer backend set. See "Managing Instance Pool Load Balancer Attachments" in the section titled "Working with Instance Pools" in the *Oracle Private Cloud Appliance User Guide*.

High Availability Configuration and Fault Domain Enforcement Default

The Service Enclave has new commands that give administrators more control over how to implement instance high availability.

- Instance high availability: When enabled, instances are automatically reboot migrated off of an unreachable compute node. The default is enabled.
- Instance fault domain resolution: When enabled, instances that are running in a fault domain that is not the fault domain that is specified in their instance configuration (their selected fault domain) are automatically migrated back to their selected fault domain when resources become available in that fault domain. The default is enabled.

  Instances can become displaced (running in a fault domain that is not their selected fault domain) during compute node evacuation or failure. You can list all currently displaced instances.
- Instance restart: When enabled, instances that were stopped by the Compute service (not by an administrator) are automatically restarted in their selected fault domain when resources become available in that fault domain. The default is enabled.

  Instances can be stopped by the Compute service during compute node evacuation or compute node failure when no fault domain has resources to accommodate the instances, or when strict fault domain enforcement is enabled and no other compute node in the selected fault domain can accommodate the instances. You can list all instances that are currently stopped by the Compute service.
- Strict fault domain enforcement: When enabled, instances that cannot be accommodated in the current fault domain during compute node evacuation or failure will be stopped by the Compute service. If the force option is not used for compute node evacuation, instances will be still running in the current compute node and the compute node evacuation will fail.

  The default is disabled: Instances will be migrated to a different fault domain if possible.

For more information, see "Migrating Instances from a Compute Node" and "Configuring the Compute Service for High Availability" in the Hardware Administration chapter of the *Oracle Private Cloud Appliance Administrator Guide*.

Routing Options in Virtual Networking

The virtual networking configuration in the Compute Enclave provides additional routing options:

- setting a private IP address as a route rule target
- associating a route table with a dynamic routing gateway (DRG) attachment.

With this enhancement, existing data center infrastructure and applications can be integrated into the network communication between Private Cloud Appliance compute instances, or between instances and other network services external to the appliance.

Features Released in Software Version 3.0.2-b819070 (March 2023)

Fault Domain Enforcement for Compute Node Evacuation

When evacuating a compute node, you can specify the behavior you want if some instances cannot be accommodated in other compute nodes in the same fault domain.

- If strict enforcement is disabled, instances that cannot be accommodated in the current fault domain will be migrated to other fault domains if possible.
- If strict enforcement is enabled, instances that cannot be accommodated in the current fault domain will be left running in the current compute node.

See "Migrating Instances from a Compute Node" in the chapter Hardware Administration of the Oracle Private Cloud Appliance Administrator Guide for more information.

New Upgrade Guide

The instructions to upgrade an appliance were included in the Oracle Private Cloud Appliance Administrator Guide. That content is now moved to a separate Oracle Private Cloud Appliance Upgrade Guide.

Features Released in Software Version 3.0.2-b799577 (February 2023)

Fault Descriptions Improved

Hardware-related fault messages appearing in command output, logs and monitoring data now describe the observed issue more accurately. When a fault message is related to resource utilization, for example when a threshold is exceeded, the description explicitly mentions it. This prevents utilization warnings from being mistaken for actual hardware problems and makes troubleshooting easier.

Mounting File Systems Across Appliances

In a deployment comprising multiple Private Cloud Appliance systems it is now possible to mount an NFS export from the ZFS Storage Appliance of one appliance on a compute instance hosted on another appliance. The VCNs, mount target and export options must be appropriately configured to grant instances access to the remote file system.

Features Released in Software Version 3.0.2-b776803 (December 2022)

Platform Images

Platform images are available to all compartments in all tenancies without being imported to any compartment by users.

The following platform images are delivered with this Private Cloud Appliance release:

Oracle Linux 8	`uln-pca-Oracle-Linux-8-2022.08.29_0.oci`
Oracle Linux 7.9	`uln-pca-Oracle-Linux-7.9-2022.08.29_0.oci`
Oracle Solaris 11.4	`uln-pca-Oracle-Solaris-11.4.35-2021.09.20_0.oci`

New platform images are delivered through Private Cloud Appliance installation, upgrade, and patch.

> **Important**
>
> The Service Enclave administrator must import platform images after Private Cloud Appliance installation and should import platform images after every upgrade and patch in case new images were delivered. See "Providing Platform Images" in Hardware Administration in the *Oracle Private Cloud Appliance Administrator Guide*.

Instance Backup and Restore

Oracle Private Cloud Appliance provides API commands that enable you to back up instances. The commands are flexible to suit a variety of use cases, including:

- Back up instances and any attached block volumes.
- Store the backups on another server for safekeeping.
- Restore a faulty instance and any attached block volumes.
- Use the backup to create matching instances.
- Use the backup and restore feature to migrate instances to another tenancy, or to another appliance.

> **Note**
>
> The maximum recommended object size supported is 10TB of total data and the maximum recommended object part size in a multipart upload is 5 GB.

For details see *Instance Backup and Restore* in the Oracle Private Cloud Appliance Concepts Guide and *Backing Up and Restoring an Instance* in the Oracle Private Cloud Appliance User Guide.

Instance Shape Update

When you update an instance, you can change the shape. You can change from any shape to any other shape. If the flexible shape is specified, you can change the shape configuration. For more information, see "Updating an Instance" in Compute Instance Deployment in the Oracle Private Cloud Appliance User Guide.

Enhanced Compute Instance Availability

If a compute node is lost due to a failure, a new reboot migration process is invoked. Its purpose is to evacuate compute instances to other compute nodes. Fault domain preference is strictly enforced with instance migration. If a compute instance cannot be migrated to another compute node in the same fault domain due to insufficient capacity, the instance is stopped and must be restarted manually.

File System Clones

You can use the OCI CLI to create file system clones. A clone is a new file system that is created from a snapshot of an existing file system. Snapshots preserve the state of the data of a file system at a particular point in time. If you take snapshots of a file system at regular intervals, you can create clones of the file system as it existed at multiple points in its lifetime.

Cloned file systems are managed in the same way that any other file system is managed. See the File System Storage chapter in the Oracle Private Cloud Appliance User Guide.

Tags for Specifying Certain Property Values

Private Cloud Appliance provides defined tags that enable you to set values for some properties. Applying these tags is the only way to set these particular properties.

The following defined tags are in the OraclePCA tag namespace.

> **Note**
>
> Do not create your own tags in the OraclePCA tag namespace.

Resource, Operation	Tag Name	Values
Block volume, create and update	logBias	LATENCY, THROUGHPUT
	secondaryCache	ALL, METADATA, NONE
File system, create	databaseRecordSize	512, 1024, 2048, 4096, 8192, 16384, 32768, 65536, 131072, 262144, 524288, 1048576

You must use the OCI CLI to set these tags. See the OCI CLI procedures in "Working with Resource Tags" in Resource Tag Management in the Oracle Private Cloud Appliance User Guide.

For examples, see "Creating a Block Volume" in Block Volume Storage in the Oracle Private Cloud Appliance User Guide and "Creating a File System" in File System Storage in the Oracle Private Cloud Appliance User Guide.

Capacity Monitoring

Administrators have direct access to the current consumption of key physical resources: CPU, memory and storage space. For more information, see "Monitoring System Capacity" in the chapter Status and Health Monitoring of the Oracle Private Cloud Appliance Administrator Guide.

Full Administration Network Segregation

In an environment with elevated security requirements, you can optionally segregate administrative appliance access from the data traffic. The administration network physically separates configuration and management traffic from the operational activity on the data network. In this configuration, only the administration network provides access to the Service Enclave, which includes the monitoring, metrics collection and alerting services, the API service, and all component management interfaces.

Service Request Diagnostic Data

If the Private Cloud Appliance is registered for Oracle Auto Service Request (ASR), certain hardware failures cause a service request and diagnostic data to be automatically sent to Oracle support. The collection of diagnostic data is also called a support bundle. A Service Enclave administrator can also create and send a service request and supporting diagnostic data separate from ASR. For more information about ASR and support bundles, see Status and Health Monitoring in the *Oracle Private Cloud Appliance Administrator Guide*.

Features Released in Software Version 3.0.1-b741265 (November 2022)

Flexible Compute Shapes

A flexible compute shape lets you customize the number of OCPUs and the amount of memory when launching your instance. This flexibility lets you create instances that meet your workload requirements, while optimizing performance and using resources efficiently. For details see Compute Shapes in the Oracle Private Cloud Appliance Concepts Guide.

GUI Support for Viewing CPU and Memory Metrics

As of this release, you can view Memory and CPU metrics at a fault domain level using the Service Enclave GUI. For details, see Monitoring System Capacity in the Oracle Private Cloud Appliance Administrator Guide.

Features Released in Software Version 3.0.1-b697160 (August 2022)

Compute Instance Availability

When compute instances go down because of a compute node reboot or failure, the system takes measures to recover the compute instances automatically. For details, see Compute Instance Availability in the Oracle Private Cloud Appliance Concepts Guide.

Optimized NUMA Alignment

Algorithm optimizations are in place to ensure that the hypervisor assigns compute instances on physical resources (CPU and memory) with best possible alignment to compute node NUMA architecture. For details, see Physical Resource Allocation in the Oracle Private Cloud Appliance Concepts Guide.

View CPU and Memory Metrics at the Fault Domain Level

Memory and CPU usage metrics are available at the compute nodes level already. Each node belongs to a fault domain. New functionality provides the option to view these metrics at a fault domain level. For details, see Fault Domain Observability in the Oracle Private Cloud Appliance Concepts Guide, and Monitoring System Capacity in the Oracle Private Cloud Appliance Administrator Guide.

Secondary Private IP Addresses

After an instance is launched, you can attach secondary private IP addresses to the primary VNIC or to any secondary VNICs. These secondary private IP addresses are especially useful when running multiple services or endpoints on a single instance, or for instance failover scenarios.

For more information, see "About Secondary Private IPs" under "IP Addressing" in the Virtual Networking Overview chapter of the Oracle Private Cloud Appliance Concepts Guide.

For procedures, see "Assigning a Secondary Private IP Address" in the Networking chapter of the Oracle Private Cloud Appliance User Guide.

3

Service Limits

This chapter contains the service limits for Oracle Private Cloud Appliance. The limits presented here have been tested and are fully supported by Oracle.

The minimum appliance configuration contains three compute nodes and one high-capacity disk shelf with 100TB of usable disk space. Both compute and storage capacity can be expanded by adding compute nodes and disk shelves.

Compute Node Physical Resources

A part of each compute node's CPU and RAM capacity is reserved for system use. The table shows available physical resources by compute node model.

Compute Node Model	Total Physical Resources	Available Compute Capacity
Oracle Server X9-2	CPU: 64 cores (2x32) RAM: 1024 GB (16x64)	CPU: 60 cores RAM: 960 GB
Oracle Server X10	CPU: 192 cores (2x96) RAM: 2304 GB (24x96)	CPU: 184 cores RAM: 2224 GB
Oracle Server X11	CPU: 192 cores (2x96) RAM: 2304 GB (24x96)	CPU: 184 cores RAM: 2224 GB

Tenancy Resource Configuration Limits

This section lists the resource limits that are dependent on the appliance architecture. Oracle Private Cloud Appliance supports up to 8 tenancies; these are default limits per tenancy, unless indicated otherwise. The numbers provided here apply to any Private Cloud Appliance installation, regardless of its hardware configuration.

Some of these limits can be customized. See the Viewing and Setting Resource Limits chapter in the *Oracle Private Cloud Appliance Administrator Guide*.

Service	Resource Type	Limit
IAM Service	Users	100
IAM Service	Groups	100
IAM Service	Users per group	100
IAM Service	Groups per user	50
IAM Service	Compartments	50
IAM Service	Policies	100
IAM Service	Policy statements	50 per policy
IAM Service	Identity providers	3
IAM Service	Group mappings	100 per identity provider
Networking Service	VCNs	80 total across all tenancies with up to 16 SR-IOV VCNs

Service	Resource Type	Limit
Networking Service	Subnets	40 per VCN 320 across all tenancies
Networking Service	Dynamic routing gateways (DRG)	32 total across all tenancies with up to 16 SR-IOV DRGs
Networking Service	DRG attachments	10 per DRG 80 across all tenancies
Networking Service	Internet gateways	1 per VCN
Networking Service	Local peering gateways	5 per VCN 150 across all tenancies
Networking Service	NAT gateways	1 per VCN
Networking Service	Service gateways	1 per VCN
Networking Service	Storage gateways	2 per VCN 80 across all tenancies, standard and high-performance combined
Networking Service	Reserved public IPs	1/16th of customer-defined block
Networking Service	Ephemeral public IPs	2 per compute instance X9 rack: 2400 across all tenancies X10 rack: 3336 across all tenancies
Networking Service	DHCP options	30 per VCN 500 across all tenancies
Networking Service	Route tables	20 per VCN 500 across all tenancies
Networking Service	Route rules	50 per route table 10000 across all tenancies
Networking Service	VNICs	5000 across all tenancies
Networking Service	Network security groups	100 per VCN 5 per VNIC 600 across all tenancies
Networking Service	VNICs in network security group	As many VNICs as are in the VCN. A VNIC can belong to max. 5 network security groups
Networking Service	Security rules	50 per network security group 12000 across all tenancies
Networking Service	Security lists	20 per VCN 5 per subnet 600 across all tenancies
Networking Service	Ingress rules	30 per security list 12000 across all tenancies
Networking Service	Egress rules	30 per security list 12000 all tenancies

Service	Resource Type	Limit
Networking Service	DNS zones	1000 across all tenancies (in addition to any internal zones)
Networking Service	DNS records	25000 per zone 8000000 across all tenancies
Networking Service	Flex networks	128 flex networks 32 DRGs 128 logical ports 32 networks per physical port
Compute Service	Custom images	100
Block Storage Service	Aggregated size of block volumes	100TB (with default storage capacity)
Block Storage Service	Block volume backups	100000 across all tenancies
File Storage Service	File systems	100
File Storage Service	Mount targets	PCA_POOL 80 total across all tenancies PCA_POOL_HIGH 80 total across all tenancies
File Storage Service	File system size	3.3PB
Object Storage Service	Buckets	10000
(Network) Load Balancing Service	Load balancers (Network LB and LBaaS combined)	Version 3.0.2-b1185392 and earlier: 32 total across all tenancies, 20 in a single VCN Version 3.0.2-b1261765 and newer: 36-144 total, depending on rack capacity and custom configuration
(Network) Load Balancing Service	IP address	1 per load balancer
(Network) Load Balancing Service	Network security groups	5 per load balancer
(Network) Load Balancing Service	Listeners	16 per load balancer
(Network) Load Balancing Service	Backend sets	16 per load balancer
(Network) Load Balancing Service	Backend servers	512 per load balancer and per backend set
Kubernetes Engine (OKE)	Clusters	10 per tenancy
Kubernetes Engine (OKE)	Worker nodes	128 per cluster (across all pools)
Kubernetes Engine (OKE)	Pods	110 per node (Kubernetes default)

System Load and Concurrency Limits

This section shows how many concurrent operations of a given type Oracle Private Cloud Appliance can manage at any given time. The limits presented in the table apply across the entire system and all tenancies. For each of these limits it is assumed that no other operations of any kind are running at the same time. When a limit is exceeded, an error with code 409 or 429 is displayed.

Resource Type	Operation	Concurrency Limit
compute instance	back up or restore an instance	10
compute instance	launch/terminate instance	15
compute instance	reset/stop/start instance	15
compute instance	update fault domain (live migration)	10
compute image	create image from instance	10
compute image	import image	10
block volume	create/delete volume	10
block volume	attach/detach boot volume	15
block volume	attach/detach data volume	15
block volume	resize volume	15
file system	create/delete file system	10
mount target	create/delete mount target	10
VCN	create/delete VCN	10
VCN gateway	create/delete gateway (all types)	10
subnet	create/delete subnet	10
route table	create/delete route table	10
security list	create/delete security list	10
network security group	create/delete network security group	10
VNIC	attach/detach VNIC	15
public IP	create/delete public IP	10
private IP	create/delete private IP	10
all networking resources	update network resource	10
Kubernetes cluster	create/update/delete cluster	10
Kubernetes node pool	create/update/delete node pool	5
Kubernetes node	create/update/delete node	15

> **Note**
>
> In addition, there is a system limit on the number of concurrent user sessions:
>
> - Compute Web UI: 10 tenancy users
> - Service Web UI: 6 administrators
>
> An authentication error is displayed when the limit is reached. An inactive user session times out after 1 hour.

Guest Operating System Matrix

Oracle Cloud Infrastructure compute images of Oracle Linux and Oracle Solaris are provided as part of the appliance software, and new image versions are added through upgrades and patches. Updates of the Oracle-provided images are listed by software version in the Feature Updates chapter.

Oracle Private Cloud Appliance supports other guest operating systems, which you can add to your appliance environment as custom images. Several guest operating systems are part of Oracle testing and are known to work in Private Cloud Appliance compute instances. The table below provides an overview.

Guest Operating System	Oracle-Provided Image	Custom Image	Oracle-Tested
Oracle Linux 9.x	Y	Y	Y
Oracle Linux 8.x	Y	Y	Y
Oracle Linux 7.x	Y	Y	Y
Oracle Solaris 11.x	Y	Y	Y
Red Hat Enterprise Linux 9.x		Y	Y
Red Hat Enterprise Linux 8.x		Y	Y
Red Hat Enterprise Linux 7.x		Y	Y
CentOS Linux 8.x		Y	
CentOS Linux 7.x		Y	
SUSE Linux Enterprise Server 15 (latest)		Y	
SUSE Linux Enterprise Server 12 SP4		Y	
Ubuntu 20.04 and later		Y	
Ubuntu 18.04 and later		Y	
AlmaLinux OS 9.2		Y	Y
Kali Linux		Y	Y
Microsoft Windows Server 2022		Y	Y
Microsoft Windows Server 2019		Y	Y
Microsoft Windows Server 2016		Y	Y

4
Known Issues and Workarounds

This chapter provides information about known issues and workarounds for Oracle Private Cloud Appliance. They are presented in separate sections per category, thus allowing you to navigate more easily.

Platform Issues

This section describes known issues and workarounds related to the appliance platform layer.

Compute Node Provisioning Takes a Long Time

The provisioning of a new compute node typically takes only a few minutes. However, there are several factors that may adversely affect the duration of the process. For example, the management nodes may be under a high load or the platform services involved in the provisioning may be busy or migrating between hosts. Also, if you started provisioning several compute nodes in quick succession, note that these processes are not executed in parallel but one after the other.

Workaround: Unless an error is displayed, you should assume that the compute node provisioning process is still ongoing and will eventually complete. At that point, the compute node provisioning state changes to *Provisioned*.

Bug: 33519372

Version: 3.0.1

Not Authorized to Reconfigure Appliance Network Environment

If you attempt to change the network environment parameters for the rack's external connectivity when you have just completed the initial system setup, your commands are rejected because you are not authorized to make those changes. This is caused by a security feature: the permissions for initial system setup are restricted to only those specific setup operations. Even if you are an administrator with unrestricted access to the Service Enclave, you must disconnect after initial system setup and log back in again to activate all permissions associated with your account.

Workaround: This behavior is expected and was designed to help protect against unauthorized access. In case you need to modify the appliance external network configuration right after the initial system setup, log out and log back in to make sure that your session is launched with the required privileges.

Bug: 33535069

Version: 3.0.1

Error Changing Hardware Component Password

The hardware layer of the Oracle Private Cloud Appliance architecture consists of various types of components with different operating and management software. As standalone products their password policies can vary, but the appliance software enforces a stricter rule set. If an error is returned when you try to change a component password, ensure that your new password complies with the Private Cloud Appliance policy for hardware components.

For more information about password maintenance across the entire appliance environment, refer to the Oracle Private Cloud Appliance Security Guide.

Workaround: For hardware components, use the Service CLI to set a password that conforms to the following rules:

- consists of at least 8 characters
  - with a maximum length of 20 characters for compute nodes, management nodes, and switches
  - with a maximum length of 16 characters for ILOMs and the ZFS Storage Appliance
- contains at least one lowercase letter (a-z)
- contains at least one uppercase letter (A-Z)
- contains at least one digit (0-9)
- contains at least one symbol (@$!#%*&)

Bug: 35828215

Version: 3.0.2

Grafana Service Statistics Remain at Zero

The Grafana Service Monitoring folder contains a dashboard named Service Level, which displays statistical information about requests received by the fundamental appliance services. These numbers can remain at zero even though there is activity pertaining to the services monitored through this dashboard.

Workaround: No workaround is currently available.

Bug: 33535885

Version: 3.0.1

Terraform Provisioning Requires Fully Qualified Domain Name for Region

If you use the Oracle Cloud Infrastructure Terraform provider to automate infrastructure provisioning on Oracle Private Cloud Appliance, you must specify the fully qualified domain name of the appliance in the region variable for the Terraform provider.

Synchronizing Hardware Data Causes Provisioning Node to Appear Ready to Provision

Both the Service Web UI and the Service CLI provide a command to synchronize the information about hardware components with the actual status as currently registered by the internal hardware management services. However, you should not need to synchronize hardware status under normal circumstances, because status changes are detected and communicated automatically.

Furthermore, if a compute node provisioning operation is in progress when you synchronize hardware data, its Provisioning State could be reverted to *Ready to Provision*. This information is incorrect, and is caused by the hardware synchronization occurring too soon after the provisioning command. In this situation, attempting to provision the compute node again is likely to cause problems.

Workaround: If you have started provisioning a compute node, and its provisioning state reads *Provisioning*, wait at least another five minutes to see if it changes to *Provisioned*. If it takes excessively long for the compute node to be listed as *Provisioned*, run the Sync Hardware Data command.

If the compute node still does not change to *Provisioned*, retry provisioning the compute node.

Bug: 33575736

Version: 3.0.1

Automatic Disk Shelf Provisioning Disabled for Storage Expansions

During the initial installation of the Private Cloud Appliance, the disk shelves present are automatically added to the appropriate pool: capacity or high-performance. When disk shelves are added at a later time to expand the storage capacity of the appliance, these are no longer automatically provisioned and added to the respective storage pools. This functional change was implemented in appliance software versions newer than 3.0.2-b1081557.

Because storage expansions are processed serially, regardless of how many disk shelves are added in a single operation, automated reconfiguration of the storage pools leads to an excessive number of spare drives. To ensure cost-effective and correctly balanced use of storage resources, it was decided to remove this automation in the latest appliance software.

Workaround: Storage expansions for Private Cloud Appliance are best configured on a case by case basis, so that the number of spare drives can be adjusted to the specific storage configuration of the rack. Contact Oracle for assistance. Storage expansion scenarios are covered in the note with Doc ID 3020837.1.

Bug: 36623140

Version: 3.0.2

Rack Elevation for Storage Controller Not Displayed

In the Service Web UI, the Rack Units list shows all hardware components with basic status information. One of the data fields is *Rack Elevation*, the rack unit number where the component in question is installed. For one of the controllers of the ZFS storage appliance, `pcasn02`, the rack elevation is shown as *Not Available*.

Workaround: There is no workaround. The underlying hardware administration services currently do not populate this particular data field. The two controllers occupy 2 rack units each and are installed in RU 1-4.

Bug: 33609276

Version: 3.0.1

Fix available: Please apply the latest patches to your system.

Switch Hardware State Reported "Up"

An expansion rack has its own set of switches, connected into the base rack. When the data and administration networks are integrated across the interconnected racks, the appliance platform recognizes the expansion hardware as part of the same system. If you query the switches, the list contains all switches of that type in the system, but the hardware state of an expansion switch is reported as "Up" instead of "OK".

```
# pca-admin switch leaf list
+----------+-----------+------------+-------------------------------------+-------------
+-----------+----------+--------------------+
|   RackID | Rack Unit | CPU Vendor | Model                               | IP Address
| Hostname  | HW State | Provisioning state |
+----------+-----------+------------+-------------------------------------+-------------
+-----------+----------+--------------------+
|        1 | 22        | Cisco      | cisco Nexus9000 C9336C-FX2 Chassis  | 100.96.2.22
| pcaswlf01 | OK       | Ready              |
|        1 | 23        | Cisco      | cisco Nexus9000 C9336C-FX2 Chassis  | 100.96.2.23
| pcaswlf02 | OK       | Ready              |
|        2 | 23        | Cisco      | cisco Nexus9000 C9336C-FX2 Chassis  | 100.96.2.40
| pcaswlf03 | Up       | Ready              |
|        2 | 22        | Cisco      | cisco Nexus9000 C9336C-FX2 Chassis  | 100.96.2.41
| pcaswlf04 | Up       | Ready              |
+----------+-----------+------------+-------------------------------------+-------------
+-----------+----------+--------------------+

# pca-admin switch mgmt list
+----------+-----------+------------+-------------------------------------+-------------
+-----------+----------+--------------------+
|   RackID | Rack Unit | CPU Vendor | Model                               | IP Address
| Hostname  | HW State | Provisioning state |
+----------+-----------+------------+-------------------------------------+-------------
+-----------+----------+--------------------+
|        1 | 24        | Cisco      | cisco Nexus9000 C9348GC-FXP Chassis | 100.96.2.1
| pcaswmn01 | OK       | Ready              |
|        2 | 23        | Cisco      | cisco Nexus9000 C9348GC-FXP Chassis | 100.96.2.46
| pcaswmn02 | Up       | Ready              |
+----------+-----------+------------+-------------------------------------+-------------
+-----------+----------+--------------------+
```

Workaround: The different hardware state label is harmless. There is no workaround.

Bug: 37076258

Version: 3.0.2

Free-Form Tags Used for Extended Functionality

You can use the following free-form tags to extend the functionality of Oracle Private Cloud Appliance.

> **Note**
>
> Do not use these tag names for other purposes.

- `PCA_no_lm`

  Use this tag to instruct the Compute service not to live migrate an instance. The value can be either True or False.

  By default, an instance can be live migrated, such as when you need to evacuate all running instances from a compute node. Live migration can be a problem for some instances. For example, live migration is not supported for instances in a Microsoft

Windows cluster. To prevent an instance from being live migrated, set this tag to True on the instance.

Specify this tag in the Tagging section of the Create Instance or Edit ***instance_name*** dialog, in the `oci compute instance launch` or `oci compute instance update` command, or using the API.

The following is an example option for the `oci compute instance launch` command:

```
--freeform-tags '{"PCA_no_lm": "True"}'
```

Setting this tag to True on an instance will not prevent the instance from being moved when you change the fault domain. Changing the fault domain is not a live migration. When you change the fault domain of an instance, the instance is stopped, moved, and restarted.

- `PCA_blocksize`

  Use this tag to instruct the ZFS storage appliance to create a new volume with a specific block size.

  The default block size is 8192 bytes. To specify a different block size, specify the `PCA_blocksize` tag in the Tagging section of the Create Block Volume dialog, in the `oci bv volume create` command, or using the API. Supported values are a power of 2 between 512 and 1M bytes, specified as a string and fully expanded.

  The following is an example option for the `oci bv volume create` command:

  ```
  --freeform-tags '{"PCA_blocksize": "65536"}'
  ```

  The block size cannot be modified once the volume has been created.

Use of these tags counts against your tag limit.

Version: 3.0.1

Terraform Apply Can Delete Default Tags

Sometimes, the OCI Terraform provider unexpectedly deletes existing tag defaults from a resource during `terraform apply`. For example, the Oracle-Tags.CreatedBy and Oracle-Tags.CreatedOn tag defaults that were automatically assigned when the resource was created might be deleted on a subsequent `terraform apply`.

Workaround: Add the `ignore_defined_tags` attribute to your provider block, listing the tags that you want the Terraform provider to ignore during `plan` or `apply`, as shown in the following example:

```
provider "oci" {
    ignore_defined_tags = ["Oracle-Tags.CreatedBy", "Oracle-Tags.CreatedOn"]
}
```

Bug: 36692217

Version: 3.0.2

Depend on the Tag Definition in a Terraform Resource Definition that Includes a New Defined Tag

If your Terraform plan includes both defined tag definitions and other resource definitions that use those defined tags, then you must tell Terraform about this dependency so that the resources are created in the correct order. In the definition of each resource that uses a tag that is defined in this same plan, include a `depends_on` meta-argument that points to where the tag is defined, as shown in the following example:

```
resource "oci_identity_tag_namespace" "example_tag_ns" {
  tag_namespace_definition
}
resource "oci_identity_tag" "example_tag" {
  tag_key_definition
}
...
resource "oci_resource" "resource_name" {
  depends_on = [
    oci_identity_tag.example_tag
  ]
  resource_definition
}
```

If you do not use `depends_on` to tell Terraform about a dependency, you can use one of the following methods:

- Create the defined tag in a separate Terraform plan, and apply that plan before you apply the plan that creates the resource that uses the tag.
- If your apply fails because the tag was unknown when the resource that uses the tag was created, apply the same plan again.

Bug: 36701647

Version: 3.0.2

Failure Creating Dynamic Groups and Policies through Terraform Plan

When using Terraform to create identity groups or dynamic groups and associated policies, it is likely that an error is returned when you apply the Terraform plan. The IAM Service does not allow a policy to be created for an identity group that does not exist. Therefore, if the policy resource defined in the Terraform plan is created before the identity (dynamic) group to which is applies, an authorization error or an object not found error is returned. For example:

```
... |
 Error: 404-NotAuthorizedOrNotFound, Authorization failed or requested resource not
found.
 Suggestion: Either the resource has been deleted or service Identity Policy need policy
to access this resource.
 Policy reference: https://docs.oracle.com/en-us/iaas/Content/Identity/Reference/
policyreference.htm
...
```

Note that all resources are typically created correctly despite the error message. When the Terraform plan is applied a second time, the command is usually successful.

Workaround: If a dependency exists between Private Cloud Appliance resource creation operations, use the Terraform `depends_on` feature to make this dependency explicit in the Terraform plan. The `depends_on` meta-argument tells Terraform to create the depended-on resource before creating the dependent resource. For example, add a `depends_on` statement similar to the highlighted line below.

```
resource "oci_identity_dynamic_group" "test_dynamic_group" {
  compartment_id = "ocid1.tenancy....unique_ID"
  description    = "Terraform test dependency"
  matching_rule  = "matching_rule1"
  name           = "testdyngrp"
}
resource "oci_identity_policy" "dg_policy" {
  compartment_id = "ocid1.tenancy....unique_ID"
  description    = "Test DG Policy"
  name           = "DGPolicy"
  statements     = [
    "allow dynamic-group testdyngrp to manage all-resources in tenancy"
  ]
  depends_on = [
    oci_identity_dynamic_group.test_dynamic_group
  ]
}
```

Bug: 36536058

Version: 3.0.2

Maximum Length of User Name Differs from Oracle Cloud Infrastructure

Oracle Cloud Infrastructure accepts accounts with very long user names. The maximum user name length in the IAM service of Private Cloud Appliance is not the same. This can be problematic when migrating a public cloud setup into the Private Cloud Appliance environment. In this case, the IAM service returns an error "`Data too long for column 'name' at row x`".

Workaround: Update the user account that causes the issue by setting a shorter user name.

Bug: 36536058

Version: 3.0.2

Terraform Requires Escaping Double Quotation Marks in Complex Tag Values

A complex tag value has a key as well as a value in the value field. In Terraform, this complex value requires that you escape double quotation marks inside the braces that surround the complex value.

The following example shows a complex tag value. In this example, the value of the *`key1_name`* tag key is another key and its value:

```
{"key1_name": {"key2_name": "key2_value"}}
```

For comparison, the following example shows how to specify this value in the OCI CLI:

```
--freeform-tags '{"key1_name": {"key2_name": "key2_value"}}'
```

The following example shows how to specify this value using Terraform:

```
freeform_tags = {"key1_name" = "{\"key2_name\": \"key2_value\"}"}
```

The following example is the Terraform for defined tags used to create an OKE cluster. Note the two key/value pairs that are the value of the OraclePCA.cpNodeShapeConfig tag:

```
defined_tags={"OraclePCA.cpNodeCount"="3","OraclePCA.cpNodeShape"="VM.PCAStandard1.Flex",
"OraclePCA.cpNodeShapeConfig"="{\"ocpus\":1,\"memoryInGBs\":10}","OraclePCA.sshkey"="sshk
ey"}
```

Bug: 36691556

Version: 3.0.2

Imported Images Not Synchronized to High-Performance Pool

In an Oracle Private Cloud Appliance with default storage configuration, when you import compute images, they are stored on the ZFS Storage Appliance in an `images` LUN inside the standard ZFS pool. If the storage configuration is later extended with a high-performance disk shelf, an additional high-performance ZFS pool is configured on the ZFS Storage Appliance. Because there is no replication between the storage pools, the images from the original pool are not automatically made available in the new high-performance pool. The images have to be imported manually.

Workaround: When adding high-performance storage shelves to the appliance configuration, import the required compute images again to ensure they are loaded into the newly created ZFS pool.

Bug: 33660897

Version: 3.0.1

API Server Failure After Management Node Reboot

When one of the three management nodes is rebooted, it may occur that the API server does not respond to any requests, even though it can still be reached through the other two management nodes in the cluster. This is likely caused by an ownership issue with the virtual IP shared between the management nodes, or by the DNS server not responding quickly enough to route traffic to the service pods on the available management nodes. After the rebooted management node has rejoined the cluster, it may still take several minutes before the API server returns to its normal operating state and accepts requests again.

Workaround: When a single management node reboots, all the services are eventually restored to their normal operating condition, although their pods may be distributed differently across the management node cluster. If your UI, CLI or API operations fail after a management node reboot, wait 5 to 10 minutes and try again.

Bug: 33191011

Version: 3.0.1

Administrators in Authorization Group Other Than SuperAdmin Must Use Service CLI to Change Password

Due to high security restrictions, administrators who are not a member of the *SuperAdmin* authorization group are unable to change their account password in the Service Web UI. An authorization error is displayed when an administrator from a non-SuperAdmin authorization group attempts to access their own profile.

Workaround: Log in to the Service CLI, find your user id in the user preferences, and change your password as follows:

```
PCA-ADMIN> show UserPreference
Data:
  Id = 1c74b2a5-c1ce-4433-99da-cb17aab4c090
  Type = UserPreference
[...]
  UserId = id:5b6c1bfa-453c-4682-e692-6f0c91b53d21  type:User  name:dcadmin
```

```
PCA-ADMIN> changePassword id=<user_id> password=<new_password>
confirmPassword=<new_password>
```

Bug: 33749967

Version: 3.0.1

Service Web UI and Grafana Unavailable when HAProxy Is Down

HAProxy is the load balancer used by the Private Cloud Appliance platform layer for all access to and from the microservices. When the load balancer and proxy services are down, the Service Web UI and Grafana monitoring interface are unavailable. When you attempt to log in, you receive an error message: "*Server Did Not Respond*".

Workaround: Log in to one of the management nodes. Check the status of the HAProxy cluster resource, and restart if necessary.

```
# ssh pcamn01
# pcs status
Cluster name: mncluster
Stack: corosync
[...]
Full list of resources:

 scsi_fencing   (stonith:fence_scsi):   Stopped (disabled)
 Resource Group: mgmt-rg
     vip-mgmt-int     (ocf::heartbeat:IPaddr2):       Started pcamn03
     vip-mgmt-host    (ocf::heartbeat:IPaddr2):       Started pcamn03
     vip-mgmt-ilom    (ocf::heartbeat:IPaddr2):       Started pcamn03
     vip-mgmt-lb      (ocf::heartbeat:IPaddr2):       Started pcamn03
     vip-mgmt-ext     (ocf::heartbeat:IPaddr2):       Started pcamn03
     l1api            (systemd:l1api):                Started pcamn03
     haproxy          (ocf::heartbeat:haproxy):       Stopped (disabled)
     pca-node-state   (systemd:pca_node_state):       Started pcamn03
     dhcp             (ocf::heartbeat:dhcpd):         Started pcamn03
     hw-monitor       (systemd:hw_monitor):           Started pcamn03
```

To start HAProxy, use the `pcs resource` command as shown in the example below. Verify that the cluster resource status has changed from "*Stopped (disabled)*" to "*Started*".

```
# pcs resource enable haproxy
# pcs status
[...]
 Resource Group: mgmt-rg
     haproxy          (ocf::heartbeat:haproxy):       Started pcamn03
```

Bug: 34485377

Version: 3.0.2

Lock File Issue Occurs when Changing Compute Node Passwords

When a command is issued to modify the password for a compute node or ILOM, the system sets a temporary lock on the relevant database to ensure that password changes are applied in a reliable and consistent manner. If the database lock cannot be obtained or released on the first attempt, the system makes several further attempts to complete the request. Under normal operating circumstances, it is expected that the password is eventually successfully changed. However, the command output may contain error messages such as "*Failed to create DB lockfile*" or "*Failed to remove DB lock*", even if the final result is "*Password successfully changed*".

Workaround: The error messages are inaccurate and can be ignored as long as the password operations complete as expected. No workaround is required.

Bug: 34065740

Version: 3.0.2

Compute Node Hangs at Dracut Prompt after System Power Cycle

When an appliance or some of its components need to be powered off, for example to perform maintenance, there is always a minimal risk that a step in the complex reboot sequence is not completed successfully. When a compute node reboots after a system power cycle, it can hang at the `dracut` prompt because the boot framework fails to build the required initramfs/initrd image. As a result, primary GPT partition errors are reported for the root file system.

Workaround: Log on to the compute node ILOM. Verify that the server has failed to boot, and is in the `dracut` recovery shell. To allow the compute node to return to normal operation, reset it from the ILOM using the `reset /System` command.

Bug: 34096073

Version: 3.0.2

No Error Reported for Unavailable Spine Switch

When a spine switch goes offline due to loss of power or a fatal error, the system gives no indication of the issue in the Service Enclave UI/CLI or Grafana. This behavior is the result of the switch client not properly handling exceptions and continuing to report the default "healthy" status.

Workaround: There is currently no workaround to make the system generate an error that alerts the administrator of a spine switch issue.

Bug: 34696315

Version: 3.0.2

ZFS Storage Appliance Controller Stuck in Failsafe Shell After Power Cycle

The two controllers of the Oracle ZFS Storage Appliance operate in an active-active cluster configuration. When one controller is taken offline, for example when its firmware is upgraded or when maintenance is required, the other controller takes ownership of all storage resources to provide continuation of service. During this process, several locks must be applied and released. When the rebooted controller rejoins the cluster to take back ownership of its assigned storage resources, the cluster synchronization will fail if the necessary locks are not released correctly. In this situation, the rebooted controller could become stuck in the failsafe shell, waiting for the peer controller to release certain locks. This is likely the result of a takeover operation that was not completed entirely, leaving the cluster in an indeterminate state.

Workaround: There is currently no workaround. If the storage controller cluster ends up in this condition, contact Oracle for assistance.

Bug: 34700405

Version: 3.0.2

Concurrent Compute Node Provisioning Operations Fail Due to Storage Configuration Timeout

When the Private Cloud Appliance has just been installed, or when a set of expansion compute nodes have been added, the system does not prevent you from provisioning all new compute nodes at once. Note, however, that for each provisioned node the storage initiators and targets must be configured on the ZFS Storage Appliance. If there are too many configuration update requests for the storage appliance to process, they will time out. As a result, all compute node provisioning operations will fail and be rolled back to the unprovisioned state.

Workaround: To avoid ZFS Storage Appliance configuration timeouts, provision compute nodes sequentially one by one, or in groups of no more than 3.

Bug: 34739702

Version: 3.0.2

Data Switch Fails to Boot Due to Active Console Connection

If a Cisco Nexus 9336C-FX2 Switch has an active local console session, for example when a terminal server is connected, the switch could randomly hang during reboot. It is assumed that the interruption of the boot sequence is caused by a ghost session on the console port. This behavior has not been observed when no local console connection is used.

Workaround: Do not connect any cables to the console ports of the data switches. There is no need for a local console connection in a Private Cloud Appliance installation.

Bug: 32965120

Version: 3.0.2

Switches in Failed State Due to Expired Certificate

During the appliance software upgrade, new certificates are installed for authentication between components. It may occur that a certificate is not uploaded to the switches. When the certificate on the switches expires, they go into a failed state, which results in critical active faults.

```
PCA-ADMIN> list fault where status EQ ACTIVE
Data:
  id                                     Name
Status   Severity
  --                                     ----
------   --------
  d38d1e3b-893e-49bd-a62a-77b0bd22e5d9   RackUnitRunStateFaultStatusFault(pcaswmn01)
Active   Critical
  c0358065-ea81-4ad3-4a6c-017194f73659   RackUnitRunStateFaultStatusFault(pcaswlf01)
Active   Critical
  2fe549b7-596c-4a6c-25d3-1f9fa4b0bd1c   RackUnitRunStateFaultStatusFault(pcaswlf02)
Active   Critical
  25d3c91d-1e69-4f73-8319-f5ed18f6a903   RackUnitRunStateFaultStatusFault(pcaswsp01)
Active   Critical
  4af35eff-994f-c400-a93a-314cc43c97a1   RackUnitRunStateFaultStatusFault(pcaswsp02)
Active   Critical
```

Workaround: Confirm that the switch certificates have expired, then reprovision the switches to force a new certificate to be uploaded. Follow the instructions in the note with Doc ID 3080032.1. When completed successfully, the switches return to *Ready* state.

Bug: 37743552

Version: 3.0.2

Federated Login Failure after Appliance Upgrade

Identity federation allows users to log in to Private Cloud Appliance with their existing company user name and password. After an upgrade of the appliance software, the trust relationship between the identity provider and Private Cloud Appliance might be broken, causing all federated logins to fail. During the upgrade the Private Cloud Appliance X.509 external server certificate could be updated for internal service changes. In this case, the certificate on the identity provider side no longer matches.

Workaround: If the identity provider allows it, update its service provider certificate.

1. Retrieve the appliance SAML metadata XML file from `https://iaas.<domain>/saml/<TenancyId>` and save it to a local file.
2. Open the local file with a text editor and find the `<X509Certificate>` element.

```
<SPSSODescriptor>
    <KeyDescriptor use="signing">
        <KeyInfo>
            <X509Data>
                <X509Certificate>
                    <COPY CERTIFICATE CONTENT FROM HERE>
                  </X509Certificate>
            </X509Data>
        </KeyInfo>
    </KeyDescriptor>
</KeyDescriptor>
```

3. Copy the certificate content and save it to a new `*.pem` file, structured as follows:

```
-----BEGIN CERTIFICATE-----
<PASTE CERTIFICATE CONTENT HERE>
-----END CERTIFICATE-----
```

4. Update the identity provider with this new service provider certificate for your Private Cloud Appliance.

If the identity provider offers no easy way to update the certificate, we recommend that you delete the service provider and reconfigure identity federation. For more information, refer to the section "Federating with Microsoft Active Directory" in the Oracle Private Cloud Appliance Administrator Guide.

Bug: 35688600

Version: 3.0.2

Ensure No Storage Buckets Are Present Before Deleting a Compartment or Tenancy

When a command is issued to delete a compartment or tenancy, the appliance software cannot reliably confirm that no object storage buckets exist, because it has no service account with access to all buckets present on the ZFS Storage Appliance. As a result, access to certain object storage buckets could be lost when their compartment is deleted.

Workaround: Before deleting a compartment or tenancy, verify that no object storage buckets are present in that compartment or tenancy.

Bug: 35811594

Version: 3.0.2

Listing Upgrade Jobs Fails with RabbitMQ Error

When you run the Service CLI command `getUpgradeJobs`, the following error might be returned:

```
PCA-ADMIN> getUpgradeJobs
Status: Failure
Error Msg: PCA_GENERAL_000012: Error in RabbitMQ service: null
```

Workaround: The issue is temporary. Please retry the command at a later time.

Bug: 35999461

Version: 3.0.2

Availability Domain Name Change in Version 3.0.2-b1001356

In software version 3.0.2-b1001356 (December 2023), Private Cloud Appliance's single availability domain has been renamed from "`ad1`" to "`AD-1`". This change was required for compatibility with Oracle Cloud Infrastructure. The availability domain is a mandatory parameter in a small set of commands, and an optional parameter in several other commands.

The `--availability-domain` parameter is required with the following commands:

```
oci bv boot-volume create
oci bv boot-volume list
oci bv volume create
oci bv volume-group create
oci compute instance launch
oci compute boot-volume-attachment list
oci fs file-system create
oci fs file-system list
oci fs mount-target create
oci fs mount-target list
oci fs export-set list
oci iam fault-domain list
```

Workaround: Ensure that the correct value is used to identify the availability domain in your commands, depending on the version of the appliance software your system is running. If you are using scripts or any form of automation that includes the `--availability-domain` parameter, ensure that your code is updated when you upgrade or patch the appliance with version 3.0.2-b1001356 or newer.

Bug: 36094977

Version: 3.0.2

No Packages Available to Patch MySQL Cluster Database

With the release of appliance software version 3.0.2-b1001356, new MySQL RPM packages were added to the ULN channel *PCA 3.0.2 MN*. However, a package signing issue prevents the ULN mirror from downloading them, which means the MySQL cluster database on your system cannot be patched to the latest available version.

When patching the system, you will see no error message or abnormal behavior related to the missing MySQL packages. Follow the workaround to obtain the new packages. Once these have been downloaded to the ULN mirror, you can patch the MySQL cluster database.

> **Note**
>
> For new ULN mirror installations, the steps to enable updates of MySQL packages have been included in the Oracle Private Cloud Appliance Patching Guide under "Configure Your Environment for Patching".

To determine if a system is affected by this issue, check the ULN mirror for the presence of MySQL packages in the yum directory referenced by the `pca302_x86_64_mn` soft link. If the search returns no results, the ULN mirror was unable to download the MySQL packages. The default location of the yum setup directory is `/var/www/html/yum`, which is used in the following example:

```
# ls -al /var/www/html/yum/pca302_x86_64_mn/getPackage/ | grep mysql
-rw-r--r--. 1 root root  85169400 Dec 19 03:19 mysql-cluster-commercial-
client-8.0.33-1.1.el7.x86_64.rpm
-rw-r--r--. 1 root root   4751220 Dec 19 03:19 mysql-cluster-commercial-client-
plugins-8.0.33-1.1.el7.x86_64.rpm
-rw-r--r--. 1 root root    689392 Dec 19 03:19 mysql-cluster-commercial-
common-8.0.33-1.1.el7.x86_64.rpm
-rw-r--r--. 1 root root  12417692 Dec 19 03:19 mysql-cluster-commercial-data-
node-8.0.33-1.1.el7.x86_64.rpm
-rw-r--r--. 1 root root   2229080 Dec 19 03:19 mysql-cluster-commercial-icu-data-
files-8.0.33-1.1.el7.x86_64.rpm
-rw-r--r--. 1 root root   2236184 Dec 19 03:19 mysql-cluster-commercial-
libs-8.0.33-1.1.el7.x86_64.rpm
-rw-r--r--. 1 root root   1279012 Dec 19 03:19 mysql-cluster-commercial-libs-
compat-8.0.33-1.1.el7.x86_64.rpm
-rw-r--r--. 1 root root   3478680 Dec 19 03:19 mysql-cluster-commercial-management-
server-8.0.33-1.1.el7.x86_64.rpm
-rw-r--r--. 1 root root 364433848 Dec 19 03:19 mysql-cluster-commercial-
server-8.0.33-1.1.el7.x86_64.rpm
-rw-r--r--. 1 root root   2428848 Dec 19 03:19 mysql-connector-j-
commercial-8.0.33-1.1.el7.noarch.rpm
-rw-r--r--. 1 root root   4570200 Dec 19 03:19 mysql-connector-odbc-
commercial-8.0.33-1.1.el7.x86_64.rpm
```

Workaround: When you import the appropriate GPG keys on your ULN mirror, it can download the updated MySQL packages. Proceed as follows:

1. Log in to the ULN mirror server.
2. Download the MySQL GPG keys from these locations:
   - https://repo.mysql.com/RPM-GPG-KEY-mysql-2022.
   - https://repo.mysql.com/RPM-GPG-KEY-mysql-2023.

3. Import the GPG keys.

   ```
   # rpm --import RPM-GPG-KEY-mysql-2022
   # rpm --import RPM-GPG-KEY-mysql-2023
   ```

4. Update the ULN mirror.

   ```
   # /usr/bin/uln-yum-mirror
   ```

   If the key was imported successfully, the new MySQL packages are downloaded to the ULN mirror.

5. For confirmation, verify the signature using one of the new packages.

   ```
   # rpm --checksig mysql-cluster-commercial-management-server-8.0.33-1.1.el7.x86_64.rpm
   mysql-cluster-commercial-management-server-8.0.33-1.1.el7.x86_64.rpm: rsa sha1 (md5)
   pgp md5 OK
   ```

Bug: 36123758

Version: 3.0.2

Uppercase Letters Are Not Supported in Domain Names

Uppercase letters aren't supported in domain names. The domain name for your system is used as the base domain for the internal network, and by Oracle Private Cloud Appliance public facing services. This attribute has a maximum length of 190 characters. Acceptable characters are "a"→"z", "0"→"9", "-"

Bug: 36484125

Version: 3.0.2

Prometheus Backup Archives Are Corrupt

Private Cloud Appliance follows an internal daily backup schedule to preserve system data in case a major outage occurs. The automated backups originally included the Prometheus monitoring data, but its volume caused significant side effects. The amount of data, even when compressed, fills the file system allocated for backups before the 14-day retention period expires. At some point, a failure occurs while building the archive, which results in a corrupt backup. For this reason, Prometheus was removed from the daily backups in appliance software version 3.0.2-b1081557.

Workaround: The monitoring data from Prometheus is not included in automated backups. To preserve your Prometheus data, create a backup and restore it manually. For more information, refer to the note with Doc ID 3021643.1.

Bug: 36623554

Version: 3.0.2

Sauron Ingress Breaks During Install or Upgrade on Host Names with Capital Letters

When upgrading the appliance, the platform upgrade could fail because of the use of capital letters in the host name.

Workaround: Run this command to change captial letters to lowercase letters in all existing copies of the host name, then retry the upgrade.

```
curl -k -X PUT -HHost:api.pca.oracledx.com https://253.255.0.32/v1/uri?
uri=<FQDN in Lowercase> -u admin:<sauron_password>
```

Bug: 36792458

Version: 3.0.2

Upgrader Log Reports Health Check Error in Post-Upgrade Tasks

When upgrading or patching to appliance software version 3.0.2-b1261765, the pca-health-checker script returns an error in post-upgrade tasks due to a missing file system mount: `253.255.12.2:/export/clamav_db`. The Upgrader is not interrupted by the error, and is expected to complete all tasks.

Workaround: This error can be ignored. It has no functional impact.

Bug: 37311137

Version: 3.0.2

Unable to Collect Support Bundles During Appliance Software Upgrade

When upgrading to appliance software version 3.0.2-b1392231, it is temporarily not possible to generate and collect support bundles. Other methods of log collection are not affected.

Workaround: When the upgrade is completed, the support bundle functionality returns to normal. For log collection during the upgrade window, use a timeslice.

Bug: 37828395

Version: 3.0.2

Cannot Add Performance Pool to Local Endpoint

Peer connections between multiple Private Cloud Appliance systems are configured between their local endpoints. The parameters of the local endpoint configuration include the IP addresses of the ZFS pools. However, if a high-performance ZFS pool is created after the local endpoint, the configuration cannot be updated with the new pool IP. The local endpoint must be deleted and re-created with the new parameters. This adversely affects the native Disaster Recovery (DR) Service. Before you can delete the local endpoint, you must also delete all DR configurations.

Workaround: Delete and re-create the local endpoint. If DR configurations exist, those also need to be deleted and created again.

Bug: 37196927

Version: 3.0.2

DR Configurations Unusable After Deleting and Re-creating a Peer Connection on One Appliance

For the native Disaster Recovery (DR) Service, a peer connection between two Private Cloud Appliance systems must be configured from each side of the connection. If the peer connection needs to be deleted on one of the two systems, and is created again, the system reports that peering is complete and fully functional. However, when you execute a DR plan from the existing DR configurations, the operation returns an error, typically containing messages like `Precheck Failed` and `DR metadata project not replicated`.

Workaround: Peer connections are designed to be symmetrical. If you delete and re-create the peer connection on one system, you must delete and re-create it on the second system as well.

Bug: 37260498

Version: 3.0.2

Peering with Unhealthy Storage Controller Results in Replication Action Test Failure

If one of the target Oracle ZFS Storage Appliance controllers is in an unhealthy state when you create a peer connection between two Private Cloud Appliance systems, the peering operation fails. In fact, the target is created but the replication action test fails, causing the peer connection to remain in 'failed' lifecycle state. The error message in the peering logs and progress records looks like this example:

```
Details = Replication target for host <serial>/<IP>/<Pool> failed post-checks.
Post-check failed during replication action test of <Pool>: Failed to create replication
action for <share>.
Reset the peer connection and try again.
  PeerConnectionId = id:ocid1.drpeerconnection.<unique_ID> type:PeerConnection
```

Workaround: The storage controllers on both systems must be in good operating condition before you create a peer connection. Clean up the configuration, ensure that all storage controllers are healthy, and create the peer connection again.

Bug: 37743102

Version: 3.0.2

Deleting Incomplete Peer Connection Prevents Creating a New One

A peer connection between two Private Cloud Appliance systems must be configured symmetrically on both racks. If the configuration on one rack is stuck in *creating* state, and the other rack's configuration becomes *active*, the peering connection cannot be completed. The normal course of action would be to delete the peering configuration on both systems, and create a new peering connection. However, the incomplete configuration cannot be deleted using the normal commands, which implies that new attempts to peer these systems will fail. Testing indicates that this problem occurs when a replication target is registered using an IP address instead of a fully qualified domain name, which suggests a DNS problem at the time of creation.

Workaround: To resolve the incomplete configuration problem and set up peering again between both systems, request support from Oracle. The replication target that was created for the incomplete configuration must be destroyed manually from the ZFS Storage Appliance. The order of operations is as follows:

1. Delete the peer connection from both systems.
2. Manually destroy the replication target that was created for the incomplete configuration. This example shows a target identified by its IP address:

   ```
   TARGET     LABEL                ACTIONS
   target-000 LOCAL-PCA_POOL_HIGH  0
   target-001 LOCAL-PCA_POOL       0
   target-002 192.168.1.43         0
   ```

   Create the peer connection between both systems again.

Bug: 37873134

Version: 3.0.2

Storage Hardware Faults May Not Clear Automatically

When a storage hardware fault occurs that includes `AK-8003-HF` in the fault code, the automatic clearing of these faults may not work properly due to a database mismatch between fault codes.

Workaround: Using PCA 3.0 Service Advisor, look at the health of the Storage Appliance to ensure the faults are resolved. If the faults are resolved on the Storage Appliance, but the fault codes are still present in the software healthchecker, you can manually clear the faults using the `clearFault id=$faultid` command.

```
PCA-ADMIN> list fault where status EQ ACTIVE
Command: list fault where status EQ ACTIVE
Status: Success
Time: 2025-05-28 12:27:31,527 UTC
Data:
  id
Name                                        Status   Severity
  --
----                                        ------   --------
  08bec50b-00b8-48df-99bb-fc31cb839e03   sn02AK00684129--AK-8003-HF--
vnic7           Active   Major
  7f7baee8-033d-4912-a759-c31c646bb30d   sn01AK00684129--AK-8003-F9--PCIe 7/
NET0     Active   Minor
  6357a915-bae9-463e-a619-8abf10c59751   sn02AK00684129--AK-8003-F9--PCIe 7/
NET0     Active   Minor
  f2370a63-4dda-470b-98ad-e7f63bf36702   sn02AK00684129--AK-8003-F9--PCIe 7/
NET1     Active   Minor
  06a377c6-2283-c11c-ad4b-90a861380b0f   sn02AK00684129--SPINTEL-8006-CE--
DIMM 0/2   Active   Minor
  e4520a8a-32e1-422f-ac9b-989459aab000   sn02AK00684129--AK-8003-HF--
aggr2           Active   Major
  ff96bce2-4ef5-43f5-9791-e9b4c64e35e8   sn02AK00684129--AK-8003-HF--
vnic8           Active   Major
  3a2f6f38-a062-4205-940f-cda0fc1b19fc   sn01AK00684129--AK-8003-F9--PCIe 7/
NET1     Active   Minor
PCA-ADMIN> show fault id=08bec50b-00b8-48df-99bb-fc31cb839e03
Command: show fault id=08bec50b-00b8-48df-99bb-fc31cb839e03
Status: Success
```

```
Time: 2025-05-28 12:27:36,373 UTC
Data:
  Id = 08bec50b-00b8-48df-99bb-fc31cb839e03
  Type = Fault
  Category = Internal
  Severity = Major
  Status = Active
  Last Update Time = 2025-05-27 14:57:24,752 UTC
  Cause = Network connectivity via datalink vnic7 has been lost.
  Message Id = AK-8003-HF
  Time Reported = 2025-05-27 14:56:52,000 UTC
  Action = Check the networking cable, switch port, and switch
configuration.  Contact your vendor for support if the datalink remains
inexplicably failed. Please refer to the associated reference document at
http://support.oracle.com/msg/AK-8003-HF for the latest service procedures
and policies regarding this diagnosis.
  Health Exporter = zfssa-analytics-exportersn02AK00684129
  Uuid = 60e580ca-f410-41f7-a10e-e9f68d8a442c
  Diagnosing Source = zfssa_analytics_exporter
  Upgrade Fault = True
  Faulted Component Type = HARDWARE
  ASR Notification Time = 2025-05-27 14:57:24,748 UTC
  Last Occurrence Activation Time = 2025-05-27 14:57:24,739 UTC
  Last Occurrence Clearing Time = 2025-05-26 11:33:25,611 UTC
  FaultHistoryLogIds 1 = id:a2a2a5f5-13e9-4e7c-bd1f-b09a32de8e36
type:FaultHistoryLog  name:
  FaultHistoryLogIds 2 = id:1f814f6f-24d3-48d3-b289-76d03a8841a5
type:FaultHistoryLog  name:
  FaultHistoryLogIds 3 = id:07ef95a5-fef0-4143-ac02-a1437dfb494d
type:FaultHistoryLog  name:
  BaseManagedObjectId = id:Unknown/vnic7/Unknown  type:HardwareComponent
name:
  Description = Network connectivity via datalink vnic7 has been lost.
  Name = sn02AK00684129--AK-8003-HF--vnic7
  Work State = Normal
PCA-ADMIN> clearFault id=08bec50b-00b8-48df-99bb-fc31cb839e03
Command: clearFault id=08bec50b-00b8-48df-99bb-fc31cb839e03
Status: Success
Time: 2025-05-28 12:27:59,397 UTC
Data:
  status = Success
PCA-ADMIN> list fault where status EQ ACTIVE
Command: list fault where status EQ ACTIVE
Status: Success
Time: 2025-05-28 12:28:04,790 UTC
Data:
  id
Name                                        Status   Severity
  --
----                                        ------   --------
  7f7baee8-033d-4912-a759-c31c646bb30d   sn01AK00684129--AK-8003-F9--PCIe 7/
NET0     Active   Minor
  6357a915-bae9-463e-a619-8abf10c59751   sn02AK00684129--AK-8003-F9--PCIe 7/
NET0     Active   Minor
  f2370a63-4dda-470b-98ad-e7f63bf36702   sn02AK00684129--AK-8003-F9--PCIe 7/
NET1     Active   Minor
```

```
  06a377c6-2283-c11c-ad4b-90a861380b0f   sn02AK00684129--SPINTEL-8006-CE--
DIMM 0/2   Active   Minor
  e4520a8a-32e1-422f-ac9b-989459aab000   sn02AK00684129--AK-8003-HF--
aggr2           Active   Major
  ff96bce2-4ef5-43f5-9791-e9b4c64e35e8   sn02AK00684129--AK-8003-HF--
vnic8           Active   Major
  3a2f6f38-a062-4205-940f-cda0fc1b19fc   sn01AK00684129--AK-8003-F9--PCIe 7/
NET1     Active   Minor
PCA-ADMIN>
```

Bug: 37999786

Version: 3.0.2

Faults AK-8003-F9--PCIe 7/NET0 | NET1 Reported on Fresh Installed Rack

For Private Cloud Appliance systems that are newly install with software build 3.0.2-b1261765, it is possible that during the first bring up of the system you might see faults similar to these:

```
      311275ec-5077-4dba-a5eb-8085df4a855d   sn02AK00684129--AK-8003-F9--PCIe
7/NET0         Active   Minor
      efb1b954-d7bc-4a00-bc8c-c7076caad192   sn02AK00684129--AK-8003-F9--PCIe
7/NET1         Active   Minor
      afa421be-193a-4124-8585-9d742c4e1c57   sn01AK00684129--AK-8003-F9--PCIe
7/NET1         Active   Minor
```

Workaround: These faults can be ignored and will clear automatically.

Bug: 37846460

Version: 3.0.2

Role Reversal Precheck Fails During DR Switchover

When executing a DR switchover plan, and the plan fails with the error `role_reversal_precheck job has failed`, this error is likely caused by a timeout.

Workaround: Rerun the switchover command.

Bug: 38068506

Version: 3.0.2

After Deleting a Peer Connection on One Appliance, Peered System Reports Active Connection

A peer connection between two Private Cloud Appliance systems must be configured from each side of the connection. If the peer connection is deleted on one of the systems, the other system continues to report that peering is active. This is not correct, but the systems are unable to track the configuration state on the remote side of the connection.

Workaround: Peer connections are designed to be symmetrical. If you delete the peer connection on one system, it must be deleted on the other system as well.

Bug: 37262830

Version: 3.0.2

Adding Instances to a DR Configuration During DR Operation Causes Failure

Administrators must not modify the compute instances included in any DR configuration while a DR operation is in progress. Especially the combination of executing a (switchover) DR plan and adding compute instances to a DR configuration with the `all=True` option is highly likely to cause errors. The execution of a DR plan might be interrupted, conflicts between DR configurations might occur, and the ZFS Storage Appliance might become overloaded and stop accepting incoming requests.

Workaround: When adding compute instances to a DR configuration, or modifying DR configurations in general, ensure that no DR plan execution is in progress. Before executing a DR plan, ensure that there are no ongoing updates to the instances list of a DR configuration. Note that adding many compute instances in a single operation, such as with the `all=True` option, result in a long-running job. Ensure that no such job is still in progress. It is also recommended to add no more than 100 compute instances to a single DR configuration.

Bug: 37299009

Version: 3.0.2

Failure Creating Peer Connection If One System Does Not Expose High-Performance Storage Pool

A peer connection between two Oracle Private Cloud Appliance systems requires a local endpoint to be configured on each side. For the native Disaster Recovery (DR) service, the local endpoint configuration must include the IP address of each storage pool. If your systems have an optional high-performance pool, but you do not include its interface in the local endpoint configuration on one of the systems, then the peer connection cannot be created. An error is returned, indicating the replication target for the high-performance pool cannot be created.

Workaround: If you are peering two systems that contain a high-performance ZFS storage pool, ensure that an IP address is allocated on each system, and expose it through their respective local endpoint configuration. Include both parameters: `zfsCapacityPoolEndpointIp` and `zfsPerformancePoolEndpointIp`.

Bug: 37316895

Version: 3.0.2

User Interface Issues

This section describes known issues and workarounds related to the graphical user interface.

Moving Resources Between Compartments Is Not Supported in the Compute Web UI

The Compute Web UI does not provide any function to move a resource from one compartment to another. Operations to change the compartment where a cloud resource resides, can only be performed through the CLI. However, note that not all resource types support compartment changes. For example, none of the network resources can be moved.

Workaround: If you need to move a resource from its current compartment to another compartment, use the CLI. After successfully executing the CLI command, you can see the resulting changes in the Compute Web UI.

Bug: 33038606

Version: 3.0.1

Saving Resource Properties Without Modifications Briefly Changes Status to Provisioning

If you open the Edit dialog box in the Compute Web UI to modify the properties of a resource, and you click Save Changes without actually modifying any of the properties, the status of the resource does change to *Provisioning* for a few seconds. This is the normal response of the UI to a user clicking the Save button. It has no adverse effect.

Workaround: To prevent the resource status from changing to *Provisioning* if you have not made any changes to it, click the Cancel button in the dialog box instead.

Bug: 33445209

Version: 3.0.1

NFS Export Squash ID Not Displayed

In the Compute Web UI, the detail page of an NFS export does not display the squash ID in the NFS export options. The squash ID is required for anonymous access to the NFS export, but you can only retrieve it by editing the export options.

Workaround: To obtain an NFS export squash ID, go to the NFS Export detail page, scroll down to the NFS Export Options, and click Edit Options. Alternatively, look up the export options through the CLI.

Bug: 33480572

Version: 3.0.1

Scrollbars Not Visible in Browser

The browser-based interfaces of Private Cloud Appliance are built with Oracle JavaScript Extension Toolkit(JET) and follow Oracle's corporate design guidelines. Scrollbars are meant to remain hidden as long as you are not actively using the part of the screen where content does not fit within the space provided – for example: large tables, long drop-down lists, and so on. Not all browsers or browser versions display scrollbars in the intended way. For example, Google Chrome typically hides the scrollbars as intended while Mozilla Firefox does not hide them at all.

Workaround: The behavior of the scrollbars is by design. It applies to both the Compute Web UI and Service Web UI. In areas where content runs beyond the allocated screen area, scrollbars appear automatically where appropriate when the cursor is placed over the content in question.

Bug: 33489195

Version: 3.0.1

Authorization Failure When Retrieving Compartment Data

The Identity and Access Management service allows you to control users' access permissions to resources in a fine-grained way through policies. Those policies determine which operations a group of users is authorized to perform on resources of a particular type or residing in a particular compartment. In certain situations, the Compute Web UI is unable to hide all the resources that a user has no access to. Consequently, a user operation may result in a request for data the account is not authorized to access.

While using the Compute Web UI you may run into authorization failures in case your operation triggers an attempt to retrieve data that you have no permission for. In this situation an error appears in your browser, indicating that the application has stopped working due to account permissions. The compartment tree, in particular, is prone to this type of failure because it can display compartments that you are not allowed to access.

Workaround: When the error is caused by a compartment tree access issue, it is likely that the intended page is displayed when you click Try Again. Otherwise, contact your tenancy administrator to request additional permissions to access the required data.

Bug: 33497526, 33520207

Version: 3.0.1

Object List Is Not Updated Automatically

In the Compute Web UI you display the objects stored in a bucket by browsing through its directory structure. The list or table of objects is not automatically refreshed at regular intervals, so any object changes will only become visible when you refresh the page manually. There is no available function for the UI to poll the status of a bucket.

Workaround: To display the current list of objects in the Compute Web UI, refresh the page manually. This behavior is not specific to the object storage service; it may occur in other areas of the UI as well. If a resource list is not updated automatically at regular intervals, you should refresh it manually.

Bug: 33519215

Version: 3.0.1

Not All Resources Shown in Drop-Down List

When you need to use a drop-down list to select a resource, you may notice that not all items are shown if the list is very long. As you scroll through the list, more items are loaded, yet you may still be unable to find the item you are looking for. The reason for this behavior is that UI components are designed to respond quickly rather than slowing down the user due to long load times. You are encouraged to filter a long list by typing part of a resource name in the text field, instead of scrolling through a complete alphabetical list. This is characteristic of Oracle JavaScript Extension Toolkit, so it affects both the Compute Web UI and the Service Web UI

Workaround: Scrolling is not the preferred way to search for an item in a long drop-down list. Instead, start typing the name of the resource you are looking for, and the available list items will be reduced to those matching what you type.

Bug: 33583708

Version: 3.0.1

When Canceling a Delete Operation from a Resource Detail Page, the Resource List Page Is Displayed

In the Compute Web UI, many resource detail pages contain a Delete button in the top-right corner. When you click it, a pop-up window prompts you to confirm the delete operation, or cancel it. If you click Cancel, the browser might not return to the individual resource detail page, but instead displays the page that lists all the resources of that type in the selected compartment. Examples of resource types for which this behavior occurs, include: identity provider, file system snapshot, image.

Workaround: Go to the individual resource detail page by clicking that resource in the table.

Bug: 36897293

Version: 3.0.2

Volume Group Can Be Created Without Name

When you create a volume group in the Block Storage area of the Compute Web UI, you are not required to enter a name. If you leave the name field blank, the volume group appears in the list as *Unnamed Item*. However, if you do not provide a name when creating a volume group in the CLI, a name is automatically assigned based on the time of creation.

Workaround: This is not a code bug: the name is technically not a required parameter. To avoid having volume groups with meaningless names, make sure you provide an appropriate name at the time of creation, in the Compute Web UI as well as the CLI. If you accidentally created the volume group without specifying a name, you can edit the volume group afterwards and add the name of your choice.

Bug: 33608462

Version: 3.0.1

File Systems and Mount Targets Not Displayed

When users have access to the resources in a particular compartment, but have no permission to view the content of the root compartment of the tenancy, the Compute Web UI might not display the resources that a user is allowed to list. Instead, an authorization error is displayed. For the file system service specifically, file systems or mount targets in a particular compartment are not displayed, even if the user has full access to that compartment and the resources it contains.

This behavior is caused by the way the API request is made from the UI, using the OCID of the root compartment. In contrast, the CLI requires that you specify the OCID of the compartment that effectively contains the requested resources, so it is not affected by the same authorization issue as the UI.

Workaround: The tenancy administrator should ensure that users of the file system service have read access to the root compartment. Users who cannot list the file systems and mount targets they are authorized to use, should ask their tenancy administrator to verify their account permissions and make the necessary adjustments.

Bug: 33666365

Version: 3.0.1

Optional ICMP Security Rule Parameters Cannot Be Removed

When you add an ingress or egress security rule to the security list of a VCN, you can specifically select the ICMP protocol. The Compute Web UI indicates that selecting a *Parameter Type* and *Parameter Code* from the respective lists is optional. This is incorrect, because the Parameter Type is mandatory for ICMP rules.

If you specified both Type and Code in your ICMP rule, it is possible to remove the Parameter Code. Edit the security rule, place your cursor in the Code text field, and delete its content. This is how drop-down lists work in the UI; there is no *"empty"* option to select.

Workaround: When working with ICMP security rules, always specify the *Parameter Type*. To remove an optional parameter selected from a drop-down list, select and delete the content of the text field.

Bug: 33631794

Version: 3.0.1

Optional Route Rule Description Changes to Mandatory Field

In the Compute Web UI, you manage route rules in the Resources section of the route table detail page. When you click Add Route Rules, the Create Route Table Rule window is displayed. It includes an optional field to enter a description for the new route rule. However, if you decide to enter a description, it becomes a required field, but your entry is automatically removed. As a result, you can no longer save the new route rule.

Workaround: Click Cancel to close the Create Route Table Rule window and start over. Create route rules from the UI without entering a description.

Bug: 36897293

Version: 3.0.2

Compartment Selector Not Available When Creating DHCP Options

When you create or modify DHCP options for a VCN through the Compute Web UI, there is no way to add the DHCP options to another compartment. Because the compartment selector is not available in the create and edit windows, the DHCP options are implicitly stored in the same compartment as the VCN itself. However, it is supported to store DHCP options in another compartment. If you wish to do so, please use the CLI.

Workaround: If you want DHCP options to be stored in a different compartment than the VCN they apply to, create the DHCP options through the CLI, or use the CLI to move them to the desired compartment.

Bug: 33722013

Version: 3.0.1

Fix available: Please apply the latest patches to your system.

DHCP Options Error Message for Custom Search Domain Is Misleading

The Networking service allows you to control certain instance boot configuration parameters by setting DHCP options at the level of the VCN and subnet. One of the DHCP options you can control is the search domain, which is appended automatically to the instance FQDN in a DNS-enabled VCN and subnet.

The search domain must be specified in the format `example.tld` – where TLD stands for top-level domain. However, the Compute Web UI does not validate this parameter; this is done by the Networking service when you save the DHCP options. The Compute Web UI checks that the value contains no spaces. If it does, an error message appears under the Search Domain field: *"Must be in the format of example.tld"*. This is technically inaccurate as it merely indicates the value contains a space.

Workaround: Enter a custom search domain in the required format: `example.tld`. Spaces are not allowed in domain names. If the error message in question appears, correct the value you entered in the Search Domain field and try to save the DHCP options again.

Bug: 33753758

Version: 3.0.1

No Details Displayed for File System Cloned from Snapshot

When you create a file system, all relevant information about the file system is displayed in the Compute Web UI detail page. It contains practically the same information as the output from the OCI CLI command `oci fs file-system get`. However, when you clone a file system snapshot through the OCI CLI, to use as a new file system, the detail page of the clone file system does not provide the same data. Relevant missing fields include Source Snapshot, Parent File System, Clone Root, Hydration, etc.

Workaround: Use the OCI CLI instead if you need those details. The CLI displays all the data fields for a clone-based file system.

Bug: 34566735

Version: 3.0.2

Unable to Display Details of Instance Backup

When you create a backup of an instance, it is stored in an object storage bucket. When the backup operation has completed, and you try to view the details of the backup object, the system may return an HTTP 404 error.

Workaround: Manually reload the browser page. The backup details should be displayed. Additional error messages might appear in a pop-up but those can be ignored.

Bug: 34777856

Version: 3.0.2

IP Address List on VNIC Detail Page Not Updated

In the Compute Web UI you can manage the IP addresses assigned to a compute instance from the detail pages of the instance's attached VNICs. In the IP Addresses table in the Resources section of the VNIC detail page you can add and remove private and public IPs. However, the Reserve Public IP pop-up window is not always rendered correctly, and changes applied there are not displayed in the VNIC IP Address table.

Workaround: No workaround is available.

Bug: 34797160

Version: 3.0.2

No Error Displayed When Attempting to Reserve Public IP Address While All Public IPs In Use

In the Compute Web UI, when you try to reserve a public IP address when no more public IPs are available from the pool, no error message is displayed. The Reserve Public IP window hangs, but provides no feedback about the operation you are attempting. Since no IPs are available to reserve, the operation does not complete.

Workaround: Close the Reserve Public IP window or reload the browser interface page. An administrator needs to expand the public IP pool for the Private Cloud Appliance environment before you can reserve another public IP address.

Bug: 34832457

Version: 3.0.2

When Modifying Listener of Load Balancer, Existing Configuration Parameters Are Ignored

When you use the Compute Web UI to modify a listener configuration of a load balancer, several parameters are not preserved in the Edit Listener window. Although you are changing the configuration of an existing listener, certain parameters are replaced with default values, forcing you to enter and verify all the parameters again.

As an example, let's assume your load balancer has a listener configured for HTTPS at port 8443, with an SSL certificate and cipher suite set up. When you edit this listener through the UI, the protocol appears as HTTP and the SSL configuration is not shown. Next, when you select the already configured HTTPS protocol again, the custom port, TLS version and cipher suite are reverted to their default values instead of the currently configured parameters.

Parameters that are not preserved in the Edit Listener window: protocol other than HTTP, custom port number, SSL settings (TLS version and cipher suite). Other parameters are not reverted: backend set, host names, path route set, idle timeout.

Workaround: If you modify a listener configuration through the Compute Web UI, always ensure that you have selected the right protocol first. Then set all listener parameters as if you were creating it from scratch, without moving back and forth between the policy options in the UI. Alternatively, modify the listener configuration using the OCI CLI.

Bug: 36032894

Version: 3.0.2

Create Backend to Add Security List/Configure Automatically Using IP Address Does Not Display Egress/Ingress Lists

If you use the following method in the Compute Web UI to create backend servers to a backend set of a load balancer, the egress and ingress security lists/rules are not displayed:

Select IP Address under the Backend Servers section, enter the backend server IP address, and then select Configure Automatically under the Security Rules section.

Workaround: Create the backend servers using one of these other methods:

- Select Computed Instances under the Backend Servers section when creating the backend, and select security rules Configure Automatically.
- Select IP Address under the Backend Servers section when creating the backend, and select security rules Configure Manually. Then, manually add the ingress and egress security list rules to the security lists attached to the corresponding subnet.

Bug: 35570701

Version: 3.0.2

Tag Area Above Resource Tables Does Not Expand

Resource pages in the UI display a table listing resources of a particular type. Just above the table you find control options to auto-reload the page, refresh the resource table, and filter the entries displayed. When filtering by tag, you can select multiple tags for your filter. However, the space available to show the filter tags does not expand, which causes elements of the UI to overlap as more tags are added.

Workaround: There is no workaround. Only the first few tags used for filtering are displayed while additional tags are hidden behind other UI elements.

Bug: 35975108

Version: 3.0.2

Compartment Selection in Resource Page Heading Does Not Meet Accessibility Requirements

In the Compute Web UI, lists or tables of resources are typically displayed on pages with a compartment selection drop-down in the page heading. Using keyboard navigation, when the compartment selection drop-down is highlighted, you press enter to activate it. Next, use the tab key to switch between the Search/Filter box and the listed Compartments, and the arrow keys to progress through the list items. To confirm your compartment selection, press enter.

This behavior is not detected by screen readers, and no messages are displayed to assist the user.

Workaround: Use the compartment selection drop-down as described.

Bug: 36700904

Version: 3.0.2

Boot Volume Backup Not Created In Selected Compartment

When creating a backup of a boot volume, the Compute Web UI allows you to select the target compartment where the backup should be stored. The compartment selection is not taken into account. The backup is created in the same compartment as the original volume.

Workaround: Ignore the compartment selection option when creating a boot volume backup.

Bug: 36750297

Version: 3.0.2

Low Privileged User Cannot View Their Groups

When a low privileged user navigates to their profile page in the Compute Web UI, it is possible that they cannot see the groups to which they belong.

Workaround: Contact the tenancy administrator to find the name of the groups to which the user is assigned.

Bug: 36779893

Version: 3.0.2

Unable to Set the Oracle ASN Value to the Default Value in the Service Web UI

If you do not set a value for the Oracle ASN, the system assumes the default value: 136025. However, if you try to type in the default value for the Oracle ASN using the Service Web UI, you will get an error saying that value is not in the allowed range.

Workaround: If you want the default Oracle ASN value, leave the field blank in the Service Web UI, and the system will automatically assign the default value. Or, you can use the CLI to set the Oracle ASN default value.

Bug: 36788619

Version: 3.0.2

Display Issues With the Compute Web UI When Using Firefox Browser 115 ESR

In release 3.0.2-b1185392 Private Cloud Appliance updated the console themes to reflect the Oracle Redwood branding common in Oracle Cloud. If you use Firefox browser version 115 ESR, rendering issues may occur which make the web console difficult to read.

Workaround: Upgrade your Firefox browser to a newer version, or use a different browser.

Bug: 36983636

Version: 3.0.2

Unable to Add Multiple Instances to a DR Configuration Using Service Web UI

When adding compute instances to a DR configuration, the Service Web UI requires that you add them one by one. It offers no options to include multiple instances in one operation.

Workaround: If you have many compute instances to add to a DR configuration, consider using the Service CLI, which allows you to add all instances in one or more compartments, or even in all mapped compartments.

Bug: 37174928

Version: 3.0.2

Networking Issues

This section describes known issues and workarounds related to all aspects of the appliance networking, meaning the system's internal connectivity, the external uplinks to the data center, and the virtual networking for users' compute instances.

Possible Impact to BGP Links After Upgrading to 3.0.2-b1081557 or Higher

When running BGP in a Mesh configuration, you may experience a situation where BGP links show an IDLE state or never connected, when upgrading to 3.0.2-b1010555 or later. If you are using BGP in a Mesh configuration and are currently running a release prior to 3.0.2-b1010555 then contact Oracle support, who can assist in updating and correcting your uplink configuration prior to upgrade. If an upgrade to 3.0.2-b1010555 or later has already been performed and you see BGP link state as IDLE then contact Oracle support who can also assist, post upgrade.

Bug: 36525352

Version: 3.0.2

DNS Zone Scope Cannot Be Set

When creating or updating a DNS zone, scope cannot be set. In command line output, the value of the `scope` property is `null`.

Bug: 32998565

Version: 3.0.1

To Update a DNS Record the Command Must Include Existing Protected Records

When updating a DNS record, it is expected that you include all existing protected records in the update command even if your update does not affect those. This requirement is intended to prevent the existing protected records from being inadvertently deleted. However, the checks are so restrictive with regard to SOA records that certain updates are difficult to achieve.

Workaround: It is possible to update existing records by either providing the SOA record as part of the command, or by setting the domain to not include the SOA domain. In practice, most record updates occur at a higher level and are not affected by these restrictions.

Bug: 33089111

Version: 3.0.1

Fix available: Please apply the latest patches to your system.

Create Route Table Fails With Confusing Error Message

When you create a route table, but make a mistake in the route rule parameters, the API server may return an error message that is misleading. That specific message reads: "*Route table target should be one of LPG, NAT gateway, Internet gateway, DRG attachment or Service gateway.*" In that list of possible targets, DRG attachment is not correct. The dynamic routing gateway itself should be specified as a target, not its DRG attachment.

Workaround: Ignore the error message in question. When configuring route rules to send traffic through a dynamic routing gateway, specify the DRG as the target.

Bug: 33570320

Version: 3.0.1

Networking Service Not Responding While Within Resource Limits

The configuration limits for networking resources, when running appliance software version 3.0.2-b1185392 or earlier, allow setups that exceed the capabilities of the Networking Service architecture. In particular, the theoretical combination of maximum 80 VCNs and 40 subnets each, generates considerably more data flows than the underlay network can manage.

Consequently, even though your configuration is within the resource limits, the Networking Service might show signs of excessive load. Its service pods might run out of memory and crash, causing internal server errors when performing networking operations, even when requesting a list of resources.

Workaround: The internal server errors are transient, and the Networking Service is expected to resume normal operation. If this problem persists, ask Oracle for assistance.

To avoid the issue, stay within the updated resource limits documented in the release notes chapter Service Limits. These stricter limits are enforced by the appliance software as of version 3.0.2-b1261765.

Bug: 36906198

Version: 3.0.2

File Storage Traffic Blocked By Security Rules

To allow users to mount file systems on their instances, security rules must be configured in addition to those in the default security list, in order to allow the necessary network traffic between mount targets and instances. Configuring file storage ports and protocols in Oracle Private Cloud Appliance is further complicated by the underlay network architecture, which can block file storage traffic unexpectedly unless the source and destination of security rules are set up in a very specific way.

Scenario A – If the mount target and instances using the file system service reside in the same subnet, create a security list and attach it to the subnet in addition to the default security list. The new security list must contain the following stateful rules:

```
+++ Ingress Rules ++++++++++++++++++++

Source            Protocol     Source Ports            Destination Ports
------            --------     ------------            -----------------
<subnet CIDR>     TCP          All                     111, 389, 445, 4045,
                                                       2048-2050, 20048
<subnet CIDR>     UDP          All                     111, 289, 445, 2048,
                                                       4045, 20048

+++ Egress Rules ++++++++++++++++++++

Destination       Protocol     Source Ports            Destination Ports
-----------       --------     ------------            -----------------
<subnet CIDR>     TCP          111, 389, 445, 4045,    All
                               2048-2050, 20048
<subnet CIDR>     TCP          All                     111, 389, 445, 4045,
                                                       2048-2050, 20048
```

```
<subnet CIDR>      UDP          111, 389, 445,          All
                                4045, 20048
<subnet CIDR>      UDP          All                     111, 389, 445,
                                                        4045, 20048
```

Scenario B – If the mount target and instances using the file system service reside in different subnets, create a new security list for each subnet, and attach them to the respective subnet in addition to the default security list.

The new security list for the subnet containing the mount target must contain the following stateful rules:

```
+++ Ingress Rules ++++++++++++++++++++

Source                        Protocol     Source Ports            Destination Ports
------                        --------     ------------            -----------------
<instances subnet CIDR>       TCP          All                     111, 389, 445, 4045,
                                                                   2048-2050, 20048
<instances subnet CIDR>       UDP          All                     111, 289, 445, 2048,
                                                                   4045, 20048

+++ Egress Rules ++++++++++++++++++++

Destination                   Protocol     Source Ports            Destination Ports
-----------                   --------     ------------            -----------------
<instances subnet CIDR>       TCP          111, 389, 445, 4045,    All
                                           2048-2050, 20048
<instances subnet CIDR>       UDP          111, 389, 445,          All
                                           4045, 20048
```

The new security list for the subnet containing the instances using the file system service must contain the following stateful rules:

```
+++ Ingress Rules ++++++++++++++++++++

Source                        Protocol     Source Ports            Destination Ports
------                        --------     ------------            -----------------
<mount target subnet CIDR>    TCP          111, 389, 445, 4045,    All
                                           2048-2050, 20048
<mount target subnet CIDR>    UDP          111, 289, 445, 2048,    All
                                           4045, 20048

+++ Egress Rules ++++++++++++++++++++

Destination                   Protocol     Source Ports            Destination Ports
-----------                   --------     ------------            -----------------
<mount target subnet CIDR>    TCP          All                     111, 389, 445, 4045,
                                                                   2048-2050, 20048
<mount target subnet CIDR>    UDP          All                     111, 389, 445,
                                                                   4045, 20048
```

Workaround: Follow the guidelines provided here to configure ingress and egress rules that enable file system service traffic. If the unmodified default security list is already attached, the proposed egress rules do not need to be added, because there already is a default stateful security rule that allows all egress traffic (destination: 0.0.0.0/0, protocol: all).

Bug: 33680750

Version: 3.0.1

Stateful and Stateless Security Rules Cannot Be Combined

The appliance allows you to configure a combination of stateful and stateless security rules in your tenancy. The access control lists generated from those security rules are correct, but may cause a wrong interpretation in the virtual underlay network. As a result, certain traffic may be blocked or allowed inadvertently. Therefore, it is recommended to use either stateful or stateless security rules.

Workaround: This behavior is expected; it is not considered a bug. Whenever possible, create security rules that are either all stateful or all stateless.

> ⓘ **Note**
>
> If you have a specific need, you can have stateful and stateless rules combined, but if you use stateless rules they must be symmetrical, meaning you cannot have a stateless egress rule, and a stateful ingress rule for the same flow.

Bug: 33744232

Version: 3.0.1

Routing Failure With Public IPs Configured as CIDR During System Initialization

When you complete the initial setup procedure on the appliance (see "Complete the Initial Setup" in the chapter Configuring Oracle Private Cloud Appliance of the Oracle Private Cloud Appliance Installation Guide), one of the final steps is to define the data center IP addresses that will be assigned as public IPs to your cloud resources. If you selected BGP-based dynamic routing, the public IPs may not be advertised correctly when defined as one or more CIDRs, and thus may not be reachable from outside the appliance.

Workaround: To ensure that your cloud resources' public IPs can be reached from outside the appliance, specify all IP addresses individually with a /32 netmask. For example, instead of entering 192.168.100.0/24, submit a comma-separated list: 192.168.100.1/32,192.168.100.2/32,192.168.100.3/32,192.168.100.4/32, and so on.

Bug: 33765256

Version: 3.0.1

Fix available: Please apply the latest patches to your system.

Admin Network Cannot Be Used for Service Web UI Access

The purpose of the (optional) Administration network is to provide system administrators separate access to the Service Web UI. The current implementation of the Administration network is incomplete and cannot provide the correct access.

Workaround: None available. At this point, *do not* configure the Admin Network during initial configuration.

Bug: 34087174, 34038203

Version: 3.0.1

Network Configuration Fails During Initial Installation Procedure

After physical installation of the appliance rack, the system must be initialized and integrated into your data center environment before it is ready for use. This procedure is documented in the chapter titled "Configuring Oracle Private Cloud Appliance" of the Oracle Private Cloud Appliance Installation Guide. If the network configuration part of this procedure fails – for example due to issues with message transport or service pods, or errors returned by the switches – there are locks in place that need to be rolled back manually before the operation can be retried.

Workaround: None available. Please contact Oracle for assistance.

If possible, confirm the state of the network configuration from the Service CLI.

```
PCA-ADMIN> show
networkConfig

Data:
[...]
  Network Config Lifecycle State = FAILED
```

Bug: 34788596

Version: 3.0.2

External Certificates Not Allowed

At this time, Oracle Private Cloud Appliance does not allow the use of external CA-signed certificates.

Workaround: Please contact Oracle support for a workaround.

Bug: 33025681

Version: 3.0.2

DNS Entries on Oracle Linux 8 Instances Incorrect After Upgrade to Release 3.0.2

After the appliance software is upgrade to Release 3.0.2, the name resolution settings in the compute instance operating system are not automatically updated. Up-to-date network parameters are obtained when the instance's DHCP leases are renewed. Until then, due to the way Oracle Linux 8 responds to DNS server messages, it can fail to resolve short host names although queries with FQDNs are successful. Oracle Linux 7 instances are not affected by this issue.

Workaround: Restart the DHCP client service (`dhclient`) on the command line of your Oracle Linux 8 instances. Rebooting the instance also resolves the issue.

Bug: 34918899

Version: 3.0.2

Network Load Balancer Does Not Report Detailed Backend Health Status

Users of Oracle Cloud Infrastructure might be familiar with the detailed health statuses it provides for backend servers of network load balancers. In case a backend server is not entirely healthy, the health check status provides an indication of the problem, for example: connection failure, time-out, regex mismatch, I/O error, invalid status code. Due to the specific load balancer implementation in Oracle Private Cloud Appliance, the Network Load Balancer service can only report whether a backend server is healthy (`OK`) or unhealthy (`CRITICAL`).

Workaround: There is no workaround. Backend health checks cannot provide extra status information.

Bug: 35993214

Version: 3.0.2

Load Balancer Backend Health Check Configuration Locked Due to Unsupported Character

On systems running appliance software version 3.0.2-b1325160 or earlier, a load balancer can be configured to parse regular expressions (regex) in health status responses sent by the backend servers. When configuring the `response-body-regex` parameter, it is possible to include the forward slash (`'/'`) escape character. However, this character leads to an invalid json configuration file, which prevents you from making further configuration changes, or removing the invalid character.

This issue also blocks the appliance software upgrade to version 3.0.2-b1392231.

Workaround: Do not use the forward slash (`'/'`) escape character in a response body regex. Otherwise, the entire load balancer setup will need to be deleted.

Bug: 37795379

Version: 3.0.2

Load Balancer Functional Changes After Appliance Software Upgrade

With version 3.0.2-b1392231 of the Private Cloud Appliance software, load balancers are migrated to a new background implementation. As a result, a few features are either different or no longer available. An existing configuration that is no longer supported in the new implementation, can have a negative impact on the appliance software upgrade.

Response body regex parsing
If you have a load balancer configured with regular expression (regex) parsing of backend responses for health status information, that will no longer work after the upgrade. Health status reporting is limited to response codes.
Workaround: Before upgrading the appliance software to version 3.0.2-b1392231, unconfigure the optional regex setting (`--response-body-regex`) for the response from the backend servers.
Bug: 37629014

Cipher suites
In the new load balancer implementation, weaker cipher suites have been removed. Going forward, SSL/TLS connections can be secured with these cipher suites:

```
AES128-GCM-SHA256, AES256-GCM-SHA384,
ECDHE-ECDSA-AES128-GCM-SHA256, ECDHE-ECDSA-AES256-GCM-SHA384,
ECDHE-RSA-AES128-GCM-SHA256, ECDHE-RSA-AES256-GCM-SHA384,
AES128-SHA, AES256-SHA, DES-CBC3-SHA,
ECDHE-ECDSA-AES128-SHA, ECDHE-ECDSA-AES256-SHA,
ECDHE-RSA-AES128-SHA, ECDHE-RSA-AES256-SHA,
PSK-AES128-CBC-SHA, PSK-AES256-CBC-SHA
```

Workaround: Before upgrading the appliance software to version 3.0.2-b1392231, ensure that cipher suites are used that remain available after upgrade. If necessary, change the existing load balancer configurations.
Bug: 37461876

Cookie-based session persistence
For existing load balancers, session persistence between clients and backend servers can be enabled using either application cookies or load balancer cookies. These are no longer supported after upgrade.
Workaround: Before upgrading the appliance software to version 3.0.2-b1392231, unconfigure cookie-based session persistence. Alternatively, load balancer cookies can be preserved on condition that the load balancing policy is set to IP hash before upgrade.
Bug: 37473362

Server order preference
The SSL parameter to prioritize server ciphers over client ciphers is not supported.

Connectivity to All Instances Lost after Appliance Upgrade

In large multitenant network configurations using BGP (Border Gateway Protocol) with layer 3 virtualization, route leaking allows routes to be shared in a controlled way between routing tables that are otherwise isolated through virtual routing and forwarding (VRF). However, after upgrading to appliance software version 3.0.2-b1261765, the number of routes that can be leaked between VRFs is restricted to 1000. If the existing route map before the upgrade is larger, certain routes are dropped and connectivity is lost. For example, traffic to and from compute instances might be blocked because the required routes are no longer available.

Workaround: Before upgrading the appliance software to version 3.0.2-b1261765, ensure that the number of routes imported from one VRF to another does not exceed 1000. If pruning the route list is not sufficient, a default route can be configured. If needed, Oracle can provide guidance for this particular upgrade scenario.

To check VRF information for BGP routes advertised between the appliance and the data center, the following command can be used on the spine switches:

```
# show ip route summary vrf default
IP Route Table for VRF “default”
Total number of routes: 1626
Total number of paths:  3192
Unicast paths:
Best paths per protocol:      Backup paths per protocol:
  urib_internal  : 16           static         : 1
  am             : 11           bgp-65410      : 2
  local          : 3
  direct         : 3
  static         : 11
  broadcast      : 9
  nat            : 5
  hsrp           : 1
  bgp-65410      : 3130
```

Bug: 37628459

Version: 3.0.2

Route Table Stuck in Provisioning State Failure

When updating a route table that is associated as an attachment to a Dynamic Routing Gateway (DRG) to have a Local Peering Gateway (LPG) as a target, this known issue can leave the route table stuck in the provisioning state:

```
{
  "timestamp": "2023-06-28T15:30:58.635+0000",
  "rid":
"7FCCBAEBA62848878983FDA3098EE4DB/330fc100-b86f-4137-a1f9-2437a512b8e8/7b003c9
7-11c4-4e4a-8c9a-11861532db0d,
  "process": 1,
  "ocid": null,
  "levelname": "ERROR"
  "src_lineno": 481
  "src_pathname": "/usr/lib/python3.6/site-packages/pcanwctl/framework.py",
  "message::
  "Exception on function call: update_route_table, error: (404,
NotAuthorizedOrNotFound', 'No Subnet was found'), start exception rollback",
  "tag": "pca-nwctl.log"
}
```

Workaround: Delete and recreate the route table to avoid the error in the update routine.

Bug: 35547644

Version: 3.0.2

Updating Route Table Using Terraform Fails Because DRG Is Not Attached

When deploying network resources with Terraform, it may occur that a route table cannot be updated because an expected Dynamic Routing Gateway (DRG) attachment appears not to exist. Although the DRG is attached to the VCN, the operation is not fully completed when the command is issued to update the route table. The quick succession of commands through Terraform can reveal this timing issue, but it is highly unlikely to occur as a result of human user actions.

Workaround: Assuming the route table update failure is the result of a timing issue, repeating the route table update command is expected to succeed. Reapply the Terraform configuration or update the route table manually.

Bug: 36297777

Version: 3.0.2

Failure Executing Terraform Destroy Due to Route Table in Provisioning State

When you run a *terraform destroy* operation, it might fail because a route table object is still in 'provisioning' state instead of 'available'. This typically occurs when many updates are made to a route table in a short amount of time, resulting in commands taking longer to complete than expected by the Terraform provider. Strictly speaking, this is not a bug but rather a timing issue.

Workaround: Assuming the failure is the result of a timing issue, no route table or other resource is permanently stuck in 'provisioning' state. Repeating the terraform destroy command is expected to successfully remove the remaining objects. If necessary, increase the wait times for specific resources in your Terraform settings.

Bug: 36352218

Version: 3.0.2

When Configuring BGP Authentication the Password Is a Required Parameter

When the appliance uplinks to the data center network are configured for dynamic routing, two Autonomous Systems – meaning the spine switches on the appliance side, and the ToR switches on the data center side – are set up as BGP (Border Gateway Protocol) peers. The sessions between the BGP peers can be protected with password-based authentication. BGP authentication can be enabled for the data network as well as the optional separate administration network.

You can set the BGP password using the `setDay0DynamicRoutingParameters` command in the Service CLI. Two command parameters must be provided for each network.

- data network: `bgpAuthentication=True` and `bgpPassword=`***`<mypassword>`***
- administration network: `adminBgpAuthentication=True` and `adminBgpPassword=`***`<mypassword>`***

However, the CLI command is accepted if you set BGP authentication to "true" without providing a password. This has no adverse effects, but BGP authentication remains disabled.

Workaround: When you enable BGP authentication on the data network, and the administration network if present, make sure you also specify the BGP password as part of the command parameters.

Bug: 35737959

Version: 3.0.2

Uplink VRRP Mesh Configuration Sets Second Switch IP Incorrectly

When you try to configure the appliance data and administration network uplinks in mesh topology with VRRP (Virtual Router Redundancy Protocol), the command results in a CLI error. The problem occurs when the spine switches' second IP address is configured: the switch interprets the parameters as overlapping network settings and rejects them.

The following example shows an administration network with a 4-port mesh uplink topology. The same behavior applies to data network uplinks.

```
PCA-ADMIN> edit networkConfig enableAdminNetwork=True adminportcount=4
admintopology=MESH adminportspeed=10
adminspine1Ip=10.1.1.97,10.1.1.98 adminspine2Ip=10.1.1.101,10.1.1.102
adminSpineVip=10.1.1.105 [...]

PCA-ADMIN> show networkconfig
Data:
  [...]
```

```
Error:
UpdateFirstBootHandler: {'http_status_code': 500, 'code': 'InternalServerError',
'message': 'SwitchCliError on 100.96.2.20:
overlapping network for ipv4 address: 10.1.1.98/28 on po46, 10.1.1.97/28 already
configured on po45\\n for cmd [...]
```

Workaround: There is no workaround. This specific uplink configuration cannot be applied at this time.

Bug: 36063880

Version: 3.0.2

Failure Disabling the Segregated Administration Network

After upgrading the appliance software to 3.0.2-b1261765, disabling the separate administration network results in an error because the spine switch configuration cannot be updated. This is caused by a missing parameter in the update request that is sent to the spine switches.

Workaround: If you need to disable the segregated administration network on an appliance where this error occurs, change the BGP topology setting as shown below, after the appliance software upgrade or after you have enabled the separate admin network.

```
PCA-ADMIN> edit networkconfig adminBgpTopology=triangle
```

Bug: 37618380

Version: 3.0.2

Editing Rack Network Configuration Fails When Spine Switch Settings Are Not Changed

Changing the rack network configuration, without any other parameters that trigger a switch configuration update, results in a failure because the internal command contains empty parameters. The network remains fully functional but the configuration changes are not applied.

Workaround: To update certain network configuration parameters – such as DNS settings, NTP settings, and public IP addresses – add another change to the network configuration update command. After a successful update, revert the additional change. In the following example, we include a change to the `adminmtu` parameter when updating the DNS settings, then revert it back to its original value.

```
PCA-ADMIN> edit networkconfig dnsip1=10.202.192.16 dnsip2=192.0.2.32 adminmtu=9200
  JobId: 1c9bbfca-7566-4e06-a6e3-8185c512cf92
  Data: created job for edit network

PCA-ADMIN> edit networkconfig adminmtu=9216
```

Bug: 37311414

Version: 3.0.2

Instances Unreachable From Flex Network with Static Gateway After Upgrade

After upgrading the appliance software to 3.0.2-b1392231, any Flex network that uses a static gateway stops functioning correctly. Any new Flex network using a static gateway that is created after an upgrade to build 3.0.2-b1392231, does not allow network traffic.

Workaround: A security change was made in this release that interferes with flex network static gateway traffic. To re-enable this network access, follow the directions in Oracle Support Document 3093595.1 ([PCA 3.x] Flex Networks with Gateways will break after upgrade to 3.0.2-b1392231)

Bug: 38113437

Version: 3.0.2

Compute Service Issues

This section describes known issues and workarounds related to the compute service.

E5.Flex Instance Shape Is Not Supported on the X9-2 Hardware Platform

Compute instance shapes are tied to the architecture of the underlying compute nodes. The VM.PCAStandard.E5.Flex shape was added specifically to create instances on Oracle Server X10 compute nodes. It is the only shape supported on the X10 rack configuration. On a Private Cloud Appliance X9-2, all other shapes – including flex shapes – are supported.

Workaround: Select a suitable shape for your Private Cloud Appliance compute node architecture. If the compute nodes in your appliance are Oracle Server X10, always select the VM.PCAStandard.E5.Flex shape. Systems with Oracle Server X9-2 compute nodes support all shapes except VM.PCAStandard.E5.Flex. If you need a flexible shape, select the VM.PCAStandard1.Flex shape instead.

Bug: 35549831

Version: 3.0.2

Displaced Instances Not Returned to Their Selected Fault Domains

A displaced instance is an instance that is running in a fault domain that is not the fault domain that is specified in the configuration for that instance. An instance can become displaced during compute node evacuation or failure.

When Auto Recovery is enabled, a displaced instance is automatically returned to the fault domain that is specified in its configuration when resources become available in that fault domain. Auto Recovery is enabled by default.

Workaround:

If your Private Cloud Appliance is running Software Version 3.0.2-b852928 or Software Version 3.0.2-b892153, or if you upgrade to either of these releases, disable Auto Recovery from the Service CLI:

```
PCA-ADMIN> disableAutoResolveDisplacedInstance
```

If your Private Cloud Appliance is running a release that is newer than Software Version 3.0.2-b892153, you can enable Auto Recovery.

See "Migrating Instances from a Compute Node" and "Configuring the Compute Service for High Availability" in the Hardware Administration chapter of the *Oracle Private Cloud Appliance Administrator Guide* for more information about these commands.

If your Private Cloud Appliance is affected by this bug and an instance is displaced, stop and restart the instance to return the instance to its selected fault domain. See "Stopping, Starting, and Resetting an Instance" in the Compute Instance Deployment chapter of the *Oracle Private Cloud Appliance User Guide*.

Bug: 35601960, 35703270

Version: 3.0.2

Terraform Cannot Be Used for Instance Update

Starting with the May 2023 release of the Oracle Private Cloud Appliance software, the Oracle Cloud Infrastructure Terraform provider cannot be used to update an instance on Oracle Private Cloud Appliance. Only the instance update operation is affected by this issue.

Instance update fails when done using Terraform because the `is_live_migration_preferred` property does not exist for Terraform. Because the property is unknown, when the property is seen, Terraform treats the property value as `false`, which is not a supported value.

Workaround: Use the Compute Web UI or the OCI CLI to perform instance update.

Bug: 35421618

Version: 3.0.2

No Consistent Device Paths for Connecting to Block Volumes

When you attach a block volume to an instance, it is not possible to specify a device path that remains consistent between instance reboots. It means that for the `attach-paravirtualized-volume` CLI command the optional `--device` parameter does not work. Because the device name might be different after the instance is rebooted, this affects tasks you perform on the volume, such as partitioning, creating and mounting file systems, and so on.

Workaround: No workaround is available.

Bug: 32561299

Version: 3.0.1

Instance Pools Cannot Be Terminated While Starting or Scaling

While the instances in a pool are being started, and while a scaling operation is in progress to increase or decrease the number of instances in the pool, it is not possible to terminate the instance pool. Individual instances, in contrast, can be terminated at any time.

Workaround: To terminate an instance pool, wait until all instances have started or scaling operations have been completed. Then you can successfully terminate the instance pool as a whole.

Bug: 33038853

Version: 3.0.1

TypeError Returned when Attaching an Instance to an Instance Pool

When you attach an existing compute instance to an instance pool, you can include parameters with the OCI CLI command so it reports when the instance reaches the intended ("active") lifecycle state. However, a bug in the OCI CLI could lead to the following error:

```
# oci compute-management instance-pool-instance attach \
--instance-id ocid1.instance....unique_ID --instance-pool-id
ocid1.instancePool....unique_ID \
--wait-for-state ACTIVE --wait-interval-seconds 120 --max-wait-seconds 1200
Action completed. Waiting until the resource has entered state: ('ACTIVE',)
Encountered error while waiting for resource to enter the specified state. Outputting
last known resource state
{
  "data": {
    "availability-domain": "AD-1",
    "compartment-id": "ocid1.tenancy....unique_ID",
    "display-name": "Standard1.4",
    "fault-domain": "FAULT-DOMAIN-3",
    "id": "ocid1.instance....unique_ID",
    "instance-configuration-id": null,
    "instance-pool-id": "ocid1.instancePool....unique_ID",
    "lifecycle-state": "ATTACHING",
    "load-balancer-backends": [],
    "region": "mypca.example.com",
    "shape": "VM.PCAStandard1.Flex",
    "state": "RUNNING",
    "time-created": "2023-10-28T03:22:45+00:00"
  },
  "opc-work-request-id": "ocid1.workrequest....unique_ID"
}
TypeError: get_instance_pool_instance() missing 1 required positional argument:
'instance_id'
```

Workaround: The command option `--wait-for-state` is unreliable at this time. As an alternative you can use the command `list-instance-pool-instances` to check the state of the instances in the pool.

Bug: 35956140

Version: 3.0.2

Network Interface on Windows Does Not Accept MTU Setting from DHCP Server

When an instance is launched, it requests an IP address through DHCP. The response from the DHCP server includes the instruction to set the VNIC maximum transmission unit (MTU) to 9000 bytes. However, Windows instances boot with an MTU of 1500 bytes instead, which may adversely affect network performance.

Workaround: When the instance has been assigned its initial IP address by the DHCP server, change the interface MTU manually to the appropriate value, which is typically 9000 bytes for an instance's primary VNIC. This new value is persistent across network disconnections and DHCP lease renewals.

Alternatively, if the Windows image contains `cloudbase-init` with the MTUPlugin, it is possible to set the interface MTU from DHCP. To enable this function, execute the following steps:

1. Edit the file `C:\Program Files\Cloudbase Solutions\Cloudbase-Init\conf\cloudbase-init.conf`. Add these lines:

   ```
   mtu_use_dhcp_config=true
   plugins=cloudbaseinit.plugins.common.mtu.MTUPlugin
   ```

2. Enter the command `Restart-Service cloudbase-init`.
3. Confirm that the MTU setting has changed. Use this command: `netsh interface ipv4 show subinterfaces`.

Bug: 33541806

Version: 3.0.1

Oracle Solaris Instance in Maintenance Mode After Restoring from Backup

It is supported to create a new instance from a backup of the boot volume of an existing instance. The existing instance may be running or stopped. However, if you use a boot volume backup of an instance based on the Oracle Solaris image provided with Private Cloud Appliance, the new instance created from that backup boots in maintenance mode. The Oracle Solaris console displays this message: "*Enter user name for system maintenance (control-d to bypass):*"

Workaround: When the new Oracle Solaris instance created from the block volume backup has come up in maintenance mode, reboot the instance from the Compute Web UI or the CLI. After this reboot, the instance is expected to return to a normal running state and be reachable through its network interfaces.

Bug: 33581118

Version: 3.0.1

Oracle Solaris Instance Stuck in UEFI Interactive Shell

It has been known to occur that Oracle Solaris 11.4 compute instances, deployed from the image delivered through the management node web server, get stuck in the UEFI interactive shell and fail to boot. If the instance does not complete its boot sequence, users are not able to log in. The issue is likely caused by corruption of the original `.oci` image file during the import into the tenancy.

Workaround: If your Oracle Solaris 11.4 instance hangs during UEFI boot and remains unavailable, proceed as follows:

1. Terminate the instance that fails to boot.
2. Delete the imported Oracle Solaris 11.4 image.
3. Import the Oracle Solaris 11.4 image again from the management node web server.
4. Launch an instance from the newly imported image and verify that you can log in after it has fully booted.

Bug: 33736100

Version: 3.0.1

Slow Data Transfer and Buffering on Oracle Solaris Instance with LRO/LSO

Oracle Solaris uses Large Send/Receive Offload (LSO and LRO respectively), a feature to optimize network performance and CPU load by offloading TCP segmentation to the network controller hardware (NIC). This feature is enabled by default in the Oracle Solaris compute image provided with Oracle Private Cloud Appliance. However, LSO/LRO in a compute instance can cause very large packet sizes and retransmissions, leading to low data transfer speeds over the Oracle Solaris (virtual) network interfaces.

Workaround: For performance reasons, we recommended disabling LSO/LRO in Oracle Solaris compute instances hosted on Oracle Private Cloud Appliance. The following commands disable LSO/LRO for the net0 interface. On instances with multiple VNICs LRO must be disabled for each interface.

```
dladm set-linkprop -p lro=off net0
ipadm set-prop -p _lso_outbound=0 ip
```

For new Oracle Solaris instance deployments, add the commands to a custom cloud initialization script and point to it when launching an instance.

Bug: 36858282, 36405591

Version: 3.0.2

Instance Disk Activity Not Shown in Compute Node Metrics

The virtual disks attached to compute instances are presented to the guest through the hypervisor on the host compute node. Consequently, disk I/O from the instances should be detected at the level of the physical host, and reflected in the compute node disk statistics in Grafana. Unfortunately, the activity on the virtual disks is not aggregated into the compute node disk metrics.

Workaround: To monitor instance disk I/O and aggregated load on each compute node, rather than analyzing compute node metrics, use the individual VM statistics presented through Grafana.

Bug: 33551814

Version: 3.0.1

Attached Block Volumes Not Visible Inside Oracle Solaris Instance

When you attach additional block volumes to a running Oracle Solaris compute instance, they do not become visible automatically to the operating system. Even after manually rescanning the disks, the newly attached block volumes remain invisible. The issues is caused by the hypervisor not sending the correct event trigger to re-enumerate the guest LUNs.

Workaround: When you attach additional block volumes to an Oracle Solaris compute instance, reboot the instance to make sure that the new virtual disks or LUNs are detected.

Bug: 33581238

Version: 3.0.1

Host Name Not Set In Successfully Launched Windows Instance

When you work in a VCN and subnet where DNS is enabled, and you launch an instance, it is expected that its host name matches either the instance display name or the optional host name you provided. However, when you launch a Windows instance, it may occur that the host name is not set correctly according to the launch command parameters. In this situation, the instance's fully qualified domain name (FQDN) does resolve as expected, meaning there is no degraded functionality. Only the host name setting within the instance itself is incorrect; the VCN's DNS configuration works as expected.

Workaround: If your instance host name does not match the specified instance launch parameters, you can manually change the host name within the instance. There is no functional impact.

Alternatively, if the Windows image contains `cloudbase-init` with the SetHostNamePlugin, it is possible to set the instance host name (*computer name*) based on the instance FQDN (*hostname-label*). To enable this function, execute the following steps:

1. Edit the file `C:\Program Files\Cloudbase Solutions\Cloudbase-Init\conf\cloudbase-init.conf`. Make sure it contains lines with these settings:

   ```
   plugins=cloudbaseinit.plugins.common.sethostname.SetHostNamePlugin
   allow_reboot=true
   ```

2. Enter the command `Restart-Service cloudbase-init`.
3. Confirm that the instance host name has changed.

Bug: 33736674

Version: 3.0.1

Instance Backups Can Get Stuck in an EXPORTING or IMPORTING State

In rare cases, when an instance is exporting to create a backup, or a backup is being imported, and the system experiences a failure of one of the components, the exported or imported backup gets stuck in an EXPORTING or IMPORTING state.

Workaround:

1. Delete the instance backup.
2. Wait 5 minutes or more to ensure that all internal services are running.
3. Perform the instance export or import operation again.

See *Backing Up and Restoring an Instance* in Compute Instance Deployment.

Bug: 34699012

Version: 3.0.1

Instance Not Started After Fault Domain Change

When you change the fault domain of a compute instance, the system stops it, cold-migrates it to a compute node in the selected target fault domain, and restarts the instance on the new host. This process includes a number of internal operations to ensure that the instance can return to its normal running state on the target compute node. If one of these internal operations fails, the instance could remain stopped.

The risk of running into issues with fault domain changes increases with the complexity of the operations. For example, moving multiple instances concurrently to another fault domain, especially if they have shared block volumes and are migrated to different compute nodes in the target fault domain, requires many timing-sensitive configuration changes at the storage level. If the underlying iSCSI connections are not available on a migrated compute instance's new host, the hypervisor cannot bring up the instance.

Workaround: After changing the fault domain, if a compute instance remains stopped, try to start it manually. If the instance failed to come up due to a timing issue as described above, the manual start command is likely to bring the instance back to its normal running state.

Bug: 34550107

Version: 3.0.2

Instance Migration Stuck in MOVING State

When migrating VMs using the Service Web UI it is possible that a migration can get stuck in the MOVING lifecycle state and you will be unable to continue further migrations.

This error can occur when administrative activities, such as live migrations, are running during a patching or upgrading process, or administrative activities are started before patching or upgrading processes have fully completed.

Workaround: Contact Oracle Support to resolve this issue.

Bug: 33911138

Version: , 3.0.1, 3.0.2

OCI CLI Commands Fail When Run From a Compute Instance

Compute instances based on Oracle Linux images provided since early 2023 are likely to have a firewall configuration that prevents the OCI CLI from connecting to the Private Cloud Appliance identity service. In Oracle Cloud Infrastructure the identity service must now be accessed through a public IP address (or FQDN), while Oracle Private Cloud Appliance provides access through an internal IP address. The Oracle Cloud Infrastructure images are configured by default to block all connections to this internal IP address.

The issue has been observed with these images:

- uln-pca-oracle-linux-7-9-2023-08-31-0-oci
- uln-pca-oracle-linux-8-2023-08-31-0-oci
- all Oracle Linux 9 images with a 2023 availability date

Workaround: If you intend to use the OCI CLI from a compute instance in your Private Cloud Appliance environment, verify its access to the identity service. If connections are refused, check the instance firewall configuration and enable access to the identity service.

1. Test the instance connection to the identity service. For example, use telnet or netcat.

   ```
   # curl -v telnet://identity.mydomain:443
   * connect to 169.254.169.254 port 443 failed: Connection refused

   -- OR --
   # nc -vz identity.mydomain 443
   Ncat: Connection refused.
   ```

2. Confirm that the firewall output chain contains a rule named `BareMetalInstanceServices`.

   ```
   # iptables -L OUTPUT --line-numbers
   Chain OUTPUT (policy ACCEPT)
   num  target                     prot   opt   source           destination
   1    BareMetalInstanceServices  all    --    anywhere         169.254.0.0/16
   ```

3. Disable the bare metal instance rules in the firewall configuration.

   a. Rename the file that defines these firewall rules (`/etc/firewalld/direct.xml`).

b. Restart the firewalld service.

Detailed instructions are provided in the note with Doc ID 2983004.1.

Bug: 35234468

Version: 3.0.2

Cannot Install OCI CLI on Oracle Linux 9 Instance

To run the OCI CLI on an Oracle Linux 9 compute instance, the package `python39-oci-cli` and its dependencies are required. These are provided through the *Oracle Linux 9 OCI Included Packages* (`ol9_oci_included`) repository, but this repository cannot be accessed outside Oracle Cloud Infrastructure.

An Oracle Linux 9 compute instance on Oracle Private Cloud Appliance must instead retrieve the required packages from the public Oracle Linux 9 repositories – specifically: *Oracle Linux 9 Development Packages* (`ol9_developer`) and *Oracle Linux 9 Application Stream Packages* (`ol9_appstream`). These repositories are not enabled by default in the provided Oracle Linux 9 image.

Workaround: Enable the `ol9_developer` and `ol9_appstream` public yum repositories to install `python39-oci-cli`.

```
$ sudo yum --disablerepo="*" --enablerepo="ol9_developer ol9_appstream" install python39-
oci-cli -y
Dependencies resolved.
=========================================================================================
=========================
 Package                               Architecture       Version
Repository             Size
=========================================================================================
=========================
Installing:
 python39-oci-cli                      noarch             3.40.2-1.el9
ol9_developer          39 M
Upgrading:
 python39-oci-sdk                      x86_64             2.126.2-1.el9
ol9_developer          74 M
Installing dependencies:
 python3-arrow                         noarch             1.1.0-2.el9
ol9_developer         153 k
 python3-importlib-metadata            noarch             4.12.0-2.el9
ol9_developer          75 k
 python3-jmespath                      noarch             0.10.0-4.el9
ol9_developer          78 k
 python3-prompt-toolkit                noarch             3.0.38-4.el9
ol9_appstream         1.0 M
 python3-terminaltables                noarch             3.1.10-8.0.1.el9
ol9_developer          60 k
 python3-wcwidth                       noarch             0.2.5-8.el9
ol9_appstream          65 k
 python3-zipp                          noarch             0.5.1-1.el9
ol9_developer          24 k

Transaction Summary
=========================================================================================
========================
Install  8 Packages
Upgrade  1 Package
[...]
Complete!
```

Bug: 35855058

Version: 3.0.2

Changing Instance Compartment in OCI CLI Returns Key Error

When you use the OCI CLI to change the compartment where a compute instance resides, the command returns a work request key error.

```
# oci compute instance change-compartment <instance id> <new compartment id> --debug
[...]
DEBUG:oci.base_client.140018383788856: 2024-06-03 18:41:52.605103: Response status: 200
DEBUG:oci.base_client.140018383788856: 2024-06-03 18:41:52.605301: Response returned
DEBUG:oci.base_client.140018383788856:time elapsed for request: 1.5186387430876493
Traceback (most recent call last):
[...]
  File "/root/lib/oracle-cli/lib64/python3.6/site-packages/services/core/src/
oci_cli_compute/compute_cli_extended.py", line 767, in change_instance_compartment
    work_request_client = cli_util.build_client('core', 'work_request', ctx)
  File "/root/lib/oracle-cli/lib64/python3.6/site-packages/oci_cli/cli_util.py", line
461, in build_client
    client_class = CLIENT_MAP[spec_name][service_name]
KeyError: 'work_request'
```

This is a known issue in the OCI CLI. The change compartment function attempts to create a work request in an incorrect way.

Workaround: We advise against changing the compartment of a compute instance using the OCI CLI, because it is unclear which effect this issue has on the code execution in Private Cloud Appliance. Testing does show that the compartment change is applied correctly despite the key error.

Bug: 36691465

Version: 3.0.2

Instance Principal Unavailable Until Next Certificate Renewal Check

An instance principal is a compute instance that is authorized to perform actions on service resources. Before allowing these operations, the Identity and Access Management Service (IAM) validates the instance principal security token: a TLS certificate that expires after 30 days.

The system checks for expired certificates every 24 hours and renews them if necessary. However, an instance principal might lose its authorization after an outage, system maintenance, or upgrade activity. In that case, it cannot obtain an updated certificate until the next renewal check, which could be up to 24 hours later.

Similarly, after upgrading from a release that does not support instance principals to a release that does support instance principals, compute instances might have to wait up to 24 hours to receive their TLS certificates.

Workaround: If you need to have this certificate installed or renewed immediately, contact Oracle for assistance.

Bug: 36165739

Version: 3.0.2

List of Platform Images Includes OKE Images

Private Cloud Appliance provides a set of standard Oracle Linux and Oracle Solaris images for convenient compute instance deployment. When the appliance is upgraded or patched, the latest available images are added. The same mechanism is used to add the images required to deploy clusters with the OKE service: Oracle Private Cloud Appliance Kubernetes Engine (OKE). When users launch an instance from the Compute Web UI, the appropriate images are listed and the OKE-specific images are filtered out. However, the OCI CLI displays all images by default, including those for the OKE service, which should not be used for regular compute instances.

```
oci compute image list --compartment-id "ocid1.tenancy.... unique_id" | grep "display-
name"
      "display-name": "uln-pca-Oracle-Linux-7.9-2024.04.19_0.oci",
      "display-name": "uln-pca-Oracle-Linux-7.9-2024.05.29_0.oci",
      "display-name": "uln-pca-Oracle-Linux-8-2024.04.19_0.oci",
      "display-name": "uln-pca-Oracle-Linux-8-2024.05.29_0.oci",
      "display-name": "uln-pca-Oracle-Linux-9-2024.04.22_0.oci",
      "display-name": "uln-pca-Oracle-Linux-9-2024.05.29_0.oci",
      "display-name": "uln-pca-Oracle-Linux8-OKE-1.26.6-20240210.oci",
      "display-name": "uln-pca-Oracle-Linux8-OKE-1.26.6-20240611.oci",
      "display-name": "uln-pca-Oracle-Linux8-OKE-1.27.7-20240422.oci",
      "display-name": "uln-pca-Oracle-Linux8-OKE-1.27.7-20240602.oci",
      "display-name": "uln-pca-Oracle-Linux8-OKE-1.28.3-20240210.oci",
      "display-name": "uln-pca-Oracle-Linux8-OKE-1.28.3-20240602.oci",
      "display-name": "uln-pca-Oracle-Solaris-11-2024.05.07_0.oci",
```

Workaround: When launching a regular compute instance or instance pool, use either the Oracle-provided images or your own custom images. Do not use the OKE-specific images.

Bug: 36112983

Version: 3.0.2

Import of Custom Images in VMDA Format Not Supported

Private Cloud Appliance does not currently support the import of custom images in the VMDA format.

Workaround: Use the QCOW2 format when importing custom images.

Bug: 37049215

Version: 3.0.2

Increasing GPU Usage of Running Instance When Capacity Is Exceeded Results in Stopped Instance

The shape of a compute instance determines the number of GPUs it uses, so you can increase GPU usage by updating the instance to a shape with a higher GPU count. However, if the shape update puts the system over its physical GPU capacity, the update is accepted without error, and the instance in question is stopped.

> **Note**
>
> When you try to launch a new GPU instance on a system with insufficient GPU capacity available, an appropriate error is returned and the instance launch fails as expected.

Workaround: When updating the shape of a GPU instance to increase GPU usage, confirm that the instance is still running after the update. If the instance is stopped, change its shape back to the original, or check if GPUs can be freed up for use by your instance. An administrator can verify GPU availability using the CLI command `getFaultDomainInfo`.

```
PCA-ADMIN> getFaultDomainInfo
Data:
  id               totalCNs    totalMemory   freeMemory   totalvCPUs   freevCPUs
totalGPUs   freeGPUs   Notes
  --               ---------   -----------   ----------   ----------   ---------
---------   --------   -----
  UNASSIGNED       6           0.0           0.0          0            0
0           0          N.A.
  UNASSIGNED-GPU   0           0.0           0.0          0            0
0           0          N.A.
  FD1              2           3208.0        3144.0       488          444
0           0          N.A.
  FD1-GPU          1           984.0         24.0         216          2
4           0          N.A.
  FD2              2           3208.0        3160.0       488          446
0           0          N.A.
  FD2-GPU          1           984.0         504.0        216          108
4           2          N.A.
  FD3              2           3208.0        3032.0       488          410
0           0          N.A.
  FD3-GPU          1           984.0         24.0         216          0
4           0          N.A.
```

Bug: 37278974

Version: 3.0.2

Instances Launched from an Instance Pool Created With an Instance Configuration Including an SR-IOV vNIC are Inaccessible

If you use an instance configuration with an SR-IOV vNIC to create an instance pool, then launch an instance from that pool, you will be unable to access that instance. At this time, it is not possible to create an instance pool with a configuration that includes an SR-IOV vNIC, as that vNIC will not attach.

Workaround: Create the instance without the SR-IOV vNIC attached, launch the instance, and then attach the SR-IOV vNIC.

Bug: 37192651

Version: 3.0.2

Compute Instance Migration Fails Because Device Cannot Be Attached

When migrating a compute instance to another compute node, the operation might fail because the path to a device is not found and it cannot be attached. The issue applies to regular live migration as well as migration of displaced instances. The migration job output looks similar to this example:

```
PCA-ADMIN> show job id=71782dc1-02d8-412e-97fa-703508c606e9
Data:
  AssociatedObj = id:a7c7bbfe-21f5-4f9d-9158-87779c7eb7b0  type:ComputeNode
name:pcacn003
  Name = OPERATION-MigrateVm
  Progress Message = Fail to attach device 600144f00d9c3e67000067bcfce30047, path not
found, server 100.96.2.66
  Run State = Failed
```

Workaround: Manually retry migrating the instance. The new job is expected to succeed.

Bug: 37574886

Version: 3.0.2

GPU Drivers Not Included in Oracle Linux Platform Images

If a Private Cloud Appliance installation includes compute nodes with GPUs, you can access them by selecting a dedicated shape. The GPU shapes can be selected for compute instances based on an Oracle Linux 8 or Oracle Linux 9 platform image. The current image versions do not include GPU drivers. The instance OS detects the allocated GPUs, but to use them, you need the CUDA Toolkit from the NVIDIA developer site to install the required drivers.

> ⓘ **Note**
>
> The large download and local repository installation need a large amount of disk space. The default 50GB boot volume is insufficient on Oracle Linux 9 and only just large enough on Oracle Linux 8. It is highly recommended to increase the boot volume size to at least 60GB, and extend the file system accordingly.

Workaround: After launching the instance, log in to the command line and install the CUDA Toolkit. Follow the instructions for your version of Oracle Linux.

Installing GPU Drivers in an Oracle Linux 9 Instance

1. From the command line of the instance, download and install the CUDA Toolkit rpm for your OS.

   ```
   $ wget https://developer.download.nvidia.com/compute/cuda/12.8.0/local_installers/
   cuda-repo-rhel9-12-8-local-12.8.0_570.86.10-1.x86_64.rpm
   $ sudo rpm -i cuda-repo-rhel9-12-8-local-12.8.0_570.86.10-1.x86_64.rpm
   $ sudo dnf clean all
   $ sudo dnf install cuda-toolkit-12-8
   ```

2. Enable the Oracle Linux 9 EPEL yum repository. Install the `dkms` package.

   ```
   $ sudo yum-config-manager --enable ol9_developer_EPEL
   $ sudo dnf install dkms
   ```

3. Install the GPU drivers.

```
$ sudo dnf install cuda-12-8
```

4. Verify the installation with the NVIDIA System Management Interface.

```
$ nvidia-smi
+-----------------------------------------------------------------------------------
------+
| NVIDIA-SMI 570.86.10              Driver Version: 570.86.10      CUDA Version: 
12.8     |
|-----------------------------------------+------------------------
+----------------------+
| GPU  Name                 Persistence-M | Bus-Id          Disp.A | Volatile 
Uncorr. ECC |
| Fan  Temp   Perf          Pwr:Usage/Cap |           Memory-Usage | GPU-Util  
Compute M. |
|                                         |                        |               
MIG M. |
|
=========================================+========================+=================
=====|
|   0  NVIDIA L40S                    Off |   00000000:00:05.0 Off 
|                    0 |
| N/A   26C    P8             23W /  350W |       1MiB /  46068MiB |      0%      
Default |
|                                         |                        
|                  N/A |
+-----------------------------------------+------------------------
+----------------------+

+-----------------------------------------------------------------------------------
------+
| 
Processes:                                                                              
    |
|  GPU   GI   CI              PID   Type   Process name                        GPU 
Memory |
|        ID   ID                                                                
Usage      |
|
====================================================================================
=====|
|  No running processes 
found                                                             |
+-----------------------------------------------------------------------------------
------+
```

Installing GPU Drivers in an Oracle Linux 8 Instance

1. From the command line of the instance, download and install the CUDA Toolkit rpm for your OS.

```
$ wget https://developer.download.nvidia.com/compute/cuda/12.8.0/local_installers/
cuda-repo-rhel8-12-8-local-12.8.0_570.86.10-1.x86_64.rpm
$ sudo rpm -i cuda-repo-rhel8-12-8-local-12.8.0_570.86.10-1.x86_64.rpm
$ sudo dnf clean all
$ sudo dnf install cuda-toolkit-12-8
```

2. Enable the Oracle Linux 8 EPEL yum repository. Install the `dkms` package.

```
$ sudo yum-config-manager --enable ol8_developer_EPEL
$ sudo dnf install dkms
```

3. Install the GPU drivers.

   ```
   $ sudo dnf install cuda-12-8
   ```

4. Install the NVIDIA kernel module.

   Confirm which toolset you need, `either gcc-toolset-11` or `gcc-toolset-13`.

   ```
   # ls -l /etc/scl/conf/
   ```

   Install the correct module. This example shows `gcc-toolset-13`.

   ```
   $ sudo scl enable gcc-toolset-13 bash
   # dkms install nvidia-open -v 570.86.10
   ```

   If this `make` error appears while the kernel module is built, you can safely ignore it.

   ```
   Cleaning build area...(bad exit status: 2)
   Failed command:
   make -C /lib/modules/5.15.0-206.153.7.el8uek.x86_64/build M=/var/lib/dkms/nvidia-
   open/570.86.10/build clean
   ```

5. Verify the installation with the NVIDIA System Management Interface.

   ```
   # nvidia-smi
   +-----------------------------------------------------------------------------------
   ------+
   | NVIDIA-SMI 570.86.10              Driver Version: 570.86.10      CUDA Version:
   12.8     |
   |-----------------------------------------+------------------------
   +----------------------+
   | GPU  Name                 Persistence-M | Bus-Id          Disp.A | Volatile
   Uncorr. ECC |
   | Fan  Temp   Perf          Pwr:Usage/Cap |           Memory-Usage | GPU-Util
   Compute M. |
   |                                         |                        |
   MIG M. |
   |
   =========================================+========================+=================
   =====|
   |   0  NVIDIA L40S                    Off |   00000000:00:05.0 Off
   |                    0 |
   | N/A   26C    P8              23W /   350W |       1MiB /   46068MiB |      0%
   Default |
   |                                         |
   |                  N/A |
   +-----------------------------------------+------------------------
   +----------------------+

   +-----------------------------------------------------------------------------------
   ------+
   |
   Processes:
       |
   |  GPU   GI   CI              PID   Type   Process name                        GPU
   Memory |
   |        ID   ID
   Usage      |
   |
   ```

```
=====================================================================================
=====|
|  No running processes
found                                                                   |
+------------------------------------------------------------------------------------
------+
```

Bug: n/a

Version: 3.0.2

Unable to Launch GPU Flex Shape Instance Using Terraform or OCI SDK

If a Private Cloud Appliance installation includes compute nodes with GPUs, you must launch compute instances with a dedicated shape to be able to use the GPUs. This can be a standard shape with fixed hardware resource ratios, or a flex shape that allows users to customize the CPU/RAM/GPU ratio. However, due to a difference in shape modeling between Private Cloud Appliance and Oracle Cloud Infrastructure, it is not possible to launch an instance with a GPU flex shape using the OCI SDK or Terraform provider. If you try to launch an instance this way, an error is returned indicating the "gpus" argument is not recognized.

Workaround: Use the Compute Web UI or the OCI CLI to launch a compute instance with a GPU flex shape. As an alternative, a direct `curl` request providing all the correct arguments is also expected to work.

Bug: 37195244

Version: 3.0.2

Forced Compute Node Evacuation Fails when Non-Migratable Instances Are Running

Evacuating a compute node is an operation to migrate all compute instances to other compute nodes, so the node can be safely taken offline for maintenance. It could also be used to soft-stop all non-migratable instances running on a node with a single command, instead of stopping the instances one by one. However, best practice is to shut down an instance from its guest OS and gracefully stop the instance from the Compute Web UI or OCI CLI.

If you decide to use forced node evacuation when non-migratable instances (such as instances based on a GPU shape or configured with SR-IOV) are running, the job will return an error and remain in failed state, even if the instances are stopped successfully.

```
PCA-ADMIN> migrateVm id=<compute_node_id> force=true
JobId: 03816731-2829-471c-9aaf-b8f5e0666bdf
Data: Running

PCA-ADMIN> show job id=03816731-2829-471c-9aaf-b8f5e0666bdf
Data:
  Name = OPERATION-MigrateVm
  Progress Message = (400, 'LimitExceeded', 'Unable to place VM instance')
                     (403, 'NotAllowed', 'instance ocid1.instance.unique_ID migration
not allowed')
  Run State = Failed
```

Workaround: After performing a forced compute node evacuation, confirm that all non-migratable instances have been stopped successfully.

```
PCA-ADMIN> getNonMigratableInstances
Data:
```

```
id                           Display Name  Compute Node Id  Domain State
--                           ------------  ---------------  ------------
ocid1.instance.unique_ID     instance202   CN_ID            shut off
ocid1.instance.unique_ID     kqh027        CN_ID            shut off
```

To clear the error from the failed job, run the evacuation command a second time. Now it should succeed.

For more information, see Migrating Instances from a Compute Node in the "Oracle Private Cloud Appliance Administrator Guide".

Bug: 37092239

Version: 3.0.2

Instance with Multiple GPUs Fails P2P Verification

When an instance is launched using a shape with multiple GPUs, direct peer-to-peer (P2P) data access between the GPUs is enabled for best performance. However, verification using the *simpleP2P* test tools may return errors, indicating that peer access between some GPU pairs is not working as expected.

Workaround: After installing the NVIDIA CUDA Toolkit in the compute instance, enable driver persistence mode and disable PCIe relaxed ordering.

1. Log in to the compute instance as a user with *sudo* privileges.
2. Enable GPU driver persistence mode.

   ```
   $ sudo systemctl enable nvidia-persistenced.service
   $ sudo systemctl start nvidia-persistenced.service

   $ systemctl status nvidia-persistenced.service
     nvidia-persistenced.service - NVIDIA Persistence Daemon
        Loaded: loaded (/usr/lib/systemd/system/nvidia-persistenced.service; enabled;
   preset: enabled)
        Active: active (running) since Tue 2025-02-04 09:50:12 GMT; 15s ago
       Process: 413704 ExecStart=/usr/bin/nvidia-persistenced --verbose (code=exited,
   status=0/SUCCESS)
      Main PID: 413705 (nvidia-persiste)
         Tasks: 1 (limit: 1284273)
        Memory: 876.0K
           CPU: 14ms
        CGroup: /system.slice/nvidia-persistenced.service
                └─413705 /usr/bin/nvidia-persistenced --verbose
   ```

3. Look up the PCI identifiers for the GPUs.

   ```
   $ lspci | grep -i nvidia
   00:05.0 3D controller: NVIDIA Corporation AD102GL [L40S] (rev a1)
   00:06.0 3D controller: NVIDIA Corporation AD102GL [L40S] (rev a1)
   ```

4. Disable PCIe relaxed ordering for the GPUs. Use this command:

   ```
   $ sudo setpci -s <gpu-device> CAP_EXP+8.w=0
   ```

   For example:

   ```
   $ sudo setpci -s 00:05.0 CAP_EXP+8.w=0
   $ sudo setpci -s 00:06.0 CAP_EXP+8.w=0
   ```

5. If the compute instance is stopped and started, because of a reboot or another operation that changes the lifecycle state, repeat the commands to disable PCIe relaxed ordering for all GPU devices.

Bug: 37279887

Version: 3.0.2

Storage Services Issues

This section describes known issues and workarounds related to the functionality of the internal ZFS storage appliance and the different storage services: block volume storage, object storage and file system storage.

Updating Terraform Changes File Storage Export Path

When you use Terraform to create a file system export, you must specify `AUTOSELECT` for the value of `path` in the `oci_file_storage_export` definition.

You must also include the `lifecycle` stanza to ignore any updates to the path. If you do not ignore updates to the path, the path is automatically deleted and re-created when you update the Terraform, even if you do not explicitly update this path. Updating this path can interrupt clients that have an active mount via the export.

Workaround: Set the path and include the `lifecycle` stanza as shown in the following example:

```
resource "oci_file_storage_export" "pcauserExport" {
  export_set_id  = local.Okit_MT_1702774958525ExportSet_id
  file_system_id = local.Okit_FS_1702774481898_id
  path           = "AUTOSELECT"
  lifecycle {
    ignore_changes = [
      path,
    ]
  }
}
```

Bug: 36116003

Version: 3.0.2

Creating Image from Instance Takes a Long Time

When you create a new compute image from an instance, its boot volume goes through a series of copy and conversion operations. In addition, the virtual disk copy is non-sparse, which means the full disk size is copied bit-for-bit. As a result, image creation time increases considerably with the size of the base instance's boot volume.

Workaround: Wait for the image creation job to complete. Check the work request status in the Compute Web UI, or use the work request id to check its status in the CLI.

Bug: 33392755

Version: 3.0.1

Large Object Transfers Fail After ZFS Controller Failover

If a ZFS controller failover or failback occurs while a large file is uploaded to or downloaded from an object storage bucket, the connection may be aborted, causing the data transfer to fail. Multipart uploads are affected in the same way. The issue occurs when you use a version of the OCI CLI that does not provide the retry function in case of a brief storage connection timeout. The retry functionality is available as of version 3.0.

Workaround: For a more reliable transfer of large objects and multipart uploads, use OCI CLI version 3.0 or newer.

Bug: 33472317

Version: 3.0.1

Use Multipart Upload for Objects Larger than 100MiB

Uploading very large files to object storage is susceptible to connection and performance issues. For maximum reliability of file transfers to object storage, use multipart uploads.

Workaround: Transfer files larger than 100MiB to object storage using multipart uploads. This behavior is expected; it is not considered a bug.

Bug: 33617535

Version: n/a

File System Export Temporarily Inaccessible After Large Export Options Update

When you update a file system export to add a large number of *'source'*-type export options, the command returns a service error that suggests the export no longer exists (`"code": "NotFound"`). In actual fact, the export becomes inaccessible until the configuration update has completed. If you try to access the export or display its stored information, a similar error is displayed. This behavior is caused by the method used to update file system export options: the existing configuration is deleted and replaced with a new one containing the requested changes. It is only noticeable in the rare use case when dozens of export options are added at the same time.

Workaround: Wait for the update to complete and the file system export to become available again. The CLI command `oci fs export get --export-id <fs_export_ocid>` should return the information for the export in question.

Bug: 33741386

Version: 3.0.1

Block Volume Stuck in Detaching State

Block volumes can be attached to several different compute instances, and can even have multiple attachments to the same instance. When simultaneous volume detach operations of the same volume occur, as is done with automation tools, the processes may interfere with each other. For example, different work requests may try to update resources on the ZFS storage appliance simultaneously, resulting in stale data in a work request, or in resource update conflicts on the appliance. When block volume detach operations fail in this manner, the block volume attachments in question may become stuck in *detaching* state, even though the block volumes have been detached from the instances at this stage.

Workaround: If you have instances with block volumes stuck in *detaching* state, the volumes have been detached, but further manual cleanup is required. The *detaching* state cannot be cleared, but the affected instances can be stopped and the block volumes can be deleted if that is the end goal.

Bug: 33750513

Version: 3.0.1

Fix available: Please apply the latest patches to your system.

Detaching Volume Using Terraform Fails Due To Timeout

When you use Terraform to detach a volume from an instance, the operation may fail with an error message indicating the volume attachment was not destroyed and the volume remains in attached state. This can occur when the storage service does not send confirmation that the volume was detached, before Terraform stops polling the state of the volume attachment. The volume may be detached successfully after Terraform has reported an error.

Workaround: Re-apply the Terraform configuration. If the errors were the result of a timeout, then the second run will be successful.

Bug: 35256335

Version: 3.0.2

Creating File System Export Fails Due To Timeout

At a time when many file system operations are executed in parallel, timing becomes a critical factor and could lead to an occasional failure. More specifically, the creation of a file system export could time out because the file system is unavailable. The error returned in that case is: "*Internal Server Error: No such filesystem to create the export on*".

Workaround: Because this error is caused by a resource locking and timeout issue, it is expected that the operation will succeed when you try to execute it again. This error only occurs in rare cases.

Bug: 34778669

Version: 3.0.2

File System Access Lost When Another Export for Subset IP Range Is Deleted

A virtual cloud network (VCN) can contain only one file system mount target. All file systems made available to instances connected to the VCN must have exports defined within its mount target. File system exports can provide access to different file systems from overlapping subnets or IP address ranges. For example: *filesys01* can be made available to IP range 10.25.4.0/23 and *filesys02* to IP range 10.25.5.0/24. The latter IP range is a subset of the former. Due to the way the mount IP address is assigned, when you delete the export for *filesys02*, access to *filesys01* is removed for the superset IP range as well.

Workaround: If your file system exports have overlapping source IP address ranges, and deleting one export causes access issues with another export similar to the example above, then it is recommended to delete the affected exports and create them again within the VCN mount target.

Bug: 33601987

Version: 3.0.2

File System Export UID/GID Cannot Be Modified

When creating a file system export you can add extra NFS export options, such as access privileges for source IP addresses and identity squashing. Once you have set a user/group identity (UID/GID) squash value in the NFS export options, you can no longer modify that value. When you attempt to set a different ID, an error is returned: "`Uid and Gid are not consistent with FS AnonId: <currentUID>`"

Workaround: If you need to change the UID/GID mapping, delete the NFS export options and recreate them with the desired values. If you are using the OCI CLI, you must delete the entire file system export (not just the options) and recreate the export, specifying the desired values with the `--export-options` parameter.

Bug: 34877118

Version: 3.0.2

Internal Backups for Instance Cloning Not Displayed

When you clone a compute instance, an internal backup of the boot and block volumes is created. In appliance software versions up to 3.0.2-b852928 those internal backups are visible to users. While not recommended, the backups could technically be used to create additional instances. Existing internal backups are not deleted during appliance upgrade or patching. However, in newer software versions the internal backups are no longer exposed.

Workaround: Do not create clones or new compute instances from the existing internal volume (group) backups. To remove old backups of storage volumes, ensure that all other backups and clones of the original source volume are terminated first.

Bug: 35406033

Version: 3.0.2

Boot Volume Counts Toward Volume Attachments Limit

The latest version of Private Cloud Appliance software allows a maximum of 32 block volume attachments. However, the required boot volume is included in the attachment count, which means up to 31 extra data volumes can be attached to a compute instance. This might confuse users of Oracle Cloud Infrastructure, because its limit is 32 data volumes *in addition* to the boot volume.

Workaround: There is no workaround. The limit of 32 block volume attachments includes the boot volume for instances deployed on Private Cloud Appliance.

Bug: 36641181

Version: 3.0.2

Limit for Volume Backups Not Enforced

The "Service Limits" chapter in the Oracle Private Cloud Appliance Release Notes specifies a limit of 100 volume backups per tenancy for a system with default storage capacity. This limit is not enforced: you can continue to create volume backups beyond the documented maximum.

Workaround: In theory, the maximum number of volume backups is limited by available storage on the ZFS Storage Appliance. The system is expected to handle thousands of volume backups across all tenancies. However, we recommend that an administrator monitors storage space consumption proactively if users create many volume backups.

Bug: 35509673

Version: 3.0.2

NFS Service Interruption During ZFS Storage Appliance Firmware Upgrade or Patching

When the firmware of the appliance's ZFS Storage Appliance is upgraded or patched, compute instances could encounter an interruption of NFS connectivity. The service outage occurs when failover/failback is performed between the storage appliance controllers, and it could take over 2 minutes to reestablish the NFS service. There could be multiple factors contributing to the delay: the NFS server's 90 second grace period to allow NFSv4 clients to recover locking state after an outage, the NFS protocol attempting to reconnect to the same TCP port, and the NFS client's kernel version.

Workaround: To reduce the outage time of NFS connectivity, it is recommended to use the mount options described in the note with Doc ID 359515.1. While the document describes optimizations for Oracle RAC and Oracle Clusterware, the mount options also improve NFS performance and stability in a Private Cloud Appliance environment.

Bug: 36348165

Version: 3.0.2

File System Create Fails With Generic Message

If you get a generic failure when creating a file system on a high performance pool, confirm that a `PCA_POOL_HIGH` is available on the rack.

Bug: 36773744

Version: 3.0.2

Export of Imported Instance Failing

When exporting an instance that was imported from the offsystem backup feature, the operation might fail if you have deleted or renamed the Custom Image.

Workaround: After importing an instance on the Private Cloud Appliance from the off system backup feature, don't delete the Custom Images or rename the display-name of imported images.

Bug: 36995638

Version: 3.0.2

Slow Block Storage Update Prevents Resolving Displaced Instances

When compute nodes are rebooted, for example to allow an appliance software upgrade to complete, the hosted compute instances are typically migrated to other compute nodes, possibly in another fault domain. The system returns such *displaced* instances to their original location when possible. When instances are moved between compute nodes, the block storage service needs to update the configuration of attached boot and block volumes accordingly. If these updates take too long to complete, instances might get stuck in moving state.

Workaround: No workaround available yet.

Bug: 37633393

Version: 3.0.2

Kubernetes Engine Issues

This section describes known issues and workarounds related to Oracle Private Cloud Appliance Kubernetes Engine (OKE).

Cloning Feature for Block Volume PV Using CSI Plugin Is Not Available

The cloning feature for existing block volumes is not available for PVCs created using the CSI volume plugin in your worker node applications.

For block volume persistent storage, use the CSI plugin as described in Creating Persistent Block Volume Storage.

Workaround: No workaround is available to clone an existing volume using the CSI plugin.

Bug: 36252730

Version: 3.0.2

Supported OCI Terraform Provider Versions

The *Oracle Private Cloud Appliance Kubernetes Engine (OKE)* guide provides example Terraform scripts to configure OKE resources. To use these scripts, you must install both Terraform and the Oracle Cloud Infrastructure (OCI) Terraform provider.

If you use Terraform scripts with Kubernetes Engine (OKE), in your `provider` block, specify the version of the OCI Terraform provider to install as at least v4.50.0 but no greater than v6.36.0:

```
provider "oci" {
    version          = ">= 4.50.0, <= 6.36.0"
...
}
```

Bug: 37934227

Version: 3.0.2

Enable Add-on Work Request Initially in Failed State

When you enable an add-on, the work request might initially show that the add-on installation failed instead of showing the add-on installation as pending. The add-on state should be Needs Attention. The add-on state should change to Active after reconciliation, and the work request state should change to Succeeded.

Workaround: Wait for the reconciliation process to run a couple of times. If the work request is still in Failed state and the add-on is still in Needs Attention state after a couple of reconciliation runs, then investigate as described in "Add-on Reconciliation" in the Managing OKE Cluster Add-ons chapter of the *Oracle Private Cloud Appliance Kubernetes Engine (OKE)* guide.

Bug: 37967658

Version: 3.0.2

Create Cluster Does Not Support Extension Parameters

In Private Cloud Appliance Release 3.0.2-b1185392, some cluster control plane node properties are specified by using OraclePCA defined tags.

In the previous release, Private Cloud Appliance Release 3.0.2-b1081557, these defined tags are not recognized. You must use free-form tags to specify these values.

Workaround: In Private Cloud Appliance Release 3.0.2-b1081557, use free-form tags to provide the following information for control plane nodes:

- Your public SSH key.

  Specify `sshkey` for the tag key. Paste your public SSH key into the Value field.

  > **Important**
  >
  > You cannot add an SSH key after the cluster is created.

- Number of nodes.

  By default, the number of nodes in the control plane is 3. You can specify 1, 3, or 5 nodes. To specify the number of control plane nodes, specify `cp_node_count` for the tag key, and enter 1, 3, or 5 in the Value field.

- Node shape.

  For Private Cloud Appliance X10 systems, the shape of the control plane nodes is VM.PCAStandard.E5.Flex and you cannot change it. For all other Private Cloud Appliance systems, the default shape is VM.PCAStandard1.1, and you can specify a different shape.

  To use a different shape, specify `cp_node_shape` for the tag key, and enter the name of the shape in the Value field. For a description of each shape, see Compute Shapes in the *Oracle Private Cloud Appliance Concepts Guide*.

- Node shape configuration.

  If you specify a shape that is not a flexible shape, do not specify a shape configuration. The number of OCPUs and amount of memory are set to the values shown for this shape in "Standard Shapes" in Compute Shapes in the *Oracle Private Cloud Appliance Concepts Guide*.

  If you specify a flexible shape, you can change the default shape configuration.

  To provide shape configuration information, specify `cp_node_shape_config` for the tag key. You must specify the number of OCPUs (`ocpus`) you want. You can optionally specify the total amount of memory you want (`memoryInGBs`). The default value for gigabytes of memory is 16 times the number you specify for OCPUs.

  The following are examples of node shape configuration values. Enter everything, including the surrounding single quotation marks, in the Value field for the tag. In the first example, the default amount of memory will be configured.

  ```
  '{"ocpus":1}'
  '{"ocpus":2, "memoryInGBs":24}'
  ```

Bug: 36979754

Version: 3.0.2

Nodes in Failing State After Upgrade or Patch

Upgrade or patch of an appliance that has OKE clusters with node pools can cause some nodes to move into the `FAILING` state even though the underlying compute instance is in the `RUNNING` state.

If you experience this issue, perform the following workaround.

Workaround: Use the following method to replace the failed nodes with new active nodes, automatically transferring workloads from the failed nodes to the new nodes.

Delete the nodes that are in state `FAILING` or `FAILED`. Do *not* increase the size of the node pool (do not scale up the node pool).

The deleted nodes are cordoned and drained and their workloads are automatically transferred to the new nodes that are created to keep the node pool at the same size.

See also [PCA 3.x] Node Pool Nodes in Failing State Post Upgrade/Patching from 302M3.8 to 302M3.9 (Doc ID 3035508.1).

Bug: 36814183

Version: 3.0.2

OKE Requires Switch Firmware Upgrade on Systems with Administration Network

If your Private Cloud Appliance is configured with a separate administration network, the appliance and data center networking need reconfiguration to enable the traffic flows required by the Oracle Private Cloud Appliance Kubernetes Engine (OKE). In addition, the reconfiguration of the network is dependent on functionality included in a new version of the switch software.

Workaround: Upgrade or patch the software of the switches in your appliance. Reconfigure the network. You can find details and instructions in the following documentation sections:

- "Upgrading the Switch Software" in the Oracle Private Cloud Appliance Upgrade Guide
- "Patching the Switch Software" in the Oracle Private Cloud Appliance Patching Guide
- "Securing the Network" in the Oracle Private Cloud Appliance Security Guide

  This section includes a port matrix for systems with a separate administration network. Use it to configure routing and firewall rules, so the required traffic is enabled in a secure way.

Bug: 36073167

Version: 3.0.2

GPU Shapes Must Not Be Selected for Creating Node Pool

On a system that includes nodes with GPUs installed, when you create an OKE node pool, it is possible to select a GPU shape. The operation will succeed, but the OKE cluster is unable to use GPUs because the compute images have no drivers for them. GPU shapes provide access to scarce and expensive resources, which are intended for dedicated workloads on regular compute instances.

Workaround: When creating an OKE node pool you must always select a standard or flexible shape.

Bug: 37576565

Version: 3.0.2

Previously Used Image Is No Longer Listed

The Compute Web UI and the `compute image list` command list only the three most recently published versions of each major distribution (for example, Oracle Linux 9) of an image. If an upgrade or patch delivers an updated version of an OKE node image, for example the same image with a newer Kubernetes version, and that major distribution image had already been delivered three times, the fourth most recently published version of that image will no longer be listed.

Previously delivered images are still accessible, even though they are not listed.

Workaround: To use an image that you have used before but is no longer listed, use the OCI CLI to create the node pool, and specify the OCID of the image. To get the OCID of the image you want, use the `ce node-pool get` command for a node pool where you used this image before.

Bug: 36862970

Version: 3.0.2

Tag Filters Not Available for Kubernetes Node Pools and Nodes

Unlike Oracle Cloud Infrastructure, Private Cloud Appliance currently does not provide the functionality to use Tag Filters for tables listing Kubernetes node pools and nodes. Tag filtering is available for Kubernetes clusters.

Workaround: There is no workaround. The UI does not provide the tag filters in question.

Bug: 36091835

Version: 3.0.2

OKE-Specific Tags Must Not Be Deleted

Certain properties and functions of OKE are enabled through resource tags. These reserved tags are not created by the IAM service, but by users who apply them to resources. Therefore, the IAM service cannot prevent users from deleting such tags. If they are deleted, the OKE service might not work as expected.

Workaround: Do not attempt to delete the resource tags used for specific OKE service functionality. If you delete these tags, you must create them again.

Bug: 37157933

Version: 3.0.2

Unable to Delete an OKE Cluster in Failed State

To deploy a cluster, Oracle Private Cloud Appliance Kubernetes Engine (OKE) uses various types of cloud resources that can also be managed through other infrastructure services, such as compute instances and load balancers. However, OKE cluster resources must be manipulated only through the OKE service, to avoid inconsistencies. If the network load balancer of an OKE cluster is deleted outside the control of the OKE service, that cluster ends up in a failed state and you will no longer be able to delete it.

Workaround: This is a known issue with the Cluster API Provider. If a cluster is in failed state and its network load balancer is no longer present, it must be cleaned up manually. Contact Oracle for assistance.

Bug: 36193835

Version: 3.0.2

UI and CLI Represent Eviction Grace Period Differently

The minimum and default grace period before a node is evicted from a worker node pool is 20 seconds. The OCI CLI displays this value accurately and allows you to modify the grace period in seconds or minutes, using the ISO8601 format. For example, you could change the default of 20 seconds (="PT20S") to 3 minutes (="PT3M") by specifying a new value in the `--node-eviction-node-pool-settings` command parameter.

In contrast, the Compute Web UI parses the ISO8601 time format into an integer value and displays the eviction grace period in minutes. As a result, the 20 second default appears as 0 minutes in the Node Pool Information tab of the Kubernetes Cluster detail page.

This behavior differs from the Oracle Cloud Infrastructure console (UI), which is capable of displaying time in minutes as a decimal value (for example: 0.35 minutes). It has no minimum grace period, so zero is a valid entry.

Workaround: To set or check the precise eviction grace period of a node pool, use the OCI CLI and specify time in the ISO8601 format. When using the Compute Web UI, consider the limitations described.

Bug: 36696595

Version: 3.0.2

Nodes in Node Pool Not Automatically Distributed Across Fault Domains

When you create an OKE node pool without selecting specific fault domains, the Compute service handles distribution of the nodes across the fault domains. By design, node pool nodes (and compute instances in general) are assigned to the compute nodes with the highest available resource capacity. Due to VM activity and differences in resource consumption, the load between the three fault domains might vary considerably. Therefore, the auto-distribution logic cannot guarantee that nodes of the same node pool are spread evenly across fault domains. In fact, all nodes might end up in the same fault domain, which is not preferred.

Workaround: For the best distribution of node pool nodes across fault domains, do not rely on auto-distribution. Instead, select the fault domains to use when creating the node pool.

Bug: 36901742

Version: 3.0.2

API Reference on Appliance Not Up-to-Date for OKE Service

Every Private Cloud Appliance provides online API reference pages, conveniently accessible from your browser. For the Compute Enclave, these pages are located at https://

console.*mypca.mydomain*/api-reference. This API reference is not current for all services, including for Oracle Private Cloud Appliance Kubernetes Engine (OKE).

Workaround: The REST API for Oracle Private Cloud Appliance Compute Enclave shows up-to-date parameters and values in the descriptions of the CreateCluster and CreateNodePool operations.

> **Note**
>
> Both the console `api-reference` and the Oracle Help Center REST API for Oracle Private Cloud Appliance Compute Enclave show parameters and parameter values that are not supported because they do not apply to Private Cloud Appliance. If you use these, you might receive a not supported error message, or the parameter or value will accepted by the API but will do nothing.

Bug: 35710716, 36852746

Version: 3.0.2

OKE Cluster Creation Fails

OKE cluster creation might fail if the system is configured with a domain name that contains uppercase characters. Uppercase characters are not supported in domain names.

Workaround: Contact Oracle Support.

Bug: 36611385

Version: 3.0.2

Review Page for OKE Cluster Creation with VCN-Native Pod Networking Displays Wrong Pod CIDR

You can create OKE clusters with VCN-Native Pod Networking, so that pods use IP addresses from the VCN range, which provides more flexible control of network traffic. However, the review page, which is displayed in the UI before you submit the new cluster configuration, shows the default Flannel Overlay subnet as the Pods CIDR Block. This information is incorrect, but it does not affect the actual cluster network configuration.

Workaround: This is a data display error. It is harmless and can be ignored.

Bug: 37815929

Version: 3.0.2

Service of Type LoadBalancer Stuck in Pending State

Allowing connections from outside Private Cloud Appliance to a containerized application requires an external load balancer. You set it up as a Kubernetes service of type *LoadBalancer*. However, if the manifest file to create the load balancer service does not explicitly disable security list management, the load balancer gets stuck in *Pending* state.

Workaround: When creating the service of type LoadBalancer to expose a containerized application outside the Private Cloud Appliance environment, ensure that the manifest file contains an annotation that sets the security list management mode to *None*. For example:

```
apiVersion: v1
kind: Service
metadata:
  name: my-nginx-svc
  labels:
    app: nginx
  annotations:
    oci.oraclecloud.com/load-balancer-type: "lb"
    service.beta.kubernetes.io/oci-load-balancer-shape: "400Mbps"
    service.beta.kubernetes.io/oci-load-balancer-security-list-management-mode: None
spec:
  type: LoadBalancer
  ports:
   - port: 80
  selector:
    app: nginx
```

Bug: 37199903

Version: 3.0.2

Node Cycling Operation Times Out for Large Pools

Node cycling in OKE node pools of more than 30 nodes sometimes ends with a timeout. This is likely caused by intermittent Cluster API Provider connection issues. If a timeout occurs during node cycling, some of the nodes might not have completed the process, and are left in a state that does not match the latest specification.

Workaround: Manually delete the nodes that do not match the specification, and scale the cluster up again to the required number of nodes.

1. To identify nodes that were not cycled, list the nodes by creation timestamp. Cycled nodes are typically only minutes old, while uncycled nodes will be the oldest in the list.

   ```
   kubectl get nodes --sort-by=.metadata.creationTimestamp --kubeconfig
   <your_cluster.kubeconfig>
   ```

2. Cordon and drain the uncycled nodes in case of existing application deployments. Ensure that the nodes have been drained before you proceed.
3. Log in to one of the management nodes and manually delete the uncycled nodes by deleting the corresponding Machine.

   ```
   kubectl delete Machine <node_name> -n oke
   ```

   As a result, a new node with updated settings is created.

Bug: 37145441

Version: 3.0.2

Serviceability Issues

This section describes known issues and workarounds related to service, support, upgrade and data protection features.

Order of Upgrading Components Has Changed

When updating the platform, **you must update the compute nodes first.** Failing to update the compute nodes in this order can cause the upgrade to fail and disrupt the system.

Workaround: Complete platform upgrades in this order:

1. Compute Nodes
2. Management Nodes
3. Management Node Operating System
4. MySQL Cluster Database
5. Secret Service
6. Component Firmware
7. Kubernetes Cluster
8. Microservices

Bug: 34358305

Version: 3.0.1

DR Configurations Are Not Automatically Refreshed for Terminated Instances

If you terminate an instance that is part of a DR configuration, then a switchover or failover operation will fail due to the terminated instance. The correct procedure is to remove the instance from the DR configuration first, and then terminate the instance. If you forget to remove the instance first, you must refresh the DR configuration manually so that the entry for the terminated instance is removed. Keeping the DR configurations in sync with the state of their associated resources is critical in protecting against data loss.

Workaround: This behavior is expected. Either remove the instance from the DR configuration before terminating, or refresh the DR configuration if you terminated the instance without removing it first.

Bug: 33265549

Version: 3.0.1

Rebooting a Management Node while the Cluster State is Unhealthy Causes Platform Integrity Issues

Rebooting the management nodes is a delicate procedure because it requires many internal interdependent operations to be executed in a controlled manner, with accurate timing and often in a specific order. If a management node fails to reboot correctly and rejoin the cluster, it can lead to a destabilization of the appliance platform and infrastructure services. Symptoms include: microservice pods in *CrashLoopBackOff* state, data conflicts between MySQL cluster nodes, repeated restarts of the NDB cluster daemon process, and so on.

Workaround: Before rebooting a management node, always verify that the MySQL cluster is in a healthy state. From the management node command line, run the command shown in the example below. If your output does not look similar and indicates a cluster issue, you should power-cycle the affected management node through its ILOM using the `restart /System` command.

As a precaution, if you need to reboot all the management nodes – for example in a full management cluster upgrade scenario –, observe an interval of at least 10 minutes between two management node reboot operations.

```
# ndb_mgm -e show
Connected to Management Server at: pcamn01:1186
Cluster Configuration
---------------------
[ndbd(NDB)]     3 node(s)
id=17   @253.255.0.33  (mysql-8.0.25 ndb-8.0.25, Nodegroup: 0)
id=18   @253.255.0.34  (mysql-8.0.25 ndb-8.0.25, Nodegroup: 0, *)
id=19   @253.255.0.35  (mysql-8.0.25 ndb-8.0.25, Nodegroup: 0)

[ndb_mgmd(MGM)] 3 node(s)
id=1    @253.255.0.33  (mysql-8.0.25 ndb-8.0.25)
id=2    @253.255.0.34  (mysql-8.0.25 ndb-8.0.25)
id=3    @253.255.0.35  (mysql-8.0.25 ndb-8.0.25)

[mysqld(API)]   18 node(s)
id=33   @253.255.0.33  (mysql-8.0.25 ndb-8.0.25)
id=34   @253.255.0.33  (mysql-8.0.25 ndb-8.0.25)
[...]
```

Bug: 34484128

Version: 3.0.2

ULN Mirror Is Not a Required Parameter for Compute Node Patching

In the current implementation of the patching functionality, the ULN field is required for all patch requests. The administrator uses this field to provide the URL to the ULN mirror that is set up inside the data center network. However, compute nodes are patched in a slightly different way, in the sense that patches are applied from an secondary, internal ULN mirror on the shared storage of the management nodes. As a result, the ULN URL is technically not required to patch a compute node, but the patching code does consider it a mandatory parameter, so it must be entered.

Workaround: When patching a compute node, include the URL to the data center ULN mirror as a parameter in your patch request. Regardless of the URL provided, the secondary ULN mirror accessible from the management nodes is used to perform the patching.

Bug: 33730639

Version: 3.0.1

Patch Command Times Out for Network Controller

When patching the platform, the process may fail due to a time-out while updating the network controller. If this is the case, logs will contain entries like "ERROR [pcanwctl upgrade Failed]".

Workaround: Execute the same patch command again. The operation should succeed.

Bug: 33963876

Version: 3.0.1

Low Transfer Speed when Downloading ISO Image for Appliance Upgrade

During preparation of an appliance software upgrade, you might observe very low transfer speeds while the ISO image is being downloaded to the appliance internal storage. If the download is expected to take many hours to complete, it is likely that the spine switches are performing a very high number of translations. It indicates that the spine switches need to be reloaded.

In addition, on systems running appliance software versions 3.0.2-b1081557 - 3.0.2-b1325160 where active Kubernetes Engine clusters are present, the OKE network load balancer might be unreachable.

Workaround: Contact Oracle for assistance. Instructions will be provided to check the NAT statistics and reload the switches.

When upgrading the appliance software to the latest version, switches are reloaded during the preparation phase. From this point forward the workaround should no longer be required.

Bug: 37807342

Version: 3.0.2

Switch Upgrade or Patch Procedure Not Blocked When Ports Are Down

The spine and leaf switches are configured in pairs for high availability (HA), and new firmware is installed through a rolling upgrade or patch operation, which is launched with a single command. If certain ports in a switch are down, the HA configuration is impacted, and the upgrade or patch operation causes a brief outage while the new firmware is installed. There is no check in place to block upgrade and patch commands when switch ports are down. Connectivity is restored, but the inactive switch ports must be fixed to reenable HA.

Workaround: Before upgrading or patching the leaf and spine switches, ensure that all necessary ports on all devices are active. Verify switch status in Grafana. If unhealthy ports are detected, ensure that this issue is fixed first. Unavailable switch ports must be fixed so the high-availability configuration of the switch pair(s) can be restored.

Bug: 37049316

Version: 3.0.1

Upgrade Oracle Cloud Infrastructure Images Fails Waiting for Response from Workflow Service

Upgrade procedures consist of many tasks, which are orchestrated through the Upgrader Workflow Service (UWS). During the upgrade of the Oracle Cloud Infrastructure images on the appliance, the UWS might fail to send a response and cause the upgrade workflow to time out. The Upgrader log records the issue as follows:

```
[2025-05-21 19:38:57 1393662] ERROR (util_tasks:306) [Waiting for UWS response (Waiting
for a response from UWS)] Failed
Did not receive a response from UWS, manually import with 'importPlatformImages' command
[2025-05-21 19:38:58 1393662] INFO (util_tasks:310) [UpgradePlanUpdateTask (None)] Not
Run
Task did not run. This task only runs when OciConfigurationTask's upgrade is True AND
Upgrade OCI Instance images has status of Passed.
[2025-05-21 19:38:58 1393662] INFO (oci_configuration:52) Component='ociImages',
path='None', upgrade-required=True, upgrade-plan=True
```

Workaround: Retry the images upgrade from the Service Web UI or Service CLI. The upgrade is expected to complete successfully at the next attempt.

Bug: 37984531

Version: 3.0.2

Upgrade Fails Due to Incomplete Backup Job

When upgrading the appliance software, the platform upgrade stage might fail because an internal backup does not complete successfully before a timeout occurs. When this happens, command output includes:

```
[2025-02-09 01:59:43 5321] INFO (util_tasks:1773) Waiting for BRS cronjob Upgrade to
finish processing.
[2025-02-09 01:59:43 5321] ERROR (util_tasks:306) [BRS cronjob Upgrade (Recreate BRS
cronjob)] Failed
```

Logs contain details similar to this example:

```
Tasks 64 - Name = BRS cronjob Upgrade
Tasks 64 - Message = Command: ['kubectl', '-n', 'default', 'exec',
'brs-76c968c746-58gm4', '-c', 'brs', '--', '/usr/sbin/default-backup'] failed (255):
stderr: time="2025-02-09T01:47:59Z" level=error msg="exec failed: unable to start
container process: error adding pid 76969 to cgroups: failed to write 76969:
openat2 /sys/fs/cgroup/systemd/kubepods.slice/kubepods-burstable.slice/kubepods-
burstable-pod4a3334cf_a8fd_4608_a709_3a6703c6627c.slice/crio-
d97e021a3b22d8d805b8fcede91266f59fb177002fab108d3f34affd43858d95.scope/cgroup.procs: no
such file or directory"
command terminated with exit code 255
```

Workaround: Log in to a management node. Delete the pod that controls the backup (BRS service) cronjob. A new pod is launched automatically.

```
# kubectl delete pod brs-76c968c746-58gm4
pod "brs-76c968c746-58gm4" deleted

# kubectl get pods -A | grep brs
default                   brs-76c968c746-kcdnh           3/3     Running    0        47s

# kubectl exec -it brs-76c968c746-kcdnh -c brs -- /usr/sbin/default-backup
# echo $?
0
```

Bug: 37572149

Version: 3.0.2

IAM Service Reports Sync Status Error After Upgrade Preparation Commands

During the preparation phase of an appliance software upgrade, the latest Upgrader functionality is added to the running system. The Admin Service is a required component in this process, which is already updated when the `preUpgrade` command is run. This causes a temporary version mismatch between the IAM Service and the Admin Service, with which it is tightly integrated.

New Admin API calls to IAM might fail until the corresponding version of the IAM Service is available on the system, as illustrated by this Service CLI example:

```
PCA-ADMIN> show iamservice
Data:
 Id = 66acfdd4-aa4e-4bda-ba9d-001d67fccf96
 Type = IamService
 IAM Link Mode = AUTO_SYNC
 Overall Communication State = Error
 Communication Error Message = Error processing iam.syncstatus.get response:
PCA_GENERAL_000014: Error returned from IAM service. Code: 'NotSupportedError'. Message:
'Not Supported'
 Name = Iam Service
 Work State = Normal
 FaultIds 1 = id:f021e0a9-11b5-4483-a077-7a62049e637b type:Fault
name:IamServiceSyncStatusFaultStatusFault(Iam Service)
```

Workaround: The error message suggests there is a sync issue with the IAM Service, but in fact all internal operations are proceeding as expected. The IAM Service is up-to-date when the platform and containerized microservices upgrade steps are completed, after which the error disappears. No workaround is required.

Bug: 37775091

Version: 3.0.2

Instances with a Shared Block Volume Cannot Be Part of Different Disaster Recovery Configurations

Multiple instances can have a block volume attached that is shared between them. If you add those instances to a disaster recovery (DR) configuration, their attached volumes are moved to a dedicated ZFS storage project. However, if the instances belong to different DR configurations, each one with its own separate ZFS storage project, the system cannot move any shared block volume as this always results in an invalid DR configuration. Therefore, the Disaster Recovery service does not support adding compute instances with shared block volumes to different DR configurations.

Workaround: Consider including instances with a shared block volume in the same DR configuration, or attaching different block volumes to each instance instead of a shared volume.

Bug: 34566745

Version: 3.0.2

DR Failover Error Because Initiator Group No Longer Exists

In the Native Disaster Recovery service, a failover plan is meant to be used when the primary system is down. However, the service does not prevent an administrator performing a failover while the primary system is up and running. During a failover, to be able to perform role reversal between primary and standby, the DR service changes the LUN information in the replicated data stored on the standby system's ZFS Storage Appliance. If the primary system is online, it sends replication updates every 5 minutes, which will revert those changes made to the LUN parameters on the standby. This causes role reversal to fail with an error similar to this example:

```
The initiator group '225fc1ba7c38_grp' no longer exists. It may have been destroyed or
renamed by another administrator, or this LUN may have been imported from another system.
```

Workaround: Do not perform a failover when the primary system is online. Use switchover instead.

If you do run into this failover error, the recovery procedure involves changes on the ZFS Storage Appliance. Contact Oracle for assistance.

Bug: 37988746

Version: 3.0.2

Time-out Occurs when Generating Support Bundle

When you request assistance from Oracle Support, it is usually required to upload a support bundle with your request. A support bundle is generated from a management node using a command similar to this example:

```
# support-bundles -m time_slice --all -s 2022-01-01T00:00:00.000Z -e
2022-01-02T00:00:00.000Z
```

If there is a very large number of log entries to be collected for the specified time slice, the process could time out with API exception and an error message that says "*unable to execute command*". In actual fact, the data collection will continue in the background, but the error is caused by a time-out of the websocket connection to the Kubernetes pod running the data collection process.

Workaround: If you encounter this time-out issue when collecting data for a support bundle, try specifying a shorter time slice to reduce the amount of data collected. If the process completes within 30 minutes the error should not occur.

Bug: 33749450

Version: 3.0.2

DR Operations Intermittently Fail

During certain conditions of heavy load, Site Guard users performing DR operations on the Private Cloud Appliance 3.0 can encounter out-of-session errors when Site Guard EM scripts attempt to perform DR operations using the PCA DR REST API.

This condition occurs when the system is overloaded with requests.

Workaround: Retry the operation.

Bug: 33934952

Version: 3.0.1, 3.0.2

MN01 Host Upgrade Fails When it is the Last Management Node to Upgrade

Upgrades and patches to the management nodes are performed in a sequential order. When `MN01` falls last in that order, the management node upgrade or patch operation fails. To avoid this issue, ensure that the Management Node Virtual IP address is assigned to `MN02` before you start any management node upgrade or patching operations.

Workaround: Assign the Management Note Virtual IP address to `MN02` before you upgrade or patch.

```
# pcs resource move mgmt-rg pcamn02
```

Bug: 35554754

Version: 3.0.2

Failure Draining Node when Patching or Upgrading the Kubernetes Cluster

To avoid that microservice pods go into an inappropriate state, each Kubernetes node is drained before being upgraded to the next available version. The Upgrader allows all pods to be evicted gracefully before proceeding with the node. However, if a pod is stuck or is not evicted in time, the upgrade or patch process stops.

Workaround: If a Kubernetes node cannot be drained because a pod is not evicted, you must manually evict the pod that causes the failure.

1. Log on to the Kubernetes node using ssh, and run the following command, using the appropriate host name:

   ```
   # kubectl drain pcamn00 --ignore-daemonsets --delete-local-data
   ```

   Wait for the draining to complete. The command output should indicate: `node/pcamn00 drained`.

2. If the drain command fails, the output indicates which pod is causing the failure. Either run the drain command again and add the `--force` option, or use the delete command.

   ```
   # kubectl delete pod pod-name --force
   ```

   For example:

   ```
   # kubectl delete pod pod-name --force
   ```

3. Rerun the Kubernetes upgrade or patch command. The Upgrader continues from where the process was interrupted.

Bug: 37291231

Version: 3.0.2

Oracle Auto Service Request Disabled after Upgrade

When a Private Cloud Appliance has been registered for Oracle Auto Service Request (ASR), and the service is enabled on the appliance, the ASR service may become disabled after an upgrade of the appliance software. The issue has been observed when upgrading to version 3.0.2-b925538.

Workaround: After the appliance software upgrade, verify the ASR configuration. If the ASR service is disabled, manually enable it again. See "Using Auto Service Requests" in the Status and Health Monitoring chapter of the Oracle Private Cloud Appliance Administrator Guide.

Bug: 35704133

Version: 3.0.2

Compute Node in `NotReady` State Blocks Upgrade or Patching

A known Linux issue may cause a compute node to block patching or upgrade. This issue occurs after a compute node is upgraded and rebooted. The node reboots to a `NotReady` state which prevents further patching or upgrading.

Workaround: Reboot the impacted compute node and continue with the upgrade or patch.

Bug: 36835607

Version: 3.0.2

Site Guard Precheck Jobs Fail

When Site Guard users perform DR prechecks, the prechecks might fail with an error:

```
"Incorrect hostname found in DNS for local IP nn.nn.nnn.nnn"
```

This error occurs when the domain name contains uppercase letters. Uppercase characters are not supported in domain names.

Workaround: Contact Oracle Support.

Bug: 36710199

Version: 3.0.2

Instance Migration Fails During Appliance Upgrade

When upgrading Private Cloud Appliance to software version 3.0.2-b1325160, instances might fail to migrate to another compute node. Rollback causes affected instances to return to their original host compute node, which interrupts active workloads. The issue is caused by competing commands and time-outs during statistics collection at the level of the hypervisor.

As part of this particular version upgrade, `vmstats-exporter` is uninstalled during the preparation phase, and reinstalled during platform upgrade. Until that time, VM stats show `NO DATA`.

Workaround: When the upgrade to version 3.0.2-b1325160 is complete, the issue is resolved.

Bug: 36936775

Version: 3.0.2

Restore NTP Configuration After Upgrade To PCA Version: PCA:3.0.2-b1392231

After an upgrade to software version: 3.0.2-b1392231, time synchronization across nodes is lost, which eventually results in cluster and certificate validation failures.

This issue is fixed in fixed in software version: 3.0.2-b1410505

Workaround: For the workaround see [PCA 3.x] Restore NTP Configuration After Upgrade To PCA Version: PCA:3.0.2-b1392231 (M3.11) (Doc ID 3089503.1).

Bug: 38035199

Version: 3.0.2

DR Configurations Are Not Supported Between Different Private Cloud Appliance Platforms

DR configurations are only supported when the DR connection is between two Private Cloud Appliances of the same platform. For example, a Private Cloud Appliance X9 rack can only be configured for DR with another Private Cloud Appliance X9 rack.

Workaround: Only create a DR configuration between two Private Cloud Appliance racks of the same platform: X9 to X9, X10 to X10, X11 to X11.

Bug: 38111294

Version: 3.0.1