Oracle® Cloud Native Environment

Release Notes for Release 1.2

F40896-06
November 2021

Oracle Legal Notices

Table of Contents

Preface

This document contains information about Oracle Cloud Native Environment. This document includes information on component versions, new features, documentation changes and known issues for Oracle Cloud Native Environment.

Document generated on: 2021-11-17 (revision: 1158)

Audience

This document is written for system administrators and developers who want to use Oracle Cloud Native Environment. It is assumed that readers have a general understanding of the Oracle Linux operating system and container concepts.

Related Documents

The latest version of this document and other documentation for this product are available at:

https://docs.oracle.com/en/operating-systems/olcne/

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.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

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.

Chapter 1 Component Versions

This section lists the version numbers of the major components included with Oracle Cloud Native Environment.

To see the version of the packages, use the `rpm -q` command, for example:

```
rpm -q olcne-api-server
olcne-api-server-1.2.x-x.el7.x86_64
```

Table 1.1 Oracle Cloud Native Environment Component Versions

Component	Release 1.0	Release 1.1	Release 1.2
Oracle Cloud Native Environment Platform API Server	1.0	1.1	1.2
Oracle Cloud Native Environment Platform Agent	1.0	1.1	1.2
Oracle Cloud Native Environment Platform Command-Line Interface	1.0	1.1	1.2
Kubernetes	1.14.9	1.17.9	1.18.18
RunC	1.0	1.0	1.0
CRI-O	1.14	1.17.0	1.18.4
Kata Containers	1.7.3	1.7.3	1.11.5
NGINX	1.17.7	1.17.7	1.17.7
Helm	—	3.1.1	3.3.4
Prometheus	—	2.13.1	2.21.0
Istio	—	1.4.10	1.9.8
Grafana	—	6.7.4	7.2.1

Chapter 2 CVE and Bug Fix Updates

Notices for Common Vulnerabilities and Exposures (CVEs) and bug fix updates for Oracle Cloud Native Environment are available on the Unbreakable Linux Network at:

https://linux.oracle.com/errata

You can subscribe to the `el-errata@oss.oracle.com` email list to receive these notices via email at:

https://oss.oracle.com/mailman/listinfo/el-errata

This document includes a list of the CVE and bug fix updates up to and including Oracle Cloud Native Environment Release 1.1.5 and Release 1.0.7. All update notices after these releases are listed on ULN and via the email list mentioned, and are not included in this document.

You may also find it helpful to check the list of new and updated packages posted on the Oracle Linux yum server available at:

https://yum.oracle.com/whatsnew.html

Chapter 3 New Features and Notable Changes

This chapter lists the new features and notable changes in each Oracle Cloud Native Environment release, including the major components delivered with Oracle Cloud Native Environment, such as Kubernetes.

3.1 Oracle Cloud Native Environment Changes

This section lists the changes made in each release of Oracle Cloud Native Environment.

3.1.1 Release 1.2.5

This section lists the notable changes in Release 1.2.5 of Oracle Cloud Native Environment.

The following components have been updated:

Istio Updated: Istio is updated to Release 1.9.8.

3.1.2 Release 1.2.4

This section lists the notable changes in Release 1.2.4 of Oracle Cloud Native Environment.

IP Masquerading: Setting IP masquerading is no longer required on Oracle Linux 7 control plane or worker nodes. IP masquerading is still required for Release 1.2.3 or earlier installations on Oracle Linux 7. IP masquerading configuration instructions have been removed from *Updates and Upgrades* as all upgrades should be made to the latest 1.2 release, which no longer requires this to be set.

The following components have been updated:

Istio Updated: Istio is updated to Release 1.9.6.

Prometheus Updated: Prometheus is updated to Release 2.21.0.

Grafana Updated: Grafana is updated to Release 7.2.1.

3.1.3 Release 1.2.2

This section lists the notable changes in Release 1.2.2 of Oracle Cloud Native Environment.

`externalIPs` Validation: The `olcnectl module create` and `olcnectl module update` commands are improved by adding options to set access to `externalIPs` in Kubernetes services.

For information on setting access to `externalIPs` in Kubernetes services, see *Container Orchestration*.

3.1.4 Release 1.2.0

This section lists the notable changes in Release 1.2.0 of Oracle Cloud Native Environment.

Oracle Linux 8: Oracle Cloud Native Environment can be installed on hosts running Oracle Linux 8 (x86_64) with the Unbreakable Enterprise Kernel Release 6 (UEK R6). A minimum of Oracle Linux 8.3 is required.

Installation Change: A new ULN channel (`ol7_x86_64_olcne12`) and a new Oracle Linux yum server repository (`ol7_olcne12`) are available for installing the Oracle Cloud Native Environment Release 1.2

packages on Oracle Linux 7. Use this new channel or repository to install or upgrade to Release 1.2 on Oracle Linux 7.

A new ULN channel (`ol8_x86_64_olcne12`) and a new Oracle Linux yum server repository (`ol8_olcne12`) are available for installing the Oracle Cloud Native Environment Release 1.2 packages on Oracle Linux 8. Use this new channel or repository to install Release 1.2 on Oracle Linux 8.

For information on setting up the ULN channel or Oracle Linux yum server repository, see *Getting Started*.

Network Interface for Kubernetes Data Plane: The `olcnectl module create` command is enhanced with a new `--pod-network-iface` option to optionally set the network interface to use for the Kubernetes data plane. For information about using the `olcnectl module create` command to create a Kubernetes cluster and setting the network interface for the data plane, see *Container Orchestration*.

SELinux: The `olcnectl module create` and `olcnectl module update` commands are improved by adding a new `--selinux` option to enable setting the SELinux mode for nodes in a cluster. You can set SELinux to either `enforcing` or `permissive` mode when you create a Kubernetes module, or change the setting after a Kubernetes module has been installed. For more information on setting up SELinux, see *Getting Started*.

TLS Configuration for Platform Agent and Platform API Server: The `olcnectl` command is improved by adding new global options to set TLS configuration for the Platform Agent and Platform API Server. The new global options for the `olcnectl` command are:

- `--olcne-tls-cipher-suites`
- `--olcne-tls-max-version`
- `--olcne-tls-min-version`

For more information on the new global options, see *Platform Command-Line Interface*.

TLS Configuration for the Kubernetes module: The `olcnectl module create` command is improved by adding new options to set TLS configuration for the Kubernetes module. The new options for the `olcnectl module create` command are:

- `--kube-tls-cipher-suites`
- `--kube-tls-min-version`

For more information on the new `olcnectl module create` options, see *Platform Command-Line Interface*.

Deprecated Platform CLI Option: The `apiserver-advertise-address` option in the `olcnectl module create` command is deprecated. This option set the IP address on which to advertise the Kubernetes API server to members of the Kubernetes cluster in a non-HA cluster, with a single control plane node. The `--master-node` option specifies the IP address and this deprecated option is no longer used.

3.1.5 Release 1.1.10

This section lists the notable changes in Release 1.1.10 of Oracle Cloud Native Environment.

`externalIPs` Validation: The `olcnectl module create` and `olcnectl module update` commands are improved by adding options to set access to `externalIPs` in Kubernetes services.

For information on setting access to `externalIPs` in Kubernetes services, see *Container Orchestration*.

3.1.6 Release 1.1.7

This section lists the notable changes in Release 1.1.7 of Oracle Cloud Native Environment.

Kernel Support: In addition to Unbreakable Enterprise Kernel Release 5, Unbreakable Enterprise Kernel Release 6 is now a supported kernel on Oracle Linux 7.

3.1.7 Release 1.1.6

This section lists the notable changes in Release 1.1.6 of Oracle Cloud Native Environment.

NGINX Load Balancer Updates: A new option is added to the Platform CLI to update the NGINX load balancer that can optionally be installed by the Platform CLI. A new `--nginx-image` option is included with the `olcnectl module update` command. This option is used to specify the location of the NGINX container image used to update NGINX on the control plane nodes.

For information about updating to this errata release, see *Updates and Upgrades*.

3.1.8 Release 1.1.5

This section lists the notable changes in Release 1.1.5 of Oracle Cloud Native Environment.

This release resolves CVE-2020-16845. This CVE relates to Go where it can have an infinite read loop in ReadUvarint and ReadVarint in encoding/binary via invalid inputs. The components updated for this are:

- **Platform API Server**: Updated to Release 1.1.5.
- **Platform Agent**: Updated to Release 1.1.5.
- **Platform CLI**: Updated to Release 1.1.5.
- **Kata Containers**: Security fixes have been back ported to Release 1.7.3.
- **CRI-O**: Security fixes have been back ported to Release 1.17.0.
- **Kubernetes**: Security fixes have been back ported to Release 1.17.9.
- **Istio**: Security fixes have been back ported to Release 1.14.10.
- **Helm**: Security fixes have been back ported to Release 3.1.1.
- **Prometheus**: Security fixes have been back ported to Release 2.13.1.
- **Grafana**: Security fixes have been back ported to Release 6.7.4.

The Platform API Server is also updated to include a fix for an issue related to the Kubernetes pod subnet flag (`--pod-cidr`) not being honored in the flannel configuration.

For information about updating to this errata release, see *Updates and Upgrades*.

3.1.9 Release 1.1.4

This section lists the notable changes in Release 1.1.4 of Oracle Cloud Native Environment.

Kata Containers Updated: Kata Containers is updated to resolve an issue where the Kata package had a hard coded dependency of a specific version of the `kernel-uek-container` package.

Kubernetes Updated: Kubernetes is updated to set the Kata version in the Kata meta-package.

Platform Agent Updated: The Platform Agent is updated to resolve an issue pulling container images using a proxy server. The Platform Agent now uses `crictl pull` instead of `podman pull` to pull container images.

CRI-O Updated: CRI-O is updated to resolve an issue with the default cni-plugins directory. This is now set to `/opt/cni/bin` instead of `/usr/libexec/cni`.

For information about updating to this errata release, see *Updates and Upgrades*.

3.1.10 Release 1.1.3

This section lists the notable changes in Release 1.1.3 of Oracle Cloud Native Environment.

Kubernetes Updated: Kubernetes is updated to resolve an issue where `kubeadm reset` does not unmount the root `/var/lib/kubelet` directory if it is mounted by the user.

For information about updating to this errata release, see *Updates and Upgrades*.

3.1.11 Release 1.1.2

This section lists the notable changes in Release 1.1.2 of Oracle Cloud Native Environment.

Kubernetes Updated: Kubernetes is updated to Release 1.17.9 to resolve the following CVEs.

- CVE-2020-8559. This CVE relates to an issue where if an attacker is able to intercept certain requests to the kubelet, they can send a redirect response that may be followed by a client using the credentials from the original request. This can lead to compromise of other nodes.
- CVE-2020-8557. This CVE relates to an issue where the `/etc/hosts` file mounted in a pod by kubelet is not included by the kubelet eviction manager when calculating ephemeral storage usage by a pod. If a pod writes a large amount of data to the `/etc/hosts` file, it could fill the storage space of the node and cause the node to fail.

Istio Updated: Istio is updated to Release 1.4.10 to resolve the following CVEs.

- CVE-2020-1764. This CVE relates to a default `signing key` to install Kiali. This can allow an attacker with access to Kiali to bypass authentication and gain administrative privileges over Istio.
- CVE-2020-10739. This CVE relates to an issue when sending a specially crafted packet, an attacker could trigger a Null Pointer Exception resulting in a Denial of Service. This could be sent to the ingress gateway or a sidecar.
- CVE-2020-11080. This CVE relates to an issue when sending a specially crafted packet, an attacker could cause the CPU to spike at 100%. This could be sent to the ingress gateway or a sidecar.
- CVE-2020-15104. This CVE relates to an issue when validating TLS certificates, Envoy incorrectly allows wildcards in DNS Subject Alternative Name (SAN) to apply to multiple subdomains.

Kata Updated: Kata security fixes have been back ported to Release 1.7.3 to resolve the following CVEs.

- CVE-2020-2024. This CVE relates to an improper link resolution vulnerability when tearing down a container. A malicious guest could trick the kata-runtime into unmounting any mount point on the host and all mount points underneath it, potentiality resulting in a host Denial of Service.
- CVE-2020-2025. This CVE relates to persistent guest file system changes to the underlying image file on the host. A malicious guest could overwrite the image file to gain control of all subsequent guest virtual machines.
- CVE-2020-2026. This CVE relates to mounting the untrusted container file system on any host path. A malicious guest that is compromised before a container creation can trick the kata-runtime into mounting the untrusted container file system on any host path, potentially allowing for code execution on the host.

For information about updating to this errata release, see *Updates and Upgrades*.

3.1.12 Release 1.1.1

This section lists the notable changes in Release 1.1.1 of Oracle Cloud Native Environment.

Kubernetes Updated: Kubernetes is updated to Release 1.17.6 to resolve two CVEs.

- CVE-2020-8555. This CVE relates to a Server Side Request Forgery (SSRF) vulnerability in `kube-controller-manager`.
- CVE-2020-10749. This CVE relates to a man-in-the-middle vulnerability.

Grafana Updated: Grafana is updated to Release 6.7.4 to resolve CVE-2020-13379. This CVE relates to an incorrect access control issue in Grafana.

For information about updating to this errata release, see *Updates and Upgrades*.

3.1.13 Release 1.1.0

This section lists the notable changes in Release 1.1.0 of Oracle Cloud Native Environment.

- **Kubernetes Updated to 1.17**: Kubernetes 1.17 is the default release installed on nodes in a new cluster in Oracle Cloud Native Environment. Existing Kubernetes Release 1.14 deployments can be upgraded to Release 1.17. For information about upgrading to Release 1.1, see *Updates and Upgrades*.
- **Kubernetes Cluster Scaling**: The `olcnectl module update` command is enhanced so that you can now scale a Kubernetes cluster by either adding control plane and worker nodes to it or removing control plane and worker nodes from it. For information about using the `olcnectl module update` command to scale a Kubernetes cluster, see *Container Orchestration*.
- **Service Mesh**: A new module is available to deploy a service mesh to a Kubernetes cluster. The Istio module for Oracle Cloud Native Environment deploys a service mesh in Oracle Cloud Native Environment. Grafana is deployed as part of the service mesh. For information about deploying and using a service mesh, see *Service Mesh*. For information about using Grafana, see *Monitoring and Visualization*.
- **Firewall Changes**: Masquerading no longer needs to be enabled in the firewall on Kubernetes nodes. Instead, the `cni0` interface must be added to the trusted zone on nodes. For information on firewall and network requirements for Kubernetes nodes, see *Getting Started*.
- **Installation Change**: A new ULN channel (`ol7_x86_64_olcne11`) and a new Oracle Linux yum server repository (`ol7_olcne11`) are available for installing the Oracle Cloud Native Environment Release 1.1

packages. Use this new channel or repository to install or upgrade to Release 1.1. For information on setting up the ULN channel or Oracle Linux yum server repository, see *Getting Started*.

3.1.14 Release 1.0.9

This section lists the notable changes in Release 1.0.9 of Oracle Cloud Native Environment.

Kernel Support: In addition to Unbreakable Enterprise Kernel Release 5, Unbreakable Enterprise Kernel Release 6 is now a supported kernel on Oracle Linux 7.

3.1.15 Release 1.0.8

This section lists the notable changes in Release 1.0.8 of Oracle Cloud Native Environment.

NGINX Load Balancer Updates: A new option is added to the Platform CLI to update or upgrade the NGINX load balancer that can optionally be installed by the Platform CLI. A new `--nginx-image` option is included with the `olcnectl module update` command. This option is used to specify the location of the NGINX container image used to update or upgrade NGINX on the control plane nodes.

For information about updating to this errata release, see *Updates and Upgrades*.

3.1.16 Release 1.0.7

This section lists the notable changes in Release 1.0.7 of Oracle Cloud Native Environment.

This release resolves CVE-2020-16845. This CVE relates to Go where it can have an infinite read loop in ReadUvarint and ReadVarint in encoding/binary via invalid inputs. The components updated for this are:

- **Platform API Server**: Updated to Release 1.0.7.
- **Platform Agent**: Updated to Release 1.0.7.
- **Platform CLI**: Updated to Release 1.0.7.
- **Kata Containers**: Security fixes have been back ported to Release 1.7.3.
- **CRI-O**: Security fixes have been back ported to Release 1.14.7.
- **Kubernetes**: Security fixes have been back ported to Release 1.14.9.

The Platform API Server is also updated to include a fix for an issue related to the Kubernetes pod subnet flag (`--pod-cidr`) not being honored in the flannel configuration.

For information about updating to this errata release, see *Updates and Upgrades*.

3.1.17 Release 1.0.6

This section lists the notable changes in Release 1.0.6 of Oracle Cloud Native Environment.

Kata Containers Updated: Kata Containers is updated to resolve an issue where the Kata package had a hard coded dependency of a specific version of the `kernel-uek-container` package.

Kubernetes Updated: Kubernetes is updated to set the Kata version in the Kata meta-package.

For information about updating to this errata release, see *Updates and Upgrades*.

3.1.18 Release 1.0.5

This section lists the notable changes in Release 1.0.5 of Oracle Cloud Native Environment.

Kubernetes Updated: Kubernetes security fixes have been pack ported to Release 1.14.9 to resolve the following CVEs.

- CVE-2020-8559. This CVE relates to an issue where if an attacker is able to intercept certain requests to the kubelet, they can send a redirect response that may be followed by a client using the credentials from the original request. This can lead to compromise of other nodes.
- CVE-2020-8557. This CVE relates to an issue where the `/etc/hosts` file mounted in a pod by kubelet is not included by the kubelet eviction manager when calculating ephemeral storage usage by a pod. If a pod writes a large amount of data to the `/etc/hosts` file, it could fill the storage space of the node and cause the node to fail.

Kata Updated: Kata security fixes have been back ported to Release 1.7.3 to resolve the following CVEs.

- CVE-2020-2024. This CVE relates to an improper link resolution vulnerability when tearing down a container. A malicious guest could trick the kata-runtime into unmounting any mount point on the host and all mount points underneath it, potentiality resulting in a host Denial of Service.
- CVE-2020-2025. This CVE relates to persistent guest file system changes to the underlying image file on the host. A malicious guest could overwrite the image file to gain control of all subsequent guest virtual machines.
- CVE-2020-2026. This CVE relates to mounting the untrusted container file system on any host path. A malicious guest that is compromised before a container creation can trick the kata-runtime into mounting the untrusted container file system on any host path, potentially allowing for code execution on the host.

For information about updating to this errata release, see *Updates and Upgrades*.

3.1.19 Release 1.0.4

This section lists the notable changes in Release 1.0.4 of Oracle Cloud Native Environment.

Kubernetes Updated: Kubernetes is updated to Release 1.14.9 to resolve two CVEs.

- CVE-2020-8555. This CVE relates to a Server Side Request Forgery (SSRF) vulnerability in `kube-controller-manager`.
- CVE-2020-10749. This CVE relates to a man-in-the-middle vulnerability.

For information about updating to this errata release, see *Updates and Upgrades*.

3.1.20 Release 1.0.3

This section lists the notable changes in Release 1.0.3 of Oracle Cloud Native Environment.

Kubernetes Updated: Kubernetes is updated to Release 1.14.9 to resolve CVE-2019-11254. This CVE relates to a denial of service vulnerability in the kube-apiserver. For information about updating to this errata release, see *Updates and Upgrades*.

3.1.21 Release 1.0.2

This section lists the notable changes in Release 1.0.2 of Oracle Cloud Native Environment.

Kubernetes Updates: The `olcnectl module update` command failed to update the Kubernetes module for Oracle Cloud Native Environment. Running this command caused the Kubernetes cluster to become unstable. This issue is fixed in this release. If there are no Kubernetes module updates available, the cluster is not updated.

3.1.22 Release 1.0.1

This section lists the notable changes in Release 1.0.1 of Oracle Cloud Native Environment.

- **Oracle Cloud Native Environment Updates**: A procedure is added to the documentation to show how to update the Oracle Cloud Native Environment packages on each node. For information on updating the packages, see *Updates and Upgrades*.
- **Kubernetes Updates**: The `olcnectl module update` command is added to enable updates to the Kubernetes module. This command updates the Kubernetes release on each node in an environment.

  

  Important

  Make sure you update the Oracle Cloud Native Environment packages to Release 1.0.1 on each node before you update the Kubernetes module.

  For information on using the `olcnectl module update` command to update the Kubernetes release, see *Updates and Upgrades*.
- **Kubernetes Installation**: The `olcnectl module install` command is changed to automatically install the Kubernetes packages, and enable and start the `crio` and `kubelet` services. You no longer need to manually install the Kubernetes packages or enable and start these services before installing the Kubernetes module. For information on using the `olcnectl module install` command to install a Kubernetes module, see *Container Orchestration*.
- **Load Balancer Installation**: The `olcnectl module install` command used with the `--virtual-ip` option is changed to automatically deploy the load balancer that comes with Oracle Cloud Native Environment. As part of deploying the load balancer, NGINX and keepalived are installed on the control plane nodes, and the `olcne-nginx` and `keepalived` services are enabled and started. For information on creating a highly available Kubernetes cluster using the load balancer deployed by the Oracle Cloud Native Environment Platform Command-Line Interface, see *Container Orchestration*.

3.2 Kubernetes Changes

This section lists the notable changes delivered as updates to the Kubernetes module for Oracle Cloud Native Environment.

3.2.1 Release 1.18

Kubernetes Release 1.18 is based on the upstream Release 1.18. A cumulative list of the major changes in this release includes:

Features

- The Container Storage Interface Driver API is now generally available and is now available under storage.k8s.io/v1.
- `BlockVolume` and `CSIBlockVolume` have reached general availability. This feature allows a block volume to be presented to a pod directly as a block volume, not a file-system.

Administrator Changes

- The `kubectl run` command no longer supports deprecated generators of `ReplicationController`, `Deployment`, `Job` and `CronJob` and now only creates `Pods`. If you need to create these objects use `kubectl create`.
- The `kubectl` flag of `--server-dry-run` that specifies server side dry runs is deprecated. The `--dry-run=` flag which had been used to specify only client side dry runs, now also specifies server side dry runs. Valid options are `server`, `client` or `none`.

API Changes

- The following APIs were made read only, in 1.2. The APIs are now removed:
  - `extensions/v1beta1`: Use the `policy/v1beta1` API for Pod security policy resources instead.
  - `extensions/v1beta1`: Use the `networking.k8s.io/v1` API Network policy resources instead.
  - `extensions/v1beta1`, `apps/v1beta1`, and `apps/v1beta2` APIs : Use the `apps/v1` API for the daemon set, deployment, and replica set resources instead.
  - `scheduling.k8s.io/v1beta1` and `scheduling.k8s.io/v1alpha1` APIs: Use the `scheduling.k8s.io/v1` API for the priority class resources instead.

3.2.2 Release 1.17

Kubernetes Release 1.17 is based on the upstream Release 1.17. A cumulative list of the major changes in Kubernetes Release 1.15 through to Release 1.17 includes:

Administrator Changes

- Custom resource definitions are now available and have been improved with pruning, defaulting, and OpenAPI publishing.
- As an extensibility mechanism, admission plugins can be developed as extensions and can now be run as webhooks configured at runtime.
- A global metrics registry has been implemented to register metrics to be exposed in a more transparent means.
- The Container Storage Interface (CSI) has been further improved to help migrate in-tree volume plugins to the CSI.
- Certificate management is more robust with `kubeadm` seamlessly rotating all certificates (on upgrades) before they expire.
- There are now improvements for scheduling nodes by using items such as schedule daemon set pods, taint nodes by condition, and node lease.
- The `kubectl get` and `kubectl describe` commands now work with Kubernetes API extensions.
- The `kubectl convert` command has been removed.

API Changes

- Pod security policy resources have been changed from the `extensions/v1beta1` API to the `policy/v1beta1` API. Existing persisted data can be retrieved via the `policy/v1beta1` API.

- Network policy resources have been changed from the `extensions/v1beta1` API to the `networking.k8s.io/v1` API. Existing persisted data can be retrieved via the `networking.k8s.io/v1` API.
- The daemon set, deployment, and replica set resources have been changed from the `extensions/v1beta1`, `apps/v1beta1`, or `apps/v1beta2` APIs to the `apps/v1` API. Existing persisted data can be retrieved via the `apps/v1` API.
- Priority class resources have been changed from the `scheduling.k8s.io/v1beta1` and `scheduling.k8s.io/v1alpha1` APIs to the `scheduling.k8s.io/v1` API. Existing persisted data can be retrieved via the `scheduling.k8s.io/v1` API.

3.2.3 Release 1.14

Kubernetes Release 1.14 is based on the upstream Release 1.14. Major changes in Kubernetes Release 1.14 include:

- **Kubernetes Updated**: The upstream Kubernetes Release 1.14 software is packaged as a Certified Kubernetes distribution for Oracle Linux.
- **Oracle Cloud Native Environment Module**: Kubernetes is now a component of the Oracle Cloud Native Environment (known as the *Kubernetes module for Oracle Cloud Native Environment*). This provides a new set up, configuration, and deployment utility provided by the Oracle Cloud Native Environment Platform Command-Line Interface (the *Platform CLI*). For information on using Oracle Cloud Native Environment to deploy and manage the Kubernetes module, see *Getting Started* and *Container Orchestration*.
- **Deprecated Set up Scripts**: The `kubeadm-setup.sh` and `kubeadm-ha-setup` utilities are deprecated. The deployment of the Kubernetes module is now performed using the Platform CLI. For information on using the Platform CLI, see *Platform Command-Line Interface*.
- **Back up and Restore**: Backing up and restoring a Kubernetes control plane node is now performed using the Platform CLI. For information on backing up and restoring a control plane node, see *Container Orchestration*.
- **Runtime Engines**: Oracle Container Runtime for Docker is no longer the container runtime engine. CRI-O is now used to delegate container runtimes. CRI-O is an implementation of the Kubernetes Container Runtime Interface (CRI) to enable using Open Container Initiative (OCI) compatible runtimes. The new runtime engines are runC and Kata Containers. The Kata Containers runtime engine uses lightweight virtual machines for improved container isolation. For information on the runtime engines, see *Container Runtimes*.
- **High Availability**: A load balancer is provided for high availability Kubernetes clusters. You can also use your own load balancer. For information on setting up the load balancer deployed by the Platform CLI, see *Getting Started*.

Chapter 4 Documentation Changes

This chapter lists notable changes to the Oracle Cloud Native Environment documentation.

4.1 Release 1.2

This section lists the notable changes in the documentation for Release 1.2 of Oracle Cloud Native Environment.

Product Name Change: The product name in the documentation set is changed from *Oracle Linux Cloud Native Environment* to *Oracle Cloud Native Environment*. The name change occurred in September 2021.

Look and Feel: The documentation set is republished in a new format which improves the look and feel. Due to this change some deep links into the documentation set may have changed.

Platform CLI: A new *Platform Command-Line Interface* book is added to provide more detailed information on using the Platform CLI. This book contains the information on how to use the `olcnectl` command, including the complete syntax. This information was previously located in *Getting Started* .

Concepts: A new *Concepts* book is added to provide high level information on the architecture and components of Oracle Cloud Native Environment. Some information in this new book was previously located in *Getting Started*.

Creating a Kubernetes module: The information related to creating and managing a Kubernetes module is moved from *Getting Started* to *Container Orchestration*. *Getting Started* now only contains the information you need to set up the hosts and the environment in which to install the Kubernetes module.

Host Requirements: Information about host requirements is from the *Release Notes* to *Getting Started* .

Kubernetes High Availability Requirements: Information about the node requirements for Highly Available Kubernetes clusters is added to *Getting Started* .

Load Balancer: Information about setting up a load balancer for a Highly Available Kubernetes cluster is added to *Getting Started*. Information about setting up a load balancer for the Istio ingress gateway is added to *Service Mesh*.

Istio Requirements: Information about the node requirements for Istio is added to *Getting Started* .

Control Plane Nodes: The term *control plane node* replaces the term *master node*.

Chapter 5 Known Issues

This chapter contains information about known issues and limitations in this release.

5.1 Upgrading Kubernetes 1.12 to Oracle Cloud Native Environment

You cannot upgrade from Kubernetes 1.12 or earlier and add the cluster to Oracle Cloud Native Environment. You must perform a new deployment of Kubernetes using the Platform CLI.

5.2 Disabled virt module on Oracle Linux 8

After deploying the Kubernetes module on Oracle Linux 8, the `virt` module is disabled in the operating system. It is recommended that you do not enable this module again unless requested to do so in this documentation or by Oracle Support.

5.3 Errors using overlay networking

A Kubernetes cluster that uses overlay networking, may result in an issue with the VxLAN configuration for the cluster. Nodes that are affected by the issue display errors similar to the following in the `dmesg` output:

```
[  610.495450] bnxt_en 0000:00:03.0 ens3: hwrm req_type 0xa1 seq id 0x67
error 0xf
[  610.498246] bnxt_en 0000:00:03.0 ens3: hwrm_tunnel_dst_port_alloc failed.
rc:15
```

This issue is commonly caused when the `tx offload` feature is enabled in the `bnxt_en` driver module. You can resolve this issue by disabling the `tx offload` feature using the `ethtool` command. For example:

```
sudo ethtool --offload $(ip -o -4 route show to default | awk '{print $5}') tx off
```

5.4 Listing environments

The Platform CLI does not yet have a method to display a list of the environments created.

5.5 Validating a module reports network ports are not open

If you open network ports on nodes using the range option, the `olcnectl module validate` command cannot validate the ports are open. This is due to an issue in the `firewall-cmd` command. For example, if you use a command like the following which opens ports using a port range:

```
sudo firewall-cmd --add-port=2379-2380/tcp
sudo firewall-cmd --add-port=2379-2380/tcp --permanent
```

The `olcnectl module validate` command reports that ports 2379 and 2380 are not open.

Workaround: Open network ports individually, without specifying a port range. For example:

```
sudo firewall-cmd --add-port=2379/tcp
sudo firewall-cmd --add-port=2379/tcp --permanent
sudo firewall-cmd --add-port=2380/tcp
sudo firewall-cmd --add-port=2380/tcp --permanent
```