Oracle® Database

Administering Oracle Blockchain Platform

F20800-22
June 2025

Oracle Database Administering Oracle Blockchain Platform,

F20800-22

Contents

Preface

Administering Oracle Blockchain Platform explains how to provision and maintain Oracle Blockchain Platform instances.

Topics:

Audience

This guide is intended for service administrators responsible for provisioning and maintaining Oracle Blockchain Platform .

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

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit https://support.oracle.com/portal/ or visit Oracle Accessibility Learning and Support if you are hearing impaired.

Related Documents

For more information, see these Oracle resources:

- *Using Oracle Blockchain Platform*

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, URLs, code in examples, text that appears on the screen, or text that you enter.

1

A Service Administrator's Roadmap to Oracle Blockchain Platform

This section walks you through an overview of Oracle Blockchain Platform Enterprise Edition, and provides a basic workflow for administrators.

Oracle Blockchain Platform Enterprise Edition Overview

Oracle Blockchain Platform provides a platform for building and running smart contracts and maintaining a tamper-proof distributed ledger.

Oracle Blockchain Platform is a network consisting of validating nodes (peers) that update the ledger and respond to queries by executing smart contract code—the business logic that runs on the blockchain. External applications invoke transactions or run queries through specialized inbuilt REST API calls or through their own custom client SDKs, which prompts selected peers to run the smart contracts. Multiple peers endorse (digitally sign) the results, which are then verified and sent to the ordering service. After consensus is reached on the transaction order, transaction results are grouped into cryptographically secured, tamper-proof data blocks and sent to peer nodes to be validated and appended to the ledger. Platform administrators can use the Blockchain Platform Manager to create and manage platform instances, while network administrators can use the Oracle Blockchain Platform console to configure the blockchain and monitor its operation.

Oracle Blockchain Platform Enterprise Edition provides a version of Oracle Blockchain Platform built on Kubernetes clusters and delivered as a set of pre-built container images for multiple Kubernetes distributions including Oracle Cloud Infrastructure Container Engine for Kubernetes (OKE) and minikube. The Oracle Blockchain Platform Enterprise Edition downloadable artifact provides a distribution package that includes all the required container images, Helm charts and with executable scripts to help setup Oracle Blockchain Platform services onto a given Kubernetes cluster. Once Oracle Blockchain Platform Enterprise Edition has successfully been installed, Blockchain Platform Manager can be used for configuring and provisioning multiple Blockchain Platform instances, which will run across the available Kubernetes worker nodes. Similar to the cloud offering, this edition enables customers to create new complete blockchain instances in minutes.

The enterprise edition enables users to scale as required to handle the evolving workloads by increasing the replicas for various nodes. Unlike typical applications, Oracle Blockchain Platform's distributed ledger and the distributed metadata database handle data replication out-of-the-box.

Feature parity with the cloud version ensures that customers can deploy chaincode and use the same chaincode APIs and extensive REST APIs across both versions. Oracle innovations in using Berkeley DB for world state with SQL-based queries, built-in transaction synchronization to off-chain rich history database, intuitive and comprehensive console with powerful operations and monitoring tools, and all the other unique enterprise-grade features are shared across the cloud and on-premises versions.

Security, Authentication, and Authorization

Introduction to Oracle Blockchain Platform Enterprise Edition Security

Oracle Blockchain Platform Enterprise Edition deals with security on several levels. At the top level is the security related to the Oracle Blockchain Platform nodes. Next is the security associated with Blockchain Platform Manager that is used to manage the life cycle on Oracle Blockchain Platform instances. Users of Blockchain Platform Manager (the control plane) are able to create, scale out, scale in, and complete other life cycle operations on instances. For each instance there are users authorized for managing, monitoring, and administering an instance. Finally there are users of the instance that access an instance either via the Fabric SDKs or the Oracle Blockchain Platform REST Proxy. All user information including roles and passwords are stored in the built-in LDAP authentication server.

All sensitive data related to Oracle Blockchain Platform services (passwords, certificates and private keys) are stored using Kubernetes Secrets. It's important to ensure Kubernetes Secrets are secured by following their guidelines: Good practices for Kubernetes Secrets.

Managing Security

Securing Data at Rest

You may want to enable disk encryption in Kubernetes to protect data at rest. All Kubernetes APIs that let you write persistent API resource data support at-rest encryption.

See Encrypting Confidential Data at Rest.

Additionally, follow typical Kubernetes best practices for securing access to the components in your cluster, especially for Kubernetes secrets, because Oracle Blockchain Platform stores confidential information there.

Ports Exposed

Oracle Blockchain Platform makes use of Istio as the ingress gateway service to accept external traffic into Oracle Blockchain Platform services. Oracle Blockchain Platform Enterprise Edition uses the `https` port of the `istio-ingressgateway` service, as a single point of entry to listen to all external traffic. However, based on the configured service type, the public port number may vary.

ServiceType	Port Name	Exposed Port Number	Configurable During Installation?
LoadBalancer (default)	https	443 (default)	Yes
NodePort	https	3xxxx (nodePort value corresponding to https port)	Yes

Configuring Authentication and Authorization

Authentication in Oracle Blockchain Platform is performed using the included LDAP server. Users must have an account in the authentication server in order to be able to use the service.

Users associated with certain authentication groups are granted specific privileges as defined in User Groups and Roles.

Workflow for Administering Oracle Blockchain Platform

To start using Oracle Blockchain Platform, refer to the following tasks as a guide.

Task	Description	More Information
Prepare your environment	Read through the prerequisites for supported Kubernetes platforms and decide which is appropriate for your configuration. Ensure your hardware meets the required prerequisites.	Supported Topologies Prerequisites
Deploy Oracle Blockchain Platform Enterprise Edition	Deploy the Oracle Blockchain Platform Enterprise Edition on the platform of your choice. Access Blockchain Platform Manager	• Deploy Oracle Blockchain Platform Enterprise Edition on Oracle Kubernetes Engine • Deploy Oracle Blockchain Platform Enterprise Edition on minikube Log on to Oracle Blockchain Platform for the First Time
Add and manage users and roles	A default LDAP server is provided with Oracle Blockchain Platform Enterprise Edition.	Configure the Built-In LDAP Server User Groups and Roles
Provision a service instance	Use the Create Instance wizard in Blockchain Platform Manager to create a service instance.	Provision an Instance using the Blockchain Platform Manager
Configure your blockchain network	Once your instance is created, you can use the Blockchain Platform Console to configure the network.	What's the Console?

After you've created your instance and any required users, you can begin to use Oracle Blockchain Platform as described in What's the Console?

2

Prepare to Install Oracle Blockchain Platform

This section lists the prerequisites and supported topologies of Oracle Blockchain Platform Enterprise Edition.

Prerequisites

This topic contains the hardware and software prerequisites for installing Oracle Blockchain Platform Enterprise Edition.

Kubernetes Platforms

The following platforms are supported:

- Oracle Cloud Infrastructure Container Engine for Kubernetes (OKE) v1.29.1 or later
- minikube v1.33.1 or later - test environment only, not for production

You must have a domain name that can be resolved by a DNS server.

Other Prerequisite Software

Additionally you'll need the following tools to assist with managing your Kubernetes platform and installing your Oracle Blockchain Platform container:

- kubectl version 1.29.3 or later - Kubernetes' command line tool
- Helm version 3.12.3 or later - a Kubernetes package manager
- Tools to manage your containers and pods - choose one of the following:
  - Podman version 4.9.4-rhel or later
  - Docker version 24.0.6 or later
- yq version 4.42.1 - a command line YAML processor
- jq v1.7.1 or later - a command line JSON processor
- Istio version 1.20.2 or later and istioctl - security and traffic management tool for deployments, and its command line tool

Web Browsers

All administrative tools that are included with Oracle Blockchain Platform can be accessed by using the following browsers:

- Mozilla Firefox
- Microsoft Edge
- Google Chrome
- Apple Safari

Install Prerequisite Software

This section provides an example walkthrough of installing the tested versions of the prerequisites. Refer to each product's documentation for additional information and any required modifications to the install instructions.

Oracle Linux

Install kubectl

The kubectl version should always be within one minor version difference of your cluster. For example if your Oracle Kubernetes Engine cluster version is v1.29.1, you can use kubectl v1.29.3. For additional information, see Kubernetes Install Tools.

```
# Download:
    curl -LO https://dl.k8s.io/release/v1.29.3/bin/linux/amd64/kubectl

# Setup:
    # Make binary file executable:
    chmod +x ./kubectl
    # Move the downloaded binary to /usr/local/bin or /usr/bin and make
"root" as the owner of this binary
    sudo mv ./kubectl /usr/bin/kubectl
    sudo chown root: /usr/bin/kubectl

# Verify:
    $ kubectl version --client --output=yaml
    clientVersion:
        buildDate: "2024-03-15T00:08:19Z"
        compiler: gc
        gitCommit: 6813625b7cd706db5bc7388921be03071e1a492d
        gitTreeState: clean
        gitVersion: v1.29.3
        goVersion: go1.21.8
        major: "1"
        minor: "29"
        platform: linux/amd64
    kustomizeVersion: v5.0.4-0.20230601165947-6ce0bf390ce3
```

Install Helm

Oracle Blockchain Platform Enterprise Edition was tested with Helm v3.12.3. For additional information, see Installing Helm.

```
#Download install script:
    curl -fsSL -o get_helm.sh https://raw.githubusercontent.com/helm/helm/
master/scripts/get-helm-3

# Provide execute permission and execute:
```

```
    chmod +x get_helm.sh
    ./get_helm.sh

# Verify:"
    $ helm version
    version.BuildInfo{Version:"v3.12.3",
GitCommit:"3a31588ad33fe3b89af5a2a54ee1d25bfe6eaa5e", GitTreeState:"clean",
GoVersion:"go1.20.7"}
```

Install Podman

Oracle Blockchain Platform Enterprise Edition was tested with Podman v4.9.4-rhel. For additional information, see Podman Installation Instructions.

```
# Update the package list:
    sudo yum update

# Install podman:
    sudo yum install podman -y

# create docker alias to run podman commands
    sudo yum install -y podman-docker

#Verify:
    $ podman --version
        podman version 4.9.4-rhel
    $ docker --version
        podman version 4.9.4-rhel
```

Install yq

Oracle Blockchain Platform Enterprise Edition was tested with yq v4.42.1. For additional information, see yq README.

```
# Download:
    wget https://github.com/mikefarah/yq/releases/download/v4.42.1/
yq_linux_amd64.tar.gz -O - | tar xz

# Setup:
    sudo mv yq_linux_amd64 /usr/bin/yq
    sudo chmod +x /usr/bin/yq

# Verify:
    yq --version
```

Install jq

Oracle Blockchain Platform Enterprise Edition was tested with jq v1.7.1. For additional information, see Download jq.

```
# Install:
    sudo dnf install jq

# Verify:
```

```
jq --version
jq-1.7.1
```

macOS

Install kubectl

The kubectl version should always be within one minor version difference of your cluster. For example if your Oracle Kubernetes Engine cluster version is v1.29.1, you can use kubectl v1.29.3. For additional information, see Kubernetes Install Tools.

```
curl -LO https://dl.k8s.io/release/v1.29.3/bin/darwin/amd64/kubectl

# Setup:
    # Make binary file executable:
    chmod +x ./kubectl
    # Move the downloaded binary to /usr/local/bin and make "root" as the
owner of this binary
    sudo mv ./kubectl /usr/local/bin/kubectl
    sudo chown root: /usr/local/bin/kubectl

# Verify:
    $ kubectl version --client --output=yaml

    clientVersion:
        buildDate: "2024-03-15T00:08:19Z"
        compiler: gc
        gitCommit: 6813625b7cd706db5bc7388921be03071e1a492d
        gitTreeState: clean
        gitVersion: v1.29.3
        goVersion: go1.21.8
        major: "1"
        minor: "29"
        platform: darwin/amd64
    kustomizeVersion: v5.0.4-0.20230601165947-6ce0bf390ce3
```

Install Helm

Oracle Blockchain Platform Enterprise Edition was tested with Helm v3.12.3. For additional information, see Installing Helm.

```
#Download install script:
    curl -fsSL -o get_helm.sh https://raw.githubusercontent.com/helm/helm/
master/scripts/get-helm-3

# Provide execute permission and execute:
    chmod +x get_helm.sh
    ./get_helm.sh

# Verify:"
    $ helm version
    version.BuildInfo{Version:"v3.12.3",
GitCommit:"3a31588ad33fe3b89af5a2a54ee1d25bfe6eaa5e", GitTreeState:"clean",
GoVersion:"go1.20.7"}
```

Install Podman

Oracle Blockchain Platform Enterprise Edition was tested with Podman v4.9.4-rhel. For additional information, see Podman Installation Instructions.

```
# Install:
     brew install podman

# After installing, you need to create and start your first Podman machine:

     podman machine init
     podman machine start

# Verify:
     podman info
     host: arch: amd64 buildahVersion: 1.36.0 cgroupControllers: - cpu - io -
memory - pids cgroupManager: systemd

# Make docker commands available via podman by creating a symlink:
     sudo ln -s /usr/local/bin/podman /usr/local/bin/docker
```

Install yq

Oracle Blockchain Platform Enterprise Edition was tested with yq v4.44.1. For additional information, see yq README.

```
# Install:
    brew install yq

# Verify:
   yq--version
   yq (https://github.com/mikefarah/yq/) version v4.44.1
```

Install jq

Oracle Blockchain Platform Enterprise Edition was tested with jq v1.7.1. For additional information, see Download jq.

```
# Install:
    brew install jq

# Verify:
   jq --version
   jq-1.7.1
```

Install Istio

Istio extends Kubernetes to provide traffic management and security to complex deployments. Oracle Blockchain Platform Enterprise Edition uses Istio as the ingress gateway service to accept incoming traffic into various services.

We recommend installing Istio and istioctl (Istio configuration command line utility). Istio version 1.20.2 and later is supported.

To download Istio:

```
# Download istioctl tool
   curl -L https://istio.io/downloadIstio | sh -

# (optional) You can move the downloaded "istio-1.22.1" directory
   mv ./istio-1.22.1 $HOME/istioctl

# Add the istioctl client to your path
export PATH=$HOME/istioctl/bin:$PATH
```

> **Note:**
>
> Istio installation will be completed after your Kubernetes cluster has been created. It has a dependency on the `.kube/config` file.

Istio's `ingressgateway` service can be configured in Kubernetes to run with either `LoadBalancer` or `NodePort` service types. See the Istio documentation for details: Istio Ingress Gateways

Load Balancer
If your Kubernetes cluster supports an external load balancer, it's recommended to configure the Istio ingress gateway service as a load balancer using the Oracle Blockchain Platform Enterprise Edition `runme` script that you'll use during deployment. Oracle Blockchain Platform Enterprise Edition will use Istio ingress gateway's https port (443) as the public port to accept the incoming traffic. This port value can be optionally customized during installation of Oracle Blockchain Platform Enterprise Edition using the `runme` script.

Node Port
In cases where the load balancer service type cannot be used, the Istio ingress gateway service can be configured with node port service type. Oracle Blockchain Platform Enterprise Edition will use the `nodePort` value of the https port in the Istio ingress gateway to route external traffic to Oracle Blockchain Platform Enterprise Edition inside the Kubernetes cluster. The value of the `nodePort` for the https port can be optionally customized (based on the allowed `nodePort` range) during installation of Oracle Blockchain Platform Enterprise Edition using the `runme` script. By default, the allowed `nodePort` range in Kubernetes cluster is 30000-32767.

> **Note:**
>
> Do not update the value of the https `port` or `nodePort` after installation of Oracle Blockchain Platform Enterprise Edition as it will affect its function.

Hostname Resolution for Oracle Blockchain Platform Enterprise Edition Services

Oracle Blockchain Platform Enterprise Edition services use uniquely generated hostnames that are configured in the Istio gateways/virtualservices. To communicate with the Oracle Blockchain Platform Enterprise Edition services inside the Kubernetes cluster, you are required to use these unique hostnames from your browsers or applications. Based on the chosen service type for `istio-ingressgateway`, these hostnames are required to be resolved to an IPv4 address in the following way:

- If `LoadBalancer`, they resolve to the external IP address generated for the `istio-ingressgateway` service
- If `NodePort`, they resolve to the worker nodes' IP addresses

Supported Topologies

In addition to creating a topology in which both the founder and participant are on Oracle Blockchain Platform Enterprise Edition, the following interoperability scenarios are supported:

- Oracle Blockchain Platform Enterprise Edition Founder, Oracle Blockchain Platform Cloud Participant
- Oracle Blockchain Platform Cloud Founder, Oracle Blockchain Platform Enterprise Edition participant

> **Note:**
>
> Interoperability between Hyperledger Fabric 1.4 and Hyperledger Fabric 2.5 is not supported.

3

Install Your Oracle Blockchain Platform Instance

This section describes how to deploy Oracle Blockchain Platform Enterprise Edition, and log on to Oracle Blockchain Platform for the first time.

Deploy Oracle Blockchain Platform Enterprise Edition on Oracle Kubernetes Engine

Before deploying Oracle Blockchain Platform Enterprise Edition, you must have a Kubernetes cluster running and you must install several prerequisites.

For detailed information about Oracle Kubernetes Engine, see Oracle Cloud Infrastructure Container Engine for Kubernetes

Create an Oracle Kubernetes Engine Cluster on OCI

Recommended minimum specifications for your Oracle Kubernetes Engine Cluster:

	Development	**Production with High Availability**
Minimum Version	v1.29.1	v1.29.1
Node Type	Managed	Managed
Node Image	Oracle Linux 8	Oracle Linux 8
Node CPU	2 OCPUs or higher	4 OCPUs or higher
Node Memory	24 GB or higher	32 GB or higher
Node Count	1 or higher	3 or higher
Boot volume size	100 GB or higher. The default boot volume of 50 GB may not be sufficient to hold Oracle Blockchain Platform Enterprise Edition container images and temporary data for chaincode pods because of limited ephemeral storage.	100 GB or higher. The default boot volume of 50 GB may not be sufficient to hold Oracle Blockchain Platform Enterprise Edition container images and temporary data for chaincode pods because of limited ephemeral storage.

- For added security, select `Private workers` for the Kubernetes worker nodes.
- Ensure that the worker nodes have access to the internet, which is required to install chaincodes on your Oracle Blockchain Platform instances.

This section walks through creating an example Oracle Kubernetes Engine on OCI. For additional options and details, see Creating Kubernetes Clusters Using Console Workflows

1. Log in to your OCI tenancy, selecting your region and compartment.
2. Open the navigation menu and click **Developer Services**. Under **Containers & Artifacts**, click **Kubernetes Clusters (OKE)**.

3. On the **Cluster List** page, click **Create cluster**.
4. In the **Create cluster** dialog, select **Quick create** and click **Submit**.
5. On the **Create cluster** page, either accept the default configuration details for the new cluster, or specify alternatives as follows:
   - **Name:** The name of the new cluster. Either accept the default name or enter a name of your choice.
   - **Compartment:** The compartment in which to create the new cluster and the associated network resources.
   - **Kubernetes version:** The version of Kubernetes to run on the control plane nodes and worker nodes of the cluster. v1.29.1 was tested with Oracle Blockchain Platform Enterprise Edition.
   - **Kubernetes API endpoint:** The type of access to the cluster's Kubernetes API endpoint. Select **Public** (accessible directly from internet). A public regional subnet is created and the Kubernetes API endpoint is hosted in that subnet. The Kubernetes API endpoint is assigned a public IP address as well as a private IP address.
   - **Node type:** Specify the type of worker nodes in the first node pool in the cluster. Select **Managed**. You have responsibility for managing the worker nodes in the node pool. Managed nodes run on compute instances (either bare metal or virtual machine) in your tenancy. As you are responsible for managing managed nodes, you have the flexibility to configure them to meet your specific requirements. You are responsible for upgrading Kubernetes on managed nodes, and for managing cluster capacity.
   - **Kubernetes worker nodes:** The type of access to the cluster's worker nodes. Select **Private** (accessible through other VCN subnets). A private regional subnet is created to host worker nodes. The worker nodes are assigned a private IP address.
   - **Node shape:** The shape to use for each node in the node pool. The shape determines the number of CPUs and the amount of memory allocated to each node. The list shows only those shapes available in your tenancy that are supported by Container Engine for Kubernetes. Oracle Blockchain Platform Enterprise Edition was tested with VM.Standard.E3.Flex and VM.Standard.E4.Flex shapes.
   - **Image:** The image to use on worker nodes in the managed node pool. An image is a template of a virtual hard drive that determines the operating system and other software for the managed node pool. Oracle Blockchain Platform Enterprise Edition was tested with Oracle Linux 8.
   - **Node count:** The number of worker nodes to create in the node pool, placed in the regional subnet created for the cluster. Select three or more.

   Select the following Advanced Options:

   - **Boot volume**: Configure the size and encryption options for the worker node's boot volume. The default boot volume of 50 GB may not be sufficient to hold Oracle Blockchain Platform Enterprise Edition images and temporary data for chaincode pods because of limited ephemeral storage. If you plan to deploy several chaincodes (more than five), increase the boot volume to approximately 100 GB.
6. Review the options you've selected, and click **Create Cluster**.
7. Ensure that your worker nodes and node pools are running:
   - Under **Resources**, select **Nodes**. For each worker node, ensure that the node is ready, active, and matches the Kubernetes cluster version.
   - Under **Resources**, select **Node pools**. For your node pool, ensure that the pool is active and matches the Kubernetes cluster version.

Install the OCI Command Line Interface

This section provides an example walkthrough of installing the OCI Command Line Interface. Oracle Blockchain Platform Enterprise Edition was tested with v3.42.0. For additional information, refer to OCI Command Line Interface.

- Oracle Linux
- macOS

Oracle Linux

```
# Install:
    sudo dnf -y install oraclelinux-developer-release-el8
    sudo dnf -y install python36-oci-cli

# Verify:
    $ oci --version
    3.42.0
```

macOS

```
# Install:

    brew update && brew install oci-cli

## If this fails with "Error: python@3.12: the bottle needs the Apple Command
Line Tools to be installed.", run below command:

    xcode-select --install

# Verify:
   oci --version
   3.43.1
```

Create Install Initiator System

Set up local access for the cluster

See the following for additional information: Setting Up Local Access to Clusters.

1. Copy your RSA key to the Oracle Linux or macOS system on which you installed the prerequisites. Your keys can be found in the OCI console: **Identity**, and then **Domains**, and then **OracleIdentityCloudService domain**, and then **Users**, and then **User name**, and then **API keys**. Secure the key: `chmod 400 your_rsa.key`
   You can create a key if needed. See How to Generate an API Signing Key
2. In the OCI console, go to your cluster and open the **Cluster Details** page.
3. Select **Access Cluster**, and then **Local Access**.
   a. Create a directory to contain the `kubeconfig` file: `mkdir -p $HOME/.kube`

b. Copy the **To access the kubeconfig for your cluster via the VCN-Native public endpoint** command.

c. Run the command on your Linux or macOS system. Because the config file doesn't exist yet, you'll be prompted for the following:

- Do you want to create a new config file? [Y/n]: y
- Do you want to create your config file by logging in through a browser? [Y/n]: n
- Enter a location for your config [/home/opc/.oci/config]: select a location
- Enter a user OCID: can be found in the OCI console
- Enter a tenancy OCID: can be found in the OCI console
- Enter a region by index or name: Enter the number corresponding to your Tenancy's Region, for example 12
- Do you want to generate a new API Signing RSA key pair? If you decline you will be asked to supply the path to an existing key. [Y/n]: n
- Enter the location of your API Signing private key file: location of RSA key file created above

This creates a config file that gives the Kubernetes control plane VM access to the cluster hosted on OCI.

d. When the OCI config file is created, you must re-run the copied **To access the kubeconfig for your cluster via the VCN-Native public endpoint** command. It will used the config file that you just created.

4. Verify that you can reach the Oracle Kubernetes Engine cluster: `kubectl get nodes`. If the setup is correct, the command will show all the worker nodes in your cluster.
5. Restrict access to the config file: `chmod 600 $HOME/.kube/config`
6. Set your `KUBECONFIG` environment variable to the file for this cluster: `export KUBECONFIG=$HOME/.kube/config`

Note:

Check whether your OCI config file has multiple profiles similar to the following text:

```
[OCI_PROFILE_A]
fingerprint = .............
key_file = .............
tenancy = .............
region = .............
user = .............

[OCI_PROFILE_B]
fingerprint = .............
key_file = .............
tenancy = .............
region = .............
user = .............
```

If so, you'll need to customize the `kubeconfig` file or you'll get an authorization error when you try to install Oracle Blockchain Platform Enterprise Edition. In the users section of the `kubeconfig` file, add a line to specify which user to use in your OCI config file. For example

```
users:
- name: user-c3xxxxxq
  user:
    exec:
      apiVersion: client.authentication.k8s.io/v1beta1
      args:
      - ce
      - cluster
      - generate-token
      - --cluster-id
      - ocid1.cluster.oc1.eu-frankfurt-1.aaaaaaxxxxxxxxxyyyyyy
      - --region
      - eu-frankfurt-1
      - --profile
      - <OCI_PROFILE_NAME>
      command: oci
      env: []
      interactiveMode: IfAvailable
      provideClusterInfo: false
```

where `<OCI_PROFILE_NAME>` would be `OCI_PROFILE_A`

Complete the Istio Install

Oracle Blockchain Platform Enterprise Edition supports version 1.20.2 and later. You must have completed the steps in Install Istio before running the following commands.

```
# Install
    istioctl install --set profile=default --set
```

```
values.pilot.env.ENABLE_TLS_ON_SIDECAR_INGRESS=true --set
components.cni.enabled=true --set values.cni.repair.deletePods="true"
    ## Enter "y" when prompted for "Proceed? (y/N)"

# Verify:
    $ istioctl version
    client version: 1.22.1
    control plane version: 1.22.1
    data plane version: 1.22.1 (1 proxies)
```

Set Up an Auth Token for Your User

Create an Auth Token for your administrative user so that you can pull images from the OCI Registry: Generating an Auth Token to Enable Login to Oracle Cloud Infrastructure Registry.

Install Oracle Blockchain Platform Enterprise Edition

1. On the Oracle Blockchain Platform Enterprise Edition page, click **Download** and follow the steps to download the Oracle Blockchain Platform Enterprise Edition package. Extract the package from the `.zip` file, and then extract the package from the downloaded archive file.

   ```
   tar -xzf <distribution-package-file>
   # example tar -xzf obpee_package_24.1.3-20240723083137.tgz
   ```

2. Update the `runme-input.yaml` file with the required values. The following example `runme-input.yaml` file can be used as reference:

   ```
   imageRegistryConfiguration:
     registry: <container_registry_name>
     imageTagPrefix: <container-image-repository-prefix>
     username: <container-registry-username>

   imageReleaseVersion: 24.1.3-20240723083137

   # storageClassName should be set to create a dynamic persistent volume. If
   empty, default storageClass is used.

   controlPlaneStorage:
     storageClassName:
     # Example 500Mi, 5Gi
     size: 4Gi

   parentDomainName: example.com
   #imagePullTimeout: Use this field to customize the wait time (in seconds)
   for pulling the required container images from the repository. Default is
   1800 seconds.
       imagePullTimeout: 1800
   ```

   In the previous example, the variables are defined as shown in the following list:

   - **`imageRegistryConfiguration.registry`**: Container registry server to use. Example: `iad.ocir.io`

- **`imageRegistryConfiguration.imageTagPrefix`**: Container base repository path with the registry, where the images will be pushed to and pulled from. Example: `iad.ocir.io/obpee/bcs`
- **`imageRegistryConfiguration.username`**: Container registry login user name
- **`imageReleaseVersion`** - Oracle Blockchain Platform Enterprise Edition release version
- **`controlPlaneStorage.storageClassName`**: Kubernetes storage class to use for PVC (PersistentVolumeClaim). If empty, the default `storageClass` is used
- **`controlPlaneStorage.size`**: PVC size for Blockchain Platform Manager (control plane) services
- **`parentDomainName`**: Domain name to use for Blockchain Platform Manager services. Example: `example.com`
- **`imagePullTimeout`**: Image pull wait timeout in seconds during Oracle Blockchain Platform Enterprise Edition installation. Default is 1800 seconds.

3. Run the `runme_oke.sh [--publish-images]` script, following the prompts.

> **Note:**
>
> The optional `--publish-images` command uploads the containers to a container image registry such as Oracle Cloud Infrastructure Registry using the details specified in the `runme-input.yaml` file.

- Enter the default LDAP admin password (the password will not be displayed): sets the administrator's password for the built-in LDAP authentication server.
- Enter the default control plane admin user password (the password will not be displayed): sets the Blockchain Platform Manager administrator's password.
- If `StorageClass` wasn't provided in the `runme-input.yaml` file, the system checks if the default storage class is set and ask if you want to use it.
- Confirm the Istio ingress gateway service type: `LoadBalancer` is the default. `NodePort` is also supported. Note that accessing `NodePorts` requires that the Kubernetes cluster was created with public worker nodes. See Install Istio.
- Confirm the Istio ingress gateway service https port: the default is 443 for the `LoadBalancer` service type.
- Enter registry *<registry name>* password: this password is used to connect to your container image registry (as specified in the `runme-input.yaml` file) for downloading images.

4. The script lists the `Istio-ingressgateway` URL as part of the output. Record the IP address listed.
5. The script installs the following services under the `obp-cp` namespace:
   - `control-plane`
   - `openldap`
   - `obp-auth-server`
   - `obp-operator`
   - `hlf-operator`

Access Blockchain Platform Manager

After installation, configure the host name resolution for the generated Blockchain Platform Manager host names.

1. Run the following command to get the list of configured host names:

```
kubectl get virtualservice -n obp-cp -o json | jq -r
'.items[].spec.hosts[0]'
```

2. Based on the chosen service type for `istio-ingressgateway`, these generated host names must be resolved to an IPv4 address according to the following requirements:
   - `LoadBalancer`: resolve to the external IP address generated for the `istio-ingressgateway` service
   - `NodePort`: resolve to the worker nodes' IP addresses

Deploy Oracle Blockchain Platform Enterprise Edition on minikube

You can use minikube for testing and internal development purposes. Do not use minikube for production environments.

Prerequisites:

- CPUs: 8 or higher
- Memory: 16 GB
- Free disk space: 50 GB or higher
- A non-root user with superuser privileges
- Ensure that the minikube node has access to the internet, which is required to install chaincodes on your Oracle Blockchain Platform instances.
- minikube v1.33.1 or later

Install minikube

This section provides an example walkthrough of installing the tested version of the minikube. For additional information, see Kubernetes Install Tools.

- Oracle Linux
- macOS

Oracle Linux

```
#Download the latest minikube binary
curl -LO https://storage.googleapis.com/minikube/releases/latest/minikube-
linux-amd64

#Install
sudo install minikube-linux-amd64 /usr/local/bin/minikube
```

```
#Verify Installation
minikube version

#Start Minikube
minikube start

#Verify Minikube Installation
minikube status
```

macOS

```
#Install Homebrew (if not already installed)
/bin/bash -c "$(curl -fsSL https://raw.githubusercontent.com/Homebrew/install/
HEAD/install.sh)"

#Install minikube using Homebrew
brew install minikube

#Start minikube
minikube start

#Verify minikube Installation
minikube status
```

Complete the Istio Install

Oracle Blockchain Platform Enterprise Edition supports version 1.20.2 and later. You must complete the steps in Install Istio before running the following commands.

```
# Install
    istioctl install --set profile=default --set
values.pilot.env.ENABLE_TLS_ON_SIDECAR_INGRESS=true --set
components.cni.enabled=true --set values.cni.repair.deletePods="true"
    ## Enter "y" when prompted for "Proceed? (y/N)"

# Verify:
    $ istioctl version
    client version: 1.22.1
    control plane version: 1.22.1
    data plane version: 1.22.1 (1 proxies)
```

Install Oracle Blockchain Platform Enterprise Edition

Download and install Oracle Blockchain Platform Enterprise Edition on your minikube instance:

1. On the Oracle Blockchain Platform Enterprise Edition page, click **Download** and follow the steps to download the Oracle Blockchain Platform Enterprise Edition package. Extract the

package from the `.zip` file, and then extract the package from the downloaded archive file.

```
tar -xzf <distribution-package-file>
# example tar -xzf obpee_package_24.1.3-20240723083137.tgz
```

2. Update the `runme-input.yaml` file with the required values. The following example `runme-input.yaml` file can be used as reference:

```
imageRegistryConfiguration:
  registry: <container_registry_name>
  imageTagPrefix: <container-image-repository-prefix>
  username: <container-registry-username>

imageReleaseVersion: 24.1.3-20240723083137

# storageClassName should be set to create a dynamic persistent volume. If
empty, default storageClass is used.

controlPlaneStorage:
  storageClassName:
  # Example 500Mi, 5Gi
  size: 4Gi

parentDomainName: example.com
#imagePullTimeout: Use this field to customize the wait time (in seconds)
for pulling the required container images from the repository. Default is
1800 seconds.
    imagePullTimeout: 1800
```

   In the previous example, the variables are defined as shown in the following list:

   - **`imageRegistryConfiguration.registry`**: Container registry server to use. Example: `iad.ocir.io`
   - **`imageRegistryConfiguration.imageTagPrefix`**: Container base repository path with the registry, where the images will be pushed to and pulled from. Example: `iad.ocir.io/obpee/bcs`
   - **`imageRegistryConfiguration.username`**: Container registry login user name
   - **`imageReleaseVersion`**: Oracle Blockchain Platform Enterprise Edition release version
   - **`controlPlaneStorage.storageClassName`**: Kubernetes storage class to use for PVC (PersistentVolumeClaim). If empty, the default `storageClass` is used
   - **`controlPlaneStorage.size`**: PVC size for Blockchain Platform Manager (control plane) services
   - **`parentDomainName`**: Domain name to use for Blockchain Platform Manager services. Example: `example.com`
   - **`imagePullTimeout`**: Image pull wait timeout in seconds during Oracle Blockchain Platform Enterprise Edition installation. Default is 1800 seconds.

3. Ensure that minikube is running.

4. Open a new terminal window and go to the distribution package directory. Run the `runme_minikube.sh` script and follow the steps as prompted by the script output:

   ```
   ./runme_minikube.sh [--publish-images]
   ```

   > **Note:**
   >
   > The optional `--publish-images` command uploads the containers to a container image registry such as Oracle Cloud Infrastructure Registry.

   - Enter the default LDAP admin password (the password will not be displayed): sets the administrator's password for the built-in LDAP authentication server.
   - Enter the default control plane admin user password (the password will not be displayed): sets the Blockchain Platform Manager administrator's password.
   - If `StorageClass` wasn't provided in the `runme-input.yaml` file, the system checks if the default storage class is set and asks if you want to use it.
   - Confirm the Istio ingress gateway service https port: the default is 443 for the `LoadBalancer` service type.
   - Enter registry *<registry name>* password: this password is used to connect to your container image registry (as specified in the `runme-input.yaml` file) for downloading images.

5. In a different terminal window, run the following command:

   ```
   export KUBECONFIG=/<path_to>/.kube/minikube
   ```

6. Ensure that the minikube tunnel is active for accessing Blockchain Platform Manager and instances:

   ```
   minikube tunnel --bind-address 0.0.0.0
   ```

7. The script installs the following services under the `obp-cp` namespace:
   - `control-plane`
   - `openldap`
   - `obp-auth-server`
   - `obp-operator`
   - `hlf-operator`

8. The script displays the Blockchain Platform Manager URL, which you can use to access the control plane UI.

Access Blockchain Platform Manager

After installation, configure the host name resolution for the generated Blockchain Platform Manager host names.

1. Run the following command to get the list of configured host names:

```
kubectl get virtualservice -n obp-cp -o json | jq -r
'.items[].spec.hosts[0]'
```

2. Use the IPv4 address of the minikube host as the mapping IP address for the generated host names.
3. Ensure the minikube tunnel is active to access Blockchain Platform Manager and Oracle Blockchain Platform instances.

Patch Oracle Blockchain Platform

After you've installed Oracle Blockchain Platform Enterprise Edition you can find patches for it on the Oracle Support site.

Patch set 4 is available for Oracle Blockchain Platform Enterprise Edition. The change log for the patch as well as prerequisites and instructions are included in the readme file that comes with the patch.

1. Go to the My Oracle Support portal https://support.oracle.com/portal/, and log in.
2. Select the **Patches and Updates** tab.
3. Search for the patch by name or number (`38020771`). Download and extract the patch.
4. Follow the instructions in the readme file to install the patch.
5. After the patch is applied, restart any existing Oracle Blockchain Platform instances. Because the container registry images are updated by the patch, any instances created after patching will use the updated images.

> **Note:**
>
> You can also roll back the patch using the same patch script and selecting the rollback option.
>
> The rollback can be performed only if no lifecycle operations have been done from Blockchain Platform Manager after the patch application. If you have completed lifecycle operations after installing the patch and need to roll back, please contact Oracle Support.

Log on to Oracle Blockchain Platform for the First Time

After you've deployed and started Oracle Blockchain Platform Enterprise Edition , you can log on to Blockchain Platform Manager (the control plane management tool) to create an instance.

You can directly log on to the Platform Manager by using the URL `https://controlplane.<parentDomainName>.com/console/index.html`. The URL for your instance is displayed at the end of successfully running the `runme` script for your install. The initial user name is `obpadmin` and the password configured during installation. This user is only meant for performing initial configuration and does not have instance creation privileges.

Enable the LDAP server

1. Log into Blockchain Platform Manager.

2. Go to **Configuration**, then **Authentication Servers**.
3. Click **Save and Set Active** to activate the default LDAP configuration.
4. Click **Test Configuration** to test your connectivity with the server.

Set the Blockchain Platform Manager Name

On the **Configuration** page **Platform Settings** tab of Blockchain Platform Manager, you can set a name for the Platform Manager.

> **Note:**
>
> Once the name for the Platform Manager has been set, any users added to the LDAP server will be associated with this name. If you change the name after adding users, those users will lose access to Blockchain Platform Manager and any Oracle Blockchain Platform instances.

Set the Notification and Console Idle Timeouts

On the **Configuration** page **Platform Settings** tab of Blockchain Platform Manager, you can set the timeouts for notifications and the console.

- **Console Idle Timeout**: in minutes, how long the console can be idle before it logs out the current user.
- **Notification Timeout**: in seconds, how long notifications will remain visible on the browser. Select `-1` if you want notifications to remain visible until you close them.

4
User Management

This section describes how to configure the included default LDAP server or an external authentication server. It also describes the user groups and roles used by Oracle Blockchain Platform.

Configure the Built-In LDAP Server

The built-in LDAP server has a default configuration already set up when you log in. You can use it as-is, or modify the configuration to meet your needs.

1. Open the **Configuration** tab.
2. Edit the configuration information for the LDAP server as needed:
   a. Configuration Name:

      Not editable
   b. Authentication Server Type:

      Not editable
   c. Host:

      Not editable
   d. Port:

      Not editable
   e. TLS Enabled:

      Not editable
   f. Connect Timeout:

      In milliseconds.
   g. Base DN:

      Enter the base distinguished name of the directory you want to connect to. It should be in the form: `ou=organizationunit,dc=mycompany,dc=com`
   h. Bind User DN:

      The distinguished name of your administrative user account.
   i. Bind User Password:

      The password for the account.
   j. UserName Attribute:

      This is the filter used when searching to convert a login user name to a distinguished name.
   k. User Class Name:

      The attribute value to a user object in the directory.
   l. GroupName Attribute:

This is the filter used when searching to convert a group name to a distinguished name.

m. Group Membership Attribute:

The membership attribute name of the group.

n. Group Class Name:

The ObjectClass attribute value for a group object in the directory.

3. Click **Test Configuration** to ensure your settings work. The test results show if the configuration was successful.
4. Click **Save**. Your configuration is now available to be used by any instances you provision.

Add Users to Your LDAP Server Using Blockchain Platform Manager

Once you've configured your LDAP server in Blockchain Platform Manager, you need to add users to the LDAP server, and then log back into Blockchain Platform Manager with one of these users to create an instance.

Add your initial user to the LDAP server. On the **Authentication Servers** tab of the **Configuration** page of Blockchain Platform Manager, click **Add User**. Once you've entered the user name and password, this user will be added to the LDAP server as an administrative user. You can now log out of Blockchain Platform Manager with your default admin user, and log in with this newly added user to create an instance.

Once you've successfully logged into Blockchain Platform Manager with this user and provisioned an instance, you may want to disable the default admin user (`obpadmin`) for security reasons. This can be done from the **Configuration** page **Platform Settings** tab.

User Groups and Roles

This overview describes the groups and roles that are relevant to Oracle Blockchain Platform. Anyone who uses or administers Oracle Blockchain Platform must be added to the authentication server and granted the correct group.

Groups

Below are the group roles that are available for Oracle Blockchain Platform.

User Role	LDAP Group Name in LDAP	Description
Application	OBP_<platform-name>_<instance-name>	Security identifier for an individual instance.
Control Plane Management	OBP_<platform-name>_CP_ADMIN	User can provision a new Oracle Blockchain Platform instance, configure existing instances, set the LDAP configuration, and perform life cycle operations on Oracle Blockchain Platform instances. A user must be a member of this group to be able to log in to the Blockchain Platform Manager or create an instance.

User Role	LDAP Group Name in LDAP	Description
CA Administrator	OBP_<platform-name>_<instance-name>_CA_ADMIN	The CA Admin group is the bootstrap and overall administrator for the Oracle Blockchain Platform application. Users must be part of this group to create an instance.
Instance Administrator	OBP_<platform-name>_<instance-name>_ADMIN	Users in this group can manage instances via the console UI or REST. Users must be part of this group to create an instance. See the table in Access Control List for Console Function by User Roles for a complete list of console functions available for this user role.
Instance User	OBP_<platform-name>_<instance-name>_USER	Users in this group can view instance via console UI or REST See the table in Access Control List for Console Function by User Roles for a complete list of console functions available for this user role.
REST Proxy Client	OBP_<platform-name>_<instance-name>_REST	Users in this group can call REST proxy to execute transactions using the default enrollment.

Access Control List for Console Function by User Roles

The following table lists which console features are available to the Instance Administrator and Instance User roles.

Feature	Instance Administrator	Instance User
Dashboard	Yes	Yes
Network: list orgs	Yes	Yes
Network: add orgs	Yes	No
Network: Ordering service setting	Yes	No
Network: Export certificates	Yes	No
Network: Export orderer settings	Yes	Yes
Node: list	Yes	Yes
Node: start/stop/restart	Yes	No
Node: view attributes	Yes	Yes
Node: edit attributes	Yes	No
Node: view metrics	Yes	Yes
Node: Export/Import Peers	Yes	No
Peer Node: list channels	Yes	Yes
Peer Node: join channel	Yes	No
Peer Node: list chaincode	Yes	Yes
Channel: list	Yes	Yes
Channel: create	Yes	No
Channel: add org to channel	Yes	No

Feature	Instance Administrator	Instance User
Channel: Update ordering service settings	Yes	No
Channel: view/query ledger	Yes	Yes
Channel: list instantiated chaincode	Yes	Yes
Channel: list joined peers	Yes	Yes
Channel: set anchor peer	Yes	No
Channel: upgrade chaincode	Yes	No
Chaincode: list	Yes	Yes
Chaincode: install	Yes	No
Chaincode: instantiate	Yes	No
Sample chaincode: install	Yes	No
Sample chaincode: instantiate	Yes	No
Sample chaincode: invoke	Yes	Yes
CRL	Yes	No

5

Provision an Instance

This section describes how to provision your Oracle Blockchain Platform instance using Blockchain Platform Manager.

Before You Create an Oracle Blockchain Platform Instance

Before you provision Oracle Blockchain Platform, decide if a developer or enterprise instance meets your needs.

Deciding Which Provisioning Shape to Use

When provisioning an instance, you choose between two configurations. Migration between these options isn't supported currently.

Configuration	Features
Developer Recommended use for this starter shape is development and evaluation.	• 1 Fabric-CA node • 3-node Fabric Ordering Service Network • 1-node repository for instance metadata • Dynamically managed chaincode execution containers • Console service for operations web user interface • REST proxy service for RESTful API • LDAP server integration for authentication and role management
Enterprise Highly available instance configuration, with higher replica count for each service.	• 3 Fabric-CA nodes • 3-node Fabric Ordering Service Network • 3-node cluster repository for high availability of instance metadata • Dynamically managed chaincode execution containers • Console service for operations web user interface • Multiple replicas for REST proxy service for RESTful API • LDAP server integration for authentication and role management

Provision an Instance using the Blockchain Platform Manager

To create a blockchain founder or participant instance in Blockchain Platform Manager, use the Create New Instance wizard.

There are two types of Oracle Blockchain Platform instances you can provision:

- **Founder organization**: a complete blockchain environment, including a new network to which participants can join later on.
- **Participant instance**: if there is already a founder organization you want to join, you can create a participant instance if your credentials provide you with access to the network. Note that a participant cannot function on its own.

1. In Blockchain Platform Manager, open the **Instances** page.
2. Select **Create Instance**.
3. Complete the following fields:

Field	Description
Instance Name	Enter a name for your Oracle Blockchain Platform instance. The service instance name: • Must contain one or more characters. • Must not exceed 15 characters. • Must start with an ASCII letter: `a` to `z`. • Must contain only ASCII letters or numbers. • Must not contain a hyphen. • Must not contain any other special characters. • Must be unique within the identity domain.
Description	Optional. Enter a short description of the Oracle Blockchain Platform instance.
Domain Name	Enter the domain name for the cluster. The hostnames generated for the Blockchain Instance services make use of the domain name and the instance name as parent domain and sub domain respectively.
Role	Select **Founder** to create a complete blockchain environment. This instance becomes the founder organization and you can onboard new participants in the network later. Select **Participant** to create an instance that will join an existing blockchain network created elsewhere before this instance can be used.
Configuration	Select a provisioning shape which meets the needs of your deployment: • **Developer** • **Enterprise**
Peers	Specify the number of peer nodes to be initially created in this service instance. You can create additional peer nodes in the Oracle Blockchain Platform console at a later time.

4. Click **Create Instance**.

Provisioning Postrequisites

Before accessing the Oracle Blockchain Platform service console, configure the hostname resolution for the blockchain instance services, similar to what you did earlier for the Blockchain Platform Manager hostnames. Use the following command to get the list of hostnames for the created blockchain instance:

```
kubectl get virtualservice -n <instance-namespace> -o json | jq -r
      .items[].spec.hosts[0]
```

Once your instance has been created and is listed in the Instances list, you can launch the service console from the menu next to the instance name. Use the console to configure your network as described in *Using Oracle Blockchain Platform*.

6

Manage Oracle Blockchain Platform

Once you've provisioned your instance, you can manage its lifecycle operations in Blockchain Platform Manager. You can also manage your ephemeral storage, worker nodes, and configure a proxy so that your network can run in an offline environment.

Manage Your Instance Lifecycle Operations

Once you've provisioned your instance, you can manage it in Blockchain Platform Manager.

View Instance Details

Clicking on your instance name in Blockchain Platform Manager opens the **Instances** tab displaying details about the instance.

The **Instance Details** page lists information such as the health of the instance, namespace and domain name.

You can manage the instance from the **Actions** menu, or launch the Oracle Blockchain Platform Service Console to manage your blockchain network.

View Instance Activity

The Activity pages shows the status of operations that have been performed on your instances.

To see the activity of an instance, select your instance name and on the **Instances** page click **Activity**.

This tab lists any operations that have been performed on your instance such as starting, stopping, and updating, as well as whether or not it was successful, the time of the operation, and the user ID who initiated the operation.

You can see and filter the activity of all instances managed by Blockchain Platform Manager on the **Activities** page. The **Activities** page can be used to see the history of operations performed on any instances, including deleted instances. These activities can be filtered by different search criteria such as instance name, operation types, and date range.

Start or Stop an Instance

You can start or stop an instance in the Blockchain Platform Manager.

To start or stop an instance:

1. In Blockchain Platform Manager, find your instance and select the menu beside it.
2. Select **Start** or **Stop**. You'll be prompted to confirm your selection.

Delete an Instance

You can delete your instance in Blockchain Platform Manager.

To delete your instance:

1. Open Blockchain Platform Manager and find your instance.
2. From the menu beside your instance, select **Terminate**.
3. You'll be prompted to confirm your action. Click **Confirm**.

Scale an Instance In or Out

You can scale an instance in or out in Blockchain Platform Manager.

Scale Out

You can scale out your instance by increasing replicas or creating peers or orderers:

1. In Blockchain Platform Manager open the **Actions** menu in the instance details page and click **Scale Out**.
2. You can scale out using any of these methods:
   - **New Replicas**: adds additional nodes; REST proxy or CA.
   - **New Peers**: adds one additional peer at a time.
   - **New Orderers**: adds additional orderers.

Scale In

You can scale in your instance by deleting peers.

Before scaling in an instance, you must transfer all this peer's responsibilities to other running peers, and then remove all the responsibilities this peer has.

- Check all other peers' gossip bootstrap address lists, remove the peer address, and add another running peer's address if needed. After the peer configuration change, restart the peer.
- Check all channels' anchor peer lists, remove the peer from the anchor peer lists, and add another running peer to the anchor peer list if needed.
- If a channel or chaincode is only joined or installed on this peer, consider using another running peer to join the same channel and install the same chaincode.

1. In Blockchain Platform Manager open the **Actions** menu in the instance details page and click **Scale In**.
2. Select the peer that you want to delete.

Manage Ephemeral Storage on Kubernetes

Kubernetes pods require ephemeral (temporary) local storage.

Kubernetes pods use ephemeral storage for scratch space, caching, and logs. This storage is temporary and specific to the life cycle of the pod. Ephemeral storage is not shared across pods and it goes away when the pod is deleted.

For more general information about Kubernetes ephemeral storage, see Local ephemeral storage in the Kubernetes documentation.

The following steps apply to Oracle Kubernetes Engine, but the concepts are similar in other Kubernetes environments.

In a node pool, the nodes use their boot volumes for pod storage. Because images are stored in the `/var` directory, most of the ephemeral storage is occupied by images in the root partition. The space needed in the boot volume increases every time that you install an instance of Oracle Blockchain Platform Enterprise Edition and create chaincodes on that node.

You can use the following kubelet API call to check the total ephemeral storage and the amount to assigned to each pod in a given node:

```
kubectl get --raw "/api/v1/nodes/<node IP>/proxy/stats/summary"
```

The `rootfs` and `fs` sections of the JSON result show the capacity and the available bytes.

You can update the amount of ephemeral storage by resizing the boot volume while a node is running. For more information, see Updating a Node Pool for Oracle Kubernetes Engine.

Complete the following steps to resize the ephemeral storage on an Oracle Kubernetes Engine cluster with running nodes.

1. On your Oracle Kubernetes Engine cluster, under **Resources**, select **Node pools**.
2. Click **Edit**. On the Edit node pool page, select **Specify a custom boot volume size** and then enter a **Boot volume size** value in GB. Any nodes that are created will use this value for ephemeral storage.
3. For each worker node in the node pool, complete the following steps to resize the boot volume.
    a. Click the down arrow beside the node to see detailed information about the node.
    b. Navigate to the **Boot volume** for the node and then click **Edit**.
    c. On the Edit volume page under **Volume size and performance**, specify a **Volume size** value in GB and then click **Save changes**.
4. Complete the following steps to set up a Bastion session and then use it to connect to the private worker nodes.
    a. On the instance details page, click the **Oracle Cloud Agent** tab, and then enable the **Bastion** plugin.
    b. Search for `bastion` in the search bar, and then click **Bastion Identity & Security** under Services in the results.
    c. Click **Create bastion**.
    d. On the Create bastion page, for the **Target virtual cloud network** (VCN) specify the Oracle Kubernetes Engine VCN followed by the cluster name. For **Target subnet**, specify the Kubernetes API endpoint. For **CIDR block allowlist**, enter `0.0.0.0/0`, and then click **Create bastion**.
    e. Click the bastion to open it, and then click **Create session**.
    f. Enter `opc` for the **Username** value and select your node from the **Compute instance** list.
    g. Paste your SSH key under **Add SSH Key**.
    h. Click **Show advanced options** and then select the IP address of the node or instance from the **Target compute instance IP address** list. This is the private IPv4 address of the node or instance, which is available in the information section for the instance.
    i. Click **Create session**.
    j. From the context menu for the session, click **Copy SSH command**.

k. You can now log in to the node via SSH by providing your private key with the `-i` parameter in the SSH command.

l. Repeat the previous steps for each worker node in the cluster.

5. For each node, log in to the node via SSH and then run the following commands, which scan for new block storage devices added to instances or nodes, and then expand the file system when storage is available.

```
sudo dd iflag=direct if=/dev/oracleoci/oraclevda of=/dev/null count=1
echo "1" | sudo tee /sys/class/block/`readlink /dev/oracleoci/oraclevda |
cut -d'/' -f 2`/device/rescan
sudo /usr/libexec/oci-growfs -y
```

Determining Ephemeral Storage Usage

You can run the following script to see the ephemeral storage usage of an instance running on Oracle Kubernetes Engine. The script uses the Kubernetes API to retrieve ephemeral storage usage for each pod that is running on each node in the cluster.

```
#!/usr/bin/env bash

kubectl proxy --append-server-path &

set -eo pipefail

{
    echo "NODE NAMESPACE POD EPHEMRAL_USED"
    for node in $(kubectl get nodes -o=jsonpath='{range .items[*]}
{.metadata.name}{"\n"}{end}'); do
        curl -fsSL "http://127.0.0.1:8001/api/v1/nodes/$node/proxy/stats/
summary" |
            yq '.pods[] | [.podRef.namespace, .podRef.name, .ephemeral-
storage.usedBytes] | join(" ")' |
            while read -r namespace name usedBytes; do
                # A pod might have no running containers and consequently no
ephemeral-storage usage.
                echo "$node" "$namespace" "$name" "$(numfmt --to iec "$
{usedBytes:-0}")"
            done
    done | sort -k4,4rh
} | column -t
```

Additional Steps When Replacing Worker Nodes

When you replace an existing worker node (where peers/orderers are running) with a new worker node, you must also complete the following additional steps:

1. Ensure that the Persistent Volumes that are mounted on the existing node can be migrated to and accessed from the new node. To do this on Oracle Kubernetes Engine, create a node in the same Availability Domain as the existing node.
2. Stop all instances that use the older node.
3. Cordon and drain the older node. This might affect Blockchain Platform Manager services, if those services are running on the older node. Wait for the running pods to move into the new node.

4. Run the following commands to get the list of all of the peers and orderers that were running on the cordoned node.

```
kubectl get peer -A -o=custom-
columns='NAMESPACE:.metadata.namespace,NAME:.metadata.name,NODESELECTOR:.sp
ec.nodeSelector'
kubectl get orderernode -A -o=custom-
columns='NAMESPACE:.metadata.namespace,NAME:.metadata.name,NODESELECTOR:.sp
ec.nodeSelector'
```

5. For the peers and orderers that were configured with `nodeSelector` for the older node, run the following commands to update the custom resource `.spec.nodeSelector` to select the new node.

```
kubectl patch peer <PEER> -n <NAMESPACE> -p '{"spec":{"nodeSelector":
{"kubernetes.io/hostname":"<NEW_NODE_HOSTNAME>"}}}' --type='merge'
kubectl patch orderernode <ORDERER> -n <NAMESPACE> -p '{"spec":
{"nodeSelector":{"kubernetes.io/hostname":"<NEW_NODE_HOSTNAME>"}}}' --
type='merge'
```

6. Verify the updated `nodeSelector` value by running the commands from Step 4 again.
7. Start all instances that were previously stopped.

Configure a Proxy

If your instance runs in a private network without internet connectivity, you must configure a proxy for the blockchain services.

Complete the following tasks to set up a proxy for your blockchain instances.

Create a Service Entry

Use the following configuration to create an Istio `ServiceEntry` object as an external proxy in your instance namespace. You must create a TCP (not HTTP) `ServiceEntry` object to enable Istio-controlled traffic to the external proxy. For more information, see Configure traffic to external HTTPS proxy in the Istio documentation.

```
apiVersion: networking.istio.io/v1alpha3
kind: ServiceEntry
metadata:
  name: obpee-ext-proxy
  namespace: <INSTANCE_NAMESPACE>
spec:
  hosts:
  - <PROXY-HOST-FQDN>
  addresses:
  - <PROXY-IP-ADDRESS>
  exportTo:
  - "."
  location: MESH_EXTERNAL
  ports:
  - number: <PROXY-PORT-NUMBER>
    name: tcp
    protocol: TCP
```

Configure the Proxy Environment

The Oracle Blockchain Platform Enterprise Edition distribution package includes the `setProxy.sh` script, which you can use to configure the proxy environment for all services of the blockchain instance. Run the following commands from the command line. When the `setProxy.sh` script runs, it restarts the required blockchain services in your Kubernetes cluster.

```
# Configure environment variables before running the script
export mspId="<INSTANCE_NAME>"
export httpProxy="<HTTP_PROXY>"
export httpsProxy="<HTTPS_PROXY>"
export noProxy="<NO_PROXY>"

# Go to the distribution package dir
cd <distribution-package-dir>

# Run the setProxy.sh script
./setProxy.sh
```

7

Logging

You can use Oracle Cloud Infrastructure (OCI) or external tools to configure persistent logging for Oracle Blockchain Platform Enterprise Edition.

Overview

Oracle Blockchain Platform Enterprise Edition is based on Kubernetes, where logs are stored locally on each pod. To prevent logs from being deleted when a pod is deleted, you must set up persistent logging, where logs are stored in a central location. There are two methods you can use for persistent logging. You can use an external logging tool such as Fluentd and Elastic Stack. Alternately, if you are running on Oracle Kubernetes Engine, you can use the centralized logging solution supported by Oracle Cloud Infrastructure (OCI).

Persistent Logging with OCI

To store logs centrally using OCI, you define log groups and configure agents to parse the logs. The logs are stored in the Object Storage service. Before you configure persistent logging with OCI, your deployment must meet the following requirements.

- A dynamic group in the Kubernetes compartment. To create a dynamic group, click **Identity & Security** in the navigation menu. Under **Identity**, click **Domains** and then click **Create dynamic group**. Add the following to your dynamic group in the **Matching rules** section, substituting the Oracle Cloud ID for your compartment.

  ```
  instance.compartment.id = '<compartment_ocid>'
  ```

  For example:

  ```
  instance.compartment.id =
  'ocid1.compartment.oc1..aaaaaaaa4ws3242343243244nyb423432rwqsxigt2sia'
  ```

- A policy that allows the dynamic group to interact with the logging service. To create a policy, click **Identity & Security** in the navigation menu. Under **Identity**, click **Policies** and then click **Create Policy**.

  ```
  Allow dynamic-group <my-group> to use log-content in compartment
  <target_compartment_name>
  ```

  For example:

  ```
  Allow dynamic-group okelogging to use log-content in compartment
  BlockchainTeam
  ```

After you have satisfied the prerequisites, complete the following steps to store logs centrally using OCI.

1. Click the menu icon in the upper left corner, search for `log`, and then select **Logs**.
2. Create a log group. Under Logging, select **Log Groups** and then click **Create Log Group**.
3. Create a custom log. Under Logging, select **Logs** and then click **Create custom log** to open the Create custom log wizard. Select the log group that you created previously.
4. On the second page of the Create custom log wizard, create an agent configuration for the custom log, specifying the Kubernetes compartment and the dynamic group.
5. In the **Configure log inputs** section of the Agent configuration page, configure the log input for the agent to use the following file path, which is the default for application containers. Select **Log path** from the **Input type** list. Enter the following file path for **File paths**. This path includes all container logs, including system and service containers.

   ```
   /var/log/pods/*/*/*.log
   ```

6. Wait until logs are ingested. Typically, logs are ingested in 3-5 minutes.
7. Select **Logs** and then navigate to the custom log and click **Explore Log**. You can analyze, parse, and filter the logs.
8. You can also use OCI to store the logs in the Object Storage service.
   a. Create a connector. Under Logging, select **Connectors** and then click **Create Connector**. Select **Logging** as the **Source** and **Object Storage** as the **Target**.
   b. Configure the source and target as needed.
   c. Under the **Enable logs** section, set **Enable Log** to **Enabled** for the connector that you created. The Create Log panel is displayed, with a default value for log retention time.
   d. Wait until logs are ingested. Typically, logs are ingested in 3-5 minutes. You can then see read and write operations in the connector logs. Logs are now being written to the Object Storage service.

For more information, see Monitor Kubernetes and OKE clusters with OCI Logging Analytics.

Persistent Logging with External Tools

You can store logs centrally using Fluentd and Elastic Stack. The following steps have been tested with Fluentd v1.16.2 and Elasticsearch 7.9.1. Use these versions or later when you complete these steps.

1. Create a Kubernetes namespace called `fluentd`.
2. Use the following command to create a role-based access control resource.

   ```
   kubectl create -f fluentd-rbac.yaml -n fluentd
   ```

   Use the following `fluentd-rbac.yaml` file with the command.

   ```
   apiVersion: v1
   kind: ServiceAccount
   metadata:
     name: fluentd
     namespace: fluentd
   ---
   apiVersion: rbac.authorization.k8s.io/v1
   ```

```
kind: ClusterRole
metadata:
  name: fluentd
  namespace: fluentd
rules:
- apiGroups:
  - ""
  resources:
  - pods
  - namespaces
  verbs:
  - get
  - list
  - watch
---
kind: ClusterRoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: fluentd
roleRef:
  kind: ClusterRole
  name: fluentd
  apiGroup: rbac.authorization.k8s.io
subjects:
- kind: ServiceAccount
  name: fluentd
  namespace: fluentd
```

3. Use the following command to create a `ConfigMap` object for Fluentd or Elastic Stack.

```
kubectl create -f fluentd-configmap_removefilter_ascii.yaml -n fluentd
```

Use the following `fluentd-configmap_removefilter_ascii.yaml` file with the command.
In the following file, remove the number sign (#) to uncomment only one of the following lines.

- Uncomment `@include file-fluent.conf` if you are writing to a file in the `/tmp/obp.log` path.
- Uncomment `@include elastic-fluent.conf` if you are writing to Elasticsearch.

The following file shows an example of writing to the `/tmp/obp.log` path.

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: fluentd-config
  namespace: fluentd
data:
  fluent.conf: |-
    ##################################################################
    # This source gets all logs from local docker host
    #@include pods-kind-fluent.conf
    #@include pods-fluent.conf
    @include pods-nofilter.conf
```

```
    @include file-fluent.conf
    #@include elastic-fluent.conf
  pods-nofilter.conf: |-
    <source>
      @type tail
      path /var/log/containers/*.log
      format //^(?<time>.+) (?<stream>stdout|stderr) (?<logtag>.)? (?
<log>.*)$/ /
      pos_file /var/log/fluentd-containers.log.pos
      tag kubernetes.*
      read_from_head true
    </source>
    <filter kubernetes.**>
     @type kubernetes_metadata
    </filter>
  file-fluent.conf: |-
     <match kubernetes.var.log.containers.**fluentd**.log>
      @type null
     </match>
     <match kubernetes.var.log.containers.**kube-system**.log>
       @type null
     </match>
     <match kubernetes.**>
       @type file
       path /tmp/obp.log
     </match>
  elastic-fluent.conf: |-
    <match kubernetes.var.log.containers.**fluentd**.log>
      @type null
    </match>
    <match kubernetes.var.log.containers.**kube-system**.log>
      @type null
    </match>
    <match kubernetes.**>
      @type elasticsearch
      host "#{ENV['FLUENT_ELASTICSEARCH_HOST'] || 'elasticsearch.elastic-
kibana'}"
      port "#{ENV['FLUENT_ELASTICSEARCH_PORT'] || '9200'}"
      index_name fluentd-k8s-3
      type_name fluentd
      include_timestamp true
    </match>
```

4. Use the following command to create a `DaemonSet` object for Fluentd. This command creates a Fluentd pod on each node.

   ```
   kubectl create -f fluentd.yaml -n fluentd
   ```

   Use the following `fluentd.yaml` file with the command.

   ```
   apiVersion: apps/v1
   kind: DaemonSet
   metadata:
     name: fluentd
     namespace: fluentd
   ```

```
    labels:
      k8s-app: fluentd-logging
      version: v1
  spec:
    selector:
      matchLabels:
        k8s-app: fluentd-logging
        version: v1
    template:
      metadata:
        labels:
          k8s-app: fluentd-logging
          version: v1
      spec:
        serviceAccount: fluentd
        serviceAccountName: fluentd
        tolerations:
        - key: node-role.kubernetes.io/master
          effect: NoSchedule
        - key: node-role.kubernetes.io/control-plane
          effect: NoSchedule
        containers:
        - name: fluentd1
          imagePullPolicy: "Always"
          image: fluent/fluentd-kubernetes-daemonset:v1.16.2-debian-
elasticsearch7-1.1
          env:
            - name:  FLUENT_ELASTICSEARCH_HOST
              value: "elasticsearch.elastic-kibana"
            - name:  FLUENT_ELASTICSEARCH_PORT
              value: "9200"
          resources:
            limits:
              memory: 200Mi
            requests:
              cpu: 100m
              memory: 200Mi
          volumeMounts:
          - name: fluentd-config
            mountPath: /fluentd/etc
          - name: logs
            mountPath: /tmp
          - name: varlog
            mountPath: /var/log
          - name: varlibdockercontainers
            mountPath: /var/lib/docker/containers
            readOnly: true
        terminationGracePeriodSeconds: 30
        volumes:
        - name: fluentd-config
          configMap:
            name: fluentd-config
        - name: varlog
          hostPath:
            path: /var/log
        - name: varlibdockercontainers
```

```
        hostPath:
          path: /var/lib/docker/containers
      - name: logs
        hostPath:
          path: /tmp
```

The Oracle Blockchain Platform logs are available in the `/tmp` directory of the Fluentd pod or the Kubernetes node.

5. To send the logs to Elastic Stack, create a Kubernetes namespace called `elastic-kibana`.
6. Use the following command to create a deployment for Elastic Stack and to expose it as a service.

```
kubectl create -f elastic.yaml -n elastic-kibana
```

Use the following `elastic.yaml` file with the command.

```
apiVersion: v1
kind: Namespace
metadata:
  name: elastic-kibana

---
apiVersion: apps/v1
kind: Deployment
metadata:
  name: elasticsearch
  namespace: elastic-kibana
  labels:
    app: elasticsearch
spec:
  selector:
    matchLabels:
      app: elasticsearch
  replicas: 1
  template:
    metadata:
      labels:
        app: elasticsearch
    spec:
      initContainers:
      - name: vm-max-fix
        image: busybox
        command: ["sysctl", "-w", "vm.max_map_count=262144"]
        securityContext:
          privileged: true
      containers:
      - name: elasticsearch
        image: elasticsearch:7.9.1
        imagePullPolicy: IfNotPresent
        ports:
        - containerPort: 9200
        env:
        - name: node.name
          value: "elasticsearch"
```

```
        - name: cluster.initial_master_nodes
          value: "elasticsearch"
        - name: bootstrap.memory_lock
          value: "false"
        - name: ES_JAVA_OPTS
          value: "-Xms512m -Xmx512m"
---
apiVersion: v1
kind: Service
metadata:
  name: elasticsearch
  namespace: elastic-kibana
  labels:
    app: elasticsearch
spec:
  type: ClusterIP
  selector:
    app: elasticsearch
  ports:
    - protocol: TCP
      name: http
      port: 9200
      targetPort: 9200
```

7. You can then use the following commands to examine the log data in the Elasticsearch index.

```
curl -X GET "localhost:9200/_cat/indices/fluentd-k8s-*?
v=true&s=index&pretty"
curl -X GET "localhost:9200/fluentd-k8s-3/_search?pretty=true"
```

8. You can also use Fluentd to store the log on the local block volume on each node.
   a. Create a block volume for each node, attach the volume, and create a directory called `/u01`.
   b. Format the attached block volume for the ext4 file system.
   c. Mount the `/u01` directory on the device path.
   d. Change the Fluentd deployment file (`fluentd.yaml`) so that the logs volume is `/u01`, not `/tmp`, as shown in the following snippet.

```
- name: logs
        hostPath:
          path: /u01
```

   e. Run the following command to apply the Fluentd deployment.

```
kubectl apply -f fluentd.yaml -n fluentd
```

   f. The logs are now visible in the /u01 directory on each node.

Set the Log Level for Operator Pods

You can set the log level for the `hlf-operator` and `obp-operator` pods. The steps to set the log level are different depending on whether Oracle Blockchain Platform is installed. If Oracle Blockchain Platform Enterprise Edition is not yet installed, complete the following steps.

1. Open the corresponding `deployment.yaml` file for editing. The file for the `hlf-operator` pod is in the following location:

   ```
   distribution_package_location/distribution-package/operators/helmcharts/
   hlf-operator/templates/deployment.yaml
   ```

   The file for the `obp-operator` pod is in the following location:

   ```
   distribution_package_location/distribution-package/operators/helmcharts/
   obp-operator/templates/deployment.yaml
   ```

2. Add the following line to the file. As shown in the comment, you can set the log level to `debug`, `info`, or `error`. In the following example the log level is set to `info`.

   ```
   --zap-log-level=info # debug, info, error
   ```

After you edit the file, that section of the file might look similar to the following text:

```
containers:
    - args:
    - --enable-leader-election
    - --zap-log-level=info # debug, info, error
```

If Oracle Blockchain Platform is already installed, complete the following step.

- Use the following commands to edit the deployment definitions for the `hlf-operator` and `obp-operator` pods. Add or update the argument that configures the log level for the `manager` container under the pod template specification.

  ```
  kubectl edit deployment -n obp-cp obp-operator
  kubectl edit deployment -n obp-cp hlf-operator-controller-manager
  ```

After you update the container arguments, the deployment definition might look similar to the following text:

```
containers:
    - args:
    - --enable-leader-election
    - --zap-log-level=info # debug, info, error
```

A

Accessibility Features and Tips for Oracle Blockchain Platform

This topic describes accessibility features and information for Oracle Blockchain Platform.

Table A-1 Keyboard Shortcuts for Blockchain Platform Manager

Task	Keyboard Shortcut
Create an Oracle Blockchain Platform instance.	Windows: Alt+Shift+C Mac: Shift+Option+C
Refresh the Instance Summary page.	Windows: Alt+Shift+R Mac: Shift+Option+R