Overview of Block Volume

The Oracle Cloud Infrastructure Block Volume service lets you dynamically provision and manage block storage volumes . You can create, attach, connect, and move volumes, as well as change volume performance, as needed, to meet your storage, performance, and application requirements. After you attach and connect a volume to an instance, you can use the volume like a regular hard drive. You can also disconnect a volume and attach it to another instance without the loss of data.

These components are required to create a volume and attach it to an instance:

Instance: A bare metal or virtual machine (VM) host running in the cloud.
Volume attachment: There are two types of volume attachments:

iSCSI: A TCP/IP–based standard used for communication between a volume and attached instance.

Paravirtualized: A virtualized attachment available for VMs.

Volume: There are two types of volumes:

Block volume: A detachable block storage device that allows you to dynamically expand the storage capacity of an instance.

Boot volume: A detachable boot volume device that contains the image used to boot a Compute instance. See Boot Volumes for more information.

For additional Oracle Cloud Infrastructure terms, see the Glossary.

Block Volume is Always Free eligible. For more information about Always Free resources, including capabilities and limitations, see Oracle Cloud Infrastructure Free Tier.
 Tip

Watch a video introduction to the service.

Typical Block Volume Scenarios

Scenario A: Expanding an Instance's Storage

A common usage of Block Volume is adding storage capacity to an Oracle Cloud Infrastructure instance. After you have launched an instance and set up your cloud network, you can create a block storage volume through the Console or API. Then, you attach the volume to an instance using a volume attachment. After the volume is attached, you connect to the volume from your instance's guest OS using iSCSI . The volume can then be mounted and used by your instance.

Scenario B: Persistent and Durable Storage

A Block Volume volume can be detached from an instance and moved to a different instance without the loss of data. This data persistence enables you to migrate data between instances and ensures that your

data is safely stored, even when it is not connected to an instance. Any data remains intact until you reformat or delete the volume.

To move your volume to another instance, unmount the drive from the initial instance, terminate the iSCSI connection, and attach the volume to the second instance. From there, you connect and mount the drive from that instance's guest OS to have access to all of your data.

Additionally, Block Volume volumes offer a high level of data durability compared to standard, attached drives. All volumes are automatically replicated for you, helping to protect against data loss, see Block Volume Durability.

Scenario C: Instance Scaling
When you terminate an instance, you can keep the associated boot volume and use it to launch a new instance with a different instance type or shape. This allows you to easily switch from a bare metal instance to a VM instance and vice versa, or scale up or scale down the number of cores for an instance. See Creating an Instance for steps to launch an instance based on a boot volume.

Volume Attachment Types
When you attach a block volume to a VM instance, you have two options for attachment type, iSCSI or paravirtualized. Paravirtualized attachments simplify the process of configuring your block storage by removing the extra commands that are required before connecting to an iSCSI-attached volume. The trade-off is that IOPS performance for iSCSI attachments is greater than that for paravirtualized attachments. You should consider your requirements when selecting a volume's attachment type.

Important

Connecting to Volumes on Linux Instances

When connecting to volumes on Linux instances, if you want to automatically mount these volumes on instance boot, you need to use some specific options in the /etc/fstab file, or the instance may fail to launch. See Traditional fstab Options and fstab Options for Block Volumes Using Consistent Device Paths for more information.

iSCSI
iSCSI attachments are the only option when connecting a block volume to any of the following types of instances:

Bare metal instances
VM instances based on Windows images that were published before February 2018
VM instances based on Linux images that were published before December 2017
After the volume is attached, you need to log in to the instance and use the iscsiadm command-line tool to configure the iSCSI connection. For more information about the additional configuration

steps required for iSCSI attachments, see iSCSI Commands and Information, Connecting to a Block Volume, and Disconnecting From a Volume.

IOPS performance is better with iSCSI attachments compared to paravirtualized attachments. For more information about iSCSI-attached volume performance, see Block Volume Performance.

Paravirtualized
Paravirtualized attachments are an option when attaching volumes to the following types of VM instances:

For VM instances launched from platform images, you can select this option for Linux-based images published in December 2017 or later, and Windows images published in February 2018 or later.
For VM instances launched from custom images, the volume attachment type is based on the volume attachment type from the VM the custom image was created from.
After you attach a volume using the paravirtualized attachment type, it is ready to use, and you do not need to run any additional commands. However, because of the overhead of virtualization, this reduces the maximum IOPS performance for larger block volumes.

Volume Access Types
When you attach a block volume, you can specify one of the following options for access type:

Read/write: This is the default option for volume attachments. With this option, an instance can read and write data to the volume.
Read/write, shareable: With this option, you can attach a volume to more than one instance at a time and those instances can read and write data to the volume. To prevent data corruption from uncontrolled read/write operations with multiple instance volume attachments you must install and configure a cluster-aware solution for your system before you can use the volume. See Configuring Multiple Instance Volume Attachments with Read/Write Access for more information.

Read-only: With this option, an instance can only read data on the volume. It cannot update data on the volume. Specify this option to safeguard data against accidental or malicious modifications.
To change the access type for a block volume, you need to detach the volume and specify the new access type when you reattach the volume. For more information, see Detaching a Volume and Attaching a Block Volume to an Instance.

The access type for boot volumes is always read/write. If you want to change the access type, you need to stop the instance and detach the boot volume. You can then reattach it to another instance as a block volume, with read-only specified as the access type. For more information, see Detaching a Boot Volume and Attaching a Block Volume to an Instance.

Device Paths

When you attach a block volume to a compatible Linux-based instance, you can select a device path that remains consistent between instance reboots. This enables you to refer to the volume using a consistent device path. For example, you can use the device path when you set options in the /etc/fstab file to automatically mount the volume on instance boot.

Consistent device paths are supported and enabled by default on instances when all of the following things are true:

The instance was created using a platform image.
The image is a Linux-based image.
The image was released in November 2018 or later. For specific version numbers, see Image Release Notes.
The instance was launched after January 11, 2019.
For instances launched using the image OCID or an existing boot volume, if the source image supports consistent device paths, the instance supports device paths.

Consistent device paths are not enabled by default for Linux-based partner images and custom images created from other sources. You can enable consistent device paths for these images by editing the image capabilities for the custom image using the steps described below. This feature does not apply to Windows-based images.

For more information about consistent device paths, see Connecting to Volumes With Consistent Device Paths.

Regions and Availability Domains
Volumes are only accessible to instances in the same availability domain . You cannot move a volume between availability domains or regions, they are only accessible within the region or availability domain they were created in. However volume backups are not limited to the availability domain of the source volume, you can restore them to any availability domain within that region, see Restoring a Backup to a New Volume. You can also copy a volume backup to a new region and restore the backup to a volume in any availability domain in the new region, for more information see Copying a Volume Backup Between Regions.

For more information, see Regions and Availability Domains.

Resource Identifiers
Most types of Oracle Cloud Infrastructure resources have a unique, Oracle-assigned identifier called an Oracle Cloud ID (OCID). For information about the OCID format and other ways to identify your resources, see Resource Identifiers.

Ways to Access Oracle Cloud Infrastructure
You can access Oracle Cloud Infrastructure (OCI) by using the Console (a browser-based interface), REST API, or OCI CLI. Instructions for using the Console, API, and CLI are included in topics throughout this documentation. For a list of available SDKs, see Software Development Kits and Command Line Interface.

To access the Console, you must use a supported browser. To go to the Console sign-in page, open the navigation menu at the top of this page and click Infrastructure Console. You are prompted to enter your cloud tenant, your user name, and your password.

For general information about using the API, see REST APIs.

Authentication and Authorization
Each service in Oracle Cloud Infrastructure integrates with IAM for authentication and authorization, for all interfaces (the Console, SDK or CLI, and REST API).

An administrator in your organization needs to set up groups , compartments , and policies that control which users can access which services, which resources, and the type of access. For example, the policies control who can create new users, create and manage the cloud network, launch instances, create buckets, download objects, and so on. For more information, see Getting Started with Policies. For specific details about writing policies for each of the different services, see Policy Reference.

If you’re a regular user (not an administrator) who needs to use the Oracle Cloud Infrastructure resources that your company owns, contact your administrator to set up a user ID for you. The administrator can confirm which compartment or compartments you should be using.

Security
In addition to creating IAM policies, follow these security best practices for Block Volume.

Encrypt volumes with a custom key, and rotate keys
Take regular backups
Use Oracle Cloud Guard to detect and respond to security problems
Perform a security audit
See Securing Block Volume.

Monitoring Resources
You can monitor the health, capacity, and performance of your Oracle Cloud Infrastructure resources by using metrics, alarms, and notifications. For more information, see Monitoring and Notifications.

Moving Resources
You can move Block Volume resources such as block volumes, boot volumes, volume backups, volume groups, and volume group backups from one compartment to another. For more information, see Move Block Volume Resources Between Compartments.

Tagging Resources
Apply tags to your resources to help organize them according to your business needs. Apply tags at the time you create a resource, or update the resource later with the wanted tags. For general

information about applying tags, see Resource Tags.

Creating Automation with Events

You can create automation based on state changes for your Oracle Cloud Infrastructure resources by using event types, rules, and actions. For more information, see Overview of Events.

The following Block Volume resources emit events:

Block volumes and block volume backups
Boot volumes and boot volume backups
Volume groups and volume group backups

Note

For troubleshooting, see Known Issues - Block Volume for a list of known issues related to Block Volume events.

Block Volume Encryption

The Oracle Cloud Infrastructure Block Volume service always encrypts all block volumes, boot volumes, and volume backups at rest by using the Advanced Encryption Standard (AES) algorithm with 256-bit encryption. By default all volumes and their backups are encrypted using the Oracle-provided encryption keys. Each time a volume is cloned or restored from a backup the volume is assigned a new unique encryption key.

You have the option to encrypt all of your volumes and their backups using the keys that you own and manage using the Vault service, for more information see Overview. If you do not configure a volume to use the Vault service or you later unassign a key from the volume, the Block Volume service uses the Oracle-provided encryption key instead. This applies to both encryption at-rest and paravirtualized in-transit encryption.

For how to use your own key for new volumes, see Creating a Block Volume. See Editing a Key to a Block Volume for how to assign or change the key for an existing volume.

Important

The Block Volume service does not support encrypting volumes with keys encrypted using the Rivest-Shamir-Adleman (RSA) algorithm. When using your own keys, you must use keys encrypted using the Advanced Encryption Standard (AES) algorithm. This applies to block volumes and boot volumes.

In-transit Encryption

All the data moving between the instance and the block volume is transferred over an internal and highly secure network. If you have specific compliance requirements related to the encryption of the data while it is moving between the instance and the block volume, the Block Volume service provides the option to enable in-transit encryption for paravirtualized volume attachments on virtual machine (VM) instances.

Note

In-transit encryption is not enabled for these shapes in the following scenarios:

Boot volumes for instances launched June 8, 2021 or earlier.
Volumes attached to the instance June 8, 2021 or earlier
To enable in-transit encryption for the volumes in these scenarios, you need to detach the volume from the instance and then reattach it.

Important

In-transit encryption for boot and block volumes is only available for virtual machine (VM) instances launched from platform images, along with bare metal instances that use the following shapes: BM.Standard.E3.128, BM.Standard.E4.128, BM.DenseIO.E4.128. It is not supported on other bare metal instances. To confirm support for certain Linux-based custom images and for more information, contact Oracle support.

Important

For bare metal instances that support in-transit encryption, including instances launched from custom images, it is always enabled by default. This applies to both boot volumes and block volumes. The following bare metal shapes support in-transit encryption for the instance's boot volume as well as iSCSI-attached block volumes:

BM.Standard.E3.128
BM.Standard.E4.128
BM.DenseIO.E4.128

Note

In-transit encryption for bare metal instances is not supported for US Government Cloud regions.

Block Volume Data Eradication

The Oracle Cloud Infrastructure Block Volume service uses eventual-overwrite data eradication with cryptographic erasure to guarantee that your data is properly disposed of. When you terminate a volume, its associated data is overwritten in the storage infrastructure with cryptographic erasure before any future volume allocations.

Block Volume Performance

Block Volume performance varies with volume size, see Block Volume Performance for more information.

You can select from one of the following volume performance levels to meet the requirements for your block volumes:

Balanced

Ultra High Performance

Higher Performance

Lower Cost

If your requirements change, you can change the performance level for the volume. For how to adjust the performance for a volume, see Changing the Performance of a Volume.

Block Volume provides dynamic performance scaling with autotuning, see Dynamic Performance Scaling for more information.

Volume Replication
The Block Volume service provides you with the capability to perform ongoing automatic asynchronous replication of block volumes and boot volumes to other regions or availability domains within the same region. Cross availability domain replication within the same region is only supported for regions with more than one availability domian. To determine which regions contain more than one availability domain, see the Availability Domains field in the table listing the regions in About Regions and Availaibility Domains.

This feature supports disaster recovery, migration, and business expansion scenarios, without requiring volume backups. See Replicating a Volume for more information.

Block Volume Durability
The Oracle Cloud Infrastructure Block Volume service offer a high level of data durability compared to standard, attached drives. All volumes are automatically replicated for you, helping to protect against data loss. Multiple copies of data are stored redundantly across multiple storage servers with built-in repair mechanisms. For service level objective, the Block Volume service is designed to provide 99.99 percent annual durability for block volumes and boot volumes. However, we recommend that you make regular backups to protect against the failure of an availability domain.

Block Volume Capabilities and Limits
Block Volume volumes can be created in sizes ranging from 50 GB to 32 TB in 1 GB increments. By default, Block Volume volumes are 1 TB.

For a list of applicable limits and instructions for requesting a limit increase, see Service Limits. To set compartment-specific limits on a resource or resource family, administrators can use compartment quotas.

Additional limits include:

Attached block volumes per instance:
32 attached block volumes for all shapes, except for the following VM shapes which have a limit of 16 paravirtualized-attached block volumes:
VM.Standard2.8
VM.DenseIO2.8
VM.Standard.E2.8
VM.Standard.E3.Flex

VM.Standard.E4.Flex
VM.Standard.A1.Flex
VM.Optimized3.Flex
Attached boot volumes per instance:
One attached boot volume

Note

Boot volumes attached to an instance as a data volume and not as the instance's boot volume count towards the limit for attached block volumes.
Number of backups

Monthly universal credits: 100,000

Pay-as-you-go: 100,000