Scaling on the cloud

Learn about scaling on the cloud by using a) Redundancy b) Monitoring c) Failover.

Highly Available (HA) Architecture

Introduction

This reference architecture provides the best practices needed for planning, designing, and deploying High Availability (HA) architectures that can be followed for any Cloud Infrastructure Service. A high availability service or application is one designed for maximum potential uptime and accessibility. To design a high availability architecture, three key elements should be considered

1. Redundancy
2. Monitoring
3. Failover

Redundancy

Redundancy means that multiple components can perform the same task. The problem of a single point of failure is eliminated because redundant components can take over a task performed by a component that has failed.

Monitoring

Monitoring checks whether a component is working properly.

Failover

Failover is the process by which a secondary component becomes primary when a primary component failsflev. Although high availability can be achieved at many \ levels, including the application level and the cloud infrastructure level.

High Availability Building Blocks is by region is a localized geographic area composed of several availability domains. An availability domain is one or more data centers located within a region.

Availability zones / domains are isolated from each other, fault tolerant, and very unlikely to fail simultaneously. Because availability domains do not share physical infrastructure, such as power or cooling, or the internal availability zone network, a failure that impacts one availability zone is unlikely to impact the availability of the others. All the availability zone/domain in a region are connected to each other by a low-latency, high bandwidth network.

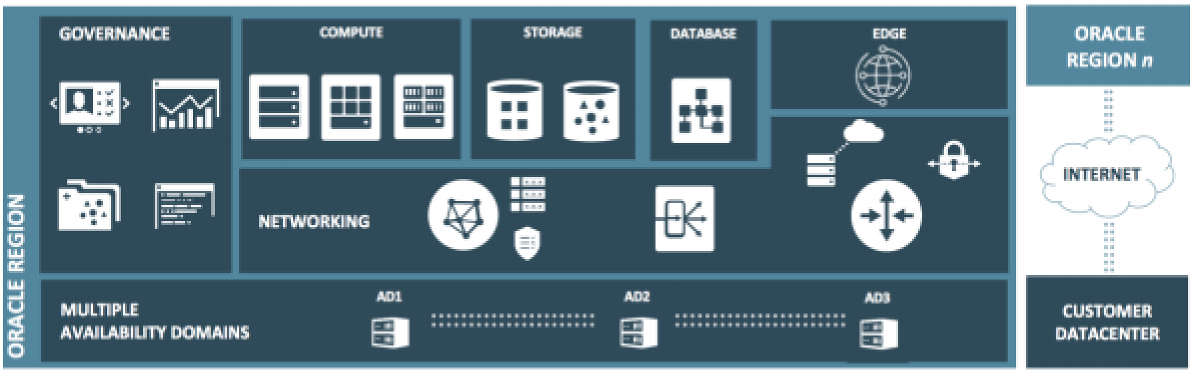
This predictable, encrypted interconnection between availability domains provides the building blocks for both high availability and disaster recovery. Note that cloud Infrastructure resources are either specific to a region, such as a virtual cloud network, or specific to an availability domain, such as a Compute instance.

When you configure your cloud services, if the services are specific to an availability domain, it is important to leverage with multiple availability domains to ensure high availability and to protect against resource failure.

For example, when you deploy a Compute instance, it resides in one particular availability domain. If there is no redundant deployment of this instance to another availability domain, the instance will be impacted when its availability domain encounters any issues.

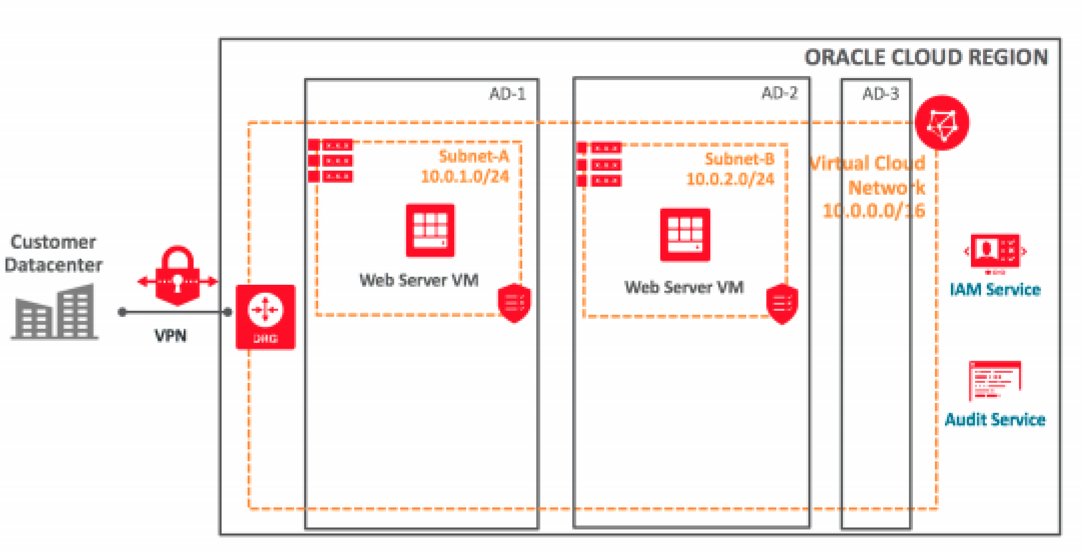
Architecting High Availability Solutions

This describes each Cloud Infrastructure layer and provides detailed best practices and design guidelines for architecting high availability solutions.



Compute High Availability Design Cloud Infrastructure

Compute provides a virtual machine (VM) instances to give the flexibility to deploy any size server that you need. This gives you the performance, flexibility, and control to run your most demanding applications and workloads in the cloud. Elimination of a Single Point of Failure One of the key principles of designing high availability solutions is to avoid single point of failure. It is recommended designing your architecture to deploy Compute instances that perform the same tasks in multiple availability domains. This design removes a single point of failure by introducing redundancy.



Deploy Web Server VMs in Two Availability Domains Depending on your system requirements, you can implement this architecture redundancy in either standby or active mode: In standby mode, a secondary or standby component runs side-by-side with the primary component. When the primary component fails, the standby component takes over. Standby mode is typically used for applications that need to maintain their states.

In active mode, no components are designated as primary or standby; all components are actively participating in performing the same tasks. When one of the components fails, the related tasks are simply distributed to another component. Active mode is typically used for stateless applications.

Network High Availability Design

One of the first steps in working with any Cloud Infrastructure service is to set up a Virtual Cloud Network (VCN) for your cloud resources. A VCN is a software-defined network that you set up in the Cloud data center. A subnet is a subdivision of a cloud network. Ensuring the high availability of your network is one of the most important items in your architecture design.

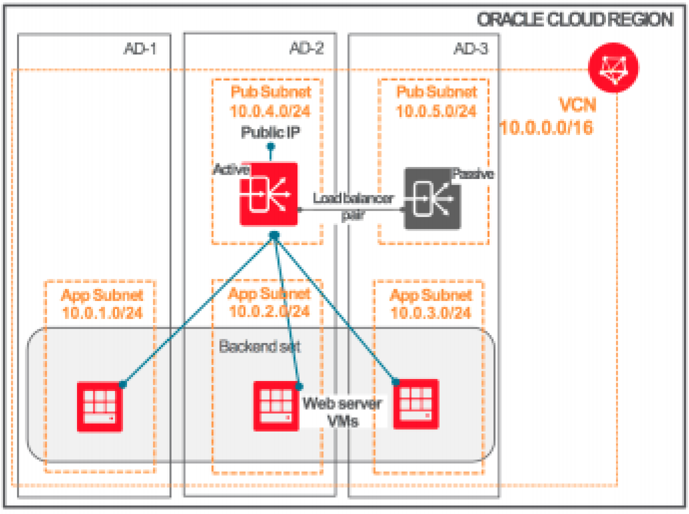
Load Balancing High Availability Design

Cloud Infrastructure services have Load Balancers provides automated traffic distribution from one entry point to multiple servers reachable from your virtual cloud network (VCN). These service offers a load balancer with your choice of a public or private IP address and provisioned bandwidth.

The Load Balancing service improves resource utilization, facilitates scaling, and helps ensure high availability. It supports routing incoming requests to various back-end sets based on virtual hostname, path route rules, or combination of both.

Public Load Balancer accept traffic from the internet. When you create a public load balancer the service assigns it a public IP address that serves as the entry point for incoming traffic. You can associate the public IP address with a friendly DNS name through any DNS vendor. A public load balancer is regional in scope and requires two subnets, each in a separate availability domain. As a result, a public load balancer is inherently highly available across availability domains.

To achieve high availability for your systems, you can put your web server VMs as back-end server sets behind a public load balancer.



Private Load Balancers help isolate your load balancer from the internet and simplify your security posture. The Load Balancing service assigns it a private IP address that serves as the entry point for incoming traffic. When you create a private load balancer, the service requires only one subnet to host both the primary and standby load balancers. In this case, private load balancer service is bounded within an availability domain.

To provide high availability across availability domains, customers can configure multiple private load balancers on Cloud Infrastructure service and use on-premises or private DNS servers to set up a round-robin DNS configuration with the IP addresses of the private load balancers.

FastConnect and VPN High Availability Design

Highly available, fault-tolerant network connections are key to a well-architected system. This section gives guidelines on how to design your network for redundancy so that it meets the requirements for the Cloud Infrastructure IPSec VPNs and FastConnect / DirectConnect service level agreement (SLA). It discusses high availability options for redundant VPN connections, redundant FastConnect connections, and a FastConnect connection with a backup VPN connection. An organization's business-availability and application requirements help determine the most appropriate configuration when designing remote connections.

Generally, however, you should consider using redundant hardware and network service providers between your location and Service Provider's data centers.

Network High Availability Design with FastConnect or Direct Connect

Cloud Infrastructure FastConnect/DirectConnect provides an easy way to create a dedicated, private connection between your data center and the Cloud Infrastructure. FastConnect provides higher-bandwidth options and a more reliable and consistent networking experience compared to internet-based connections. With FastConnect, you can choose to use private peering, public peering, or both. Use private peering to extend your existing infrastructure into a virtual cloud network (VCN) in the Cloud for example, to implement a hybrid cloud, or in a lift and-shift scenario.

FastConnect / Direct Connect - Redundancy

To avoid a single point of failure with redundancy use -

1. Multiple FastConnect locations within each metro area
2. Multiple routers in each FastConnect location
3. Multiple physical circuits in each FastConnect location

4. Cloud Providers normally handle the redundancy of the routers and physical circuits in the FastConnect locations.

In your network design with FastConnect / DirectConnect, it is recommended considering the following redundancy configurations for your high availability requirements:

Availability domain redundancy:

Connect to any FastConnect location and access services located in any availability domain within a region. This now provides availability domain resiliency via multiple POPs per region. Peering connections terminate on routers in the POP.

Data center location redundancy:

Connect at two different FastConnect locations per region.
Router redundancy: Connect to two different routers per FastConnect location.

Circuit redundancy:

Have multiple physical connections at any of the FastConnect locations. Each of these circuits can have multiple physical links in an aggregated interface/LAG, which adds another level of redundancy.

Partner/provider redundancy:

Connect to the FastConnect locations by using single or multiple partners.

Continuous Testing of Redundant Paths

During normal operation, it is recommended using all available paths between your on-premises network and the Cloud. Doing so ensures that if a failure occurs, your redundant path is already working. Alternatively, using an active/backup design means that you trust that your backup path will work during a failure Storage High Availability Design Cloud Infrastructure provides the following storage services:

1. Block Volume
2. Object Storage
3. File Storage

Cloud Infrastructure Block Volume

Cloud Infrastructure Block Volume enables you to dynamically provision and manage block storage volumes. You can create, attach, connect, and move volumes as needed to meet your storage and application requirements. When a volume is attached and connected to an instance, you can use it like a regular hard drive. Volumes can also be disconnected and attached to another Compute instance while the data on the volume is maintained.

Cloud Infrastructure Object Storage

Cloud Infrastructure Object Storage are generally built an internet-scale, high-performance storage platforms that offers reliable and cost-efficient data durability. The Object Storage service can store an unlimited amount of unstructured data of any content type, including analytic data and rich content, like images and videos. Object Storage is a regional service and is available across all the availability domains within a region. Data is stored redundantly across multiple storage servers and across multiple availability domains.

Cloud Infrastructure File Storage

Cloud Infrastructure File Storage provides a durable, scalable, distributed, enterprise-grade network file system. You can connect to a File Storage file system from any virtual machine, or container instance in your Virtual Cloud Network (VCN).

You can also access a file system from outside the VCN by using Cloud Infrastructure FastConnect and IPSec VPNs. Large Compute clusters of thousands of instances can use File Storage for high-performance shared storage, and it provides redundant storage for resilient data protection. To achieve high availability and durability, we recommended the following best practices for the storage layer:

Use Object Storage to back-up application data. Data is stored redundantly across multiple storage servers across multiple availability domains. Data integrity is actively monitored by using checksums, and corrupt data is detected and automatically repaired. Any loss in data redundancy is automatically detected and corrected, without any customer impact.

Use Block Volume policy-based backups to perform automatic, scheduled backups and retain them based on a backup policy. Consistently backing up your data allows you to adhere to your data compliance and regulatory requirements. If you need an immediate, point-in-time, direct disk-to-disk copy of your block volume, use the Block Volume cloning feature. Volume cloning is different from snapshots because there is no copy-on-write or dependency to the source volume. No backup is involved. The clone operation is immediate, and the cloned volume becomes available for use right after the clone operation is initiated. You can attach and use the cloned volume as a regular volume as soon as its state changes to available.

If you need to safeguard data against accidental or malicious modifications by an untested or untrusted application, use a block volume with a read-only attachment. A read-only attachment marks a volume as read-only, so the data in the volume is not mutable. You can also use read-only attachments when you have multiple Compute instances that access the same volume for read-only purposes.

For example, the instances might be running a web front end that serves static product catalog information to clients.

When your workload requires highly available shared storage with file semantics, and you need built-in encryption and snapshots for data protection, use File Storage. File Storage uses the industry-standard Network File System (NFS) file access protocol and can be accessed concurrently by thousands of Compute instances. File Storage can provide high performance and resilient data protection for your applications. The File Storage service runs locally within one availability domain. Within an availability domain, File Storage uses synchronous replication and high availability failover to keep your data safe and available.

If your application needs high availability across multiple availability domains, use GlusterFS on top of the Block Volume service. Plan and size your storage capacity by considering future growth needs.

Cloud Database High Availability Design

The Cloud Infrastructure Database service enable you launch a Database System (DB System) and create one or more databases on it. The Database service supports several types of DB Systems, ranging in size, price, and performance.

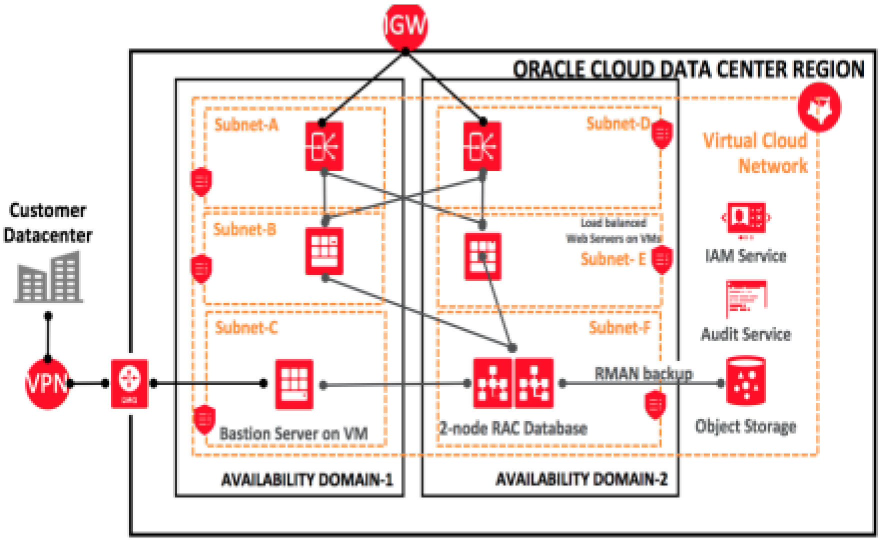
You can configure automatic backups, optimize for different workloads, and scale up the system to meet increased demands.

scale up the system to meet increased demands.

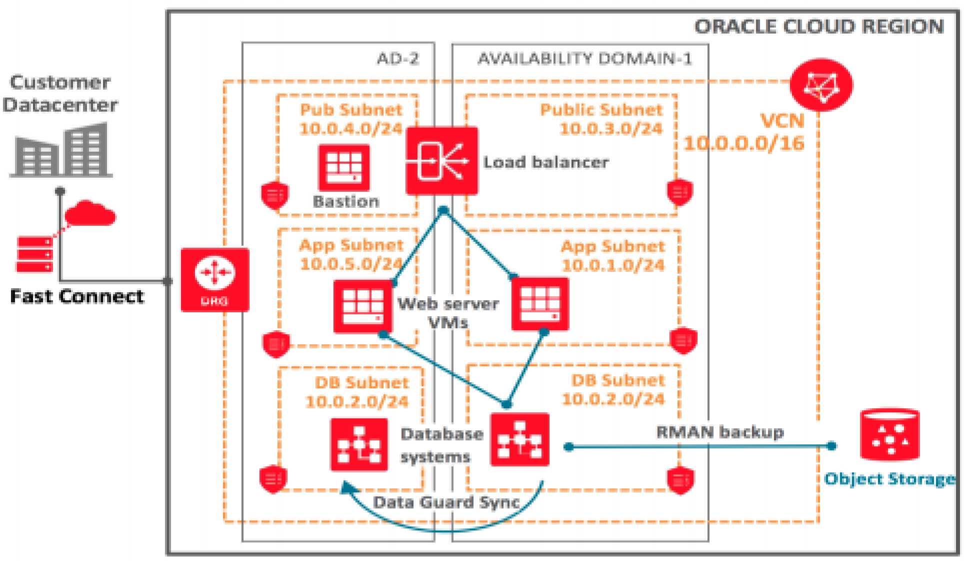
Using 2-node RAC DB Systems - This is exclusively offered by Oracle Cloud

Oracle Infrastructure offers 2-node RAC DB Systems on virtual machine Compute instances. 2-node RAC DB systems provide built-in high availability capabilities, it is recommended using 2-node RAC DB Systems for your solutions that require high availability.

You can configure the Database service to automatically backup to the Object Storage. The following diagram shows the deployment of a 2-node RAC DB System to support the high availability of a two-tier web application:



Working with Data Guard For solutions with a single-node DB system, we recommended using Oracle Data Guard to achieve high availability. Data Guard ensures high availability, data protection, and disaster recovery for enterprise data. Implementation of Data Guard service requires two databases, one in a primary role and one in a standby role. The two databases compose a Data Guard association. Most of your applications access the primary database. The standby database is a transactional consistent copy of the primary database. To improve availability and disaster recovery, it is recommended placing the DB System of the standby database in a different availability domain from the DB System of the primary database.



Data Guard maintains the standby database by transmitting and applying redo data from the primary database. If the primary database becomes unavailable, you can use Data Guard to switch the standby database to the primary role.

You can perform following actions with Data Guard configuration to support high availability:

Switchover:

Reverses the primary and standby database roles. Each database continues to participate in the Data Guard association in its new role. A switchover ensures no data loss. You can use a switchover before you perform planned maintenance on the primary database.

Failover:

Transitions the standby database into the primary role after the existing primary database fails or becomes unreachable. A failover might result in some data loss when you use Maximum Performance protection mode.

Reinstate:

Reinstates a database into the standby role in a Data Guard association. You can use the reinstate command to return a failed database to service after correcting the cause of the failure.

Automated CPU and Storage Scaling

To achieve high availability for your solutions, you must ensure that your DB

Systems have sufficient capacity. Database services on Cloud Infrastructure can dynamically scale CPU cores or database storage based on the different shapes of your Database service.

For DB Systems based on bare metal Compute instances, we recommend that you start with minimum CPU cores and dynamically increase the number of CPU cores as needed. For DB Systems based on virtual machine Compute instance, you can dynamically increase the storage size.

Conclusion

When planning any deployment, planning for availability is a key concern. This reference architecture provides guidance to help design high availability (HA) solutions on any Cloud Infrastructure Service, include the compute, network, storage, and database layers, and provides several best practices to help guide your planning:

1. Eliminate single points of failure with redundancy
2. Deploy your application or solution components across multiple availability domains
3. Design with future growth in mind and ensure that you have sufficient resource capacity
4. Leverage Database Data Guard and dynamic scaling capabilities
5. Replicate your application data across availability domains
6. Automate problem resolution and failover processes