OCI Architecture

- OCI Regions — 21 Available + 15 Planned; Commercial, Govt, Microsoft Azure Interconnect
- Region — Localized Geographical area comprised of 1 or more AD
- Availability Domains — One or more fault-tolerant, isolated DC located within a region, but connected to each other by low latency, high bandwidth network; Do not share physical infra
- Fault Domains — Grouping of hardware and infrastructure with in an AD to provide anti-affinity (logical data center); 3 FD per AD; Do not share SPOHF; change procedures are isolated at FD
- One AD Regions — within one year second AD or region will be made available
- Choosing Region — Location, Data Residency & Compliance, Service Availability
- Avoid SPOF — Design architecture to deploy instances that perform same tasks in different FD or different AD for multiple AD regions
- Data Guard — Data replication across AD
- HA Design — FD, AD, Region Pair

- Compartments — collection of related resources; helps to isolate and control access to resources; Tenancy/Root compartment; Compartment Network, Compartment Storage etc;

- Each resource belongs to a single compartment; Resource can interact with other resource in diff compartment; Resources and compartments can be added/deleted anytime;

- Resources can be moved from one to another; Resources from multiple regions can be in the same compartment; Compartments can be nested (6 levels deep); can give group of users access to compartments by writing policies; Analyse cost and assign budget for resources in compartments

OCI Compute Services

- Bare Metal — Code, App Container, Language Runtime, OS, Virtualization; No virtualization
- Dedicated Virtual Hosts — Code, App Container, Language Runtime, OS;
- Virtual Machines — Code, App Container, Language Runtime, OS; Guset on a host server with hypervisor-based virtualization;
- Container Engine — Code, App Container (Docker);
- Functions — Code; Consumption based pricing
- BM — Direct Hardware access; Single Tenant server; Use Case: Performance intensive workloads (DB), workloads not virtualized; workload that require specific Hypervisor, workload requires BYO licensing (SQL, Exchange etc)
- VM — Multi-tenant VMs; Use cases: to control all aspects of env, to deploy legacy app running on windows/linux, to move apps from on-premise to OCI
- Dedicated Virtual Host — Single-tenant VMs
- Instance Basics — various instance sizes(CPU, RAM, Bandwidth); Support both Intel and AMD processors; Provide GPU and HPC instance options(RDMA); instance placed on virtual network with powerful connectivity options; Depends

on other OCI services such as Block volume (Boot(OS)/Data) and VCN(Virtual Nic)

- Vertical Scaling — Scale up/Down; Downtime required;
- Autoscaling — Enable large scale deployment of VM from a single gold image with automatic configuration; Scale out/Scale in; If one VM fails, others will keep working; based on metrics; Running Instance -> Config (Gold Image — OS image, metadata, shape, VNICs, Storage, subnets) -> Instance Pool (put in diff ADs, Manage all together) -> Scaling Rule
- How to Deploy containers?
  1. Manually SSH into machines and run Docker
  2. Scripting or Config mgmt tools
  3. Orchestration Systems
- Oracle Kubernetes Engine — K8S; Containers in Pods, Pods in Node (Instances); OKE and OCIR
- Functions — small but powerful blocks of code that generally do one simple thing; stores as Docker image; invoked in response to a CLI command or signed HTTP request Push container to Registry -> Configure Function Trigger -> Code runs only when triggered -> Pay for code execution time only; based on FN project

OCI Storage Services

- Block Volume, Local NVMe, File Storage, Object Storage, Archive Storage
- Storage Requirements — Persistent vs Non-persistent, What type of data? (Database, videos, audio, photos, text), Performance (max capacity, IOPS, throughput), Durability (Copies of data), Connectivity (Local vs network, How does apps access the data), Protocol (Block vs File vs HTTPs)
- Block Storage — Hard drive in a server(on a remote chassis); stored on device in fixed sized blocks (512 bytes); Access by OS as mounted drive volume; Storage for compute services; 2 types (Boot Volume/OS Disk, Block Volume/Data Disks) Use cases — Databases, Exchange, VMWare, Server Boot. Block volume stores replica of data in 3 separate FDs; No need to configure s/w based protection(RAID-10 etc); Periodic backups
(automated schedule backups);
- Block volume backup — Complete point-in-time snapshot copy of block volumes; Encrypted and stored in Object Storage and can be restored as new volumes to any AD within same region; Can copy block volume backups from one-region to another(X-Region Backup); Backups can be scheduled
- Block Volume Tiers — (50 GB — 32 TB, up to 32 volumes/instance (32x32=1PB); Data encrypted at rest and in-

transit(oracle managed/customer managed key)
* Basic(2 IOPS/GB, 240 KB/s/GB Throughput); throughput intensive workloads with large sequential I/O such as big data & streaming, log processing and data warehouses.
* Balanced (60 IOPS/GB, 480 KB/s/GB); most workloads that perform random I/O such as boot disks
* High Performance (75 IOPS/GB, 600 KB/s/GB); workload require best possible performance including large DB’s

- Local NVMe — temp storage, locally attached to compute instance; app require high performance local storage; Use case — NoSQL DB, In-memory DB, Scale-out txn DB, Data warehousing. Storage non-persistent but survives reboot. OCI uses NVMe(Non-Volatile Memory Express) interface for very high performance. OCI provides no RAID, snapshots, backup capabilities

- File Storage — Hierarchical collection of docs organized into named directories which are themselves structured files. Distributed file systems make distributed look exactly like local file systems. Distributed file standards — NFS and SMB (provide access over networks). FSS — supports NFS v.3; Data protection: Snapshots(10000 per file system); Security (Data at rest, in-transit encryption). Use cases: Oracle Apps, HPC, Big Data and Analytics, General purpose file systems. FS — replicates data in 3 FDs; can take snapshot and restore snapshot

- Object Storage — All data, managed as objects; Each object stored in a bucket, relies on standard HTTP verbs; flat

structure; OSS — An internet-scale, high performance storage platform; ideal for unstructured data;
regional service; storage classes (hot/cold); Use cases: content repo for data, images, logs & video etc; Archive/Backup, Storing log data for analysis; Storing large datasets; Big Data/Hadoop storage
OS replicates in 3 FDs; stores replica of data in more than AD

- OS Tiers — Standard Storage Tier(Hot) Fast, immediate, and frequent access; Data retrieval in instances; Always serves the most recent copy of the data when retrieved; Standard buckets can't be downgraded to archive storage. Archive Storage Tier (Cold) Seldom or rarely accessed data but must be retained and preserved for long periods of time; 10x cheaper than standard tier ($0.0026 vs $0.0255 Gb/month); 90 days min retention period; objects needs to be restored before download; TTFB after restore request is made: 4 hours; Archive bucket can't be upgraded to Standard

OCI Network Services

- Virtual Cloud Network — software defined private network that you setup in OCI; Enable OCI resources to communicate
- VCN address space — Address space 10.0.0.0/16; Every resource will get its own unique private IP address; subnet — divide VCN into one or more sub networks;
- Gateways — IGW; Public Subnet(DMZ);
- NAT Gateway (Blocks inbound connection)
- DRG — virtual router that provides a path for private traffic between your VCN and destinations other than the internet; DRG to establish a connection with on-premises network via IPsec VPN, FastConnect(private, dedicated connectivity)
- Service Gateway — Communication to public OCI services — access without using internet
- Peering — process of connecting multiple VCN; Local VCN peering (same region); Remote VCN peering (Different Region) No transitive peering
  VCN Security — Firewall rules (Subnet layer); Network Security Group (VNIC layer)
- Load Balancer — sits between client and backends; performs tasks such as: Service Discovery, Health Check, Algorithm. LB Benefits — Fault tolerance and HA; Scale; Naming abstraction. LB Types — Public LB, LB pair for HA

OCI IAM

- IAM — Identities, Permissions
- Principals — IAM entity that is allowed to interact with OCI resources; IAM users and Instance Principals
- IAM Users and Groups — 1st IAM user is default admin; Users -> Groups -> at least one policy
- Instance Principals — let instances make API calls against other OCI services
- Network Admin, Storage Admin etc — Policies
- Authentication — deals with user identity; Username/Password, API Signing key, Auth Tokens
- Authorization — actions performed by principals; Policies; Allow group <> to <> resource-type in tenancy/compartment where conditions <>
  Policies — Allow <subject> to <verb> <resource-type> in <location> where <conditions>
  Verb — inspect(list resources), read(inspect_user-specified metadata), use (Read+Update), manage(all permissions)
  Resource type — all-resources, database-family, instance-family, object-family etc
- Common Policies — Network admin(manage virtual-network-family), Instance Launchers(manage instance-family, use volume-family, use virtual-network-family)

OCI Database Services

- OCI DB Options — VM (Fast Provisioning), Bare metal(Fast performance), RAC (Managed HA), Exadata DB systems(Managed Exadata Infra), Autonomous — Shared/Dedicated(Self-driving, Self-Securing, Self-Repairing)
- DB Systems — Managed DB systems, Complete Lifecycle automation (Provisioning, Patching, Backup & Restore), HA and DR (RAC & Data Guard), Scalability (Dynamic CPU and Storage Scaling), Security (Infra(IAM, VCN, Audit), Database(TDE, Encrypted RMAN backup/Block volume encryption)), BYOL
- DB Systems Operations — Launch, start, stop or reboot DB systems(Billing continues in stop state for BM DB systems), Scale (CPU cores (BM DB), Storage(VM DB)), Patching (2 step process, For Exadata and RAC patches are rolling)
- DB Systems Backup — Manual/Automatic Backups, Auto backups written to Oracle owned Object storage buckets, Runs between midnight — 6 AM in DB system time zone, Preset retention periods: 7, 15, 30, 45 and 60 Days; Recover DB from backup stored in Object storage(Last known good state, Timestamp specified, Using SCN)
- DB Systems HA and DR — Oracle Data Guard — survive disasters and data corruptions (maintain sync between primary and standby DB); Active Data Guard (adv features for data protection and availability, included in Extreme

Performance edition and Exadata service); 2 modes — switchover(planned migration, no data loss), Failover (unplanned, min data loss)

- MAA — Primary and standby DB can be either a single-instance oracle db or RAC DB
- Autonomous Databases — Fully managed DB with 2 workload types; TP, DWH; Deployment options — Dedicated/Shared; Automates backing up DB, patching w/o downtime, Upgrade DB, Tune DB

OCI Security

- Shared Security Model — OCI upto virtualization; Customer (Patching app and OS, OS config, IAM, Network security, Endpoint protection, Data Classification and Compliance)
- Security Services — OCI IAM, MFA, Federation, Storage and DB services, Data Safe, Key Management, OS Management Service, Bare Metal, Dedicated VM hosts, VCN, NSG, SL, WAF
- IAM — RBAC; Authentication -> OCI IAM -> Authorization -> Compartments -> Resources; MFA; SSO using IDP
- Data Protection — Block volume (Data enc at-rest/in-transit, BYOK) File Storage (Data enc at-rest/in-transit, BYOK) Object Storage (Data enc at-rest, BYOK, Private Buckets, Pre authenticated requests) Database(TDE, Data safe, Data Vault) Key Management (BYOK, use HSM)
- OS & Workload isolation — OS Mgmt service configured by default for Oracle Linux; Network protection — Tiered subnet strategy for VCN, Gateways, Security Lists, NSG, OCI WAF (XSS, SQL Injection), Protection against layer 7

OCI Pricing and Billing

- Pricing Models — Pay as you go; Monthly Flex (Universal Credits) $1000 monthly charge/12 months -> 33% — 60% savings vs PAYG; BYOL (apply on-premise Oracle license); All OCI region have same pricing;
- Block volume (Storage cost $0.0255 per GB/month, Performance Cost (VPU/GB) — NA for Basic, 10 VPU at $0.0017 for balanced, 20 VPU at $0.0034 for higher performance); Data Transfer costs — Ingress/Egress free b/w data transfers, Egress charge for different regions; To and from internet (Egress charged), DRG/FastConnect both Ingress/Egress free
- Pricing Example — Outbound Data Transfer 10 TB free
- Billing — Cost Tracking Tags, Cost Analysis, Budgets, Alert every 15 mins, Usage reports (automatically generated CSV file, 24 hrs data, retained for 1 year)
- Free Tier — $300 free credit for 30 days; upto 8 instances, 5TB storage
- Always Free — 2 Oracle Autonomous DB, 2 OCI Compute VMS, Block, Object and Archive Storage, LB and Data egress, Monitoring and Notifications–