

OCI



By:Mostafa Mahmoud Bahgat

LinkedIn:<https://www.linkedin.com/in/mostafamahmoudbahgat>

OCI

IAM-1



What is OCI IAM?

Identity	Access Management
● Authentication	● Authorization
● Centralized identity lifecycle management	● Fine-grained access controls
● Integration with existing identities and applications	● Define granular permission
● Secure and easy access	

ال identity هي ال Authentication وهي اني بقول مين مصرح ليه بالدخول
ال Access Management وهي ال Authorization ودي الي هيدخل أي الصلاحية بتاعته (يقدر أي access)

ال Account يسمى principal وأول user هو ال administrator بتاع ال

ال User Group تكون علي ال Permission مش ال

ال App instance هو اني بعطي instance principal او vm سواء instance permission

عشان يقدر يعمل لـ Services Access لـ ال محتاجها

عندی 3 وسائل عشان اقدر اعمل login وهي

username and password-1

API Key-2

Auth Tokens-3

وال API وال Auth بيكونوا داخل ال profile بتاعك

Resources

My groups

Integrated applications

API keys

Auth tokens

ah) ✓

Profile

Default/mostafa.mahmoud@nt-me.com

Identity domain: Default

My profile

Tenancy speedlaboci

ال Policies : في عندي Policies

فقط Monitoring لـ Permission : inspect -1

List لـ Resources : بيعمل read -2

Use : اقدر اعدل Resources موجودة قبل كدا

Manage : دي Full Access -4

Policy Syntax

Allow <subject> to <verb> <resource-type> in <location> where <conditions>

Verb	Type of access	Aggregate resource-type	Individual resource type
inspect	Ability to list resources	all-resources	
read	Includes inspect + ability to get user-specified metadata/actual resource	database-family	db-systems, db-nodes, db-homes, databases
use	Includes read + ability to work with existing resources (the actions vary by resource type)*	instance-family	instances, instance-images, volume-attachments, console-histories
manage	Includes all permissions for the resource	object-family	buckets, objects
* In general, this verb does not include the ability to create or delete that type of resource		virtual-network-family	vcn, subnet, route-tables, security-lists, dhcp-options, and many more resources (link)
		volume-family	volumes, volume-attachments, volume-backups
		Cluster-family	clusters, cluster-node-pool, cluster-work-requests
		File-family	file-systems, mount-targets, export-sets
		dns	dns-zones, dns-records, dns-traffic,..

The IAM Service has no family resource-type, only individual ones

ال Policies بتكتب بالطريقه دي

Allow group 'Prod'/'NetworkAdmin' to manage virtual-network-family in compartment Sandbox

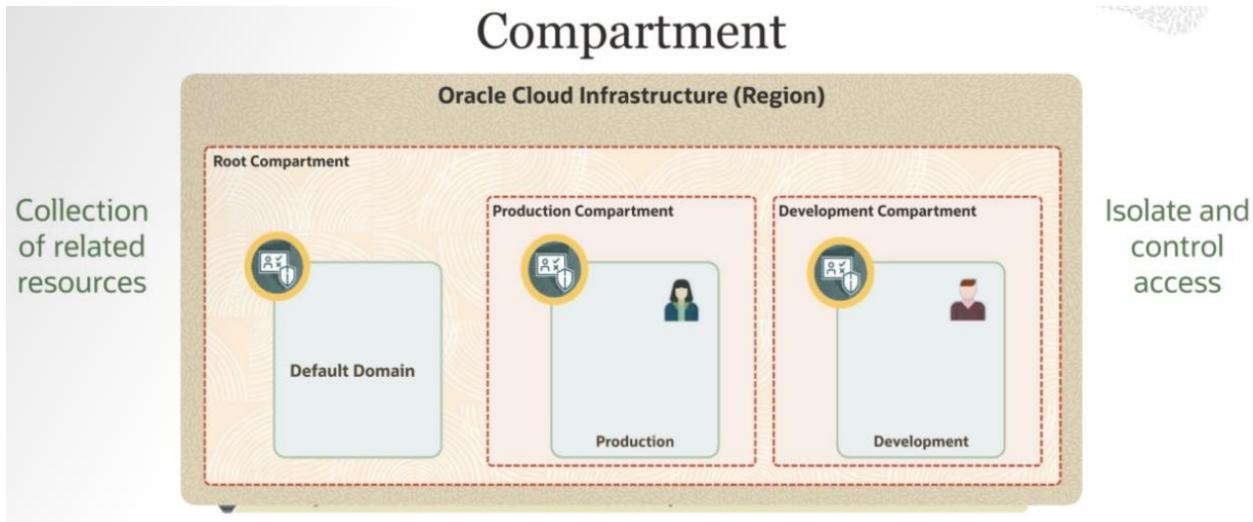
بقوله ال Group ال اسمه Networkadmin ال في ال domain ال اسمه prod هيقدر يعمل Compartement ال VNF Manage مكان ال compartment sandbox

وقدر اعمل policies وانا بكتب ال Conditions وبتكون بناءا علي :

Request -1 : region معينه هي و

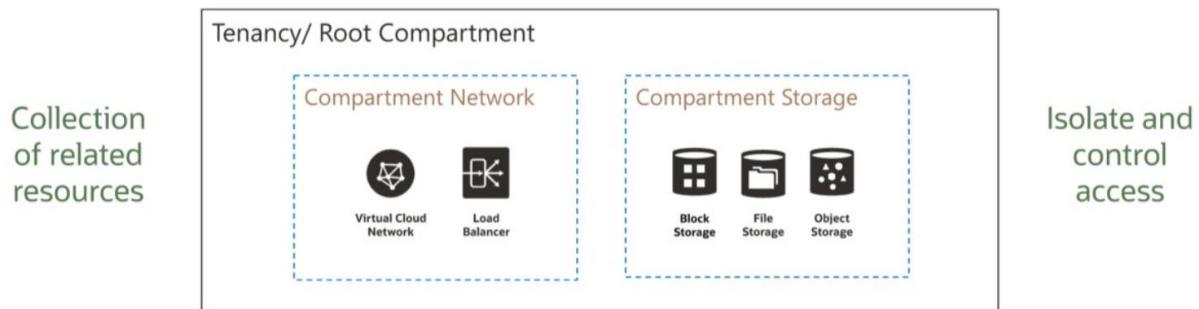
target -2 : معين resource هي

: Compartments



جمع فيها ال Resources المتشابهة مثلا مع بعض ول يكن
وهكذا Storage لـ Compartment و Network Compartment
ودا بيغبني في اني بعزل كل Resource عن بعض وبيسهل عليا اني اوصله

Compartments



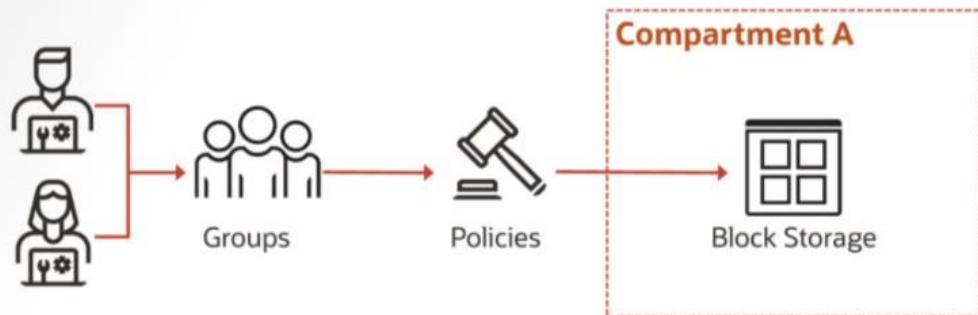
Root Compartments can hold all the cloud resources

Best practice: Create dedicated compartments to isolate resources.

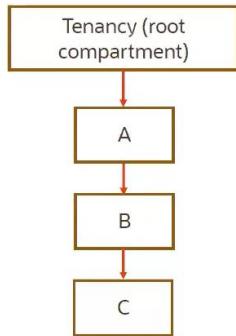
- وممكن اعمل Compartment واحد واحظ فيه كل ال Resources ال عندي
لكن الأفضل هي اني اعمل Compartment مختلفه

- بيسهل عملية ال Access وال Policies

Compartments Access



Users + Policies = Access to Compartments



- اقدر اعمل Compartment تحت ال Root او Sub Compartment وقدر اعمل لحد 6 sub Compartment (يعني مثلا هعمل comp تحت ال root اسمه prod وتحت prod هعمل Compartment prod1 وهكذا لحد 6sub compart) وال compartment policies من ال parent بتاعه لو اديت full access لـ root compart فـ full access ه يكون معه برضو على كل ال compartments تحت ال root لأن ال تحت ال root بيتعلمle inherit من ال root وهذا

لكن لو عاوز افصل فـ hadd أقول ال group ال اسمه test مثلا يعرف ال network access بتاع ال compartment A فقط وهكذا

ال Compartment Resource بيتتحط في واحد فقط
لكن اقدر استخدم ال Compartment من Resource مختلفه بمعنى مثلا عملت
في Compartment2 VM في Compartment1 وعملت VNET اخلي Compartment2 تكون تبع ال
Compartment2 الي في vnet

Resources can interact with other resources
in different compartments.

Interaction of Resources

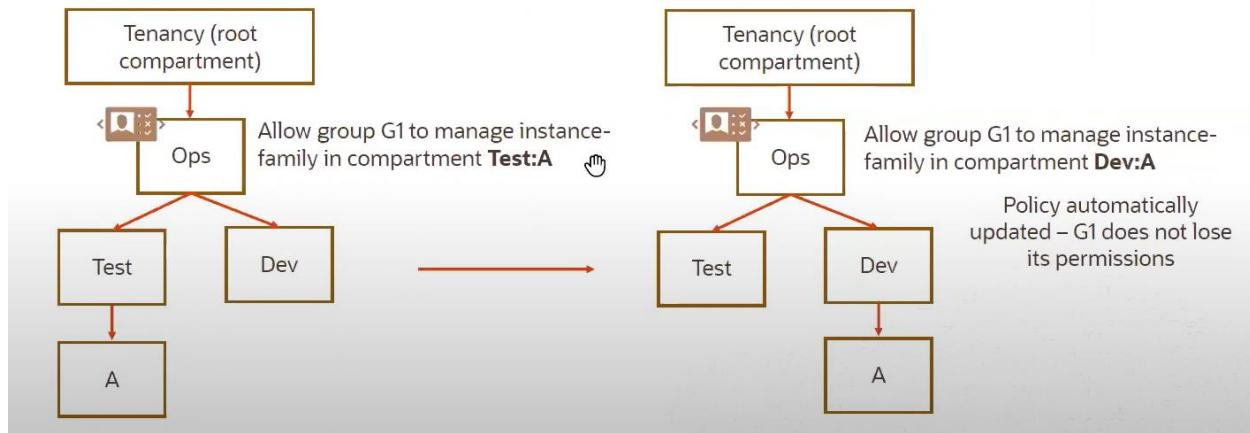


(دا الاکونت بتاعك) Tenancy

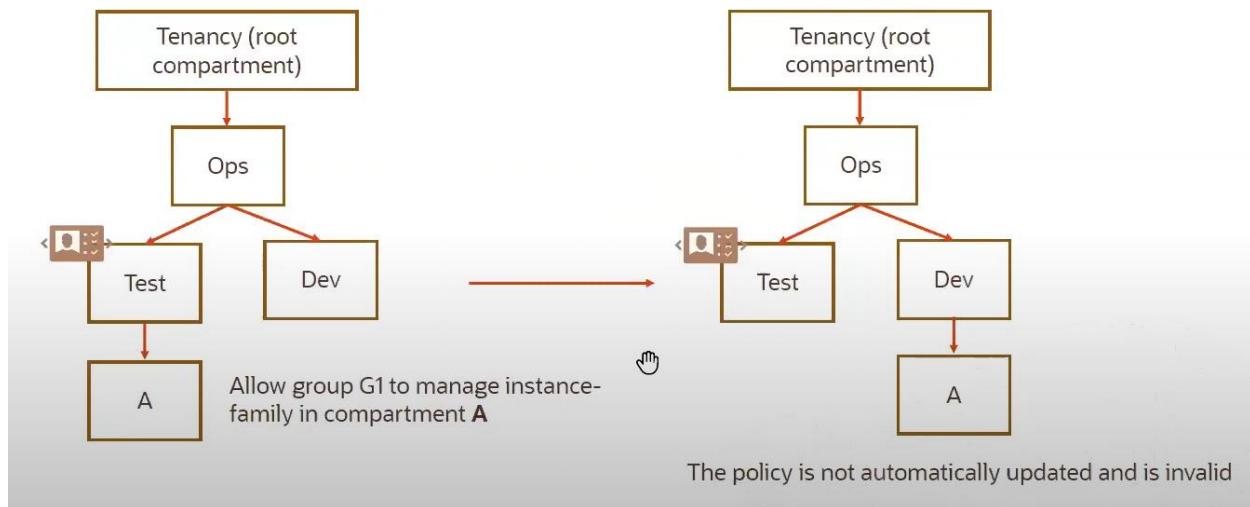
(دا اوں Root Compartment (tenancy) compart auto ویتمل بشکل ویکون ب اسک الاکونت او

يعني ال tenancy الاکونت اسمه test فال root compartment هیکون اسمه

-اقدر اعمل Move لـ Compartment من Resource Compartment لـ Compartment
 -الـ policies بياخد الـ Sub Compartment بتاعته من الـ Parent



لو نقلت ال A من Test ل Dev وكتبت كاتب ال policies بالـ parent بتاعها اول م انقلها ال policies هتتعدل تلقائياً لوحدها لأن الـ Parent policies واحد للاثنين



لكن لو مش كاتب ال policies ونقلتها فال policies مش هتتعدل انت بایدك ال لازم تعدها

Resources : من خاللها بعمل Metadata لـ Resources وبالطريقة دي بقدر انظم ال Tags-ال عندي مثلاً بعمل tag معين لاي Resources خاصه بال Storage او Network وهذا يكون ال tag من Key و Value يمكن ان يكونا أي قيمة تريدها.

- فيه نوعين في ال Tags :

: Free-Form Tags-1

هي أكثر بساطة و مرونة .

يمكن استخدامها بدون قيود أو تعاريف مسبقة .

تحتوي على مفتاح (Key) وفي قيمة (Value) ويمكن أن تكون أي نص تريده .

مثال :

Key: Environment

Value: Production

Defined Tags -2 : دي بقا اعقد شويا لأن أنا ال بعملها ب ايدي واخلي ال user يستخدمها ال بيحصل ان بعمل NS و داخل ال NS دا بعمل ال Tags ال أنا عاوزها ول يكن مثلاً ال Key عندي لو يساوي الكلمة Status يكون ال Value بناعطي قيمة من التلاتة دول value فلو أي user دخل key Environment هيلافي تلاقي التلاتة ال ظهرروا ويختار منهم واحد

The screenshot displays two main components of the Oracle Cloud Infrastructure Tag Management interface:

- Left Panel (Tag Key Definition View):**
 - Header: TAG KEY STATUS
 - Table: Shows a single row for "Status" with three values: Prod, Test, and Dev.
 - Buttons: "Create VCN" and "Cancel".
- Right Panel (Tag Key Definition Details):**
 - Header: Governance > Tag Namespaces > Tag Namespace Details > Tag Key Definitions > Tag Key Definition
 - Status:** ACTIVE
 - TKD Logo:** A large green circular logo with the letters "TKD" in white.
 - Buttons:** "Edit Tag Key Definition" (blue), "Retire Tag Key Definition" (red).
 - Information:**
 - Tag Definition Information: Placeholder for information.
 - Description: Resource Status
 - Namespace: TAGNS
 - OCID: ...sbz62a (with "Show" and "Copy" links)
 - Cost Tracking: No
 - Tag Value Type: List
 - Tag Values: Prod, Test, Dev

الفرق بين Free-form Tags و Defined Tags

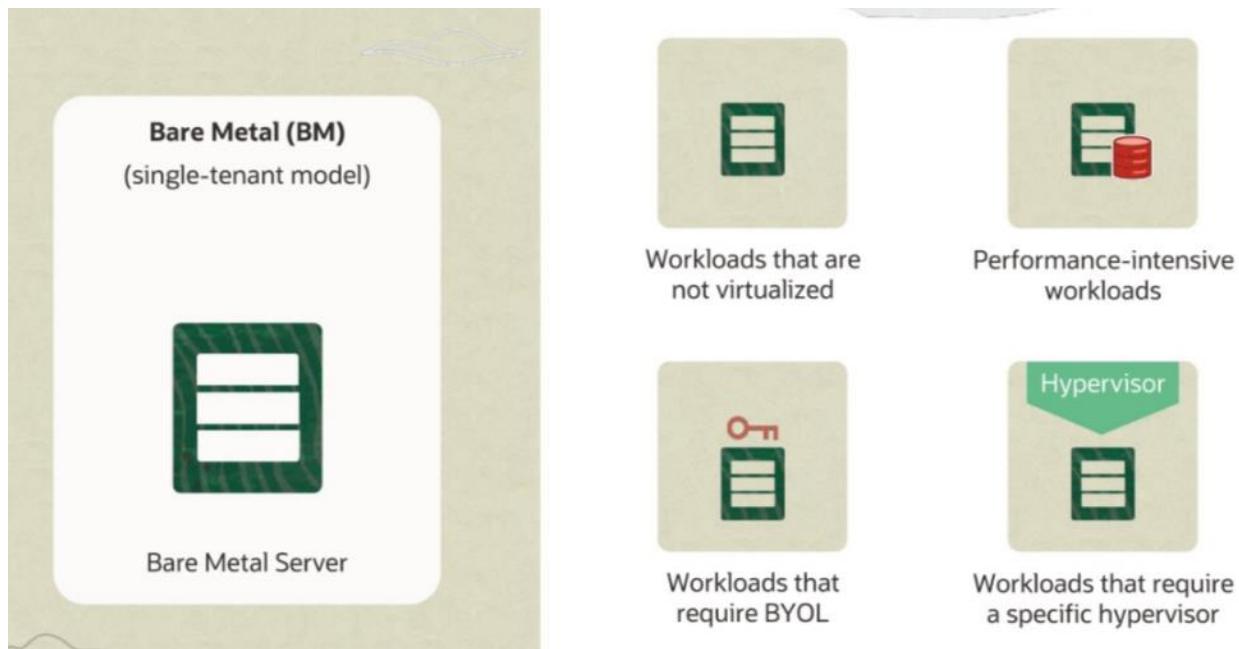
Free-form Tags:

- مرنّة وسهلة الاستخدام.
- لا تحتاج إلى إعداد مسبق.
- قد تؤدي إلى عدم اتساق إذا لم تُستخدم بطريقة موحدة.

Defined Tags:

- تحتاج إلى إعداد مسبق.
 - تضمن اتساق تسمية الموارد عبر المؤسسة.
 - تُستخدم لفرض سياسات محددة على الموارد.
 - تُساعد في التقارير والتحليلات المنظمة.
-

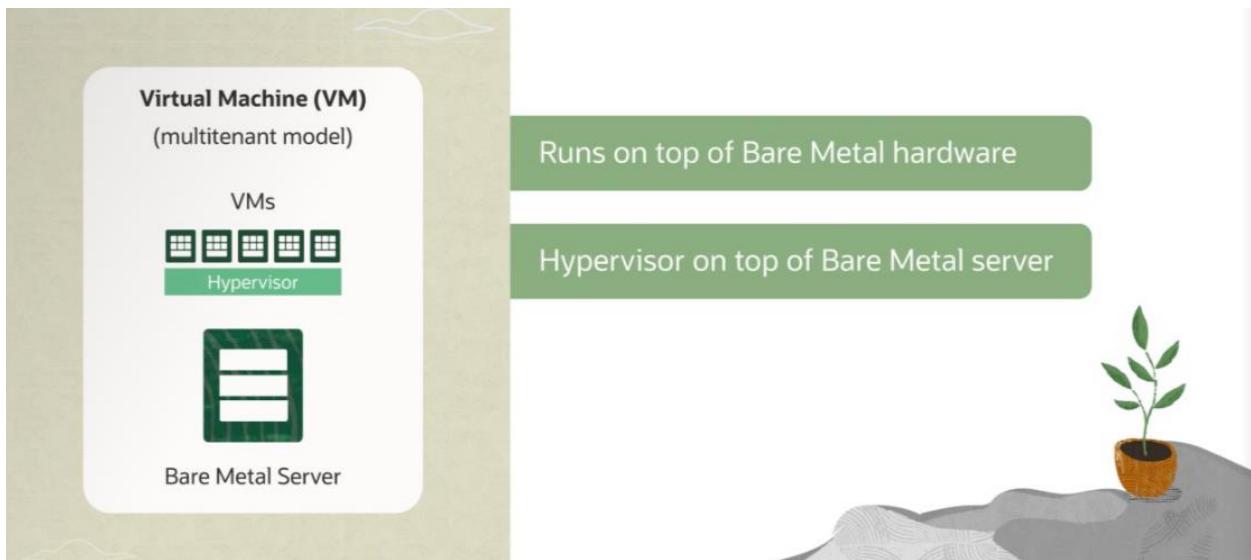
Compute -2



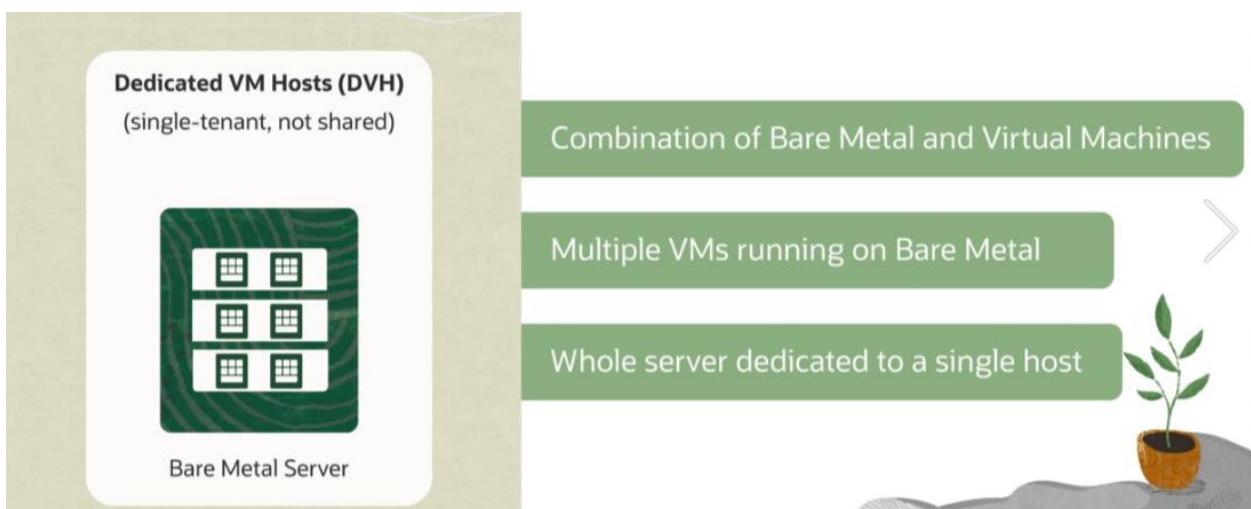
1- ال Bare Metal ودا بيكون عباره عن Oracle Server Hardware بدهولك وانت تبدا تعمل

عليه ال انت عاوزه . وهو عباره عن Single-Tenant Model بمعنى ان محدش بيشارك في

الهاردوير او السيرفر دا انت بس ال بتمتلكه ويتقسمه زي ما انت عاوز



2- ال VM هنا بتاخد VM مش Server لا بتاخد VM معينه جاهزه انت بتختارها سواء بيكون Multi-tenant Model . يعني ان في حد بيشاركك في الهايدور . يعني لو هو Server عليه 10VM وانت واحد VM واحد فيه 9 اشخاص كمان مشركون في ال لكن هنا محدش بيقدر يشوف غير ال VM بتاعته والداتا بتاعته فقط



3- ال DVH وهنا انا باخد ال Server لوحدي كهاردوير مفيش حد مشاركتي فيه زي بالظبط ال لكن بيكون جاهز بال Hypervisor ال محتاجه . وبيكون Single Bare Metal محدش بيشاركتي فيه

Images

في ال Linux

ال User في ال CentOS و Oracle Linux بيكون اسمه opc

في ال Ubuntu بيكون اسمه ubuntu

في ال Windows

بيكون اسمه opc

وال user دا بيكون معه صلاحيات ال Root

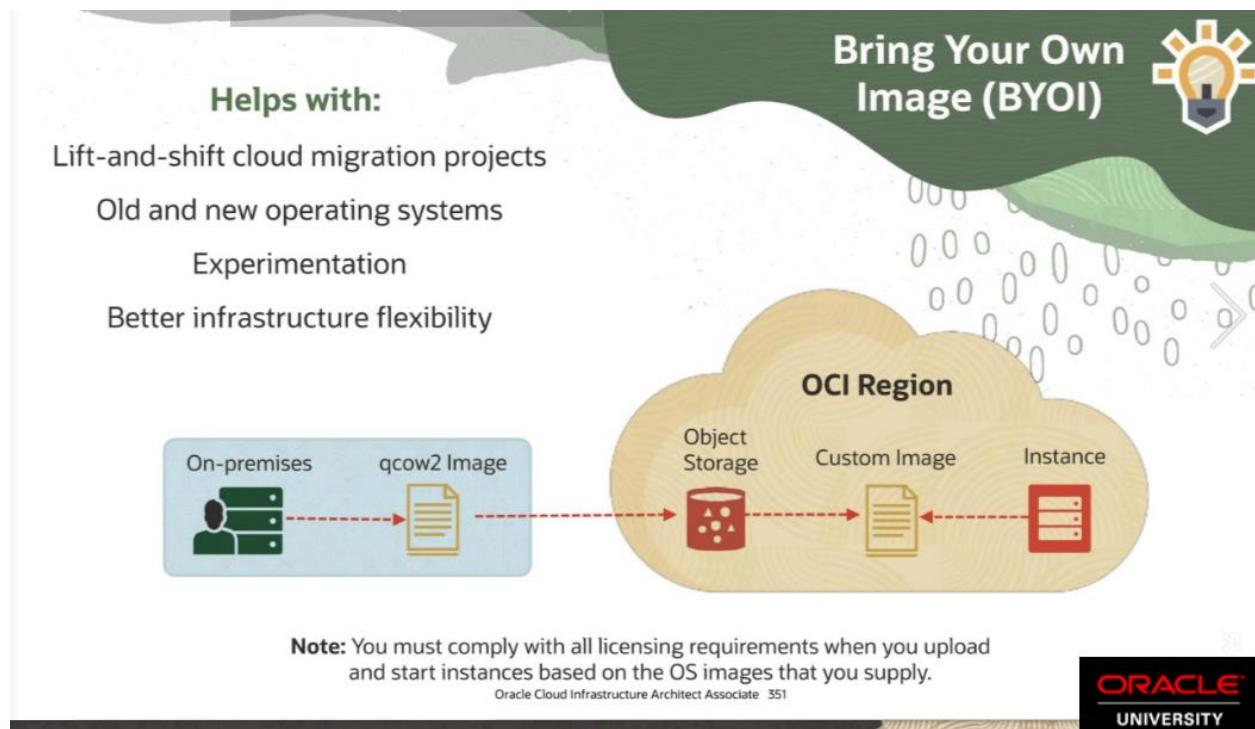
-قدر اعمل Custom Image من Image موجوده عندي وال Custom Image بتاخذ فقط ال Boot Disk

ويكون مساحته مش اكثـر من 300G – لو عندي Block Volume مش هياخدـها

وال Custom Image بتسمـي أيضا بال Bring Your Own Image (BYOI)

ـ هنا بقدر مثـلا اعمل Import/Export Image- export or import في Region مختلفـه او tenancy .

قدر لو عامل VM عندي في ال On-prem اقدر اعملـها Import في OCI



-في عندي Import/Export 3 لـ Mode

1- Emulation : يتم تنفيذ أجهزة الإدخال/الإخراج للأجهزة الافتراضية (القرص والشبكة) ووحدة المعالجة المركزية والذاكرة في برنامج تمت محاكاته بواسطة VM يعني أصلاً مش بـ support الـ Hardware (بitem محاكاة الـ vm الفعلي يعني الـ Virtualization تكون مش عارفه أنها شغاله في بيئه (Virtualization) والأداء هنا بيكون بطئ جداً)

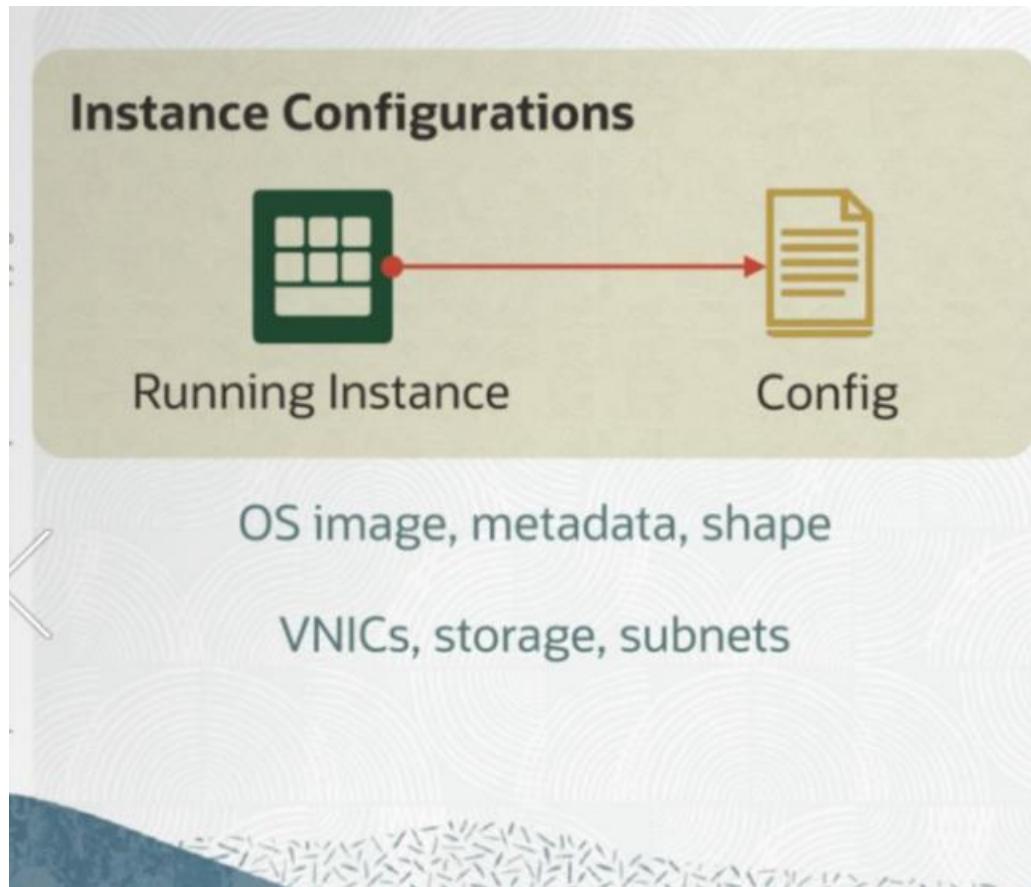
2- Paravirtualization : يتضمن برنامج تشغيل مصمم خصيصاً لتمكين المحاكاة الافتراضية يعني بـ (Virtualization) الـ vm بيكون عارف انه شغال (Virtualization) الـ support وأداء هنا بيكون افضل بكثير

3- Native : هنا os and App بتشغل عطول على الـ hardware بتاع server وبالتالي هي شيفه انها شغاله ع Hardware فعلي بيكون الأداء افضل واسرع من الاتنين السابقين

Boot Volume - Custom Image : دا ال بعمل منه الـ Custom Image يعني ممكن احذف الـ VM واسيب الـ Images واقدر بعد كدا اعمل منه Boot Volume ويكون encrypted واقدر اعمله Resize

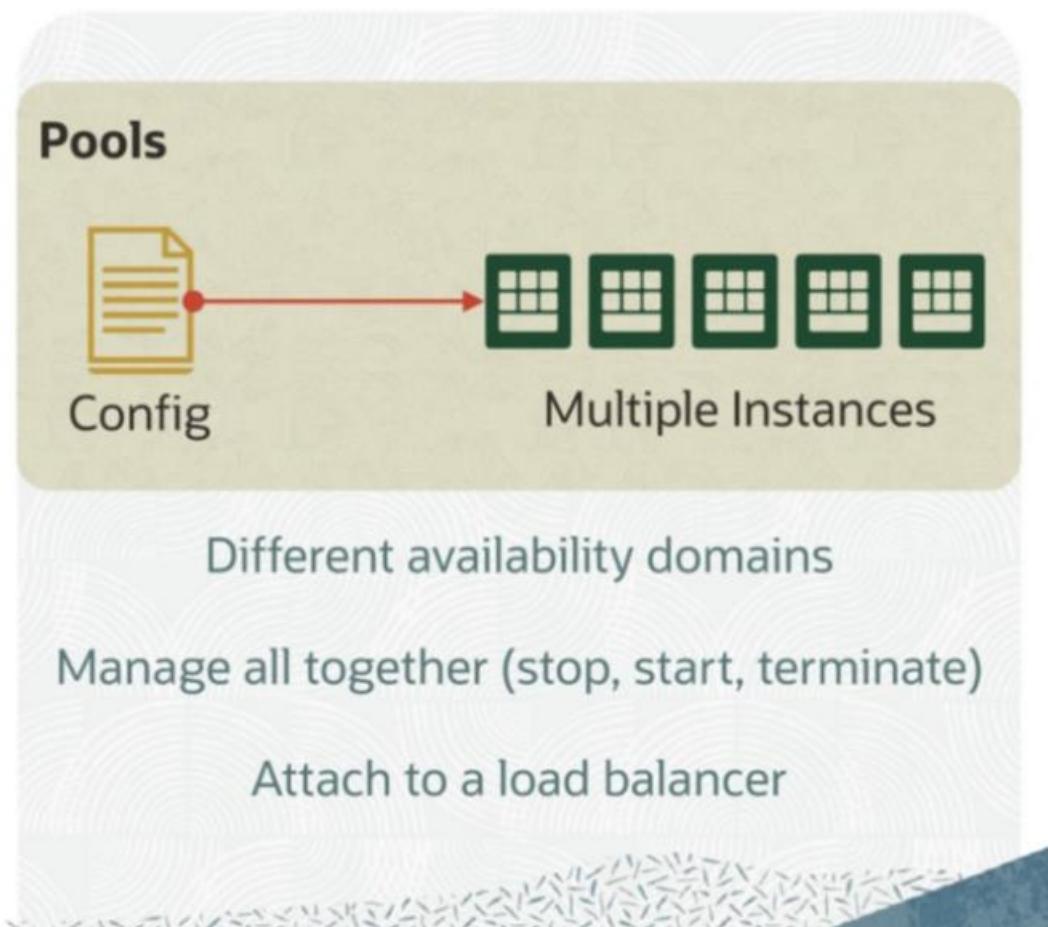
Custom Image	Boot Volume Backup
بيكون فيه Downtime وإيقاف حتى انهاء العملية وبتعمل من خلالها Import/export لـ tenancies مختلفه و Region . -- لا يوجد تكلفة ، لكن الحد الأقصى بيكون Compartment 25 لـ Image	لا يطلب إيقاف الـ image وبالتالي مفيش Downtime لكن هناك تكلفة عالية بسبب استخدام الـ Object Storage للاحتفاظ بالـ Backup -- يحتفظ بالـ OS بالحالة الـ هو عليها حالياً Backup لكن بسبب انه بيأخذه وهي شغاله Crash Consistent بيحصلها

: Instance Configuration -



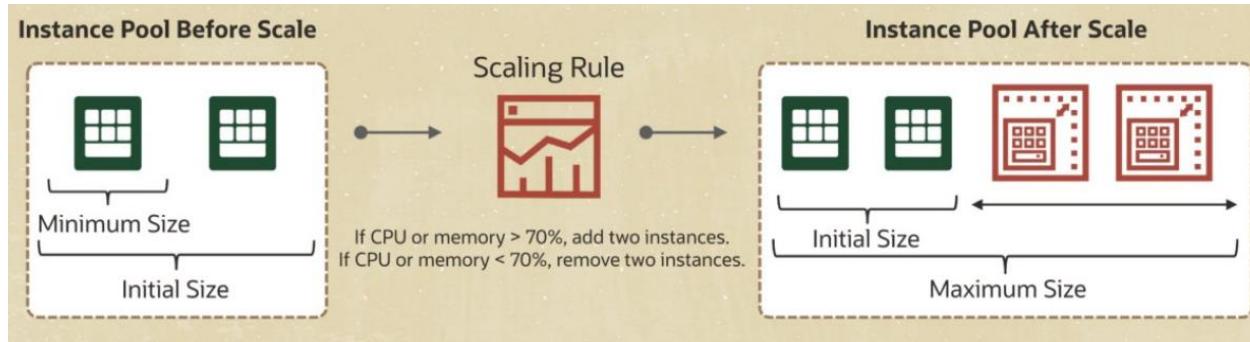
بادخ Configuration من ال config وال Running Instance بيكون عباره عن ال
OS-Metadata-shape-VNICs-Storage-Subnets
وال Config دي من خاللها بقدر اعمل Pooling

: Instance Pool -



الفکره عن لو عندي Workload معرفش الأداء هيكون عامل ازاي
فبعمل pool بقوله ان مثلا ال maximum instance يكون 10vm وانك تبدا تشغيل 2 بس
وتعمل شرط معين انه يزود او يحذف instance امتي
Autoscaling ودا يسمى بال

: Autoscaling -



ال AS بعمله من ال Pool ال عملتها Create ومنها بقدر ازود او اقل عدد ال instance بشكل بناء علي حاجه من اتنين ي اما ال CPU او ال RAM مثلا
أقوله لو ال CPU زاد عن ال 75% زود Instance لو قل عن ال 35% احذف

يبقي عشان اقدر اعمل ال Autoscaling بمر ب 4 مراحل :

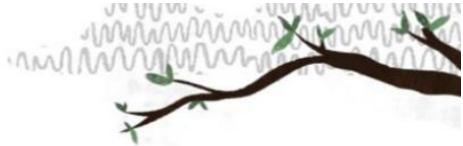


-1 بعمل Config Create لـ
-2 بعمل Pooling Create لـ
-3 بعمل pool Config لـ
Autoscaling Create -4

:Networking -3

CIDR(Classless inter domain routing) -1
 طريقة تحديد نطاقات عناوين IP في ال
 ال عندي ول يكن 192.168.1.0/24 فالنطاق بتاعي هي تكون من 256ip الي هو من
 192.168.1.255 الي 192.168.1.0
 (من الاخر هو رنج ال ips ال ه تكون عندي)

CIDR: Example

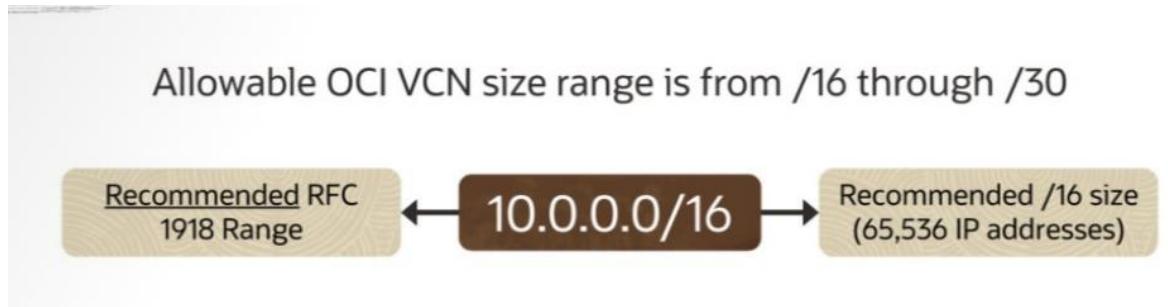


192.168.1.0/24 would equate to IP range 192.168.1.0 – 192.168.1.255

- › 128 64 32 16 8 4 2 1 -> $2^7 \ 2^6 \ 2^5 \ 2^4 \ 2^3 \ 2^2 \ 2^1 \ 2^0$
- › 192 is represented as 1 1 0 0 0 0 0 0

192.168.1.2	1 1 0 0 0 0 0 0	1 0 1 0 1 0 0 0	0 0 0 0 0 0 0 1	0 0 0 0 0 0 1 0
/24 subnet mask	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	0 0 0 0 0 0 0 0
Logical AND	1 1 0 0 0 0 0 0	1 0 1 0 1 0 0 0	0 0 0 0 0 0 0 1	0 0 0 0 0 0 0 0

الى هيكون فيها ال Virtual network : بحد من خلالها ال VCN(virtual cloud network) -2 instance or storage Resources بتاعتي زي مثلا ال بنحدد ال CIDR Block واحنا بنعمل vcn ومش هينفع تغييرها بعد كدا ال vcn بتكون في واحد region وال 10.0.0.0/16 هو Recommended



ال vcn بيحتفظ بعض ال ip وهي اول ip وهو 192.168.1.0 بيستخدم كعنوان لل network الثاني ip 192.168.1.1 بيستخدم ك Gateway قبل الاخير 192.168.1.254 ويستخدم ك router لل last host الأخير 192.168.1.255 يستخدم ك broadcast address

Examples:

Network ID:

192.168.1.0

First Host:

192.168.1.1

Last Host:

192.168.1.254

Broadcast Address:

192.168.1.255

ال subnet : ممکن اور ز عها علی اکتر من Availability Domain و ممکن اخليها فی Region کامله

و فيين نوعين من ال Subnet

- ال Private : للشبکة الداخلية فقط

- ال Public : عشان تقدر توصلها من خارج ال cloud

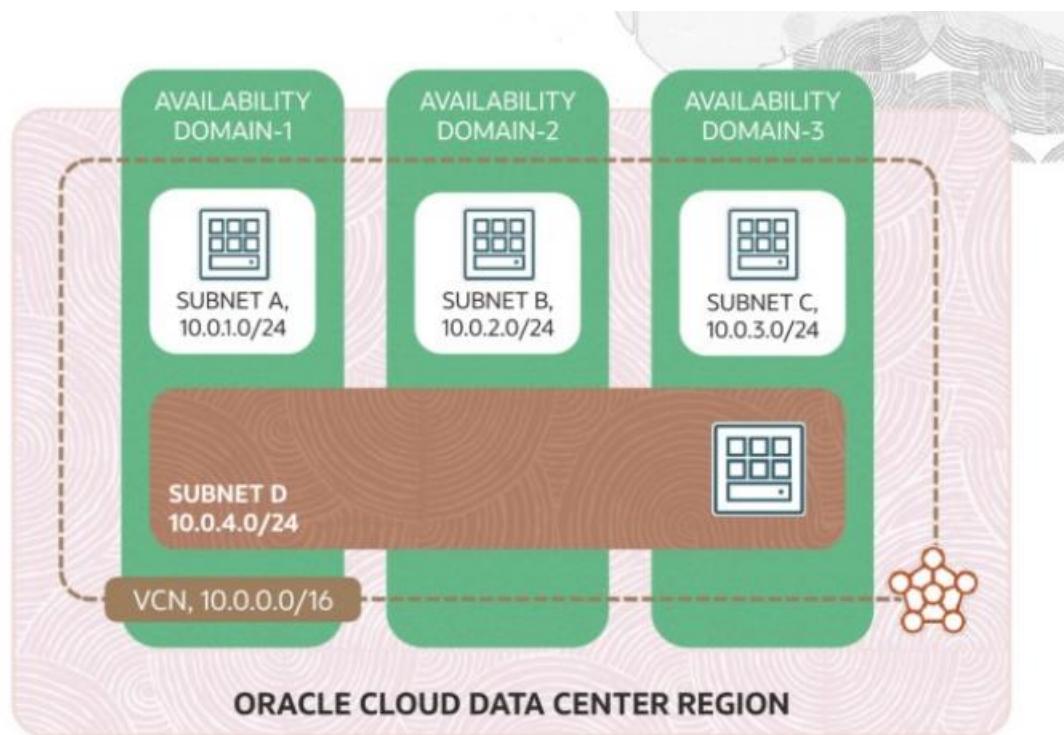
فيه نوعين من ال Public

هو عباره عن temporary IP يعني موجود طول م ال vm موجوده لو اتحذفت هو

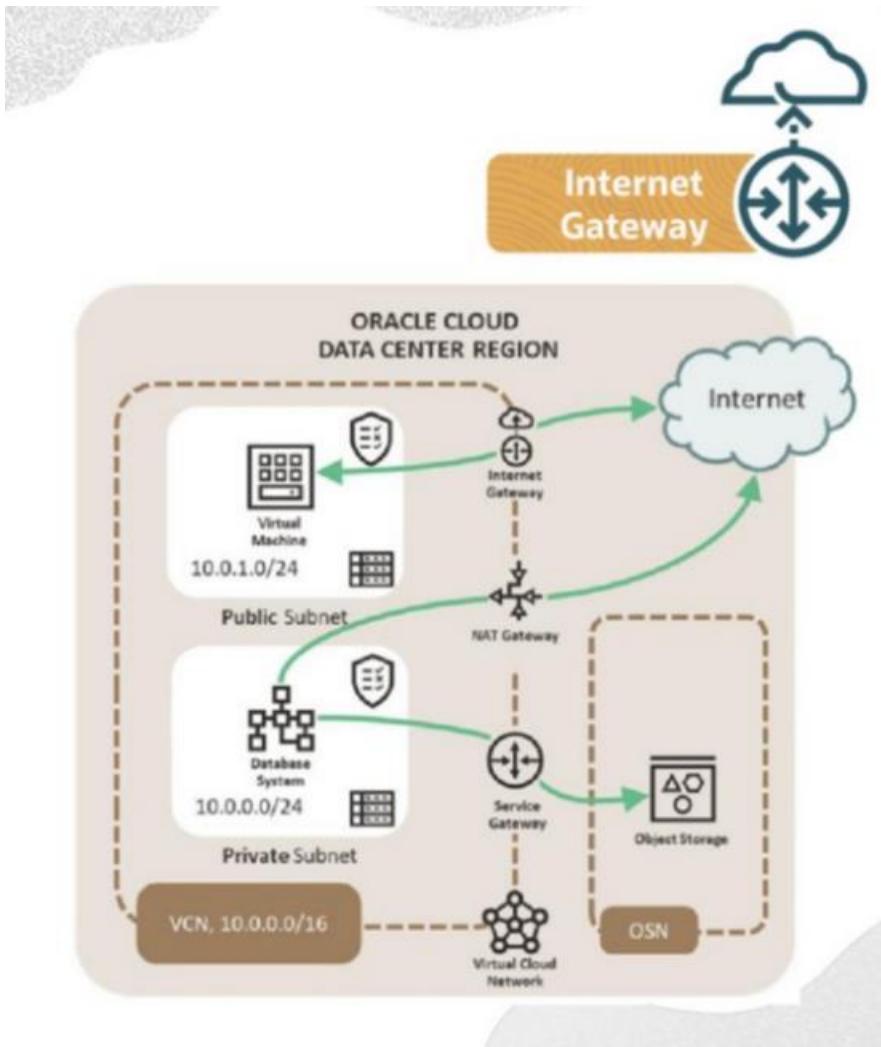
هيتحذف برضو

دا بيكون معاك عطول سواء ال vm اتحذفت او لا

علي ال الواحده اقدر اعمل اکثر من VNIC



ال Internet Gateway : يسمح لل private network انها توصل للانترنت او ان اي حد من الانترنت يصلها



ال Route Tables : من خلاله بعمل توجيه traffic داخل ال network وخارجها
: Route table
- بعمل الأول internet Gateway ول يكن هسميتها GW

Subnets (3)
CIDR Blocks/Prefixes (1)
Route Tables (1)
Internet Gateways (1)
Dynamic Routing Gateways Attachments (0)

Create Internet Gateway		
Name	State	Route Table
GW	Available	-

-بعد كدا هعمل ال RT وبختار ال compartment name وبعد كدا اضيف ال Rule

Create Route Table

Rule

Target Type
Internet Gateway

Destination CIDR Block
0.0.0.0/0
Example: 10.0.0.0/24

Target Internet Gateway in. [\(Change compartment\)](#)
GW

Description *Optional*

Create [Cancel](#)

بقوله لو عاوز توصل لاي ip هتستخدم ال اسمها GW

بعد كدا بجي علي ال VCN بتاعتي واعمل Assign لـ GW علي ال Subnet

Networking > Virtual cloud networks > [Subnet Details] Edit Subnet

DB-SN-Pul [Edit] Move resources

AVAILABLE

Subnet Information

OCID: ...sedbya S IPv4 CIDR Block:

IPv6 Prefix: - Virtual Router MA

Subnet Type: Reg

IPv4 CIDR Block

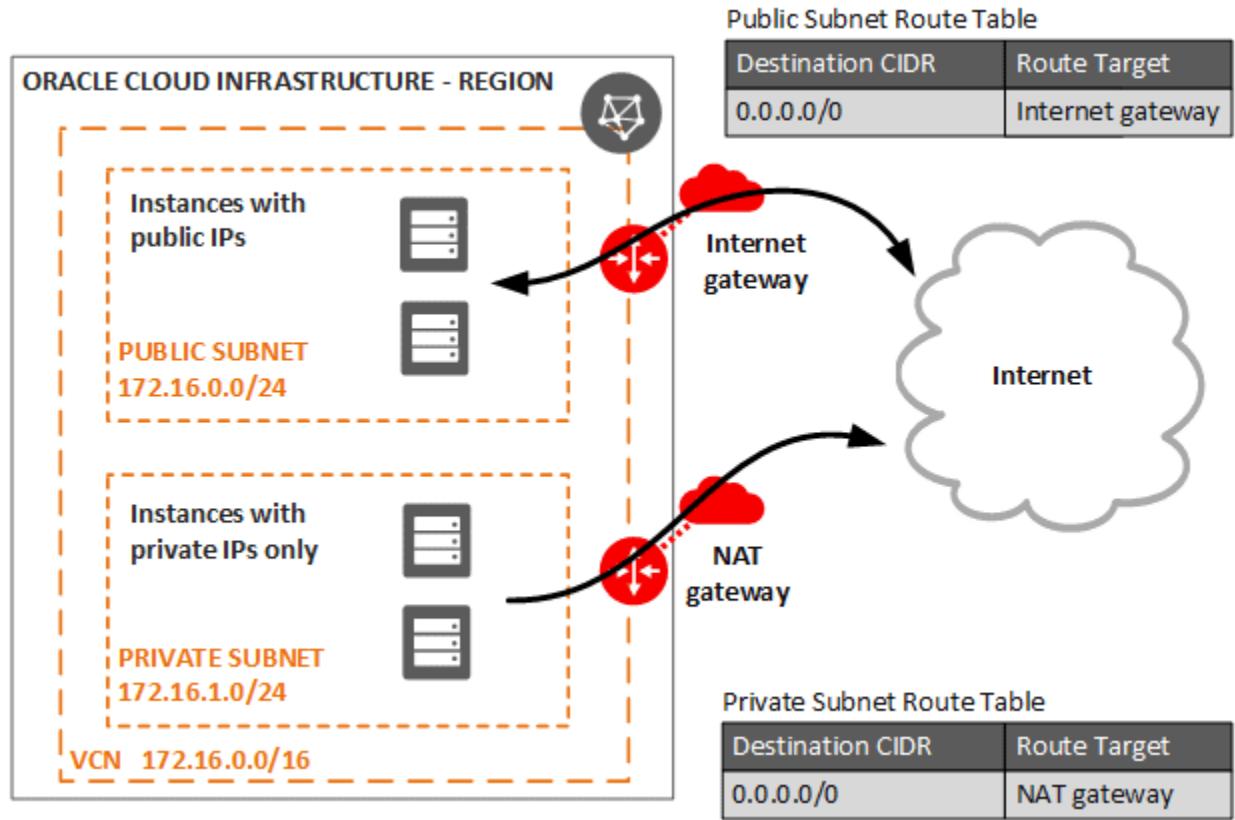
IPv4 CIDR Block Address / Mask
Mask must be between 16 and 30 [Learn more](#)

Dhcp Options Compartment in [\(Change compartment\)](#)

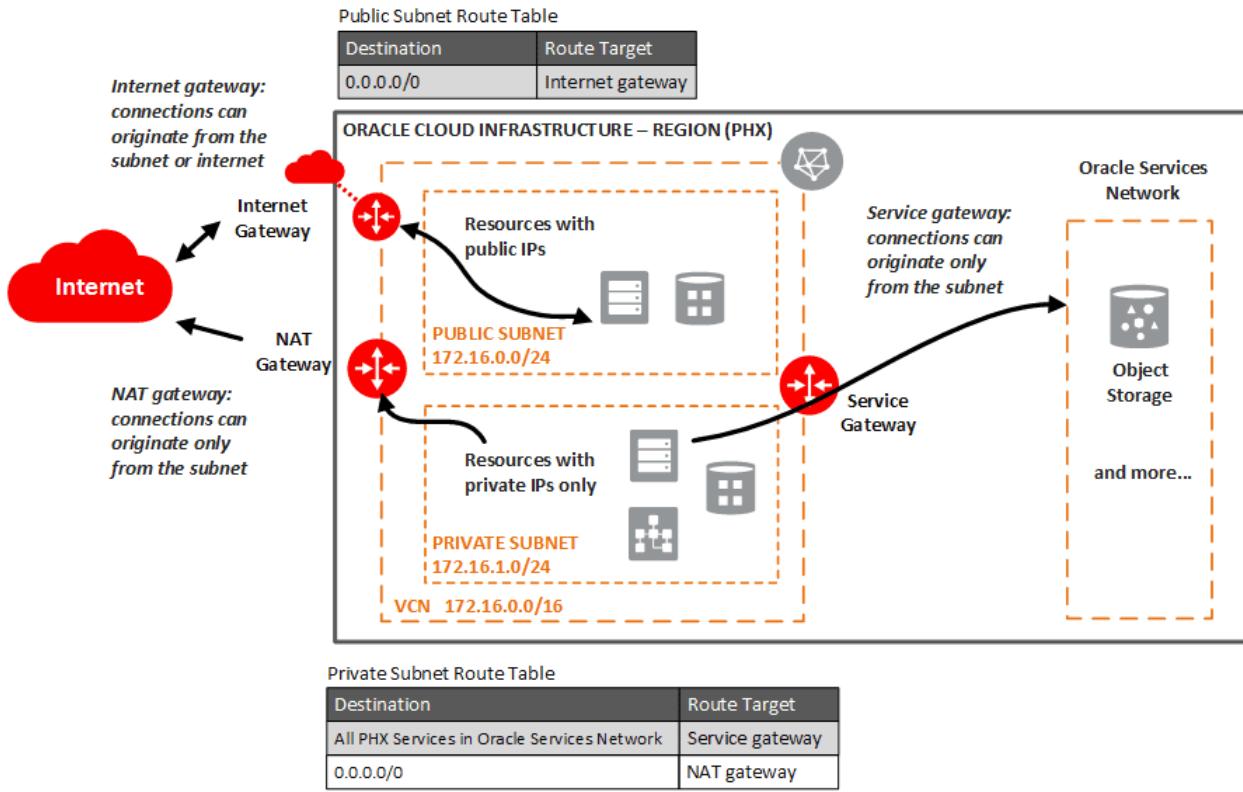
Route Table Compartment in [\(Change compartment\)](#)

Save changes [Cancel](#)

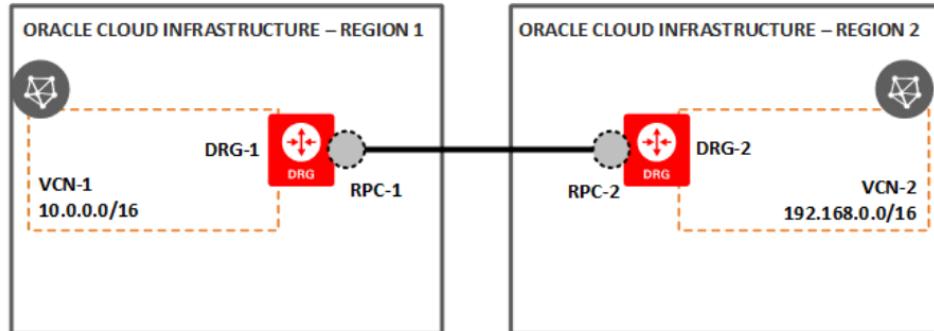
ال NAT Gateway : يستخدمه في إن لو عندي private ip ب vm وعاوز ال تطلع انترنت لكن
محدش من الانترنت يوصل لـ VM دي فبعملها ال Nat Gateway



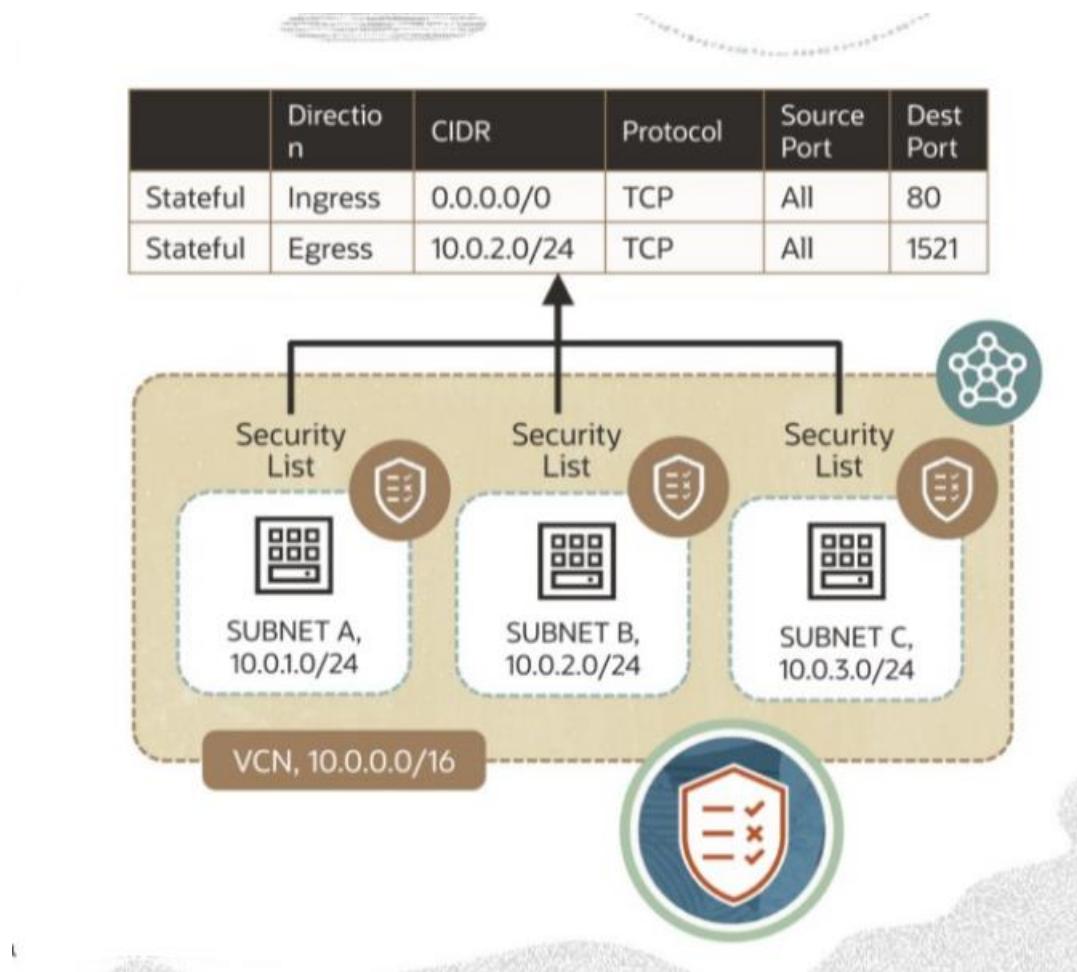
ال Service Gateway : لو عندي service من oracle فالاكونت بتاعي ول يكن storage مثلا
وواحد public ip وانا عاوز اوصله من vm داخل الاكونت فبدل م اوصله عن طريق الانترنت فبعمل
block storage وبعد كدا هقوله لو ال vm عاوزه توصل لـ service gateway من ال
Service gateway دي



ال Dynamic Routing Gateway : دي لو عاوز اربط ال OCI بال On-prem بتاعي



ب تكون داخل ال Network تحديد ال Traffic المسموحه او الممنوعه من والي ال Instance .



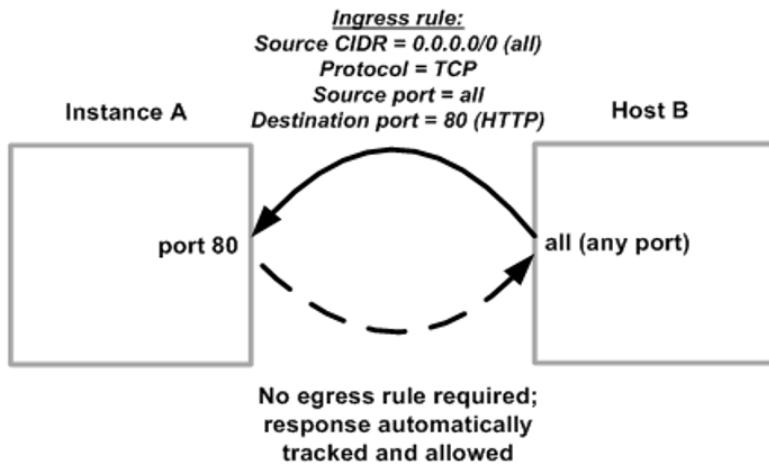
وفين نوعين :

و دا بيحدد ال Traffic ال داخل لل Instance هيدخل عن طريق Port اي مثلا - Ingress -

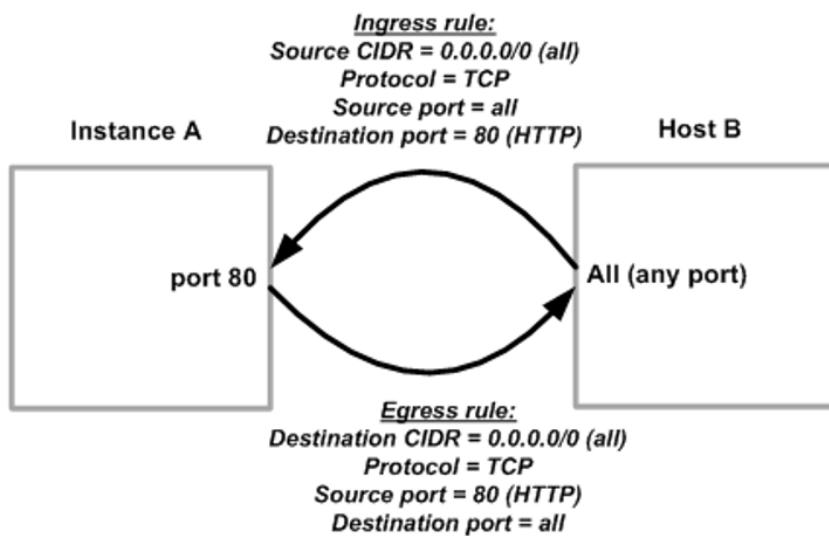
و دا العكس بيحدد الخارج من ال Instance - Egress -

و فيه عندي حالتين وهما :

port 80 : بمعنى لو عندي Host A و Host B و عاوز B يوصل ل A عن طريق Stateful - فهعمل rule تسمح بالخروج من port80 ومش شرط اعمل Rule للدخول

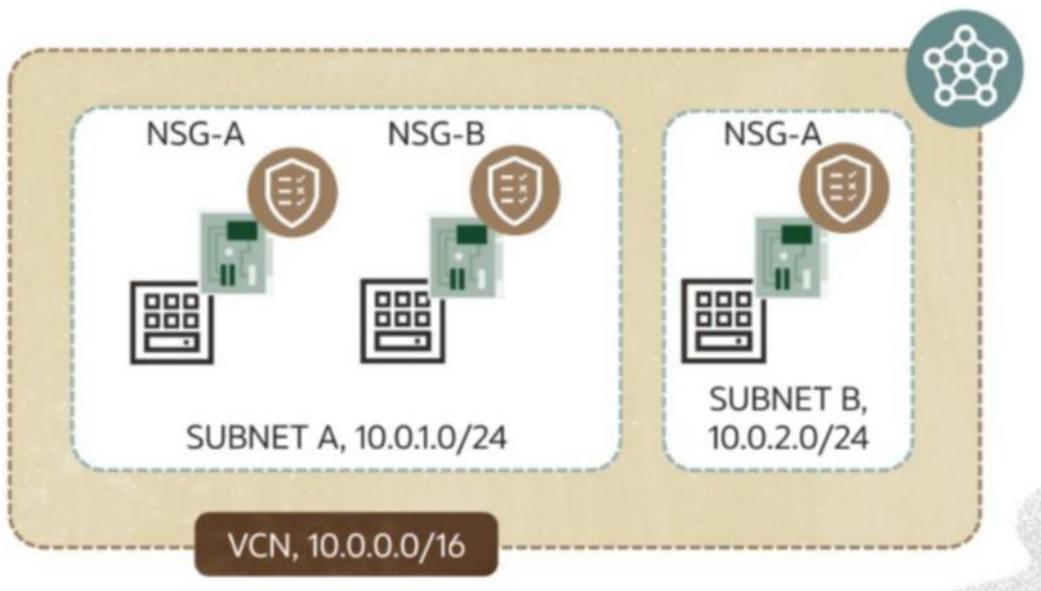


هي العكس لازم اعمل 2 rule للدخول والخروج Stateless -



ال NSG(Network Security Group) : دا بيكون علي ال Instance فقط مش علي ال Network كلها

		Direction	CIDR	Protocol	Source Port	Dest Port
NSG-A	Stateful	Ingress	0.0.0.0/0	TCP	All	80
NSG-B	Stateful	Ingress	0.0.0.0/0	TCP	All	22



مثال : لو عندي دولت 10VM وعاوز افتح port 80 على VM واحد فقط
مش هيكون صح لو عملت Security list لأنها هتطبق على ال Network كلها وال port هيفتح على كل ال VM وهذا يجي دور ال NSG بعمل NSG بال Port الحتاجه وهجي على ال VM ال تحتاجها وہتعملها لـ NSG assign فال port هيفتح على ال VM دي فقط

Rule

Stateless (i)

Direction	Source Type <small>(i)</small>	Source CIDR <small>(i)</small>
Ingress	CIDR	0.0.0.0/0
IP Protocol <small>(i)</small>	Source Port Range <small>Optional (i)</small>	Destination Port Range <small>Optional (i)</small>
TCP	All	80

Allows:

Description Optional

Save changes Cancel

ال DNS : ودا بيكون Internal DNS مش

1- ال VCN : بيكون ال DNS بتاعها عباره عن

vcnname.oraclevcn.com

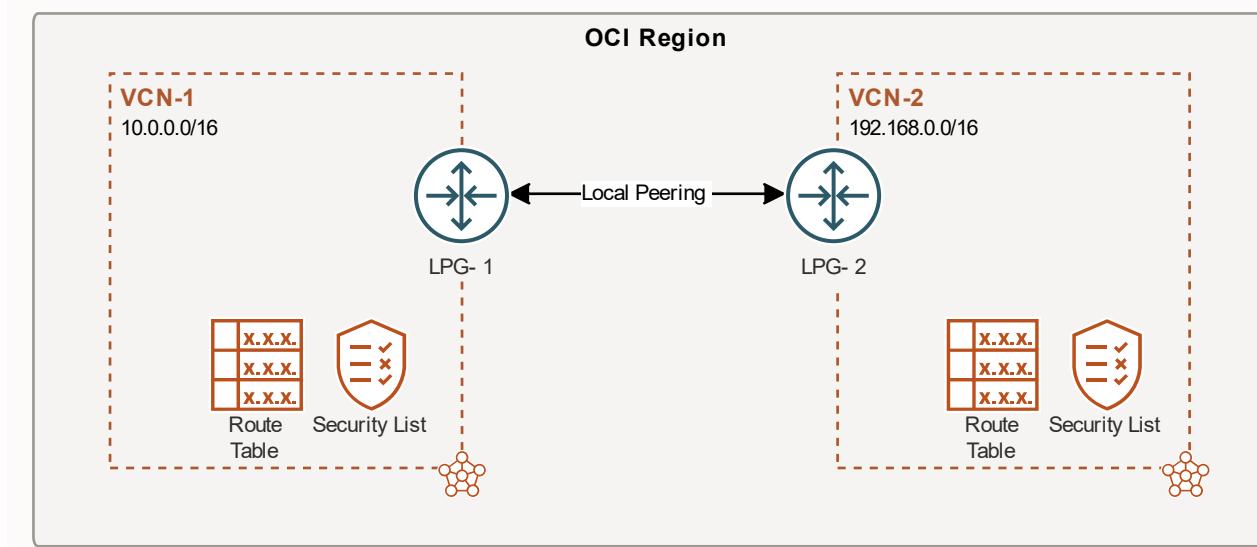
2- ال DNS : بيكون ال DNS عباره عن Subnet

subnetname.vcnname.oraclevcn.com

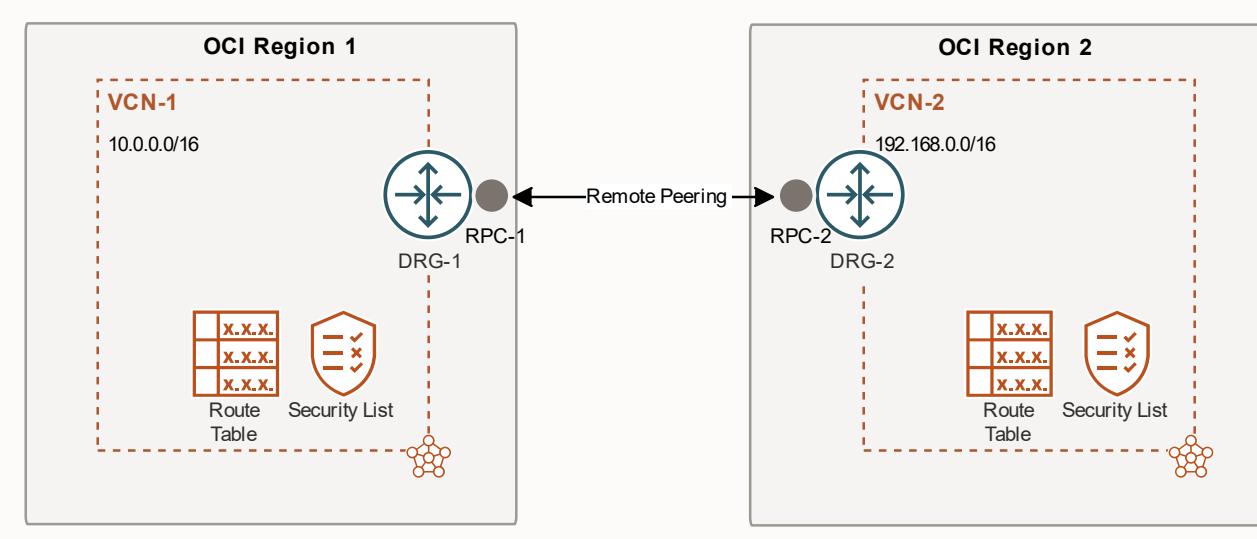
3- ال DNS : بيكون ال DNS عباره عن Instance

instancename.subnetname.vcnname.oraclevcn.com

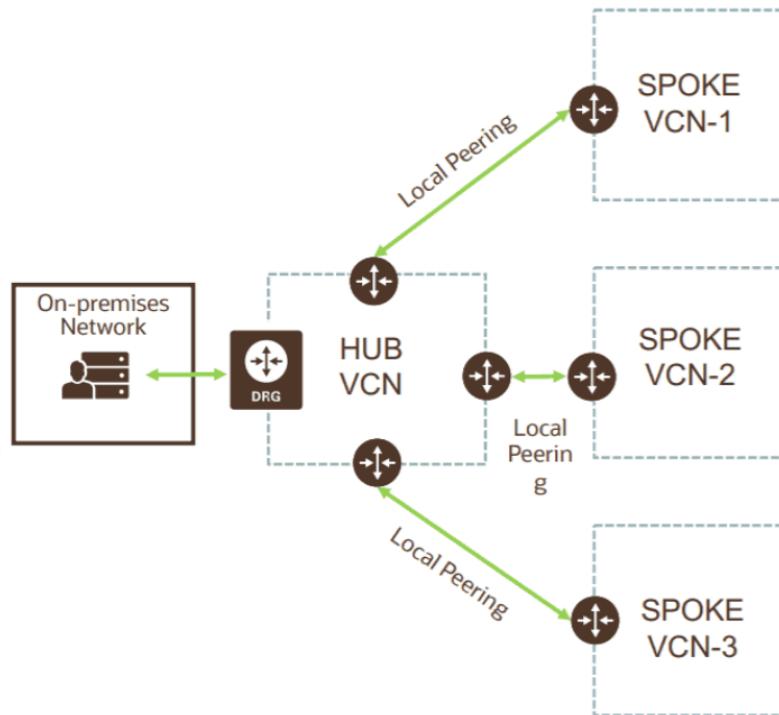
ال Local Peering : من خلالها بقدر اربط 2VCN مختلفين في نفس ال Region



ال Remote Peering(DRG) : من خلالها بقدر اربط 2VCN مختلفين في不同的 Regions



ال (Transit Routing (hub and Spoke)) عاوز 3VCN(spoke) : هنا الفكره لو عندي
اربطةهم بال on-prem (On-prem) فعمل vcn(hub) واربط ال vcn(hub) بال local peering
وال 3vcn(spoke) بال vcn(hub) واربط ال Remote peering



بشاعتك Instance Connect على ال Cloud Connectivity Options : عشان تقدر تعمل

3 أنواع ل support ب Oracle :

FastConnect (private connection) -

Site-to-Site VPN -

Public internet -

	Max Bandwidth	Latency	Jitter	Performance	Private	Oracle Charge
FastConnect	Up to 100-Gbps	Predictable	Predictable	Predictable	Yes	Port Charge Only
Site-to-Site VPN	Variable*	Variable	Variable	Variable	Yes	Above 10TB per/m
Public internet	Depends of internet quality	Variable	Variable	Variable	No	Above 10TB per/m

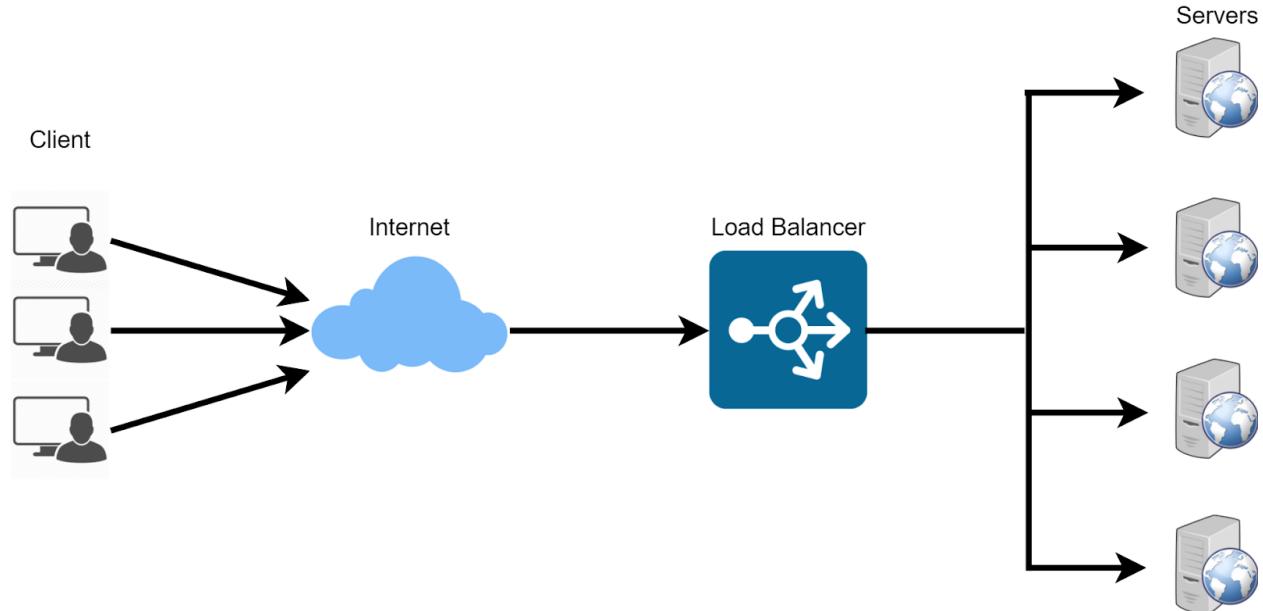
: Considerations for Cloud Connectivity Options

Cloud Connectivity Option	Considerations
FastConnect	Higher data throughput, lower latency, consistent performance Network costs may be higher than internet costs
Site-to-Site VPN	Added layer of tunneled encryption to internet connections; recommended for Proofs of Concept (POCs) Best effort performance
Public internet	Best effort performance Suited for SaaS applications and consumer/SMB use

Load Balancer : هو توزيع ال Load بين ال Servers ال عندي ولكن عندي 5web App .

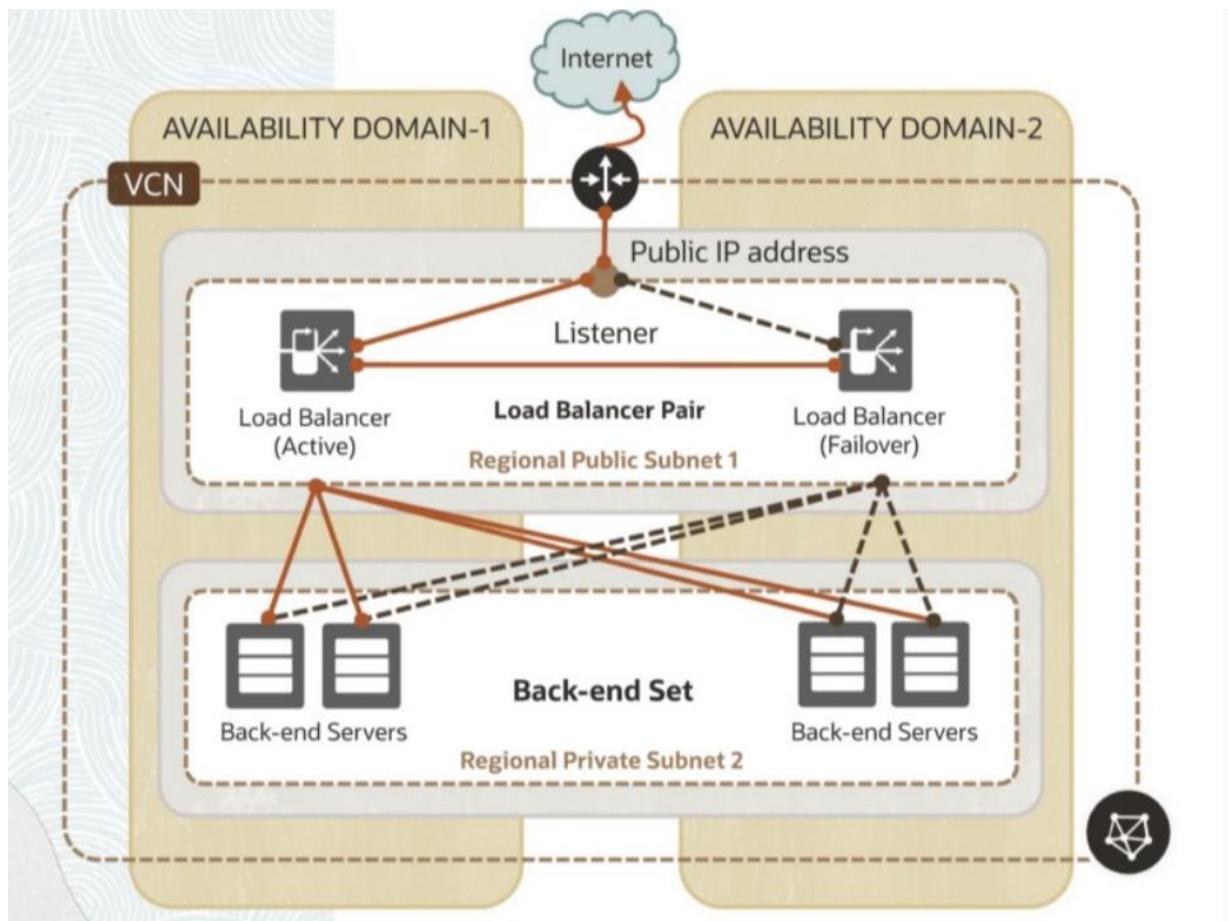
ف يعمل LB بيهما وال user ي يعمل connection على ال LB وال Request يبعث ال ل

5 من ال Server

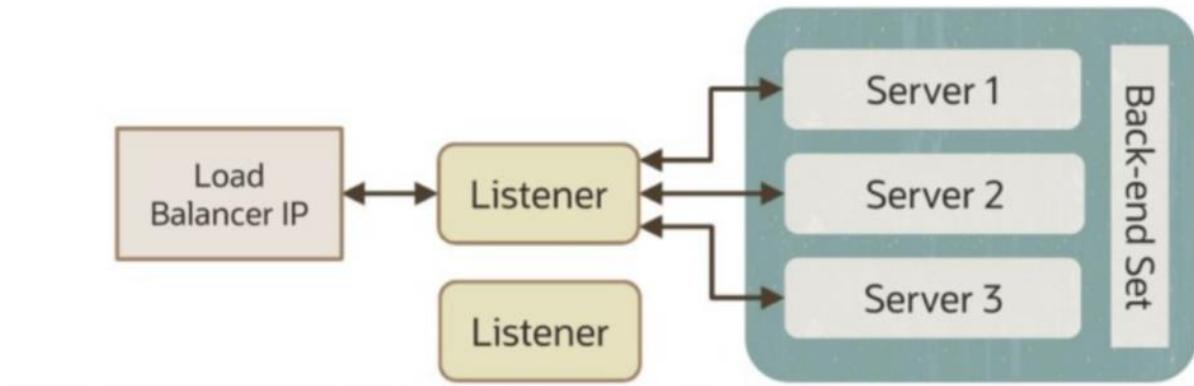


ب يكون فيه نوعين ال Public – Private
(High Availability - Scaling)
يتوفر ال Support
ال 100mbps-400mbps-8gbps في Bandwidth
ي SSL ال Support
قدر تعلم LB واحد فقط لل TCP and HTTP

لما باجي اعمل Public LB Create هو Automatic Public LB create 2 مش واحد لكن انت شايف واحد فقط وبيعمل كدا عشان يضمن لك ال High Availability



: LB Polices



ال LB هي الطريقة ال 3 هيوزع ببها ال Load و فيه عندي 3

هنا هيوزع ال Connection بالتساوي Round-Robin -1

هنا لما ال Client يدخل اول مره على ال LB بيشوف ال IP بتاعه على انهي IP Hash -2 .
ويعمله Hash وكل مره يدخل هيروح على نفس السيرفر يعني ان ال Client1 عمل server connection وراح على 2 فال LB Hash للي IP ولما ال Client1 يجي يدخل تاني برضو هيروح على Server2 (Session Persistence)

هذا يعني لما يجي له Client يوزع ال connection بناء على Least Connection -3 .
يعنى يشوف اقل Request عليه Load Server ويبعتله ال Connection

: Load Balancer Components

Load : دی ال servers الى عاوز ال LB يوزع بيهم ال Backend Server-1

health check-2 : من خلالها بتاكد ان ال servers بتعتني مفهاش مشاكل وفيه نوعين

TCP- : بتاكد ان ال IP وال Port مفهمش أي مشاكل

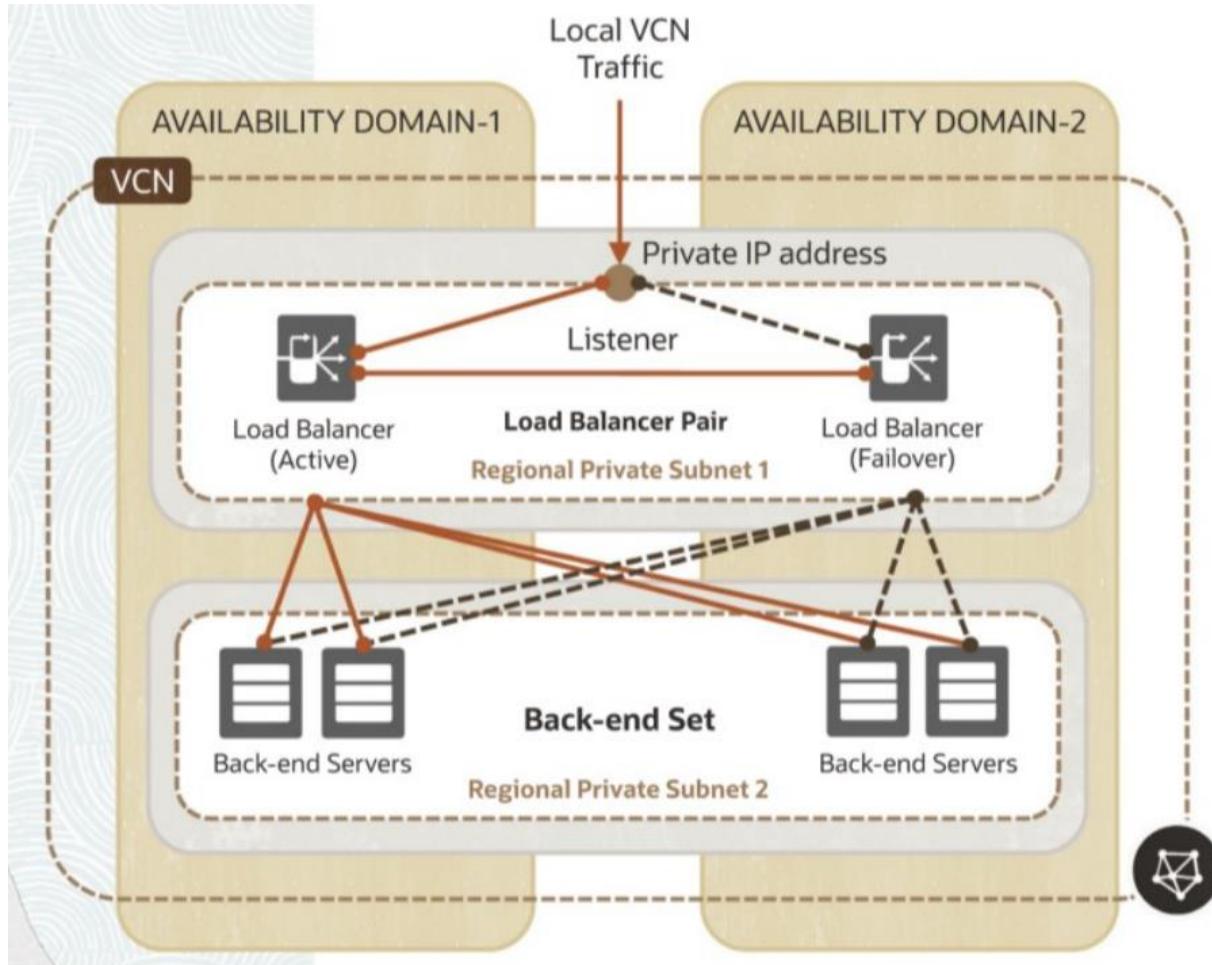
HTTP- : بتاكد ان server نفسه مفهوش مشاكل

ولو فيه أي server فيه مشكله ال LB مبيعرفش عليه أي Traffic

health check : دی حاجه logical يعرف فيها ال Backend Server وال Backend Set-3

Traffic : عباره عن ال IP وال Port ال بيجلبي عليه ال Listener-4

زی ال Public لکن هنا بیعمل LB لل Local Traffic ال Local LB فقط



از ای اعمل Create ل Load Balancer

Networking

Overview

Virtual cloud networks

Web Application Acceleration

Load balancers

DNS management

Customer connectivity

Cluster Placement Groups

IP management

Network Command Center

من Network LB هختار

The screenshot shows the 'Add details' step of the OCI Load Balancer creation wizard. It includes:

- A sidebar with numbered steps: 1. Add details (highlighted), 2. Choose backends, 3. Configure listener, 4. Manage logging.
- A 'Load balancer name' field containing 'OCI-LB'.
- A 'Choose visibility type' section with two options:
 - Public** (selected): 'You can use the assigned public IP address as a front end for incoming traffic.'
 - Private**: 'You can use the assigned private IP address as a front end for internal incoming VCN traffic.'
- An 'Assign a public IP address' section with two options:
 - Ephemeral IP address**: 'You can have an IP address from the pool automatically assigned to you.'
 - Reserved IP address**: 'You can provide either an existing reserved IP address, or create a new one by assigning a name and source IP pool.'

بعد کدا create LB و أول حاجه بحدد ال Name ثم انه هو هيكون Public ولا Private

Choose the minimum bandwidth [\(i\)](#)

Mbps

10 Mbps
8000 Mbps

Choose the maximum bandwidth *Optional* [\(i\)](#)

Mbps

10 Mbps
8000 Mbps

The maximum service limit is currently 138888 Mbps. For more bandwidth, request a service limit increase from the service limits page in the Console.

بحدد ال Bandwidth

Choose networking

Virtual cloud network in **devops** [\(Change compartment\)](#)

devops

Specify the subnet to host your load balancer. If backends have public IP addresses, configure a NAT gateway for connecting the public load balancers to its public IP address-based backends. Learn more about [configuring NAT gateway](#).

Subnet in **devops** [\(Change compartment\)](#)

public subnet-devops (regional)

Use network security groups to control traffic [\(i\)](#)

بحدد ال Subnet وال Compartment

✓ [Add details](#)

2 **Choose backends**

3 [Configure listener](#)

4 [Manage logging](#)

Choose backends

A load balancer distributes traffic to backend servers within a backend set. A backend set is a logical entity defined by a load balancing policy, a health check policy, and a list of backend servers (Compute instances).

Specify a load balancing policy

Weighted round robin

This policy distributes incoming traffic sequentially to each server in a backend set list.

IP hash

This policy ensures that requests from a particular client are always directed to the same backend server.

Least connections

This policy routes incoming request traffic to the backend server with the fewest active connections.

بعد كدا بختار ال Polices ال هشتغل بيها

Select backend servers *Optional*

No backend servers selected. Click **Add backends** to select resources from a list of available compartments. You can choose instances from one compartment at a time. After you add instances from one compartment, click **Add more backends** to add instances from another compartment. You can also add backend servers to a load balancer.

Add backends

هذا هضيف ال Servers بتابعني

Add backends

Specify the Compute instances to include in your service.

Instances in **devops** [\(Change compartment\)](#)

<input type="checkbox"/>	Name	IP address

Add selected backends

[Cancel](#)

Specify health check policy

A health check is a test to confirm the availability of backend servers. A health check can be a request or a connection attempt. Based on a time interval you specify, the load balancer applies the health check policy to continuously monitor backend servers.

Protocol Port *Optional*

Ensure your backend set's health check protocol matches the listener protocol.

Force plaintext health checks (i)

Interval in milliseconds *Optional*

Timeout in milliseconds *Optional*

A minimum value of 3 seconds is recommended, otherwise the health check might fail.

[Previous](#) [Next](#) [Cancel](#)

حدّد ال Health Check

Create load balancer

Configure listener

A listener is a logical entity that checks for incoming traffic on the load balancer's IP address. To handle TCP, HTTP and HTTPS traffic, you must configure at least one listener per traffic type. You can configure additional listeners after you create your load balancer.

Listener name

Specify the type of traffic your listener handles

Specify the port your listener monitors for ingress traffic

[Previous](#) [Next](#) [Cancel](#)

وهنا بحدّد ال Listener هيشتغل أي

: OCI Storage Services -4

OCI Storage Services



Block
Volume



Local
NVMe



File
Storage



Object
Storage

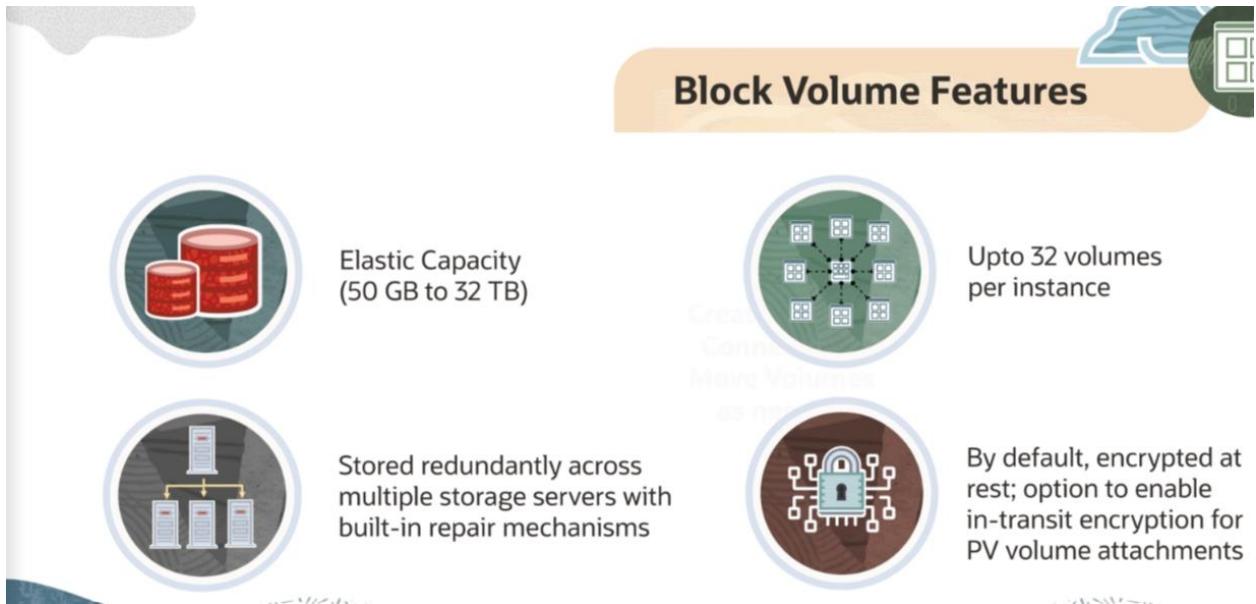


Archive
Storage

DenseLO : دي بتكون local instance في ال shape بتاعها من نوع Local NVMe -
الداتا بتكون موجوده طول ما ال VM موجوده حتى لو عملت Restart او Reboot لكن
لو اتحذت بتتحذف معها - ال durability of data مسؤولية ال Customers

lsblk						
NAME	MAJ:MIN	RM	SIZE	RO	TYPE	MOUNTPOINT
sda	8:0	0	46.6G	0	disk	
└─sda1	8:1	0	512M	0	part	/boot/efi
└─sda2	8:2	0	8G	0	part	[SWAP]
└─sda3	8:3	0	38G	0	part	/
nvme0n1	259:6	0	2.9T	0	disk	
nvme1n1	259:8	0	2.9T	0	disk	
nvme2n1	259:0	0	2.9T	0	disk	
nvme3n1	259:1	0	2.9T	0	disk	
nvme4n1	259:7	0	2.9T	0	disk	
nvme5n1	259:4	0	2.9T	0	disk	
nvme6n1	259:5	0	2.9T	0	disk	
nvme7n1	259:2	0	2.9T	0	disk	
nvme8n1	259:3	0	2.9T	0	disk	

BV : يكون منفصل عن ال Instance بمعنى حتى لو حذفت ال VM ال BV -
هيفضل موجود عادي.



اقدر اعمل Scaling و اقدر اعمل Backup
ببیدا من 50GB وتقدر توصله لحد 32TB
ال Disks بتكون من نوع NVMe SSD
ال IOPS بيكون من 60GB الى 25K GB
تقدر تعمل لحد 32 Attach لـ VM الواحد
الداتا بتكون Encrypted
بيكون فيه Redundancy

فیه نو عین من ال : Attach

Network Hardware Virtualization ال gust OS و ال ISCSI -1
وعشان كدا بيكون اسرع وافضل .

API : بيستخدم ال Hypervisor بتابع ال VM من خلال Para Virtualized -2

iSCSI Versus Paravirtualized

iSCSI:

- Uses the internal storage stack in the guest OS and network hardware virtualization
- Does not use hypervisor in the attachment process

Paravirtualized:

- Light virtualization technique
- Hypervisor APIs used by VM to access remote storage
- More efficient than full virtualization

The screenshot shows a navigation sidebar on the left with links: Home, Compute, Storage (highlighted with a yellow box), Networking, Oracle Database, Databases, Analytics & AI, Developer Services, and Identity & Security. The main content area has a header "Storage". Under "Block Storage", "Block Volumes" is highlighted with a yellow box. Other options include Block Volume Backups, Block Volume Replicas, Volume Groups, Volume Group Backups, Volume Group Replicas, and Backup Policies. Under "File Storage", options include File Systems and Mount Targets. To the right, there is a section for "Object Storage & Archive Storage" with "Buckets" listed.

عشان اعمل BV من ال Storage بختار BV

Block Volumes in Compartments

Block volumes provide high-performance network storage to support a broad range of workloads.

Create Block Volume					
Name	State	Size	Default performance	i	Auto-tuned performance
No items					

عمل create

Create block volume

Name

BV

Create in compartment

speedlaboci (root)/devops

Availability domain

اختار ال compartment وال AD

Volume size and performance

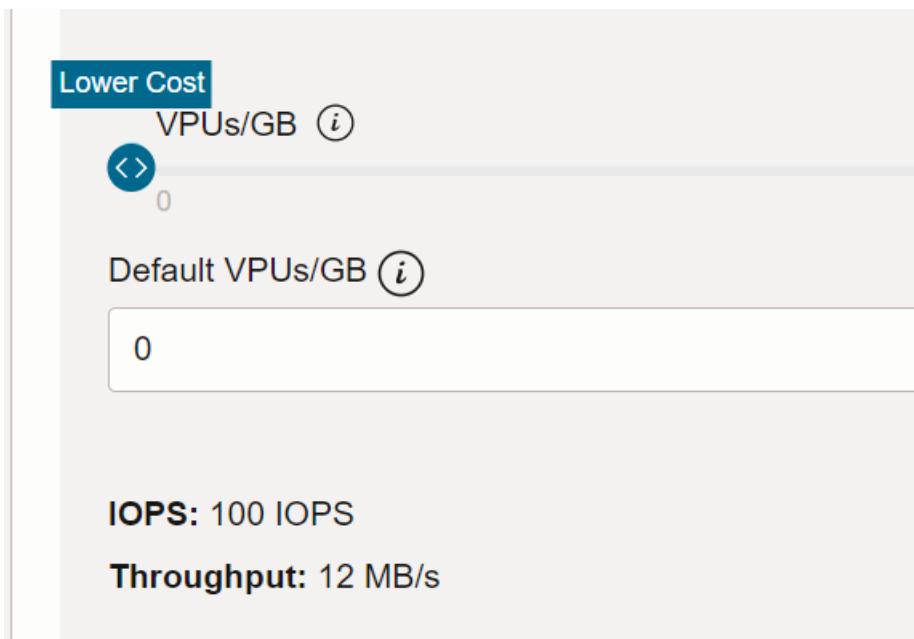
Default Custom

Volume size (in GB)

50

Size must be between 50 GB and 32,768 GB (32 TB). Volume performance varies with volume size.

Size ال بختار



ال Performance و ال IOPS بحدد

Volume Encryption

Encrypt using Oracle-managed keys
Leaves all encryption-related matters to Oracle.

Encrypt using customer-managed keys
Requires you to have access to a valid Key Management key.

 [Show Tagging Options](#)

View detail page after this block volume is created

[Create Block Volume](#) [Save as stack](#) [Cancel](#)

لاحظ انا هي بتكون Key encrypt بال خاص ب Oracle وممكن تستخدم Key خاص بيك
وبعد كدا Create

اقدر اعمل BV resize لـ

Edit volume

Name
ociarchassdemobv

Volume Size and Performance

Volume Size (in GB)
1024

Size must be an integer between the current size (1,024 GB) and 32,768 GB (32 TB). Volume performance varies with volume size.

 After the volume is provisioned, for the volume resize to take effect, you need to extend the partition. [Learn More](#)

Target Volume Performance

VPU  Balanced

10 0 120

Access Type

- ReadWrite**
Configures the volume attachment as read/write, not shareable with other instances. This enables attachment to a single instance only and is the default configuration.
- ReadWrite - Shareable**
Configures the volume attachment as read/write, shareable with other instances. This enables read/write attachments to multiple instances. To prevent data corruption you must configure a clustered file system on the volume.
- Read-only - Shareable**
Configures the volume attachment as read-only. This enables attachments to multiple instances.

ال Access Type

لما بتتجي تعمل Attach بيكون فيه option خاص بال Access

- instance write : يكون علي read و write واحد فقط
- Readwrite - Shareable : يكون read و write لكن علي اكتر من instance
- Read-only - Shareable : هيكون Read علي اكتر من instance

Backup : باخد باكب ويتحفظ في Object Storage

فيه 3 Backup Policies

- ودا بيأخذ Full Backup كل شهر و Incremental Backup كل سنة

ويعمل Backup لـ Save دا لمدة 5 سنين

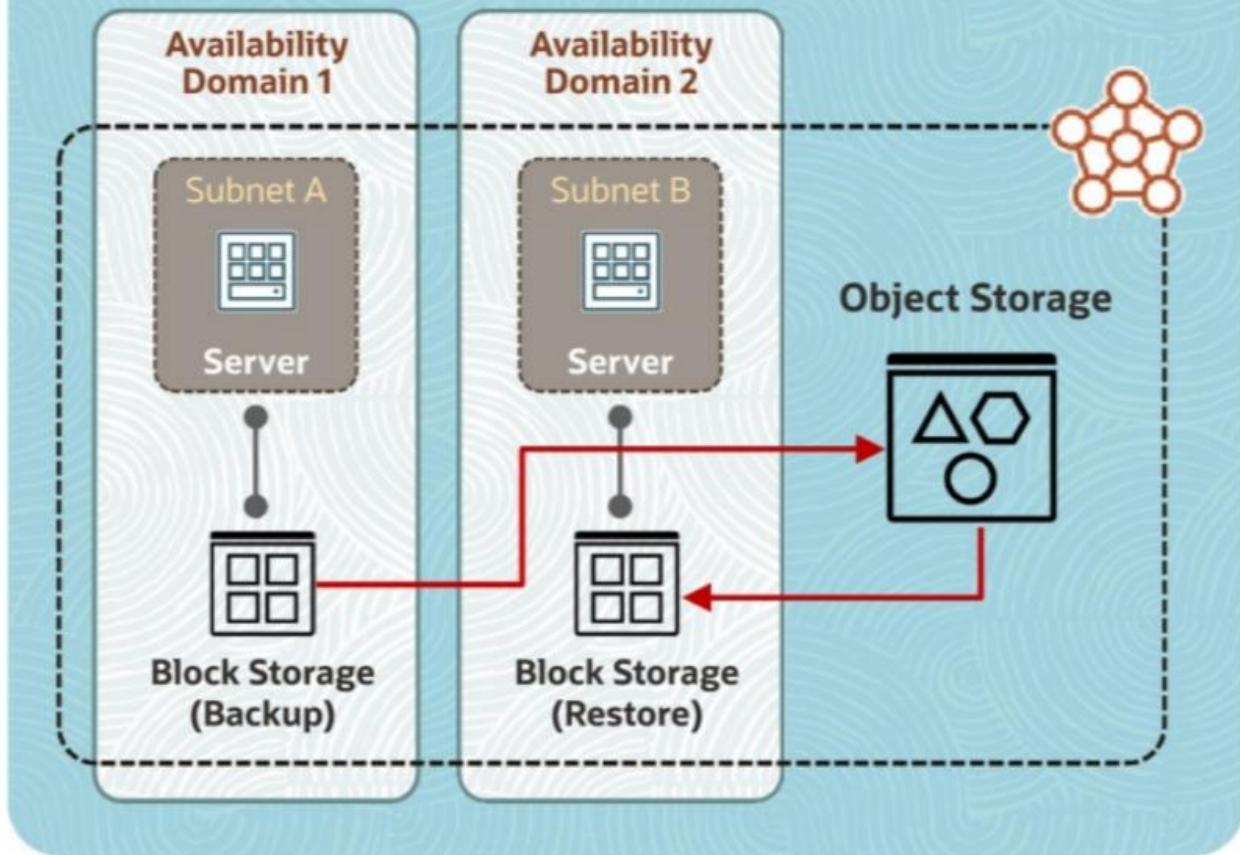
- نفس ال Bronze بس بيأخذ ال Incremental Backup كل أسبوع

- نفس ال Silver و Bronze بس بيأخذ ال Incremental Backup كل يوم

وال Backup اقدر اعمل منه Volume create لـ

ال backup بيأخذ فقط مساحه الdata الفعليه مش كل المساحة يعني لو عندي VM عباره عن 100G ومستخدم منها 40G فال backup هيكون لـ 40G

ORACLE CLOUD INFRASTRUCTURE (REGION)



Clone : باخد نسخة طبق الأصل من ال BV ال عندي واعمل منه واحد جديد بنفس الحاله بتاعته

ال Volume Group : جمع ال Block Volume المتشابه مثلا مع بعض عشان يسهل التحكم فيهم
وقدر اخد ال Volume Group backup من نفسها

: Object Storage



OCI Object Storage

- Highly Durable and Scalable
- Secure and Cost Efficient
- Highly reliable
- Internet scale and high performance storage platform
- Store unlimited amount of data
- Designed for unstructured data
- Regional Service
- Access data from anywhere
- Supports private access from OCI resources in a VCN
- Three Storage Tiers



الاستخدامات الخاصة بالـ OS

OCI Object Storage Use Cases



Content Repository



Unstructured and
semi-structured data

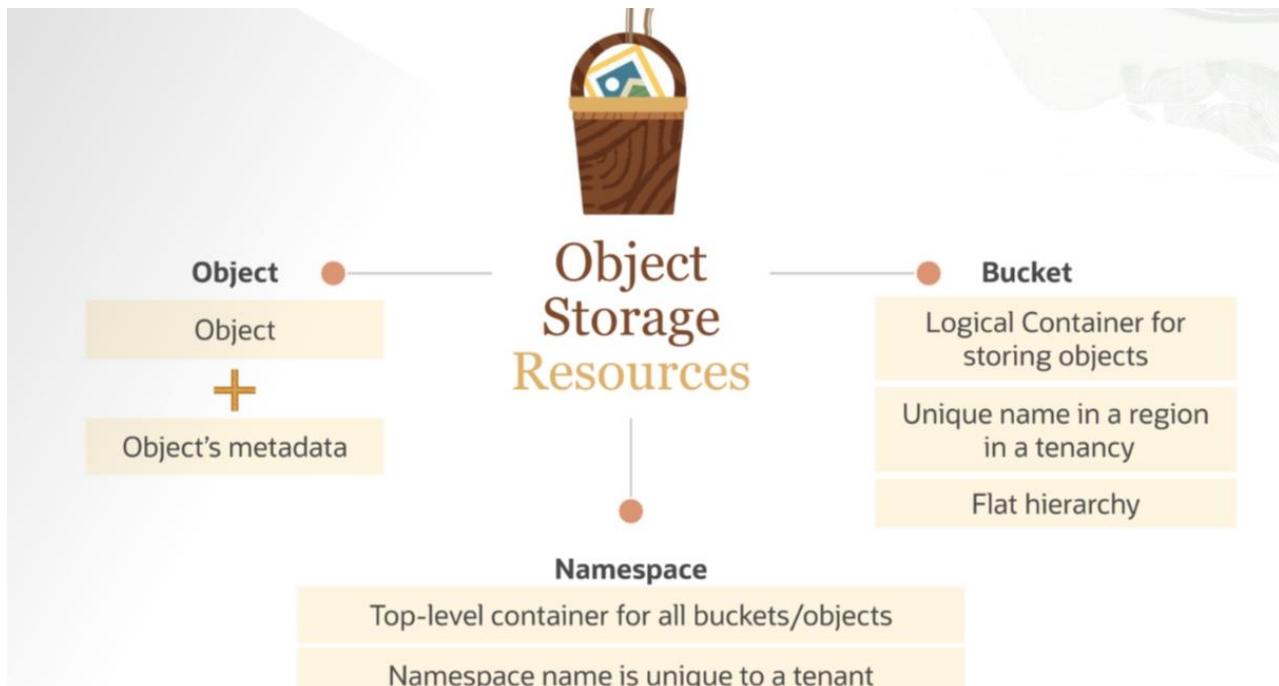


Big Data/Spark/
Hadoop/Data Analytics



Archive/Backup

: Object Storage Resources



عندی 3

ال Object ودا عباره عن ال Files بتاعتي ال هخزنهما

ال Objects دا زي Container بيكون بداخله ال Bucket

ال Namespaces وبيكون unique علي مستوى ال tenant وبقدر انظم من خلالها ال

Objects وال Buckets

Search

- Home
- Compute
- Storage**
- Networking
- Oracle Database
- Databases
- Analytics & AI
- Developer Services
- Identity & Security

Block Storage

- Block Volumes
- Block Volume Backups
- Block Volume Replicas
- Volume Groups
- Volume Group Backups
- Volume Group Replicas
- Backup Policies

File Storage

- File Systems
- Mount Targets

Object Storage & Archive Storage

- Buckets

عشان اعمله create بختار Storage من object storage

--

Object Storage & Archive Storage

Buckets

Buckets in Compartments

Object Storage provides unlimited, high-performance, durable, and secure data storage. Data is uploaded as objects that are stored in buckets. [Learn more](#)

Name	Default Storage Tier	Visibility	Created
No items found.			

Showing 0 items < 1 of 1 >

Service logs [Manage logs](#)

Resources: 0 (0 total logs) [①](#)
Logs enabled: 0
Logs not enabled: 0

بعد كدا بعمل create

Create Bucket

[Help](#)

Bucket Name

object-S

Default Storage Tier

- Standard
 Archive

The default storage tier for a bucket can only be specified during creation. Once set, you cannot change the storage tier in which a bucket resides. [Learn more about storage tiers](#)

- Enable Auto-Tiering

Automatically move infrequently accessed objects from the Standard tier to less expensive storage. [Learn more](#)

- Enable Object Versioning

Create an object version when a new object is uploaded, an existing object is overwritten, or when an object is deleted. [Learn more](#)



بعد كدا بختار ال Storage Tire

بعد ال upload ببدا اعمل create للداتا

وبيكون فيه نوعين : Storage Tire

ال (Hot) Standard ودي لـ data المستخدمه بكثـر وبيتعمل عليها Access كـثير

ال (Cold) Archive ودي لـ data كـثير مش بيحصل عليها Access مثل ال Backup

Object Storage Tiers

Standard Storage Tier (Hot)

Default storage tier

Quick, immediate and frequent access

Higher storage costs compared to other tiers

Content repository

Data repository

Infrequent Access Storage Tier (Cool)

Infrequently accessed data

Must be immediately available

Storage costs are lower than the Standard Storage Tier

The minimum storage retention period is 31 Days

Data retrieval fees

Backup of on-premises data

Archive Storage Tier (Cold)

Seldom or rarely accessed data

Lowest storage costs

The minimum storage retention period is 90 days

Must be restored before they are available for access

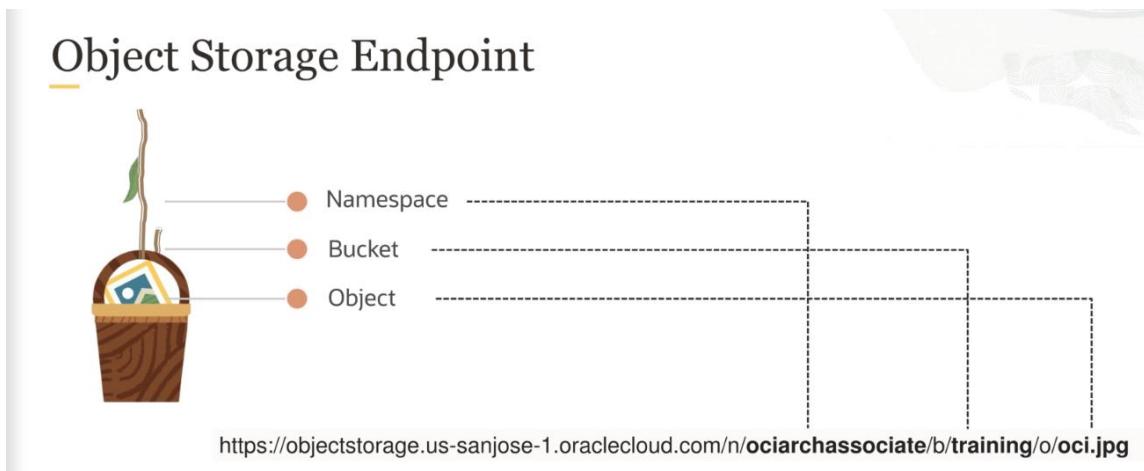
Restore time: 1 hour

Compliance and audit mandates

Object Name : بيكون عباره عن

/n/namespacename/b/bucketname/o/objectname

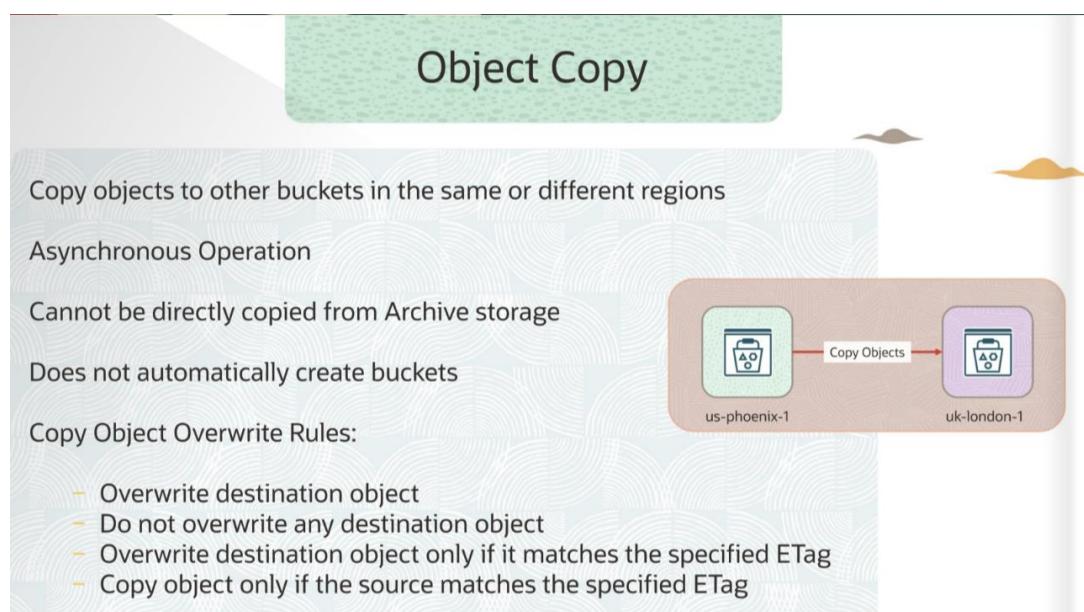
عشن اعمل Access بعمله Public كدا الكل هيقدر يعمله
او Pre-Authentication ودا بعمله ب URL معينه وبيطلعي Permissions بقدر من خلاله اعمل
وال URL بيكون تقسيمة كدا object بتاعي لـ Access



بيكون عباره عن ال

Objectstorageurl/P/Password/n/NSname/b/ bucketname /O/objectname

اقدر اخد Object Copy لـ region تاني : اقدر اخذ Object Copy لـ region من Cross-region copy



Life cycle policies : يحدد من خلالها المدة الخاصة بال files ال هتفضل موجوده في ال delete وبعد المده دي تنتقل لل Archive او يحصلها Standard مثلا بعد 30 يوم هينتقل ال Files من Standard لل Archive وبعد مثلا 150 يوم يحصل Files لل Delete

Create Lifecycle Rule

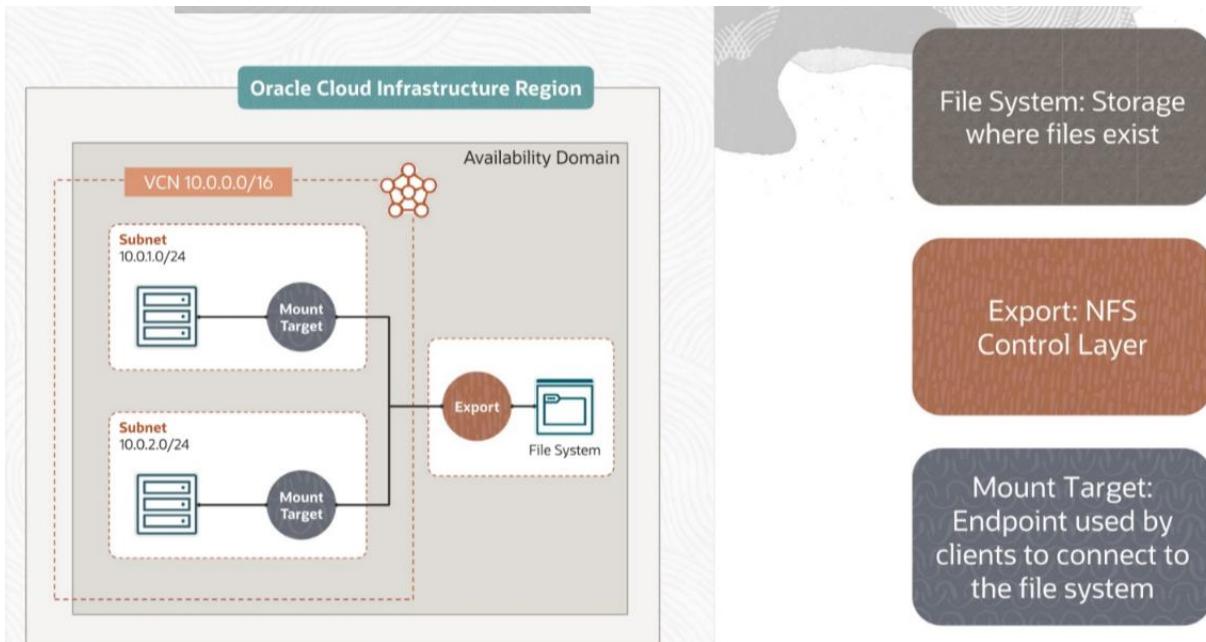
Name testrule	Target	
<div style="display: flex; justify-content: space-between;"> <div style="width: 33%;"> <p>Latest Version of Objects</p> <p>Create a lifecycle rule that applies to the latest version of either:</p> <ul style="list-style-type: none"> • All objects in the bucket • Objects that match the object name filters that you specify </div> <div style="width: 33%;"> <p>Previous Versions of Objects</p> <p>Create a lifecycle rule that applies to the previous versions of either:</p> <ul style="list-style-type: none"> • All objects in the bucket • Objects that match the object name filters that you specify </div> <div style="width: 33%;"> <p>Uncommitted Multipart Uploads</p> <p>Create a lifecycle rule that deletes uncommitted or failed multipart uploads.</p> </div> </div>		
Lifecycle Action Move to Infrequent Access		
Number of Days 30		
<p>Object Name Filters (Optional)</p> <p>Use object name filters to specify which objects the lifecycle rule applies to. You can choose objects using prefixes and pattern matching. If no name filter is specified, the rule applies to all objects in the bucket. Learn more about using object name filters</p> <p>You can add object filters in any order. Object Lifecycle Management takes care of the evaluation precedence.</p>		

هـو File Storage network file system زـي الـ Share كـدا
اقدر اعمل من أي bare metal او VM داخل الـ VCN Connect to the file system
اقدر اعمل من خـارج الـ VCN عن طـريق الـ Access the file system
VCN peering, FastConnect, and IPSec VPN
بـ Support و NFSv3 protocol Network Lock Manager

: استخدامـه



: File Storage Concept



ال File System : بيعتوري علي ال Files ال عاوز اخزنها واعملها Share
ال Mount Target : هو ال بيتيح توصيل ال File System بأجهزة أو أنظمة مختلفة بيتعمل داخل ال VCN ودا ال Client Connect عليه

ال Export : دي الطريقة ال بيحصل بيها ال Share لل File System من خلال Mount Target

Search

- Home
- Compute
- Storage**
- Networking
- Oracle Database
- Databases
- Analytics & AI
- Developer Services
- Identity & Security
- Observability & Management

Storage

- Block Storage**
 - Block Volumes
 - Block Volume Backups
 - Block Volume Replicas
 - Volume Groups
 - Volume Group Backups
 - Volume Group Replicas
 - Backup Policies
- Object Storage & Archive Storage**
 - Buckets
- File Storage**
 - File Systems
 - Mount Targets**

عشن اعمله Create Storage هختار File Storage وابدا بلا Mount Targets من

Mount Targets are NFS

Create Mount Target

<input type="checkbox"/>	Name
	MountTarget1

0 selected

New Mount Target name *Optional*

MountTarget1

Availability Domain *i*

Virtual Cloud Network

Subnet *i*

Use Network Security Groups to control traffic *i*

Show advanced options

Create **Save as stack** **Cancel**

بعد كدا بعمل Create واحد دل AD وال VCN وال subnet واضغط

File Storage

File Systems

Mount Targets

Additional resources

Outbound Connectors

File Systems in Compartment

File Storage provides durable, scalable, secure, enterprise-grade network File System container instance in your Virtual Cloud Network (VCN). [Watch a video introduction.](#)

	Name	State	Availability Domain
No File Systems found using the selected compartment			

عشان اعمل ال File System من storage من هختار File System

Create File System

[Help](#)

This workflow creates a new File System. To get started, choose the type of File System you want to create. Then, you can keep the provided information or click **Edit details** to change it. Click **Create** to finish.

File System for NFS

Create a File System and an associated Export in a Mount Target. You can mount and access the File System as soon as it is created. [Learn more about mounting File Systems.](#)

File System for Replication

Create an unexported File System. Unexported File Systems can be used as target File Systems for replicated data. [Learn more about replication.](#)

File System information

[Edit details](#)

Name: FileSystem-01



Availability Domain:

Compartment:

Encryption key:

بحدد ال AD وبحدد ال NFS

Export information

[Edit details](#)

Exports control which File Systems are available to a given Mount Target. Create a new Export to make your File System available through the selected Mount Target. [Learn more.](#)



Export path: /FileSystem-01

Use secure Export options: Disabled

Use LDAP for group list: Disabled

بحدد ال Export Path

Mount Target information

[Edit details](#)

Mount Targets are endpoints used to access your File Systems. The following Mount Target will be created and associated with your new File System. [Learn more.](#)

New Mount Target name: MountTarget1

Compartment:

Virtual Cloud Network:

Subnet:



بحدد ال Mount target ولو مكتش عامل create هنا كان هينشاً واحد عشان يضع به ال FS ال هينشاً

By: Mostafa Mahmoud Bahgat

LinkedIn:<https://www.linkedin.com/in/mostafamahmoudbahgat>