**Essential Google Cloud Infrastructure: Foundation**

**Virtual Networks**

Virtual Private Cloud (VPC)

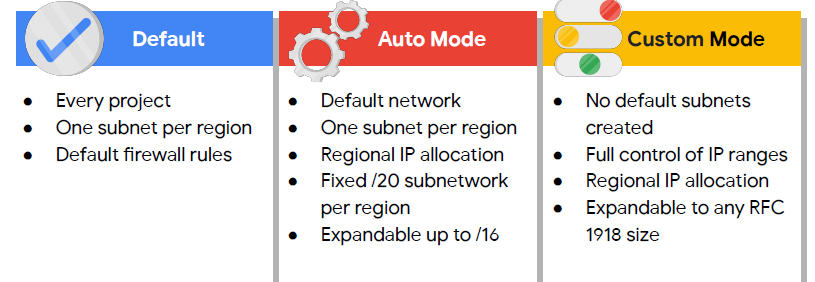
* Projects
* Networks
* Subnetworks
* Regions
* Zones
* IP address (internal and external)
* Virtual Machines
* Routes
* Firewall Rules

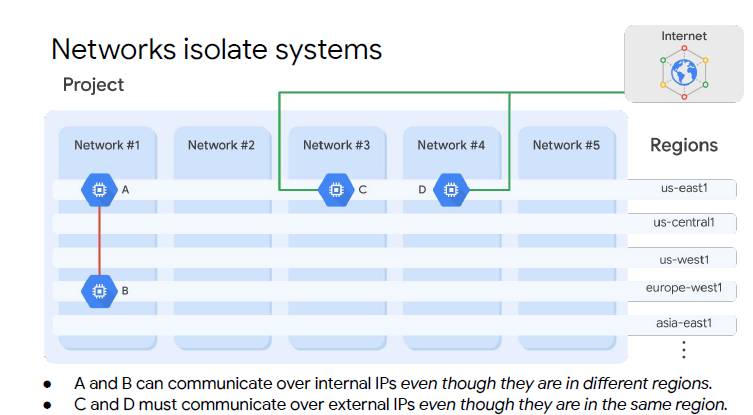
Project

* Associates objects and services with billing
* Contains up to 5 networks that can be shared/peered

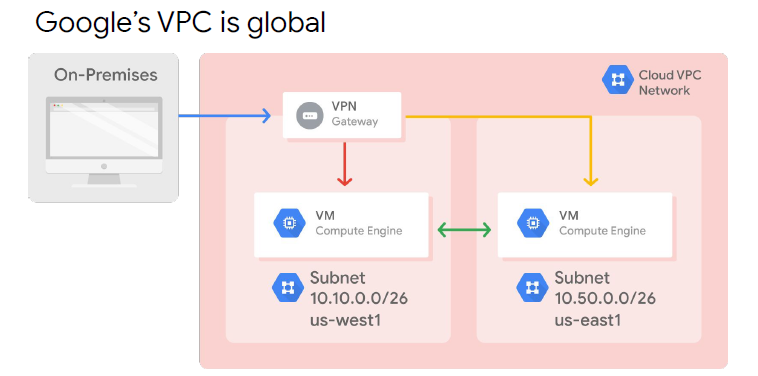
Network

* No IP address range
* Global, spans all regions
* Contains subnetworks
* Available as default, auto or custom

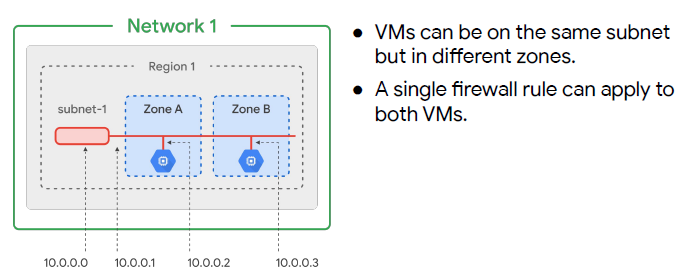


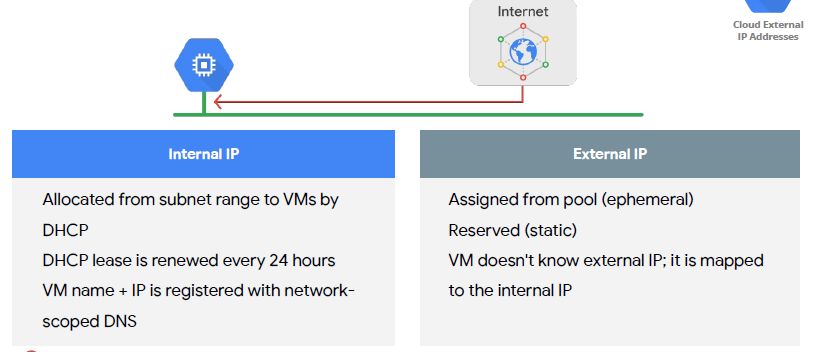


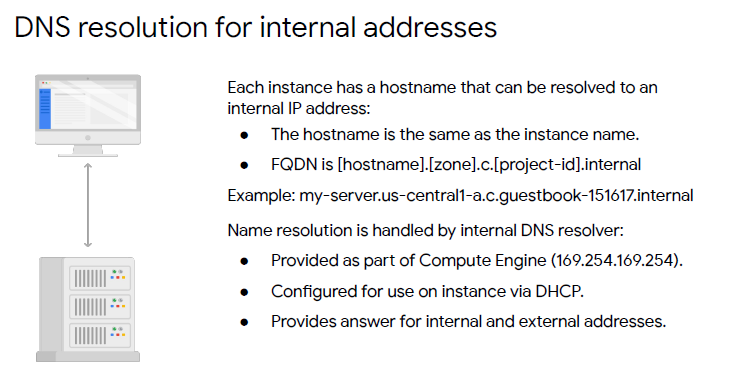
A single VPN can connect on-prem to your GCP network

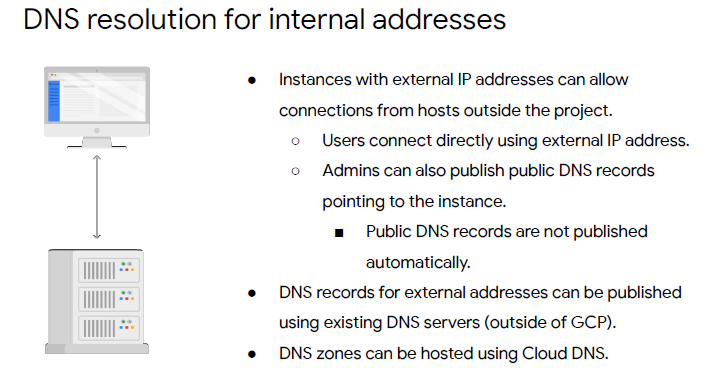


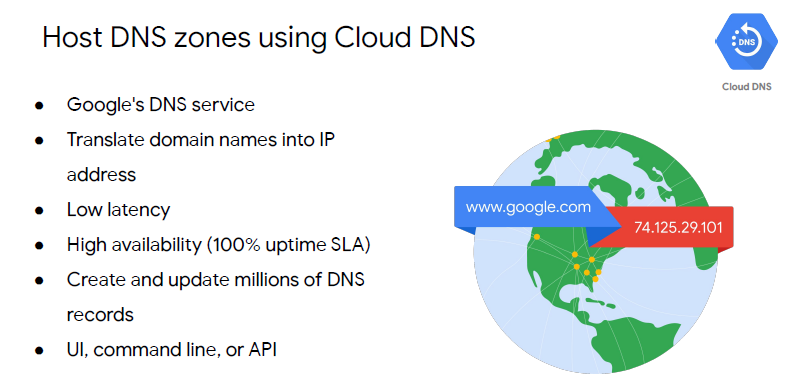
Because a region contains different zones, subnets can cross zones

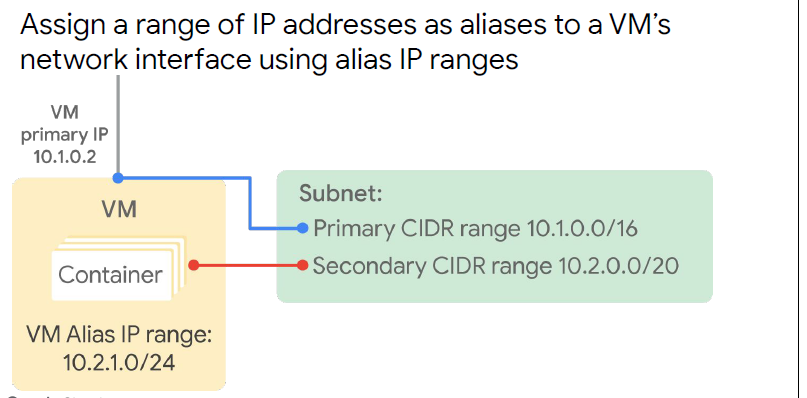


VMs have internal IP address and optional external IP address







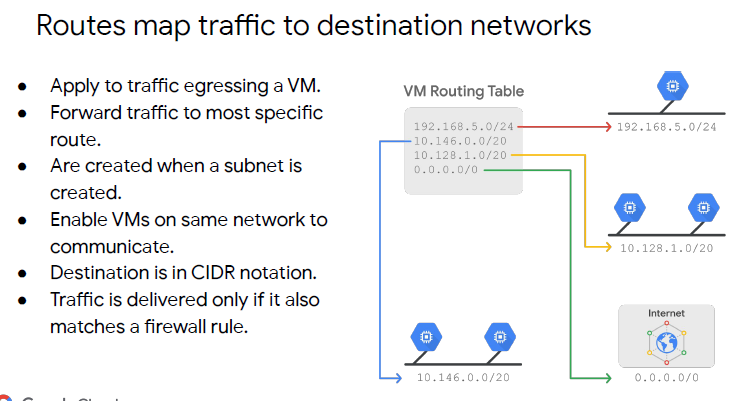


Every network has:

Routes that let instances in a network send traffic directly to each other

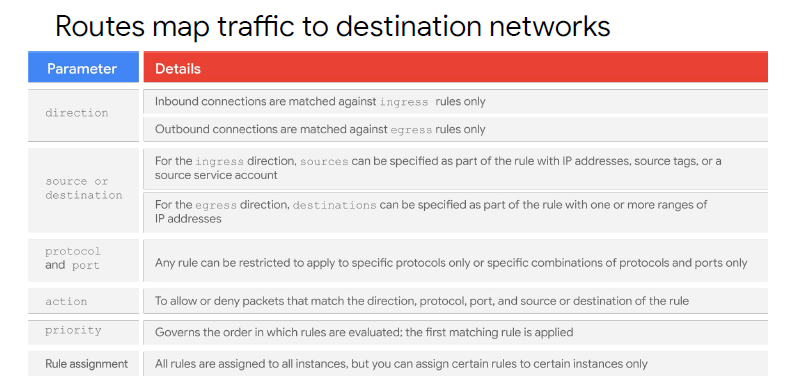
A default route that directs packets to destinations that are outside the network

Firewall rules must allow the packet



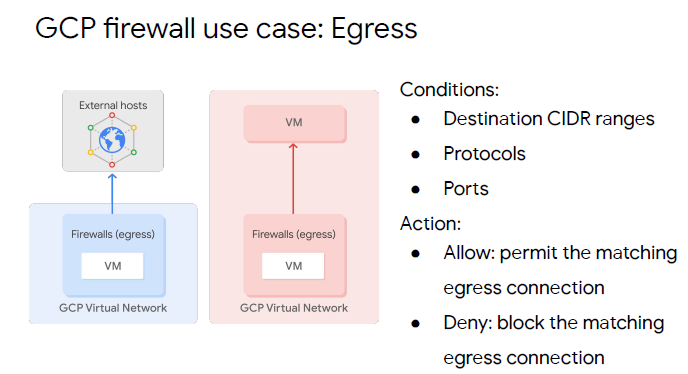
Firewall rules protect your VM instances from unapproved connections:

* VPC network functions as distributed firewall
* Firewall rules are applied to the network as a whole
* Connections are allowed or denied at the instance level
* Firewall rules are stateful (all traffic in either direction allowed)
* Implied deny all ingress and allow all egress



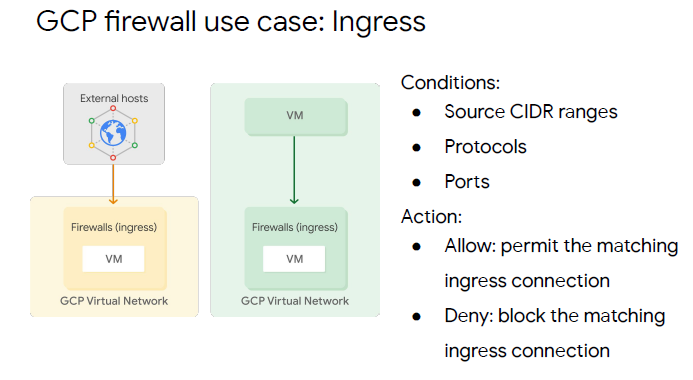
Egress firewall

* Egress firewall rules control outgoing connections originating from GCP network
* Use destination ranges to protect from undesired connections initiated by VM instance to external hosts or other internal VMs

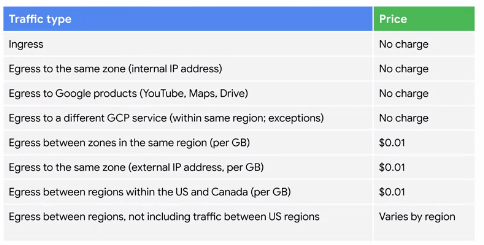


Ingress firewall:

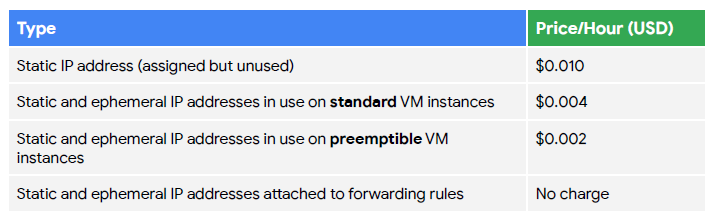
* Ingress firewall rules protect against incoming connections to the instance from any source
* Source slide rangers used to prevent undesirable incoming connections from either external host or internal VMs



Network Pricing Table

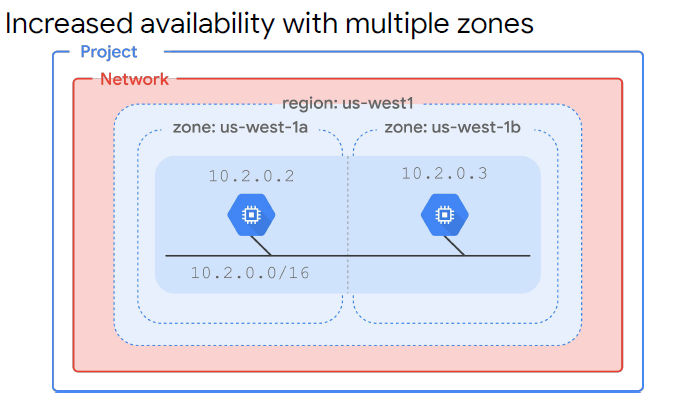
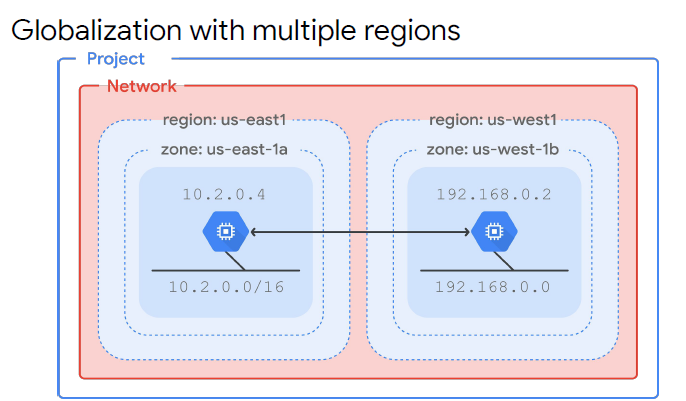


External IP pricing



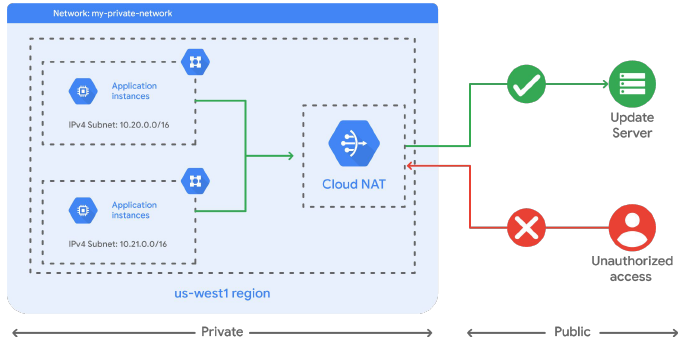
More expensive to have an unassigned static IP address than an assigned static IP address

Below are some common network designs:

* Increase network availability, place 2 VMs in multiple zones but within the same subset. Create firewall rules against subnet   
  
* Globalisation with multiple regions: provides an even higher degree of failure independence. Robust systems across different failure domains. Use load balance to route traffic to the region that is closest to the user. Better latency 

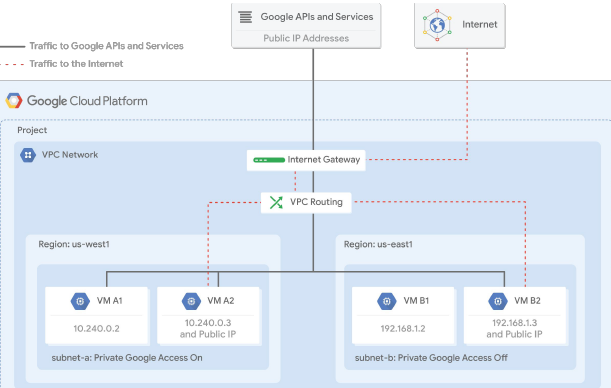
Cloud NAT

* Cloud NAT (Network Address Translation service) enables VMs without an external IP address to access the internet in a controlled manner (i.e. updates, patching, config management)



Private Google Access

* Enable Private Google Access to enable instances without external IP address to reach external IP addresses of Google APIs and services (e.g. if internal instance needs to access cloud storage bucket)
* Enabled on a subnet-by-subnet basis
* Has no affect on a VM that has an internal IP address
* In the below image, VM B1 is the only instance unable to access Google APIs and Services



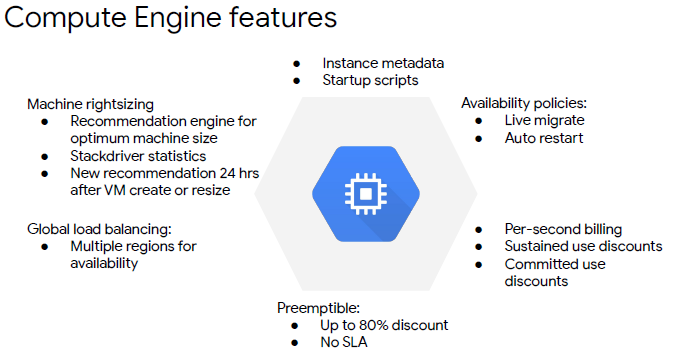
**Virtual Machine**

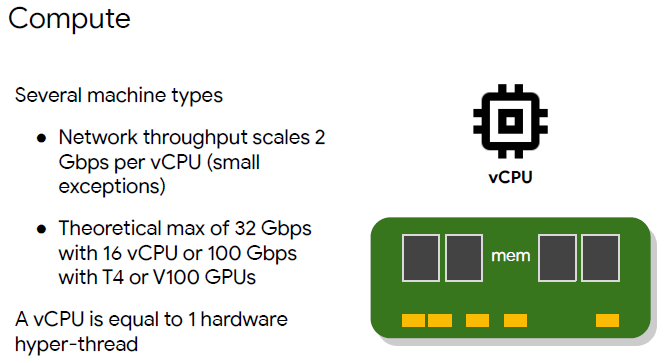
Compute Engine

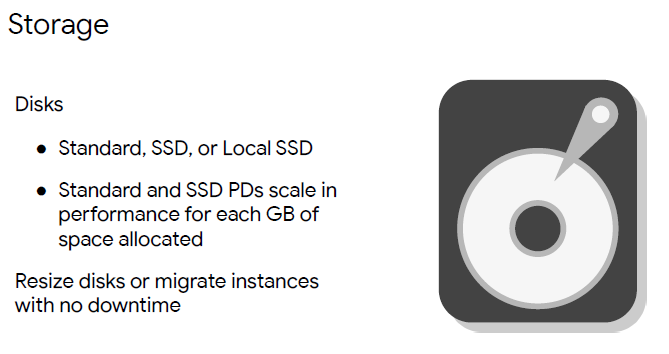
* Supports any language
* IaaS
* Server autoscaling
* Used for general workloads

Compute engine can be predefined or custom, allowing you to choose:

* vCPUs and Memory (Cores and RAM)
* Disks (HDD, SSD and local SSD)
* Networking
* Linux or windows

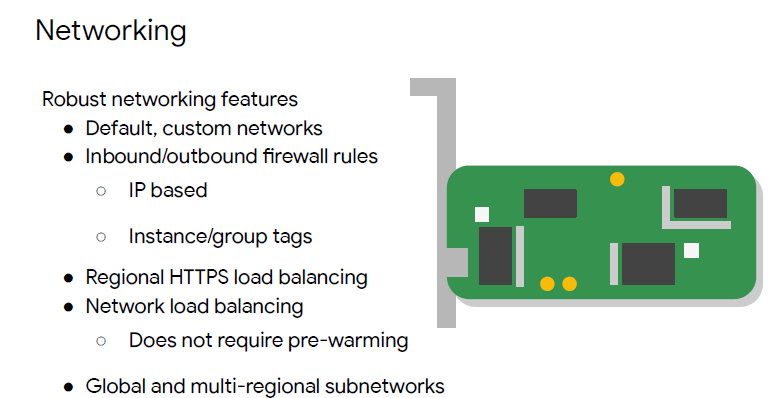


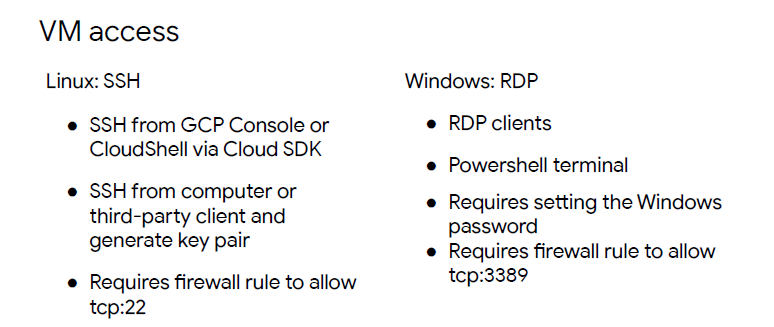


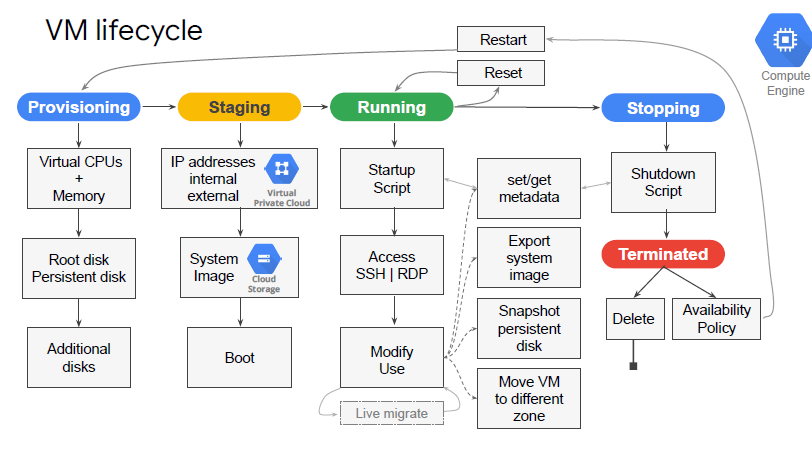


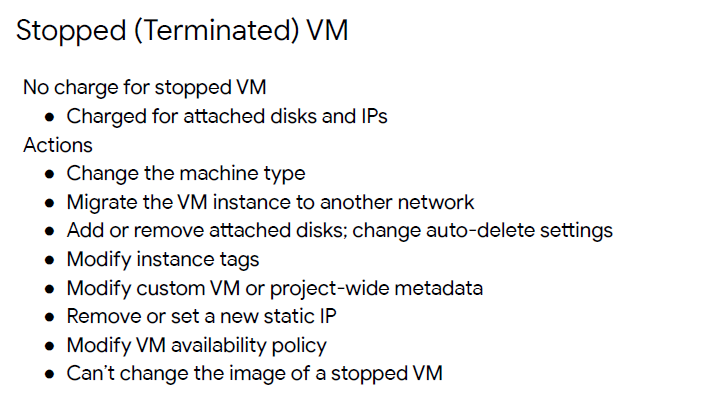
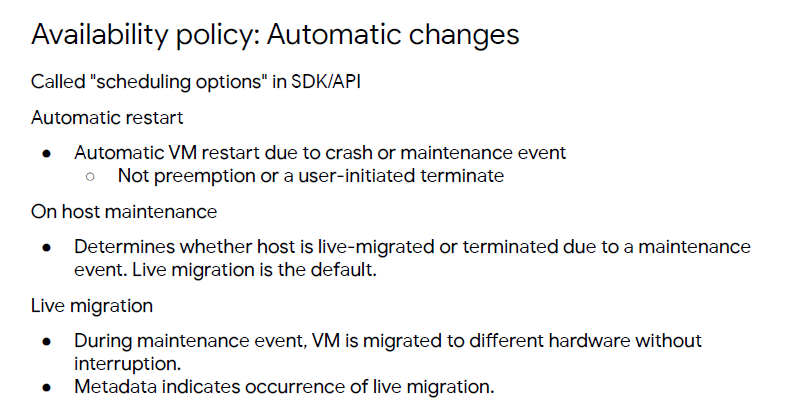
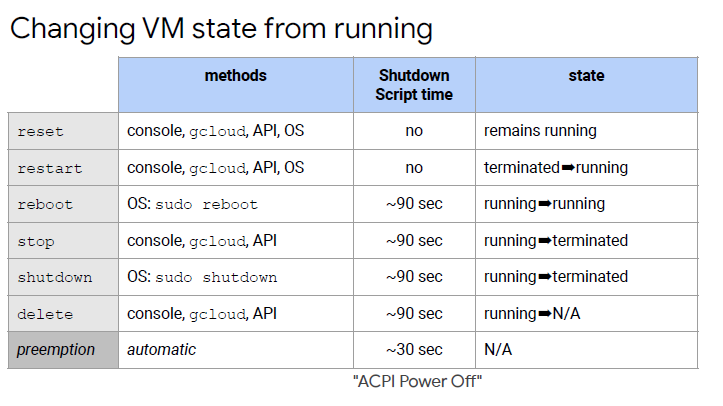
Local SSD give higher throughput and lower latency than SSD as they are attached to the physical hardware (mostly used as a swap disk). Data on local SSD persists only until you stop or delete the instance

Local SSD up to 3 TB, HD and SSG up to 64TB



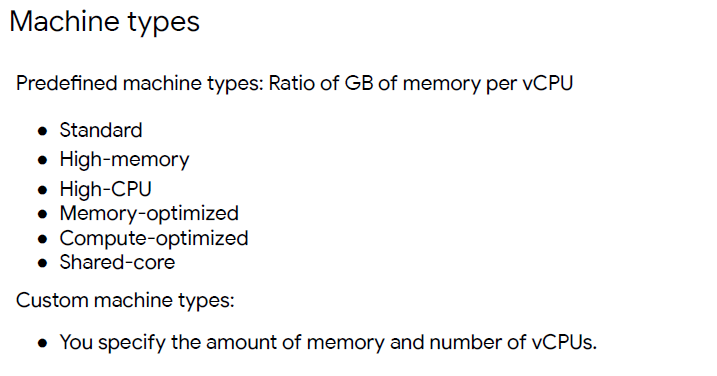




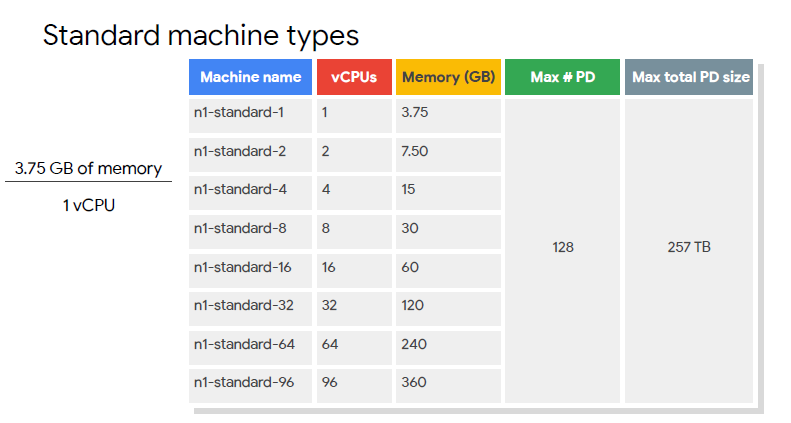


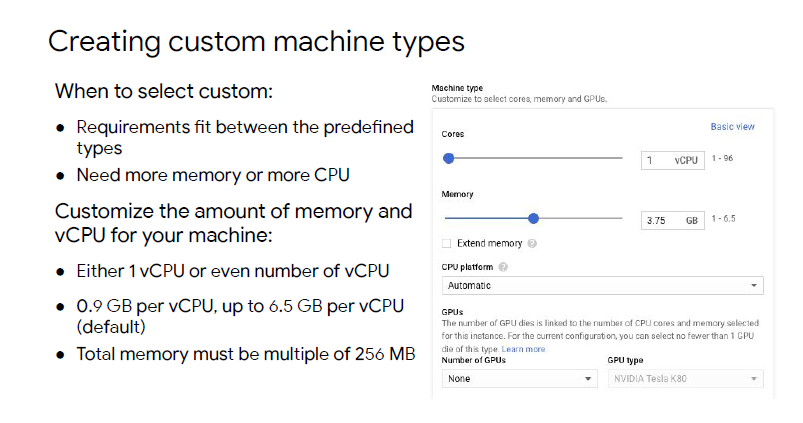
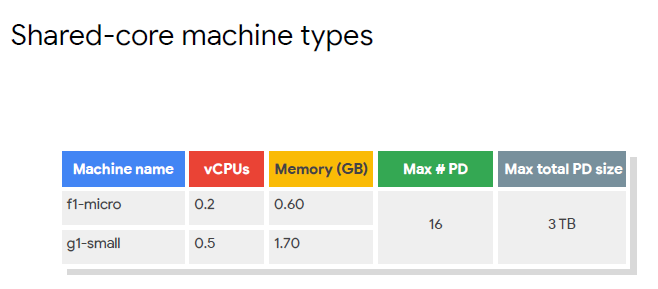
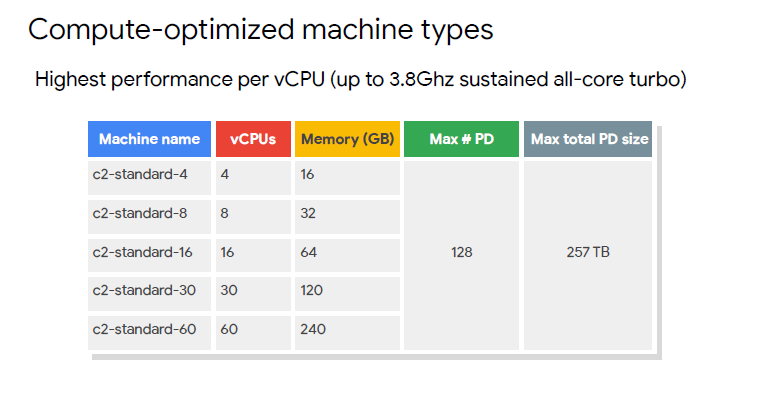
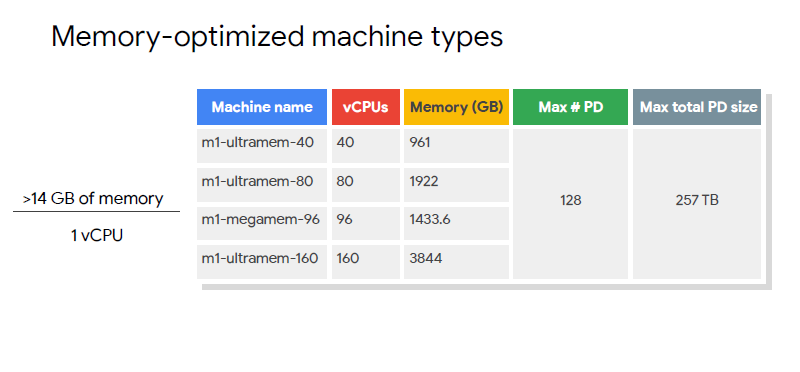
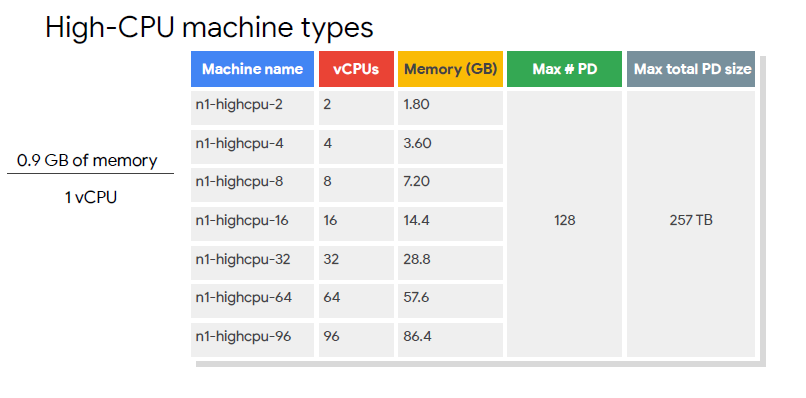
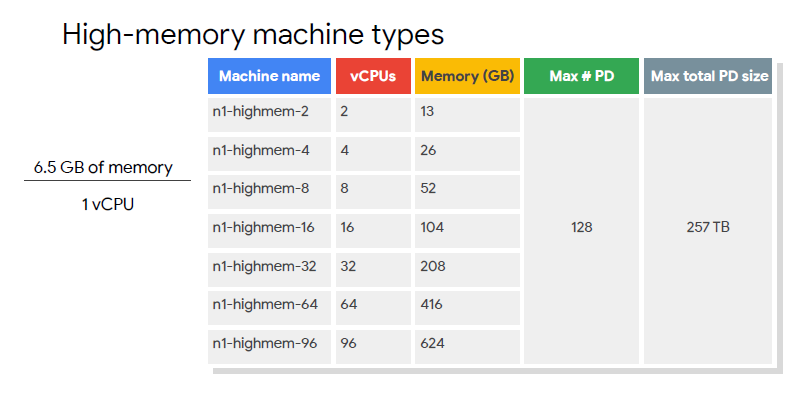
Compute Options

VM can be create vis console, Cloudshell or REST API

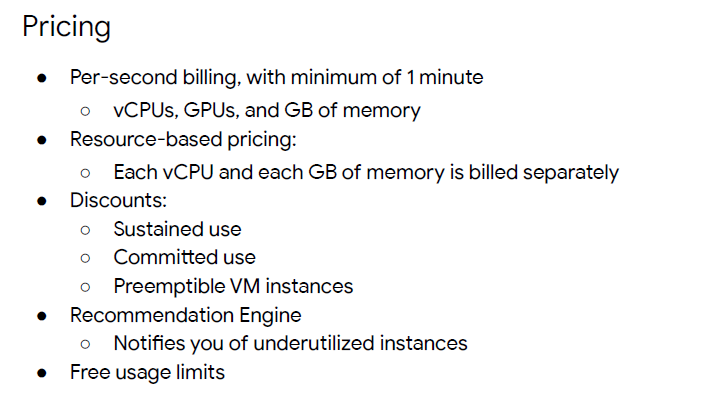


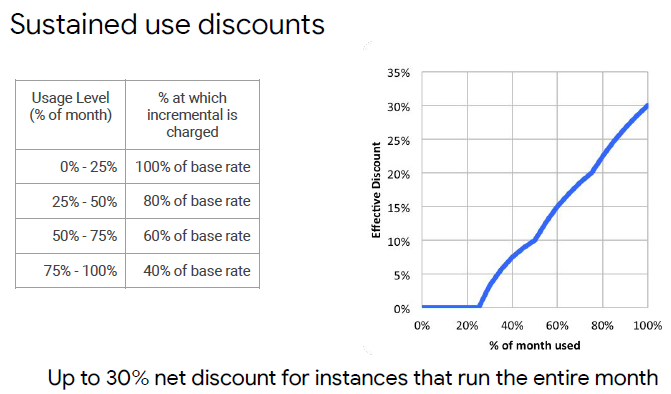
Custom machines have a slider to change the memory and vCPUs



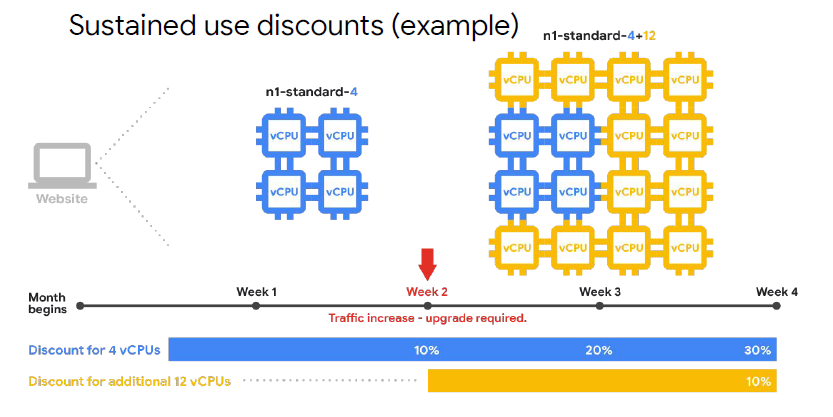


Compute Pricing

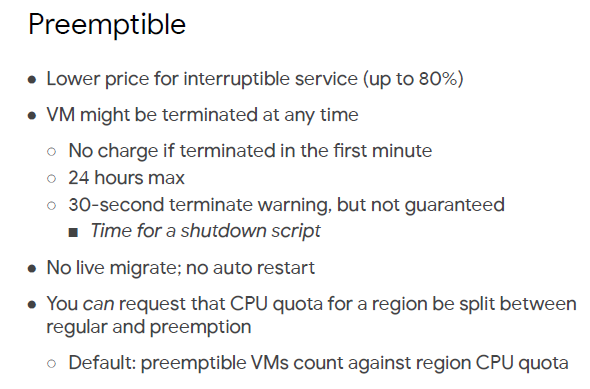




^ Counted from the 1st day of the month



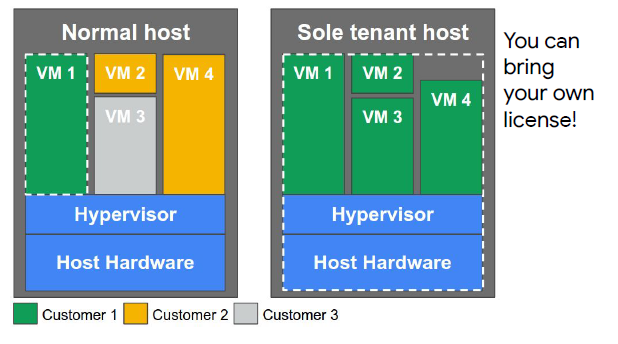
Special compute configurations



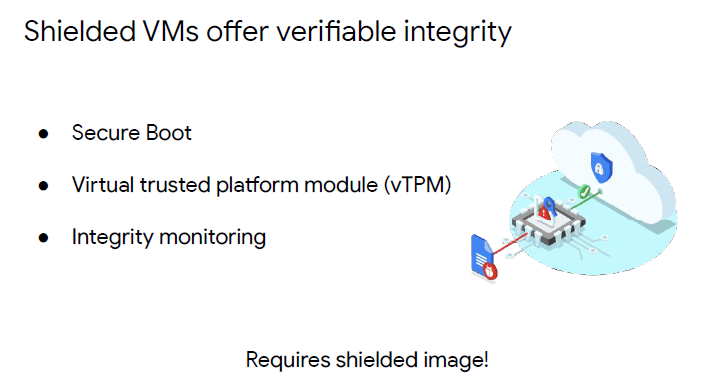
^ Used for non-production, short lived jobs, such as batch processing

Sole-Tenant Node

* Physically isolated from other workloads and VMs
* Physical compute engine server that is dedicated to host instances for your project along
* Useful if you have compliance requirements



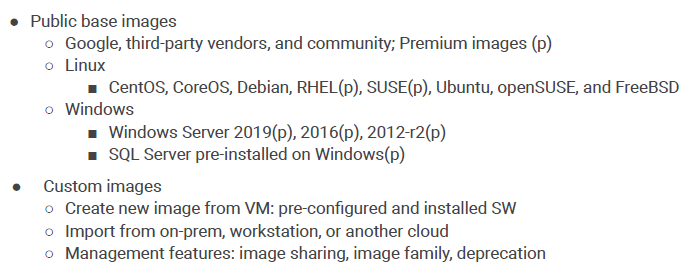
^ accommodates VM instances up to 96 vCPUs and 624gb of memory (can be a combination of smaller VMs as long as combined they don’t exceed these values)

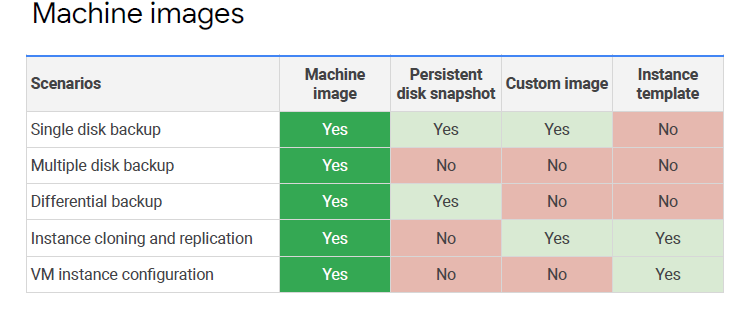


^ confident that instances not compromised but boot or kernel level malware or rootkits

Images

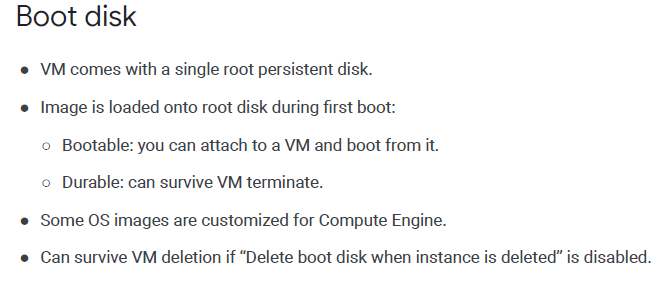
Image includes:

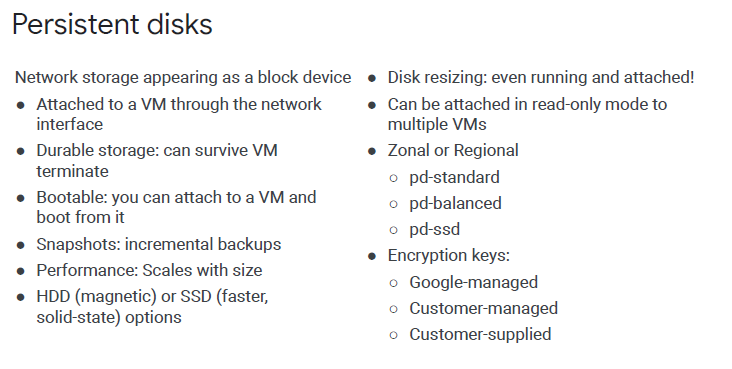
* Boot loader
* OS
* Fil system structure
* Software
* Customisations
* Either Linux or Windows
* Can be public or custom (premium public images have a charged associated to using them)

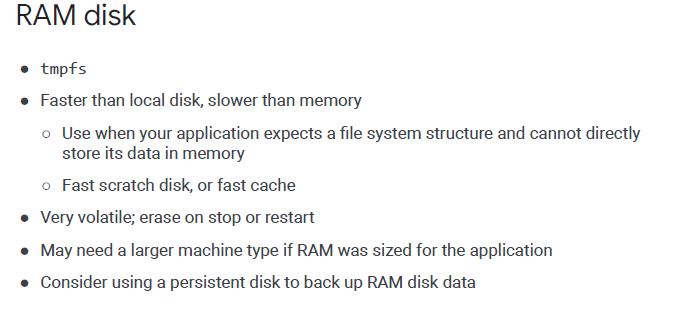
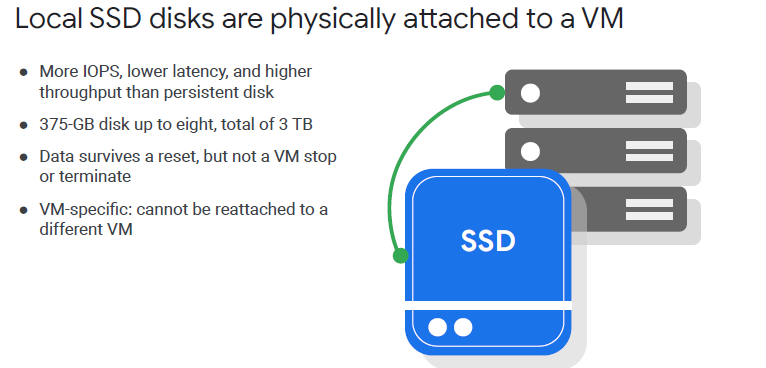


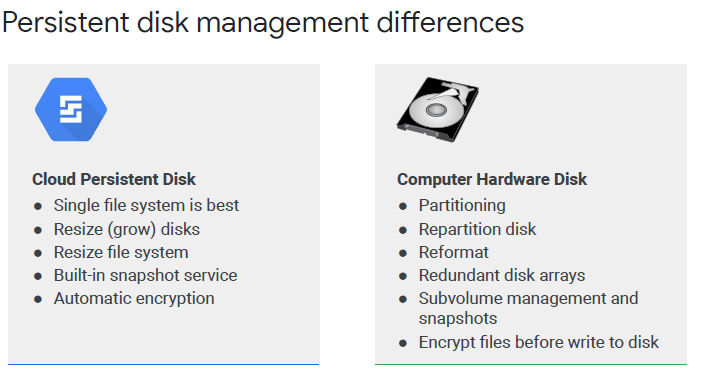
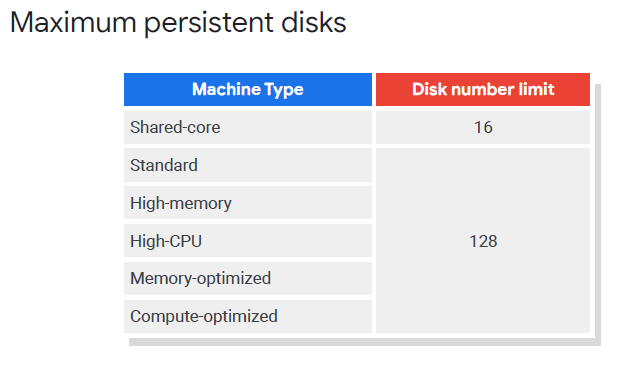
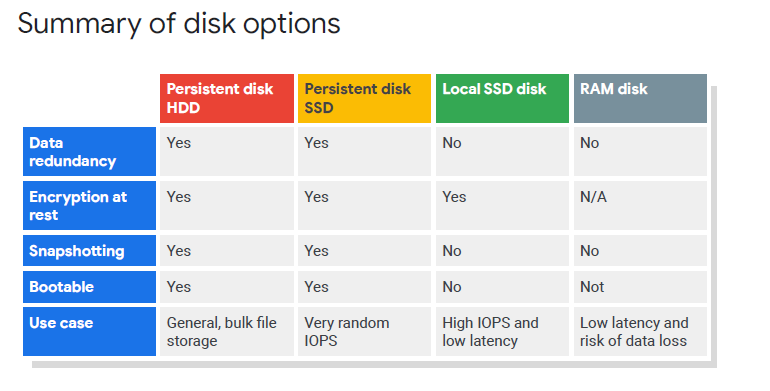
^ Machine image most ideal for disk backups and instance cloning/replication

Disk Options





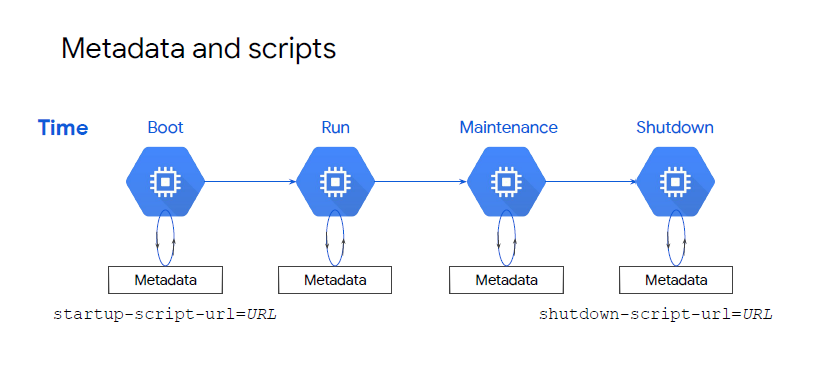




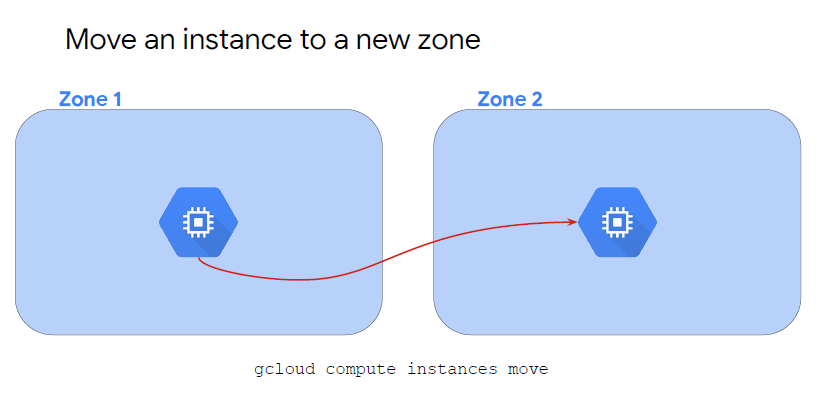
Common compute Engine Actions

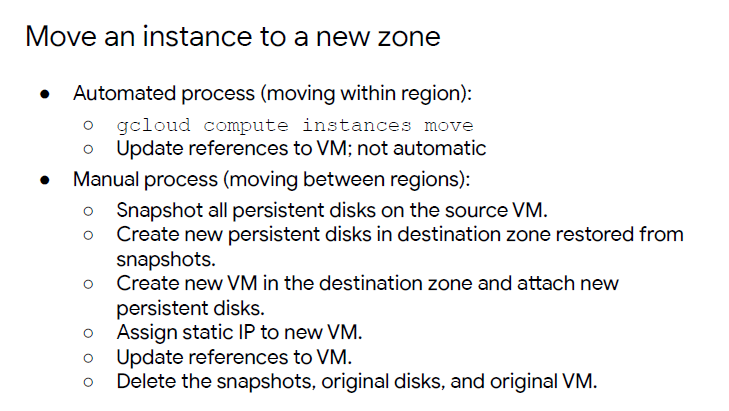
Metadata and scripts

* Every VM instance stores its metadata on a metadata server
* Useful in combination with start-up and shutdown scripts as can use the metadata to get info about the instances without additional authorization
* Start-up and shutdown scripts recommend to store in Cloud Storage



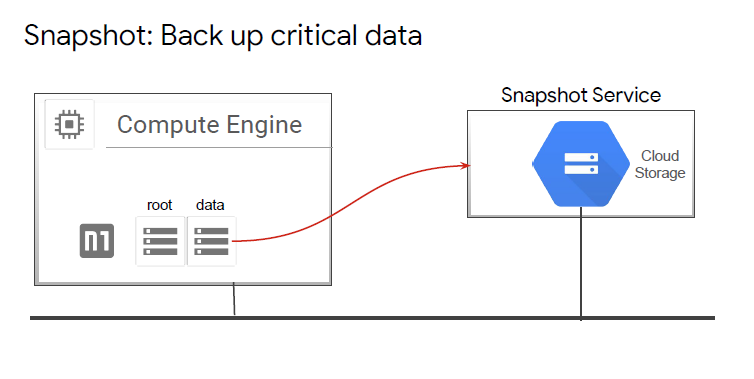
Move an instance to a new zone

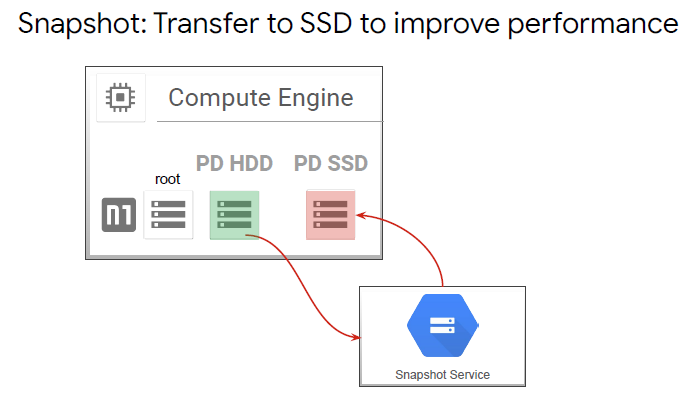
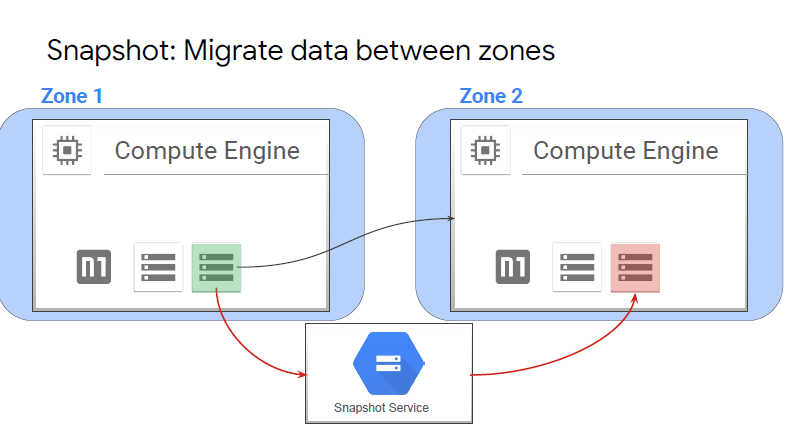


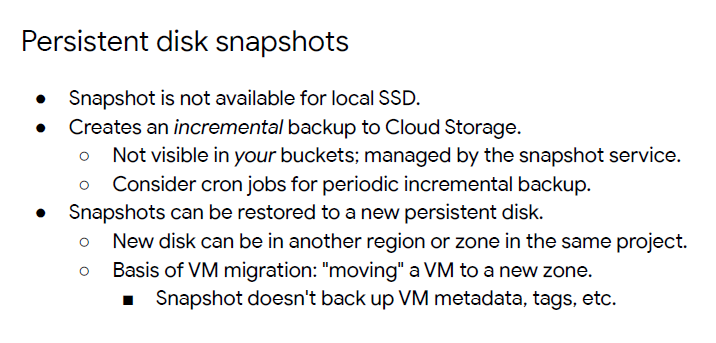


Snapshots

* Stored in cloud storage

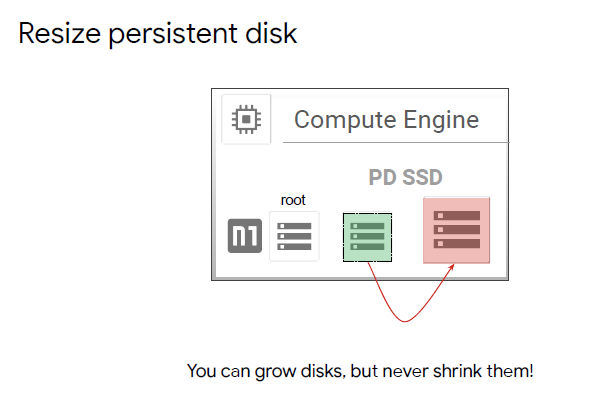






^ cannot snapshot a local SSD

* Useful of periodic backup or data
* Incremental and auto compressed – create regular snapshots faster and lower cost compared to creating an image

Resize persistent disk

^ can be done while the disk is running without having to create a snapshot