ORACLE
Cloud Infrastructure

OCI-Classic to OCI IaaS Migration
Migration Concepts
Level 300

Sanjay Narvekar

April 2019

ORACLE

OCI-Classic to OCI Migration - Objectives

After completing this lesson, you should be able to:

- Describe the benefits of moving from OCI-Classic to OCI
- Have an understanding of the requirements, migration strategy and tools for migrating infrastructure from OCI-Classic to OCI

Deploying workloads in OCI instead of OCIC

Differentiated capabilities for enterprise applications and databases

- Predictable storage and network performance
  - Consistent IOPS and throughput for block storage regardless of volume size
  - Non-oversubscribed, non-blocking network
  - Storage and networking performance SLAs
- Better than customers' existing hardware
  - Bare metal and VM compute (latest CPU and GPU)
  - Lowest cost, highest core density compute
  - Highest speed local, block, and file storage (NVMe)
- Stronger foundation for HA/DR deployments
  - Support for Availability and Fault Domains
- Strong and broad SLAs for performance, availability, manageability
- Improved Governance and Security
  - Fine grained logical and network isolation
  - API auditing
- Direct access and common console for advanced services
  - Autonomous Transaction Processing
  - Autonomous Data Warehouse
- Edge Services
  - DNS, Web Application Firewall, Email, DDoS Protection
- ~25% less cost per OCPU-hour moving to equivalent Linux OCI shapes from OCIC
- Container Service, Streaming, Monitoring, Resource Manager, other OCI services

General Considerations for migration

Considerations for migrating your workloads to OCI

- General (Customer technical expertise, Timing and downtime expectations, Business constraints)
- Environment Information (Development, Test or Production)
- Financial Account Information - Current subscription type : Non-metered, Metered (traditional), Government/Public Sector, Universal credits
- Data Region Location (Current data region/data center, Availability of OCI data center)
- Services used (IaaS only, IaaS and PaaS, Lift and shift applications – Apps Unlimited/Fusion Middleware)

Network and Database Considerations for migration

Network considerations for migrating your workloads to OCI

- General network requirements
- Network security
- OCI Classic to OCI Network connection
- On-Premise to Oracle Cloud connection (FastConnect Classic, VPN (Corente) and VPN as a Service (VPNaaS))

Database considerations for migrating your database workloads to OCI

- General (number of databases to migrate, purpose of each database, application dependencies and average size of each database
- Oracle databases (type of database deployment, version and edition of each database)
- Third-party Databases (Brand, version and edition of each third-party database)
- Migration method
- Identify suitable targets for Oracle databases on OCI – IaaS, VM, BM, ATP, ADW and ExaCS

Virtual Machine Considerations for migration

Considerations for migrating your virtual machine workloads to OCI

- How is access to the instance secured? e.g. ssh for Linux, Remote Desktop for Windows
- Is there a bastion host?
- How is the system patched? Is there a way to audit the fleet of VMs for patches?
- Is malware/anti-virus installed?
- How are system level logs captured?
- Is the image hardened?
- What monitoring of the system is in place?
- Is there a firewall running on this instance?
- Does the system sync time using NTP?
- How are the attached disks backed up?
- Are fault domains being leveraged?
- Any 3rd party licensing requirements?

Block Storage and Custom Image Considerations for migration

Considerations for migrating your block storage volumes from OCI-C to OCI

- Verify performance (IOPS, latency, throughput) is reasonable for your workload
- Verify block volume backup plan
- When using iSCSI, enable CHAP authentication (for security purpose)

Considerations for migrating your custom images from OCI-C to OCI

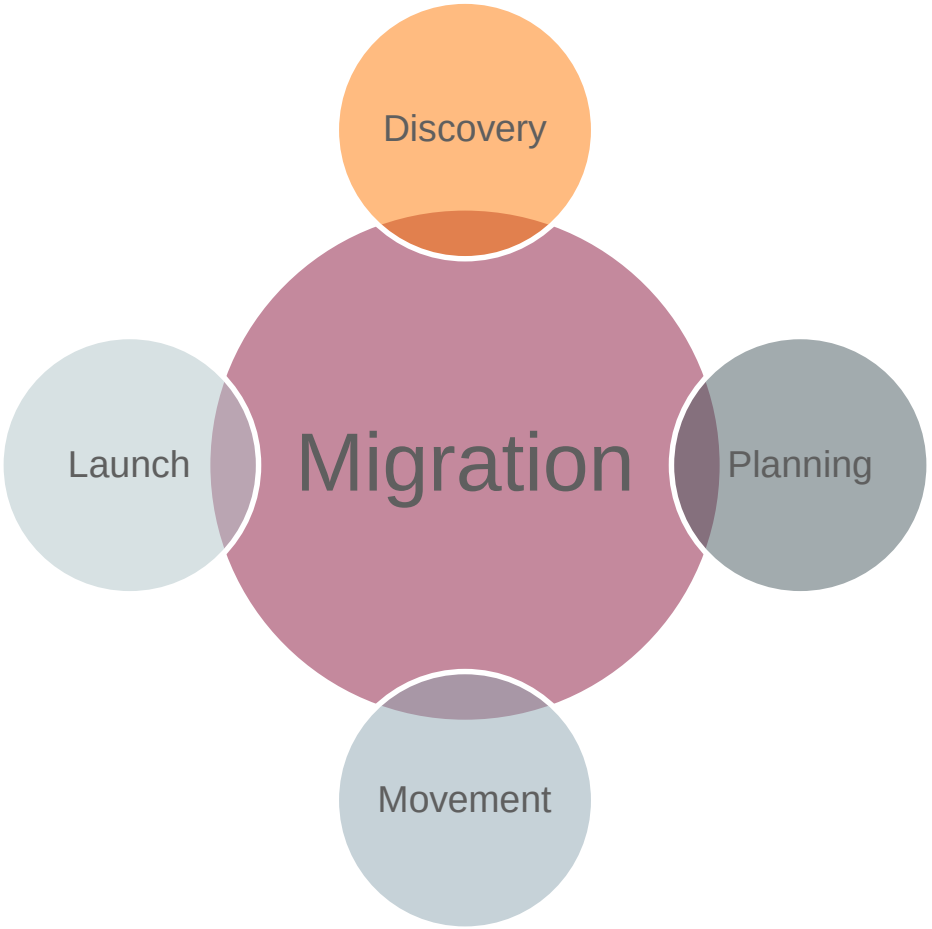
- Be aware of limitations (size, reserved IP addresses, Windows export..) of the custom image
- Since images can be shared across regions, upload images only as needed for startup time

Application-Level Disaster Recovery Considerations for migration

Application-level disaster recovery considerations for OCI-C to OCI migration:

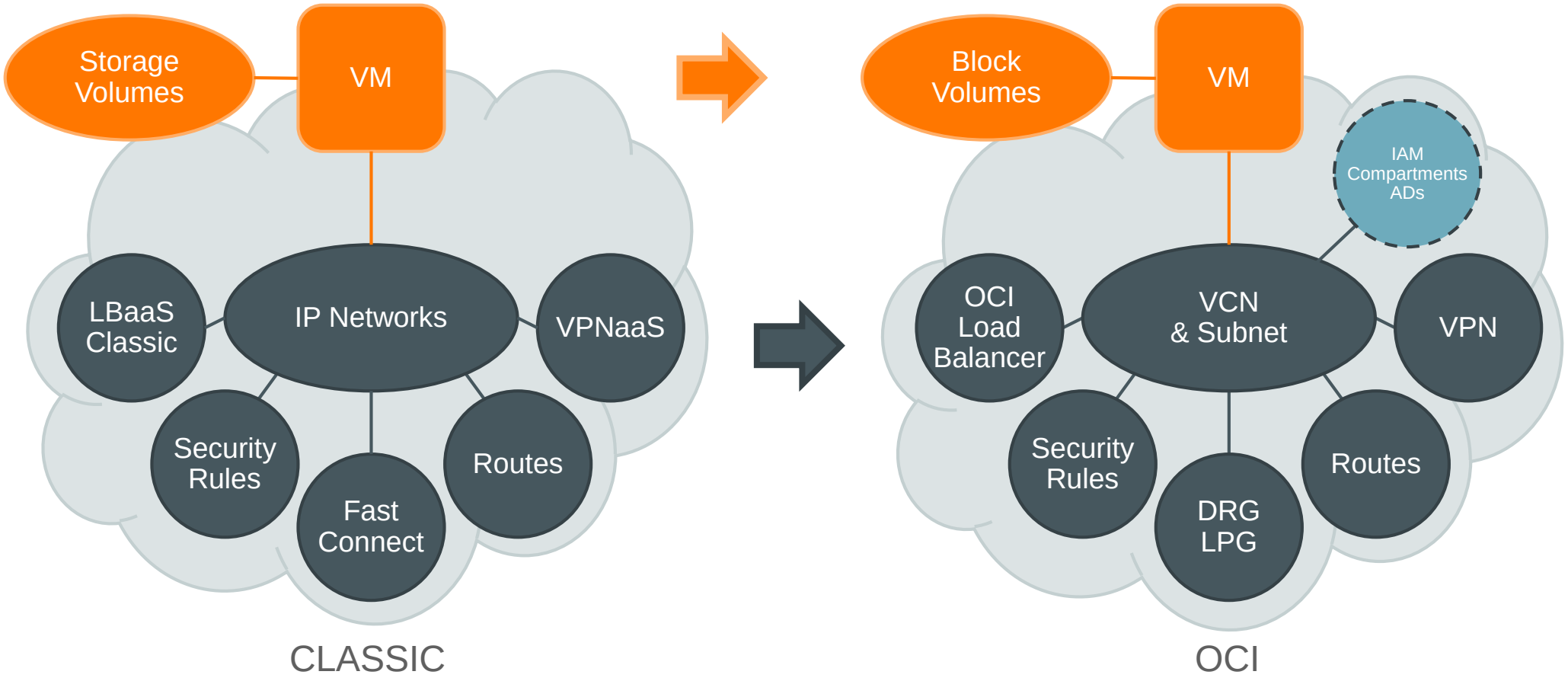
- Is the application accessed via a DNS FQDN or by IP address directly?
- Will failover between prod and DR be accomplished by making DNS changes?
- Are there any other IP requirements between DR, prod and any other environments or are these largely undefined/nonexistent (such as using the same IP addressing for both prod and DR, etc.)?
- Compile a list of all applications that will be running in OCI environment. Specify where each application currently resides (on-premises, OCIC, other cloud, etc.).

OCI Classic to OCI Migration Process



- **Discovery** of the Classic resources and service to be migrated (instances, storage volumes, networks, security rules, …)
- **Mapping** network and security definitions from Compute Classic to OCI Compute
- **Movement** of Compute instances and data volumes from Compute Classic to OCI Compute
- **Generation** of Terraform to create target VCN and launch migrated instances

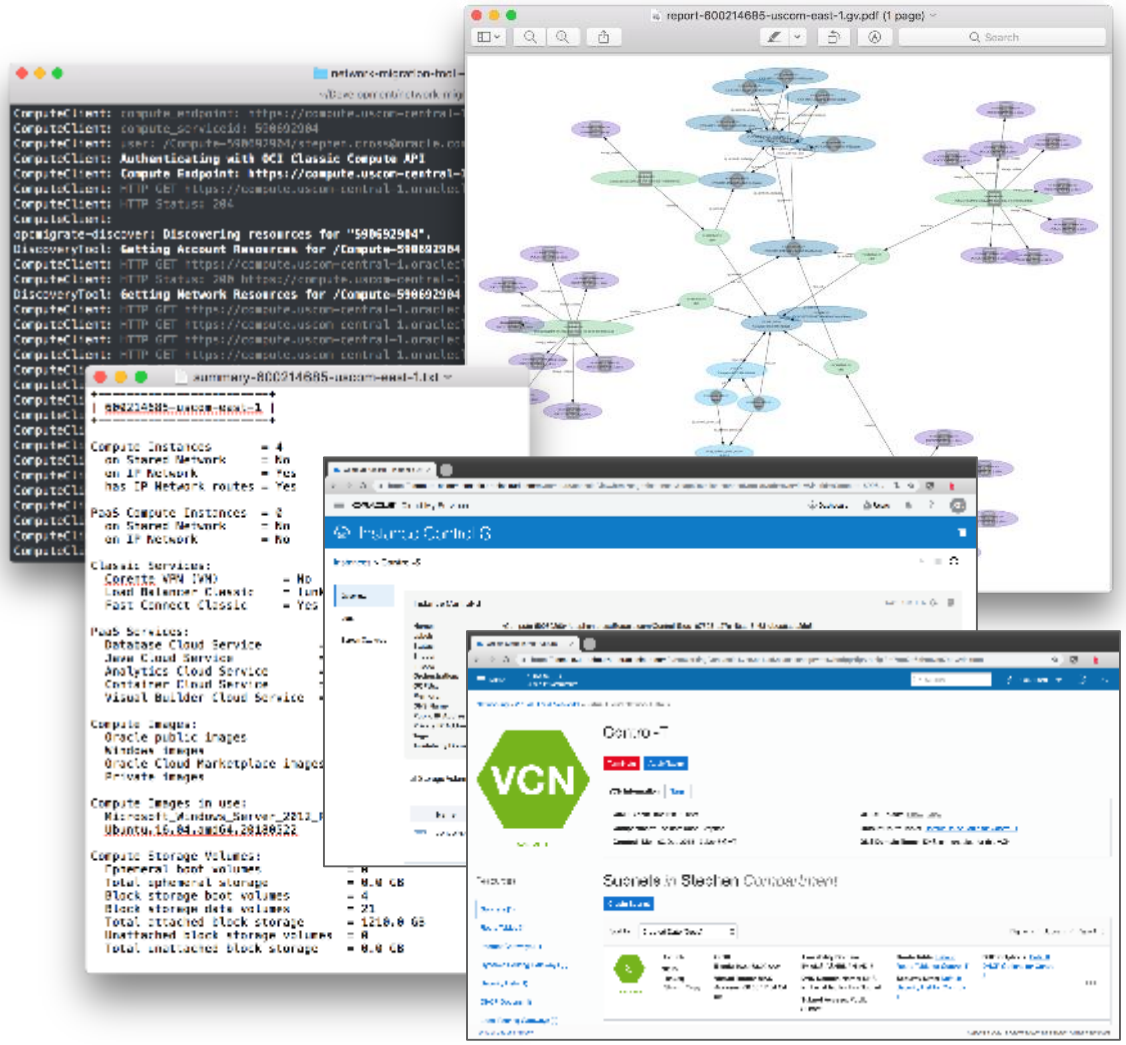
OCI Classic to OCI Migration



Migration Tools

Discovery and Translation Tool

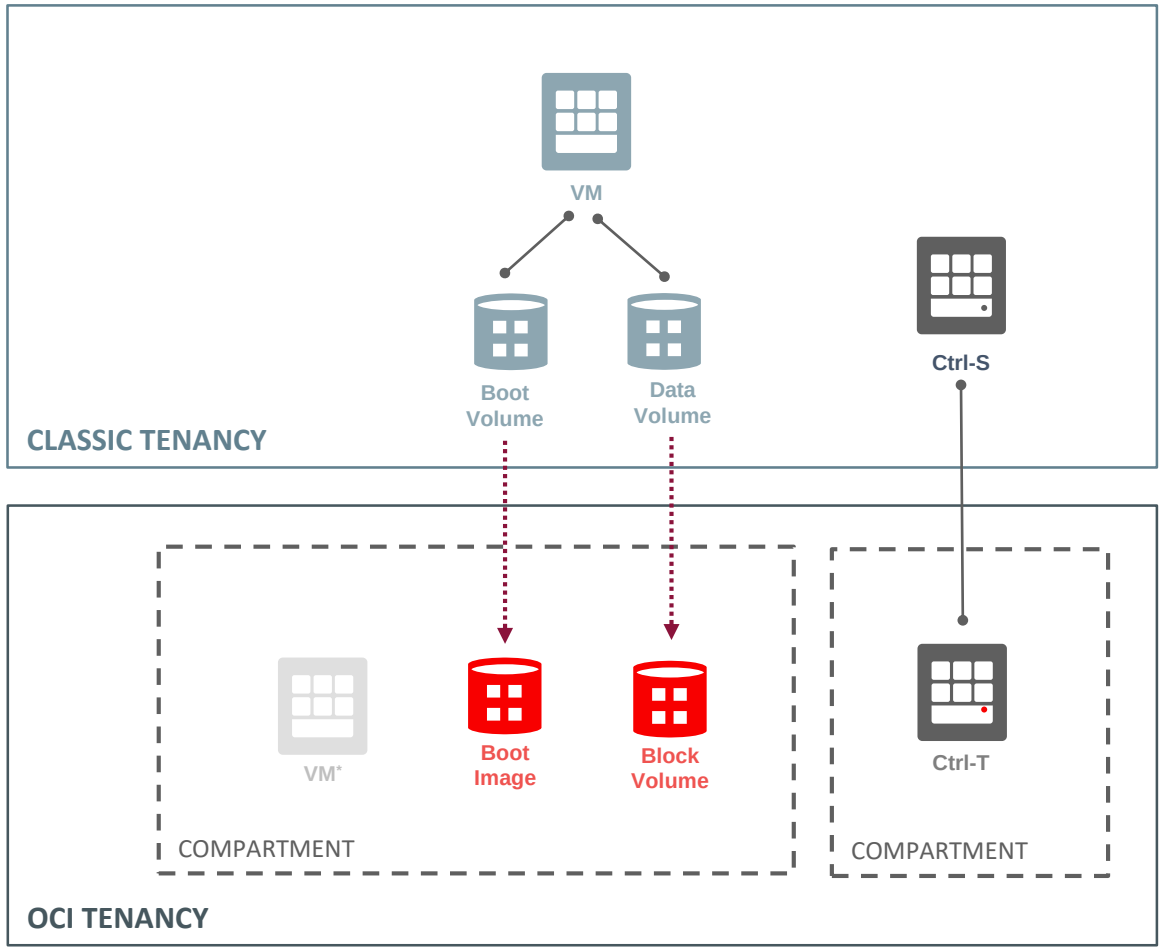
- OCI Classic resource and service **Discovery**
- Analysis and **Reporting** of source environment details
- **Mapping** of Compute Classic Network configuration and Security Rules to OCI VCN
- **Export** of Compute Classic Instance and Storage Volumes details for migration
- Generation of **Terraform** scripts for VCN creation and launching migrated instances



Migration Tools

VM and Block Volume Migration

- Copies VM boot and attached storage volumes from Classic to OCI
- Boot volumes converted to OCI Custom images to launch new instance from
- Storage Volume converted to OCI Block Volumes
- Migration jobs managed by the migration control servers Ctrl-S (source) and Ctrl-T target
- Migrated instances can either be manually launched from the UI, or created using the generated Terraform

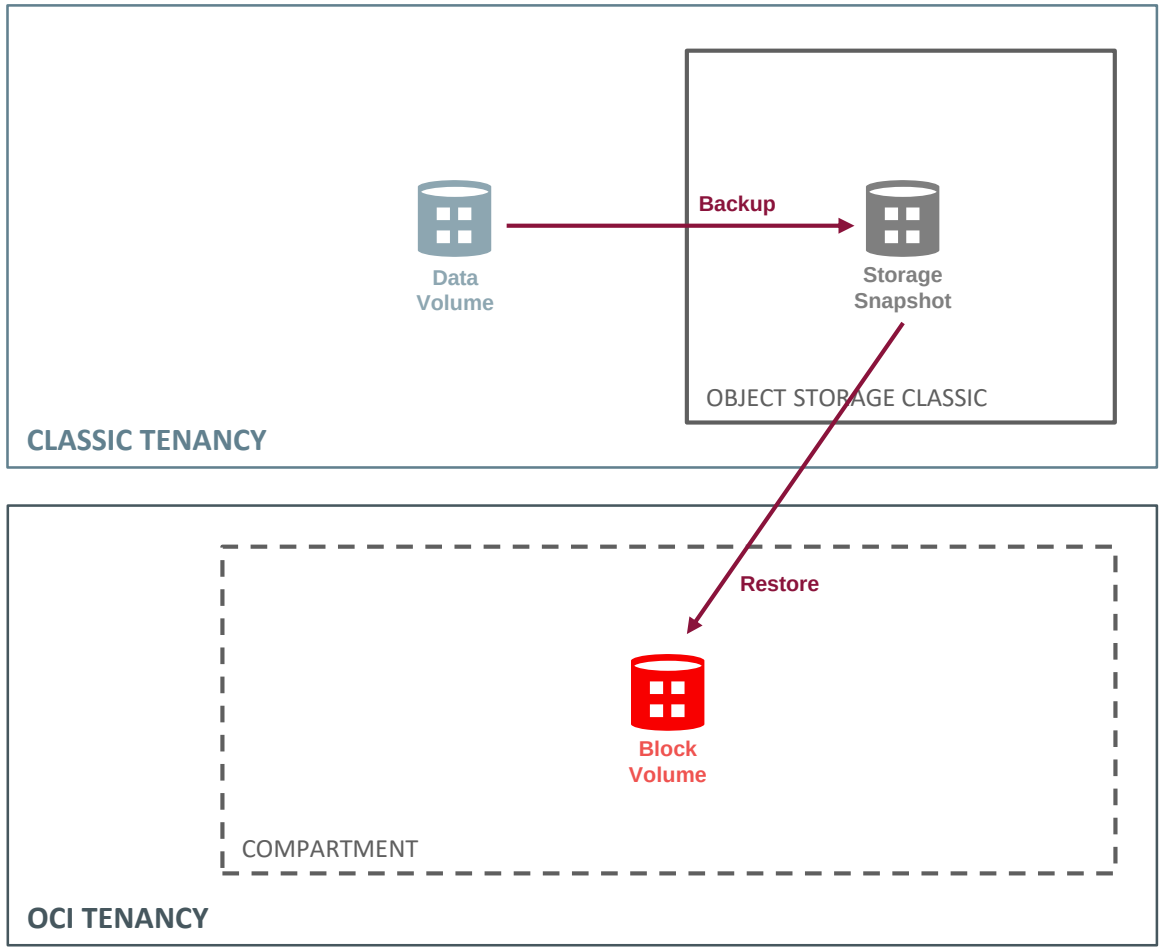


*VM must be manually launched via the UI or using Terraform

Migration Tools

Block Volume Backup and Restore

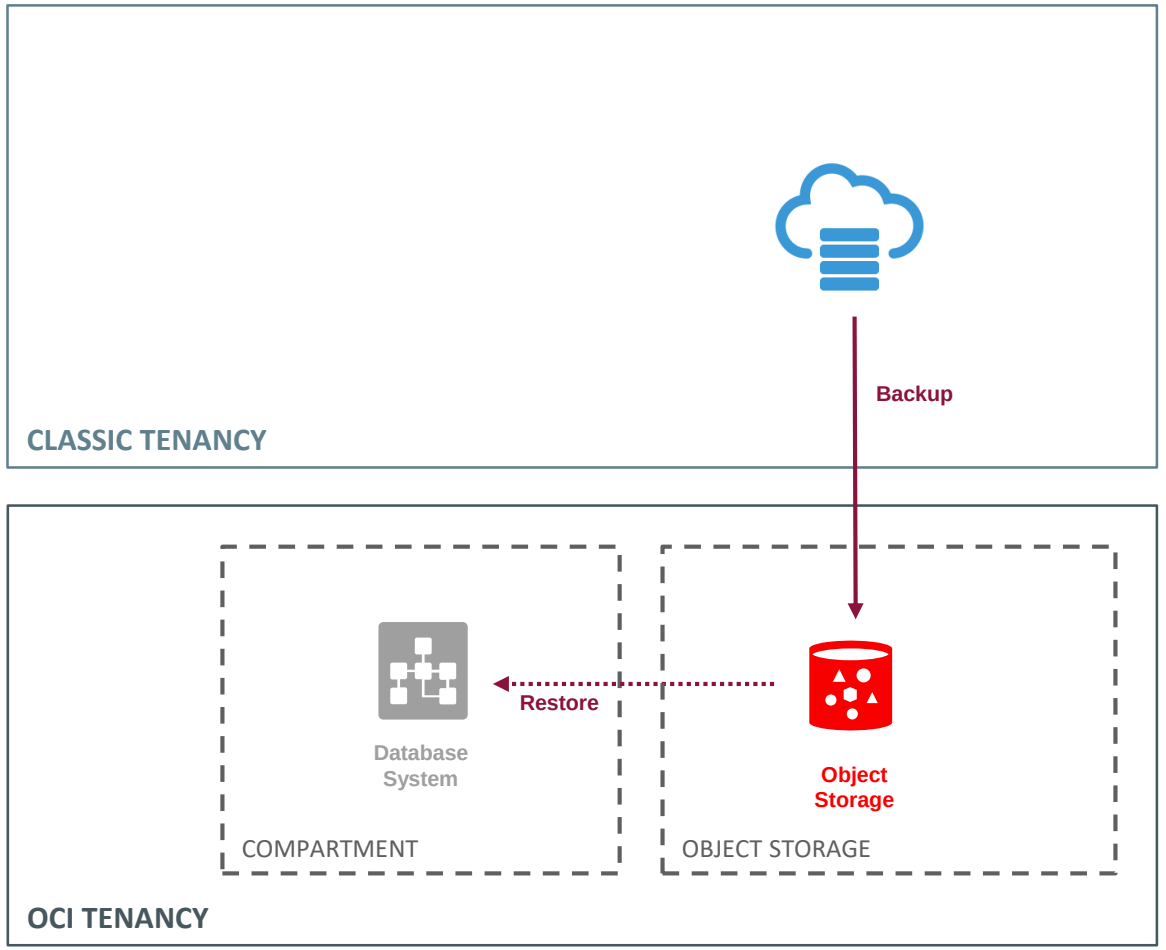
- Restore an OCI-C volume's (remote) backup to an OCI volume.
- Attach the volume to an OCI VM, or convert to an OCI backup.
- Automatic volume creation in the chosen availability domain. Restoring backups to different availability domains can be done concurrently.
- Asynchronous operation with the ability to monitor job progress.
- Backup conversion takes place in an OCI compartment that is isolated from the customer's workload.



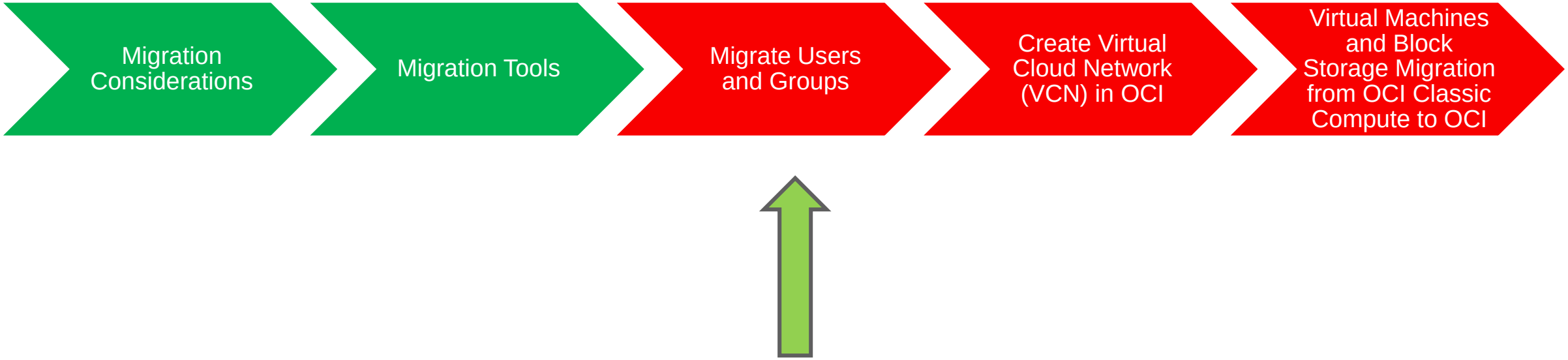
Migration Tools

Database Backup Migration Tool

- Migrate OCI Classic DBCS instances (both single node and RAC) to OCI.
- Creates a Recovery Manager (RMAN) backup of OCI classic DBaaS instance , and automatically transfers the backup to Oracle Cloud Infrastructure Object Storage as a standalone backup
- This is primarily to be used for development or test DBCS instances as migration down time is needed



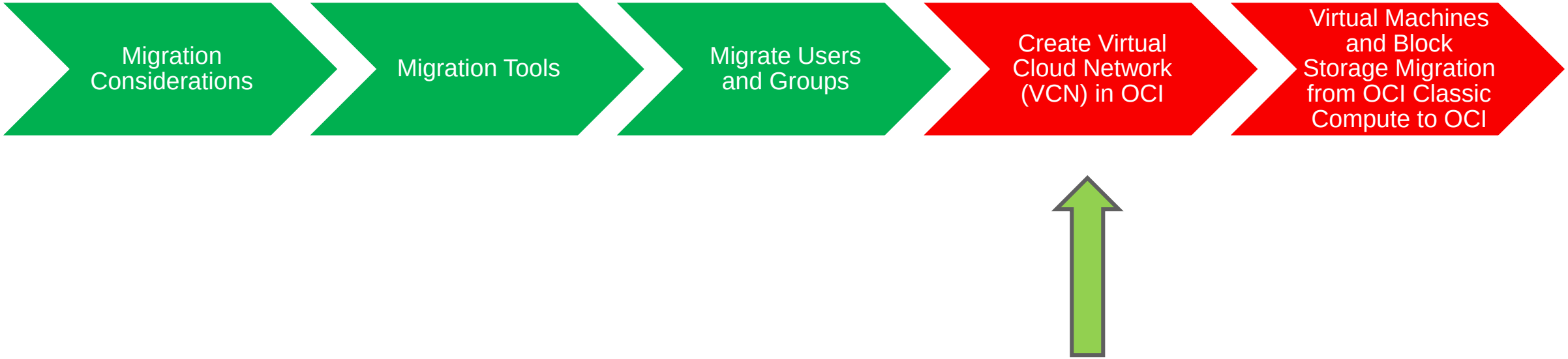
*Database is manually launched from backup via the UI or using Terraform



Migrate Users and Groups

Checklist for migrating users and groups

- Verify that Your OCI account is Federated with IDCS
- Run reports to list OCI Classic Users, Groups, and Assigned Privileges in IDCS
- Create IDCS Groups for each required Role
- Create a new OCI Group for your Compute Administrators
- Map the IDCS Group to the OCI Group
- Create a Policy to grant the Group Permissions on OCI Resources



Design the Virtual cloud network (VCN) in OCI

Before you can migrate from an OCI-C environment to an OCI environment, you must consider the network architecture. You typically use the following steps to create a Virtual cloud network (VCN):

1. Create one or more VCNs
2. Create an Internet Gateway and/or NAT Gateway
3. (optional) Configure Service Gateway (e.g. for Object Storage access)
4. Create one or more Subnets in each VCN
5. (optional) Configure local peering gateways between VCNs if required
6. Configure each Subnets Security List and Route Table

You can use the terraform file output by the opcmigrate tool for creating the VCN in OCI or you can also manually create the VCN.

Considerations for Migrating Your Network

- When you migrate your network, some network configuration might change.
- In OCI-C Compute, security rules are applied to groups of vNICs called vNICsets.
- However, in OCI, there is no equivalent grouping and security rules are applied to an entire subnet.
- Prioritizing the network topology means that your IP networks are mapped to separate VCNs and subnets, so you can easily identify your networks and manage your IP address ranges.
- Prioritizing the security context means that the same set of security rules is applied to each interface, but with this strategy there is no clear mapping between IP networks and VCNs or subnets.

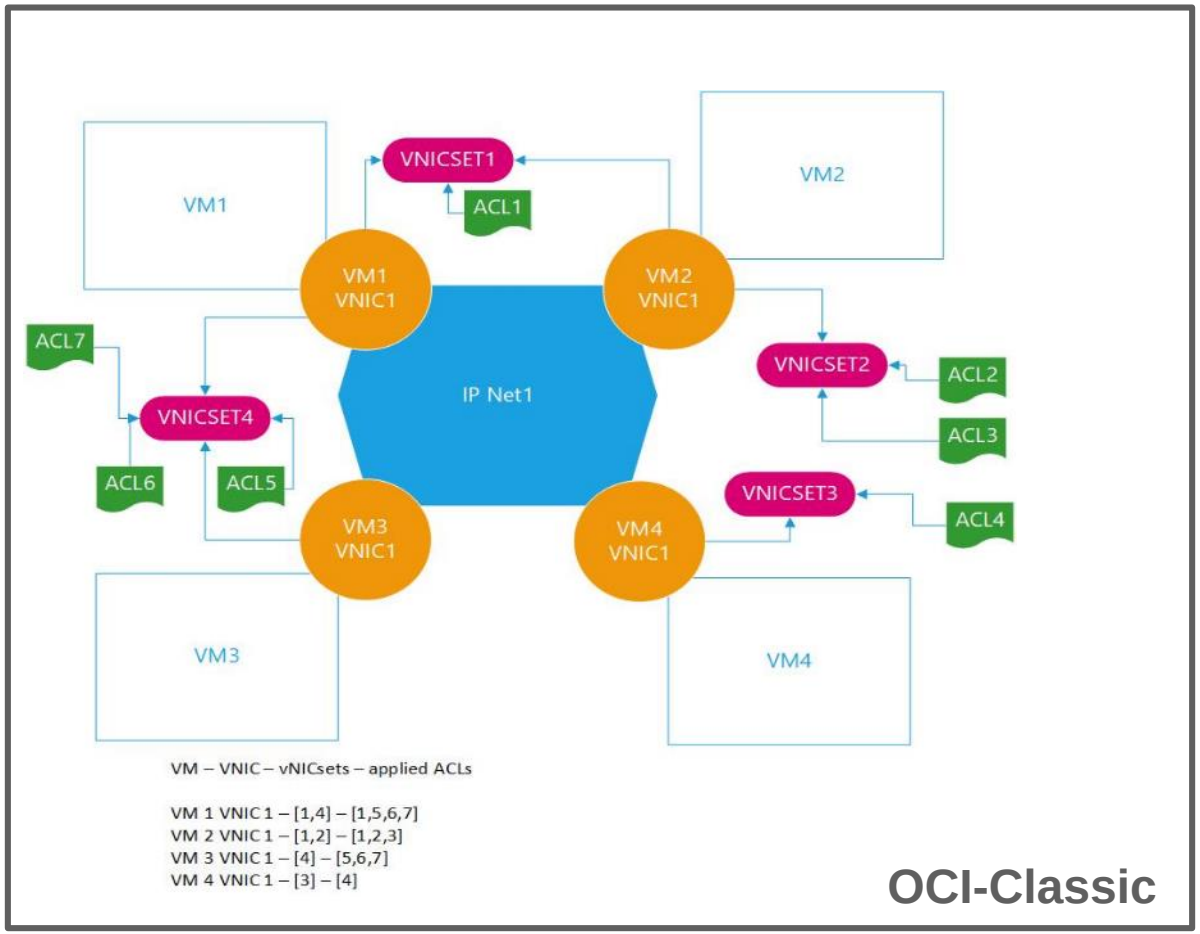
Considerations for Migrating Your Network

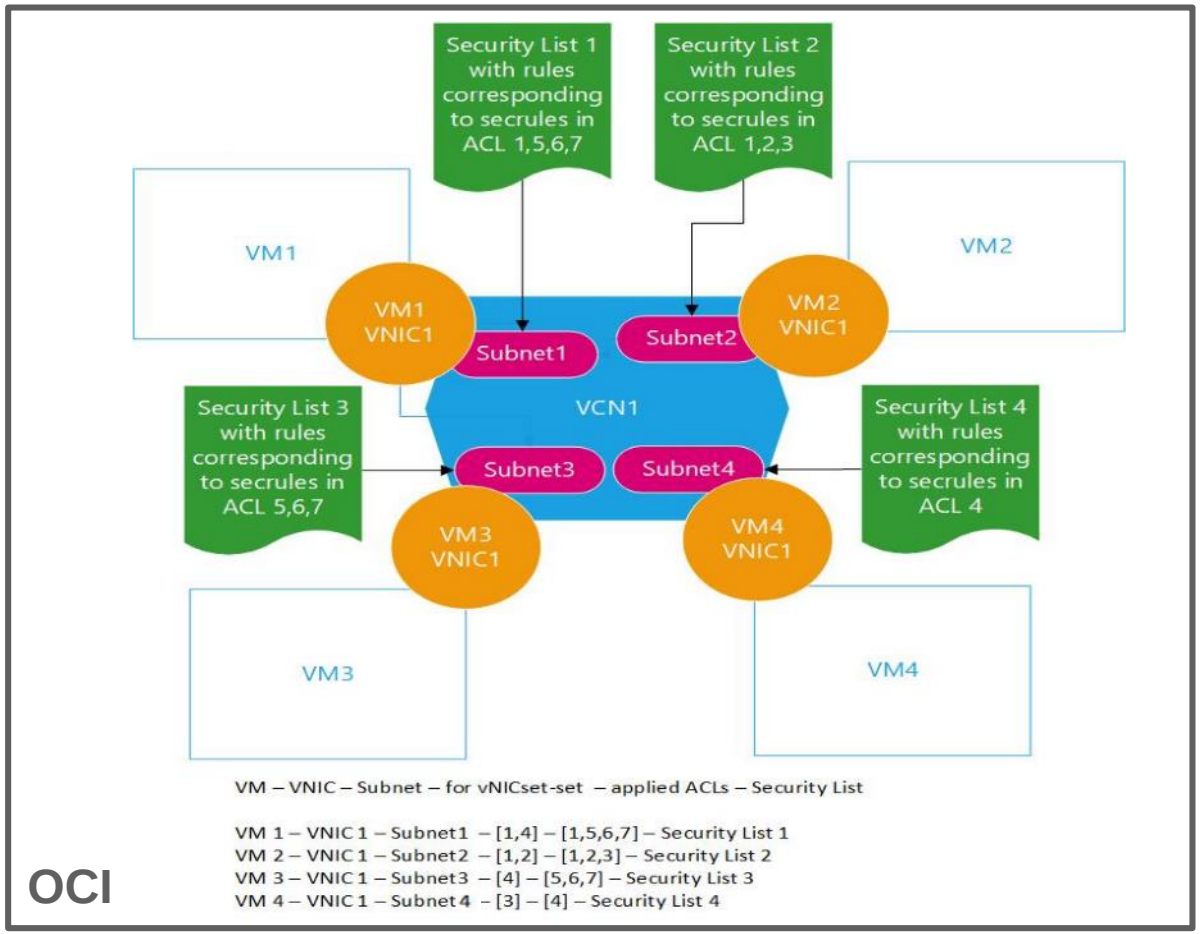
Security context mapping	Network topology mapping
This strategy maintains the security model. It allows you to apply the same set of security rules to each vNIC in OCI as you had done in OCI-C Compute	This strategy allows you to keep your network topology unchanged
Depending on the source network topology, it can be quite a complex task to map the vNICs from vNICsets to subnets and it can result in a large number of subnets being created, with a large number of security lists	Aggregated security rules applied to a subnet could expose some interfaces to traffic that it was previously not exposed to, as some ports might be opened that were previously blocked
Some parts of the procedure could require manual steps using the OCI Console	Implementing this network migration is simpler and can be automated with Terraform
While you might have assigned static private IP addresses to instances on IP networks in the source environment, some of these private IP addresses might change during migration	Each IP network maps to a separate VCN or to a separate subnet in a VCN. This allows you to assign the same private IP address to each interface as you had in the source environment

Considerations for Migrating Your Network

Security Context Mapping

The following diagram shows an example of migrating a single IP network to OCI such that the same set of security rules are applied to each network interfaces

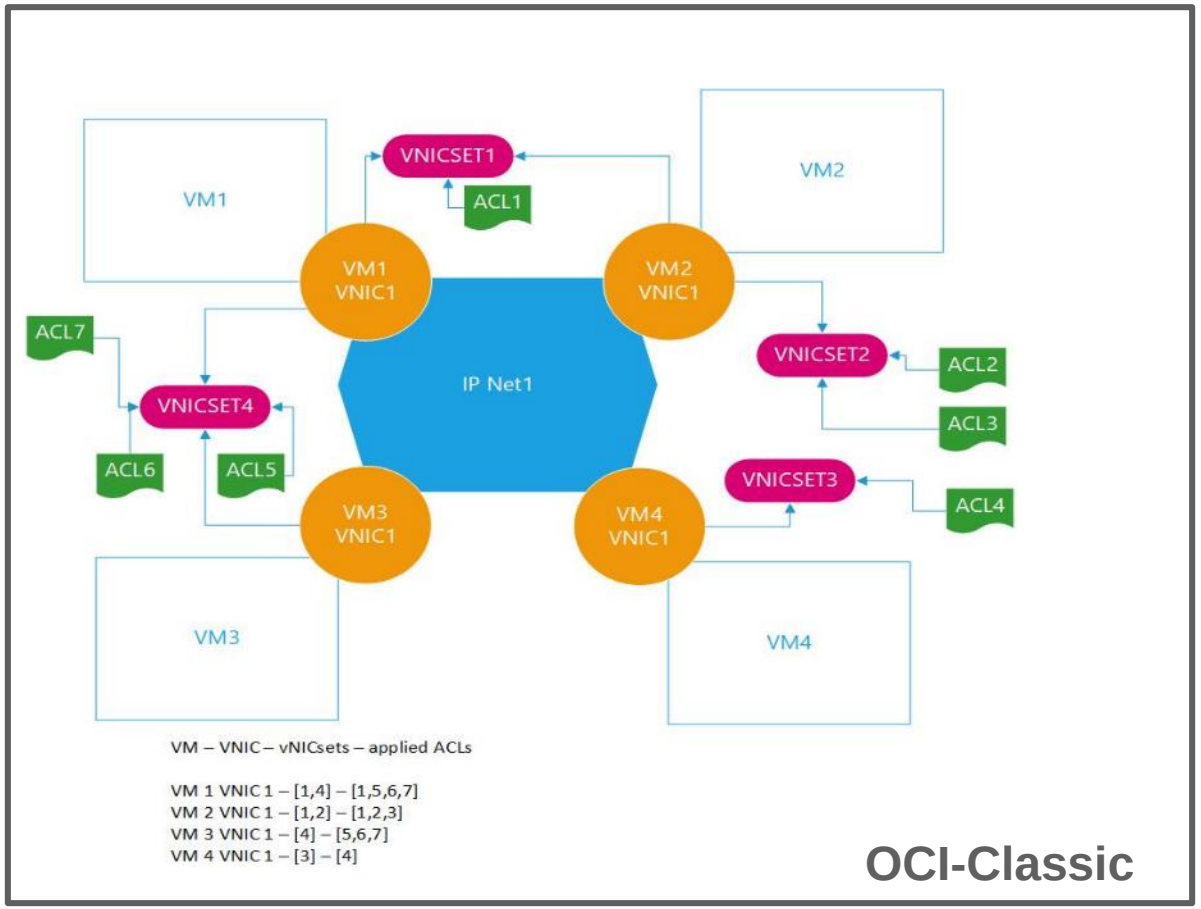


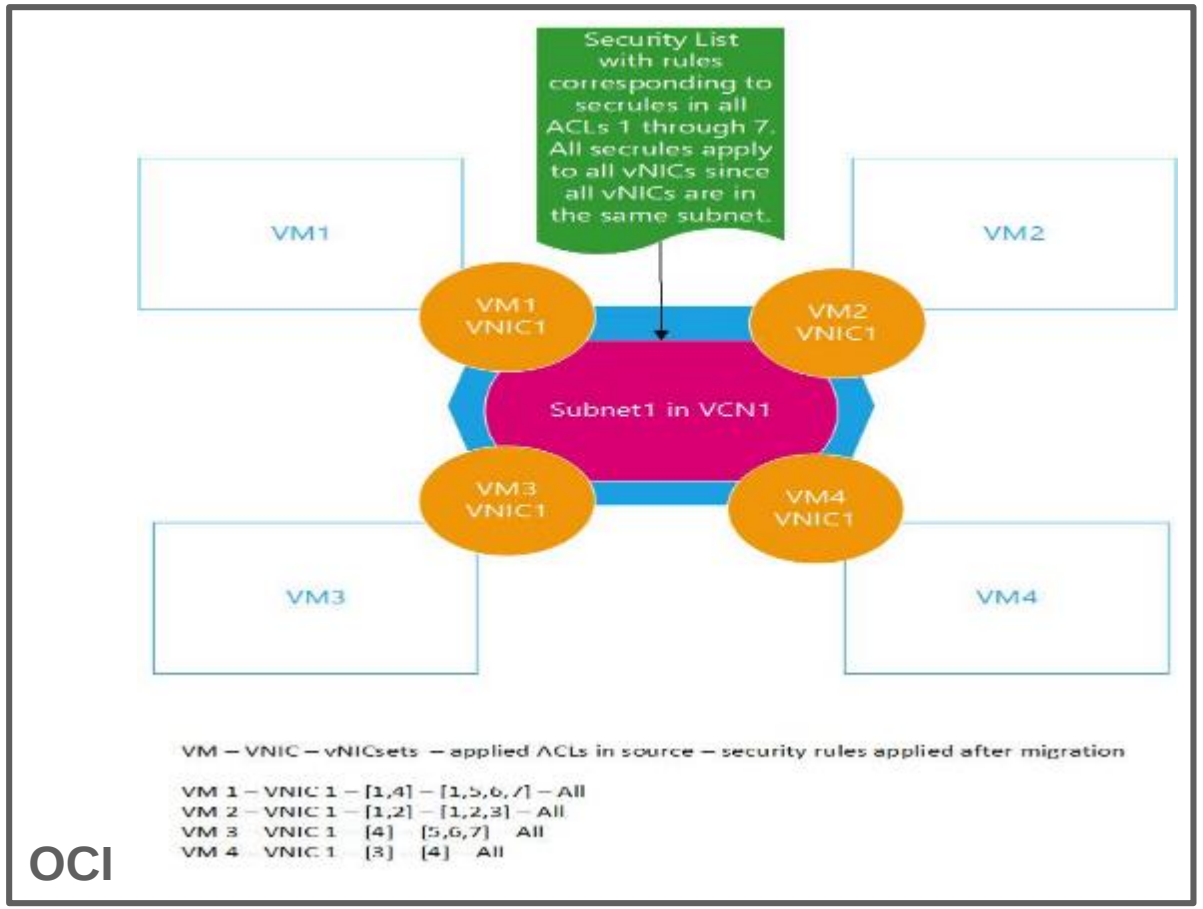


Considerations for Migrating Your Network

Network Topology Mapping

The following diagram shows an example of a network in OCI-C and how it can be migrated to OCI such that the network topology is similar





Considerations for Migrating Your Network

Network Topology Mapping

Considerations for Connecting VCNs Using Local Peering Gateways

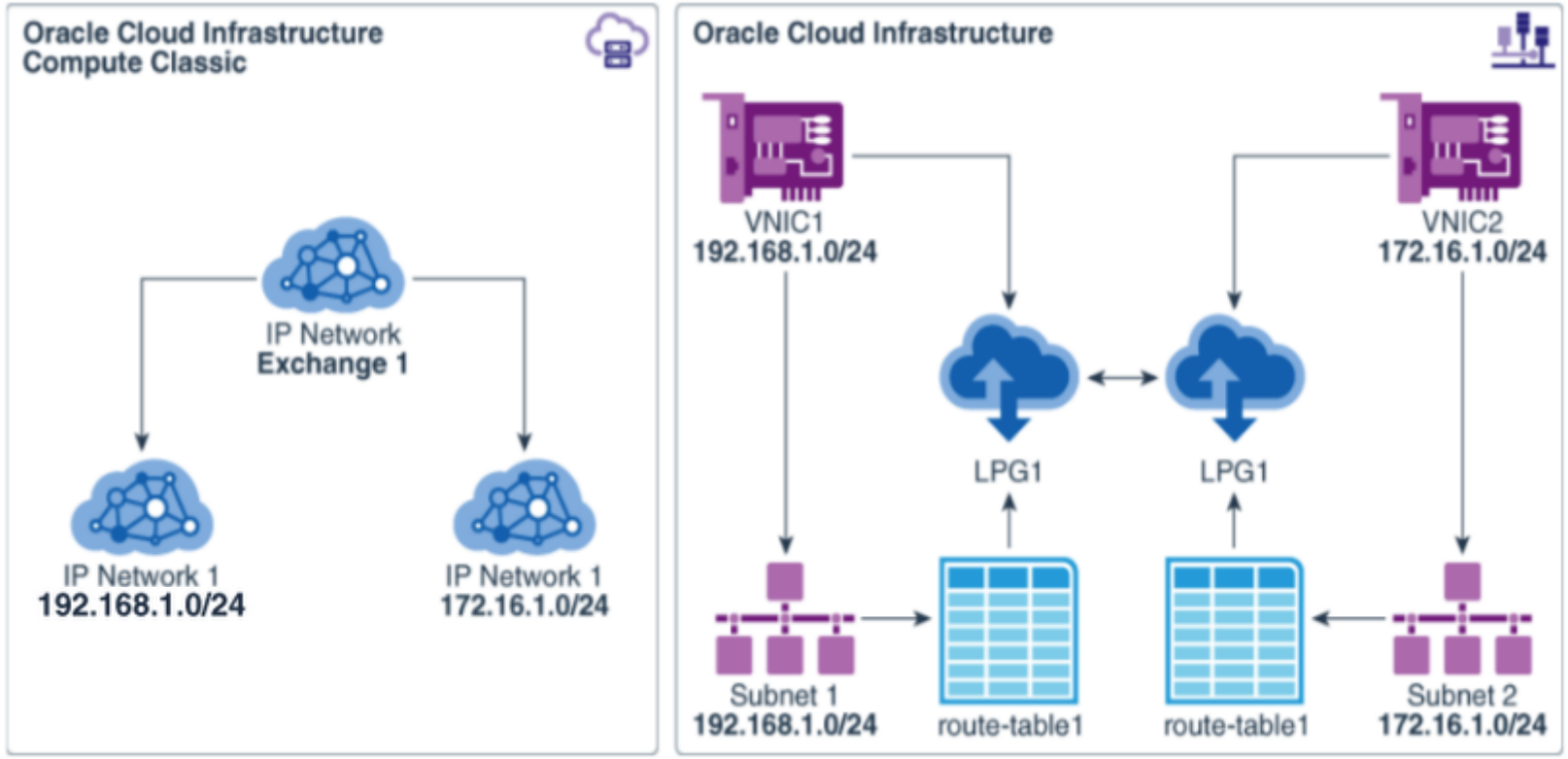
Before setting up VCN peering, consider the following:

- While VCN peering is an effective way to allow traffic across VCNs, a better solution is to restructure your IP networks whenever possible, so that they can be migrated as subnets in a single VCN with a /16 CIDR block. One of the limitations of VCN peering is that local host name resolution for hosts outside the subnet won't work.
- If you use the security context mapping strategy, given that private IP addresses might change anyway, consider restructuring your network such that vNICs that need to communicate with each other are created in the same VCN or subnet. With this approach, you generally won't need to implement VCN peering.
- If you use the network topology mapping strategy, and you want each of your IP networks to be migrated as a separate VCN, then you might need to adopt VCN peering to provide connectivity across those VCNs.

Considerations for Migrating Your Network

Network Topology Mapping

The following figure shows how VCN peering in Oracle Cloud Infrastructure allows you to replicate the connectivity provided by IP network exchanges in Oracle Cloud Infrastructure Compute Classic



Connect OCI-C and OCI Networks (Optional step)

Option 1: Connection over the Oracle network

In regions where this is supported it allows for much faster data transfer because the interconnect is across the shared fast connect routers at 40g.

- The two environments must be in the same geographical area (Ashburn or London), and the connection is available only between these specific regions:
  - Between OCI us-ashburn-1 region and OCI-Classic uscom-east-1 region
  - Between OCI uk-london-1 region and OCI-Classic gbcom-south-1 region
- The two environments must belong to the same company. Oracle validates this when setting up the connection.

Option 2: Connection over an IPSec VPN

- You set up an IPSec VPN between the IP network's VPN as a Service (VPNaaS) gateway and the VCN's attached DRG. The connection runs over the internet.
- The two environments do not have to be in the same geographical area or regions.
- The two environments do not have to belong to the same company.

Connect On-premises Network to OCI Network (Optional step)

Oracle Cloud Infrastructure provides both IPSec VPN and FastConnect options for connecting a customer's data center to the Oracle Cloud network.

- Use of an IPSec VPN site-to-site tunnel will allow customers to use the public internet for communication. Traffic between the customer’s data center to the Oracle Cloud network will be encrypted, significantly lowering the chances of information theft.
- FastConnect provides an easy way to create a dedicated, private connection between a customer’s data center and Oracle Cloud Infrastructure. FastConnect provides higher-bandwidth options, and a more reliable and consistent networking experience compared to internet-based connections.

Migrate Virtual Machines and Block Storage to OCI

Considerations for Migration

Before you start your migration, consider the following factors that could have an impact on your migration process: proof-of-concept, boot volume size, etc.

Required services and roles

This solution requires the following services and roles:

- Oracle Cloud Infrastructure Compute Classic: You'll need the Compute_Operations role to create the migration controller instance and to create snapshots of the boot and block volumes.
- Oracle Cloud Infrastructure: Ensure that you have policies in place that allow you to read the required OCIDs from the Web Console. You'll also need to create an API user, who must belong to a group that has policies in place to create the required resources.

Migrate Virtual Machines and Block Storage to OCI

Plan for the migration

Before you start the migration, you should:

- Collect information about the source instances that you want to migrate.
- Generate and have available required SSH and PEM keys to access the source and target environments.
- Configure the source environment.
- Set up the network in the target OCI environment
- Collect information from the target environment:
    - Tenancy Oracle Cloud ID (OCID).
    - User OCID
    - Compartment OCID
    - OCI API PEM key fingerprint
    - Subnet OCID of the Virtual Cloud Network (VCN)

Complete the Prerequisites

Before you begin your migration, complete the prerequisites

Migrate Virtual Machines and Block Storage to OCI

Perform migration

Use the migration tool to perform the migration of all the Virtual machines and block storage volumes from OCI-C over to OCI.

Post migration tasks

These tasks may not be applicable to all customers and this is also not an exhaustive list.

- Update your organization's DNS servers with the new Public IP addresses for the application servers.
- If your organization uses code migration tools and/or monitoring tools for your application, you will have to update them also.
- If you had whitelisted (on an on-premises firewall) the Public IP addresses of your applications deployed on OCI-Classic, you will have to update the firewall rules with the new Public IP addresses

Summary

You should now be able to:

- Describe the benefits of moving from OCI-Classic to OCI
- Have an understanding of the requirements, migration strategy and tools for migrating infrastructure from OCI-Classic to OCI

Additional Information

Mapping OCI-Classic Network resources to OCI Virtual Cloud Network

Mapping General OCI Compute Classic Network concepts

OCI Compute Classic Network Resource	OCI Network Resource
Shared Network	A single subnet in a VCN.
IP Network	Subnets within a single VCN or Multiple VCNs with local peering configured – if the subnets span different parent CIDR block ranges and need to be interconnected
VPN Corente or VPNaaS	IPSec VPN
OCI FastConnect Classic	OCI FastConnect

Mapping OCI-Classic Network resources to OCI Virtual Cloud Network

Mapping General OCI Compute Classic Shared Network concepts

OCI Compute Classic Shared Network Resource	OCI Network Resource
Security Lists	A security list for a subnet in a VCN*
Security Rules	An Ingress and Egress security rule within a security list
Security Applications	The TCP, UDP or ICMP options within a security rule
Security IP lists	No direct equivalent. Security rules must be defined for a single source or destination IP prefix

*Security lists in OCI are applied at the Subnet level, Security Lists in OCI Compute Classic are applied at the Instance/VNIC level

Mapping OCI-Classic Network resources to OCI Virtual Cloud Network

Mapping General OCI Compute Classic IP Network concepts

OCI Compute Classic IP Network Resource	OCI Network Resource
IP network exchanges	Partially maps to a VCN. IP network exchanges provide connectivity between IP networks. In Oracle Cloud Infrastructure subnets under a VCN are connected by default. If an IP Network translates to multiple subnets across multiple VCNs, then a Local Peering Gateway is required to connect the subnets.
Virtual NIC sets	No equivalent*
Access Control Lists (ACLs)	A security list for a subnet in a VCN*
Routes	Routes
Security rules	An ingress and egress security rule within a security list
IP Address Prefix Sets	No direct equivalent. Security rules must be defined for a single source or destination IP prefix

*Security lists in OCI are applied at the Subnet level, while ACLs in OCI Compute Classic are applied to a set of instance VNICs

Mapping Virtual Machine Shapes in OCI-C to OCI

Mapping Oracle Cloud Infrastructure Compute Classic Instance Shapes to Oracle Cloud Infrastructure VM and BM Shapes

Oracle Cloud Infrastructure Compute Classic			Oracle Cloud Infrastructure		
Shape	OCPU/GPU	RAM	Shape	OCPU/GPU	RAM
oc3	1	7.5	VM.Standard2.1	1	15
oc4	2	15	VM.Standard2.2	2	30
oc5	4	30	VM.Standard2.4	4	60
oc6	8	60	VM.Standard2.8	8	120
oc7	16	120	VM.Standard2.16	16	240
oc8	24	180	VM.Standard2.24	24	320
oc9	32	240	BM.Standard2.52	52	768
oc1m	1	15	VM.Standard2.1	1	15
oc2m	2	30	VM.Standard2.2	2	30
oc3m	4	60	VM.Standard2.4	4	60
oc4m	8	120	VM.Standard2.8	8	120
oc5m	16	240	VM.Standard2.16	16	240
oc8m	24	360	VM.Standard2.24	24	320
oc9m	32	480	BM.Standard2.52	52	768
ocio1m	1	15	VM.DenseIO2.8	8	120
ocio2m	2	30	VM.DenseIO2.8	8	120
ocio3m	4	60	VM.DenseIO2.8	8	120
ocio4m	8	120	VM.DenseIO2.8	8	120
ocio5m	16	240	VM.DenseIO2.16	16	240
ocsg2-k80	6 / 2	120	VM.GPU3.2	12 / 2	180
ocsg2-m60	6 / 2	120	VM.GPU3.2	12 / 2	180
ocsg1-k80	3 / 1	60	VM.GPU3.1	6 / 1	90
ocsg1-m60	3 / 1	60	VM.GPU3.1	6 / 1	90

Mapping Virtual Machine Shapes in OCI-C to OCI

If instances in your Oracle Cloud Infrastructure Compute Classic account have multiple virtual NICs (vNICs), then you might need to select a larger shape in Oracle Cloud Infrastructure, to ensure that the appropriate number of vNICs is supported.

Oracle Cloud Infrastructure Compute Classic Shape	Oracle Cloud Infrastructure Shape for 1 or 2 vNICs	Oracle Cloud Infrastructure Shape for 3 or 4 vNICs	Oracle Cloud Infrastructure Shape for 5 or more vNICs
oc3	VM.Standard2.1	VM.Standard2.4	VM.Standard2.8
oc4	VM.Standard2.2	VM.Standard2.4	VM.Standard2.8
oc5	VM.Standard2.4	VM.Standard2.4	VM.Standard2.8
oc1m	VM.Standard2.1	VM.Standard2.4	VM.Standard2.8
oc2m	VM.Standard2.2	VM.Standard2.4	VM.Standard2.8
oc3m	VM.Standard2.4	VM.Standard2.4	VM.Standard2.8

Considerations for Migrating Your Network

Network Topology Mapping

Migrate the Shared Network with Network Topology Mapping

- If your source environment uses the shared network, then to migrate your network to OCI, you can create a single VCN with multiple subnets.
- In Oracle Cloud Infrastructure Compute Classic, the shared network doesn't allow you to select or specify private IP addresses and private IP addresses aren't persistent. However, when you create the VCN and subnets in OCI, you can specify the IP address range for private IP addresses and the primary private IP addresses are persistent.
- Use the network and resource discovery tool to generate the terraform file for creating the network and security list rules.
- Review the generated Terraform and make any required modifications before creating the network and applying the security rules to subnets in OCI.
- Migrate your instances. After your instances are migrated, launch your instances in the subnet for the shared network, so that the appropriate security rules are applied. The process of launching instances in the appropriate subnet must be performed manually.

ORACLE
Cloud Infrastructure

cloud.oracle.com/iaas

cloud.oracle.com/tryit