h_da

HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES

fbi

FACHBEREICH INFORMATIK

Cloud Overview &
Oracle Cloud Infrastructure

Robert Marz

Databees.

Robert Marz – Independent Consultant

Primary Job Role

Senior Technical Architect
with database centric view of the world

DOAG (German Oracle User Group)

Active Member of Database Community
Responsible for Cloud Topics

@RobbieDatabee

robbie.databee.org

robert@databee.org

Databees.

ORACLE ACE

500+ Technical Experts Helping Peers Globally

ORACLE ACE PROGRAM

---

bit.ly/OracleACEProgram

Nominate yourself or someone you know: **acenomination.oracle.com**

What is a Cloud?

Cloud?

Begriffsbestimmung Cloud

"Cloud Computing ist ein **Modell**, das es erlaubt **bei Bedarf**, **jederzeit** und überall bequem über ein Netz auf einen geteilten Pool von konfigurierbaren **Rechnerressourcen** […] zuzugreifen, die **schnell** und mit minimalem Managementaufwand oder **geringer Serviceprovider-Interaktion** zur Verfügung gestellt werden können."

BSI (basierend auf der NIST-Definiton von 2011)

Cloud Computing

Cloud Computing bezeichnet
das **dynamisch** an den Bedarf **angepasste**, **hochautomatisierte**

- Anbieten
- Nutzen
- Abrechnen

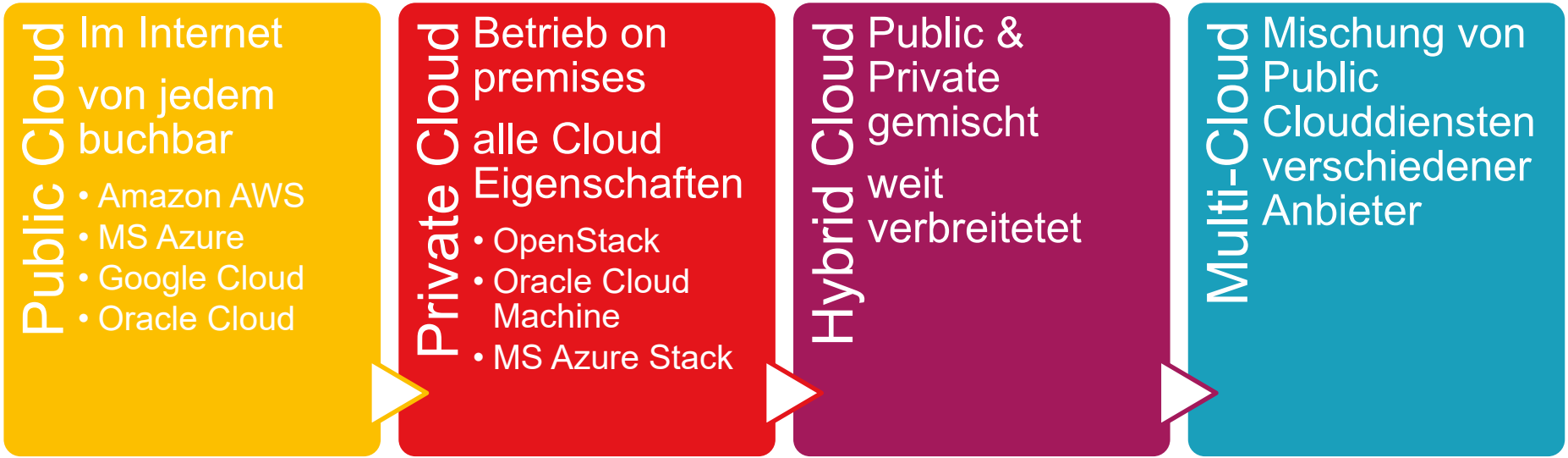
von IT-Dienstleistungen über ein Netz.

BSI (basierend auf der NIST-Definiton von 2011)

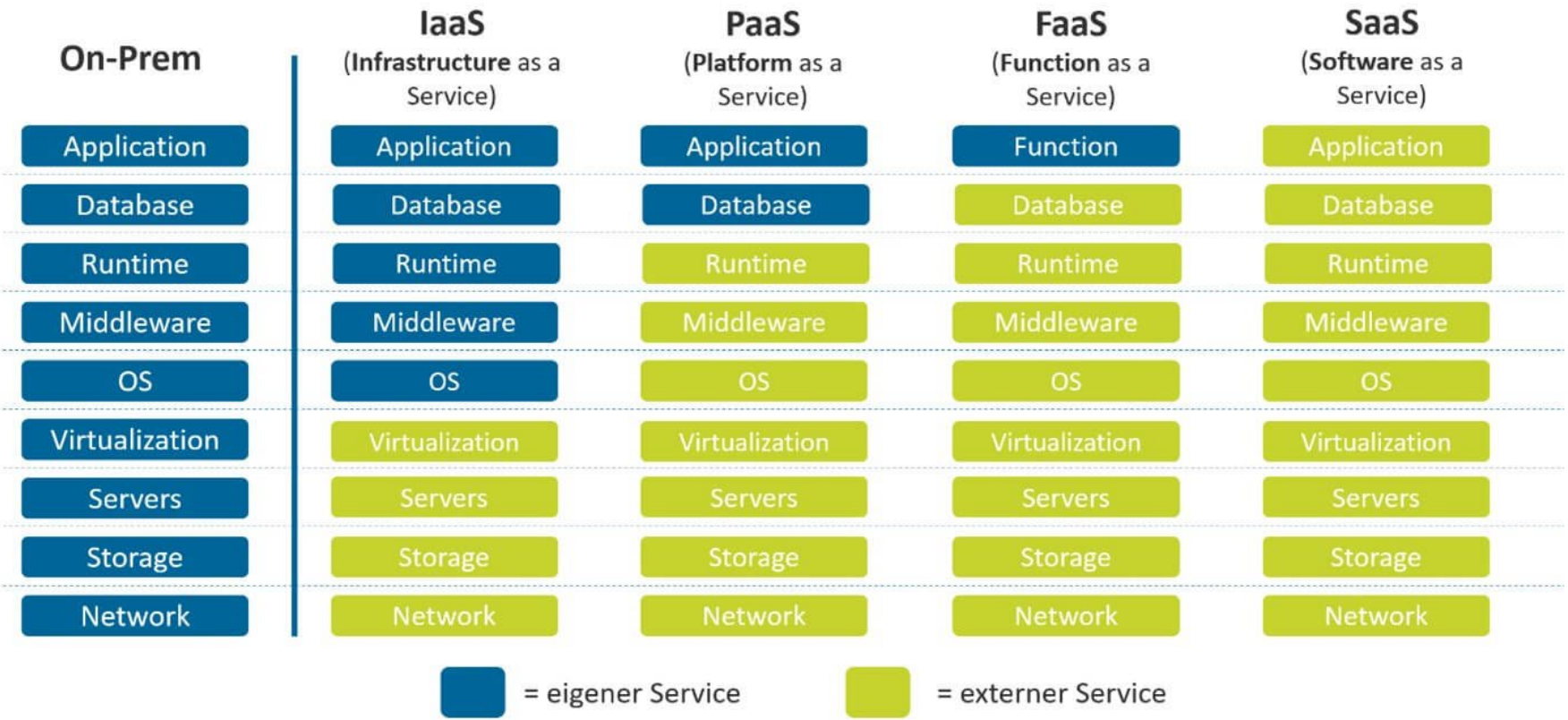
Cloud charakteristische Eigenschaften

On-demand Self Service	Die Provisionierung der Ressourcen (z. B. Rechenleistung, Storage) läuft automatisch ohne Interaktion mit dem Service Provider ab.
Broad Network Access	Die Services sind mit Standard-Mechanismen über das Netz verfügbar und nicht an einen bestimmten Client gebunden.
Resource Pooling	Die Ressourcen des Anbieters liegen in einem Pool vor, aus dem sich viele Anwender bedienen können (Multi-Tenant Modell). Dabei wissen die Anwender nicht, wo die Ressourcen sich befinden, sie können aber vertraglich den Speicherort, also z. B. Region, Land oder Rechenzentrum, festlegen.
Rapid Elasticity	Die Services können schnell und elastisch zur Verfügung gestellt werden, in manchen Fällen auch automatisch. Aus Anwendersicht scheinen die Ressourcen daher unendlich zu sein.
Measured Services	Die Ressourcennutzung kann gemessen und überwacht werden und entsprechend bemessen auch den Cloud-Anwendern zur Verfügung gestellt werden.

Cloud Geschmacksrichtungen



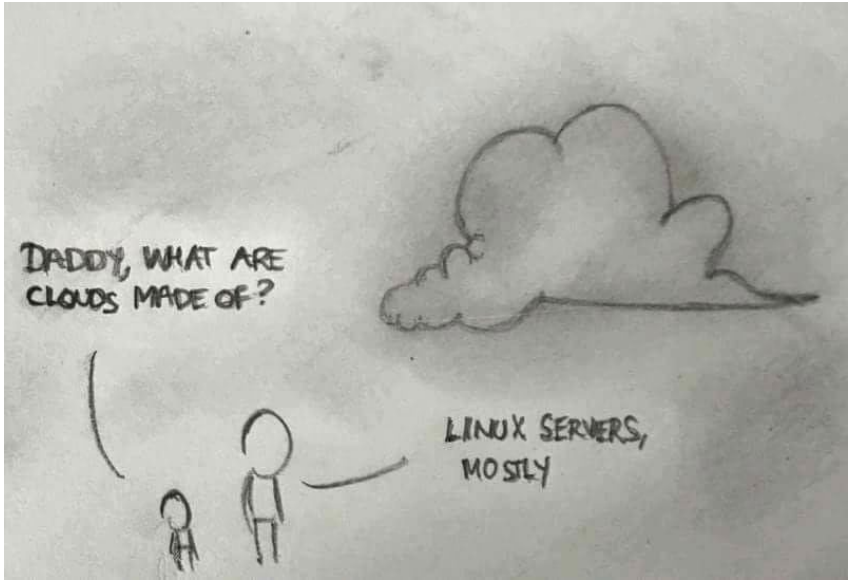
Cloud Servicemodelle



What means IaaS?

After Subscribing to IaaS Cloud Services
You start with an empty virtual Datacenter

IaaS Clouds

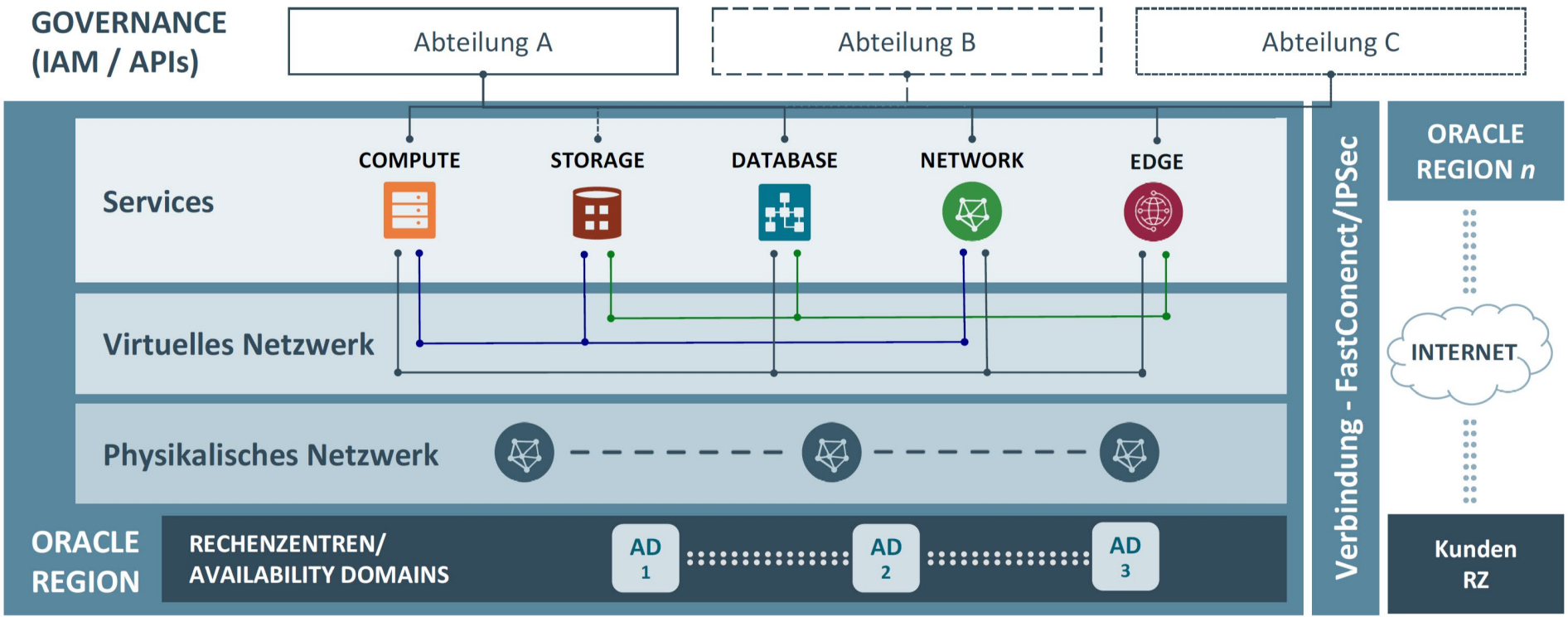


What are Clouds made of?

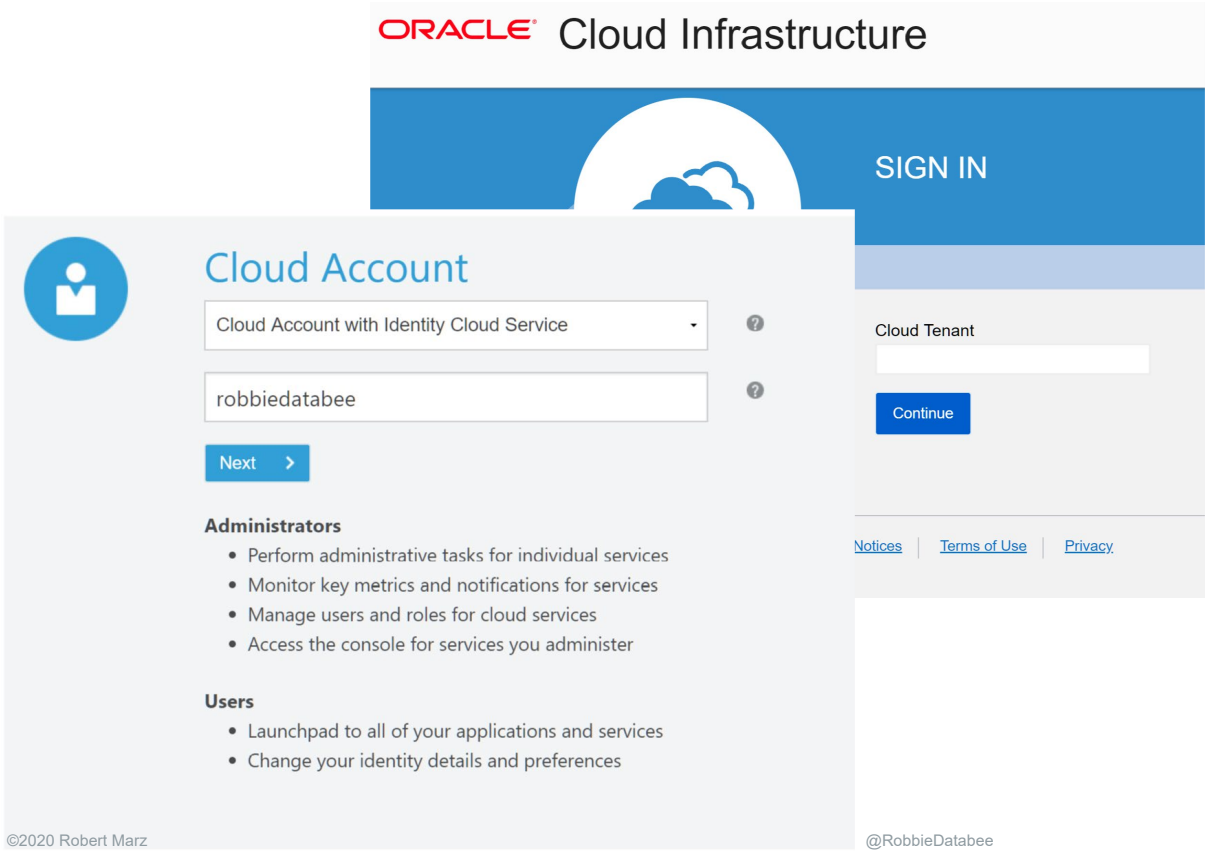
Linux Servers	Mostly
Network Components	Other supporting stuff
Software Defined (SDx)	Everything is Virtual
	For Cloud-Users

OCI Basics

Oracle Cloud Infrastructure Overview



Identity Domains, Tenants & Cloud-Account



Identity Domains, Tenants & Cloud Account

Mean the same thing: Your Cloud Space

Part of your Cloud URLs

Enter your Identity Domain; Login with user & password

Compartments

Compartments

Logical Dividers	Namespaces	
	Subdomains	
Separation	Departments	
	Applications	
“New Features”	nestable (6 levels)	*Nov. 1, 2018*
	Renameable	*Sept. 7, 2017*
	Deleteable	*Oct. 18, 2018*
Cloud Resources	Stay in their Compartment (not anymore)	
	See each other	


DEMO
delete
©nitroworld - stock.adobe.com

Virtual Cloud Network Wizard

Virtual Cloud Network Wizard

VCN Wizard

Launched via Menu

Networking
> Virtual Cloud Networks
> Create Virtual Network

Creates Resources

in one easy step

Start VCN Wizard

VCN with Internet Connectivity

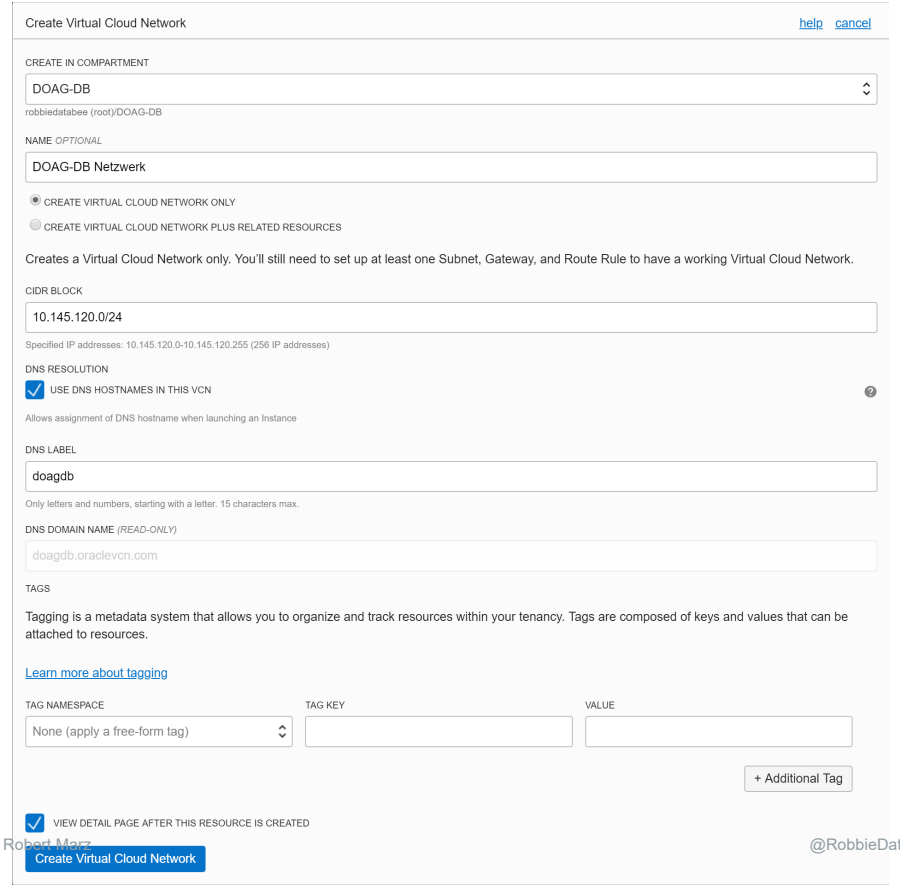
… and Site-to-Site VPN Connect

All created resources

can be modified afterwards

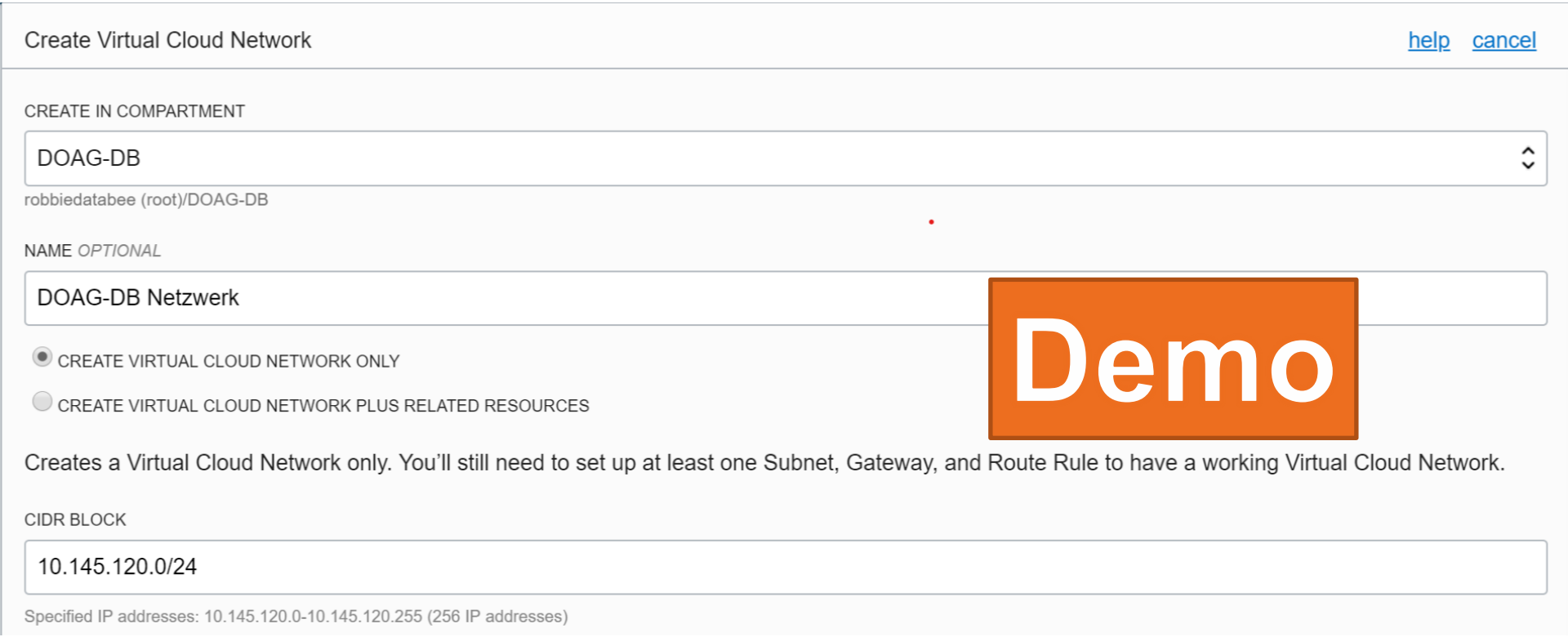
Exception: VCN IP Range

The Virtual Cloud Network Wizard (Network only)

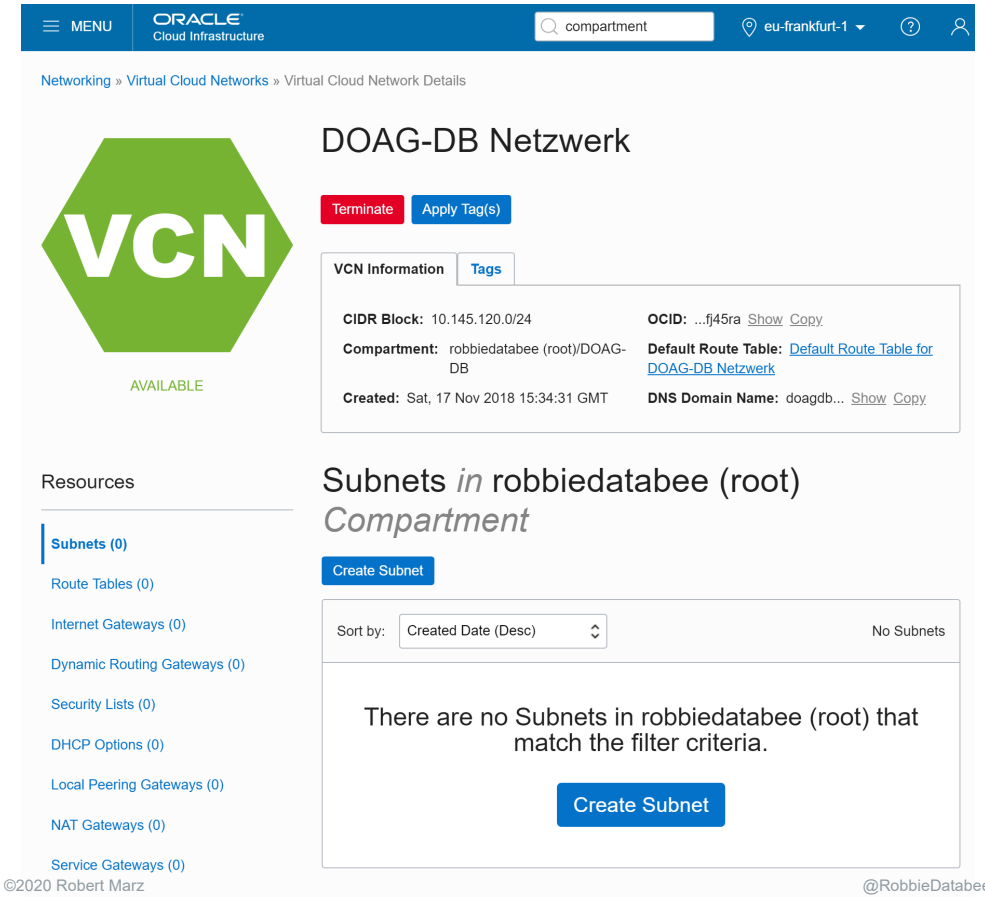


Demo

The Virtual Cloud Network Wizard (Network only) [zoom]

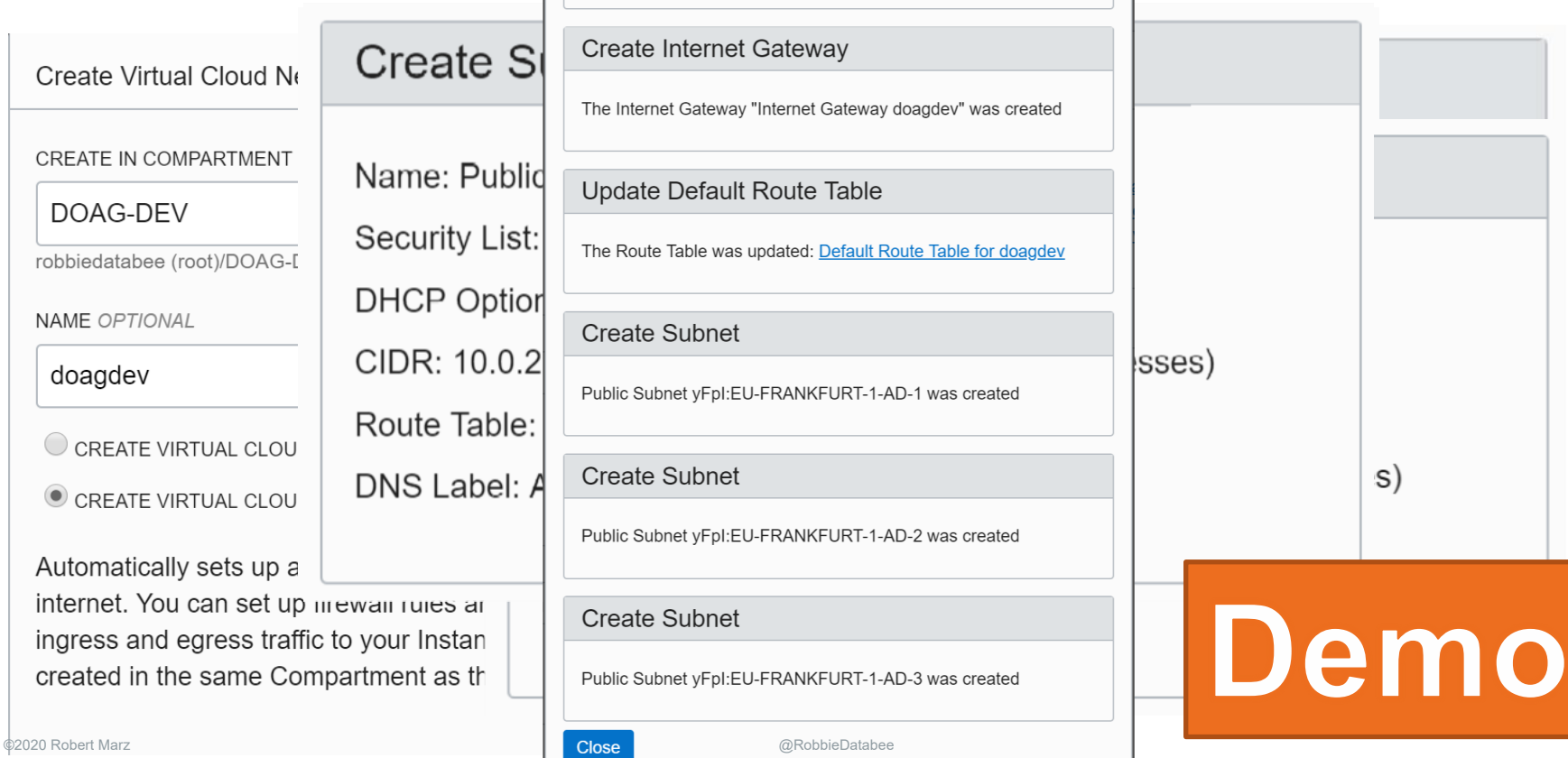


The Virtual Cloud Network Wizard (Network only) - Results



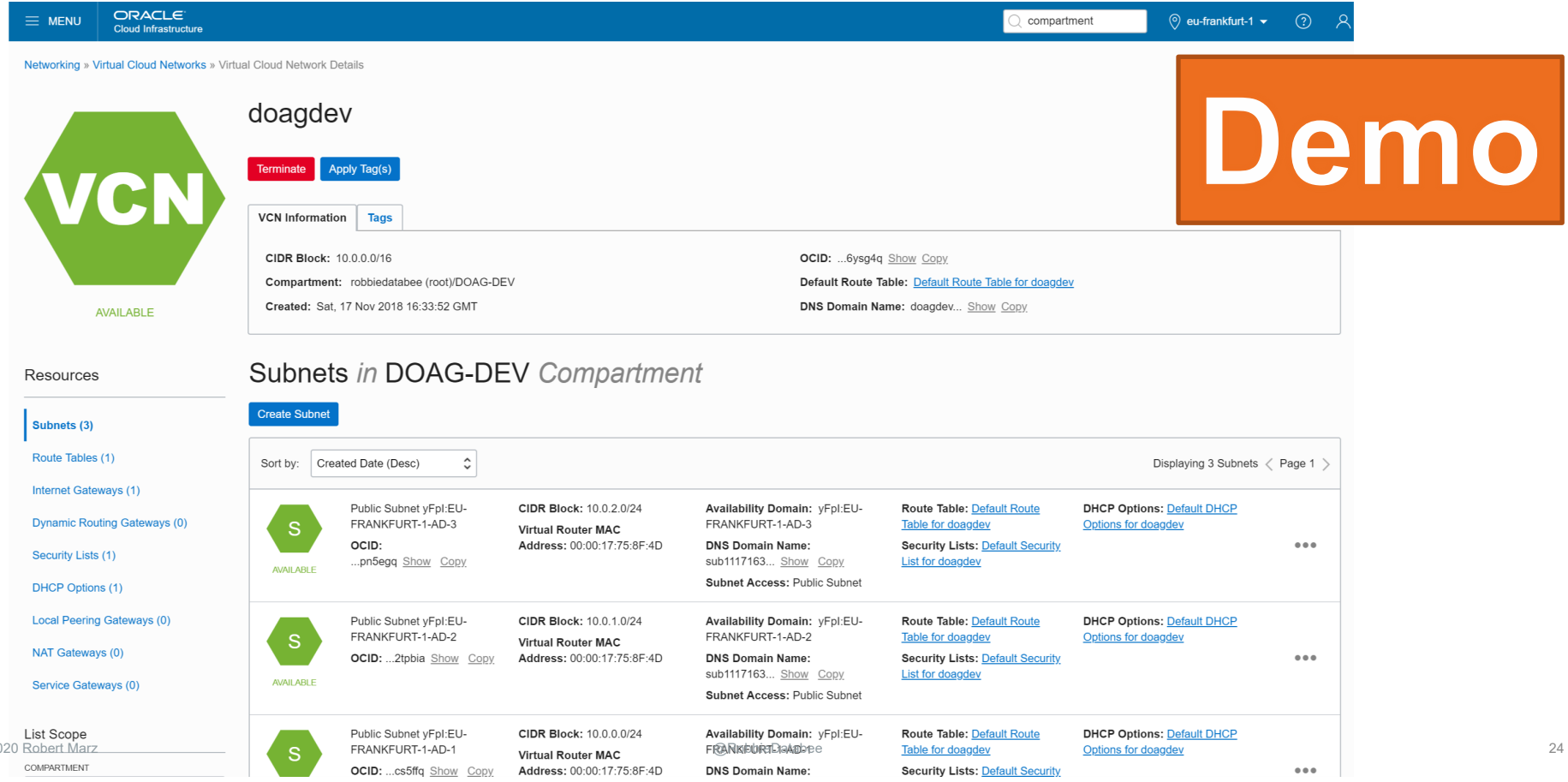
Demo

The Virtual Cloud N…related Resources)



Demo

The Virtual Cloud Network Wizard (+ related Resources) Results



Demo

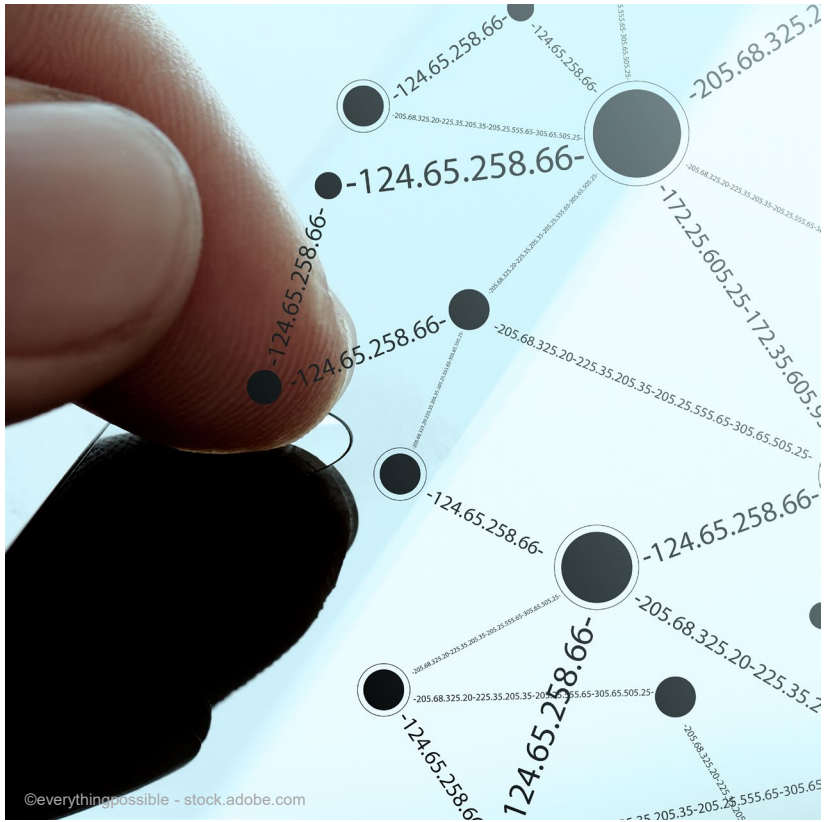
Networking in OCI

OCI Networking Components (1/3)

Networking

VCN	Virtual Cloud Network	**IPv4 only**
	Covers Network Addresses	single, contiguous CIDR block
Subnets	Scope	Regional Availability Domain specific
	contain VNICs with same	route table security lists DHCP Options

Private & Public IPs



Public IPs are Unique

World Wide

IPv4 Addresses are limited

Not enough unique IPs

Standardized Private IP-Adresses

Used over and over again

Packets with private IP address aren't forwarded into the Internet

Private IP Networks

RFC1918 name	IP address range	number of addresses	largest CIDR block (subnet mask)	classful description
24-bit block	10.0.0.0 – 10.255.255.255	16777216	10.0.0.0/8 (255.0.0.0)	single class A network
20-bit block	172.16.0.0 – 172.31.255.255	1048576	172.16.0.0/12 (255.240.0.0)	16 contiguous class B networks
16-bit block	192.168.0.0 – 192.168.255.255	65536	192.168.0.0/16 (255.255.0.0)	256 contiguous class C networks

https://en.wikipedia.org/wiki/Private_network

IP Subnetworks – Masking & CIDR

IP Addresses in the same Subnet are considered local

no routing required

Subnet Masking

Binary Operation “AND”

Google

“Network Calculator”
“IP Subnet Calculator”

Network	192.168.132.0 mask 255.255.255.0
CIDR	192.168.132.0/**24**

IPv4 Addresses are 4 Bytes	192	168	132	197
Each Byte has 8 Bits, 0-255	1100 0000	1010 1000	1000 0100	1100 0101
Subnet Masks	255	255	255	0
CIDR counts the 1s (3 x 8 = **24**)	1111 1111	1111 1111	1111 1111	0000 0000
Network Adress (logical AND)	192	168	132	0

Subnet masking in Action

Network 192.168.132.197/28
netmask 255.255.255.240

IP	Masked IP
192.168.132.197	192.168.132.192

Subnet masking in Action

Network 192.168.132.197/28
netmask 255.255.255.240

IP	Masked IP
192.168.132.197	192.168.132.192
192.168.132.190	192.168.132.176

Subnet masking in Action

Network 192.168.132.197/28
netmask 255.255.255.240

IP	Masked IP
192.168.132.197	192.168.132.192
192.168.132.190	192.168.132.176
192.168.132.209	192.168.132.208

Subnet masking in Action

Network 192.168.132.197/28
netmask 255.255.255.240

IP	Masked IP
192.168.132.197	192.168.132.192
192.168.132.190	192.168.132.176
192.168.132.209	192.168.132.208
192.168.132.200	192.168.132.192

Examples of IP-Subnets

Network	Low IP Network Adr	High IP Broadcast Adr	# Adrs	Netmask
192.168.132.197/28	192.168.132.193 192.168.132.192	192.168.132.206 192.168.132.207	14	255.255.255.240
172.24.19.100/20	172.24.16.1 172.24.16.0	172.24.19.254 172.24.19.255	4096	255.255.240.0
10.100.0.0/16	10.100.0.1 10.100.0.0	10.100.255.254 10.100.255.255	65534	255.255.0.0

IP Routing – Why planning ahead is important

IP Routing

whenever a Packet has to leave its subnet	“Destination is not on the switch”
Addresses in own Subnet are considered local	no routing
NEVER OVERLAP	IP-Ranges in Networks

Plan Ahead

Use only “new” IP-Ranges for Networks	as small as possible	
	as big as necessary	at least 3 Subnets for Availability Domains
A Cloud Account is a new Datacenter	Chance for a fresh Start	
Quick and Dirty Trials	Don’t let them become productive	
	Destroy and rebuild	

OCI Networking Components (2/3)

Networking

VNIC	Virtual Network Interface Card	
Private IP	Assigned to each VNIC	primary unchanged during lifetime
Public IP	Routable	from Internet
	Optional	Assigned to VNIC 50 static IPs free of charge
	Requirements	Public Subnet, Internet Gateway

OCI Networking Components (3/3)

Networking

Route Tables	Routes from Subnet to outside VCN	
	Default	empty
Security Lists	Virtual Firewall Rules	Stateful, Stateless Ingress = inbound; egress = outbound
	Default Set (stateful)	Ingress: allow ssh, icmp type 3+4 Egress: allow any
DHCP Options	Configuration Set	
	Limited Options	DNS Type Search Domain


DEMO
delete
©nitroworld - stock.adobe.com

OCI Ne

Networking » Virtual Cloud Networks » Virtual Cloud Network Details » Security Lists » Security List Details

AVAILABLE

Default Security List for DOAG-DB Netzwerk

Edit All Rules | Terminate | Apply Tag(s)

Security List Information | Tags

OCID: ...sunwca Show Copy

Created: Sat, 17 Nov 2018 15:34:31 GMT

Instance traffic is controlled by firewall rules on each Instance in addition to this Security List

Resources

- Ingress Rules (3)
- Egress Rules (1)

Ingress Rules

Stateless Rules

No Ingress Rules

There are no stateless Ingress Rules for this Security List.

Stateful Rules

Source: 0.0.0.0/0	**IP Protocol:** TCP	**Source Port Range:** All	**Destination Port Range:** 22	**Allows:** TCP traffic for ports: 22 SSH Remote Login Protocol
Source: 0.0.0.0/0	**IP Protocol:** ICMP	**Type and Code:** 3, 4		**Allows:** ICMP traffic for: 3, 4 Destination Unreachable: Fragmentation Needed and Don't Fragment was Set
Source: 10.145.120.0/24	**IP Protocol:** ICMP	**Type and Code:** 3		**Allows:** ICMP traffic for: 3 Destination Unreachable

verk

HCP Options

Demo

OCI Networking Gateways

Gateways (GW) Virtual Routers

Dynamic Routing GW (DRG)	private Network traffic VCN and on-Premises	
Internet GW	provides direct Internet Access	
NAT GW	Network Address Translation	Connects Cloud resources to Internet without Public IP
Service Gateway	Peers VCN with other Oracle Cloud Services	e.g. Object Storage
Local Peering GW (LPG)	Peer VCNs in **same** Region	
Remote Peering Connection	Peer VCNs in **different** Regions	

Connecting to the Cloud

Connecting on-Premises to the Cloud

Paths into the Cloud

ssh Tunnel	to public IP	Ends on Compute Server
	Testing and Development only	
Custom Firewall Appliance	Compute Instance	Custom Image
	Custom VPN Setup	e.g. OpenVPN
IPSec VPN	Connect on-Premises VPN to Dynamic Routing Gateway (DRG)	Routing through public Internet
OCI FastConnect	Private Connection	
	Peering	Private Public
	Expensive	+ Provider (leased Line) + Datacenter

Paths into the Cloud: ssh Tunnel

ssh Tunnel

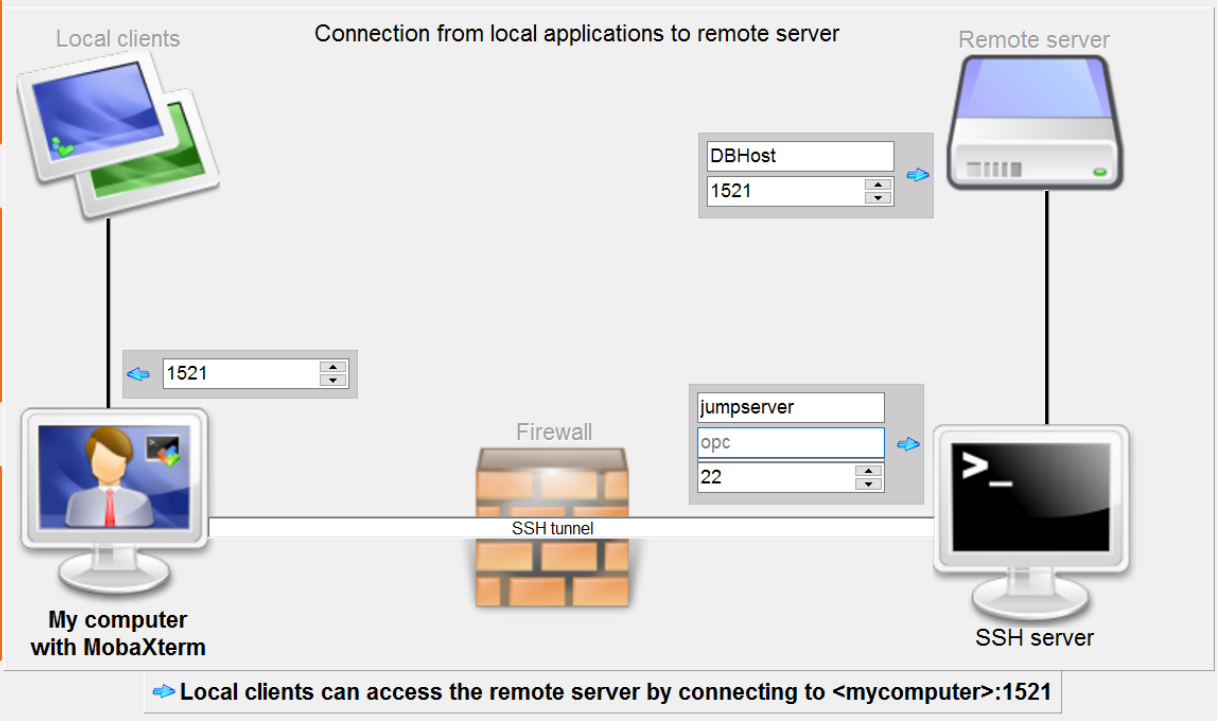
opens Port on local host

tunnels

IP Packets to ssh-destination „jumpserver“

forwards

IP Packets to any host/port accessable from jumpserver



Paths into the Cloud: Automomous Database

Autonomous DBs

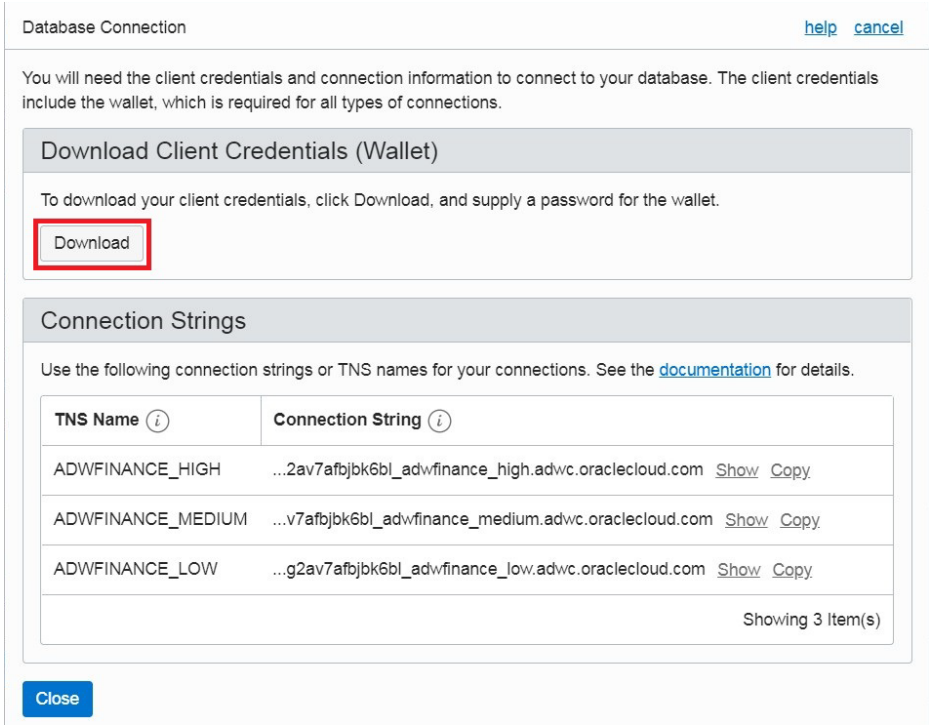
can‘t have VNICs

Access

encrypted via Internet

Wallet

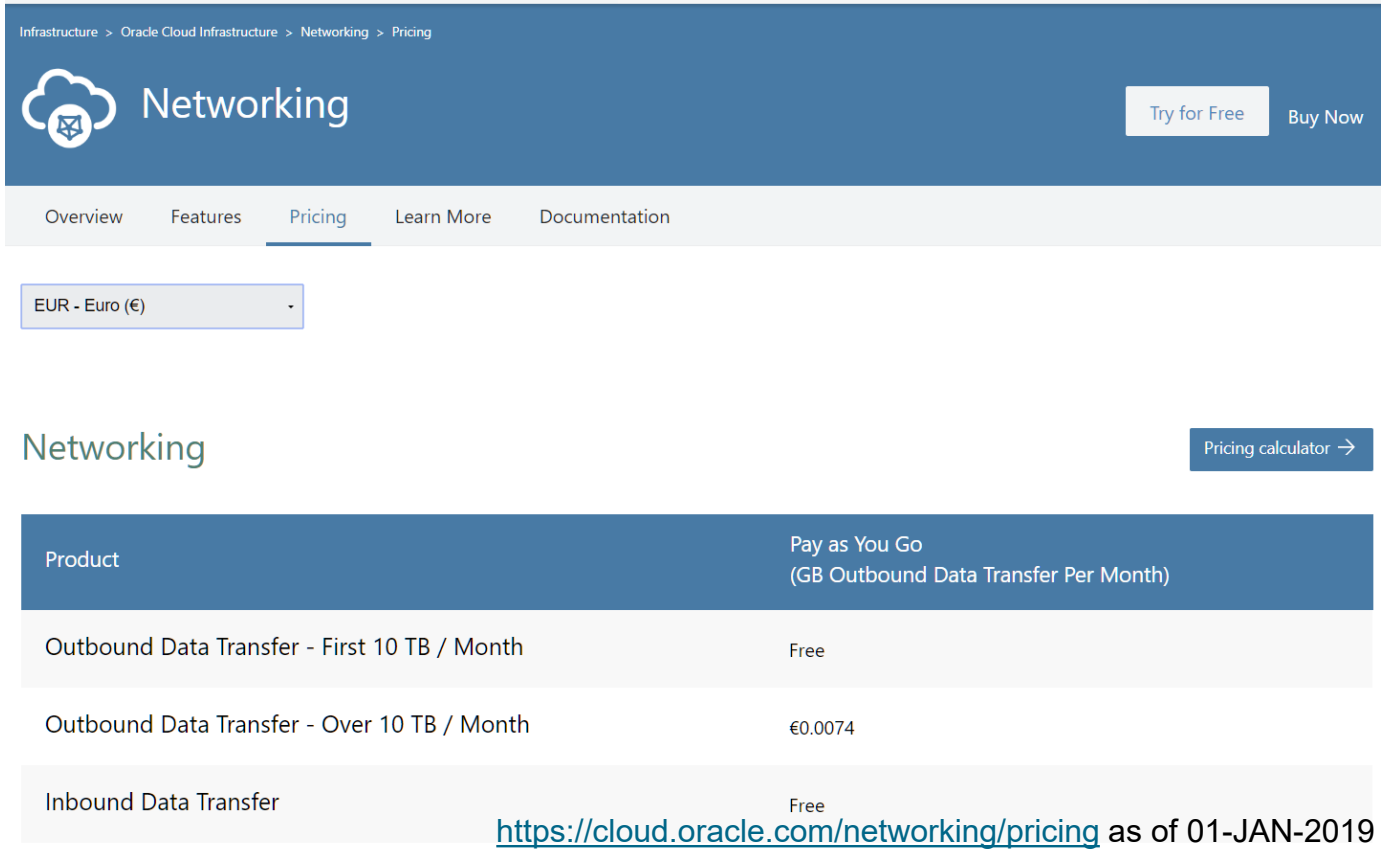
Download zip-Archive
Import directly to SQL Developer
unzip & configure for SQLNet



OCI Networking Costs - Currencies

Next Topic

OCI Networking – Costs EUR - Euro (€)

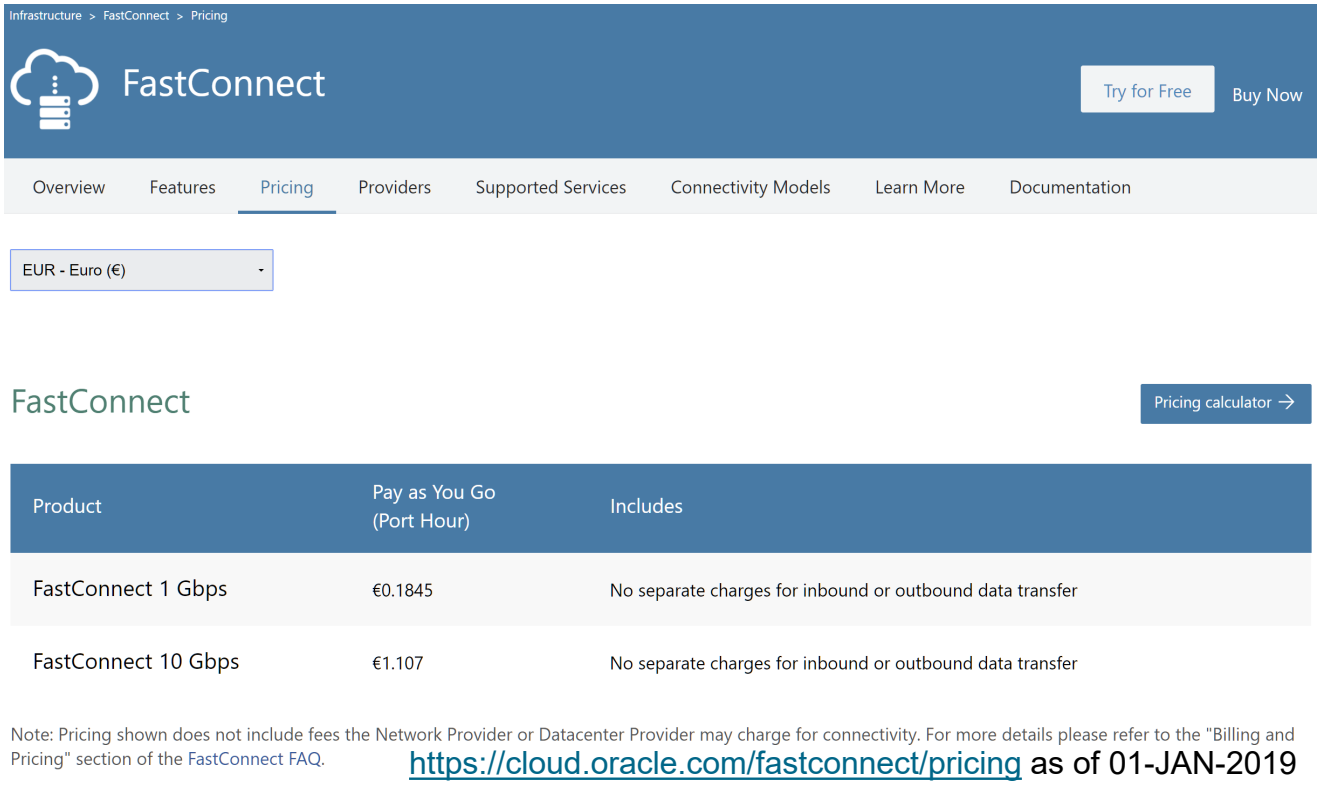


https://cloud.oracle.com/networking/pricing as of 01-JAN-2019

Assumptions:
1GBit Connection
1 TB Data transfer
takes 3h (roughly)

24h x 30 / (3h * TB) ≈ 240 TB
240 TB – 10 TB ≈ 230.000 GB
230.000 * 0,0074€ = 1.702€
max per Month

FastConnect Pricing EUR - Euro (€)



https://cloud.oracle.com/fastconnect/pricing as of 01-JAN-2019

24h * 31 = 744h

1 Gbps:
744 * €0,1845 = €137,27

10 Gbps:
744 * €1,107 = €823,61

Additional costs:
+ Network Provider (leased line)
+ Datacenter Provider

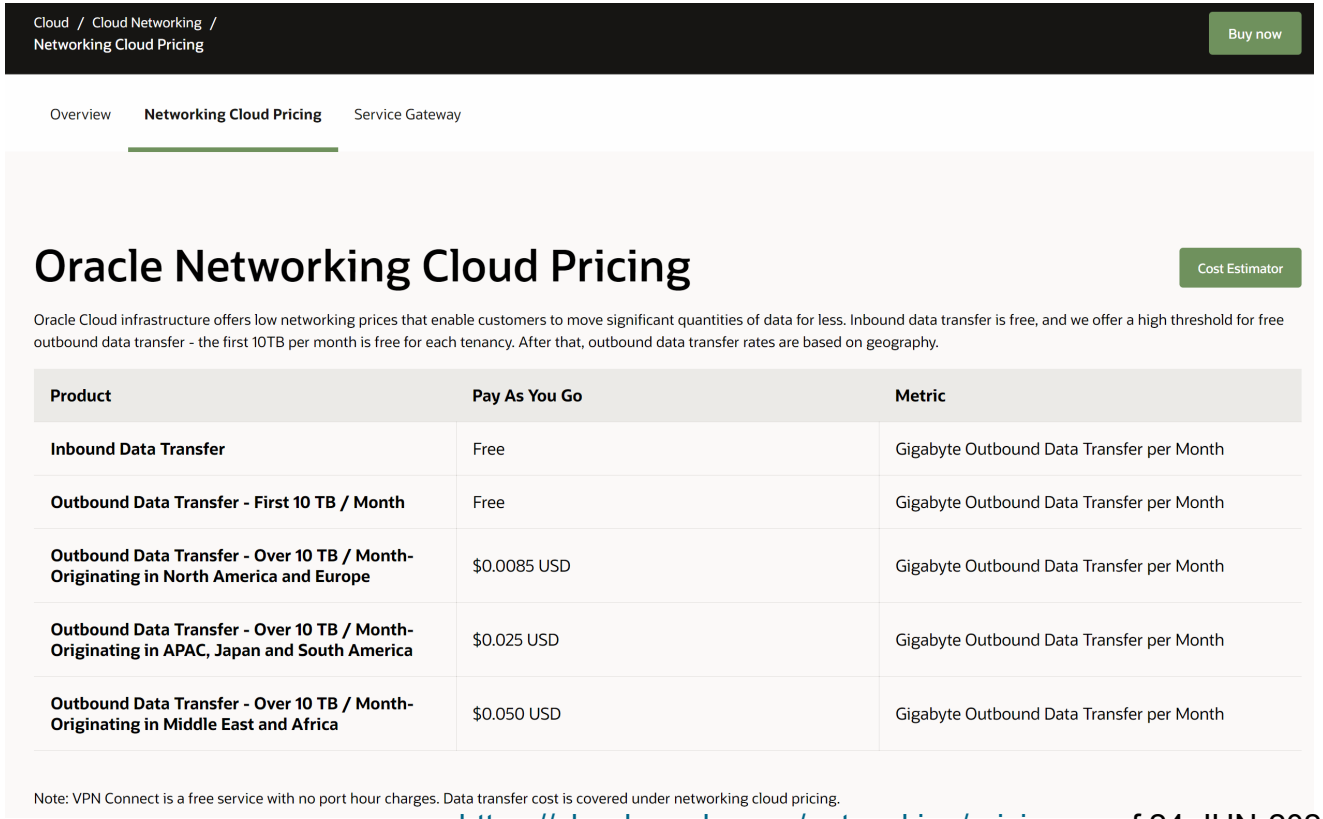
Oracle Cloud Cost Estimator EUR – Euro (€)

Configuration Options

	Pay As You Go	Monthly Flex
Oracle Cloud Infrastructure - FastConnect	€2,656	€2,656
Network	€2,656	€2,656
Utilization		
Number of Instances / 1 Instance(s)		
Average Days Usage per Month / 31 day(s)		
Average Hours Usage per Day / 24 hour(s)		
Configuration		
FastConnect 1 Gbps (B88325) / 1	€137	€137
Port Hour	1	
Outbound Data Transfer (B88327) / 240000	€1,696	€1,696
Gigabyte Outbound Data Transfer Per Month	240000	
FastConnect 10 Gbps (B88326) / 1	€824	€824
Port Hour	1	

https://cloud.oracle.com/en_US/cost-estimator as of 01-JAN-2019

OCI Networking – Costs USD - US-Dollar ($)



Assumptions:
1GBit Connection
1 TB Data transfer
takes 3h (roughly)

24h x 30 / (3h * TB) ≈ 240 TB
240 TB – 10 TB ≈ 230.000 GB
230.000 * $0.0085 = $1,955.0
max per Month

https://cloud.oracle.com/networking/pricing as of 24-JUN-2020

FastConnect Pricing USD - US-Dollar ($)

FastConnect Cloud Pricing

Cost Estimator

USD - US Dollar ($)

Product	Pay as You Go (Port Hour)	Includes
FastConnect 1 Gbps	$0.2125	No separate charges for inbound or outbound data transfer
FastConnect 10 Gbps	$1.275	No separate charges for inbound or outbound data transfer

Note: Pricing shown does not include fees the network provider or data center provider may charge for connectivity. For more details please refer to the "Billing and Pricing" section of the FastConnect FAQ.

https://www.oracle.com/cloud/networking/fastconnect.html#pricing as of 24-JUN-2020

24h * 31 = 744h

1 Gbps:
744 * $0.2125 = $158.10

10 Gbps:
744 * $1.275 = $948.60

Additional costs:
+ Network Provider (leased line)
+ Datacenter Provider
(+ OCI Outbound Traffic)

Oracle Cloud Cost Estimator – USD - US-Dollar ($)

Configuration Options

	Pay As You Go	Monthly Flex
Oracle Cloud Infrastructure - FastConnect	$3,060	$3,060
Network	$3,060	$3,060

Utilization

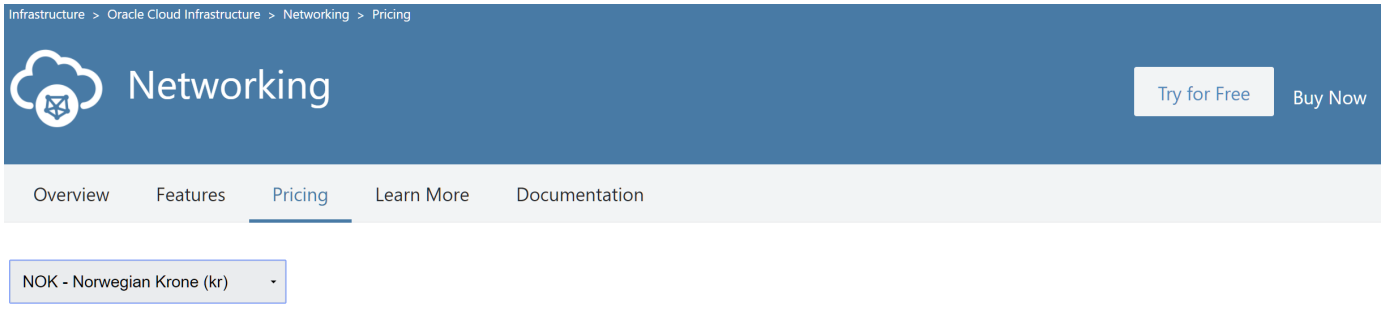
- Number of Instances / 1 Instance(s)
- Average Days Usage per Month / 31 day(s)
- Average Hours Usage per Day / 24 hour(s)

Configuration

FastConnect 1 Gbps (B88325) / 1	$158	$158
Port Hour	1	
Outbound Data Transfer (B88327) / 240000	$1,953	$1,953
Gigabyte Outbound Data Transfer Per Month	240000	
FastConnect 10 Gbps (B88326) / 1	$949	$949
Port Hour	1	

https://cloud.oracle.com/en_US/cost-estimator as of 24-JUN-2020

OCI Networking – Costs NOK – Norwegian Krone (kr)



Networking

Pricing calculator →

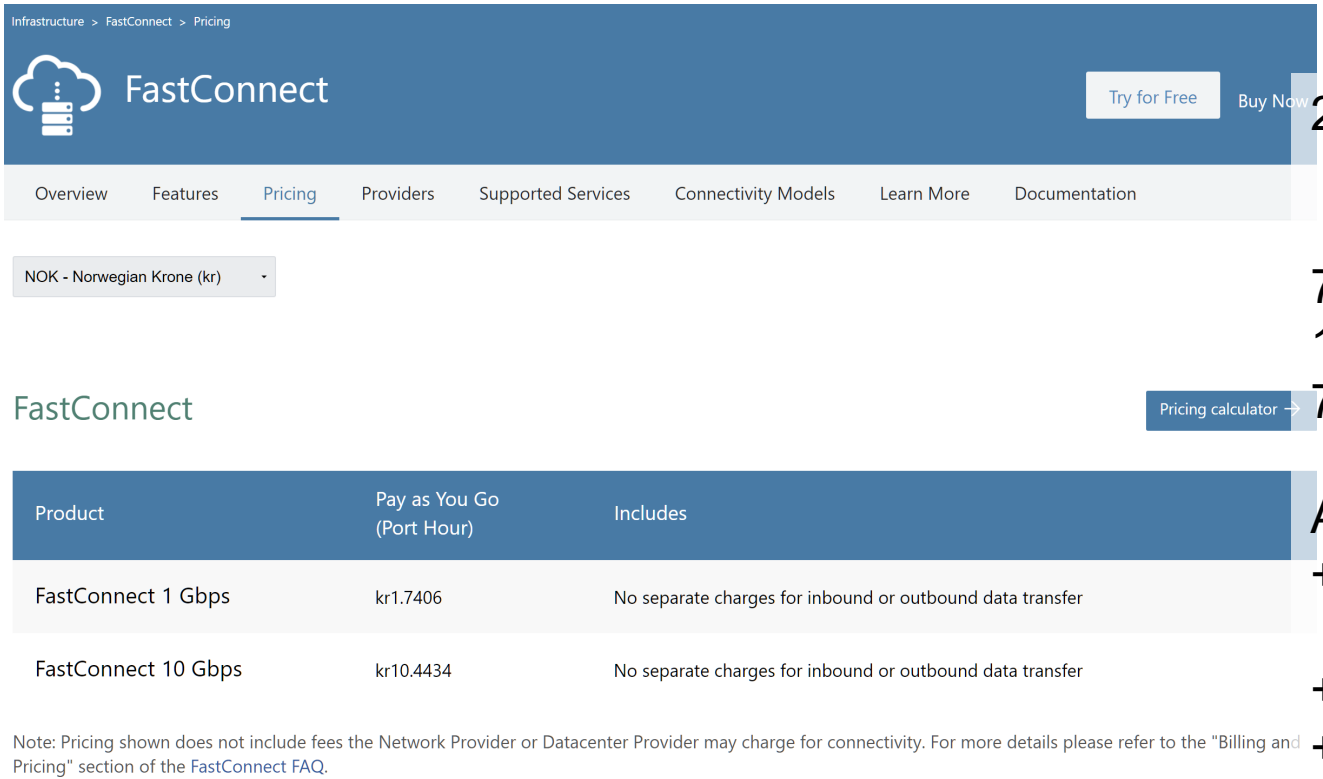
Product	Pay as You Go (GB Outbound Data Transfer Per Month)
Outbound Data Transfer - First 10 TB / Month	Free
Outbound Data Transfer - Over 10 TB / Month	kr0.0696
Inbound Data Transfer	Free

Assumptions:
1GBit Connection
1 TB Data transfer
takes 3h (roughly)

24h x 30 / (3h * TB) ≈ 240 TB
240 TB – 10 TB ≈ 230.000 GB
230.000 * kr0.0696 = kr16,008
max per Month

https://cloud.oracle.com/networking/pricing as of 01-JAN-2019

FastConnect Pricing USD - NOK – Norwegian Krone (kr)



24h * 31 = 744h

1 Gbps:
744*kr1.7406 = kr1,295.01
10 Gbps:
744*kr10.4434 = kr7,769.89

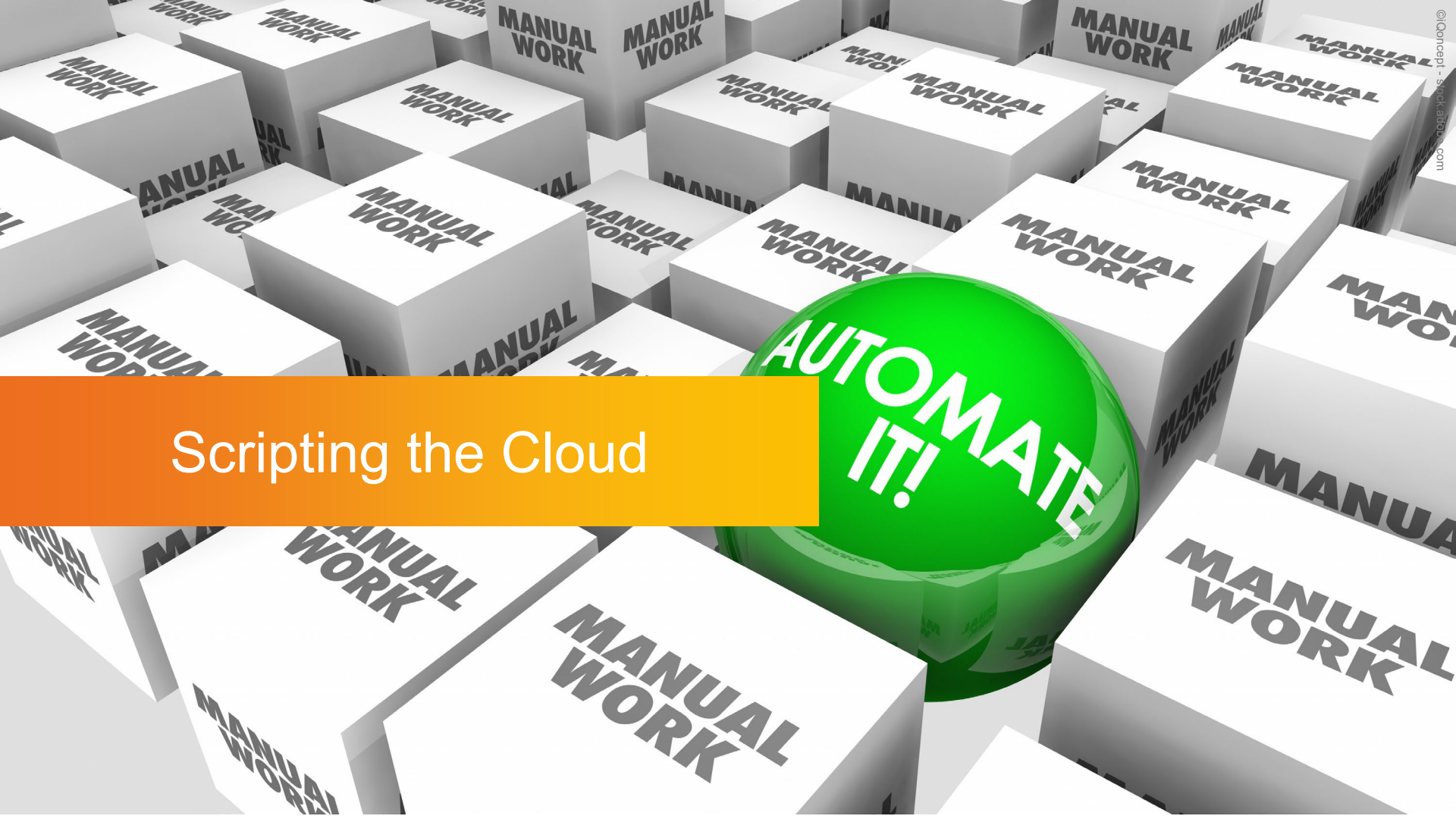
Additional costs:
+ Network Provider (leased line)
+ Datacenter Provider
+ OCI Networking

https://cloud.oracle.com/fastconnect/pricing as of 01-JAN-2019

Oracle Cloud Cost Estimator NOK – Norwegian Krone (kr)

Configuration Options	Pay As You Go	Monthly Flex
Oracle Cloud Infrastructure - FastConnect	kr25,061	kr25,061
Network	kr25,061	kr25,061
Utilization		
Number of Instances / 1 Instance(s)		
Average Days Usage per Month / 31 day(s)		
Average Hours Usage per Day / 24 hour(s)		
Configuration		
FastConnect 1 Gbps (B88325) / 1	kr1,295	kr1,295
Port Hour	1	
Outbound Data Transfer (B88327) / 240000	kr15,997	kr15,997
Gigabyte Outbound Data Transfer Per Month	240000	
FastConnect 10 Gbps (B88326) / 1	kr7,770	kr7,770
Port Hour	1	

https://cloud.oracle.com/en_US/cost-estimator as of 01-JAN-2019



Scripting the Cloud

Scripting means Automation: Infrastructure as Code

Building up and tearing down of virtual environments happens frequently in the Cloud

Some changes can only be made by recreating the resource

Provisioning Cloud Resources by Clicking the UI is tedious and error prone

Use the Web-UI for Orientation only

Scripting is automation and documentation at the same time: **Software Defined Infrastructure**

Scripting Options – Automate all the Things!

Scripting Options

REST API	"The Master"
	Provides Access to ALL Resources and Options
	More Programming than Scripting
OCI CLI	Python Based CLI
	Unix & Windows
	OpenSource Hosted on GitHub
HashiCorp Terraform	Scripting across all Major IaaS Providers
	Provider by Oracle
	Defacto Standard for Scripting Cloud Resources
Ansible	Agentless Orchestration and Automation
	OCI Module provided by Oracle

Conclusion

Automate your Cloud

- **Networking** — in the Cloud: **same as on premises**
- **Cloud-Account** — is like a new Datacenter: **Plan ahead**
- **The Web-UI** — is only second-best: **script everything**

The Sky Cloud is the Limit