ORACLE

HOUG Oracle Cloud workshop-sorozat II. rész

Oracle Cloud Infrastructure (OCI) alapozó

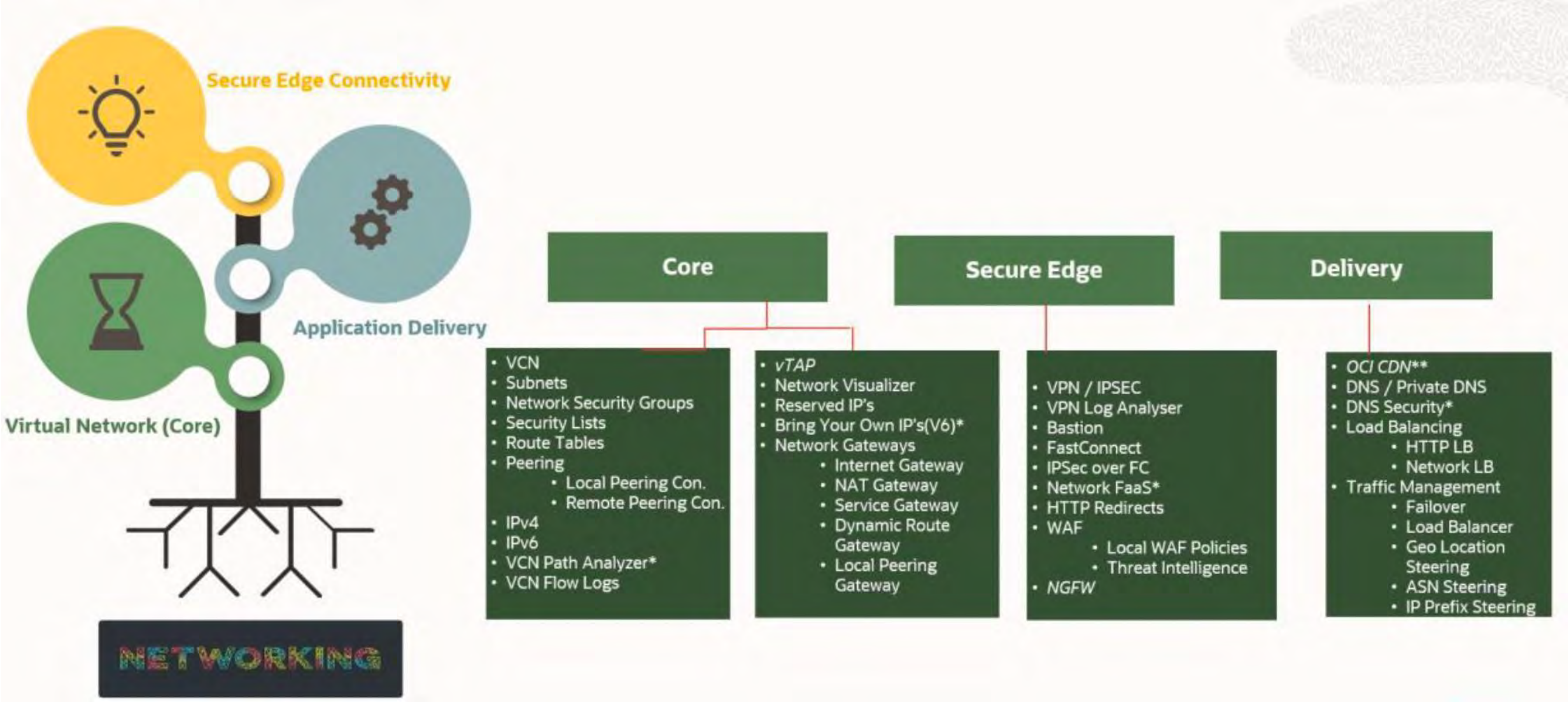
Kovács Norbert, Farkas **Miklós**

2023. szeptember 14.

Hálózati komponensek

Virtual Cloud Network, Gateways, Security List, Network Security Group, Network Fitewall, Load Balancer, Web Application Firewall

Hálózat áttekintő



Core

- VCN
- Subnets
- Network Security Groups
- Security Lists
- Route Tables
- Peering
    - Local Peering Con.
    - Remote Peering Con.
- IPv4
- IPv6
- VCN Path Analyzer*
- VCN Flow Logs

- *vTAP*
- Network Visualizer
- Reserved IP's
- Bring Your Own IP's(V6)*
- Network Gateways
    - Internet Gateway
    - NAT Gateway
    - Service Gateway
    - Dynamic Route Gateway
    - Local Peering Gateway

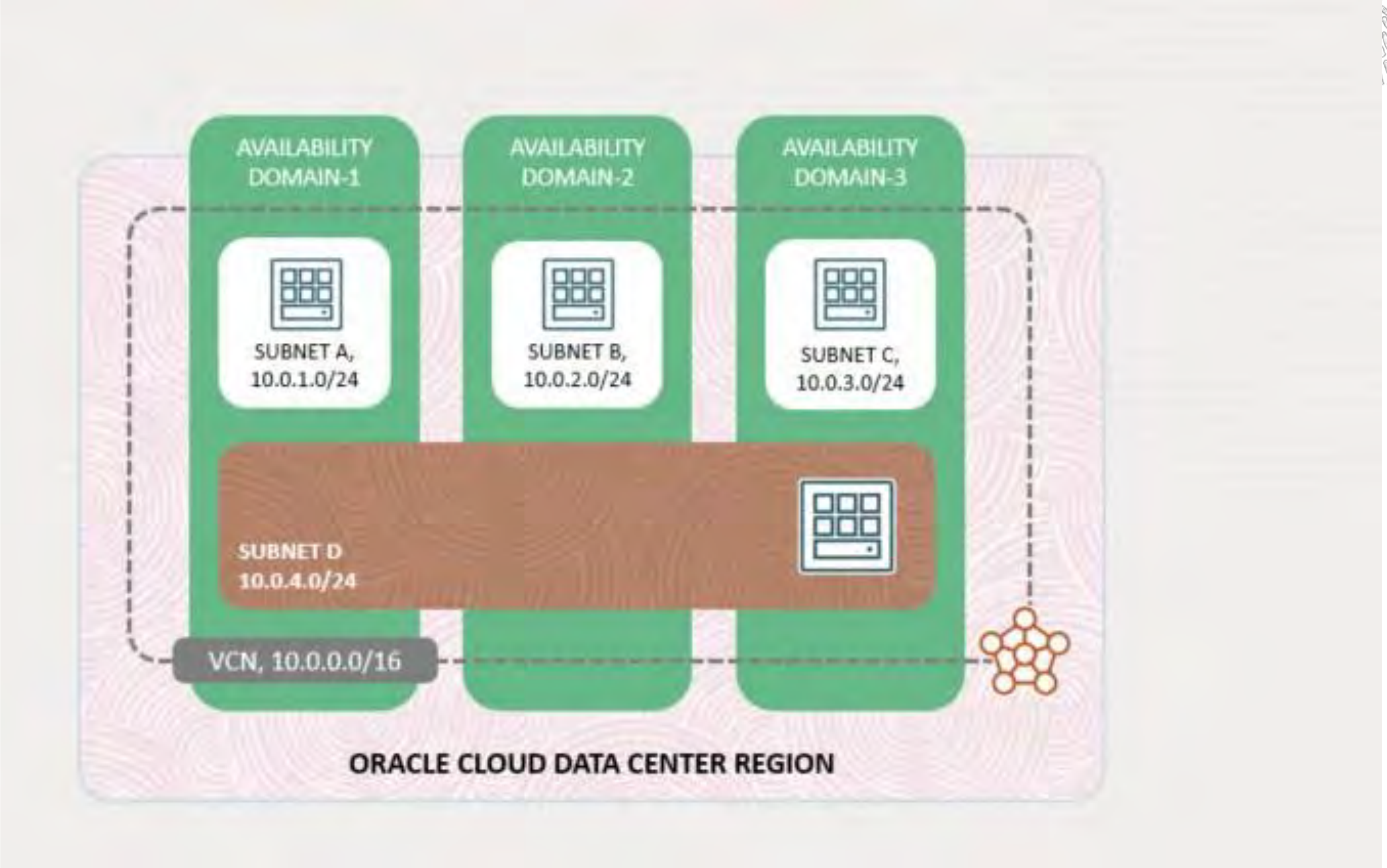
Secure Edge

- VPN / IPSEC
- VPN Log Analyser
- Bastion
- FastConnect
- IPSec over FC
- Network FaaS*
- HTTP Redirects
- WAF
    - Local WAF Policies
    - Threat Intelligence
- *NGFW*

Delivery

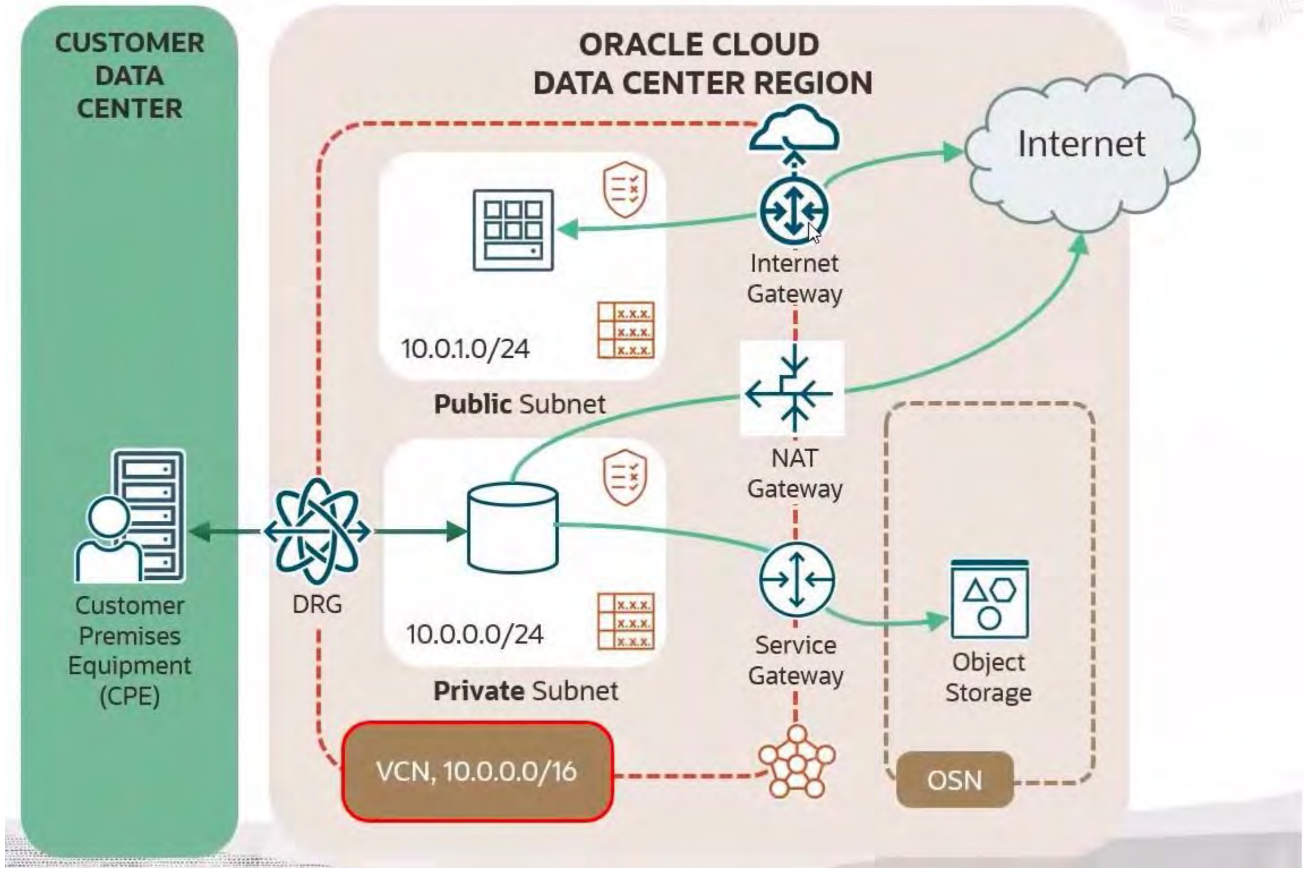
- *OCI CDN***
- DNS / Private DNS
- DNS Security*
- Load Balancing
    - HTTP LB
    - Network LB
- Traffic Management
    - Failover
    - Load Balancer
    - Geo Location Steering
    - ASN Steering
    - IP Prefix Steering

VCN és Subnet



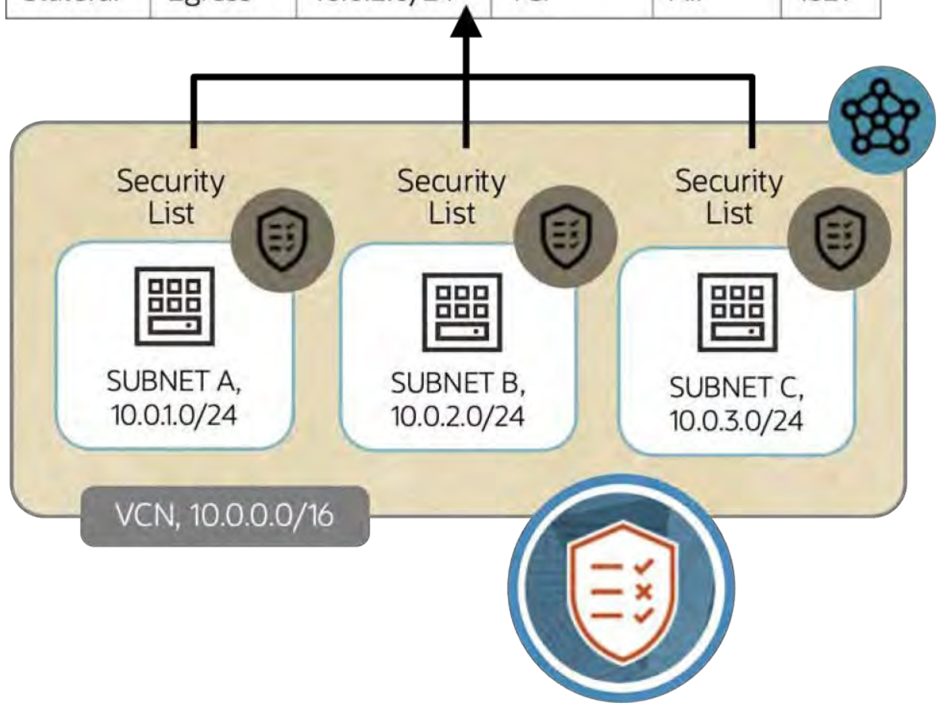
Gateway funkciók

Feature	Gateway to use	Comments
Traffic in and out of OCI. Can be initiated from OCI or internet	Internet Gateway	Need to have a public subnet and a resource with public IP
Resources in OCI who need access internet securely	NAT Gateway	Use private subnet, cannot receive internet traffic initiated from internet
Access to Object Storage or other Service in Oracle Service Network (OS management Service, Oracle Linux Yum Service etc...)	Service Gateway	List of services is long https://www.oracle.com/cloud/networking/service-gateway/service-gateway-supported-services
Connection between OCI and on-premise and between VCNs.	Dynamic Routing Gateway	This is a virtual router that connect VCNs and on-premise locations together. Central connection point that also connect between regions and different tenancies

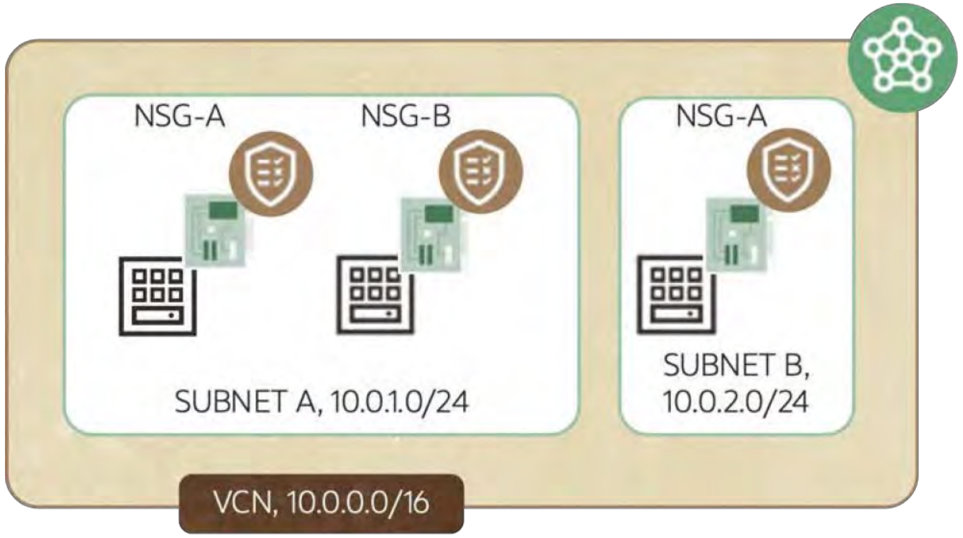


Security list és Network Security Group

	Direction	CIDR	Protocol	Source Port	Dest Port
Stateful	Ingress	0.0.0.0/0	TCP	All	80
Stateful	Egress	10.0.2.0/24	TCP	All	1521

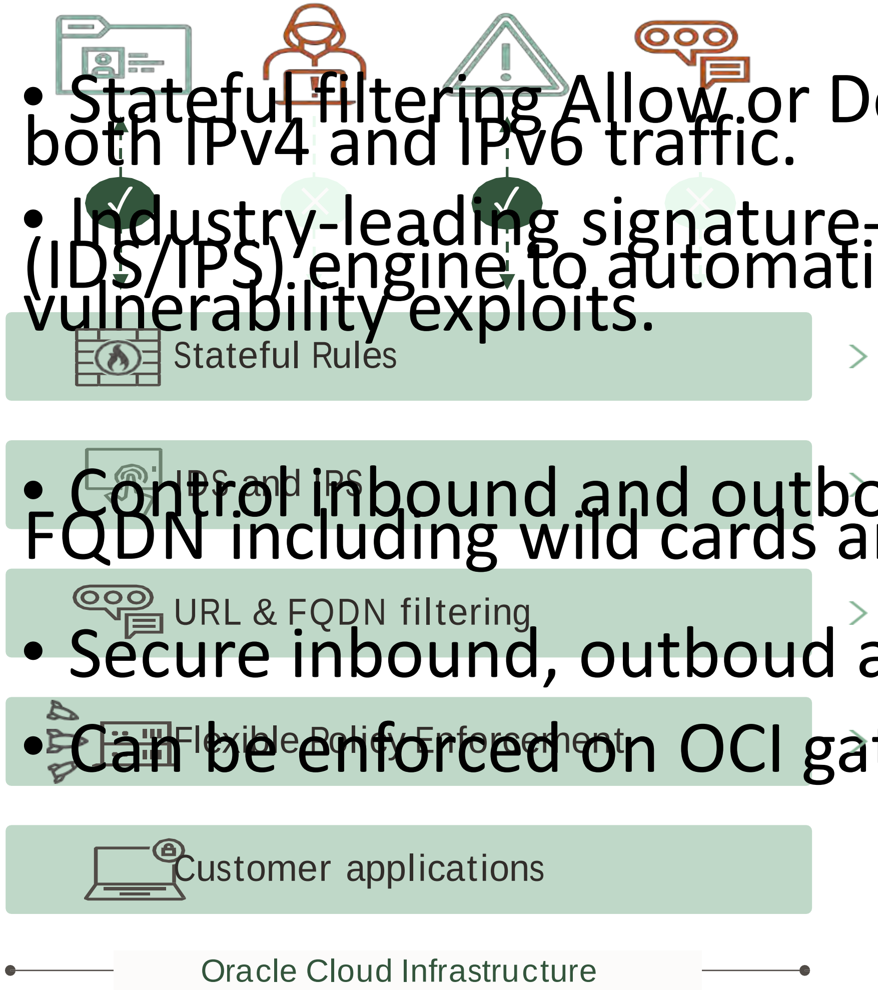


		Direction	CIDR	Protocol	Source Port	Dest Port
NSG-A	Stateful	Ingress	0.0.0.0/0	TCP	All	80
NSG-B	Stateful	Ingress	0.0.0.0/0	TCP	All	22

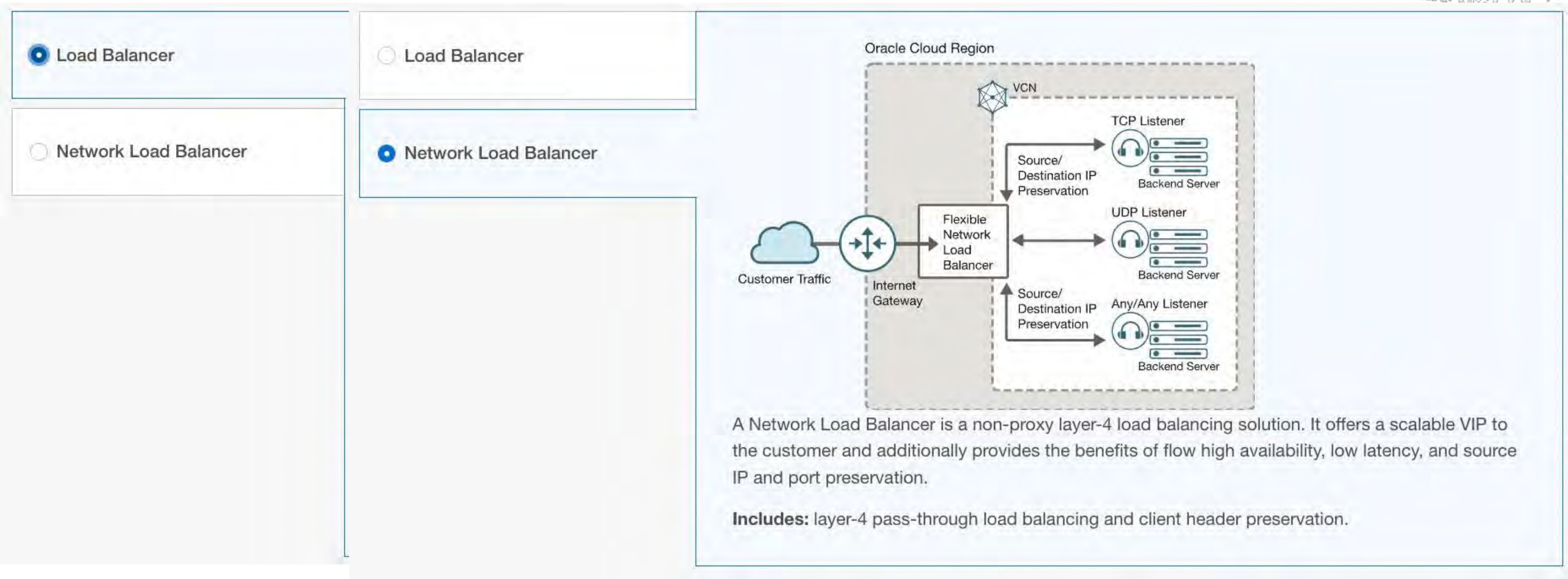


OCI Network Firewall

- Stateful filtering Allow or Deny rules based on 5-tuple information for both IPv4 and IPv6 traffic.
- Industry-leading signature-based threat detection and prevention (IDS/IPS) engine to automatically stop known malware, spyware, C2 and vulnerability exploits.
- Control inbound and outbound HTTP/S traffic to a specified list of FQDN including wild cards and custom URLs.
- Secure inbound, outboud and lateral network/application traffic.
- Can be enforced on OCI gateways as well as intra-vcn subnet traffic.



Load Balancer típusok



● Load Balancer

○ Network Load Balancer

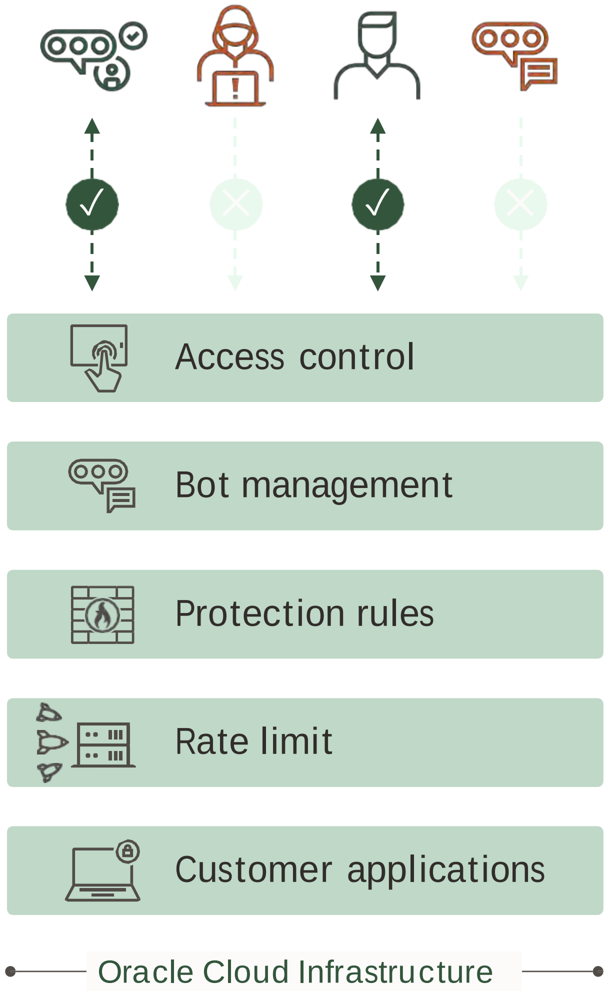
○ Load Balancer

● Network Load Balancer

A Network Load Balancer is a non-proxy layer-4 load balancing solution. It offers a scalable VIP to the customer and additionally provides the benefits of flow high availability, low latency, and source IP and port preservation.

Includes: layer-4 pass-through load balancing and client header preservation.

Web Application Firewall



Access control
- Restrict or control access to critical web applications, data and service

Bot management
- Identifies whether request are from a human or a machine
  Controls or blocks non-human suspicious requests

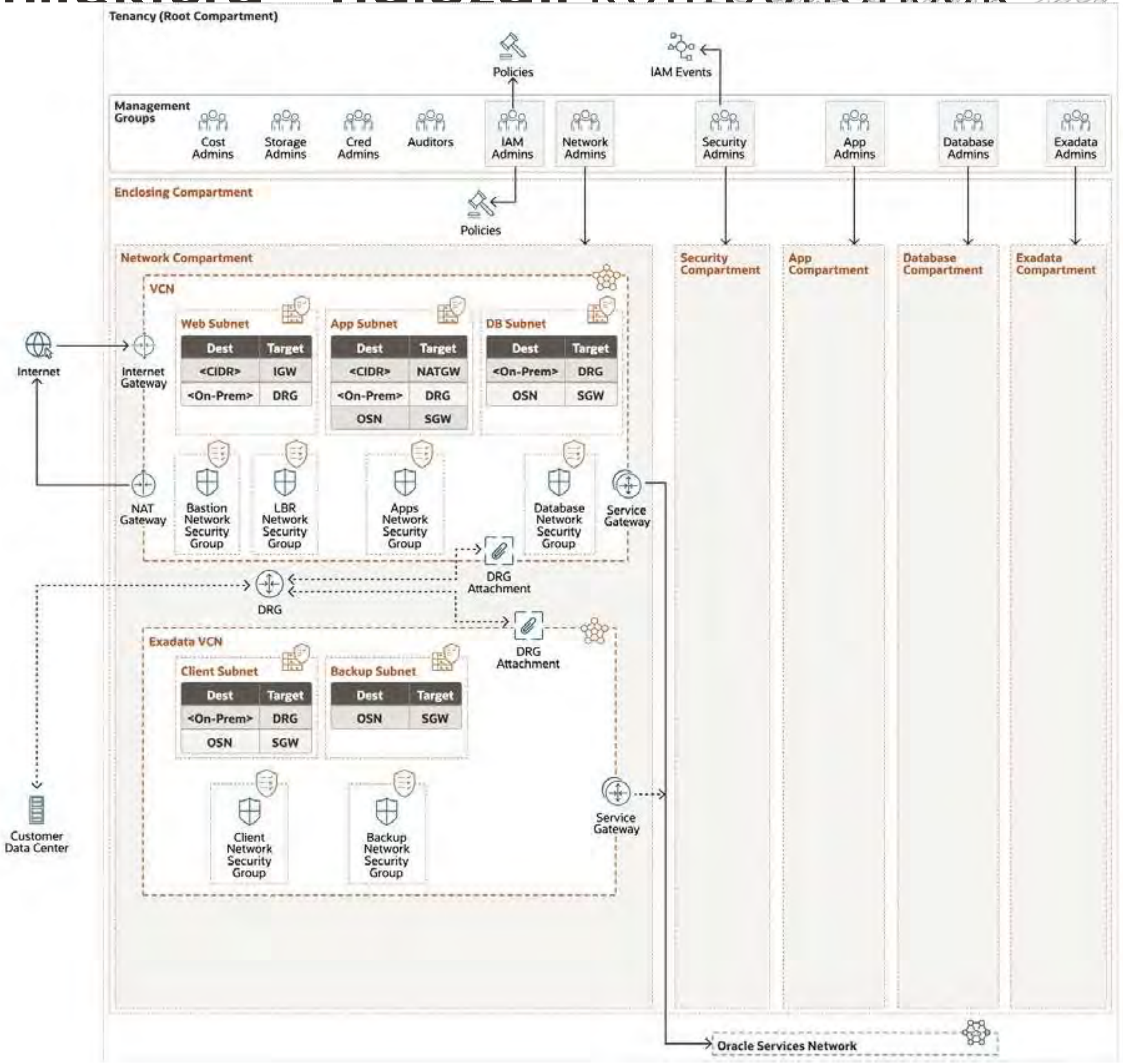
Protection rules
- Hides the origin server
  Inspects traffic as it tries to access the server or as it leaves the server

Rate limit
- Provides protection against L7 DDOS

Customer applications

Oracle Cloud Infrastructure

Landing Zone **architektúra – Hálózati** komponensek



Web Subnet

Dest	Target
<CIDR>	IGW
<On-Prem>	DRG

App Subnet

Dest	Target
<CIDR>	NATGW
<On-Prem>	DRG
OSN	SGW

DB Subnet

Dest	Target
<On-Prem>	DRG
OSN	SGW

Client Subnet

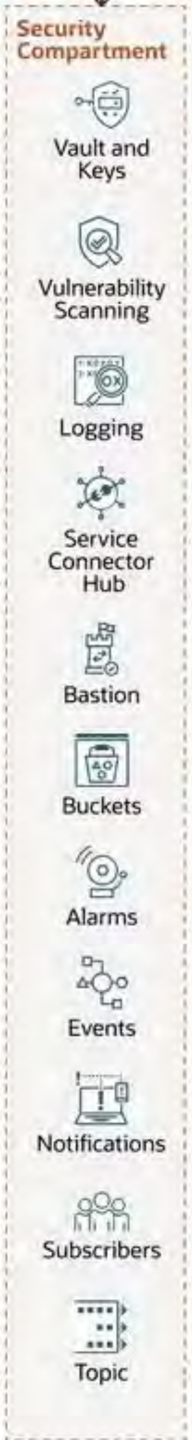
Dest	Target
<On-Prem>	DRG
OSN	SGW

Backup Subnet

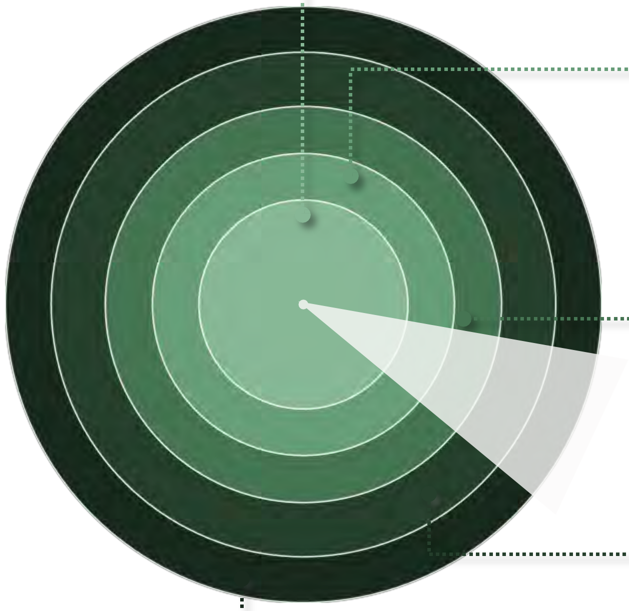
Dest	Target
OSN	SGW

Biztonsági funkciók

Vault, Cloud Guard, Security Zones, Vulnerability Scanning



Defense-in-depth, from data to the edge



Storage and Database Safeguards

- Data Safe
- Always-on at-rest, in-transit encryption
- Oracle-managed or customer-managed keys
- Integrated secrets management
- Cross-region replication
- Hardware security modules

Compute

- Hardware root of trust
- Signed firmware
- Off-box networking
- Harden disk images
- Autonomous Linux
- Certificates rotation

Network Security

- Virtual cloud network
- Interface segmentation
- Private networks
- FastConnect & IPSEC
- Secure VPN
- P2P, NAT, DRG gateways
- Bastion
- Network Firewall

Identity and Operator Access

- Identity and access management
- Identity federation
- Role-based policy
- Ephemeral bastions

Monitoring and Prevention

- Cloud Guard
- Custom Security Zones
- Cloud Guard Threat Detector
- Threat Intelligence
- Cloud Guard Fusion Apps Detector
- Built-in vulnerability scanning
- Logging/Flows
- Governance
- Compliance

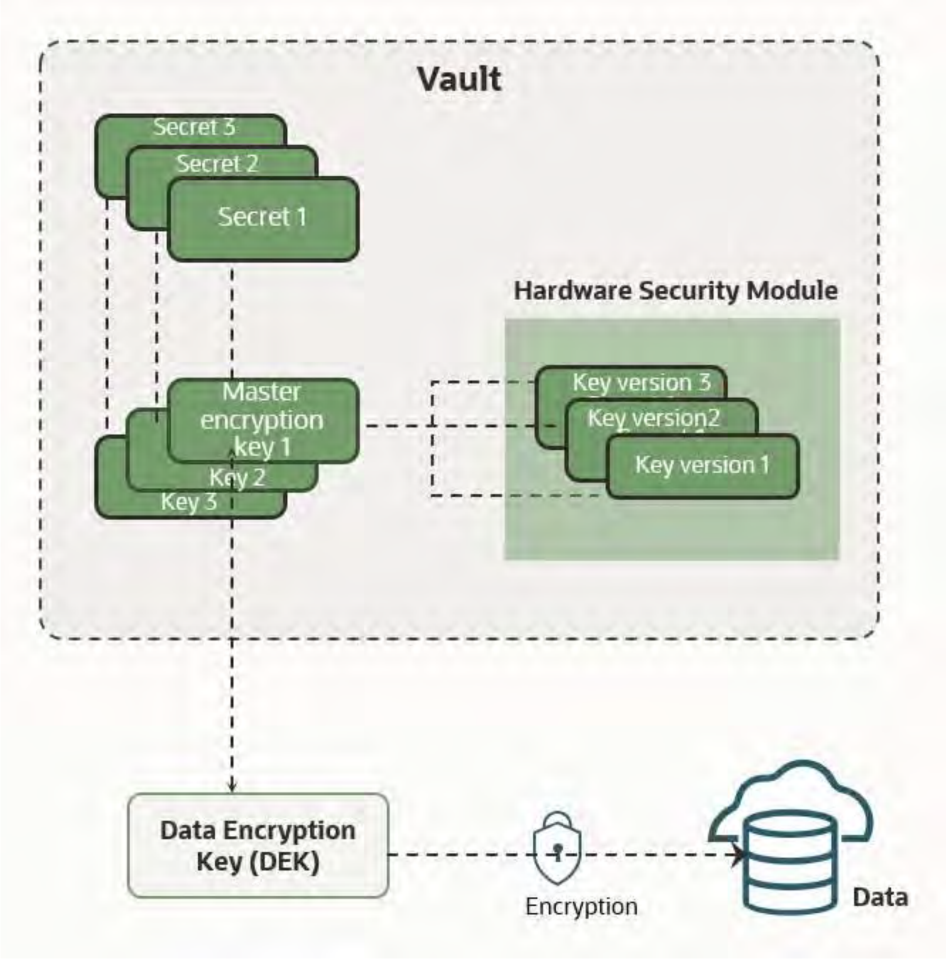
Internet and Edge

- DDoS protection
- SD-WAN
- Enhanced WAF protection

OCI Vault

Protect data and the secret credentials to securely access resources

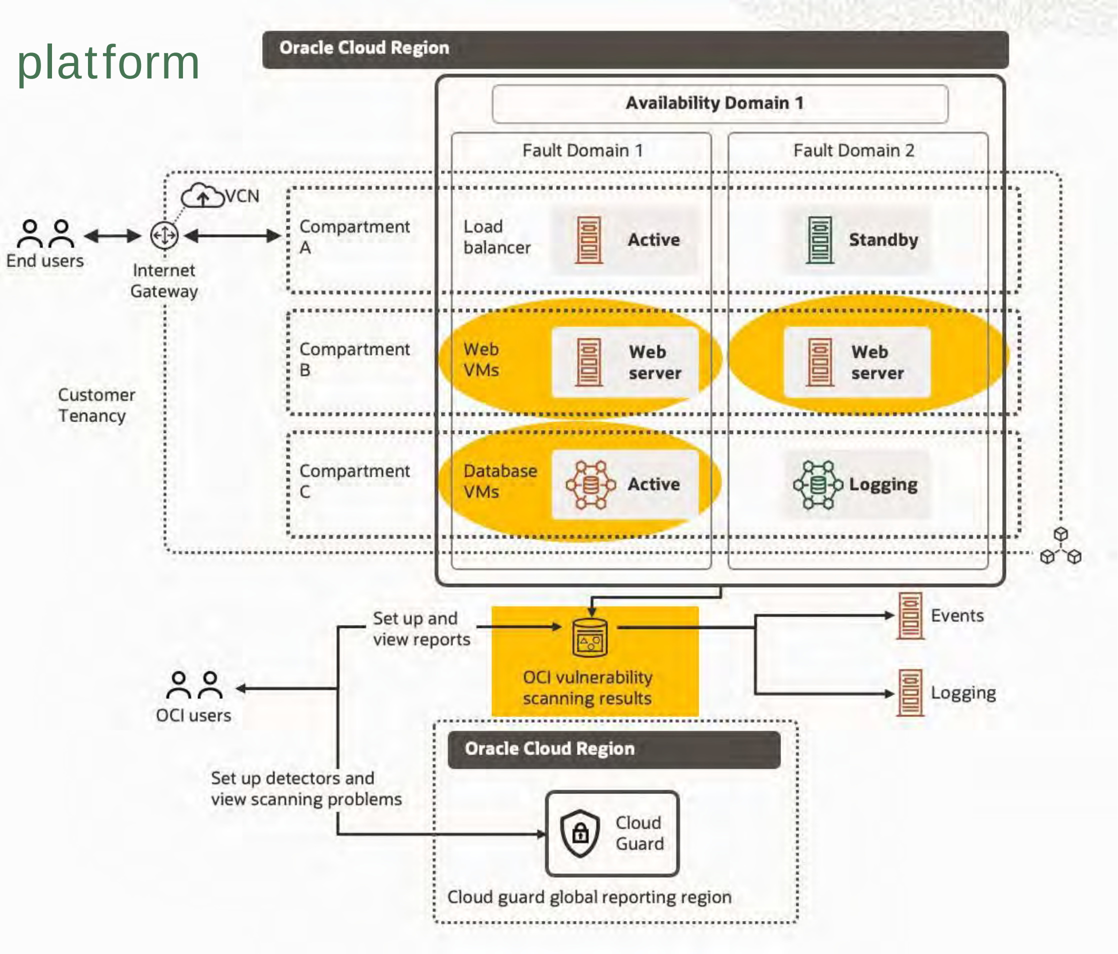
- Managed service that allows central management of master encryption keys
- Stores master encryption keys and secrets that might otherwise be stored in configuration files or in code
- Create and manage Vaults, Keys, and Secrets
- Centralized and customer controlled key management
  - Natively integrated to many OCI services: OCI-Native Storage, DBaaS (ADB-D, ExaCS), OKE, Streams
- Shared or isolated
  - Virtual private vault is an isolated partition on a hardware security module (HSM). Vaults otherwise share partitions on the HSM with other vaults
- Support regulatory compliance
  - Meets PCI DSS and FIPS 140-2 Level 3 standard for cryptographic processing



OCI Vulnerability Scanning Service

Free scanning suite that is tightly integrated with the OCI platform

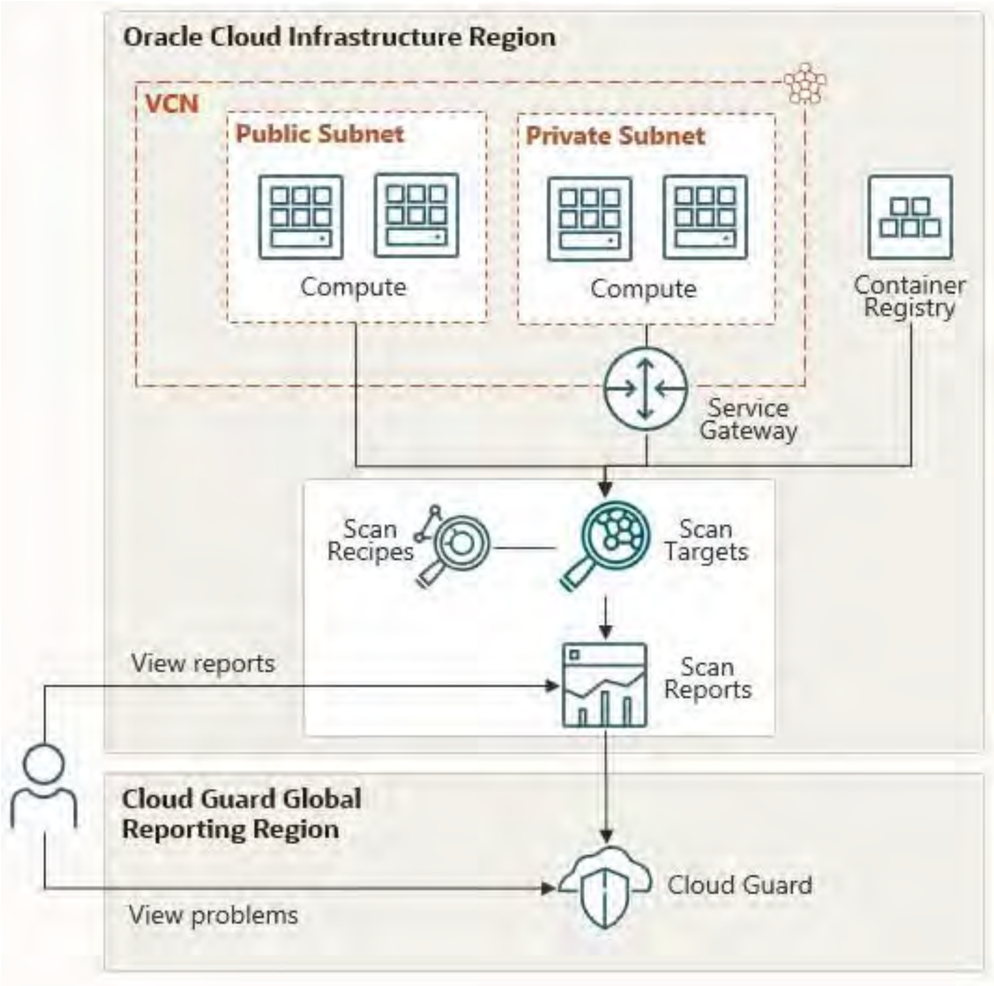
- Oracle Cloud Infrastructure Vulnerability Scanning Service helps improve your security posture by routinely checking hosts and container images for potential vulnerabilities
- Visibility into misconfigured or vulnerable resources
- Scan results are also visible as problems in your Cloud Guard global reporting region
- The Scanning service can identify several types of security issues:
  - Ports that are unintentionally left open
  - OS packages that require updates and patches to address vulnerabilities
  - OS configurations that hackers might exploit
  - Industry-standard benchmarks published by the Center for Internet Security (CIS)
  - Vulnerabilities in third-party applications such as log4j and spring4shell



The Scanning service only supports compute instances created from supported platform images. Scanning isn't available for any image with the label end of support.

To scan a compute instance for vulnerabilities, the instance must use an image that supports Oracle Cloud Agent.

OCI Vulnerability Scanning Service



Scan Recipe

Scanning parameters for a type of cloud resource, including what information to examine and how often.

Target

One or more cloud resources that you want to scan using a specific recipe. Resources in a target are of the same type, such as compute instances.

Host Scan

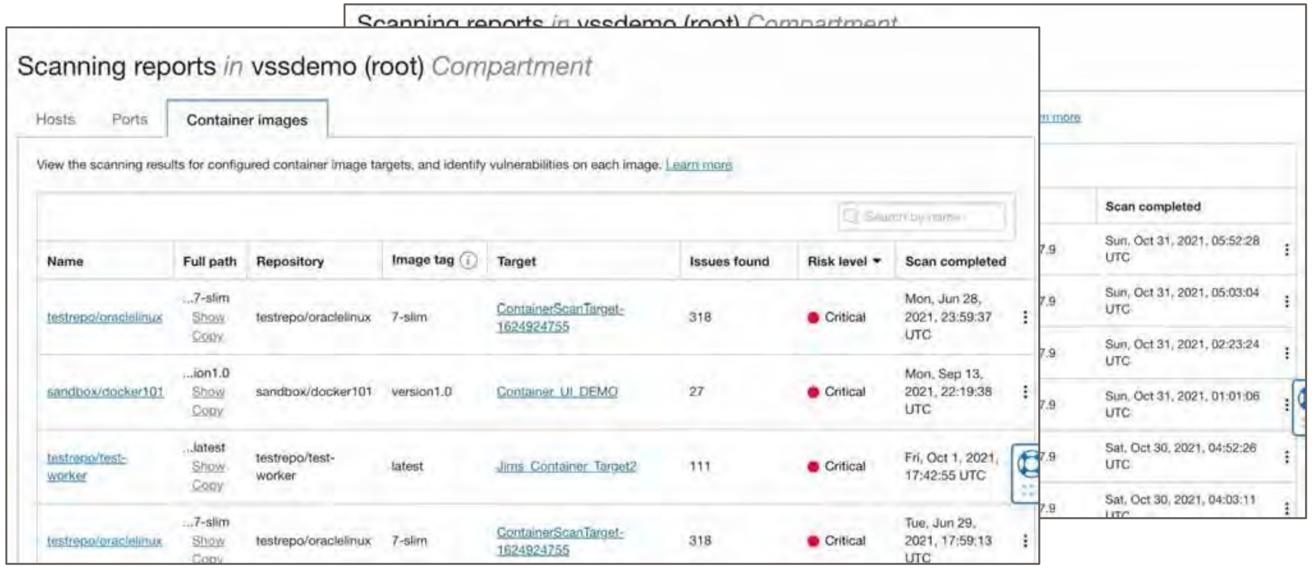
Metrics about a specific compute instance that was scanned, including the vulnerabilities that were found, their risk levels, and CIS benchmark compliance.

Container Image Scan

Metrics about a specific Container Registry image that was scanned, including the vulnerabilities that were found and their risk levels.

Vulnerabilities Report

Information about a specific type of vulnerability that was detected in one or more targets, like a missing update for an OS package.



Scanning reports *in* vssdemo (root) *Compartment*

View the scanning results for configured container image targets, and identify vulnerabilities on each image. Learn more

Name	Full path	Repository	Image tag	Target	Issues found	Risk level	Scan completed
testrepo/oraclelinux	...7-slim Show Copy	testrepo/oraclelinux	7-slim	ContainerScanTarget-1624924755	318	● Critical	Mon, Jun 28, 2021, 23:59:37 UTC
sandbox/docker101	...ion1.0 Show Copy	sandbox/docker101	version1.0	Container_UI_DEMO	27	● Critical	Mon, Sep 13, 2021, 22:19:38 UTC
testrepo/test-worker	...latest Show Copy	testrepo/test-worker	latest	Jims_Container_Target2	111	● Critical	Fri, Oct 1, 2021, 17:42:55 UTC
testrepo/oraclelinux	...7-slim Show Copy	testrepo/oraclelinux	7-slim	ContainerScanTarget-1624924755	318	● Critical	Tue, Jun 29, 2021, 17:59:13 UTC

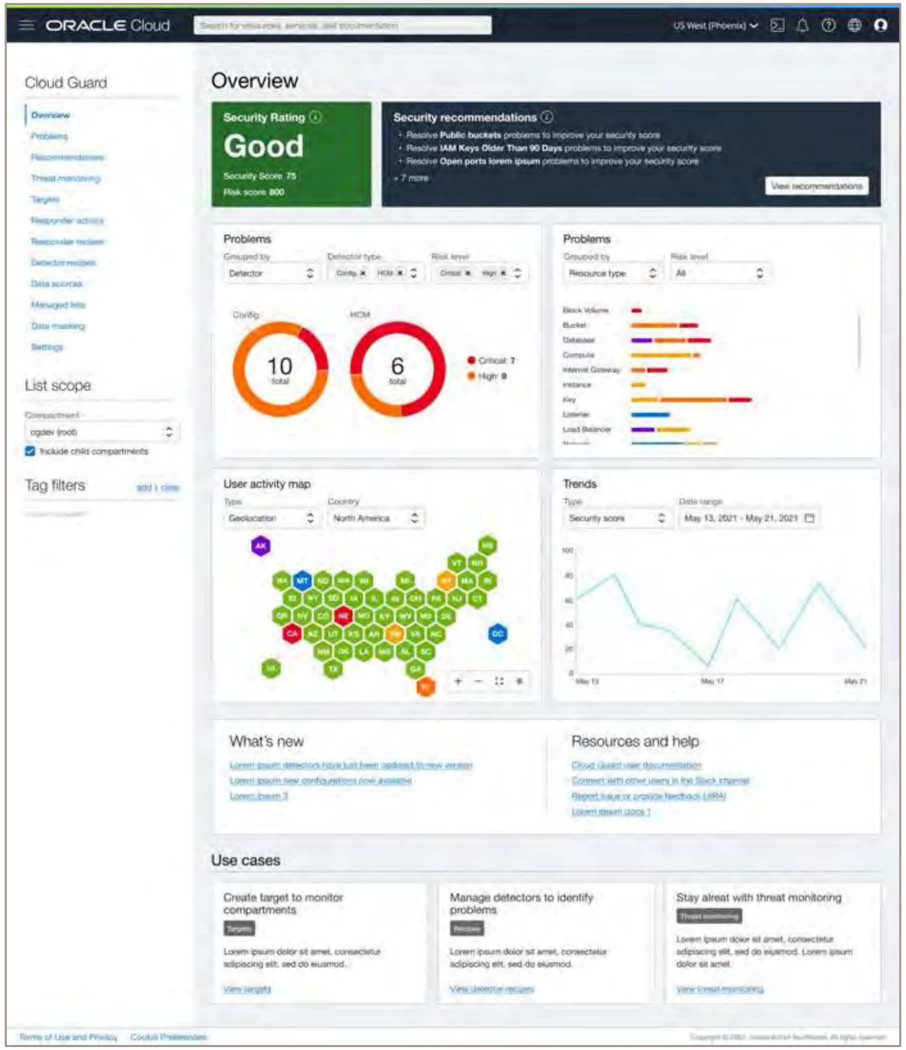
Scanning reports *in* vssdemo (root) *Compartment*

	Scan completed
7.9	Sun, Oct 31, 2021, 05:52:28 UTC
7.9	Sun, Oct 31, 2021, 05:03:04 UTC
7.9	Sun, Oct 31, 2021, 02:23:24 UTC
7.9	Sun, Oct 31, 2021, 01:01:06 UTC
7.9	Sat, Oct 30, 2021, 04:52:26 UTC
7.9	Sat, Oct 30, 2021, 04:03:11 UTC

Oracle Cloud Guard

Cloud Guard helps you maintain good security posture by detecting misconfigured resources, insecure activity drifts, and malicious behaviors.

- Consolidated view: A single pane of glass to view global security concerns
- Easy to use: Out of the box recipes to find common issues with notification & remediation features to drive fixes
- Inexpensive: Provided for no-charge to paid OCI tenancies



- Resolve **Public buckets** problems to improve your security score
- Resolve **IAM Keys Older Than 90 Days** problems to improve your security score
- Resolve **Open ports lorem ipsum** problems to improve your security score
- + 7 more

Lorem ipsum detectors have just been updated to new version
Lorem ipsum new configurations now available
Lorem ipsum 3

Cloud Guard user documentation
Connect with other users in the Slack channel
Report issue or provide feedback (JIRA)
Lorem ipsum docs 1

Create target to monitor compartments
Targets
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod.
View targets

Manage detectors to identify problems
Recipes
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod.
View detector recipes

Stay alert with threat monitoring
Threat monitoring
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod. Lorem ipsum dolor sit amet.
View threat monitoring

Cloud Guard Terms

Targets

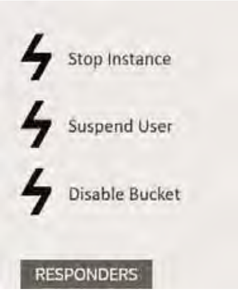
Targets set the scope of resources to be examined. For OCI, compartments and their descendent structures are used.

Detectors

Detectors are Cloud Guard components that identify issues with resources or user actions and alert when an issue is found

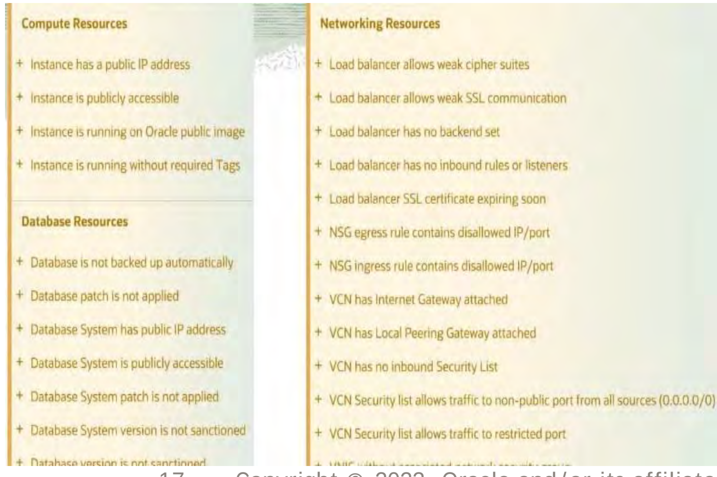
Problems

Problems are notifications that a configuration or activity is a potential security issue.



Responses

Responders provide notifications and corrective actions to for security problems.



Compute Resources

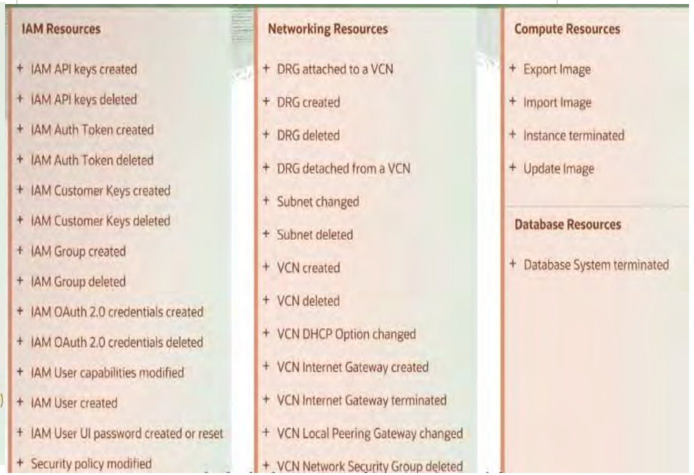
- Instance has a public IP address
- Instance is publicly accessible
- Instance is running on Oracle public image
- Instance is running without required Tags

Database Resources

- Database is not backed up automatically
- Database patch is not applied
- Database System has public IP address
- Database System is publicly accessible
- Database System patch is not applied
- Database System version is not sanctioned
- Database version is not sanctioned

Networking Resources

- Load balancer allows weak cipher suites
- Load balancer allows weak SSL communication
- Load balancer has no backend set
- Load balancer has no inbound rules or listeners
- Load balancer SSL certificate expiring soon
- NSG egress rule contains disallowed IP/port
- NSG ingress rule contains disallowed IP/port
- VCN has Internet Gateway attached
- VCN has Local Peering Gateway attached
- VCN has no inbound Security List
- VCN Security list allows traffic to non-public port from all sources (0.0.0.0/0)
- VCN Security list allows traffic to restricted port



IAM Resources

- IAM API keys created
- IAM API keys deleted
- IAM Auth Token created
- IAM Auth Token deleted
- IAM Customer Keys created
- IAM Customer Keys deleted
- IAM Group created
- IAM Group deleted
- IAM OAuth 2.0 credentials created
- IAM OAuth 2.0 credentials deleted
- IAM User capabilities modified
- IAM User created
- IAM User UI password created or reset
- Security policy modified

Networking Resources

- DRG attached to a VCN
- DRG created
- DRG deleted
- DRG detached from a VCN
- Subnet changed
- Subnet deleted
- VCN created
- VCN deleted
- VCN DHCP Option changed
- VCN Internet Gateway created
- VCN Internet Gateway terminated
- VCN Local Peering Gateway changed
- VCN Network Security Group deleted

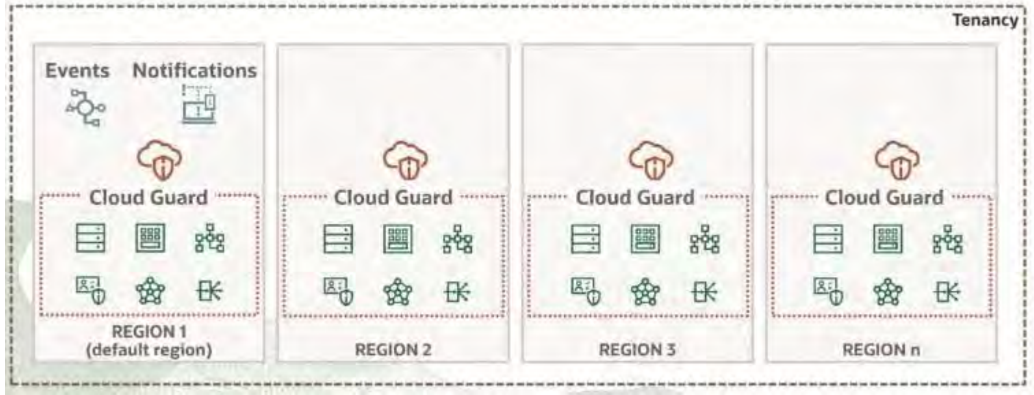
Compute Resources

- Export Image
- Import Image
- Instance terminated
- Update Image

Database Resources

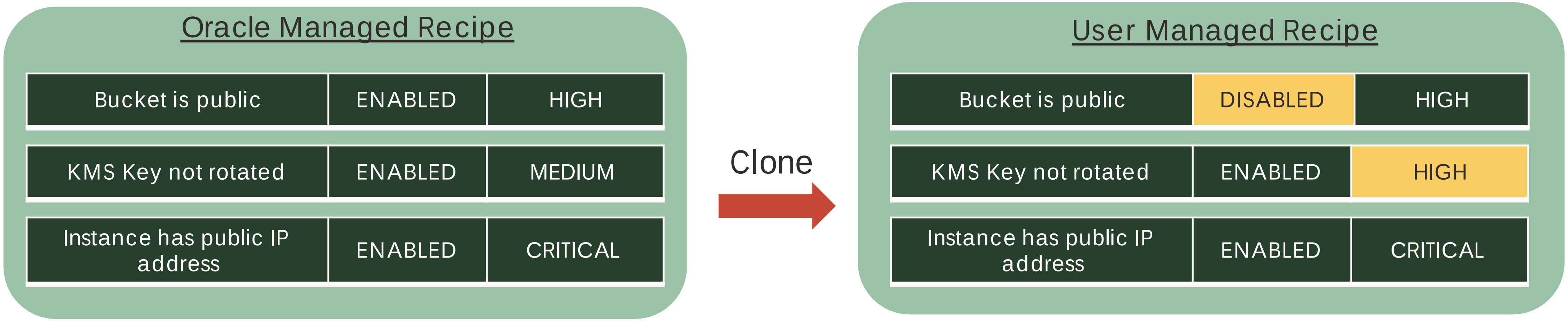
- Database System terminated

Targets in all regions can be monitored, though the reporting region is the default region of the tenancy. Integration with Events and Notification services happen only in the Reporting Region.



Detector Recipes

- Cloud Guard provides a global set of Configuration and Activity detectors in an Oracle-managed recipe upon enablement.
- There are two types of detector recipes in Cloud Guard:
  - Oracle Managed
  - User Managed Recipes
- In the User Managed recipes, users can enable/disable, change risk level, apply conditional parameters, and make other changes.
- Users can then apply that customized recipe to their targets instead of using the Oracle Managed Recipe.



Oracle Managed Recipe

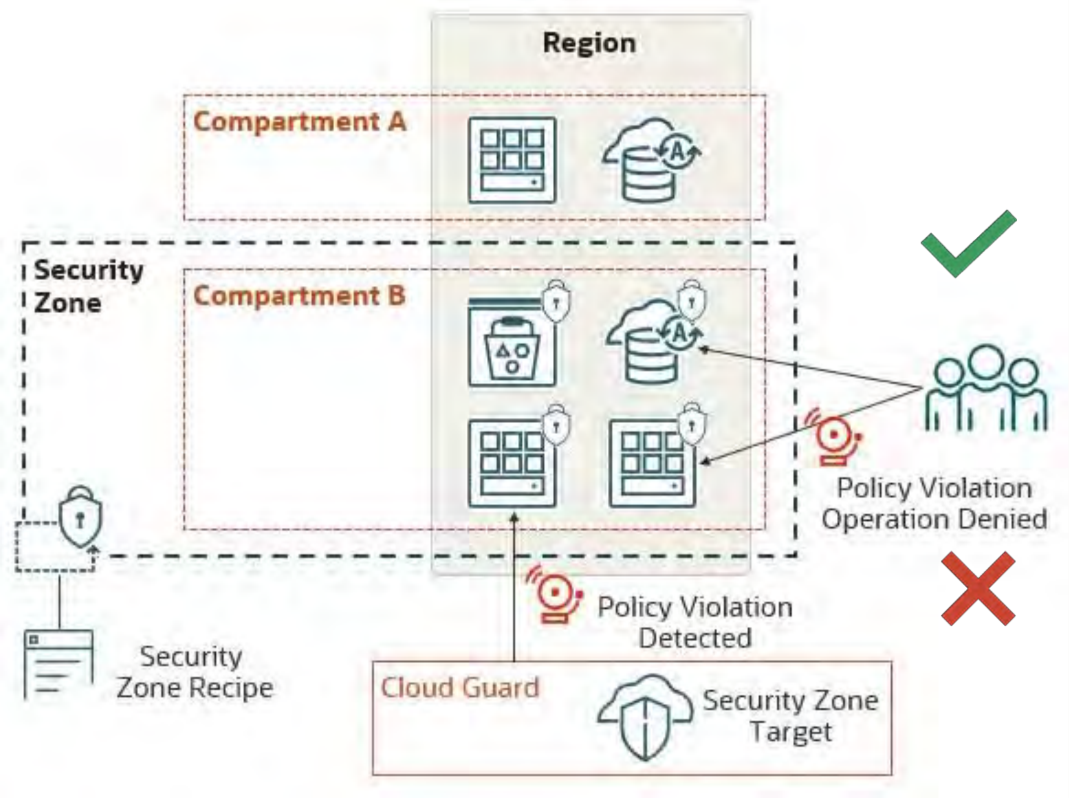
Bucket is public	ENABLED	HIGH
KMS Key not rotated	ENABLED	MEDIUM
Instance has public IP address	ENABLED	CRITICAL

User Managed Recipe

Bucket is public	DISABLED	HIGH
KMS Key not rotated	ENABLED	HIGH
Instance has public IP address	ENABLED	CRITICAL

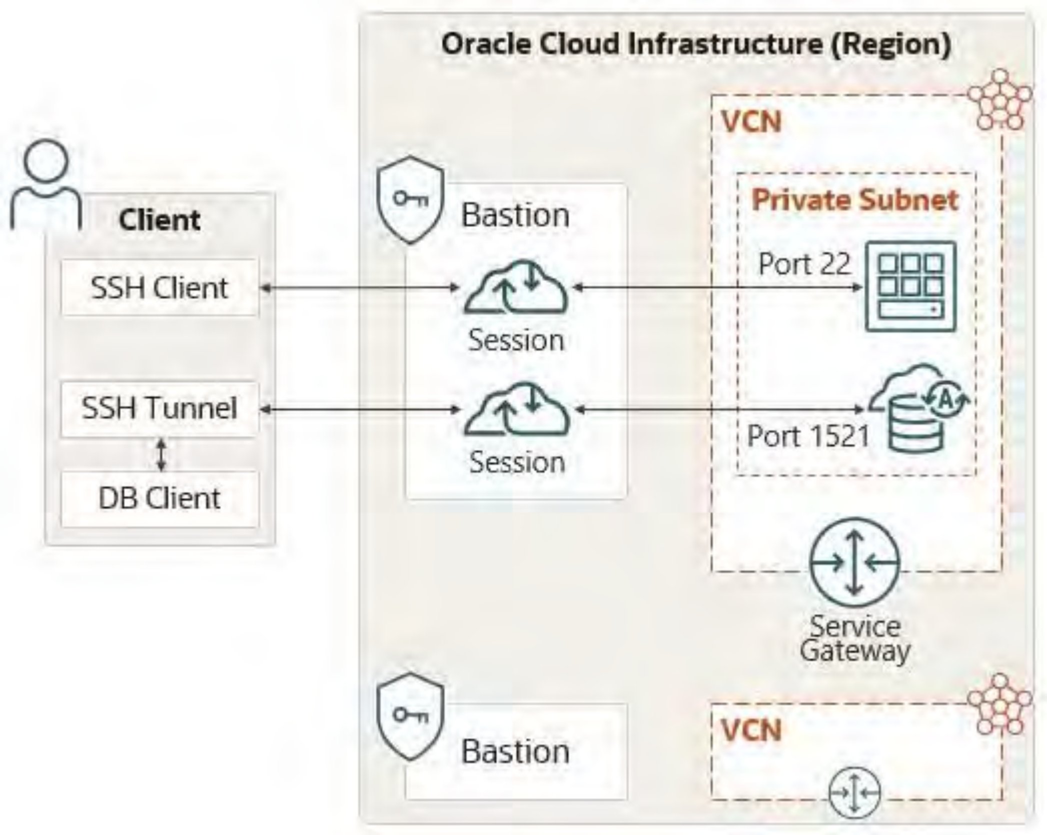
Security Zone

- Security Zones let you be confident that your Compute, Networking, Object Storage, Database, and other resources comply with Oracle security principles and best practices.
- A security zone is associated with one or more compartments and a security zone recipe.
- When you create and update resources in a security zone, Oracle Cloud Infrastructure validates these operations against security zone policies in the zone's recipe.
- If any security zone policy is violated, then the operation is denied.

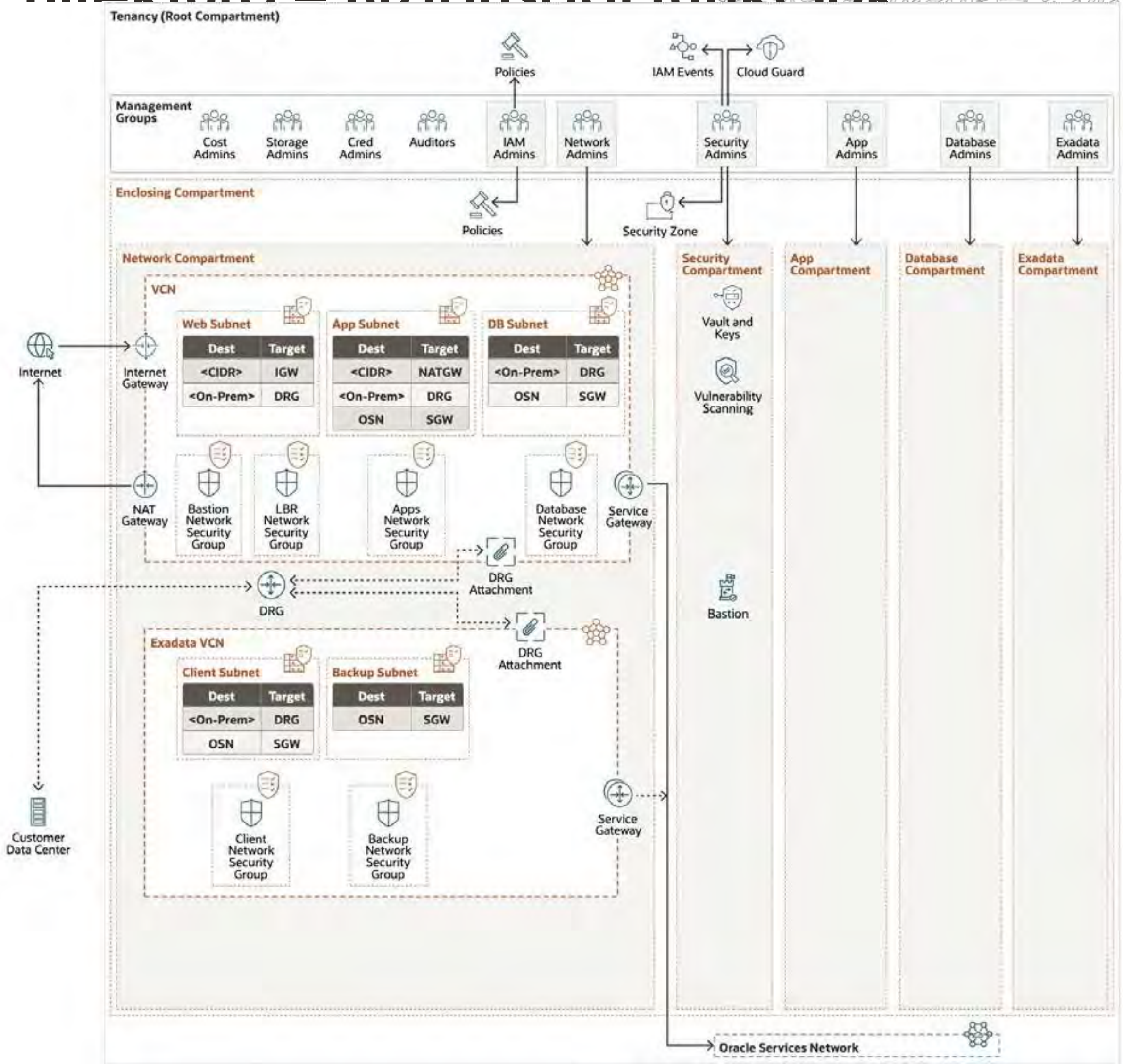


What is OCI Bastion?

- OCI Bastion is a fully managed OCI service which improves the security posture of the hosts in OCI by providing secure access to the private target hosts within the customer VCN.
- OCI Bastion is a core cloud infrastructure security product.
- The access to the target hosts via Bastions is time-bound. The access is governed by OCI IAM policies.
- You can restrict the incoming SSH connections to certain IPv4 address ranges.
- All administrative actions like who/when created/deleted/updated/fetched bastion and session are recorded in OCI Event and Audit service



Landing Zone architektúra – Biztonsági funkciók



Web Subnet

Dest	Target
<CIDR>	IGW
<On-Prem>	DRG

App Subnet

Dest	Target
<CIDR>	NATGW
<On-Prem>	DRG
OSN	SGW

DB Subnet

Dest	Target
<On-Prem>	DRG
OSN	SGW

Client Subnet

Dest	Target
<On-Prem>	DRG
OSN	SGW

Backup Subnet

Dest	Target
OSN	SGW

Felügyelet és riasztás

Logging, Monitoring, Alarms

Logging

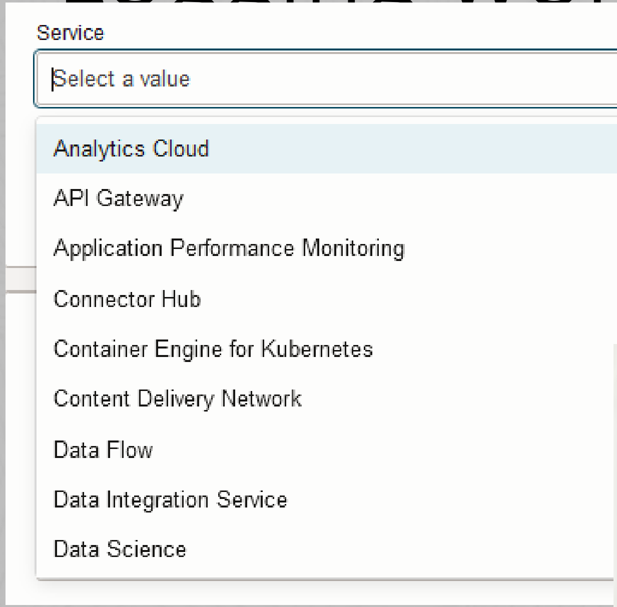
A *log* is a first-class Oracle Cloud Infrastructure resource that stores and captures log events collected in a given context. For example, if you enable Flow Logs on a subnet, it has its own dedicated log. Each log has an OCID and is stored in a log group. A *log group* is a collection of logs stored in a compartment. Logs and log groups are searchable, actionable, and transportable.

- Audit logs: Logs related to events emitted by the Oracle Cloud Infrastructure Audit service.
- Service logs: Emitted by OCI native services, such as API Gateway, Events, Functions, Load Balancer, Object Storage, and VCN Flow Logs.
- Custom logs: Logs that contain diagnostic information from custom applications, other cloud providers, or an on-premises environment (Unified Monitoring Agent).

Logical grouping: When you enable a log, you must add it to a log group that you create. *Log groups* are logical containers for logs.

Search: You can view and search logs on the Logging Search page. When searching logs, you can correlate across many logs simultaneously.

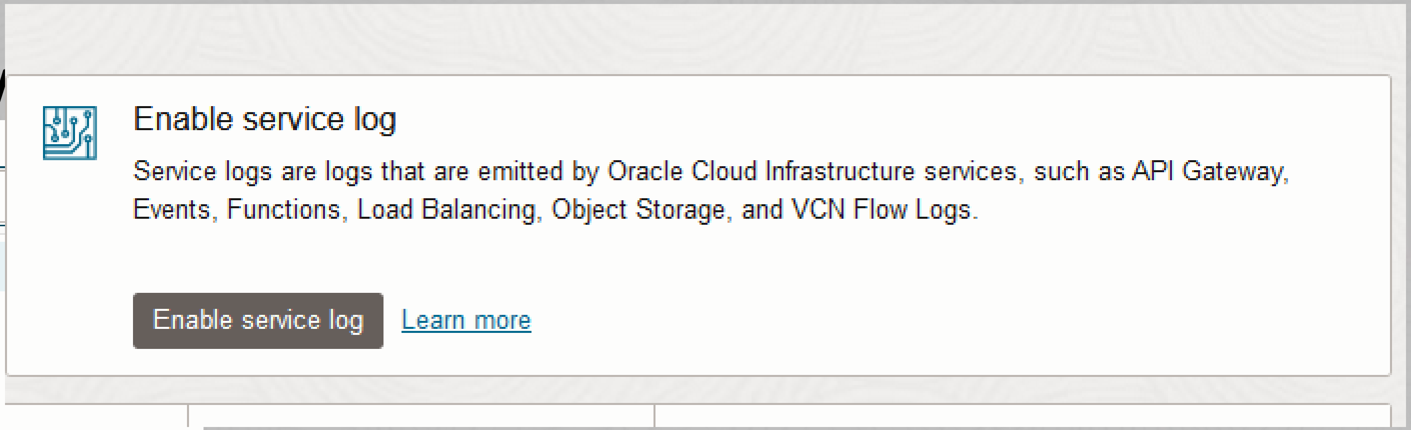
Logging workflow



Service

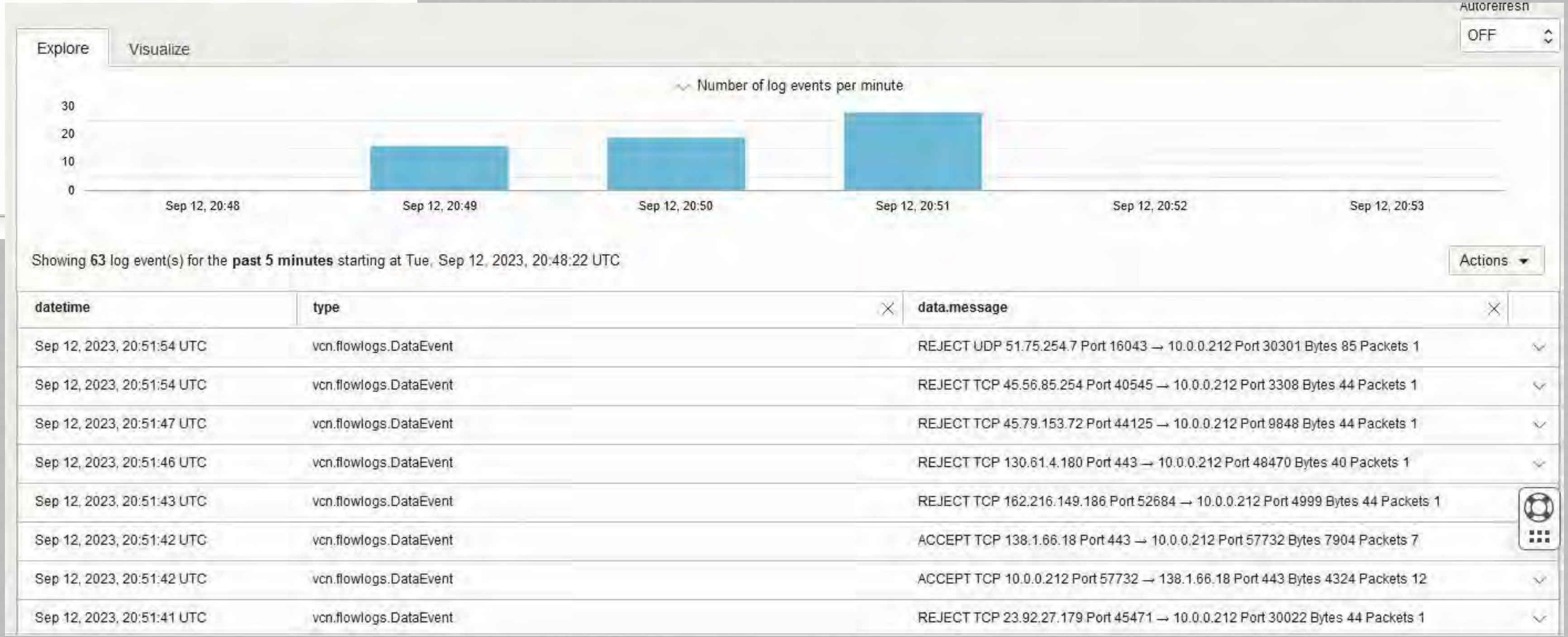
Select a value

- Analytics Cloud
- API Gateway
- Application Performance Monitoring
- Connector Hub
- Container Engine for Kubernetes
- Content Delivery Network
- Data Flow
- Data Integration Service
- Data Science



Enable service log

Service logs are logs that are emitted by Oracle Cloud Infrastructure services, such as API Gateway, Events, Functions, Load Balancing, Object Storage, and VCN Flow Logs.



Showing **63** log event(s) for the **past 5 minutes** starting at Tue, Sep 12, 2023, 20:48:22 UTC

datetime	type	data.message
Sep 12, 2023, 20:51:54 UTC	vcn.flowlogs.DataEvent	REJECT UDP 51.75.254.7 Port 16043 → 10.0.0.212 Port 30301 Bytes 85 Packets 1
Sep 12, 2023, 20:51:54 UTC	vcn.flowlogs.DataEvent	REJECT TCP 45.56.85.254 Port 40545 → 10.0.0.212 Port 3308 Bytes 44 Packets 1
Sep 12, 2023, 20:51:47 UTC	vcn.flowlogs.DataEvent	REJECT TCP 45.79.153.72 Port 44125 → 10.0.0.212 Port 9848 Bytes 44 Packets 1
Sep 12, 2023, 20:51:46 UTC	vcn.flowlogs.DataEvent	REJECT TCP 130.61.4.180 Port 443 → 10.0.0.212 Port 48470 Bytes 40 Packets 1
Sep 12, 2023, 20:51:43 UTC	vcn.flowlogs.DataEvent	REJECT TCP 162.216.149.186 Port 52684 → 10.0.0.212 Port 4999 Bytes 44 Packets 1
Sep 12, 2023, 20:51:42 UTC	vcn.flowlogs.DataEvent	ACCEPT TCP 138.1.66.18 Port 443 → 10.0.0.212 Port 57732 Bytes 7904 Packets 7
Sep 12, 2023, 20:51:42 UTC	vcn.flowlogs.DataEvent	ACCEPT TCP 10.0.0.212 Port 57732 → 138.1.66.18 Port 443 Bytes 4324 Packets 12
Sep 12, 2023, 20:51:41 UTC	vcn.flowlogs.DataEvent	REJECT TCP 23.92.27.179 Port 45471 → 10.0.0.212 Port 30022 Bytes 44 Packets 1

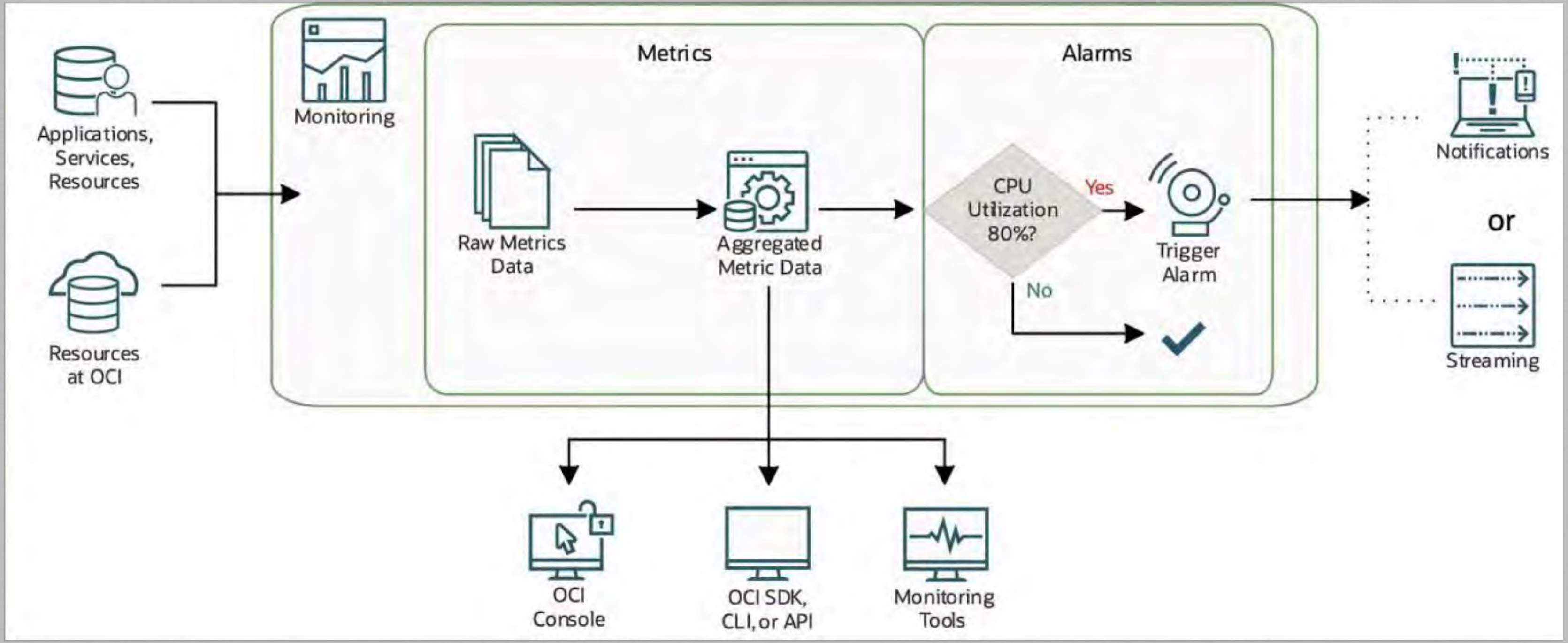
1. Create Log Group & policies
2. Enable logging for Cloud service
3. Create custom log agent
4. Review Log data

Monitoring

The Monitoring service uses metrics to monitor resources and alarms to notify you when these metrics meet alarm-specified triggers.

Metrics come from a variety of sources:

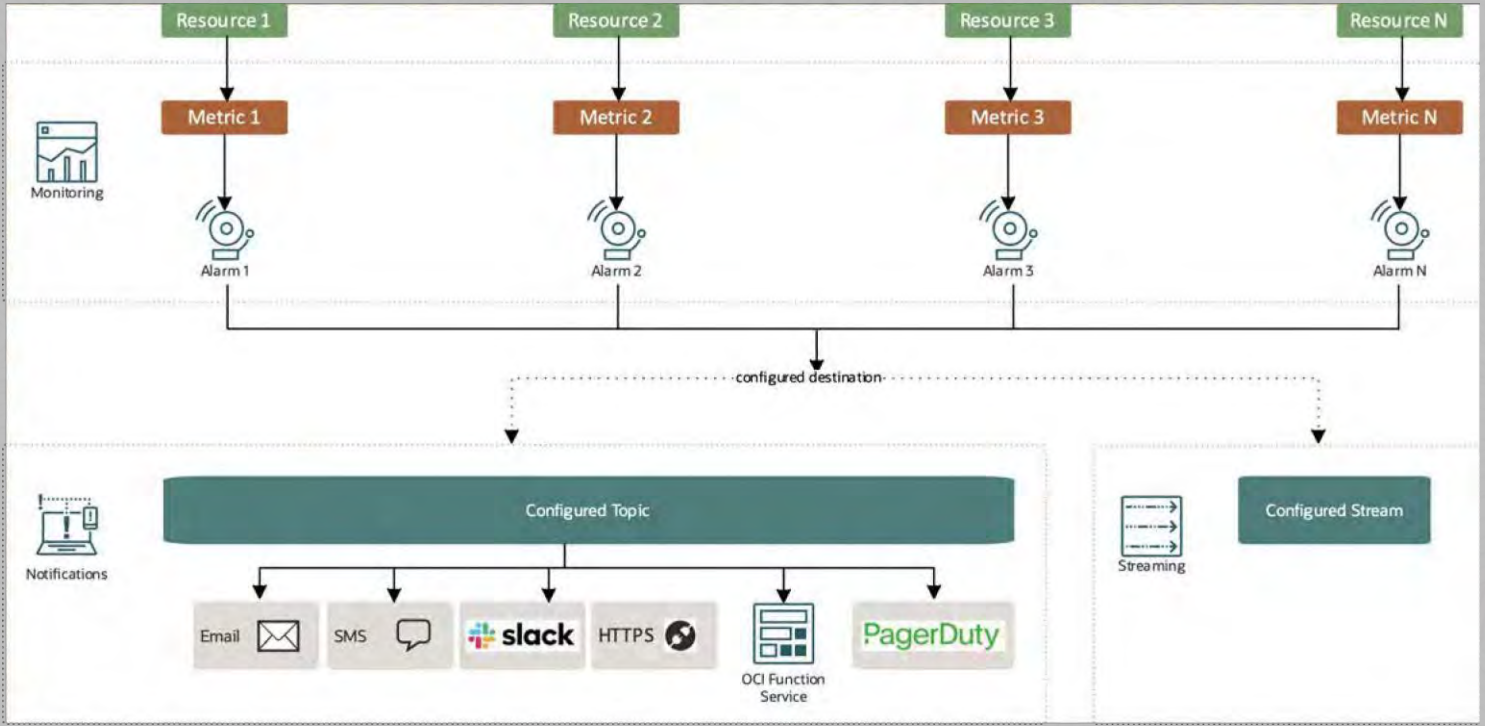
- Resource metrics automatically posted by Oracle Cloud Infrastructure resources. (For example, the Compute service posts metrics for monitoring-enabled compute instances through the oci_computeagent namespace. One such metric is CpuUtilization.)
- Custom metrics published using the Monitoring API or CLI.
- Data sent to new or existing metrics using Connector Hub (with Monitoring as the target service for a connector).



Alarms

The Alarms feature of the Monitoring service publishes alarm messages to configured destinations, such as topics in Notifications and streams in Streaming.

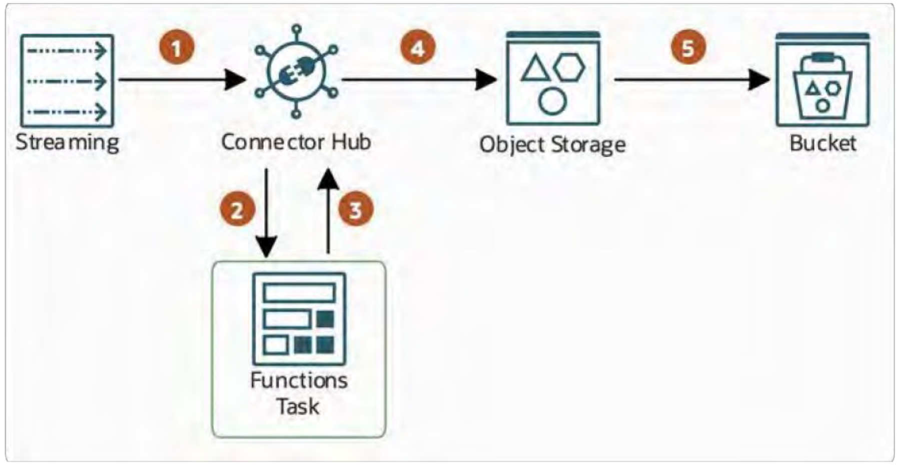
- The Alarms feature of the Monitoring service works with the configured destination service to notify you when metrics meet alarm-specified triggers.
- When triggered, an alarm sends an alarm message to the configured destination.
- For Notifications, messages are sent to subscriptions in the configured topic.

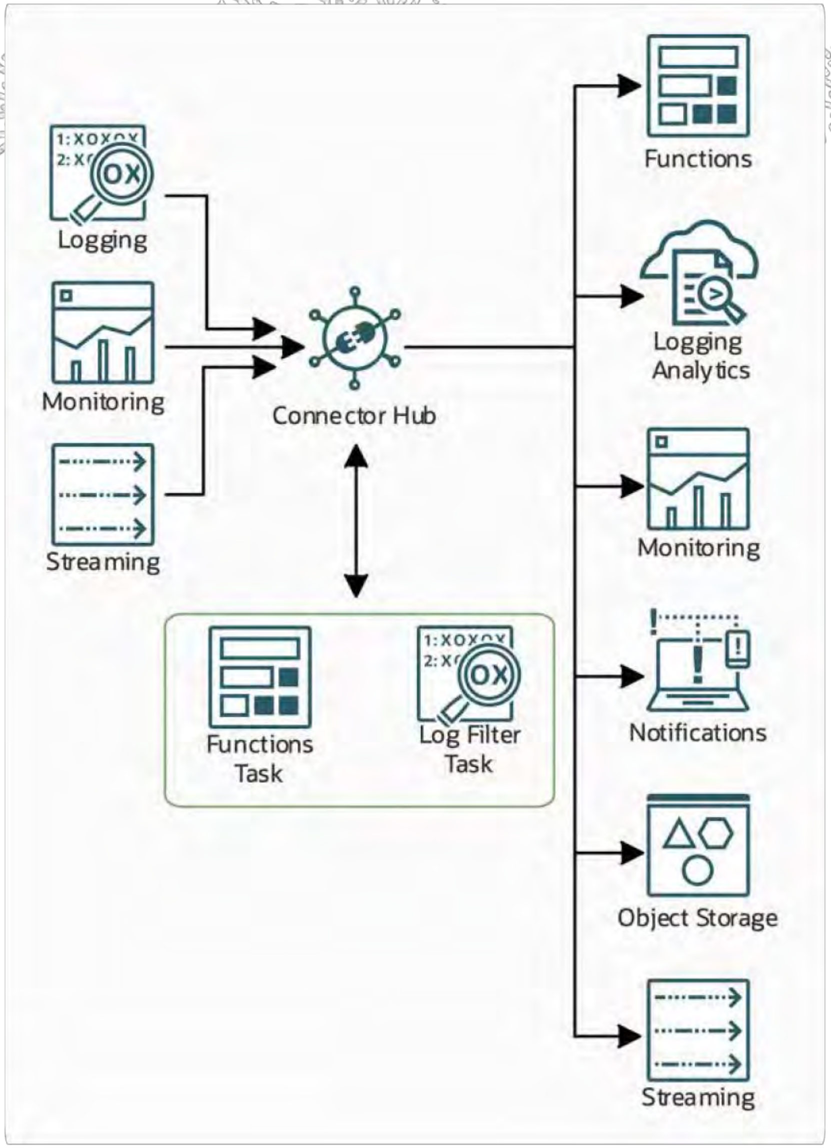


Connector Hub

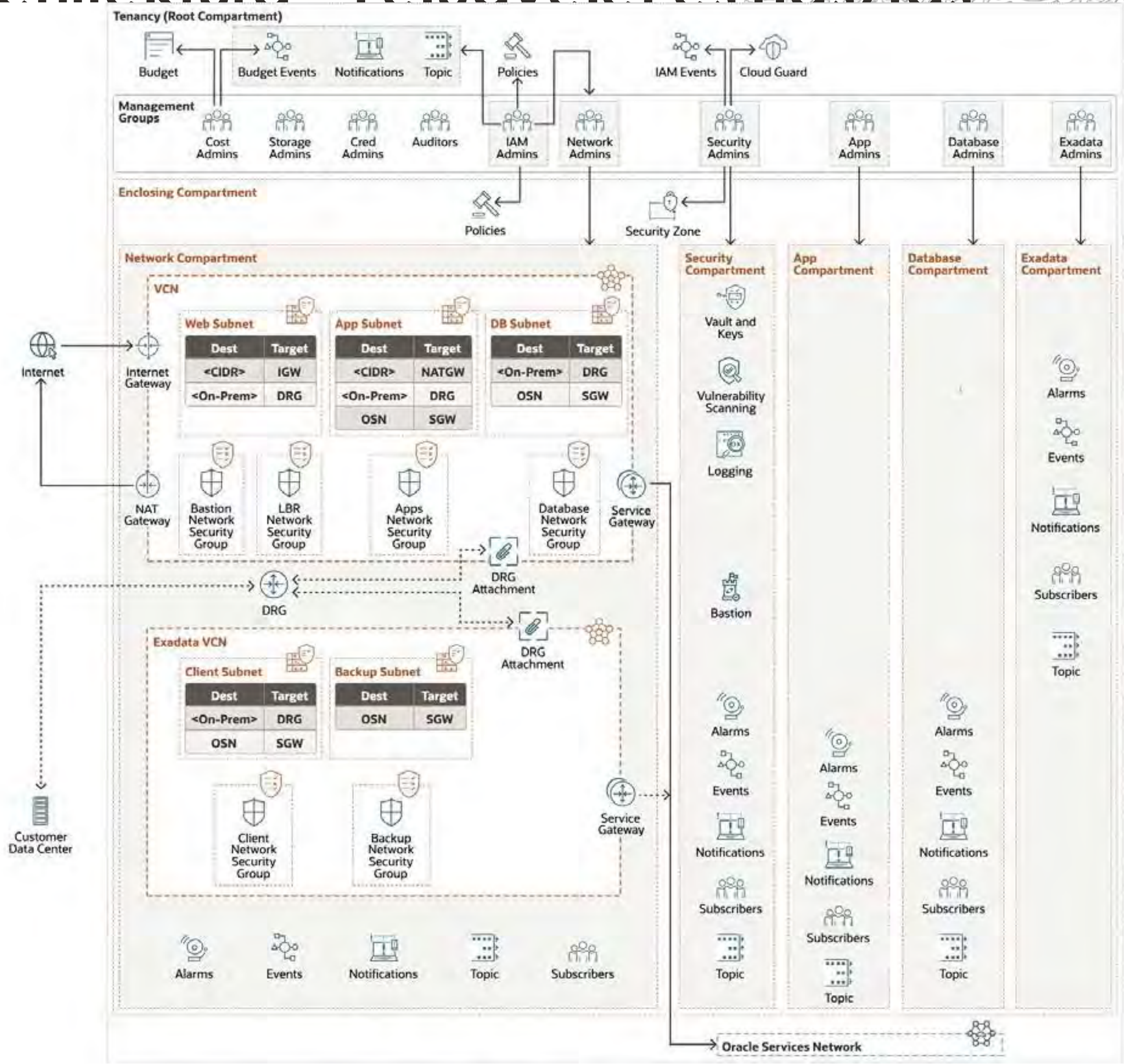
Connector Hub is a cloud message bus platform that offers a single pane of glass for describing, executing, and monitoring interactions when moving data between Oracle Cloud Infrastructure services. Connector Hub is formerly known as Service Connector Hub.

- Data is moved using connectors
- Connector: specifies the source service that contains the data to be moved, optional tasks, and the target service for delivery of data when tasks are complete





Landing Zone architektúra – Felügyelet és riasztás



Web Subnet

Dest	Target
<CIDR>	IGW
<On-Prem>	DRG

App Subnet

Dest	Target
<CIDR>	NATGW
<On-Prem>	DRG
OSN	SGW

DB Subnet

Dest	Target
<On-Prem>	DRG
OSN	SGW

Client Subnet

Dest	Target
<On-Prem>	DRG
OSN	SGW

Backup Subnet

Dest	Target
OSN	SGW

Demó

LiveLabs: Deploy a Secure Landing Zone in OCI

LiveLabs: .NET Development with Oracle Autonomous Database

Köszönjük a figyelmet!