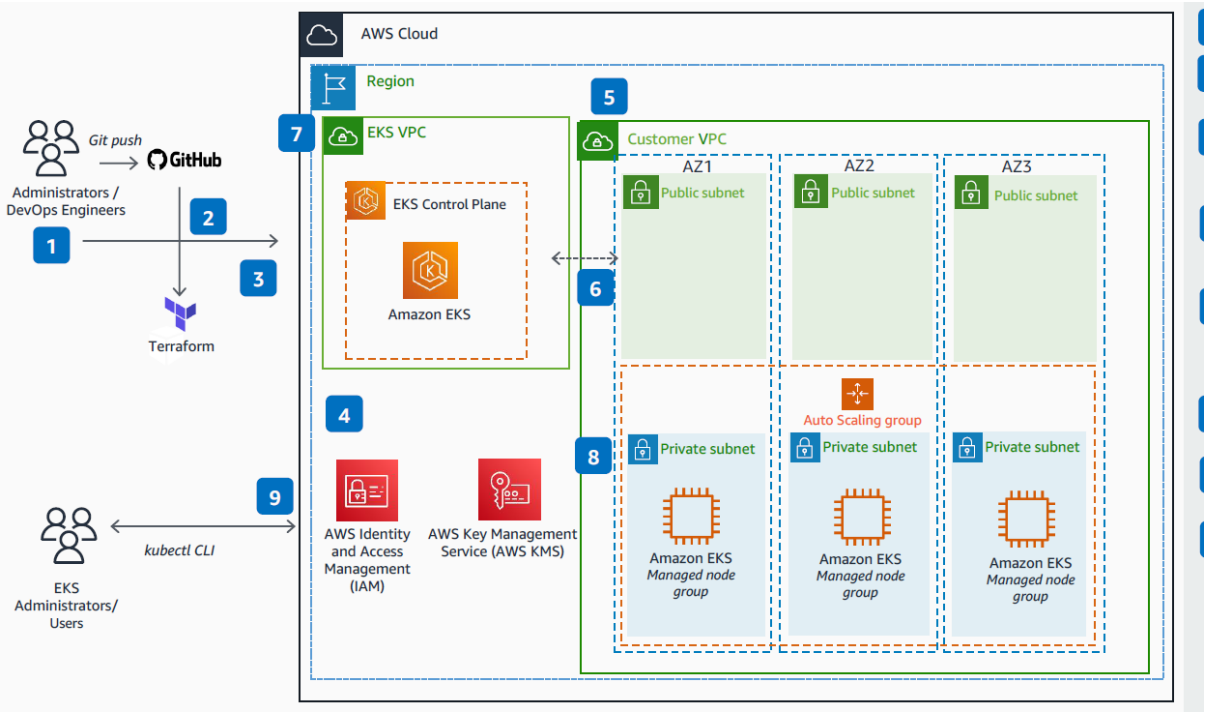
Oracle Interview with Amit Sides | OCI DevOps Specialist Position

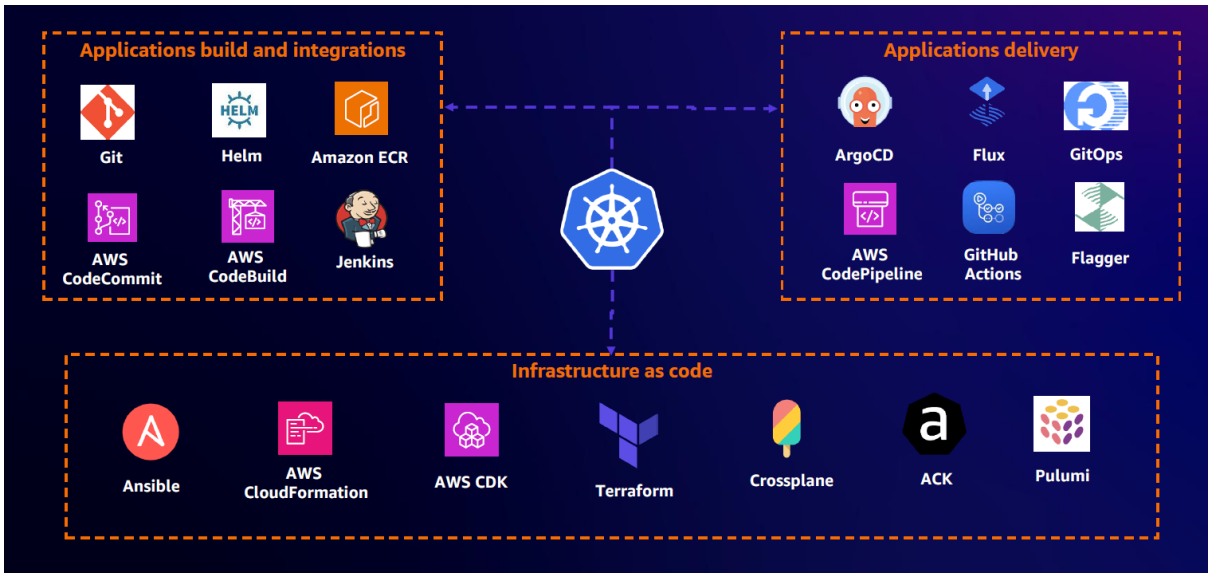
Secured Multi-Cluster, Multi-Tenancy Banking Infrastructure & CI/CD Pipeline

Infrastructure Architecture: From AWS VPC/ECR/EKS to OCI VCN/OCR/OKE

Bankore is already using AWS VPC/ECR/EKS inter-region, multi-availability zones and **we'll move to** OCI VCN/OCR/OKE.

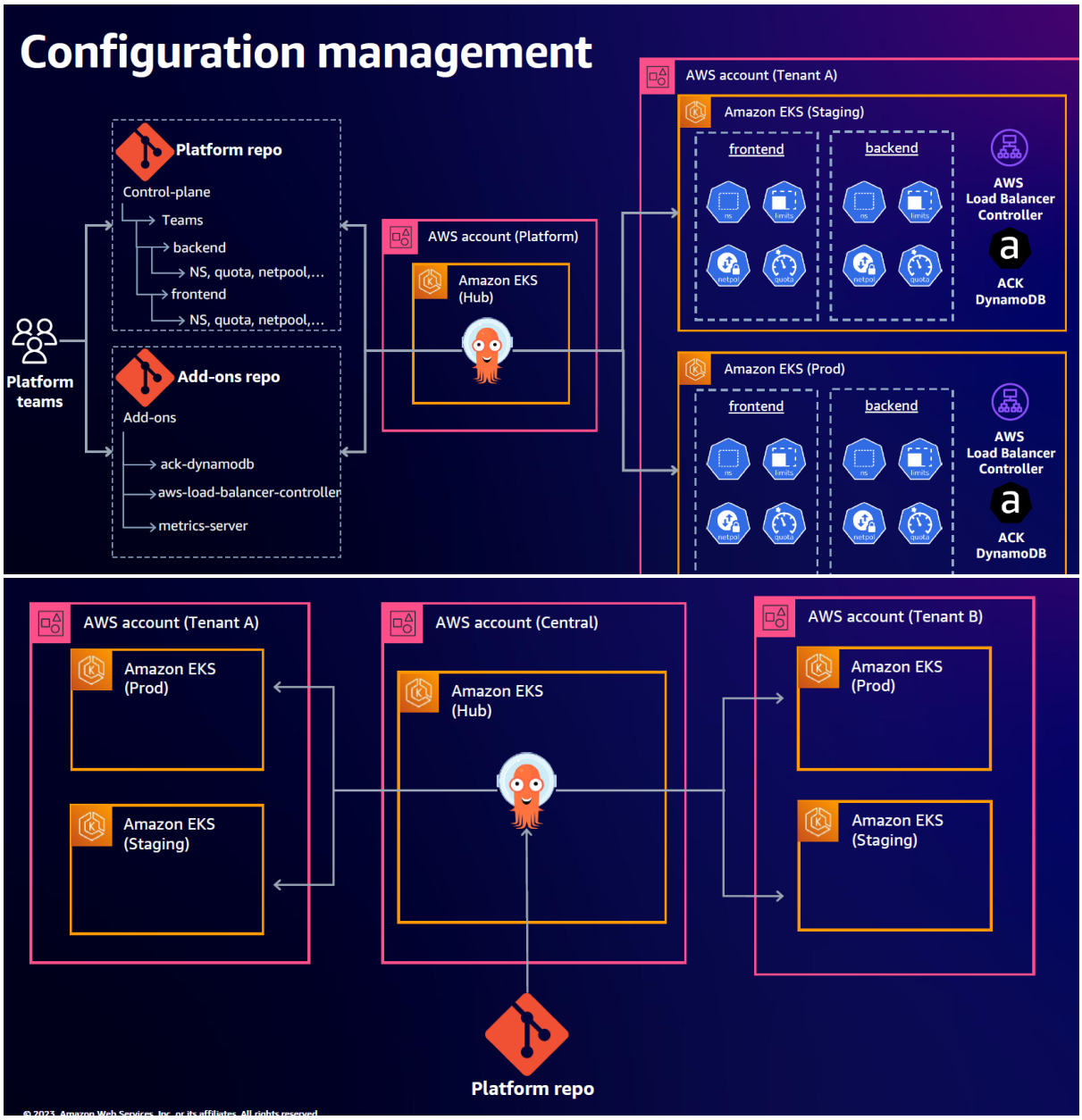


First and foremost, Oracle is proposing to migrate those applications to a Containerized architecture by using the Oracle Container Registry (OCR) & Oracle Kubernetes/Container Engine (OCE/OKE).



Infrastructure initialization Multi-Tenancy + Multi-Env: Terraform + Terragrunt: (Stage, QA, Prod) [see Oracle Resource Manager]

Multi-Tenancy Preview



https://terragrunt.gruntwork.io/docs/features/keep-your-terragrunt-architecture-dry/

https://terraspace.cloud/docs/learn/aws/new-project/

https://www.oracle.com/il-en/devops/resource-manager/

```
└── live
    ├── terragrunt.hcl
    ├── prod
    │   ├── app
    │   │   └── terragrunt.hcl
    │   ├── mysql
    │   │   └── terragrunt.hcl
    │   └── vpc
    │       └── terragrunt.hcl
    ├── qa
    │   ├── app
    │   │   └── terragrunt.hcl
    │   ├── mysql
    │   │   └── terragrunt.hcl
    │   └── vpc
    │       └── terragrunt.hcl
    └── stage
        ├── app
        │   └── terragrunt.hcl
        ├── mysql
        │   └── terragrunt.hcl
        └── vpc
            └── terragrunt.hcl
```

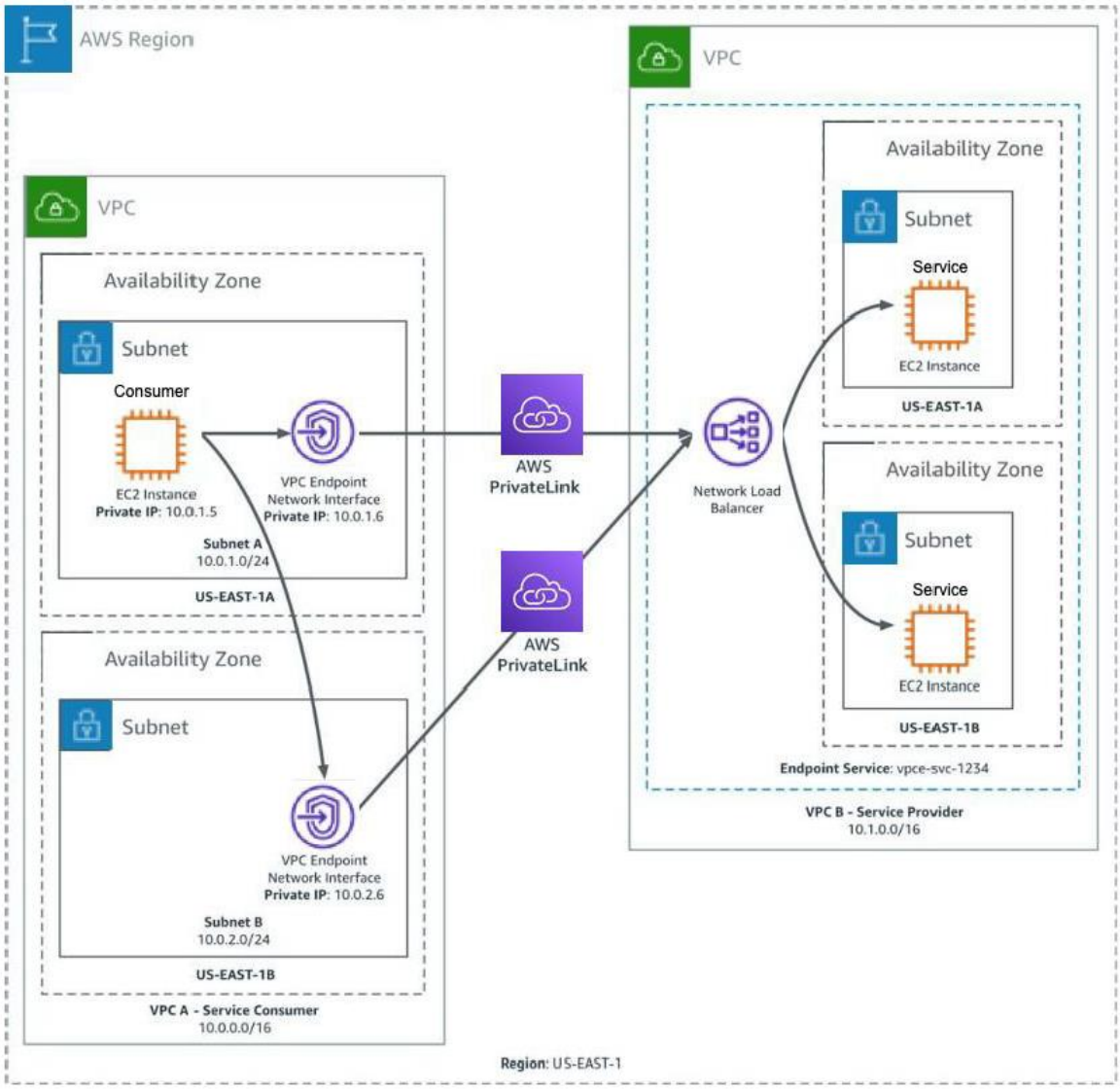
Terraform to bring up and running OKE https://github.com/oracle-devrel/terraform-oci-arch-oke-atp and Secondly, Databases (https://github.com/oracle-devrel/terraform-oci-arch-oke-atp/blob/main/database.tf)

1. Autonomous Database
2. Oracle DB 12c

And thirdly, Streaming (TEQ) and MQs

1. Oracle Cloud Infrastructure Streaming or Oracle TEQ https://docs.oracle.com/en/database/oracle/oracle-database/23/adque/Kafka_cient_interface_TEQ.html

Networking & Security



OCI Provides Multi-Regional Architectures DRG/VCN (Site-to-Site VPN (IPSec) Best Practices

Network Segmentation: VCN Subnets

Formulate a tiered subnet strategy for the VCN, to control network access. A common design pattern is to have the following subnet tiers:

DMZ subnet for load balancers

Public subnet for externally accessible hosts such as NAT instances, intrusion detection (IDS) instances, and web application servers

Private subnet for internal hosts such as databases

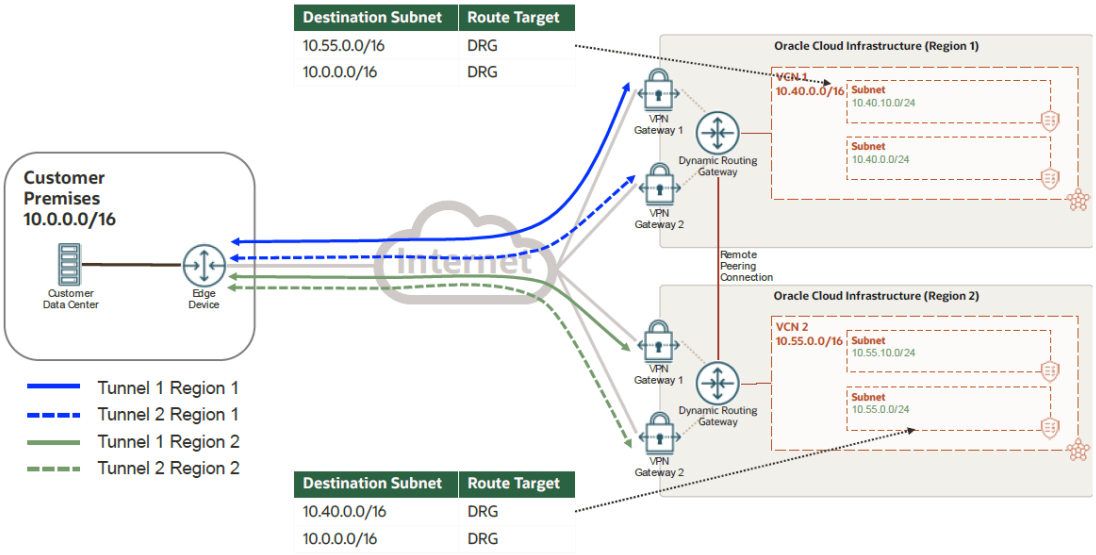


Figure 12: Site-to-Site VPN for Dual Regions with a Single Customer Edge Device Routing

NSG https://docs.oracle.com/en-us/iaas/Content/Network/Concepts/networksecuritygroups.htm

VNIC https://docs.oracle.com/en-us/iaas/Content/Network/Tasks/managingVNICs.htm

VCN/DRG

Consider the following steps for a successful deployment:
1. Create a dynamic routing gateway (DRG).

2. Attach the DRG to your VCN.

3. Create a customer-premises equipment (CPE) object.

4. Create a Site-to-Site VPN connection.

5. Configure routing: o During the Site-to-Site VPN configuration, specify your on-premises network prefixes. This configuration tells the DRG how to reach your on-premises network.

o The VCN in OCI must have a route rule that points to the DRG attached to the VCN for any routes destined to the on-premises network. The route rule can be in the default route table or in a subnet-specific route table.

o You can control which subnets in the VCN can communicate with your on-premises network. In the route tables for each of your VCN's subnets, specify some subnets instead of advertising your whole on-premises network.

o Each Site-to-Site VPN connection has two tunnels, and Oracle uses any of them based on availability. The traffic might be asymmetric between OCI and the on-premises network. Ensure that traffic is allowed on the on-premises network for both tunnels.

Networking Security Private access

https://docs.oracle.com/en-us/iaas/Content/Network/Concepts/privateaccess.htm

Security
Use Oracle Cloud Guard to monitor and maintain the security of your resources in Oracle Cloud Infrastructure proactively. Cloud Guard uses detector recipes that you can define to examine your resources for security weaknesses and to monitor operators and users for risky activities. When any mis-configuration or insecure activity is detected, Cloud Guard recommends corrective actions and assists with taking those actions, based on responder recipes that you can define.

For resources that require maximum security, Oracle recommends that you use security zones. A security zone is a compartment associated with an Oracle-defined recipe of security policies that are based on best practices. For example, the resources in a security zone must not be accessible from the public internet and they must be encrypted using customer-managed keys. When you create and update resources in a security zone, Oracle Cloud Infrastructure validates the operations against the policies in the security-zone recipe and denies operations that violate any of the policies.

OCI Bastion
TTL at the bastion level will ensure that none of the sessions created in the context of that bastion would have TTL more than the bastion. You should set the TTL to the minimum limit as per your use case. The min is 30 mins and the max is 3 hours. The TTL is also configurable at the session level.

Allow list CIDR block should be as narrow as possible as per your scenario. With this, you can restrict the IP address ranges from where the SSH connections are allowed to the private target resources.

The size of the target subnet to which a bastion is created should be thought through. Each bastion creation takes 2 IP addresses. So, it is better to have /29 range at least so that it has 6 usable IP addresses. /30 would have 2 IP addresses but if in the future you want the second instance of the bastion to point to the same subnet, you won't be able to create it. Please remember, the target subnet can either be the subnet where your target resource is present or from where other subnets in the target VCN can allow traffic from.

Security policies recommendations

- The ingress rules on the subnet which has the target resources should allow the incoming TCP traffic from just one IP address which is the private endpoint IP of the bastion.
- Specify the exact port on a destination like 22 for Linux, 3389 for windows, 33060 for MySql, and so on. Refrain from using ALL for ports.

Use specific IAM policies for admin and operator scenarios.

Bastion https://docs.oracle.com/en-us/iaas/Content/Bastion/home.htm

Bastion https://docs.oracle.com/en-us/iaas/tools/oci-cli/3.44.3/oci_cli_docs/cmdref/bastion.html

Keycloak and SSO

https://docs.oracle.com/en/cloud/iaas/verrazzano/1.2/vzdoc/docs/security/keycloak/keycloak/

Verrazzano user roles & K8s RBAC

https://docs.oracle.com/en/cloud/iaas/verrazzano/1.2/vzdoc/docs/security/rbac/rbac/

Verrazzano user roles

The following table lists the defined Verrazzano user roles. Each is a ClusterRole intended to be granted directly to users or groups. (In some scenari

Verrazzano Role	Binding Scope	Description
verrazzano-admin	Cluster	Manage Verrazzano system components, clusters, and projects. Install/update Verrazzano.
verrazzano-monitor	Cluster	View/monitor Verrazzano system components, clusters, and projects.
verrazzano-project-admin	Namespace	Deploy/manage applications.
verrazzano-project-monitor	Namespace	View/monitor applications.

Use the Bastion CLI to provide restricted and time-limited access to target resources that don't have public endpoints. Bastions let authorized users connect from specific IP addresses to target resources using Secure Shell (SSH) sessions. For more information, see the Bastion documentation

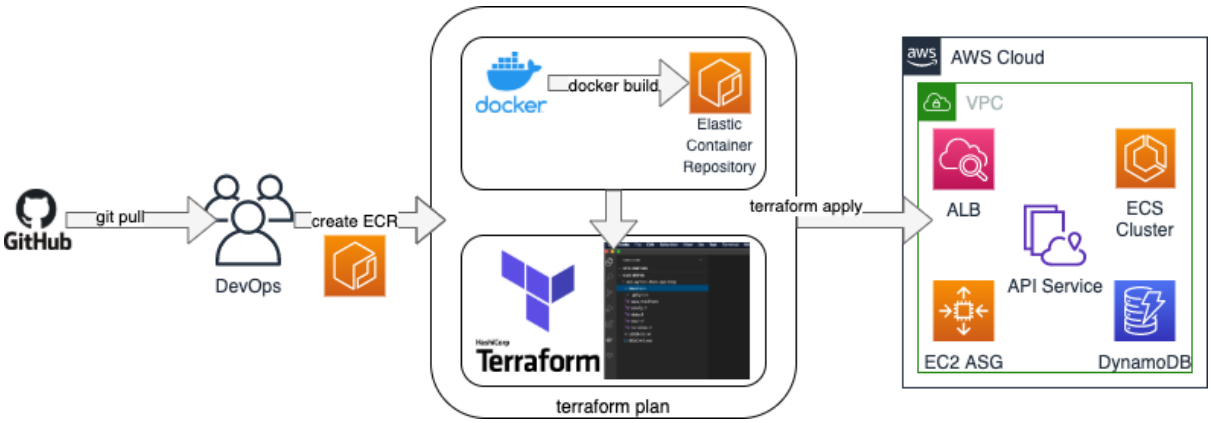
Security Credentials:

https://docs.oracle.com/en-us/iaas/Content/General/Concepts/credentials.htm

ORACLE WAF

https://docs.oracle.com/en-us/iaas/Content/WAF/Firewall/firewall_management.htm

CI Pipeline: Cobol & Java Dockerfile + Github Actions to OCIR or Jenkins OCI Plug-in



Now that we have infrastructure ready, we can easily build dockerfiles for 3 Application types on the programming languages and frameworks level of Cobol, JAVA.

A. Cobol running on Mainframe-

a. Cobol Application Dockerfile and we can deploy them to Oracle Container Registry and then to Oracle Kubernetes/Container Engine.

B.
```
FROM centos:7
RUN yum update -y && \
    yum install -y wget gcc make ncurses-devel
RUN wget https://sourceforge.net/projects/gnucobol/files/gnucobol/3.1/gnucobol-3.1.tar.gz && \
    tar -xvf gnucobol-3.1.tar.gz && \
    cd gnucobol-3.1 && \
    ./configure && \
    make && \
    make install && \
    cd .. && \
    rm -rf gnucobol-3.1 gnucobol-3.1.tar.gz
WORKDIR /app
COPY your_cobol_program.cob .
RUN cobc -x -o your_cobol_program your_cobol_program.cob
CMD ["./your_cobol_program"]
```

C. Java Enterprise + Oracle Database + PostgreSQL + IBM MQ

```
FROM openjdk:11-jdk
WORKDIR /app
COPY target/your-application.jar app.jar
COPY lib/ojdbc8.jar /app/lib/
COPY lib/postgresql.jar /app/lib/
EXPOSE 8080
ENV ORACLE_URL=jdbc:oracle:thin:@oracle-host:1521/your_service_name
ENV ORACLE_USER=your_oracle_username
ENV ORACLE_PASSWORD=your_oracle_password
ENV POSTGRES_URL=jdbc:postgresql://postgres-host:5432/your_database
ENV POSTGRES_USER=your_postgres_username
ENV POSTGRES_PASSWORD=your_postgres_password
CMD ["java", "-cp", "app.jar:/app/lib/*", "com.yourcompany.YourMainClass"]
```

D. Cloud-native- Spring Boot and Quarks with MongoDB and Oracle. It's fully containerized within Kubernetes and/or OpenShift
   a. we can use existing deployments tools to deploy them into OCR/OCE.

(https://github.com/oracle-quickstart/oke-soa)

Workflow file

```
name: Build and Push Docker Image to OCIR

on:
  push:
    branches:
      - main

jobs:
  build-and-push:
    runs-on: ubuntu-22.04
    env:
      OCI_CLI_USER: ${{ secrets.OCI_CLI_USER }}
      OCI_CLI_TENANCY: ${{ secrets.OCI_CLI_TENANCY }}
      OCI_CLI_FINGERPRINT: ${{ secrets.OCI_CLI_FINGERPRINT }}
      OCI_CLI_KEY_CONTENT: ${{ secrets.OCI_CLI_KEY_CONTENT }}
      OCI_CLI_REGION: ${{ secrets.OCI_CLI_REGION }}
```

```
  steps:
    - name: Checkout code
      uses: actions/checkout@v2

    - name: Set up Docker Buildx
      uses: docker/setup-buildx-action@v1

    - name: Get or create an OCIR Repository
      id: get-ocir-repository
      uses: oracle-actions/get-ocir-repository@v1.3.0
      with:
        name: oraclelinux
        compartment: ${{ secrets.OCI_COMPARTMENT_OCID }}

    - name: Log into OCIR
      id: login-ocir
      uses: oracle-actions/login-ocir@v1.3.0
      with:
        auth_token: ${{ secrets.OCI_AUTH_TOKEN }}

    - name: Build and push Docker image
      id: tag-and-push-image
      run: |
        docker build -t oraclelinux:8-slim .
        docker tag "oraclelinux:8-slim" "${{ steps.get-ocir-repository.outputs.repo_path }}:8-slim"
        docker push "${{ steps.get-ocir-repository.outputs.repo_path }}:8-slim"
```

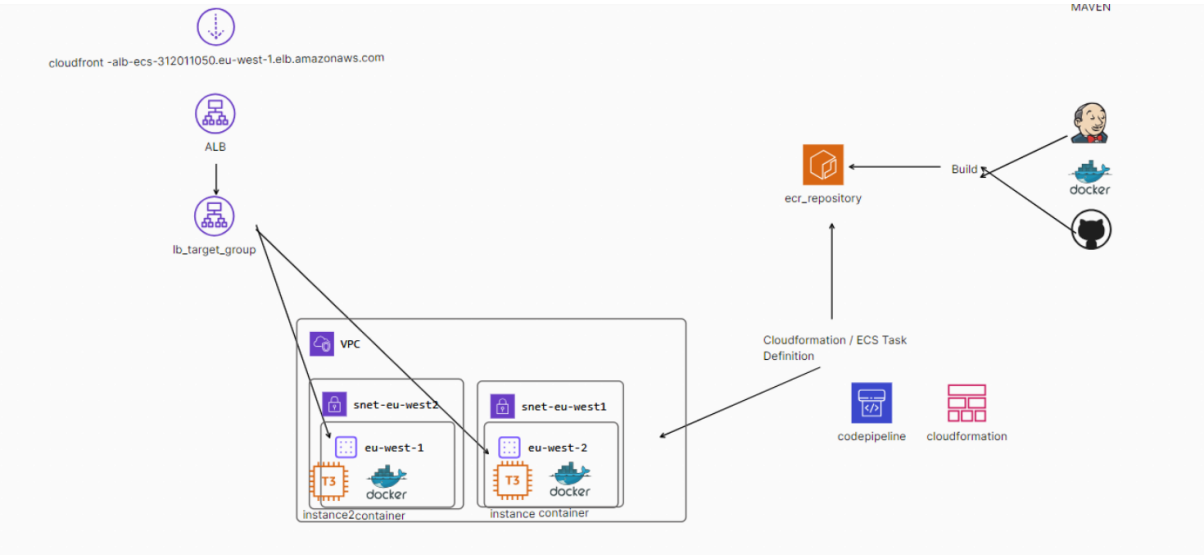
Jenkins + OCI

Oracle Cloud Infrastructure Compute Plugin allows users to access and manage cloud resources on the Oracle Cloud Infrastructure (OCI) from Jenkins. A Jenkins master instance with OCI Compute Plugin can spin up OCI Instances (slaves or agents) on demand within OCI, and remove the Instances and free its resources automatically once the Job completes

https://plugins.jenkins.io/oracle-cloud-infrastructure-compute/

https://github.com/lhagemann/jenkins-oci-plugin

.



CD & Deployments / Multi-Cluster deployments

OKE deployment / Oracle WebLogic Server / Verrazzano / ArgoCD / HelmCharts

See ALSO About Oracle WebLogic Server for OKE

https://docs.oracle.com/en/cloud/iaas/verrazzano/vzdoc/docs/applications/delivery/

https://github.com/verrazzano/verrazzano

https://docs.oracle.com/en/cloud/iaas/verrazzano/1.5/vzdoc/docs/applications/multicluster/mcresources/

https://docs.oracle.com/en/cloud/iaas/verrazzano/1.5/vzdoc/docs/applications/multicluster/intro/

https://docs.oracle.com/en/cloud/iaas/verrazzano/1.4/vzdoc/docs/reference/api/multicluster/multiclusterapplicationconfiguration/

Adding a Trigger Deployment Stage

https://docs.oracle.com/en-us/iaas/Content/devops/using/triggerdeploy_stage.htm#triggerdeploy_stage

Oracle Helm Charts Repository

https://github.com/oracle/helm-charts

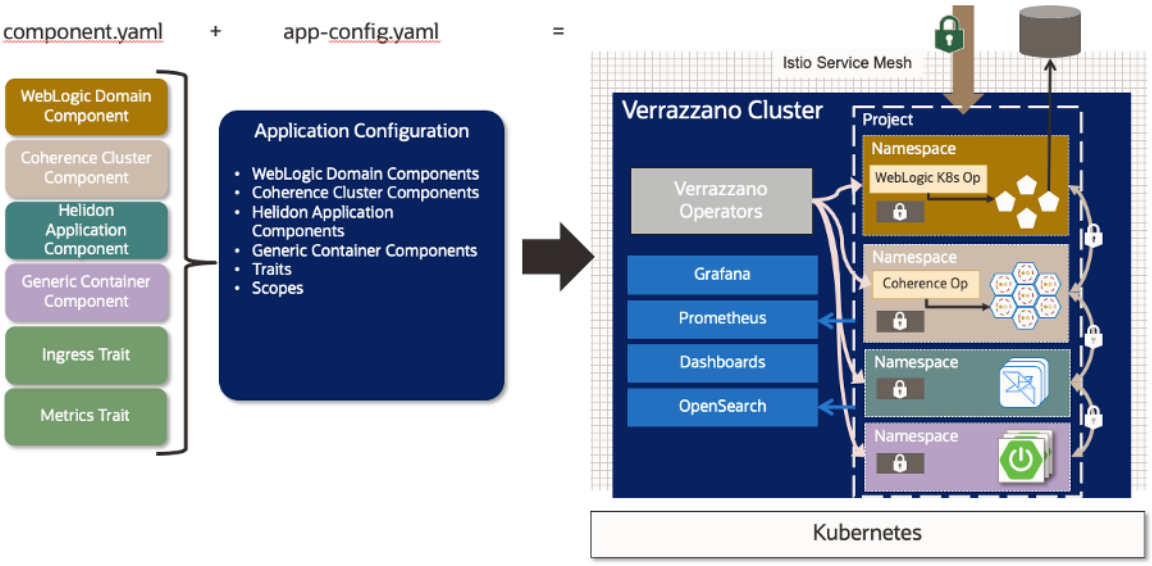
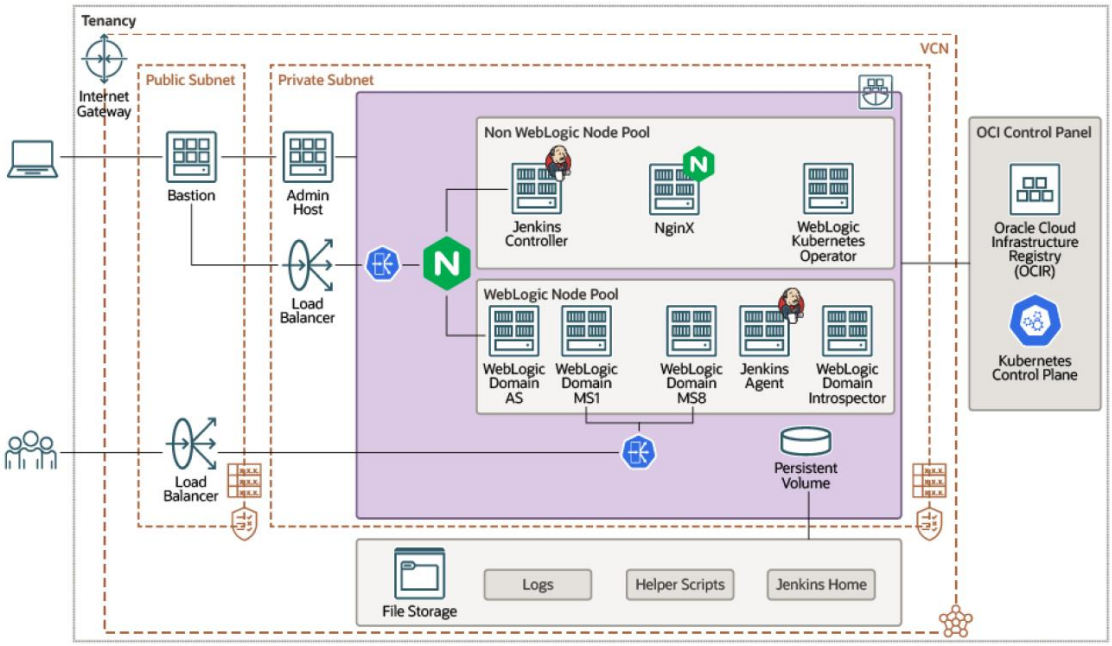
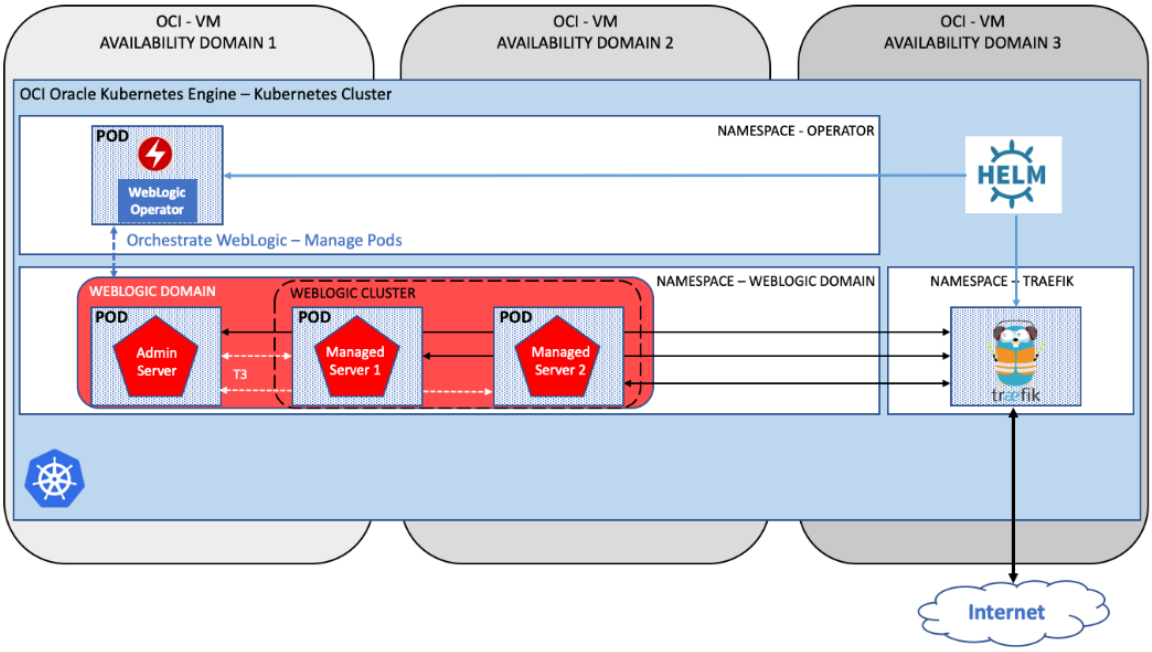


Figure 1-1 Components of a typical Oracle WebLogic Server for OKE deployment

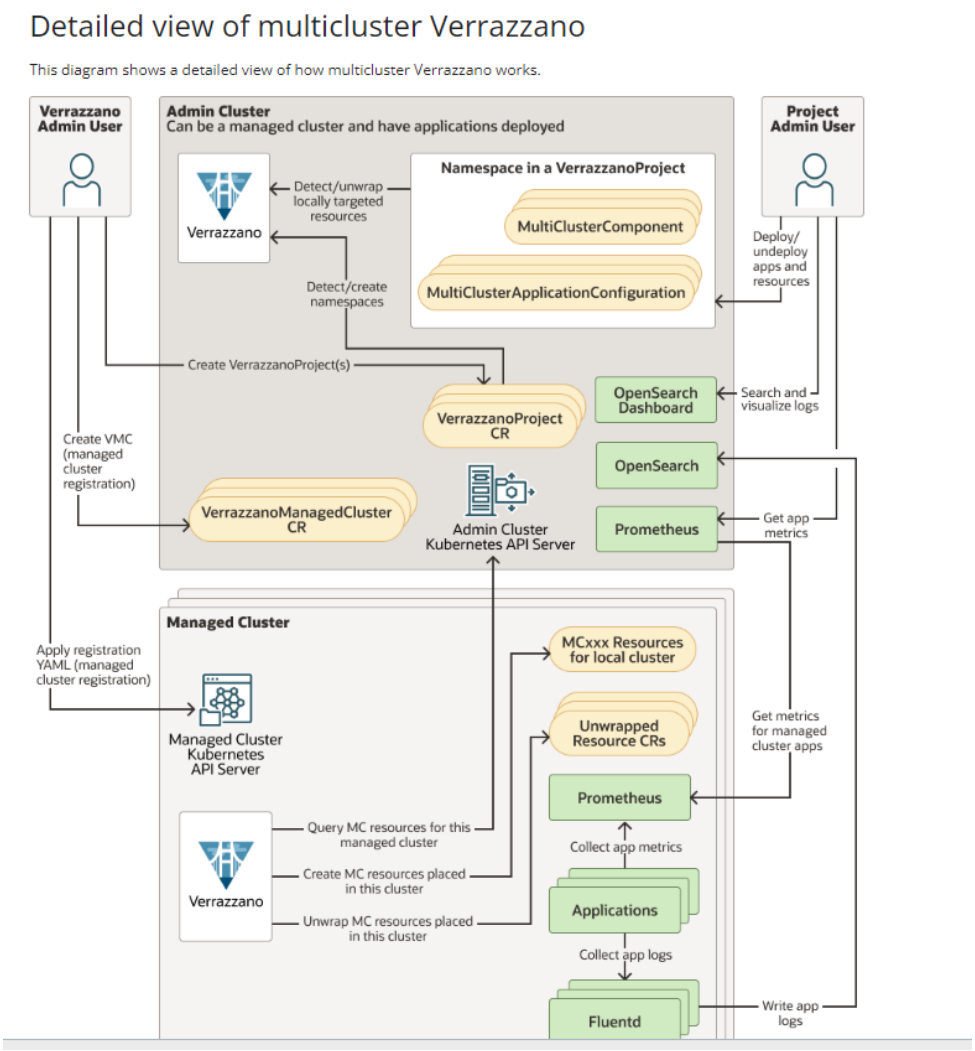


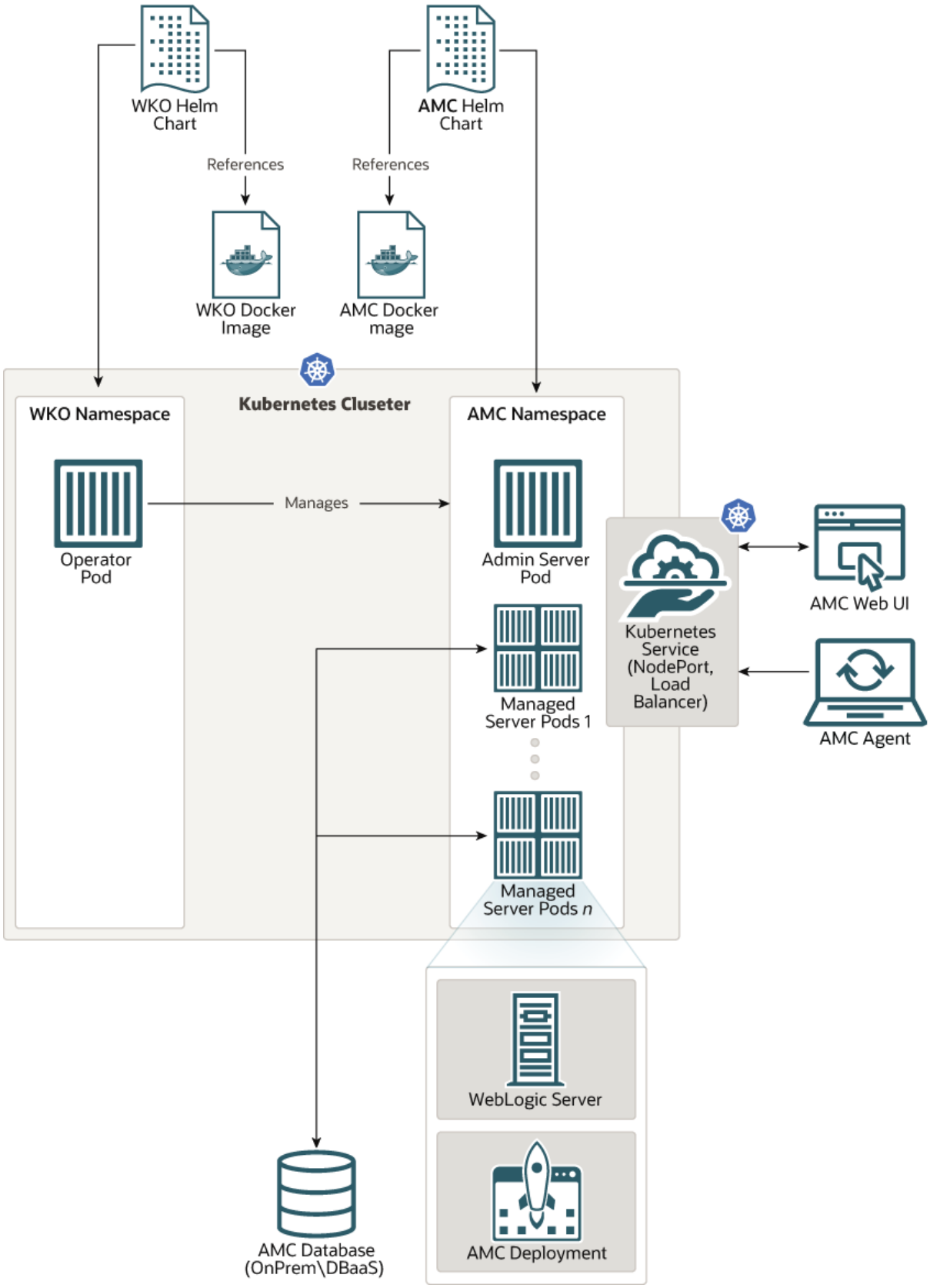
Oracle WebLogic Operators

https://github.com/nagypeter/weblogic-operator-tutorial/blob/master/tutorials/domain.home.in.image_short.md

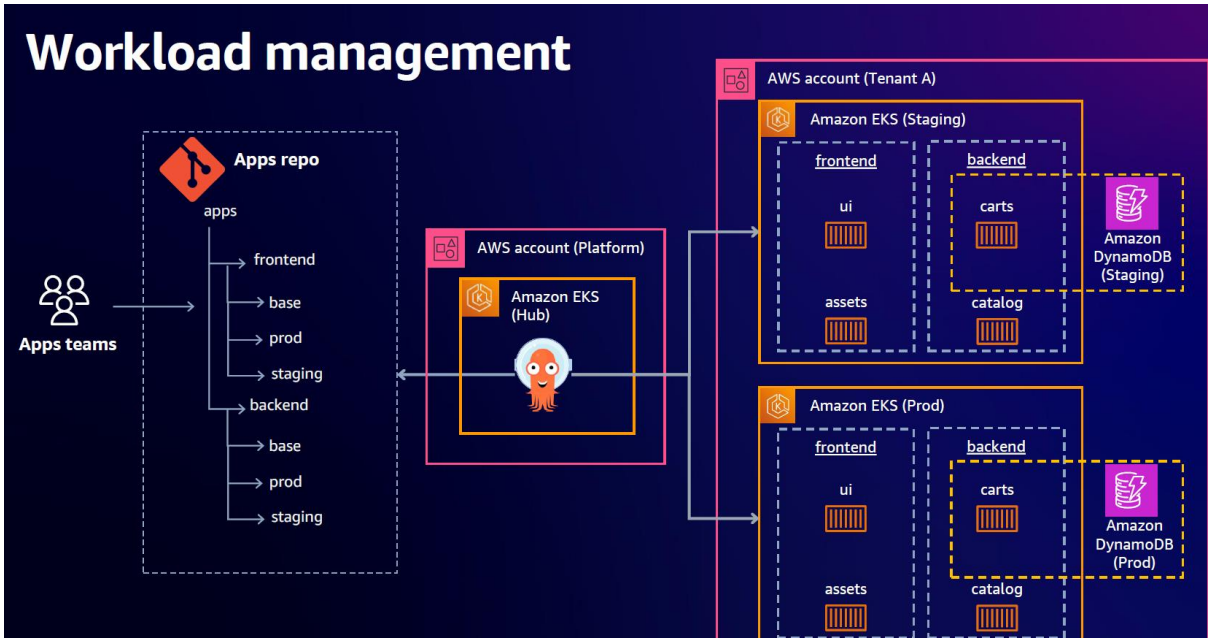

OCI - VM
AVAILABILITY DOMAIN 1
OCI - VM
AVAILABILITY DOMAIN 2
OCI - VM
AVAILABILITY DOMAIN 3
OCI Oracle Kubernetes Engine – Kubernetes Cluster
POD
WebLogic Operator
NAMESPACE - OPERATOR
HELM
Orchestrate WebLogic – Manage Pods
WEBLOGIC DOMAIN
WEBLOGIC CLUSTER
NAMESPACE – WEBLOGIC DOMAIN
NAMESPACE – TRAEFIK
POD
Admin Server
T3
POD
Managed Server 1
POD
Managed Server 2
traefik
Internet

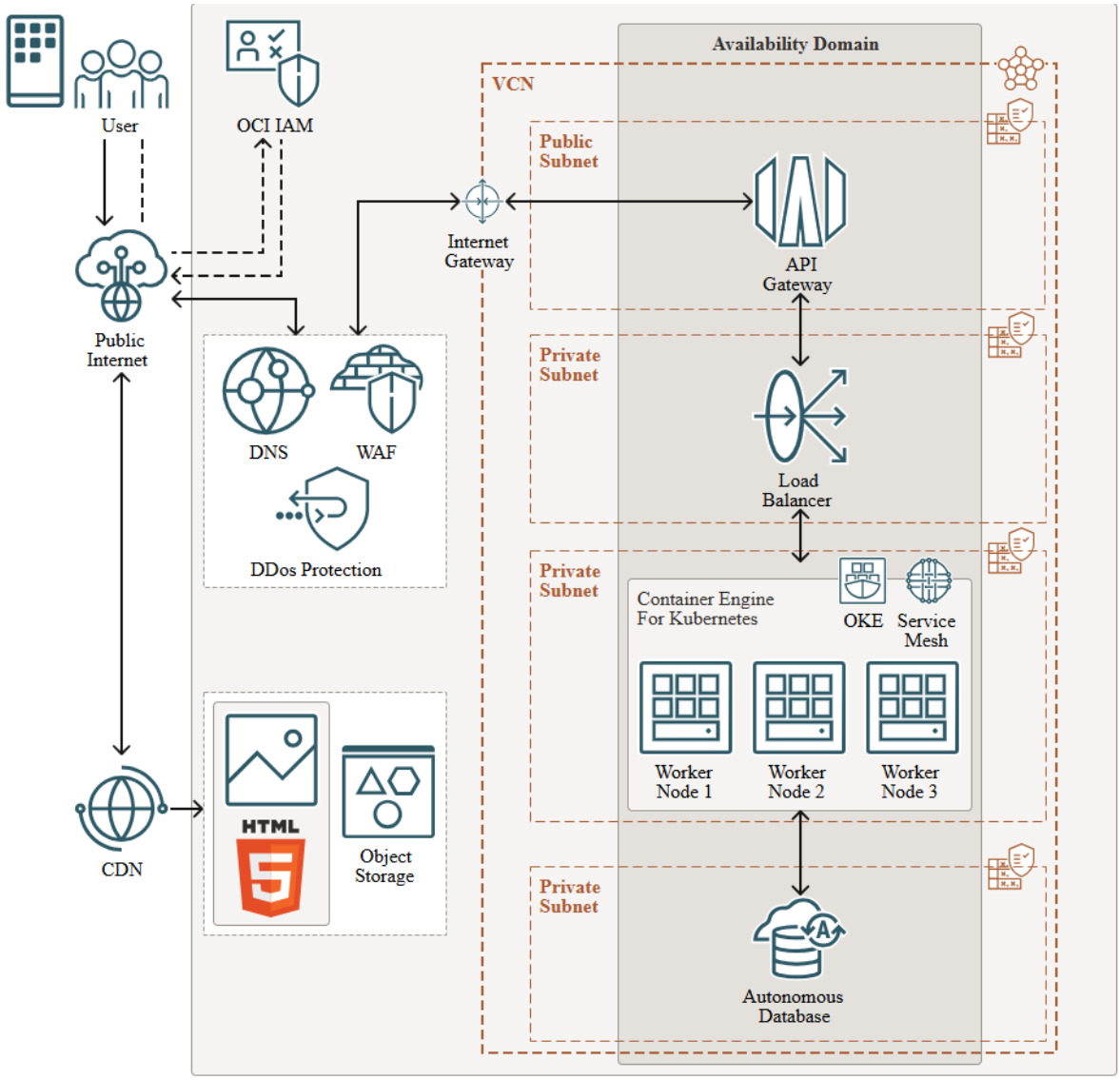
Multi-Cluster Verrazzano




WKO Helm Chart
AMC Helm Chart
References
References
WKO Docker Image
AMC Docker mage
Kubernetes Cluseter
WKO Namespace
AMC Namespace
Operator Pod
Manages
Admin Server Pod
Managed Server Pods 1
Managed Server Pods n
Kubernetes Service (NodePort, Load Balancer)
AMC Web UI
AMC Agent
WebLogic Server
AMC Deployment
AMC Database (OnPrem\DBaaS)

Websites, DNS & CDNs

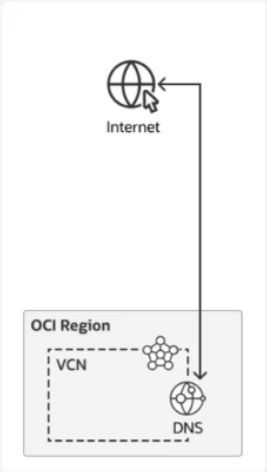



User
OCI IAM
Availability Domain
VCN
Public Subnet
Internet Gateway
API Gateway
Public Internet
Private Subnet
DNS
WAF
Load Balancer
DDos Protection
Private Subnet
Container Engine For Kubernetes
OKE
Service Mesh
Worker Node 1
Worker Node 2
Worker Node 3
HTML
Object Storage
CDN
Private Subnet
Autonomous Database

Use cases for OCI DNS

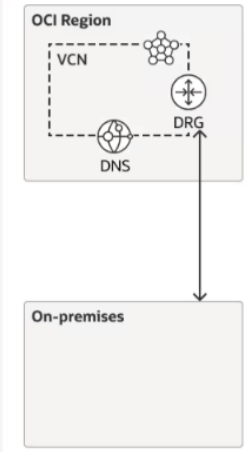
View more DNS scenarios

Public DNS



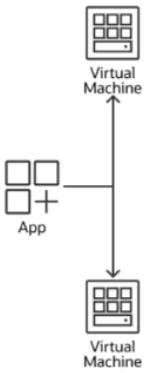
Public DNS zones hold the authoritative DNS records that reside on OCI's nameservers. You can create public zones with publicly available domain names that are reachable on the internet.

Private DNS



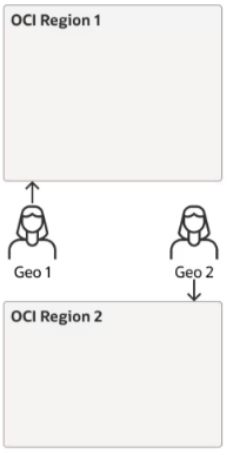
Create private zones with domain names that you specify. Fully manage the zones and records to provide hostname resolution for apps running within and between virtual cloud networks (VCNs), on-premises environments, or private networks.

Traffic load balancing



Guide traffic to endpoints based on equal or custom weights, taking endpoint health into account.

Traffic steering

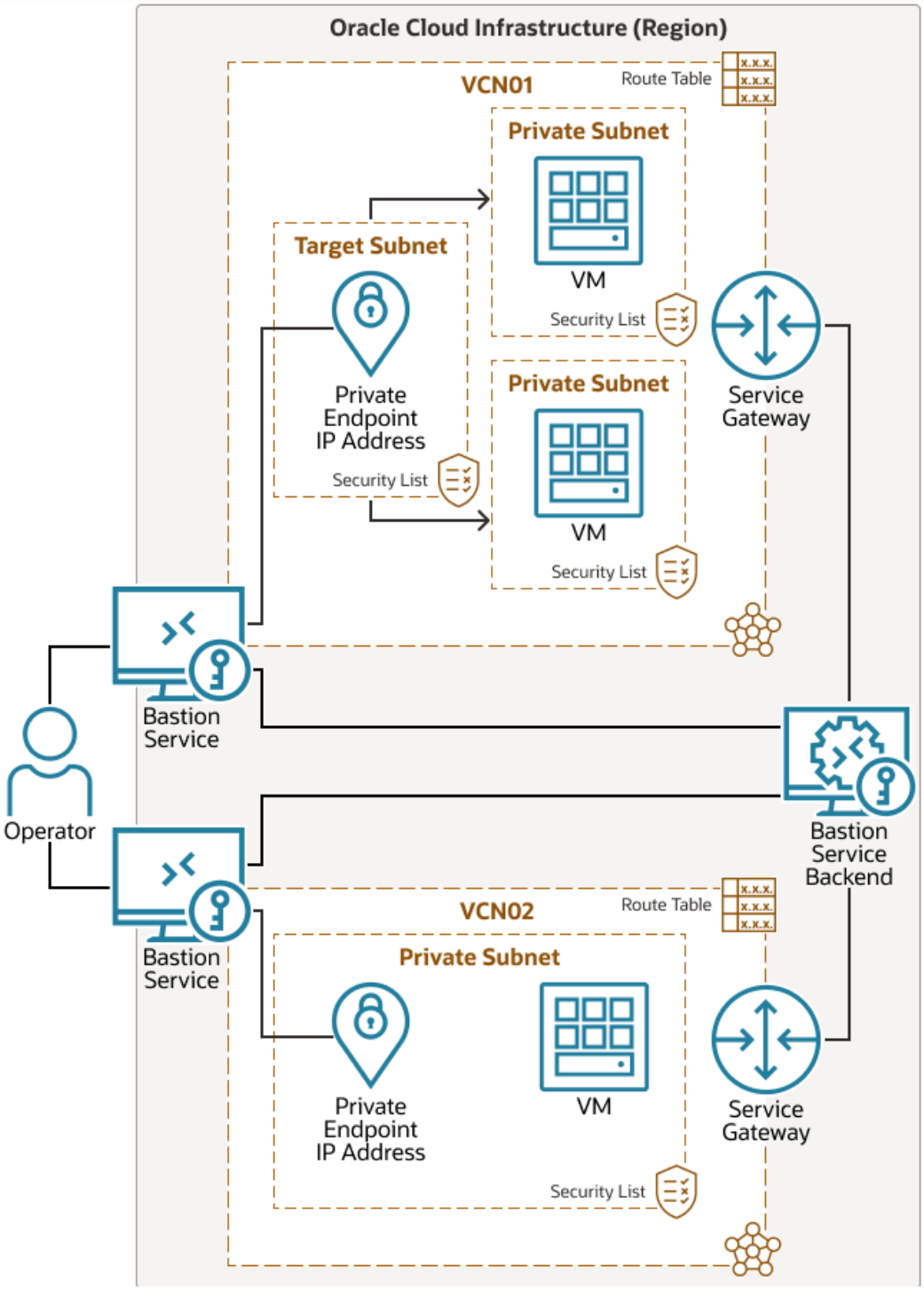


Guide traffic to endpoints based on the geographic origin of the DNS request or source network address.

Oracle Database Gateway for WebSphere MQ

https://docs.oracle.com/en-us/iaas/database-management/doc/create-database-management-private-endpoint.html

https://www.oracle.com/database/technologies/gateways/pg4mq.html



Private endpoint for RAC Oracle Cloud Databases

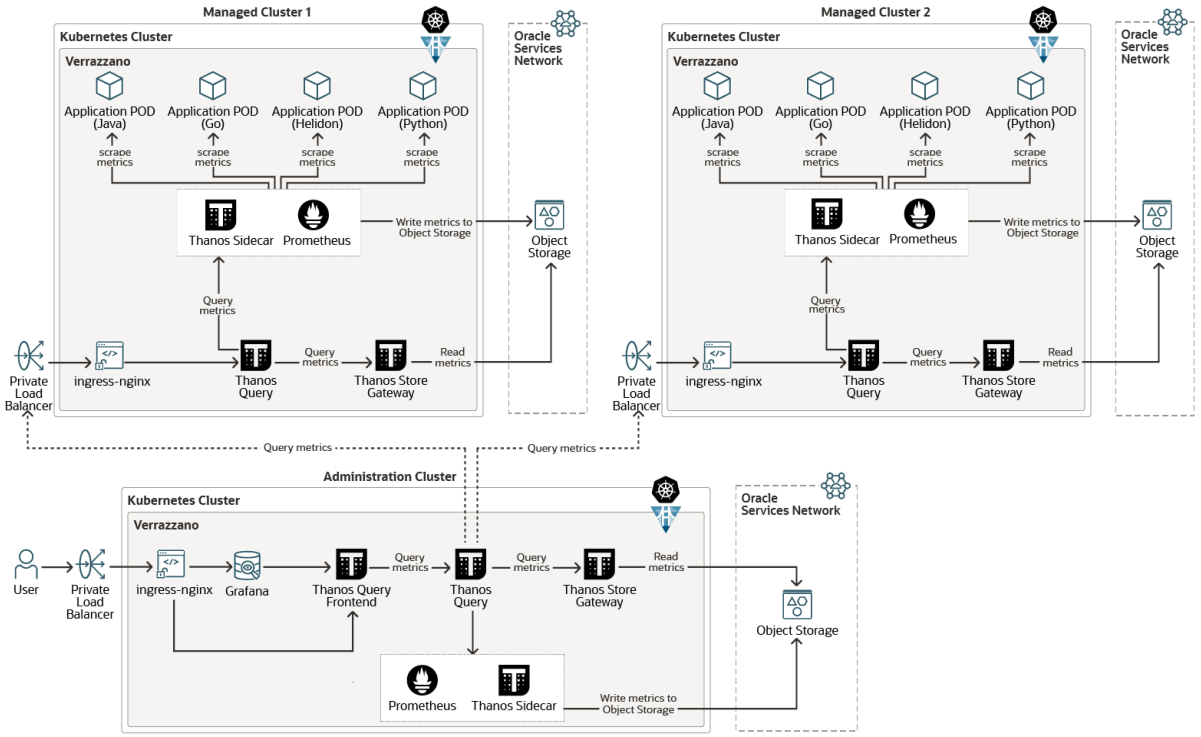
https://docs.oracle.com/en-us/iaas/database-management/doc/create-database-management-private-endpoint.html

Observability

https://docs.oracle.com/en/solutions/mad-messaging-pattern/index.html#GUID-B4CA4052-F67B-406C-BC46-3196C2EED2DC

Multi-Cluster Monitoring

https://docs.oracle.com/en/cloud/iaas/verrazzano/vzdoc/docs/observability/monitoring/multicluster-metrics/



To design complete observability for your Kubernetes cluster using Datadog, New Relic, and application performance monitoring (APM), I'll outline a comprehensive approach that leverages the strengths of each platform:

1. Kubernetes Cluster Monitoring:

- Use Datadog's Kubernetes integration for comprehensive cluster monitoring. Datadog is known for its user-friendly interface and extensive Kubernetes support, providing metrics on cluster workloads and infrastructure.

- Deploy the New Relic Kubernetes monitoring quickstart to gain additional visibility into your clusters and workloads. This will provide dashboards for proactive monitoring of:
    - Resource usage
    - Number of Kubernetes objects
    - Namespaces per cluster
    - Pods by namespace
    - Container CPU usage
    - Container restarts
    - Missing pods by deployment
    - Node resource consumption

2. Log Management:

- Implement Fluent Bit within your cluster to collect and forward logs from pods.
- Ship logs to Datadog for centralized log management and analysis, taking advantage of its powerful log processing and visualization capabilities.

3. Application Performance Monitoring (APM):

- Utilize New Relic's APM capabilities, which offer excellent application-level insights and can be integrated with their Kubernetes monitoring solution.
- Implement Datadog APM for a second perspective on application performance, leveraging its strong integration with the Kubernetes monitoring data.
- Choose a third APM tool based on your specific application stack and requirements. Consider options like Dynatrace, AppDynamics, or Elastic APM.

4. Tracing and Distributed Tracing:

- Implement New Relic's tracing capabilities, which can provide context-aware logging and visualization of request flows across microservices.
- Use Datadog's tracing features for an additional layer of distributed tracing visibility.

5. Infrastructure Monitoring:

- Leverage Datadog's infrastructure monitoring capabilities for a holistic view of your entire stack, including the underlying infrastructure supporting your Kubernetes cluster.

6. Dashboards and Alerting:

- Create custom dashboards in both Datadog and New Relic to visualize key metrics and KPIs across your entire observability stack.
- Set up alerts in both platforms to ensure rapid response to any issues in your cluster or applications.

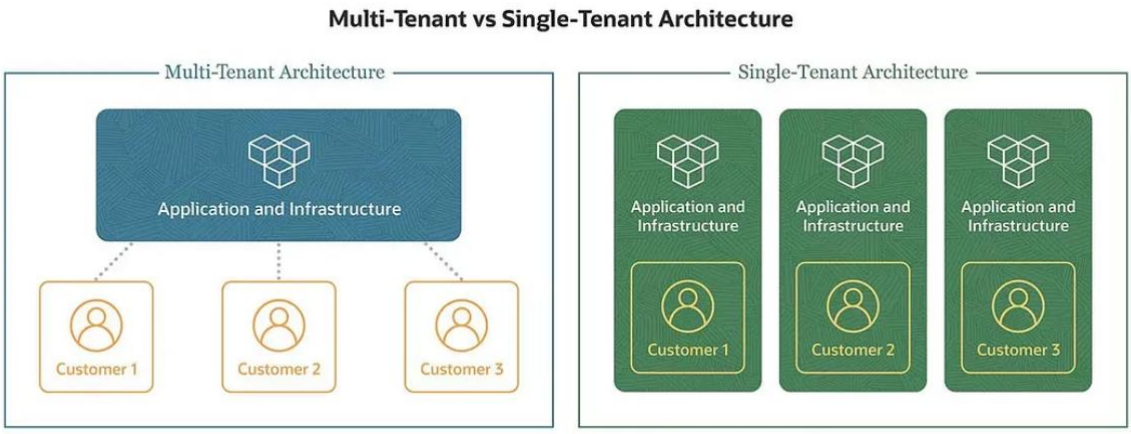
7. Service Mesh Observability:
- If you're using a service mesh like Istio, integrate it with both Datadog and New Relic for enhanced visibility into service-to-service communication.
8. Continuous Integration/Continuous Deployment (CI/CD) Integration:
- Integrate your observability tools with your CI/CD pipeline to correlate deployments with performance changes and potential issues.
9. Cost Management:
- Utilize Datadog's container cost allocation features to optimize resource usage and control cloud spending.
10. Security Monitoring:
- Implement Datadog's security monitoring features to detect and alert on potential security threats within your Kubernetes environment.

Load balancing

https://docs.oracle.com/en-us/iaas/Content/Balance/Tasks/managingloadbalancer_topic-Creating_Load_Balancers.htm#top

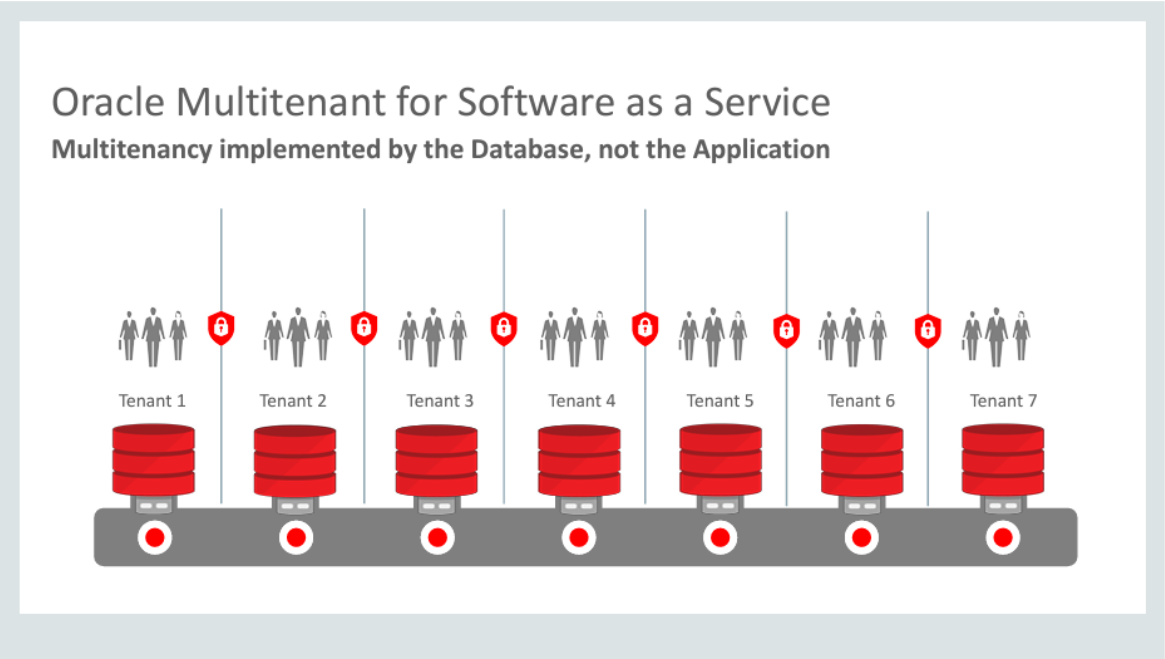
Multi-Tenancy Isolation & Security: VCN vs. DB

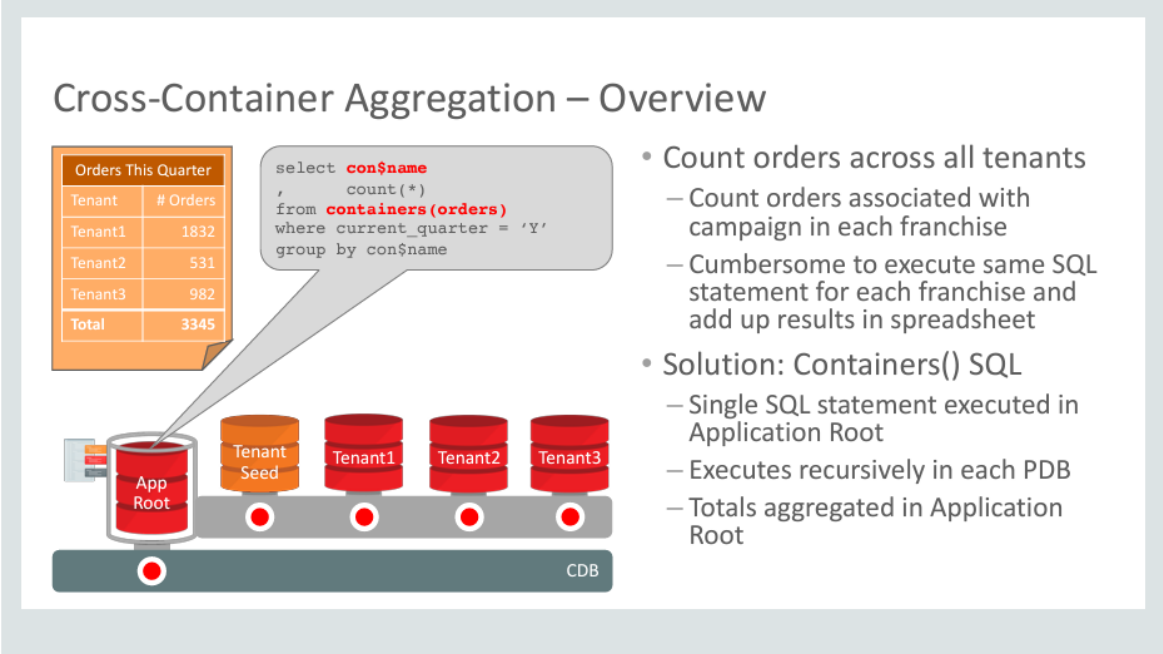
separate Tenants from various perspectives are discussed (different VCNs with Security Lists (Security Groups), different databases.



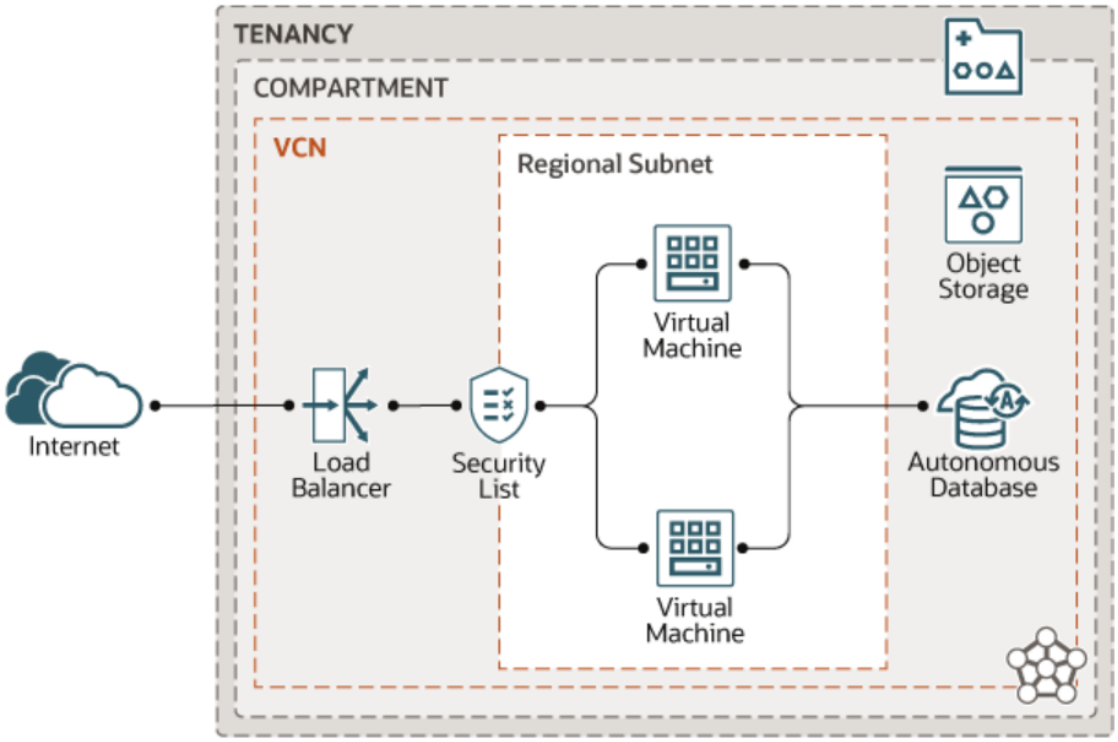
Databases Multi-Tenancy

Oracle Database Multitenant architecture revolutionizes the way we manage databases, offering improved efficiency, reduced costs, and simplified database consolidation. Its resource optimization capabilities, cost-effective approach, and inherent agility make it a preferred choice for organizations seeking streamlined database management and migrating from the former architecture.

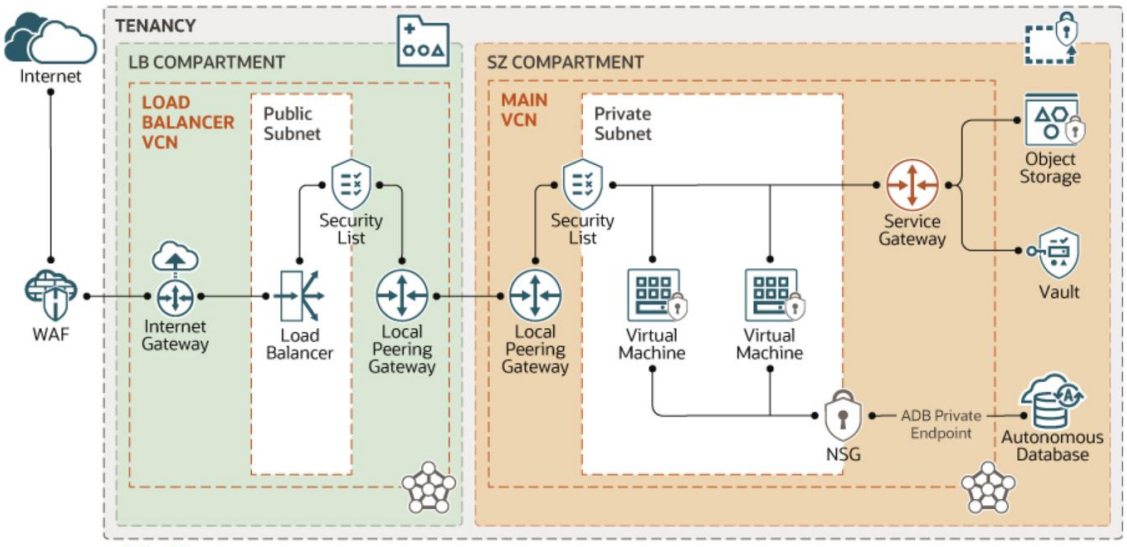




VCNs



Description of the illustration mcz_01.png



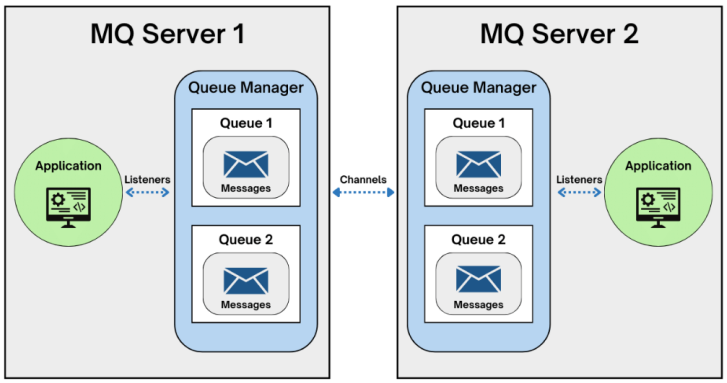
Queue & Event Streaming

(Transactional Event Queues and Advanced Queuing User's Guide
https://docs.oracle.com/en/database/oracle/oracle-database/23/adque/loe.html#GUID-6E031525-8D92-4862-AF11-F433184EF4B6)

1. Oracle Cloud Infrastructure (OCI) Streaming:
   OCI Streaming provides a fully managed, scalable, and durable solution for ingesting and processing high-volume data streams in real-time. It offers Kafka compatibility, allowing applications to use Kafka APIs to interact with OCI Streaming.
2. Oracle Cloud Infrastructure Queue:
   OCI Queue is a managed service for message queuing, supporting RESTful APIs and the STOMP protocol.
3. Oracle Transactional Event Queues (TEQ):
   TEQ is integrated with the Oracle Database and provides Kafka-compatible APIs. It allows Kafka applications to connect to an Oracle database and use TEQ as a messaging platform without significant code changes.
4. Oracle Advanced Queuing (AQ):
   AQ is another queuing feature available in Oracle Autonomous Database, offering messaging capabilities within the database.

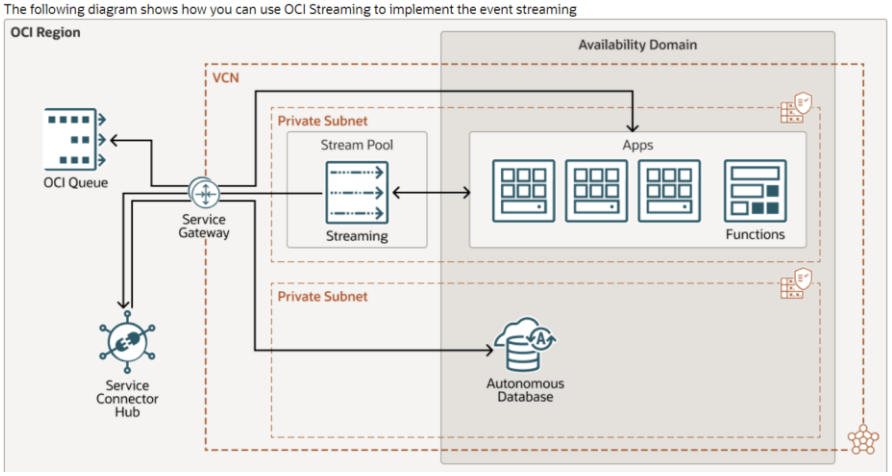
Key features and benefits of these solutions include:

- Managed services: These offerings are fully managed, eliminating complexity in application development and operations.
- Kafka compatibility: OCI Streaming and TEQ provide Kafka-compatible APIs, allowing easy migration of existing Kafka applications.
- Integration with Oracle Database: TEQ and AQ are tightly integrated with Oracle Database, simplifying state management by storing events and messages in the same database used by the application.
- Scalability and durability: These services offer high availability, automatic replication across availability domains, and support for scaling automation.
- Security: They leverage Oracle Cloud Infrastructure Identity and Access Management (IAM) for access control and support network isolation through private endpoints.
- Observability: Integration with Oracle Cloud Observability and Management Platform provides comprehensive monitoring and tracing capabilities.



Architecture

The following diagram shows how you can use OCI Streaming to implement the event streaming



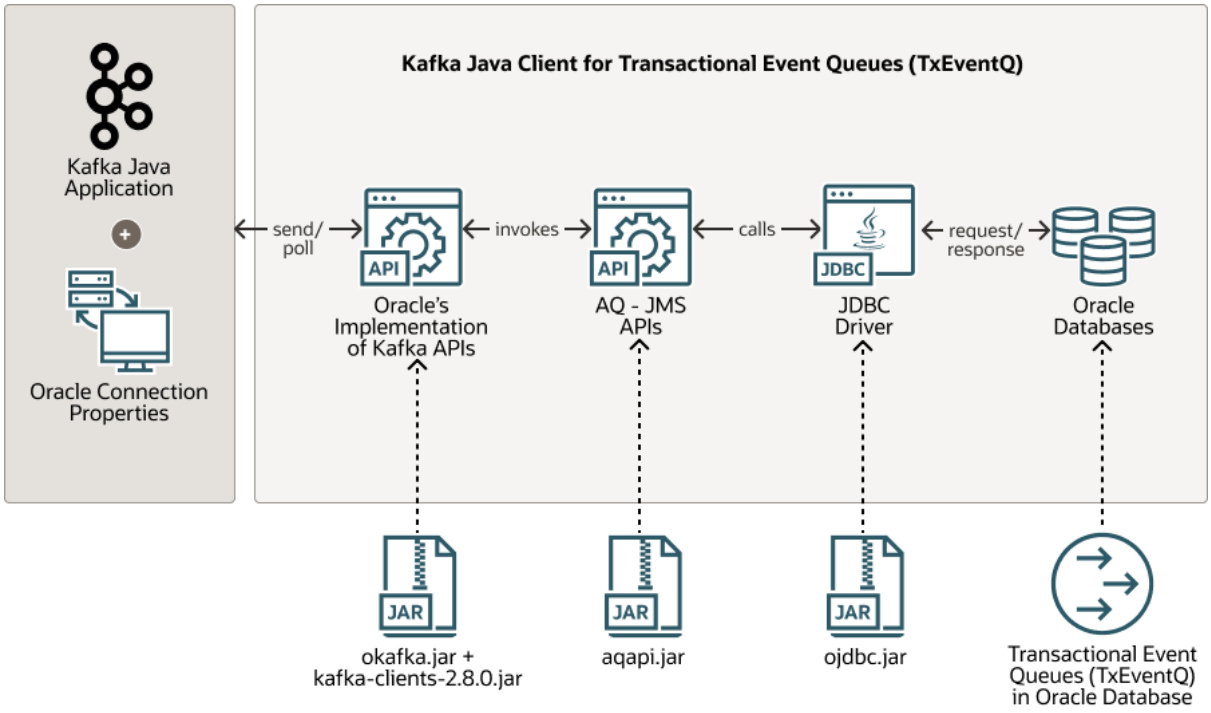
Change Data Capture (CDC) & Oracle GoldenGate

https://docs.oracle.com/en/middleware/goldengate/core/23/coredoc/install-oracle-goldengate.html#GUID-1F67CD47-DE23-412F-9C05-A80EAD10A53A

https://docs.oracle.com/en/solutions/oci-security-zones/index.html#GUID-DC4C6DC8-B1C5-4E60-B3A5-591BF7837482

Kafka: Use Java with Kafka API or Kafka Connect

https://docs.oracle.com/en-us/iaas/Content/Streaming/Tasks/kafkacompatibility_topic-Kafka_Connect.htm



https://docs.oracle.com/en-us/iaas/Content/Streaming/Tasks/kafkacompatibility_topic-Kafka_Connect.htm

https://www.oracle.com/webfolder/technetwork/tutorials/obe/cloud/compute-iaas/compiling_psft_cobol/compile_cobol_linux_cmpnode.html

https://docs.oracle.com/en/solutions/mad-messaging-pattern/index.html#GUID-B4CA4052-F67B-406C-BC46-3196C2EED2DC

https://docs.oracle.com/en/database/oracle/oracle-database/23/adque/Kafka_cient_interface_TEQ.html#GUID-450E3352-08B7-4471-AA87-168B47782078

https://docs.oracle.com/en/solutions/mad-web-mobile/#GUID-3D021003-8598-4438-8733-674BAFF9A718

https://docs.oracle.com/iaas/Content/Resources/Assets/whitepapers/ipsec-vpn-best-practices.pdf

https://medium.com/schmiedeone/abstracting-kubernetes-with-helm-library-chart-4da85c3be8f5

https://docs.oracle.com/en/solutions/mad-messaging-pattern/index.html#GUID-BE81EE1C-CC30-478F-8579-37E44636BA07

https://docs.oracle.com/en/database/oracle/oracle-database/23/adque/Kafka_cient_interface_TEQ.html#GUID-450E3352-08B7-4471-AA87-168B47782078

https://docs.oracle.com/en/solutions/mad-messaging-pattern/index.html#GUID-B4CA4052-F67B-406C-BC46-3196C2EED2DC

IBM MQ Queue Management Best Practices

https://avadasoftware.com/ibm-mq-queue-management-tips/

https://docs.oracle.com/en-us/iaas/database-management/doc/create-database-management-private-endpoint.html