Anotações CORE: OCI Multicloud Architect Professional

1. Introdução ao Multicloud (10%)

O que é Multicloud?

É o uso coordenado de serviços de nuvem de **dois ou mais provedores** (ex: OCI + Azure + GCP).

Benefícios e Casos de Uso

- **Evitar Vendor Lock-in:** Não depender de um único fornecedor.
- **Best-of-Breed:** Usar o melhor serviço para cada tarefa (ex: Bancos de Dados Oracle no OCI e serviços de IA/ML no Google Cloud).
- **Otimização de Custos:** Aproveitar os melhores preços de cada provedor.
- **Redundância e Resiliência:** Usar uma nuvem como DR para outra.
- **Conformidade e Soberania de Dados:** Atender a requisitos regulatórios que exigem a presença em provedores ou regiões específicas.

Implementação em OCI

A estratégia multicloud do OCI se manifesta principalmente através de:

1. **Conexões de Rede Dedicadas:**
    - **Oracle Interconnect for Azure:** Conexão direta de baixa latência.
    - **Oracle Interconnect for Google Cloud:** Conexão direta de baixa latência.
2. **Serviços Co-localizados:**
    - **Oracle Database@Azure:** Infraestrutura OCI (Exadata) rodando **dentro** dos data centers do Azure.
    - **Oracle Database@Google Cloud:** Infraestrutura OCI rodando **dentro** dos data centers do Google Cloud.

2. Visão Geral dos Serviços Core do OCI (20%)

Federação de Identidade (OCI IAM)

- **Conceito:** Permite que usuários de um **Identity Provider (IdP)** externo (como Azure AD ou Google Cloud Identity) se autentiquem para acessar recursos no OCI (**Service Provider - SP**).
- **Protocolo:** Utiliza **SAML 2.0**.
- **Benefício: Single Sign-On (SSO)**. Os usuários usam suas credenciais corporativas existentes, sem precisar de um novo login/senha para o OCI.
- **Usuários:**
    - **Federado:** Autenticado via IdP.

    - **Local:** Criado e gerenciado diretamente no OCI IAM.

Componentes da VCN (Virtual Cloud Network)

- **VCN:** Sua rede privada e isolada em uma **única região** do OCI.
- **Sub-redes:**
    - **Pública:** Recursos podem ter IPs públicos e se comunicar com a internet.
    - **Privada:** Recursos só têm IPs privados. O acesso à internet é feito via NAT Gateway.
    - **Escopo:** Podem ser **Regionais** (abrangem todos os ADs) ou **Específicas de AD**.
- **Gateways:**
    - Internet Gateway: Permite tráfego de/para a internet para sub-redes públicas.
    - NAT Gateway: Permite que recursos em sub-redes privadas iniciem conexões com a internet.
    - Service Gateway: Permite acesso a serviços públicos do OCI (ex: Object Storage) sem passar pela internet.
    - Dynamic Routing Gateway (DRG): **Hub central** para tráfego que **não** é da internet. Conecta a VCN com redes on-premises (VPN/FastConnect), VCNs em outras regiões (Remote Peering) e outras nuvens.
    - Local Peering Gateway (LPG): Conecta duas VCNs na **mesma região**.
- **Segurança (Firewall Virtual):**

Característica	Security List (SL)	Network Security Group (NSG)
Escopo	**Sub-rede inteira**	**vNICs individuais** (recursos)
Aplicação	Aplicada a todos os recursos da sub-rede.	Aplicada a recursos específicos, independentemente da sub-rede.
Fonte/Destino	Bloco CIDR	Bloco CIDR **OU outro NSG**
Uso Ideal	Regras de segurança amplas para a sub-rede.	Regras granulares para camadas de aplicação (ex: NSG-Web só pode falar com NSG-App).

- **Tabelas de Rota:** Direcionam o tráfego para fora da sub-rede para o gateway correto. A rota **mais específica** (prefixo CIDR mais longo) sempre vence.

Serviços de Banco de Dados OCI

- **Base Database Service (VM):**
  - **Modelo:** Co-gerenciado (você gerencia o BD, Oracle gerencia a infra).
  - **Opções:** Single Instance ou 2-Node RAC.
  - **Armazenamento:** LVM ou **ASM** (ASM é **obrigatório** para RAC).
- **Autonomous Database (ADB):**
  - **Modelo:** Totalmente gerenciado ("automático").
  - **Workloads:** ATP (transacional), ADW (analítico), JSON, APEX (low-code).
  - **Implantação: Serverless** (compartilhado) ou **Dedicated** (em infraestrutura Exadata dedicada).
- **MySQL HeatWave:**
  - **Finalidade:** Acelerar cargas de trabalho **analíticas (OLAP)** em um banco de dados MySQL **transacional (OLTP)**.
  - **Benefício Core:** Elimina a necessidade de um banco de dados analítico separado e de processos de **ETL**. Permite análise em tempo real sobre dados transacionais.

3. Opções de Conexão Multicloud (20%)

Site-to-Site VPN vs. FastConnect

Característica	Site-to-Site VPN	FastConnect
Meio	Internet Pública	Privada, Dedicada
Desempenho	Variável, menor largura de banda	Previsível, alta largura de banda (até 100 Gbps)
Custo	Serviço gratuito (paga pela saída de dados)	Pago (taxa de porta)
Segurança	Criptografia IPSec (obrigatória)	Privado por natureza (criptografia opcional)
Uso Ideal	Provas de conceito, baixo custo, backup para FastConnect	Cargas de trabalho de produção, dados sensíveis, alta performance

Oracle Interconnect for Azure

- **Tecnologia:** Conexão direta entre **OCI FastConnect** e **Azure ExpressRoute**.
- **Latência:** Muito baixa (~2ms), pois não há parceiro intermediário.
- **Setup:** Inicia no **Azure** para obter a **Service Key**, que é usada para provisionar o FastConnect no OCI.

- **Suporte:** Colaborativo (pode abrir chamado na Oracle ou na Microsoft).
- **Roteamento Transitivo: NÃO SUPORTADO**. A conexão é estritamente para tráfego entre OCI e Azure. Não pode ser usada para conectar on-premises ao Azure através do OCI.

Oracle Interconnect for Google Cloud

- **Tecnologia:** Conexão direta entre **OCI FastConnect** e **Google Cloud Partner Interconnect**.
- **Setup:** Inicia no **Google Cloud** para criar um VLAN attachment e obter a **Pairing Key**, que é usada no OCI.
- **Suporte:** Colaborativo.
- **Custos:** Sem cobrança de transferência de dados entre as nuvens.
- **Roteamento Transitivo: SUPORTADO**. Pode ser usado em topologias de trânsito (ex: on-premises -> GCP -> OCI).

4. Implementar Oracle Database@Azure (30%)

Arquitetura e Onboarding

- **Arquitetura Core:** É uma **infraestrutura OCI (OCI Pod)** fisicamente localizada **dentro de um data center do Azure**. Este "child site" é conectado a uma região "parent" do OCI para operações de controle.
- **Conectividade:** Existe um link de rede **direto, privado e de latência ultra baixa** entre o OCI Pod e a rede do Azure, tudo dentro do mesmo data center. O tráfego **nunca sai** do data center.
- **Onboarding:** O serviço é adquirido via **Azure Marketplace**. As permissões de compra (Billing account owner, Enterprise administrator) são cruciais.

Provisionamento e Gerenciamento

A responsabilidade é dividida:

Tarefa	**Realizada em**
Provisionar/Gerenciar **Infraestrutura Exadata e VM Cluster**	**Portal do Azure** (ou APIs/SDKs do Azure)
Provisionar/Gerenciar **Bancos de Dados (CDBs/PDBs)**	**Console do OCI**

Networking

- **Subnet Delegation:** É um recurso **obrigatório** do Azure. Você deve delegar as

sub-redes de **cliente** e **backup** para o serviço Oracle.Database/networkAttachments.
- **Requisitos de IP (Mínimo para 2 VMs):**
  - **Client Subnet:** (2 VMs * 4 IPs) + 3 SCAN IPs + 13 IPs de serviço = 24 IPs
  - **Backup Subnet:** (2 VMs * 3 IPs) + 3 IPs de serviço = 9 IPs

Alta Disponibilidade e Disaster Recovery (HA/DR)

- **Backups:**
  - Configurados no **console do OCI**.
  - Destino é o **OCI Object Storage**.
  - São espelhados em 3 vias para durabilidade.
- **Data Guard:**
  - Configuração **totalmente automatizada** via console do OCI, seguindo as melhores práticas da MAA.
  - **Standby Local (Cross-AZ):** Protege contra falhas de um data center.
  - **Standby Remoto (Cross-Region):** Protege contra desastres regionais.
  - **DR Híbrido:** É possível configurar um Data Guard entre um banco on-premises e o Oracle Database@Azure.

5. Implementar Oracle Database@Google Cloud (20%)

Arquitetura e Onboarding

- **Arquitetura Core:** Semelhante ao Azure, com um **"OCI child site"** dentro de uma **Zone do Google Cloud**, conectado a uma região "parent" do OCI.
- **Onboarding:**
  - Adquirido via **Google Cloud Marketplace**.
  - **Private Offer:** Permite ADB e Exadata; pode usar uma conta OCI existente.
  - **Public Offer (PAYG):** Permite apenas ADB; **exige a criação de uma nova conta OCI**.

Provisionamento e Gerenciamento

- **Responsabilidade Dividida:**
  - **Google Cloud Console:** Provisiona a infraestrutura (ADB, Exadata Infra, VM Cluster).
  - **OCI Console:** Provisiona os bancos de dados (CDBs/PDBs).
- **Federação de Identidade:** Recomendada para um SSO transparente entre os consoles. O link "MANAGE IN OCI" no Google Console facilita a navegação.

Topologias de Rede

O serviço pode ser integrado a diferentes arquiteturas de rede no Google Cloud:

1. **Single VPC:** Aplicações e banco de dados na mesma VPC. Mais simples, menor latência.
2. **Multiple VPCs:** Isolação forte entre diferentes linhas de negócio.
3. **VPC Peering:** O banco de dados fica em uma VPC de trânsito centralizada, conectada às VPCs das aplicações via peering.
4. **Hub-and-Spoke:** Usa um Network Virtual Appliance (NVA) como hub para centralizar a segurança e o roteamento entre as VPCs (spokes).