

SaaS Tenant Isolation Strategies



AWS White Paper

CloudSiksha

Tenant Isolation

- Tenant isolation is fundamental to the design and development of (SaaS) systems.
- It enables SaaS providers to reassure customers that even in a multitenant environment their resources cannot be accessed by other tenants
- While the need for tenant isolation is viewed as essential to SaaS providers, the strategies and approaches to achieving this isolation are not universal.

Isolation: Key Tenets

- Isolation is not optional
- Authentication and Authorization does not equal isolation
- Isolation enforcement should not be left to service developers
- If there's not out-of-the box isolation solution, you may have to build it yourself
- Isolation is not a resource-level construct
- Domains may impose specific isolation requirements

Silo Isolation

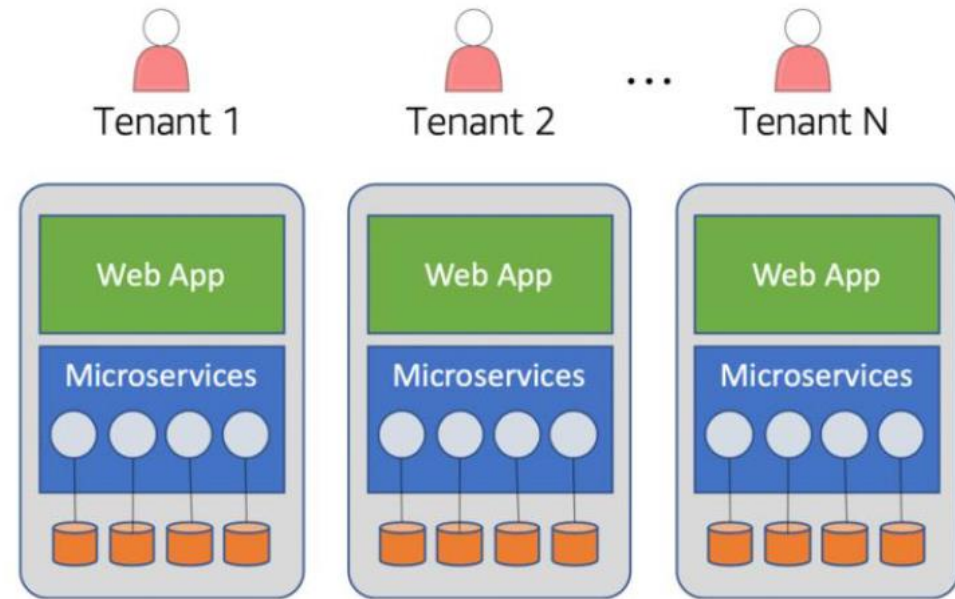


Figure 1 – Full Stack View of Isolation

Account Based Silos

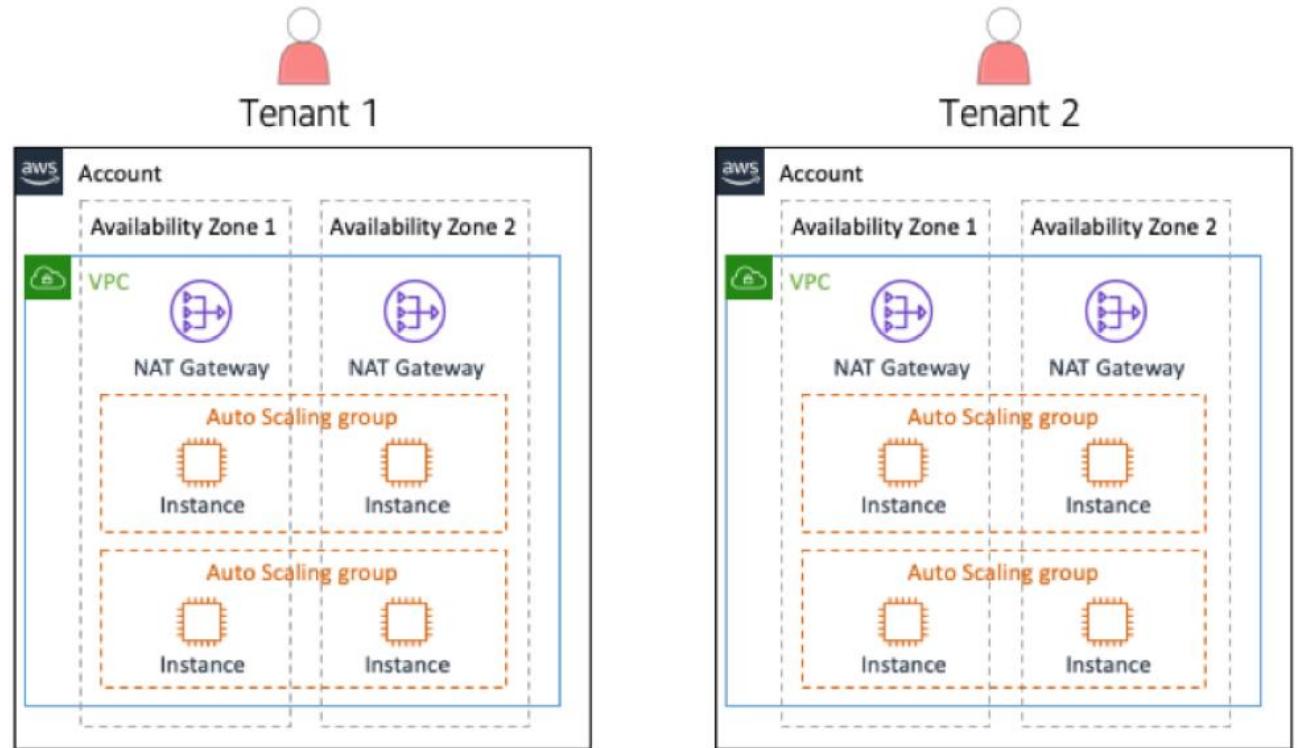


Figure 6 - Account-based Silo and Isolation

VPC Silo Isolation

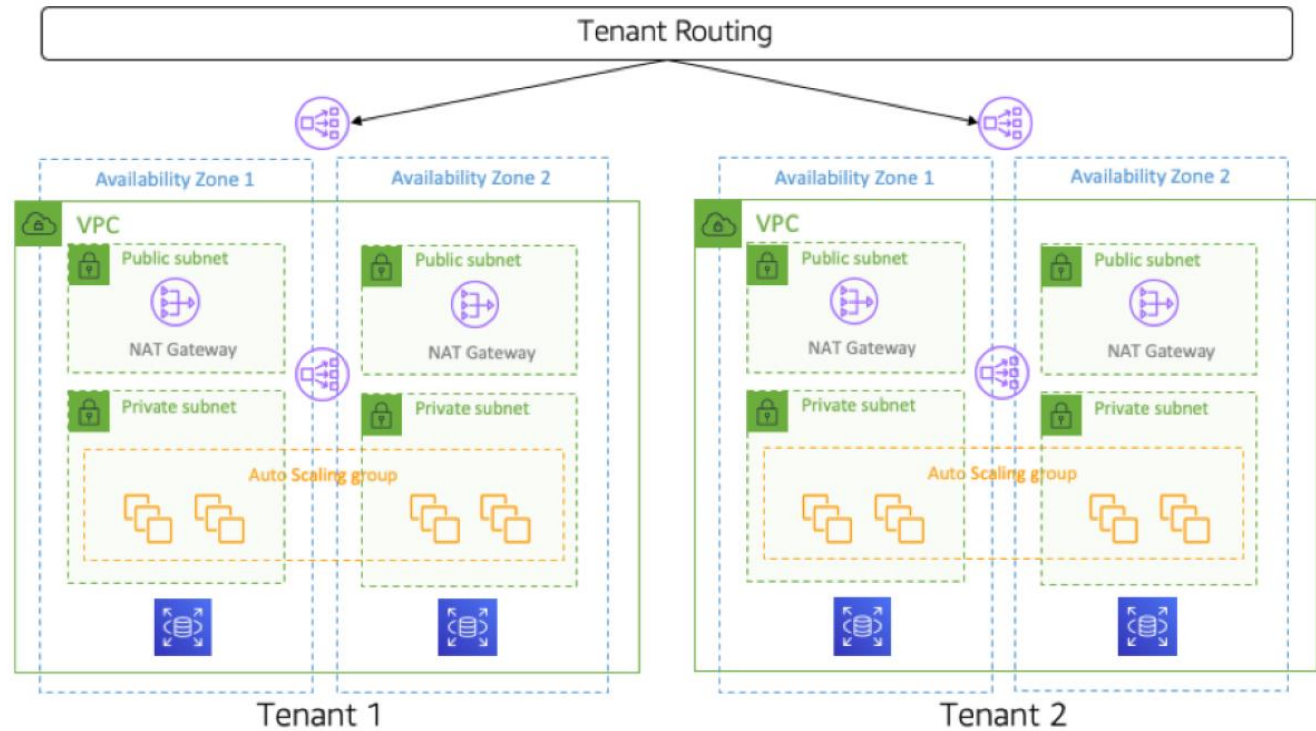
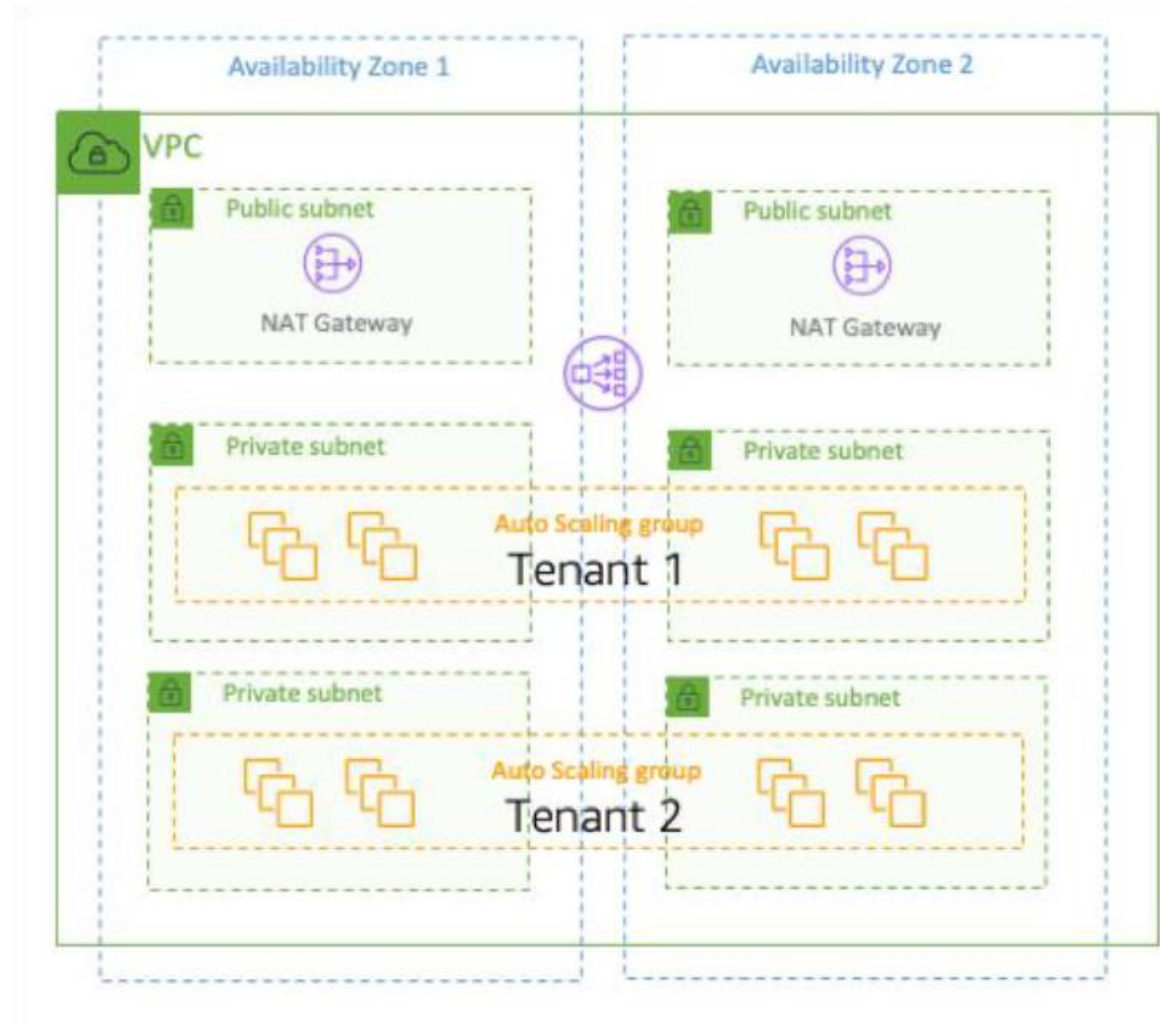
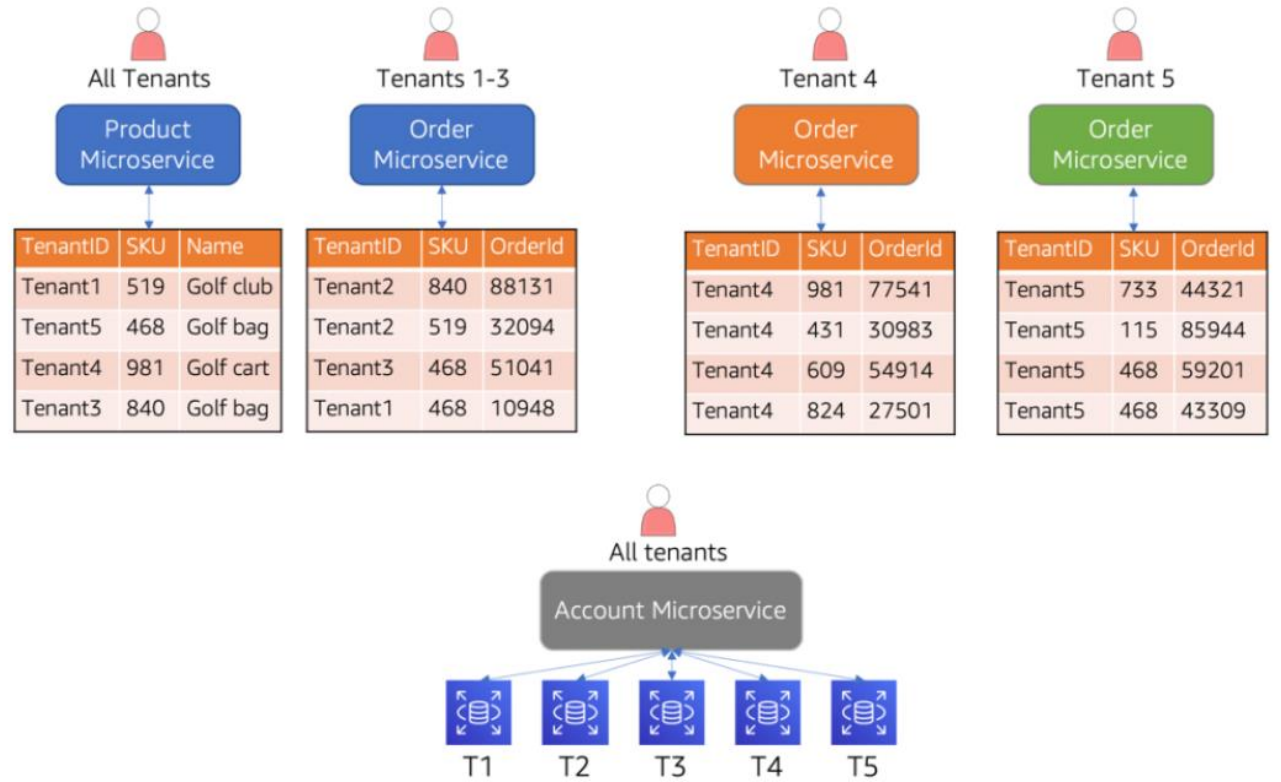


Figure 7 – VPC Silo Isolation

Subnet Silo Isolation



Targeted Silo Isolation



Container Silo Isolation



Pooled Isolation

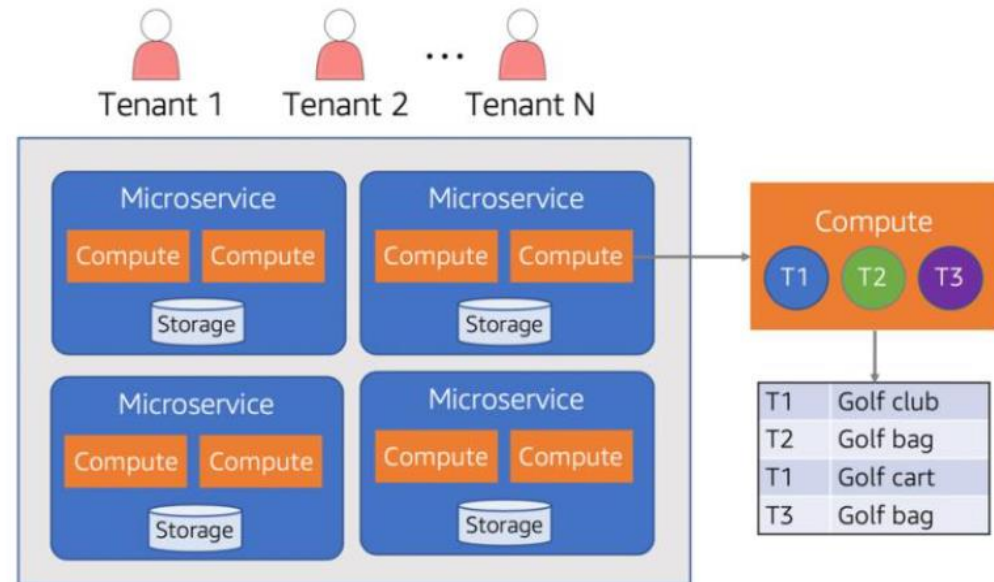
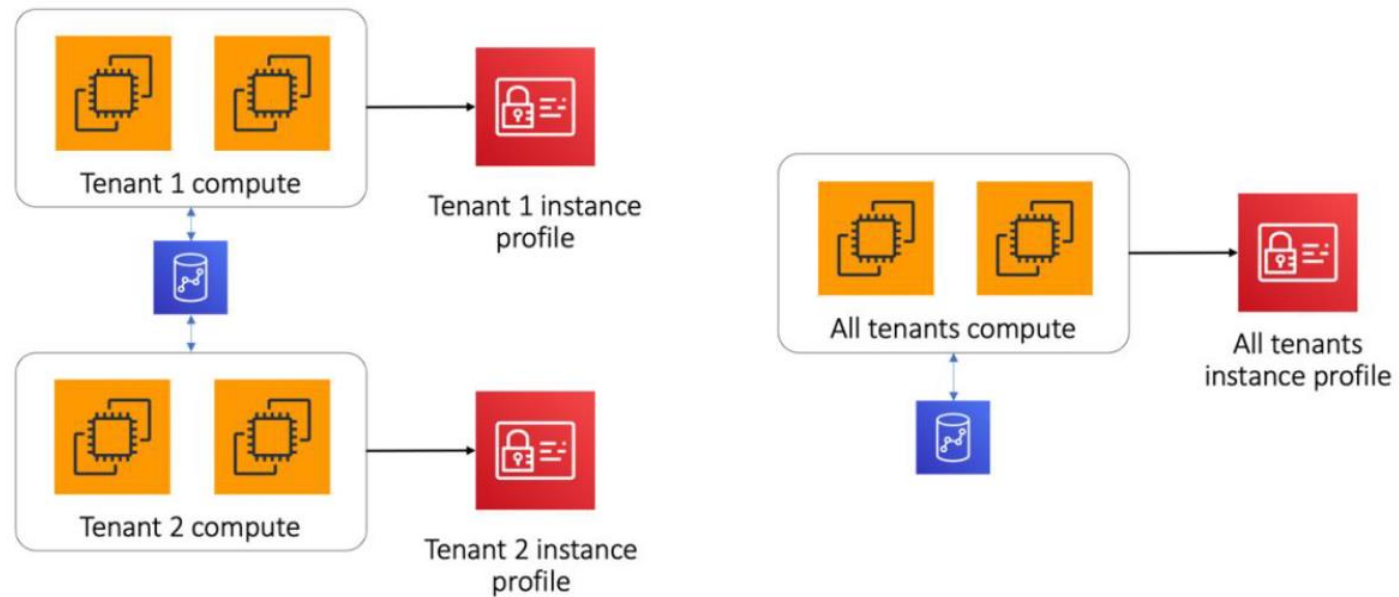


Figure 2 – Pooled Isolation

Identity and Isolation



Identity and Isolation

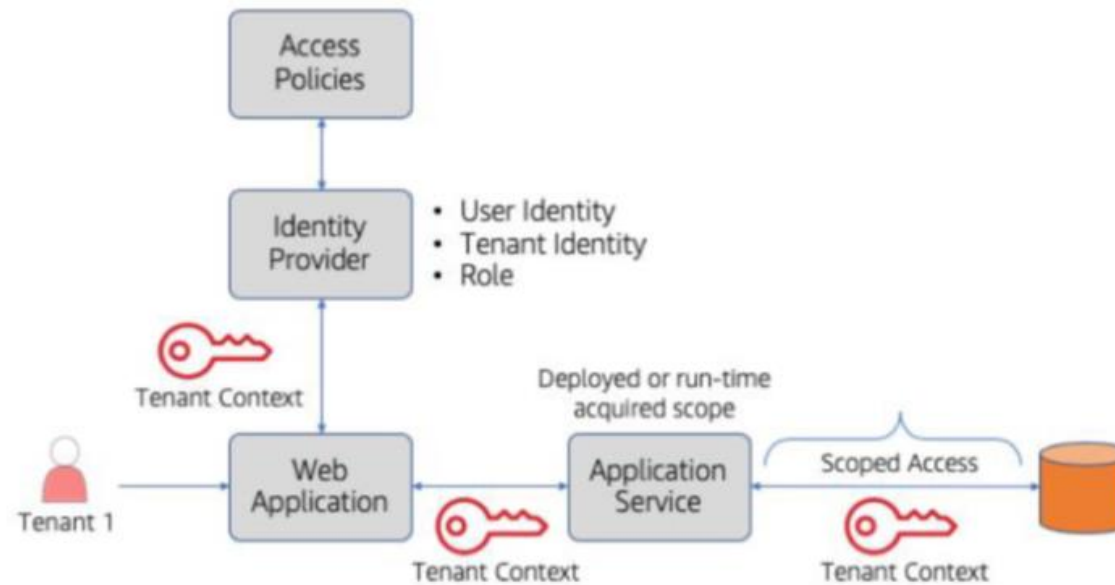
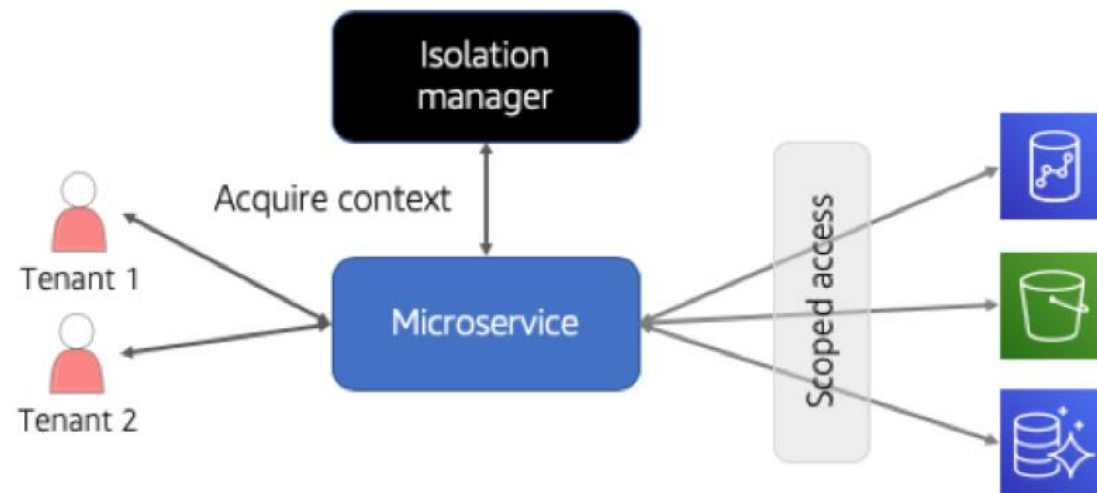
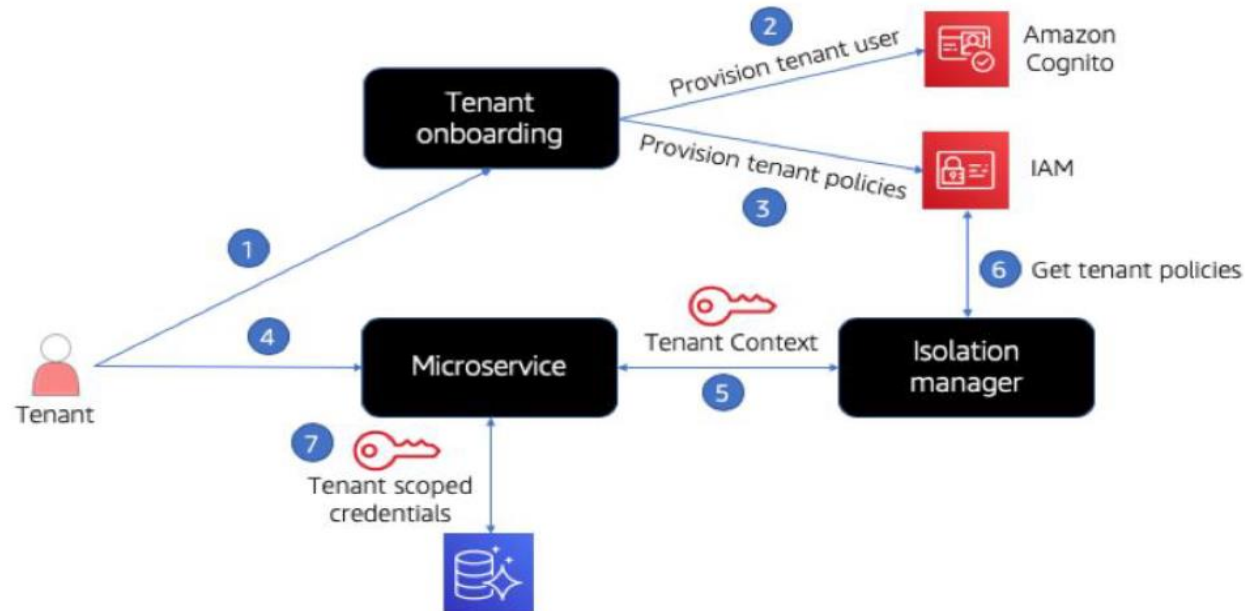


Figure 5 – Connecting Identity and Isolation

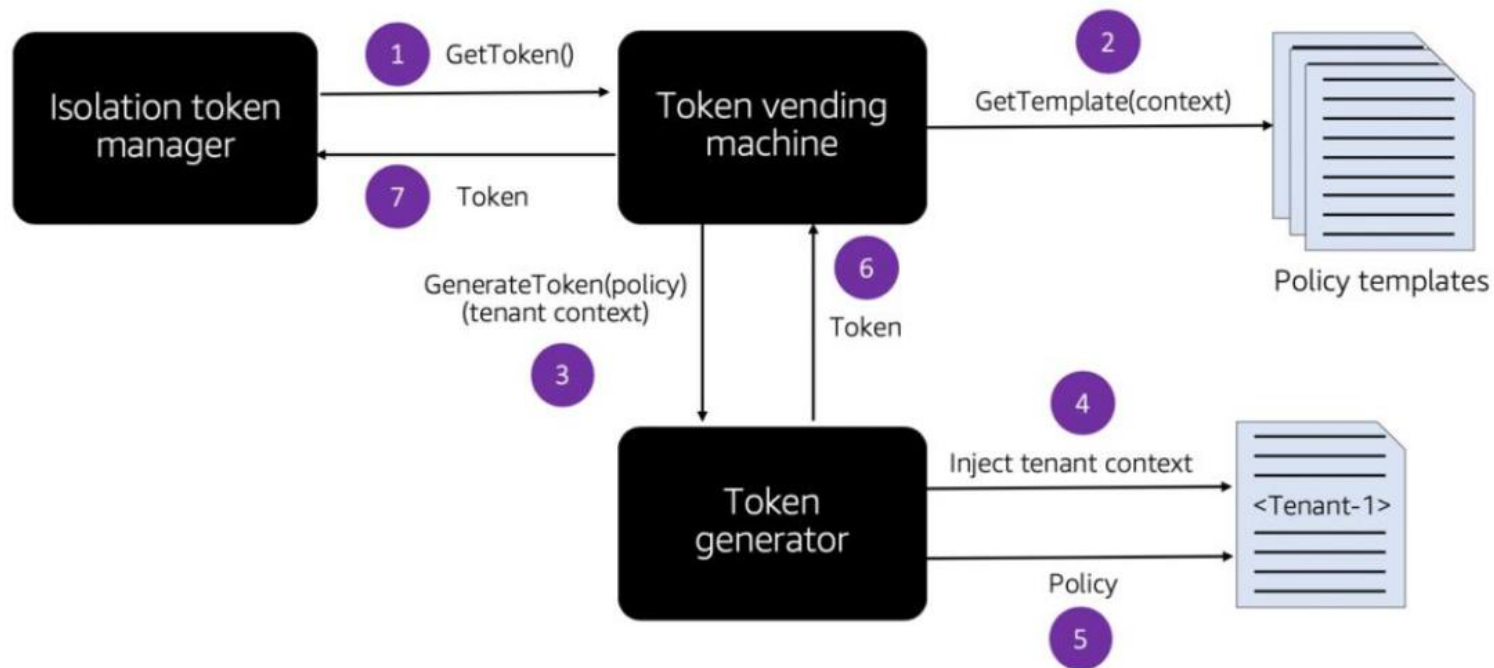
Run Time Policy Based Isolation



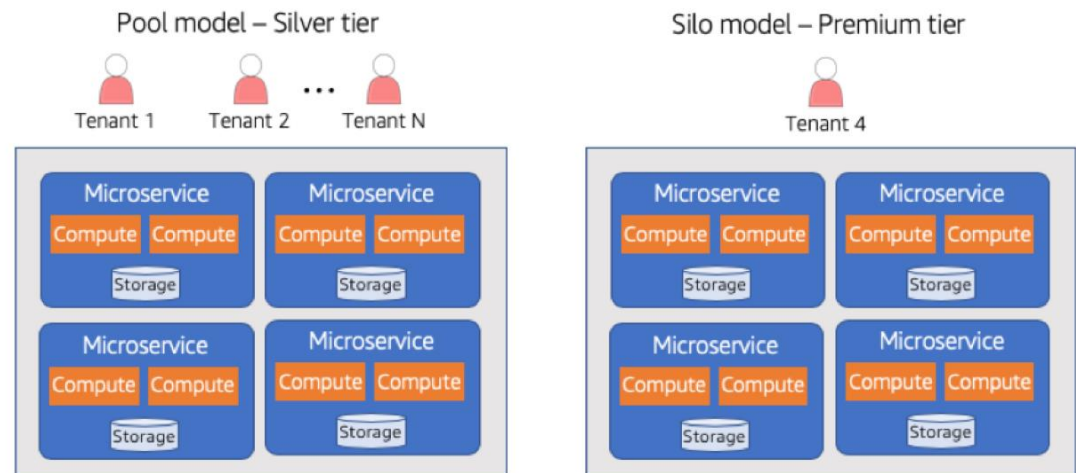
Scoping with IAM Policies



Dynamic Policy Generation



Tier Based Isolation



Bridge Isolation Model

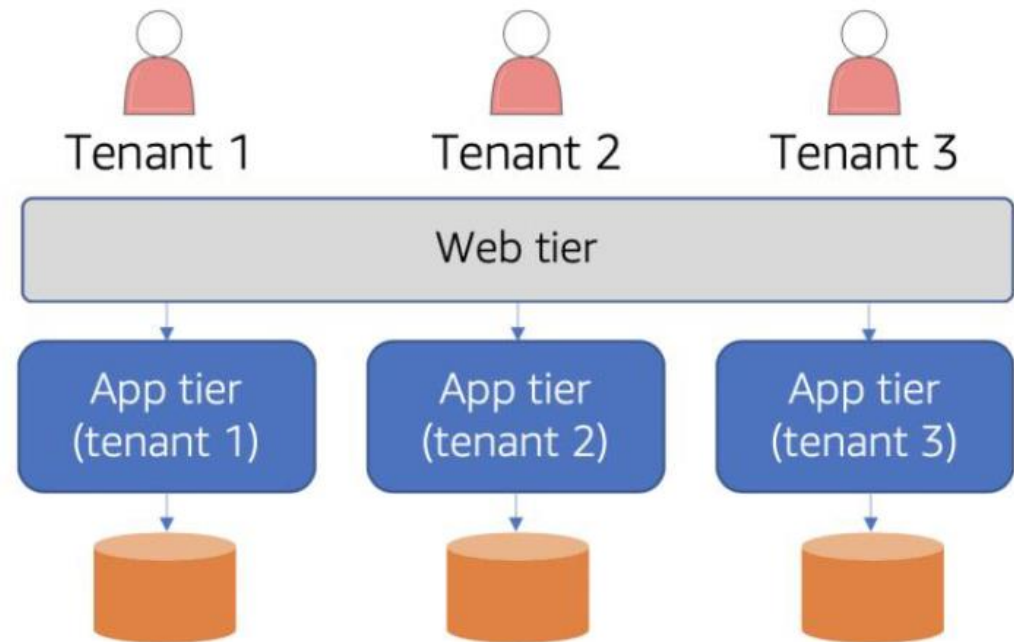


Figure 3 - Bridge Isolation Model

Thanks

CloudSiksha