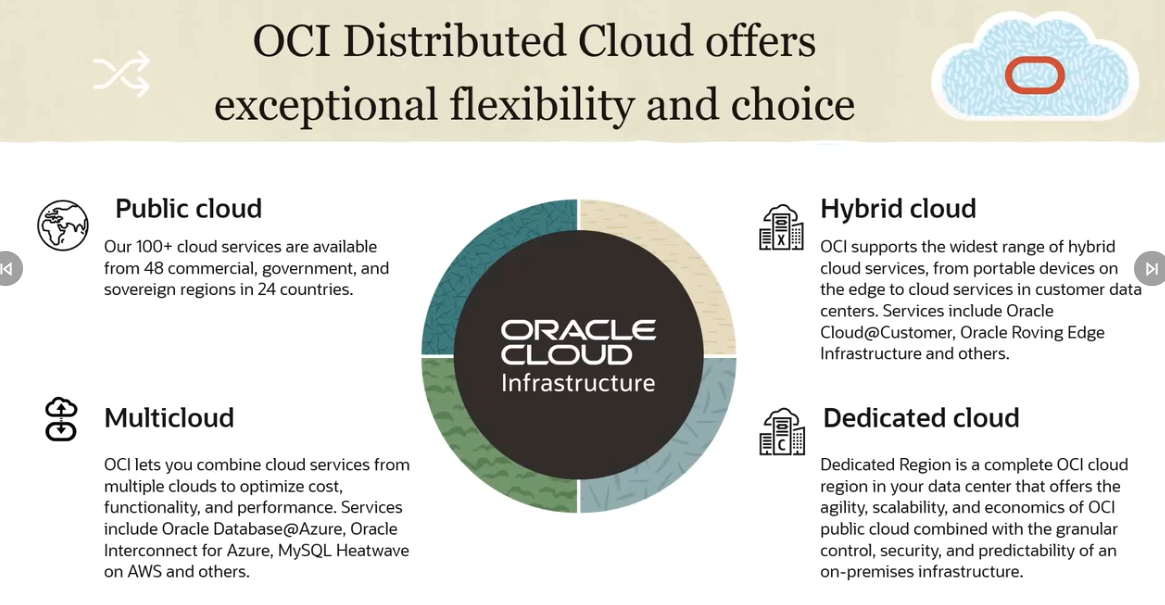
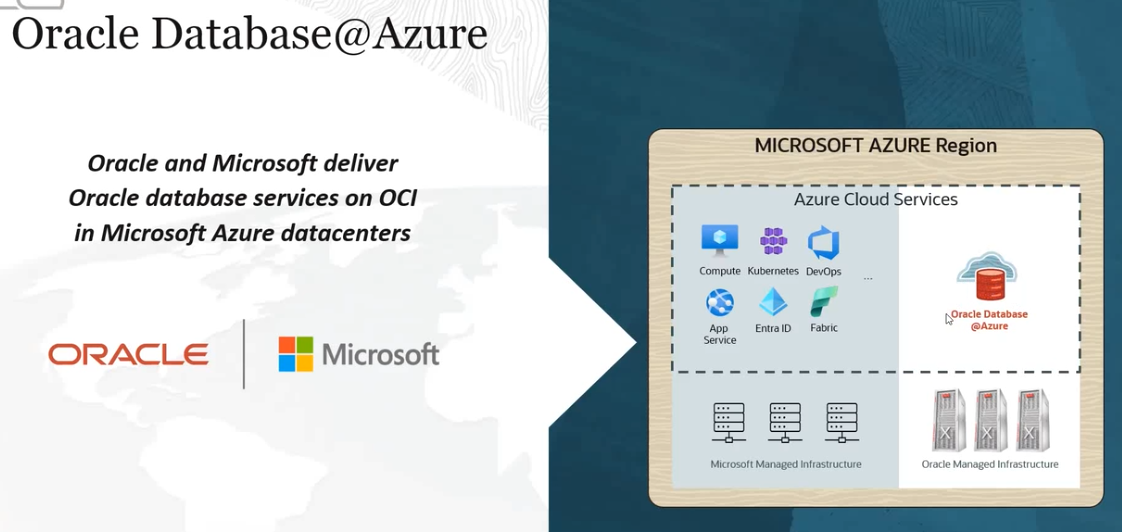


Let's summarize what we learned in this lesson. So we looked at region. Region comprises of availability domains. Availability domains comprise of fault domains. So let's look at the inside-out view. So first let's start with fault domain. Fault domain provide protection against failure within an availability domain. Availability domain themselves provide protection from entire availability domain failures, particularly in a multi-AD region.

And then you have this concept of region pair where in every country we operate on, most of the countries we operate, we have at least two data centers. So you could use the second data center for disaster recovery or backup, or it also helps you with to comply with data residency and compliance requirements. And then not only this, we also have SLAs on availability, management, and performance.

To recap, we looked at the physical architecture of OCI with regions, which are geolocations. We looked at availability domains. And then every availability domain has three fault domains. So use these architectural constructs to design your applications which are highly available and avoid single points of failure Thanks for watching.

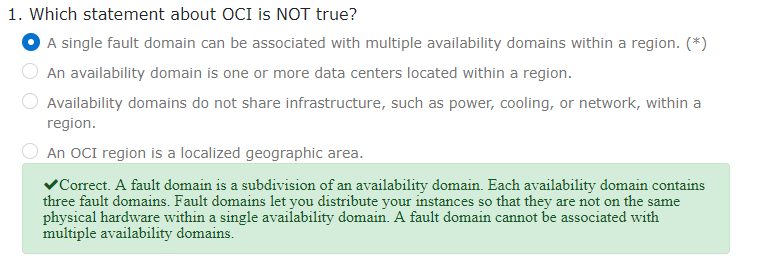


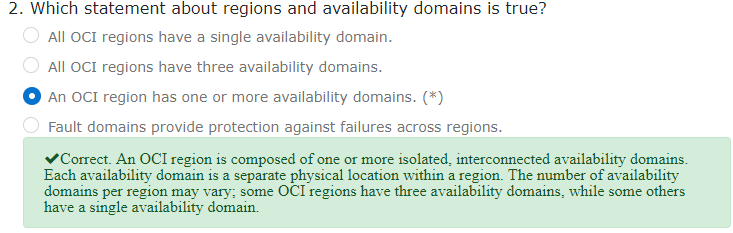


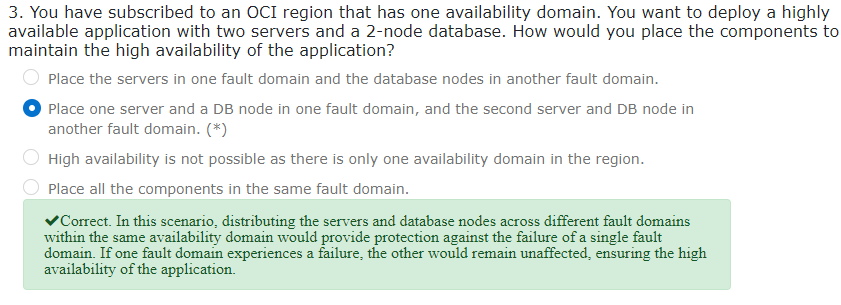


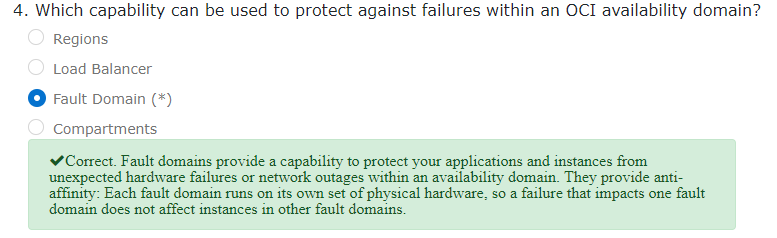
So in a nutshell, that's our distributed cloud story. There are three main advantages of using Distributed Cloud. First is you can deploy services where you need to or how you need to. So that's number one. Number two is you get the same platform, pricing, and experience across whether you are running in the public cloud, dedicated cloud, hybrid cloud, or multicloud.

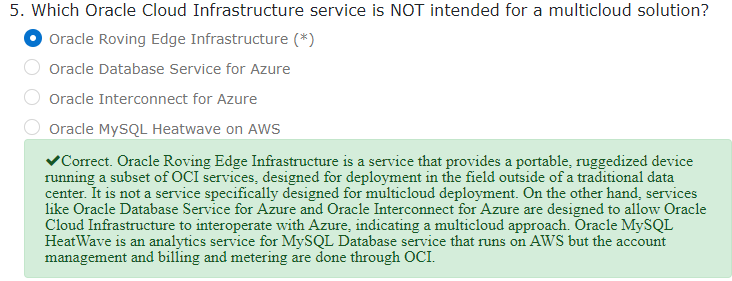
And then that's the second and then the third is you can address regulatory and sovereignty needs through offerings such as Dedicated Region and some of our hybrid services.

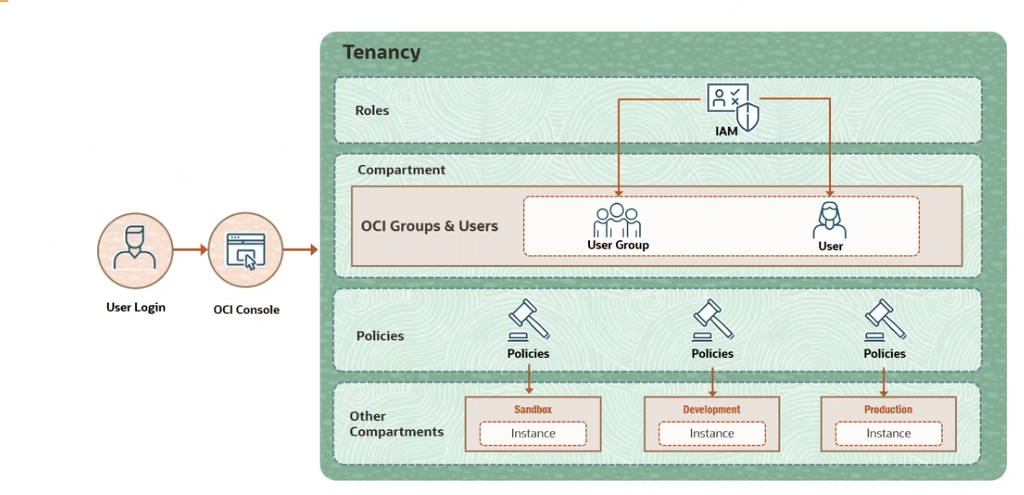












To wrap up, we looked at how you do authentication in OCI, the three mechanisms, user name, passwords, APIs signing keys, authentication tokens. And then we looked at how you do authorization in OCI through policies. Policies are really powerful. They are very easy to understand, human readable. But at the same time, they give you a lot of advanced capabilities to implement really fine-grained access control.



