The technical impact of the
ORACLE/MICROSOFT
cloud partnership

The announcement of the OCI/Azure interoperability deal made big headlines right across the tech industry. But what could this mean in reality for your organisation?

By Philip Brown

If you're new to the cloud then you may see Oracle's recent announcement of its 'cloud interoperability partnership' with Microsoft's Azure (see News, page 6) as a removal of technical barriers that will enable true multi-cloud architectures. But if you've been working with cloud for some time, you might think… hold on, I can do this already!

The Oracle and Microsoft partnership is a genuinely interesting development and a first within the industry. However, the immediately obvious possibility of connecting two clouds together isn't actually where the true benefit lies, in my opinion. Here, I'll drill into some of the detail and explain why.

CONNECTING CLOUDS

If you wanted to connect two clouds together – be it AWS, Oracle, Azure or GCP – you could already do this. Let's start at the beginning: with an on-premises-to-cloud connection, cloud providers

---

⏱ 10-SECOND SUMMARY

▸ **The ability to connect clouds is not a new thing – but it has often created complexity and performance issues.**

▸ **The biggest upside of the OCI/ Azure partnership is most likely to** be its Unified Cloud Management.

▸ **As multi-cloud environments become more commonplace, the partnership is likely to help simplify connections, creating real user benefits.**

---

offer a site-to-site VPN-as-a-Service (VPNaaS) connection. This allows you to deploy a VPN endpoint in your cloud virtual network then specify the IP ranges and routing to enable traffic to flow between your on-premises site and the cloud. For all cloud providers, the cloud side of the ▶

VPN is nothing more than specifying a few settings in the UI and then completing the configuration of your on-premises VPN endpoint / firewall normally administered by the network team (see Figure 1).

Networking teams see VPNs as a security minimum if they are to connect an on-premises network to the cloud network – and it's always been very easy to set up. All cloud providers' VPNs have the ability to support different Phase 1 and Phase 2 configurations which means that *most* on-premises endpoints have a reasonable chance of getting connected, unless you're using really old or obscure configurations.

The challenge with VPNaaS is that you can't connect one VPNaaS to another. VPNaaS works primarily due to the fact that the main configuration is done on your on-premises equipment – which means you're very limited as to what you can specify in the VPNaaS configuration and the connection is established once you've added the VPNaaS settings / IPs into your on-premises equipment. Therefore connecting Azure and Oracle together using the VPNaaS is impossible as they're both expecting the bulk of the configuration to be done on 'the other side' as one VPNaaS is not designed to work against another VPNaaS.

The typical way to connect two clouds together is to use one side's VPNaaS and then, on the other side, to create an IaaS Virtual Machine and deploy something like StrongSwan to act as the VPN endpoint (see Figure 2). Deploying a software VPN in IaaS enables you to have more control of the configuration and hence is something akin to having your own VPN appliance.

The challenge with this approach is that, now you have an IaaS instance that you need to manage, you potentially need to make it high-availability, plus there are all the other issues of patching and maintenance which come into play.

Also, this connection is across the internet which means it may suffer from latency problems and not deliver a consistent level of performance. This solution works, but if performance levels are important, you will need to make use of dedicated connections.

> Since most enterprises are running Oracle and Microsoft workloads, this partnership will be of great benefit to them

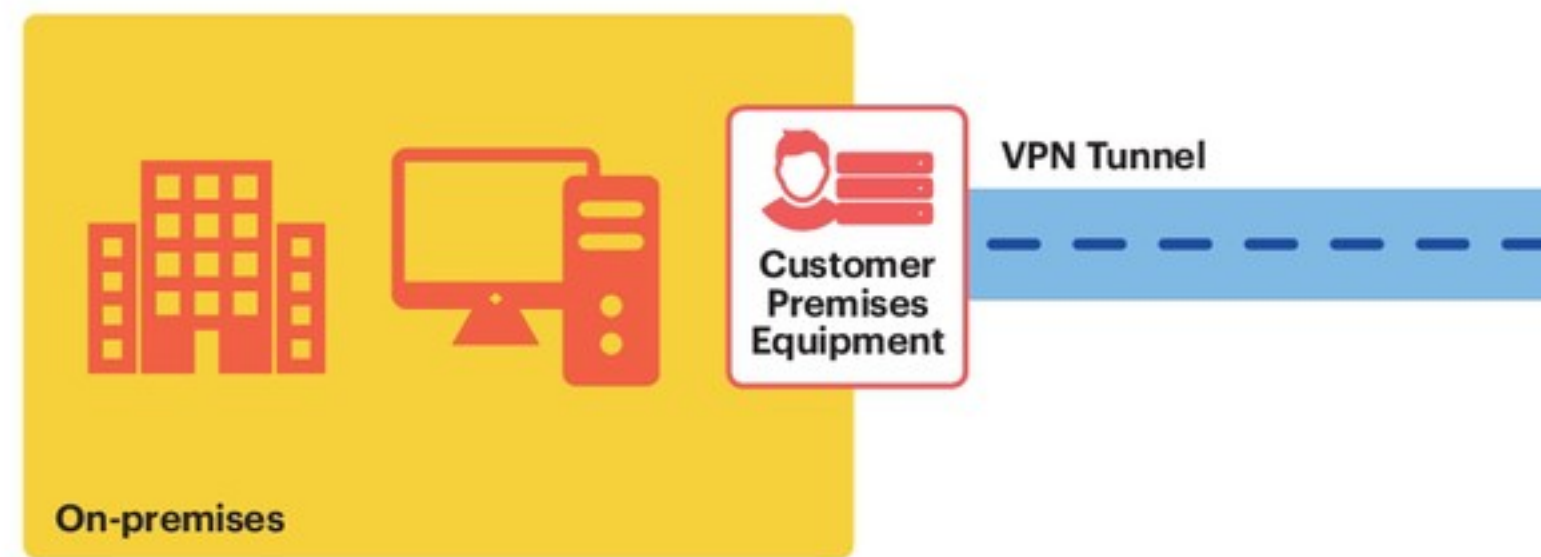**Figure 1:** Connectivity from on-premises to Oracle Cloud

VPN Tunnel
Customer Premises Equipment
On-premises

Figure 2: How you would historically connect another cloud to Oracle Cloud

IaaS VM machine 'acts' as the on-premises equipment which enables the VPN tunnel to be established as you have more control over and above a Cloud VPNaaS option
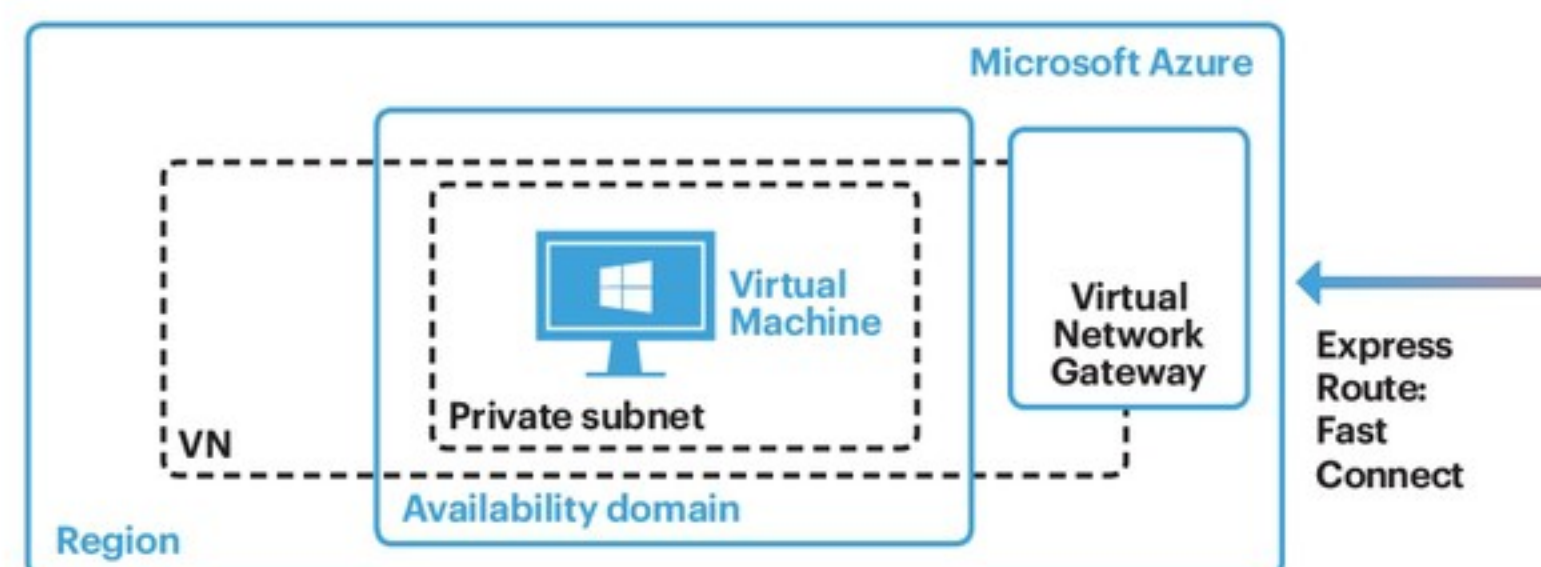
Virtual Machine

VPN Tunnel
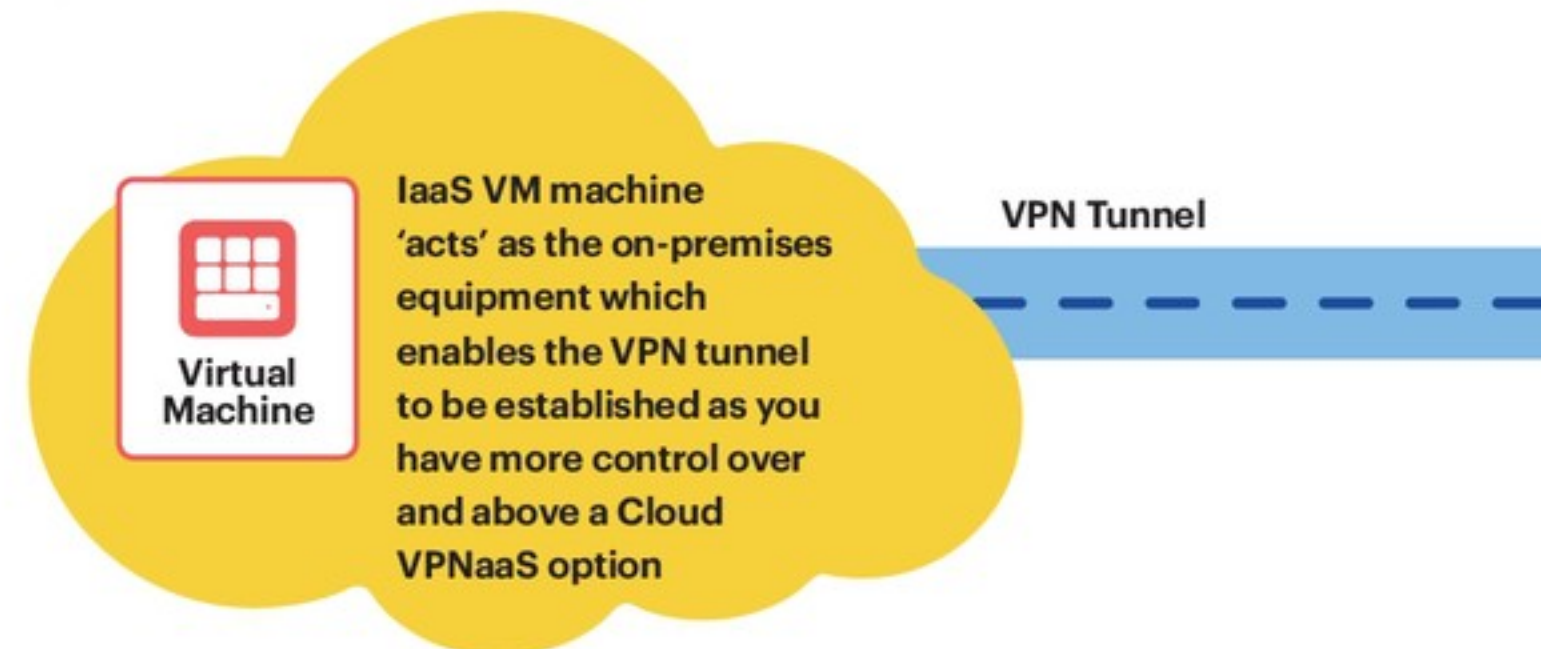
Figure 3: Direct connectivity between clouds using Express Route and Fast Connect

Microsoft Azure
Virtual Machine
Private subnet
Virtual Network Gateway
VN
Availability domain
Region
Express Route: Fast Connect

Dedicated cloud connections have been around as long as VPNs, and like VPNs they are relatively easy to set up, but normally require some additional plumbing between your on-premises data centres and the cloud provider's. A recent innovation, however, has been the dedicated inter-cloud connectivity provided by companies like Megaport and Equinix.

At the same time, cloud exchanges have been providing the ability to link two dedicated cloud connections from two different cloud providers – so, for example, you could have your Azure Express Route linked directly to your Oracle Fast Connect. The great thing about this is that the traffic between the two clouds doesn't go via your on-premises network and there isn't any additional plumbing to be configured as the cloud exchanges already have the connections in place. I've seen this configured in real time and it's impressive.
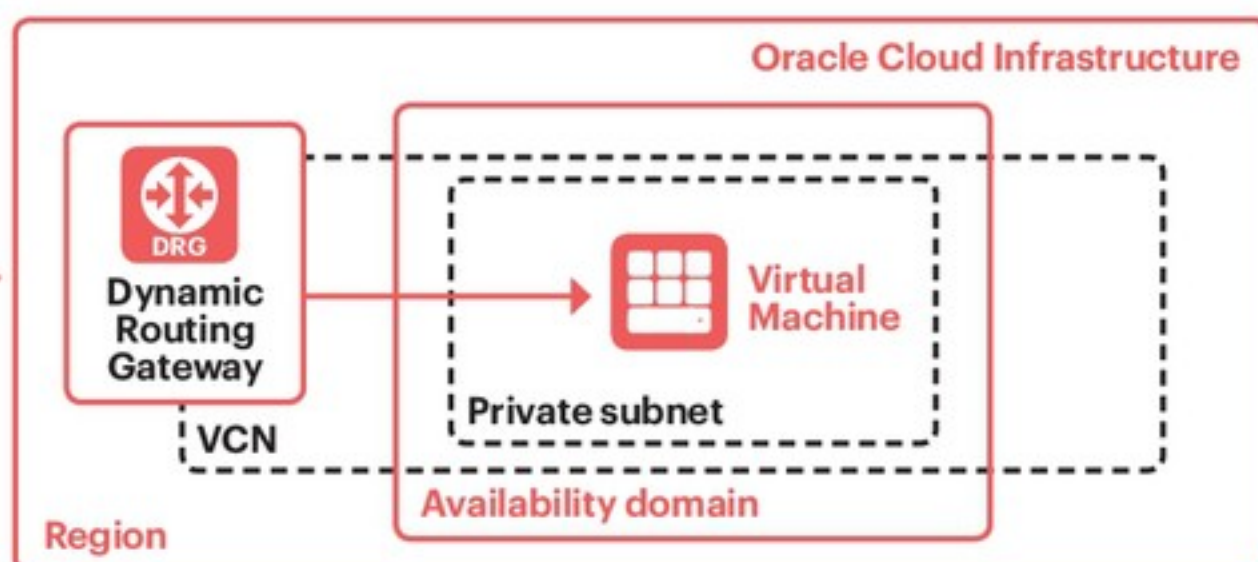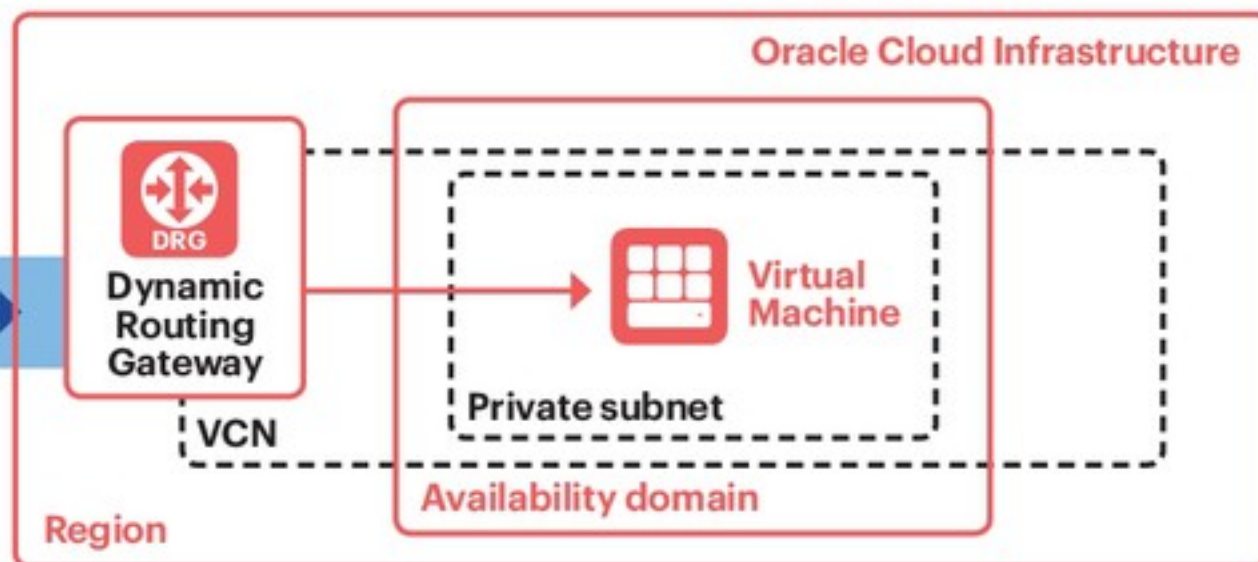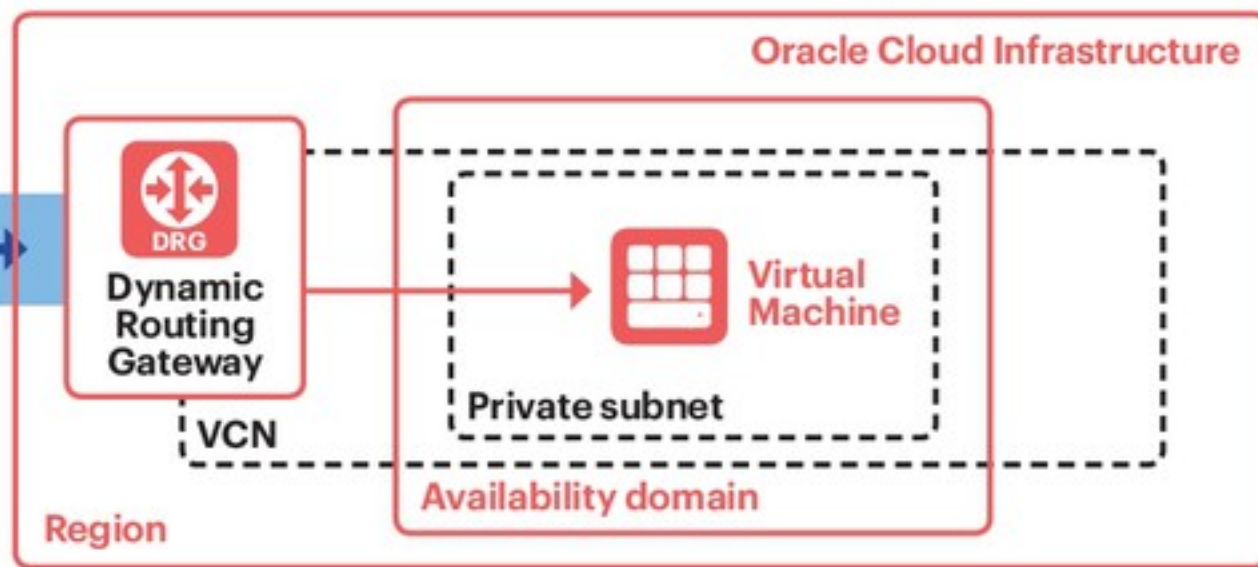
ABOUT THE AUTHOR

Philip Brown is head of Oracle Cloud Services at DSP. He's an Oracle ACE and has been presenting and writing articles for the technical community for over 10 years.

It's also worth pointing out that this inter-cloud connectivity using cloud exchange *isn't* like a VPN solution in the sense that traffic isn't encrypted. It's a dedicated private connection so it's secure, but if you require encryption from a compliance perspective then a dedicated connection alone will not provide it. The same is true for using Express Route or Direct Connect from on-premises to the Cloud – they are dedicated connections and not VPNs.

IS THE PARTNERSHIP JUST HYPE?

So, if you could do this before with VPNs, or if I can do this now with cloud exchanges, then surely this partnership is no more than hype? Well… not really. The enabling of inter-cloud connectivity without a cloud exchange is likely to lead to a lower total cost of ownership for that connection, which is good. But, what's more, it

will be a fully-managed and highly-available connection that doesn't require complex networking between multi-cloud deployments (see Figure 3).

The connectivity of clouds is great, of course, and anything that reduces the cost and complexity can only be seen as a benefit. However, it really gets interesting when you can manage both Azure and Oracle from a single cloud UI.

Unified Identity and Access Management (IAM) seems like the least exciting element of this partnership, but in reality it could turn out to be the most important. This is because cloud security – i.e. the security of the cloud console and its users – will always be a challenge in a multi-cloud environment. You will have two UIs which gives you two different users who then require two different security policies which have different policy language to configure. The problem this creates is either one of laziness or complexity.

Laziness simply means that it's easier to administer your multi-cloud environment with two super administrators, which isn't great. This goes against the principle of least privilege, and super admins in a cloud console can ultimately affect the security of the resources running in the cloud (think ingress and egress rules for VM access). Therefore, this is not an approach we would want to endorse.

Complexity means you need to create lots of users and policies to manage cloud security across these two cloud portals. This fixes the issue of least privilege but the resulting complexity can lead to mistakes and misconfiguration.

The partnership talks about the future capabilities of unified IAM and the ability to control both Azure and Oracle resources from a single pane of glass. There are increasingly blurred lines on corporate and cloud infrastructure which has led to the switch from perimeter network security to asset security – so anything that provides simplicity must be seen as a massive advantage.

Oracle have also stated that there will be a joint support model, which again points towards creating additional simplicity in a multi-cloud environment.

Since most enterprise organisations are running both Oracle and Microsoft workloads, this partnership is likely to be of great benefit to them. At the end of the day, it boils down to simplicity – in terms of the networking connectivity but, more importantly, the management of what's only going to become a more commonplace scenario in the coming years: multi-cloud environments. ⊠