



Microsoft meets Community: Windows Virtual Desktop

Disaster Recovery and Business Continuity (BCDR)
options for Windows Virtual Desktop

Ryan Mangan
CTO @ appCURE

Twitter Handle @Rymangan / ryanmangansitblog.com

3rd edition

Contents

- Meet the Speaker
- Introduction
- Networking
- Virtual Machines
- Managing Identities
- Shared Image Galleries
- FSLogix Profile Containers
- MSIX App attach
- Summary

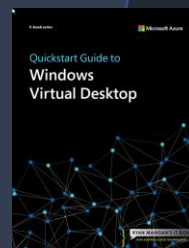


Ryan Mangan
Data Centre & Cloud Technologist

Twitter: @rymangan
Blog: Ryanmangansitblog.com

Ryan is an end-user computing (EUC) specialist & Cloud technologist. Currently works for AppCURE and Systech IT Solutions. A speaker and presenter, who has helped customers and technical communities with end-user computing solutions, ranging from small to global 30,000-user deployments in various Fields. Ryan is the owner and author of ryanmangansitblog.com which currently has over 3 million visitors and over 200+ articles on Windows Virtual Desktop, Remote Desktop Services and VMware. Some of Ryan's community and technical awards include:

- VMware vExpert***** Seven years running
- Parallels RAS VIPP 2019, 2020
- LoginVSI Technology Advocate
- Technical person of the year 2017 KEMP Technologies
- Parallels RAS EMEA Technical Champion 2018
- Microsoft Community Speaker
- Experts Exchange Verified Expert
- Top 50 IT Blogs 2020 – Feedspot
- Top 50 Azure Blogs 2020 – Feedspot
- Author of “Quickstart guide of Windows Virtual Desktop”



Introduction

Traditional vs Cloud VDI Disaster Recovery Options

- Traditional solutions can be expensive with a up front capital cost associated.
- Potentially complex in design, management and maintaining.
- Physical outages can have an impact *“waiting for physical resources the restored or replaced”*.
- Connectivity limitations – speed of which you can replicate and restore

What does the “Cloud” offer

- Access 54 data centres across multiple geographic regions. These are typically 100's of miles apart.
- You can access Microsoft Azure in over 140 countries.
- Opex Expenditure (monthly subscriptions / consumption), pay for what you consume.
- Connect existing services to MS Azure. This could be on-premises or Multi cloud.

What Does This Mean for Windows Virtual Desktop.















- Fast Recovery times, utilising Microsoft's core infrastructure.
- Multiple regions accessible from a single Web browser
- Take advantage of Microsoft's Multi-Session Desktop providing a Windows 10 experience across regions.
- No Physical Hardware to worry about.

Find out where your nearest datacentre is

<http://azurespeedtest.azurewebsites.net/>

Azure Speed Test 2.0

Measuring the latency from your web browser to the Blob Storage Service in each of the Microsoft Azure Data Centers.

Data Center	Average Latency	History
 South UK	20ms	
 West UK	28ms	
 France Central	29ms	
 North Europe	30ms	
 West Europe	31ms	
 Switzerland West	35ms	
 Germany North	38ms	
 Switzerland North	39ms	

Windows Virtual Desktop BCDR Summarised

- Replication of Virtual Machines to a second location
- Standby Virtual Machines in a secondary location
- Profile container access from the secondary location
- User identities (Domain Controllers) are accessible / available in the secondary location
- Line-of-business applications are accessible from the secondary location.

Reserved instances

- Reduce the cost of virtual machines by using Reserved instances.

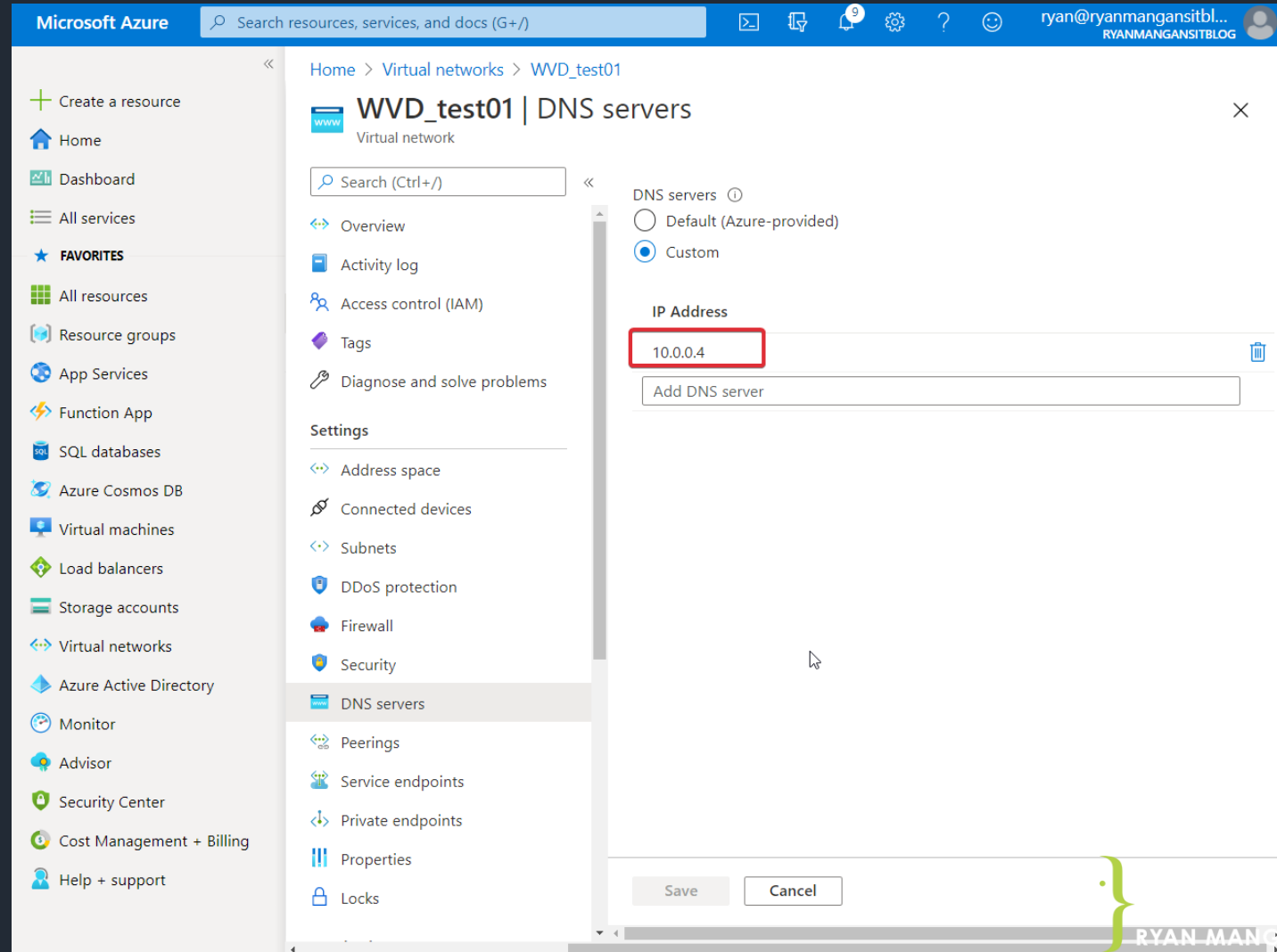
Networking

Consider your networking during an outage

- A vNET must be setup in the second region.
- For users who need access to on-premises resources, you will also need to ensure the VNET can access them. This can be done using a VPN, NVA, ExpressRoute, or virtual WAN.
- Azure Site Recovery (ASR) is recommended for setting up a VNET in the failover region as it preserves your primary networks settings whereas peering does not.

DNS.... DNS... DNS...

- Does your failover region have the correct DNS settings ?

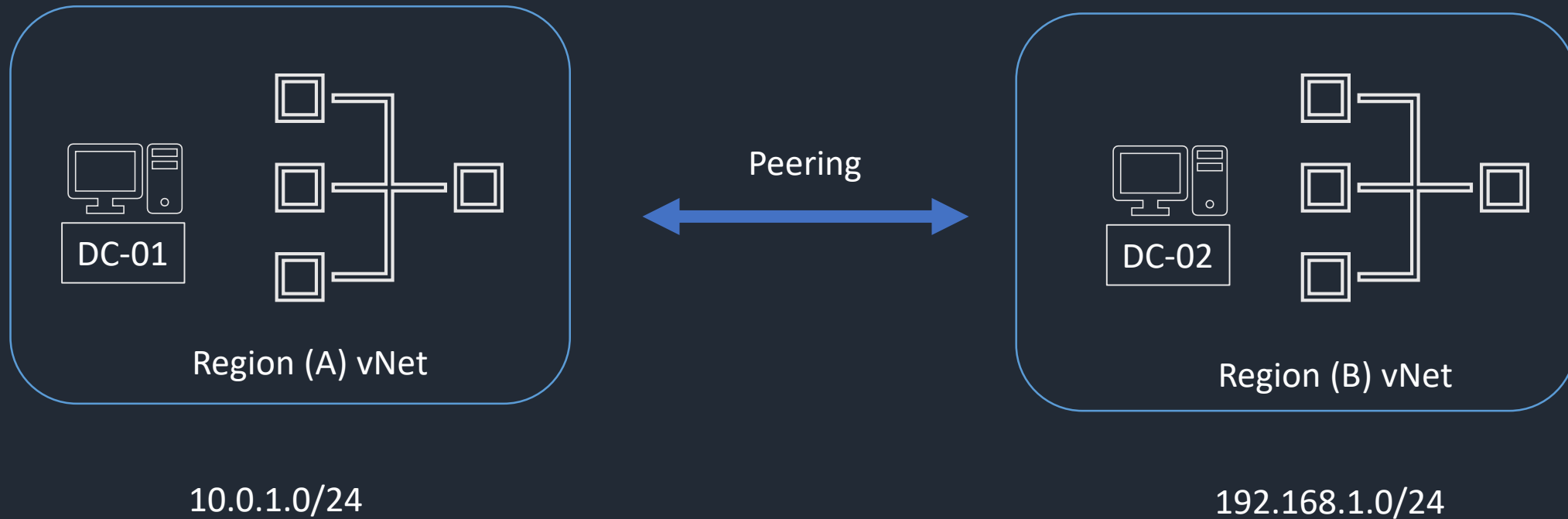


The screenshot displays the Microsoft Azure portal interface. The main content area shows the configuration for the virtual network 'WVD_test01'. Under the 'DNS servers' section, the 'Custom' option is selected. The 'IP Address' field contains the value '10.0.0.4', which is highlighted with a red box. Below this field is an 'Add DNS server' input box. At the bottom of the configuration pane, there are 'Save' and 'Cancel' buttons. The left sidebar shows the navigation menu with 'Virtual networks' selected. The top navigation bar includes the search bar and user profile information.

Using a Network Virtual Appliance (NVA)

- Have you included all the required Microsoft exceptions / Rules for Windows Virtual Desktop.
- Can the NVA communicate correctly with the WVD Management plane.
- Make sure you test...

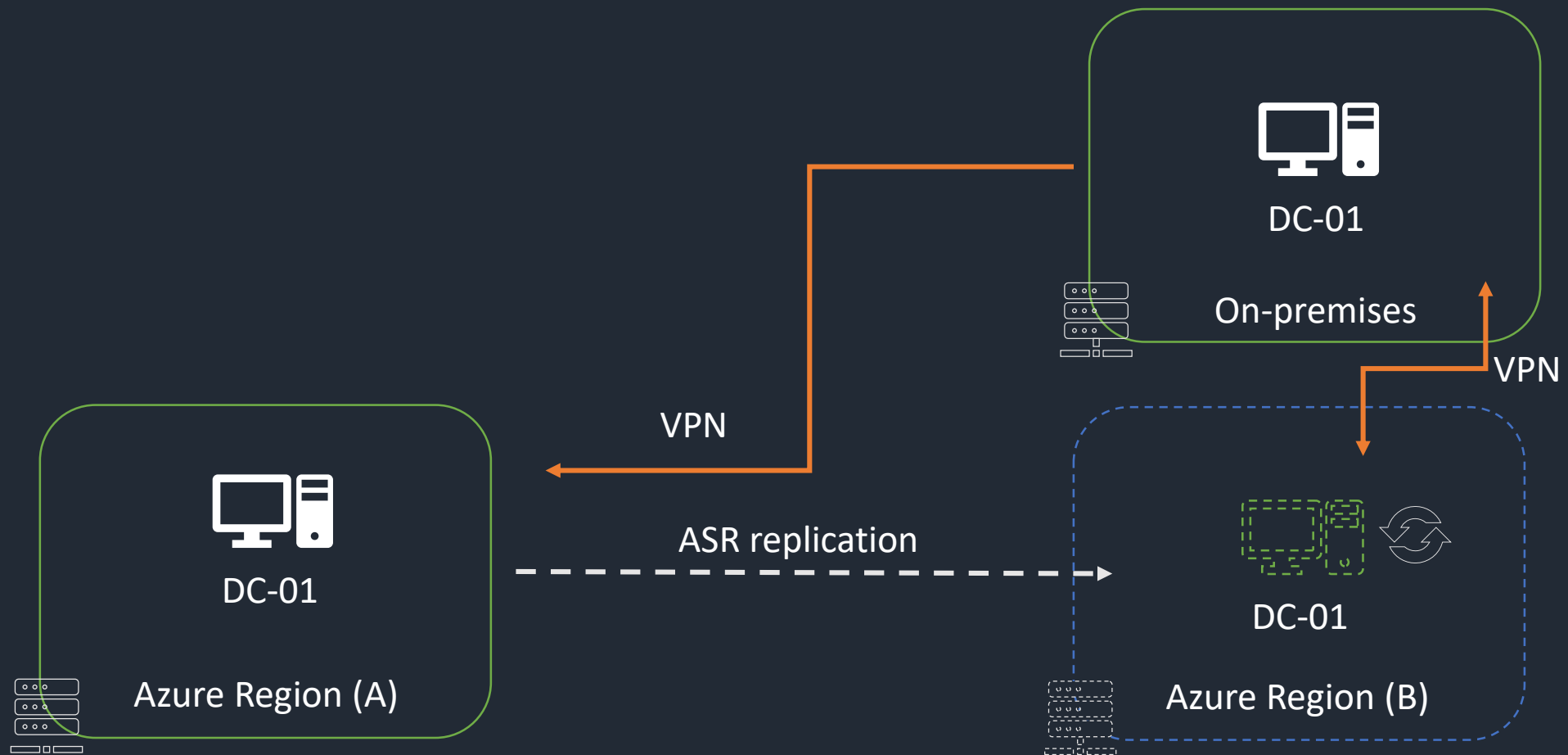
What does peering look like



Domain controllers in Azure



Domain controllers in Azure



Virtual Machines

Virtual Machine Options

- Azure Site Recovery (ASR) replicate all your VM's in the Second region
- Create a New Host Pool in the second region and leave Turned Off
- A single host pool with Virtual Machines from two regions. Leave Region two VM's turned off.

You have an Outage – Before you do anything

You need to end user sessions in the current region

1. WVD Classic: `Invoke-RdsUserSessionLogoff`

OR

2. Azure-Integrated Version of Windows Virtual Desktop: `Remove-AzWvdUserSession`

Once all Users are signed out of the primary region, you can then failover the virtual machines.

Demo of WVD Session Host Failover

Managing Identities

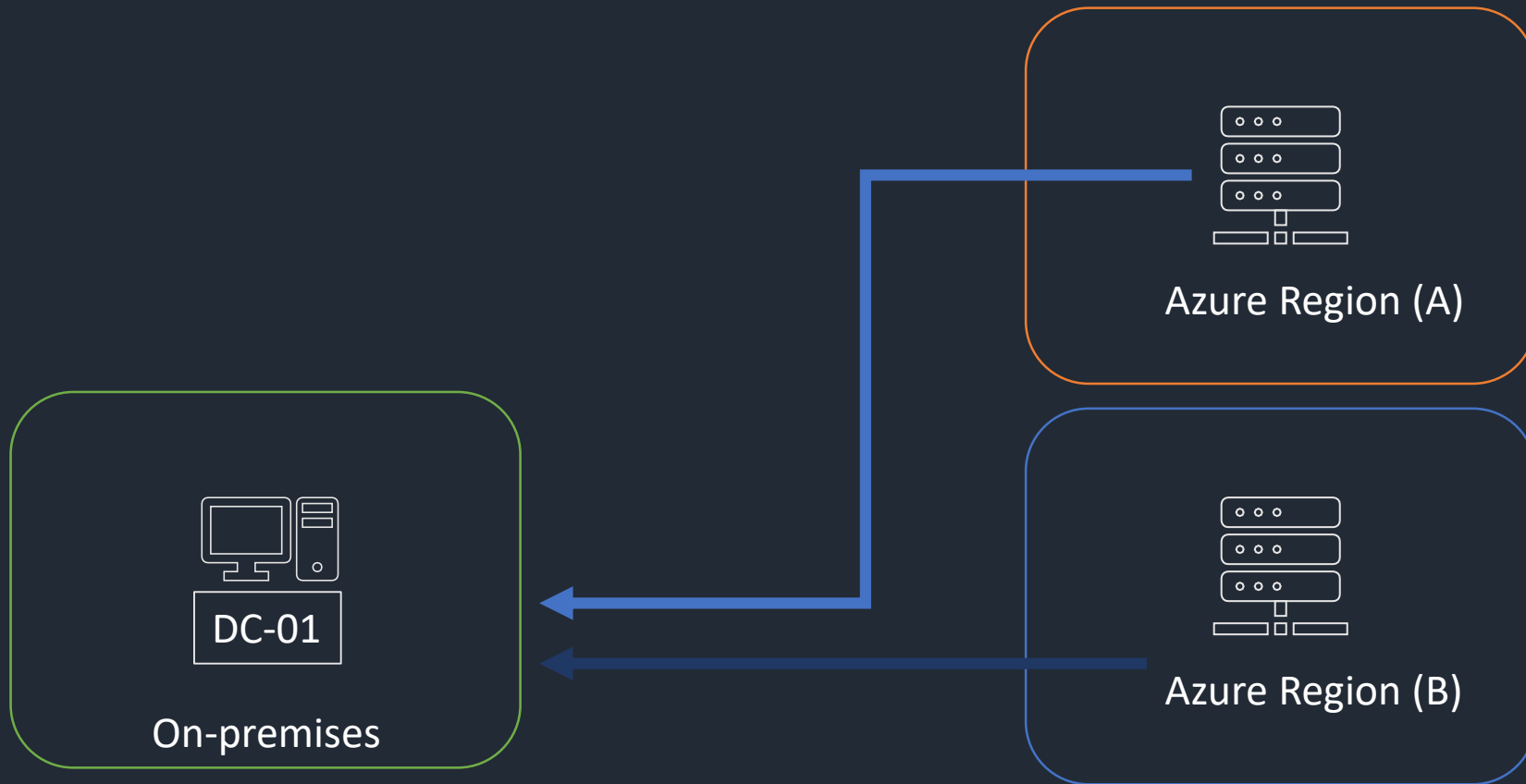
Domain Controllers

- With most things Windows related, you need a Domain. This includes Windows Virtual Desktop
- There are several options available to you.
- Communication on the primary and secondary region must be able to communicate with AD DS or Azure AD DS.

Three ways to keep the domain controller available

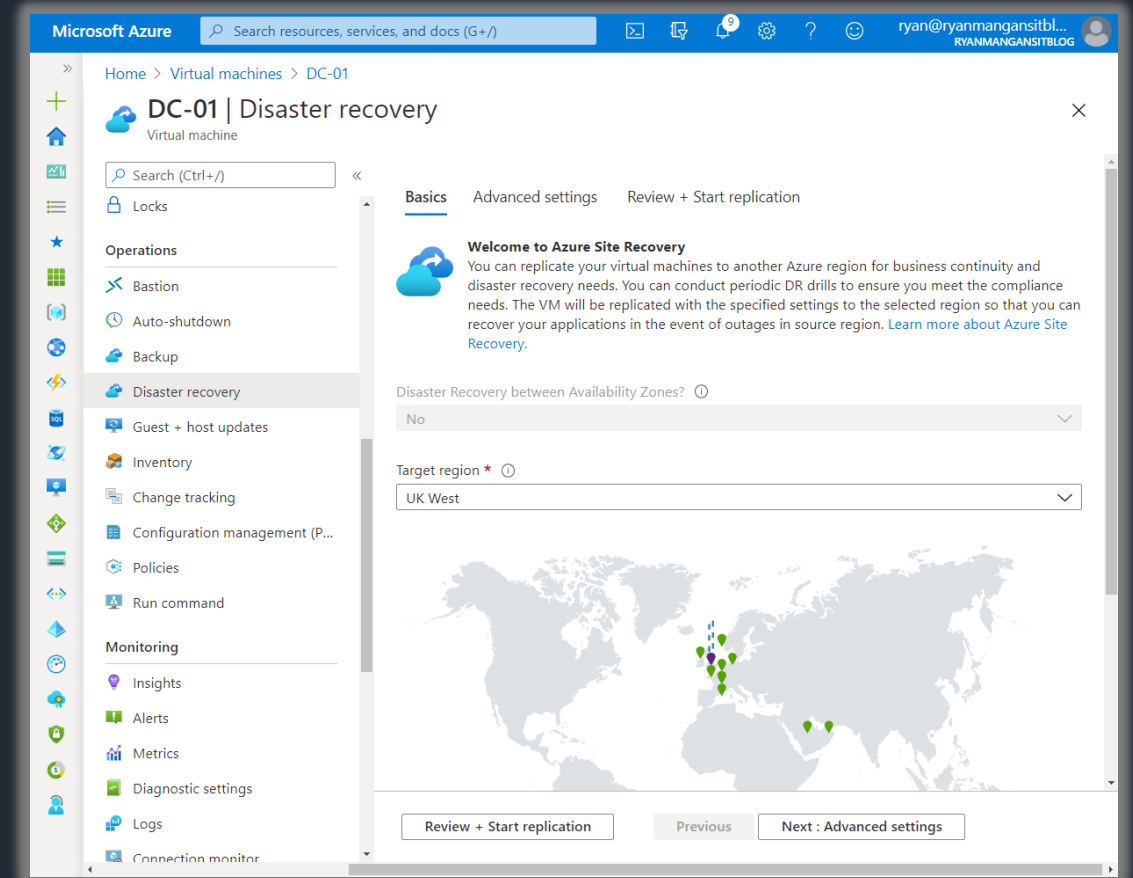
- Have Active Directory Domain Controller at secondary location
- Use an on-premises Active Directory Domain Controller
- Replicate Active Directory Domain Controller using [Azure Site Recovery](#)

Azure Regions accessing a DC via VPN



Some of the options available to you.

- Use ASR to replicate your Domain controller between primary and failover regions.
- Deploy a DC to your failover region.
- Link your secondary region back to on-premises.



Shared Image Galleries (SIG)

Shared Image Gallery (SIG)

- Replicate Windows 10 Images from the primary region to multiple other regions.
- Offering global replication of images for easy management
- Standardise your image globally from a single source.

Microsoft Azure Search resources, services, and docs (G+/)

Home > Virtual machines > WVDTemplate >

Create an image

Target image definition * [Create new](#)

Version

Name (version number) *

Exclude from latest

End of life date

Replication

An image version can be replicated to different regions depending on what makes sense for your organization. One example is to always replicate the latest image in multiple regions while all older versions are only available in 1 region. This can help save on storage costs for image versions.

Default replica count *

Target regions	Target region replica count	Storage account type
(Europe) UK South	1	Standard HDD
(Europe) UK West	1	Standard HDD
	1	Standard HDD

[Review + create](#) < Previous Next : Tags >

Demo - Shared Image Galleries

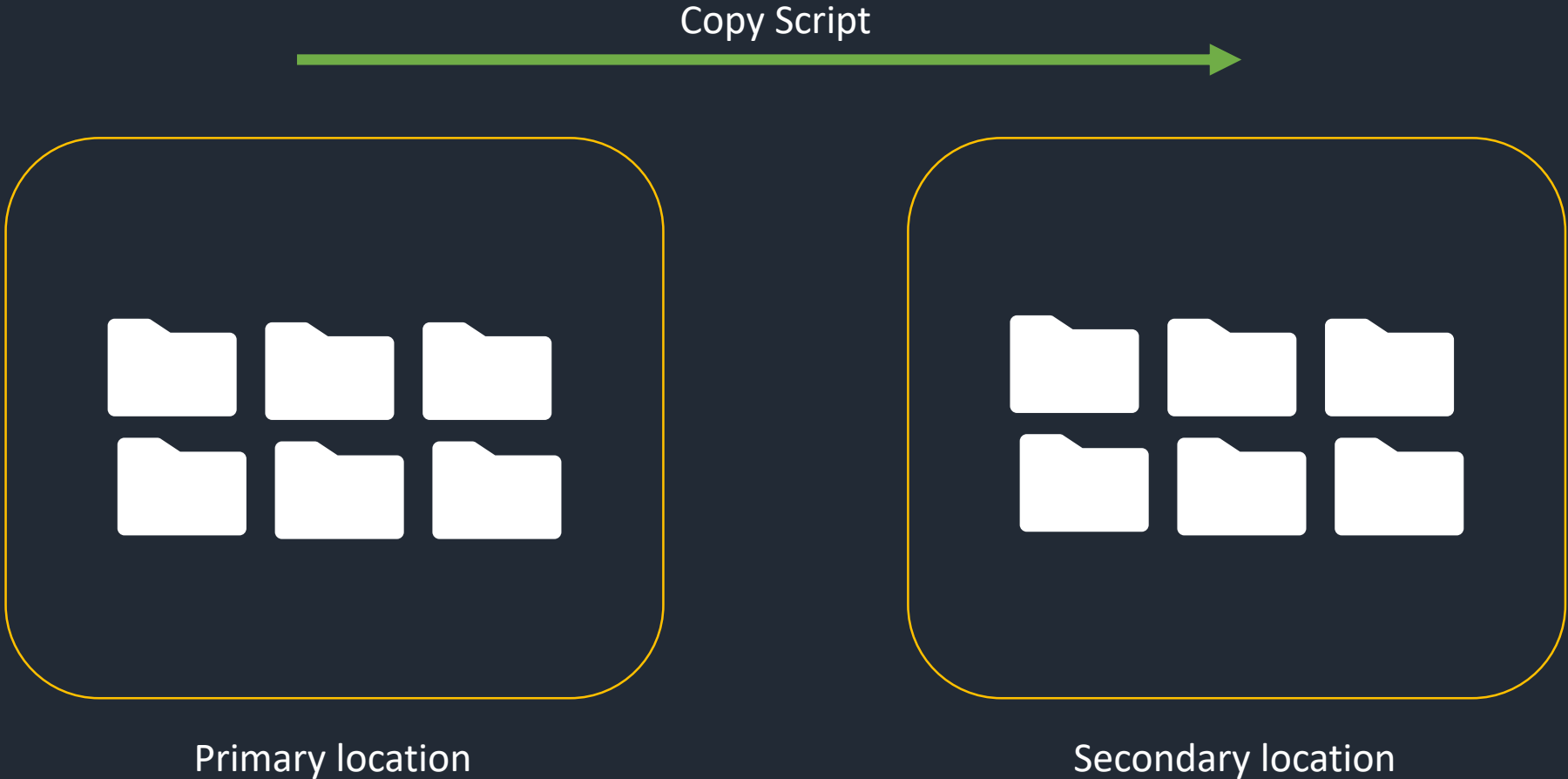
FSLogix Profile Containers

FSLogix Profile Containers

FSLogix Profile containers have be delivered in 5 different ways:

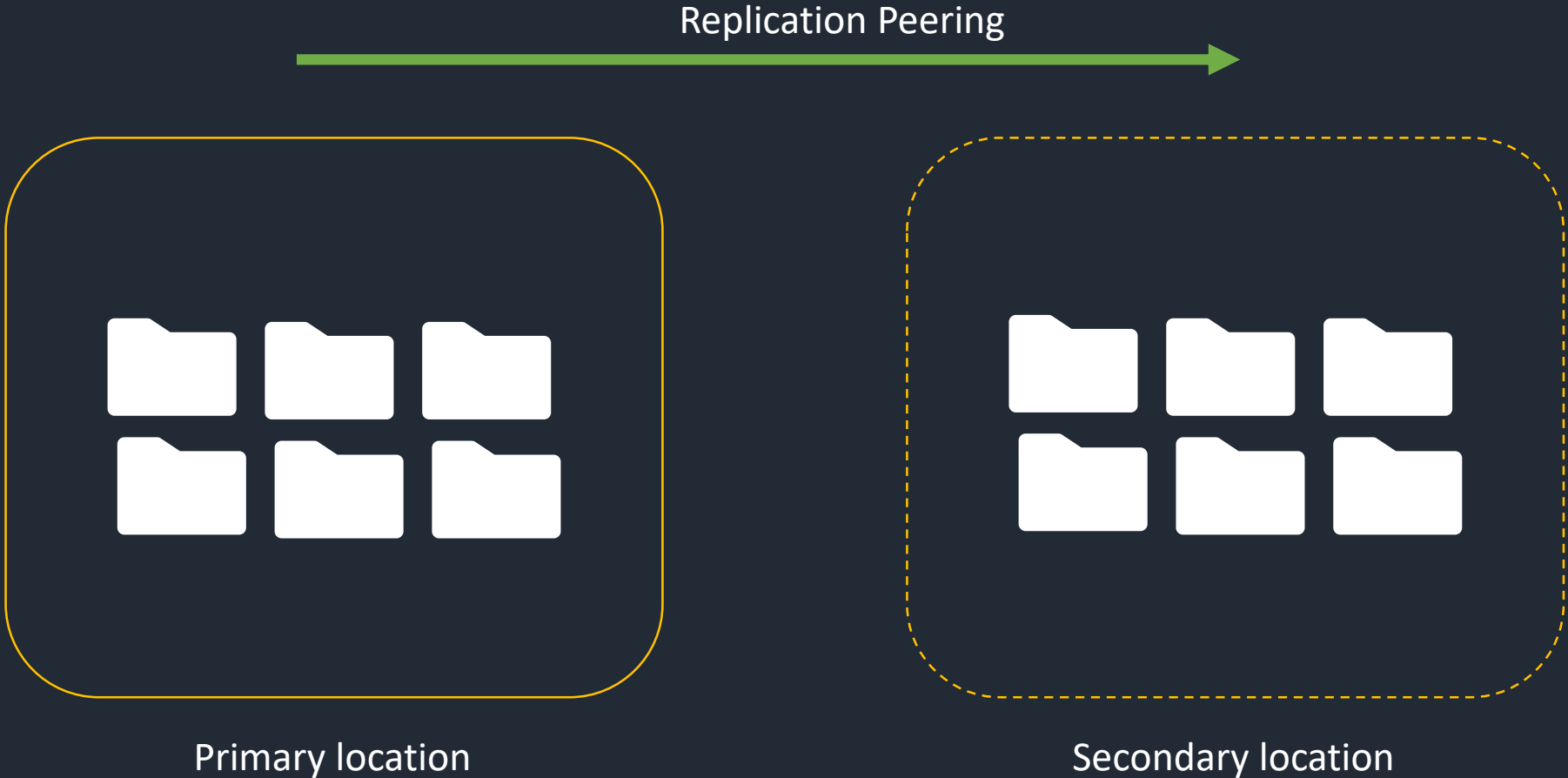
- Storage Spaces Direct (S2D)
- Network drives (VM with extra drives)
- Azure Files
- Azure NetApp Files
- Cloud Cache for replication

FSLogix Profile Containers

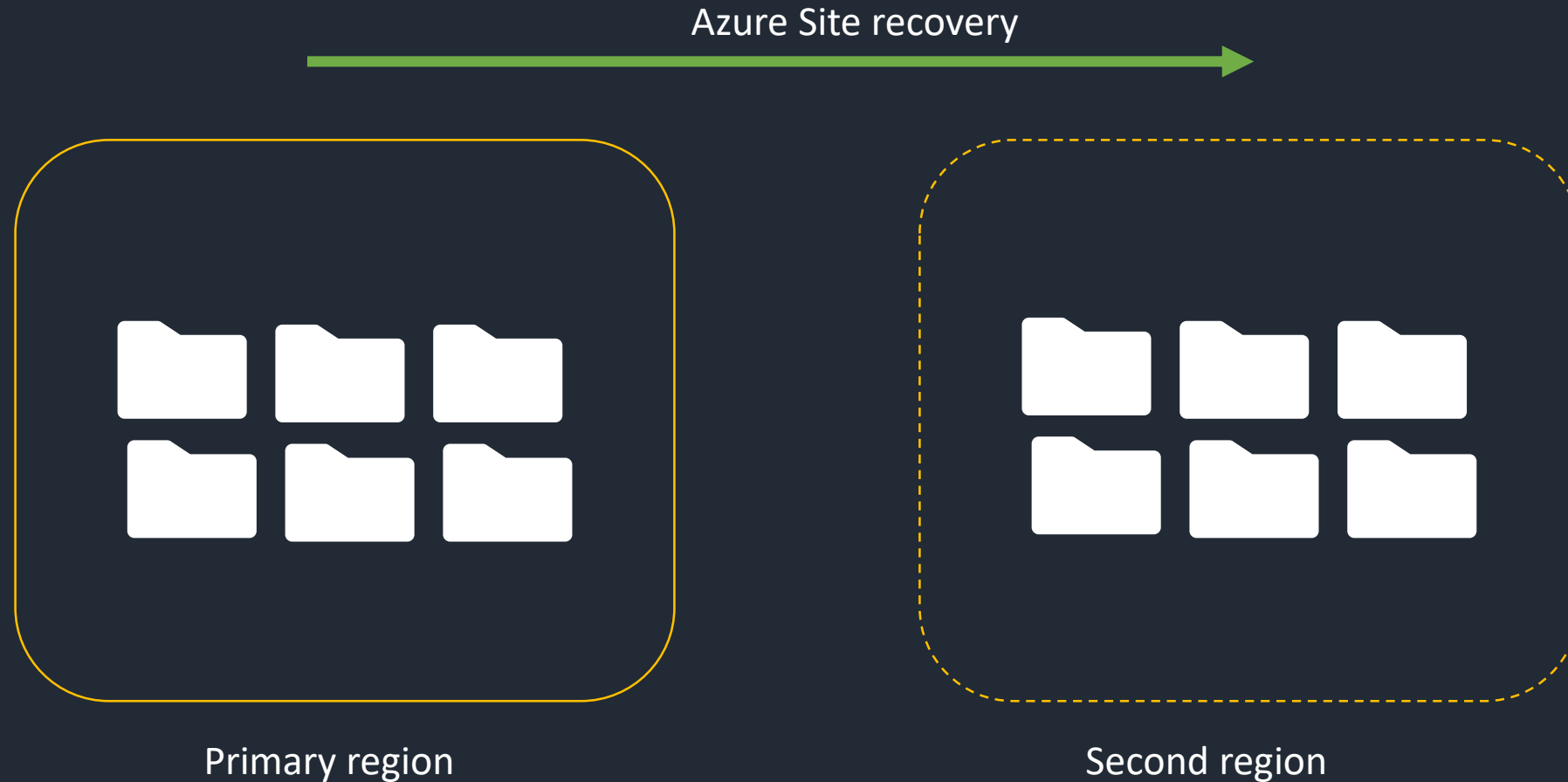


Azure NetApp Files

FSLogix Profile Containers



FSLogix Profile Containers



FSLogix Cloud Cache

- Cloud Cache uses a local profile to service reads from a redirected profile container.
- Cloud Caches offers protection for short term connectivity loss to remote profile containers
- As well as Active / Active redundancy for profile containers.
- It is important that you carefully spec the storage performance for cloud Cache.

Cloud Cache Demo

MSIX App Attach (MSIXAA)

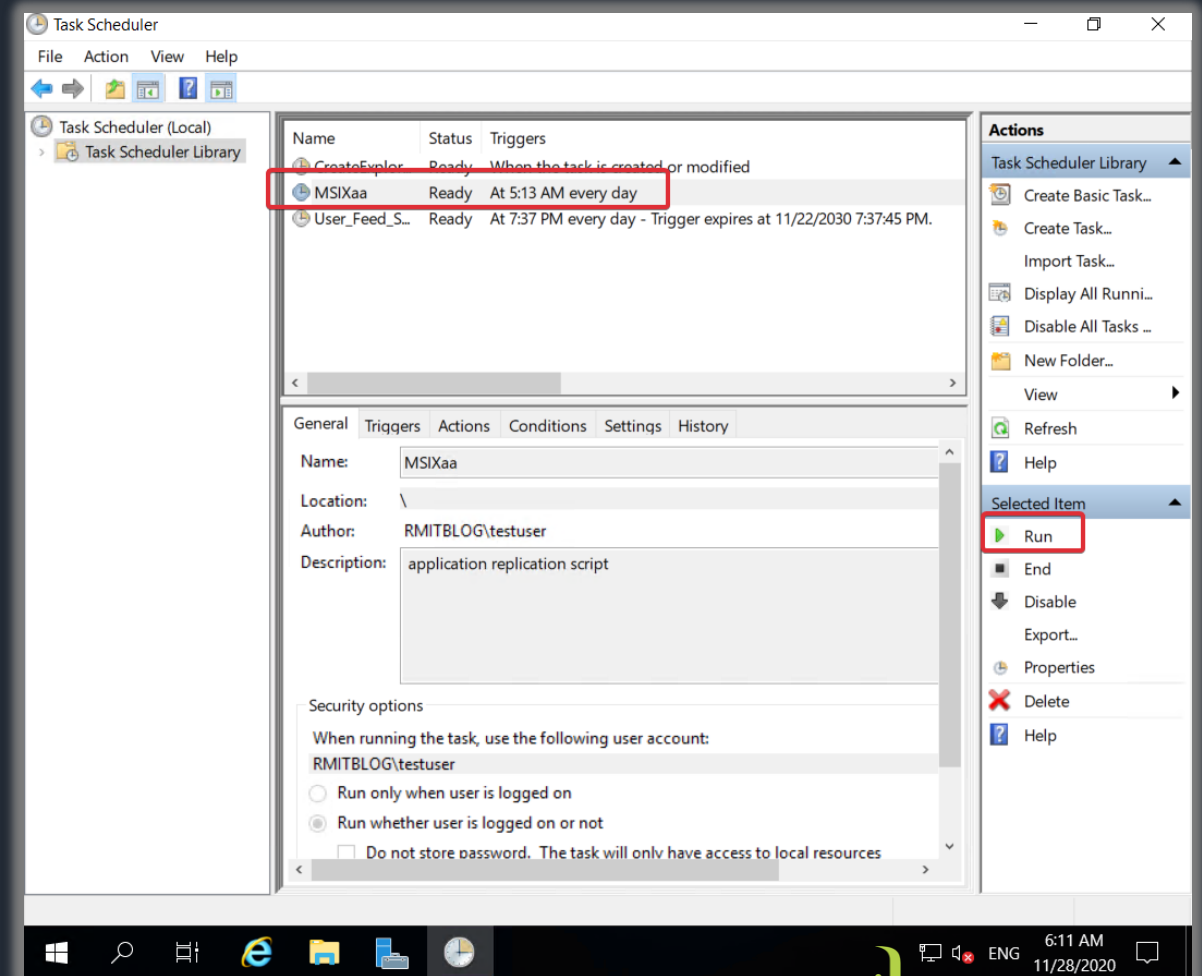
MSIX app attach (MSIXAA)



```
robocopy.exe "S:\MSIXAASTORE1" "T:\MSIXAASTORE2" /E /XO /LOG+:"T:test.log
```

Replicating MSIX images (MSIXAA)

- Similar offerings as shown with FSLogix.
- As MSIX images are read only , you can use Robocopy or Azure automation replicate between the two regions.



MSIX App Attach Demo

Summary

Summary

- Regular testing should still be carried out.
- Only failover 100 VMs at a time, if you need more complete in batches of 100 every 10 minutes.
- Always ensure that Users are logged of session hosts before carrying out failover.