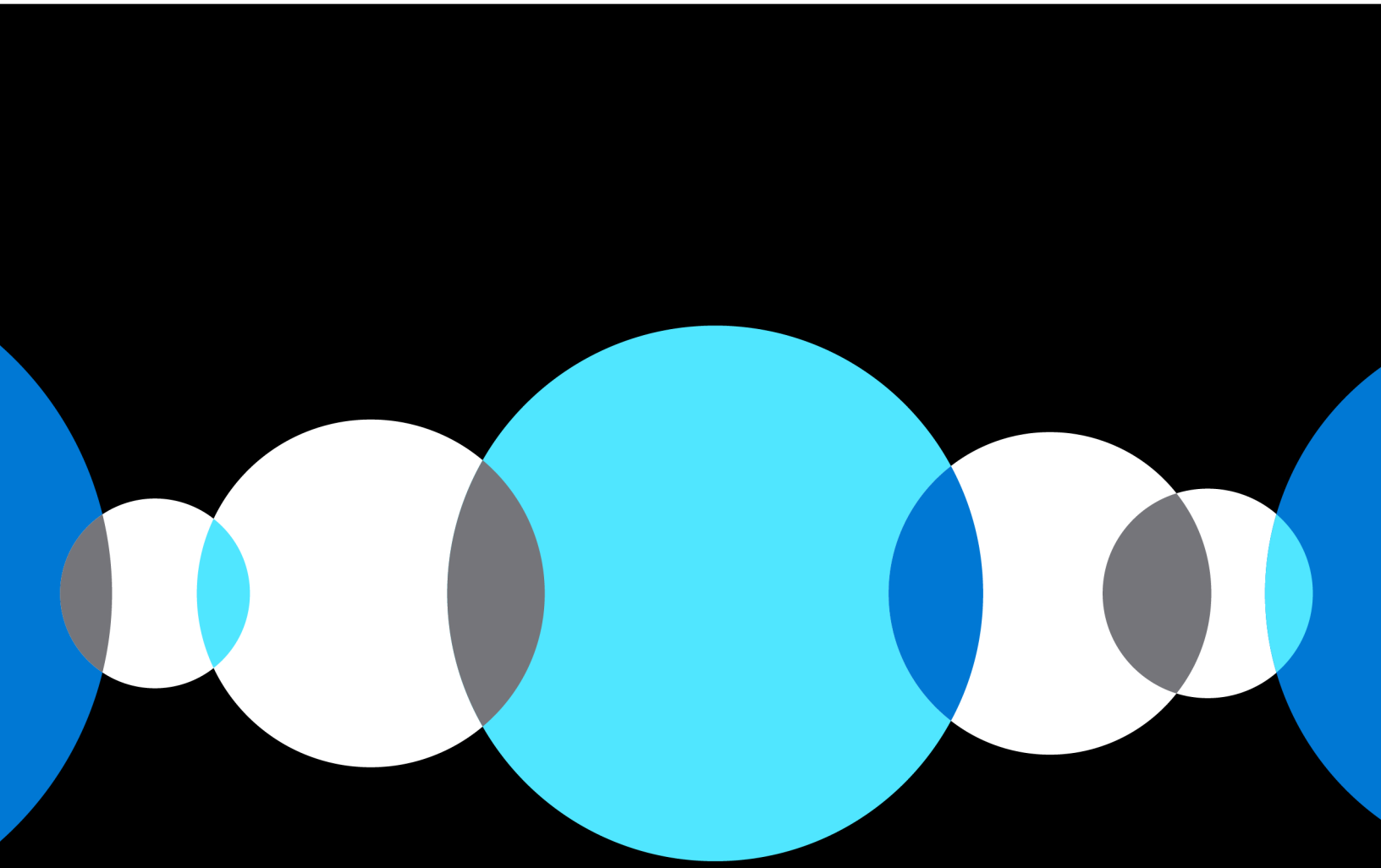
Azure e-book series

Microsoft Azure

Azure Virtual Desktop Handbook:
Disaster Recovery



Introduction

As you progress on your journey of enabling remote working for your organization with Azure Virtual Desktop, it is important to understand the disaster recovery capabilities and best practices to strengthen reliability across regions and provide a good user experience.

This handbook will provide you with considerations on **business continuity and disaster recovery (BCDR)** prerequisites, deployment steps, and best practices. This will enable you to prepare a successful BCDR plan, helping you bring more resilience to your business during downtime and outages. If you have any questions about technical requirements or want to get advice on short- and long-term solutions for enabling remote working, you can talk to an Azure sales specialist.

Azure Virtual Desktop overview

Azure Virtual Desktop is a comprehensive desktop and app virtualization service running on Microsoft Azure that helps enable a secure remote desktop experience, helping organizations strengthen business resilience. It delivers simplified management, Windows 10 Enterprise multi-session, optimizations for Microsoft 365 Apps for enterprise, and support for migrating **Remote Desktop Services (RDS)** environments. Azure Virtual Desktop also allows you to deploy and scale your Windows desktops and apps on Azure in minutes, providing integrated security and compliance features to help you keep your apps and data secure.

As a flexible cloud VDI platform, Microsoft manages many infrastructure-related parts of the solution on your behalf. Other parts, mainly related to the desktop and application workloads, are managed by you or a partner.

Figure 1 shows the components are grouped into four different buckets. The **Azure Virtual Desktop service** and **Azure infrastructure** buckets are managed by Microsoft. The **Desktop and remote apps** and **Management and policies** buckets are managed by you, which provides you with the full flexibility of being in control of your session host servers and application landscapes.

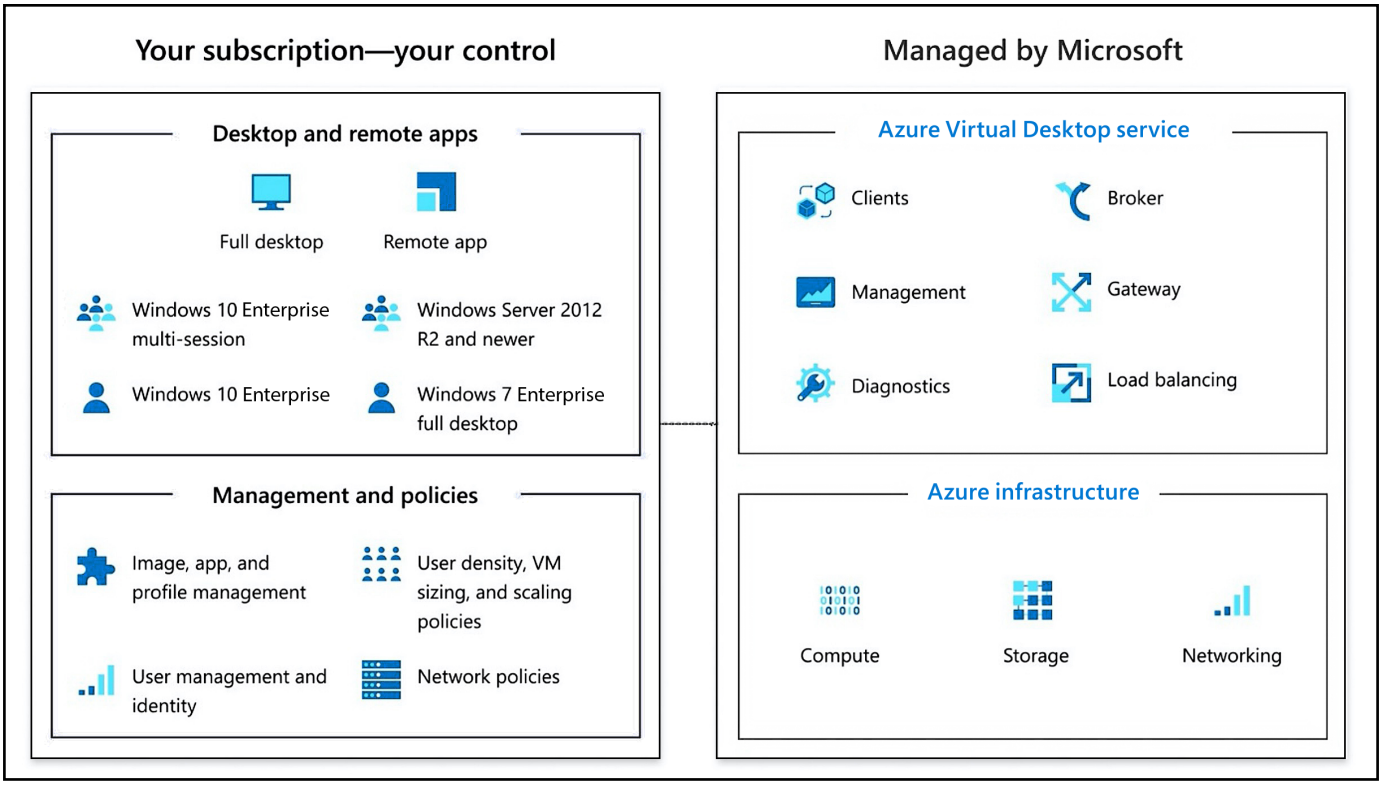


Figure 1: Azure Virtual Desktop components and responsibilities

The application's back-end components are on your on-premises network. ExpressRoute extends the on-premises network into the Azure cloud. Optionally, the back-end components can also be migrated to Azure based on a datacenter migration scenario. The Azure AD Connect components synchronize identities from **Active Directory Domain Services (AD DS)** or **Azure Active Directory Domain Services (Azure AD DS)** with Azure AD. You manage AD DS and Azure AD, Azure subscriptions, **virtual networks (VNets)**, Azure Files or Azure NetApp Files, and the Azure Virtual Desktop host pools and workspaces. *Figure 2* shows a typical Azure Virtual Desktop architectural setup.

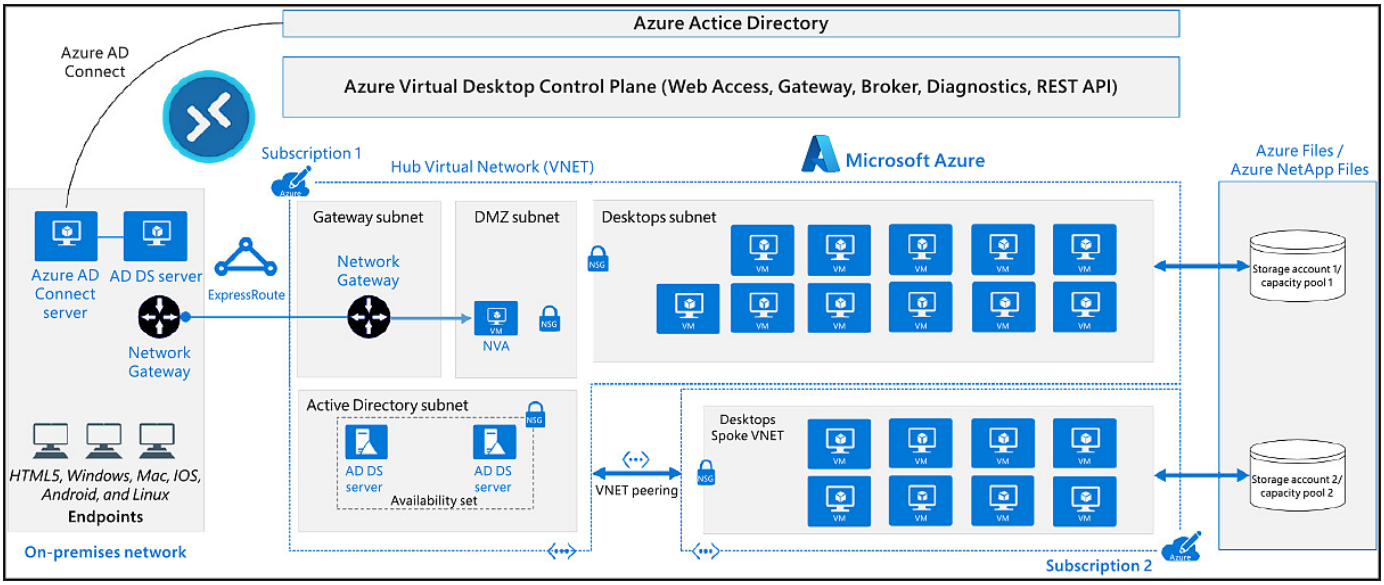


Figure 2: Typical Azure Virtual Desktop architectural setup

The Azure Virtual Desktop service architecture is similar to that of Windows Server RDS. However, with Azure Virtual Desktop, Microsoft manages the infrastructure and brokering components, while you manage your own desktop host **virtual machines (VMs)**, data, and clients. This allows you to shift your focus to what is really important to you, the user experience. To understand the differences between RDS on-premises, migrating to Azure, and migrating to Azure Virtual Desktop, take a look at *Table 1*.

Responsibility	RDS on-premises	RDS on Azure	Azure Virtual Desktop
Identity	Customer	Customer	Customer
End user devices (mobile and PCs)	Customer	Customer	Customer
Application security	Customer	Customer	Customer
Session host operating	Customer	Customer	Customer
Deployment configuration	Customer	Customer	Customer
Network controls	Customer	Customer	Customer
Virtualisation control plane	Customer	Customer	Microsoft
Physical hosts	Customer	Microsoft	Microsoft
Physical network	Customer	Microsoft	Microsoft
Physical datacenter	Customer	Microsoft	Microsoft

Table 1: Responsibilities in RDS on-premises, RDS on Azure, and Azure Virtual Desktop

For more information on Azure Virtual Desktop for the enterprise, visit this page.

Introduction to disaster recovery for Azure Virtual Desktop

To strengthen your organization's Azure Virtual Desktop availability and to keep data safe, you should implement a BCDR strategy. A good BCDR strategy keeps your apps and workloads up and running during planned and unplanned service or Azure outages. *Figure 3* depicts the **recovery point objective (RPO)** as the loss of data and the **recovery time objective (RTO)** as the time to recover from a disaster.

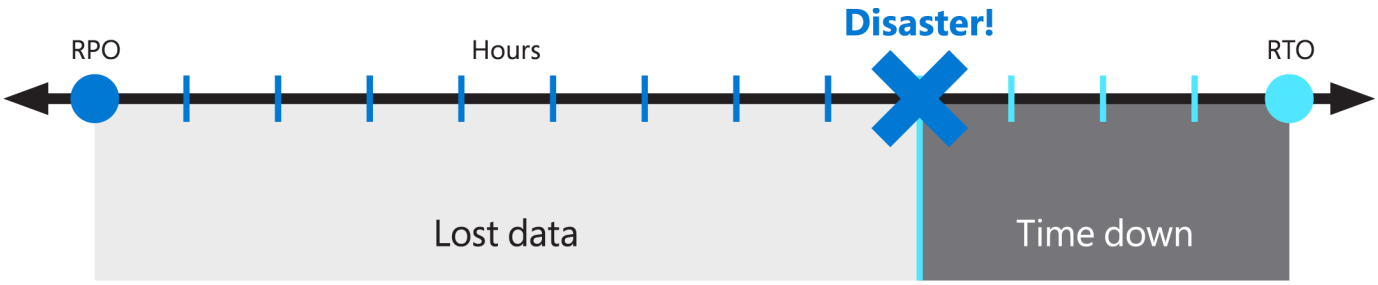


Figure 3: RPO loss and RTO time to recover

The Azure Virtual Desktop service offers BCDR to preserve customer metadata during outages. When an outage occurs in an Azure region, the service infrastructure components will failover to a secondary location and continue functioning as expected.

To make sure your users can still connect during an Azure region outage, you may need to replicate personal VMs to a different Azure region (the secondary location). During outages, the primary region fails over to the replicated VMs in the secondary location. Users can continue to access apps from the secondary location without interruption. In addition to VM replication, you'll need to ensure user identities are accessible at the secondary location. This can be achieved by using profile containers. You may also use multiple Pooled host pools with automated provisioning across regions as an alternative to VM replication.

Note: Ensure business applications that rely on data in the primary Azure region can fail over with the rest of the data.

To ensure your users are connected during an outage, you should consider the five components shown in *Table 2* in chronological order.

	Component	Description
1	Virtual network	Consider your network connectivity during an outage.
2	Virtual machines	Replicate the VMs in a secondary location or deploy multiple non-persistent host pools across Azure regions.
3	User and app data	Using FSLogix profile containers, set up data replication in the secondary location. Data replication is also required for those using MSIX app attach.
4	User identities	Ensure user identities you set up in the primary location are available in the secondary location.
5	Application dependencies	Ensure any line-of-business applications relying on data in your primary location are failed over to the secondary location.

Table 2: Five areas to consider for Azure Virtual Desktop disaster recovery

We will now look at steps to set up the five key components of disaster recovery for Azure Virtual Desktop, starting with Azure VNets.

Setting up disaster recovery in Azure Virtual Desktop

Each Azure Virtual Desktop environment is different in terms of design and configuration. When designing and implementing a disaster recovery solution for Azure Virtual Desktop, the following five key components should be considered.

Virtual network

As a starting point, you should consider your network connectivity during an outage. For Azure resources to fail over or communicate with a secondary region, you need to make sure that a VNet has been set up in your secondary region/location.

Suppose your users need to access on-premises resources and services. In this scenario, you will also need to configure the VNet to access these via a VPN. On-premises connections can be established with an ExpressRoute, VPN, or virtual WAN. You can also use a **network virtual appliance (NVA)** to connect to on-premises environments.

Azure Site Recovery can also be used to set up the VNet in a failover region, as it preserves your primary network's settings and doesn't require network peering. This could be considered as a plug-and-play service for the smaller Azure Virtual Desktop deployment due to its simplicity in terms of setup requirements. *Figure 4* depicts a simple VPN gateway connecting to an on-premises site. This is a common connectivity method for connecting to on-premises from Azure.

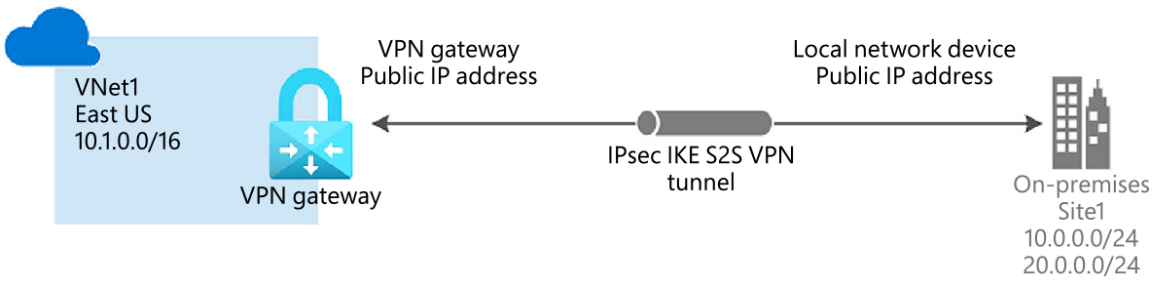


Figure 4: Simple VPN gateway connecting to an on-premises site

Figure 5 depicts VNet peering between two Azure regions. Peering is useful for those who want to connect two VNets together without using a VPN.

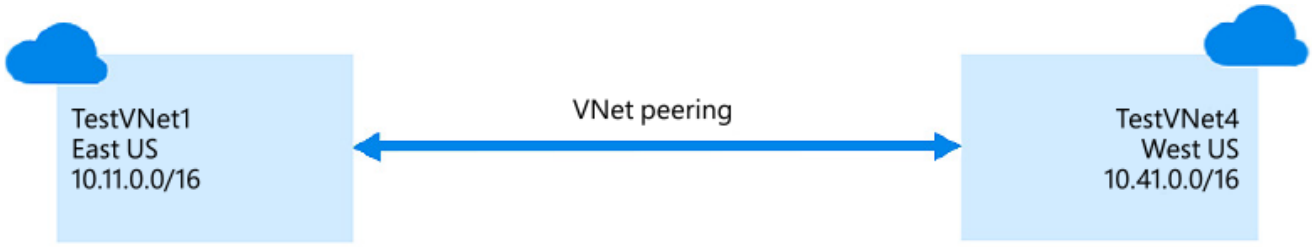


Figure 5: VNet peering between two Azure regions

DNS

A common problem that customers face with Azure Virtual Desktop is DNS configuration issues relating to the VNet. Ensure your VNet is set up correctly with DNS. You can resolve the Azure Virtual Desktop FQDNs and AD DS between the two regions.

Read more here on the required URL list for Azure Virtual Desktop.

Virtual machines

For Azure Virtual Desktop host pools, both *active-active* and *active-passive* can be viable BCDR options.

With active-active, a single host pool can have VMs from multiple Azure regions. In this scenario, the usage of FSLogix Cloud Cache would be required to actively replicate the user Profile/Office containers between the regions. For VMs in each region, the Cloud Cache registry entry specifying locations needs to be inverted to give precedence to the local one. Active-active can be summarized in the following way:

- This is a complex configuration. If active-active is chosen, it gives the business protection against storage outages without the need to re-log the user while also enabling continuous testing of the disaster recovery location. This configuration type is considered neither a performance nor a cost optimization solution; it continually tests disaster recovery.

- The load balancing of incoming user connections cannot consider proximity: all hosts will be equal, and users may be directed to a remote, but not optimal, Azure Virtual Desktop host pool VM.
- This configuration is limited to a *Pooled* (shared) host pool type. For a *Personal* (dedicated) type, once a desktop is assigned to a user on a certain session host VM, it sticks and will not change, even if not available.

With *active-passive*, Azure Site Recovery or a secondary host pool (hot standby) in the disaster recovery region, the following options can be used:

- Azure Site Recovery is supported for both *Personal* (dedicated) and *Pooled* (shared) host pool types and will allow you to maintain a single host pool entity.
- Creating a new host pool in the failover region is also possible, allowing you to keep all those resources turned off. For this method, you would need to set up new application groups in the failover region and assign users to them. You can then use an Azure Site Recovery "*recovery plan*" to turn on host pools and create an orchestrated process.

It is suggested that you use Azure Site Recovery to manage replicating VMs in other Azure regions, as described in Azure-to-Azure disaster recovery architecture. It is also recommended that you use Azure Site Recovery for personal host pools because Azure Site Recovery supports server- and client-based SKUs.

For further guidance on Azure Virtual Desktop disaster recovery design considerations, check this documentation.

Note: The maximum number of VMs inside an availability set is 200, as documented in this article.

The default resiliency option for Azure Virtual Desktop host pool deployment is an availability set: it will only ensure host pool resiliency at the single Azure datacenter level, with formal 99.95% high availability. You can find out more here.

We recommend that you use Azure Backup to protect personal desktops, especially if you are not using profile containers for these desktops. Read more about the Azure Backup service here.

Figure 6 shows Azure Site Recovery's role in replicating the workloads on three VMs located in the East and West US regions.

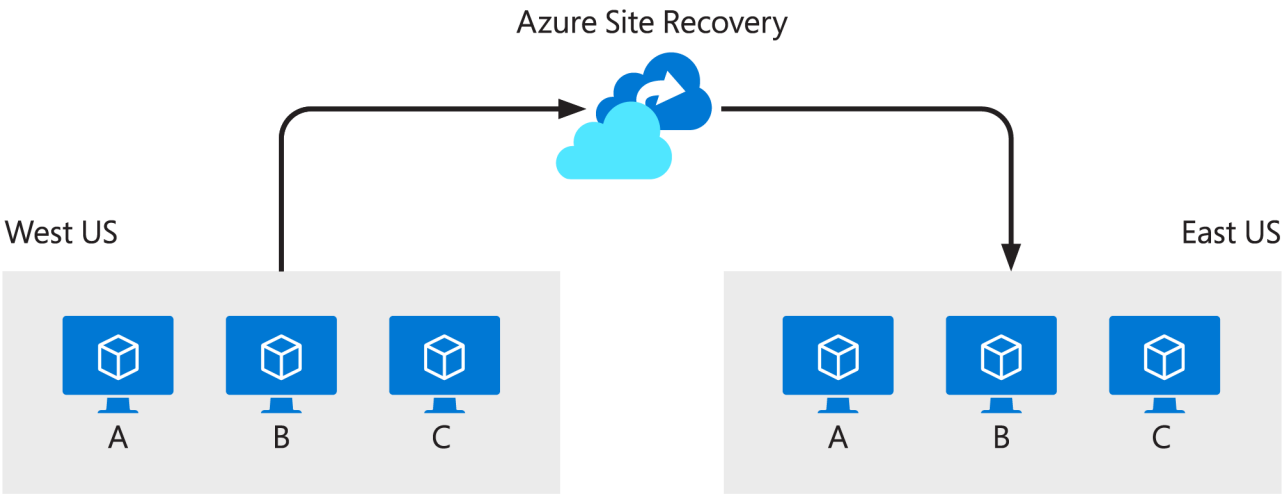


Figure 6: Azure Site Recovery replicating workloads from a primary region to a secondary

When using Azure Site Recovery, you do not need to register these VMs manually. The Azure Virtual Desktop agent configured on the secondary VM will automatically use the latest security token to connect to the Azure Virtual Desktop service instance closest to it. The VM (session host) in the secondary region will automatically become part of the host pool. The customer will only have to reconnect during this process. Apart from the user reconnecting this once, there are no other manual processes required.

Disconnect users in Azure Virtual Desktop

There can be no existing user connections during an outage. Before the administrator can start the failover to the secondary region, you will need to "end" the user connections in the current Azure region. To disconnect users from Azure Virtual Desktop, you can run this cmdlet:

```
Remove-AzWvdUserSession
```

Once all users are signed out of the primary Azure region, you can then go ahead and fail over the VMs in the primary region. Once complete, you can let users connect to the VMs in the secondary region. For more information about how this process works, see Replicate Azure VMs to another Azure region.

It is advised that a runbook or script be created to automate user sessions' disconnection during a failover to a second region. It can be time-consuming to complete this task manually. You can create an Azure Automation runbook using this guide.

Backup protection

As mentioned at the start of this *Virtual machines* section, preventing the loss of critical user data is important. The first step is to assess the data that needs to be saved and protected. Here are a few considerations:

- If using OneDrive or another form of non-local storage, saving the user profile or Office container data may not be necessary.
- An appropriate mechanism must be considered to protect critical user data:
  - The Azure Backup service can protect Profile and Office container data when stored on Azure Files, either on the Standard or the Premium tier.
  - Azure NetApp Files Snapshots and Policies can be used for Azure NetApp Files (all tiers).
  - Azure Backup can also be used to protect host pool VMs; this practice is supported even if host pool VMs should be stateless.

Golden image availability

When using custom images to deploy Azure Virtual Desktop host pool VMs, it is important to ensure those artifacts are available in all regions, even if in the event of a major disaster. The Azure Shared Image Gallery service can be used to replicate images across all regions where a host pool is deployed, with redundant storage and in multiple copies.

Now that you know how to design and implement a disaster recovery solution with VMs, the next key component is managing user identities and configuring user and app data.

Managing user identities

In this section, we'll see how to manage user identities and also explore the different options available to you.

In case of a failover, it must be ensured that the domain controller is available at the secondary location/region. The following three options are available for keeping the domain controller available during an outage:

1. Deploy an AD domain controller at the secondary location. *Figure 7* depicts two VNets configured using network peering, allowing two domain controllers to communicate across two VNets using peering.

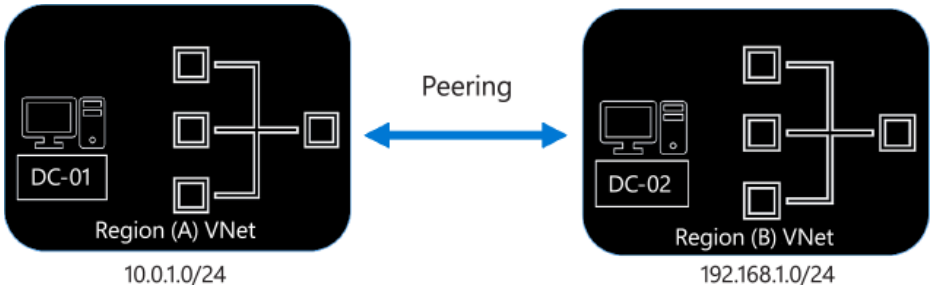


Figure 7: Network peering example

2. Use an on-premises AD domain controller. *Figure 8* depicts an on-premises environment connecting two Azure VNets using a VPN gateway to an on-premises site.

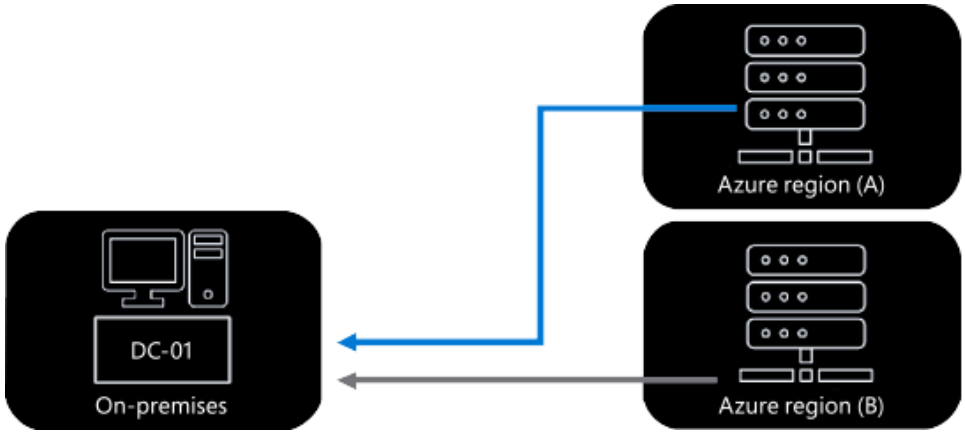


Figure 8: Multiple regions connecting via a VPN gateway to an on-premises site

3. Replicate your AD domain controller using Azure Site Recovery. *Figure 9* shows an AD domain controller being replicated using Azure Site Recovery.

Figure 9: Domain controller replicating to the secondary region using Azure Site Recovery

Now that we have covered the user identity options available to you when designing a BCDR solution for Azure Virtual Desktop, let's see how to configure user and app data.

Configuring user and app data

If you are using local profiles, it is advised that Azure Site Recovery is used to replicate user data and the session hosts to the second region. For most organizations using profile containers, the next step would be to set up profile container replication to the secondary location.

In a BCDR situation, it is possible to reduce the time taken to back up, restore, and replicate data with the separation of the user Profile and the Office container disks. FSLogix offers the possibility and capability to allocate them in separate storage locations. In normal usage, the Office disk can consume much more capacity (measured in GB) than the profile. Backup, replication, and restoration of the profile disk will be far quicker without the inclusion of the cache data. The Office disk is not required to be made resilient, as this can be downloaded again; the data it contains is already present inside Office 365 online services.

Note: The FSLogix Cloud Cache feature is "write back" by design to increase performance characteristics to high-latency targets, thus using asynchronous replication.

There are three standard options for storing FSLogix profiles:

- Azure Files
- Azure NetApp Files
- FSLogix Cloud Cache for replication

Microsoft Azure offers multiple storage solutions that you can use to store your FSLogix Profile and Office containers. Storage options for FSLogix profile containers in Azure Virtual Desktop compares the various managed storage solutions Azure offers for Azure Virtual Desktop FSLogix user profile containers.

When setting up disaster recovery for profiles, the following options are available to you:

- Set up Azure replication (for example, Azure Files Standard storage account replication, Azure NetApp Files replication, or Azure Files Sync for file servers).
- Set up FSLogix Cloud Cache for both application and user data. Read more on how to use Cloud Cache for resiliency and availability.
- The third option is to set up disaster recovery for app data only to ensure access to business-critical data at all times. In this scenario, you can retrieve user data after the outage is over. This essentially means users would get new user profiles and a first-time sign-in experience during the outage period.

Note: NetApp replication is automatic after you first set it up. With Azure Site Recovery plans, you can add pre-scripts and post-scripts to fail over non-VM resources.

Let's now look at Cloud Cache in more detail to see how it can benefit your BCDR design.

Cloud Cache

Cloud Cache uses a local profile to service reads from a redirected Profile or Office container after completing its first read. Cloud Cache can use multiple remote locations that are updated continuously during the user session. Cloud Cache can essentially insulate users from the risk of short-term loss of connectivity to remote profile containers. It is also important to note that Cloud Cache can provide active-active redundancy for Profile and Office containers.

Note: Please checkout the key factors regarding Cloud Cache in the *Design Considerations* chapter. It is advised to configure the session hosts with **Premium SSD** disks for the local cache file in order to help ensure no loss of data.

Configuration of FSLogix profile containers using multiple profile locations

The FSLogix agent supports multiple profile locations when you configure the registry entries for FSLogix. To configure the registry entries:

1. Open **Registry Editor**.
2. Go to **Computer** > **HKEY_LOCAL_MACHINE** > **SOFTWARE** > **FSLogix** > **Profiles**.

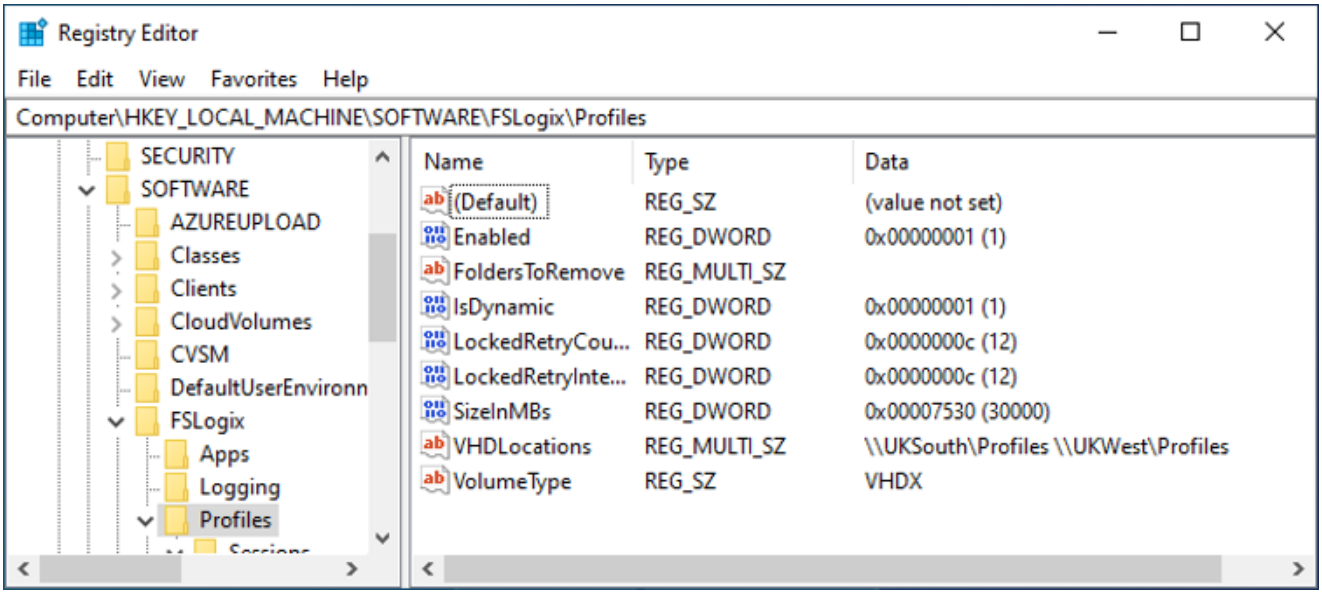


Figure 10: Registry settings for FSLogix Profile containers

3. Right-click on **VHDLocations** and select **Edit Multi-String**.

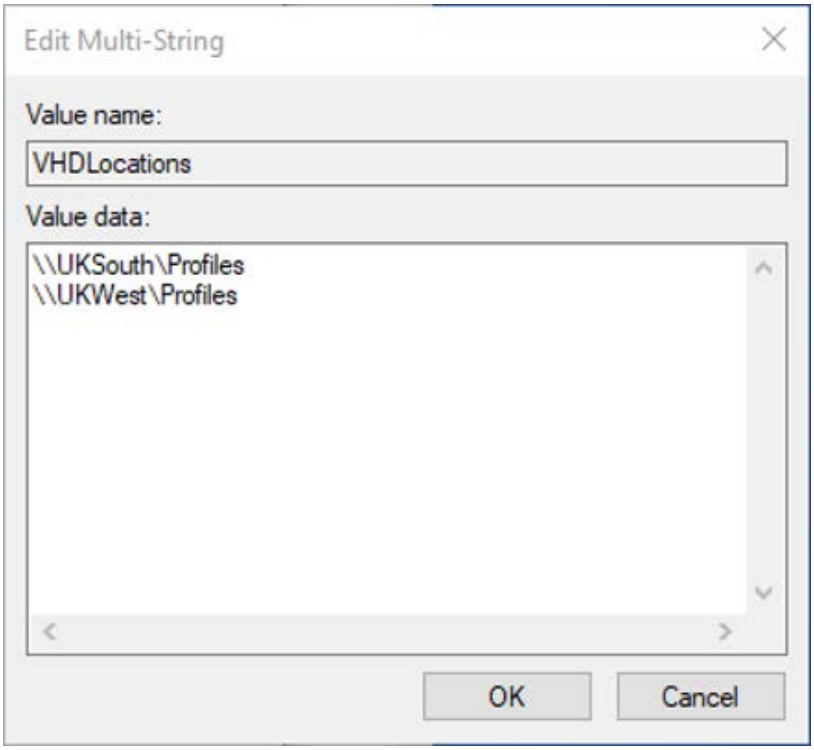


Figure 11: The VHDLocations option in the registry for FSLogix profile containers

4. In the **Value data** field, enter the storage locations you would like to use. When finished, select **OK**.

If the first storage location is unavailable, the FSLogix agent will automatically fail over to the second. We recommend that you pre-configure the FSLogix agent with a secondary location path while configuring the primary region session hosts (initial deployment).

Tip: To configure these by group policy, please see this link.

Suppose the primary region/location shuts down. In that case, the FSLogix agent configuration will replicate as a part of the VM (Azure Site Recovery replication). Once the replicated VMs are ready on the secondary region, the agent will automatically attempt the secondary region's path, as this has been pre-configured.

Configuration of FSLogix profile Cloud Cache

The following steps outline the requirements for setting up Cloud Cache.

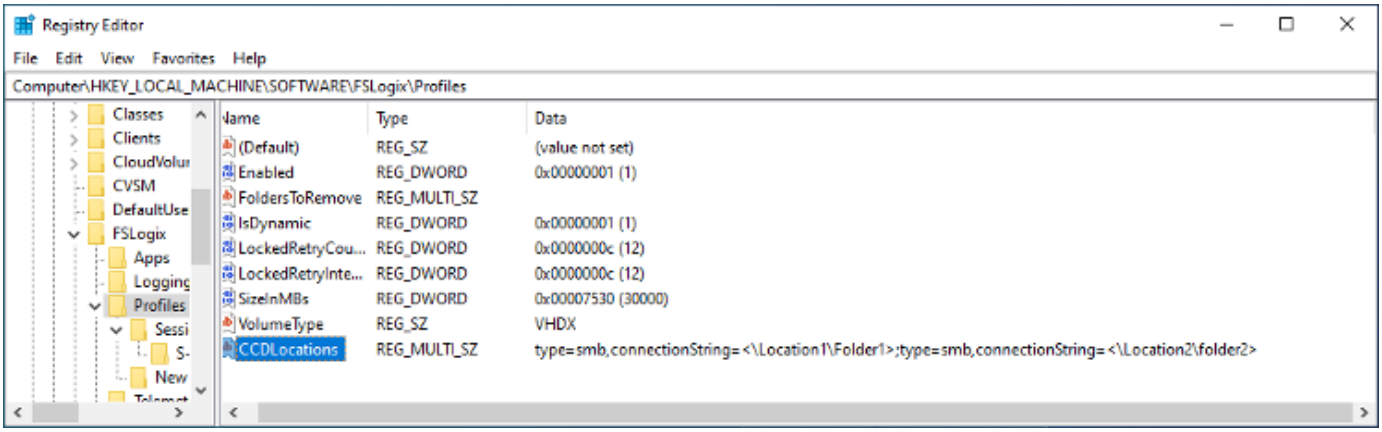


Figure 12: The registry for FSLogix profile containers

1. Open **Registry Editor**.
2. Go to **Computer** > **HKEY_LOCAL_MACHINE** > **SOFTWARE** > **FSLogix** > **Profiles**.
3. Remove any settings for **VHDLocations**.
4. Add **CCDLocations** as **REG_MULTI_SZ** and add the following value to include location 1 and location 2: **type=smb,connectionString=<\Location1\Folder1>;type=smb,connectionString=<\Location2\folder2>**

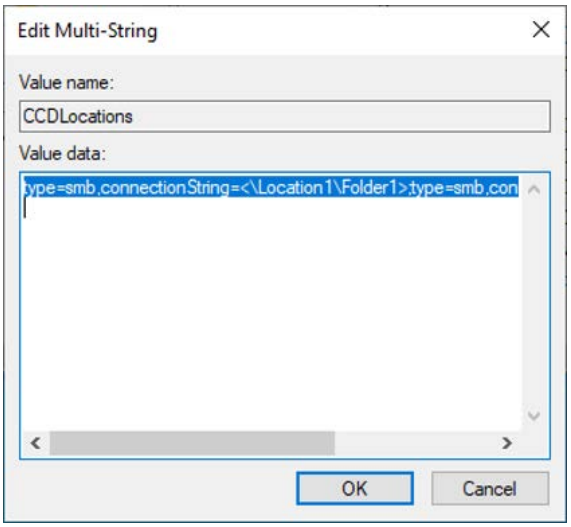


Figure 13: CCDLocations for FSLogix Cloud Cache

Once the setup is completed, Cloud Cache will replicate the profile between the two locations.

Azure Files

Azure Files supports cross-region asynchronous replication that you can specify when you create a storage account. If the asynchronous nature of Azure Files already covers your disaster recovery goals, you don't need to carry out additional configurations.

Azure Files offers a storage account failover replication option against the other region configured in your storage account redundancy plan. This is only supported for the standard storage account type using **geo-redundant storage (GRS)**. Other options include the use of *AzCopy* or any other file copy mechanism, such as *Robocopy*.

Note: With Azure Files share premium tier or Azure Files share standard tier with large file support enabled, GRS is not available. Read more here about Cross-region replication of Azure NetApp Files volumes.

Azure NetApp Files

Azure NetApp Files is a high-performance file storage service that can run your most demanding file workloads in Azure without the need for any code modification. It is a primary Azure service, built on NetApp's ONTAP technology and supported by Microsoft. Taking only minutes to set up, Azure NetApp Files enables both Linux and Windows applications to seamlessly migrate and run in the cloud for an on-premises-like experience and corresponding performance. *Figure 14* depicts an Azure Virtual Desktop environment using NetApp Files.

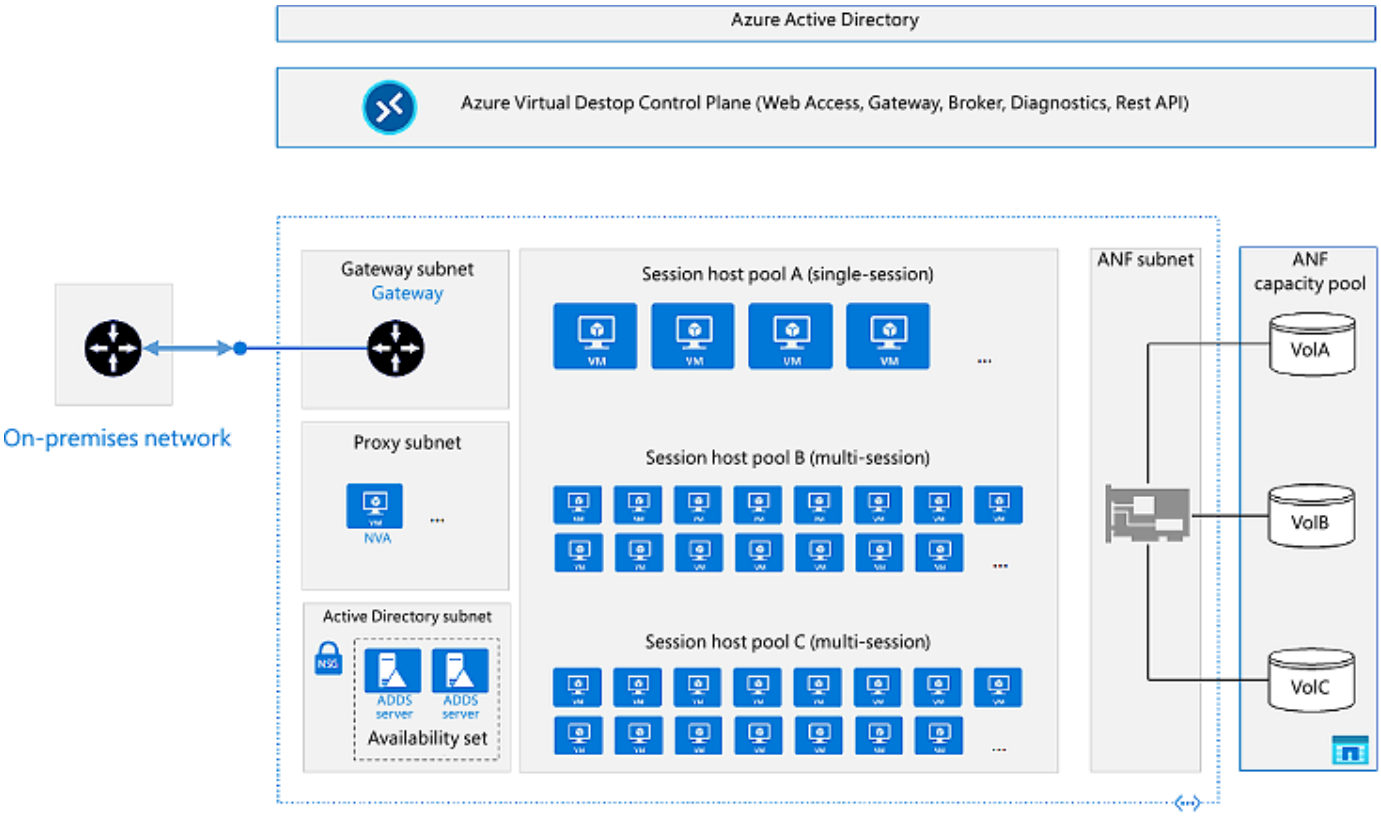


Figure 14: Architectural diagram of Azure Virtual Desktop using Azure NetApp Files

Read more about Azure NetApp Files at Create replication peering for Azure NetApp Files. More can also be found out at FSLogix for the enterprise - Azure Architecture Guide.

The use of OneDrive

OneDrive can redirect known folders (Desktop, Documents, Pictures, Screenshots, and Camera Roll) if present. This would increase the resilience of these special folders as they would be handled by OneDrive rather than needing special consideration in a BCDR scenario.

MSIX app attach

MSIX app attach is a Microsoft application-delivery feature in Azure Virtual Desktop designed for a modern workspace. With MSIX app attach, you can use one application format (MSIX) to deliver applications to Pooled and Personal desktops within Azure Virtual Desktop.

Figure 15 depicts how MSIX app attach works. You will note that file shares are needed to store MSIX images.

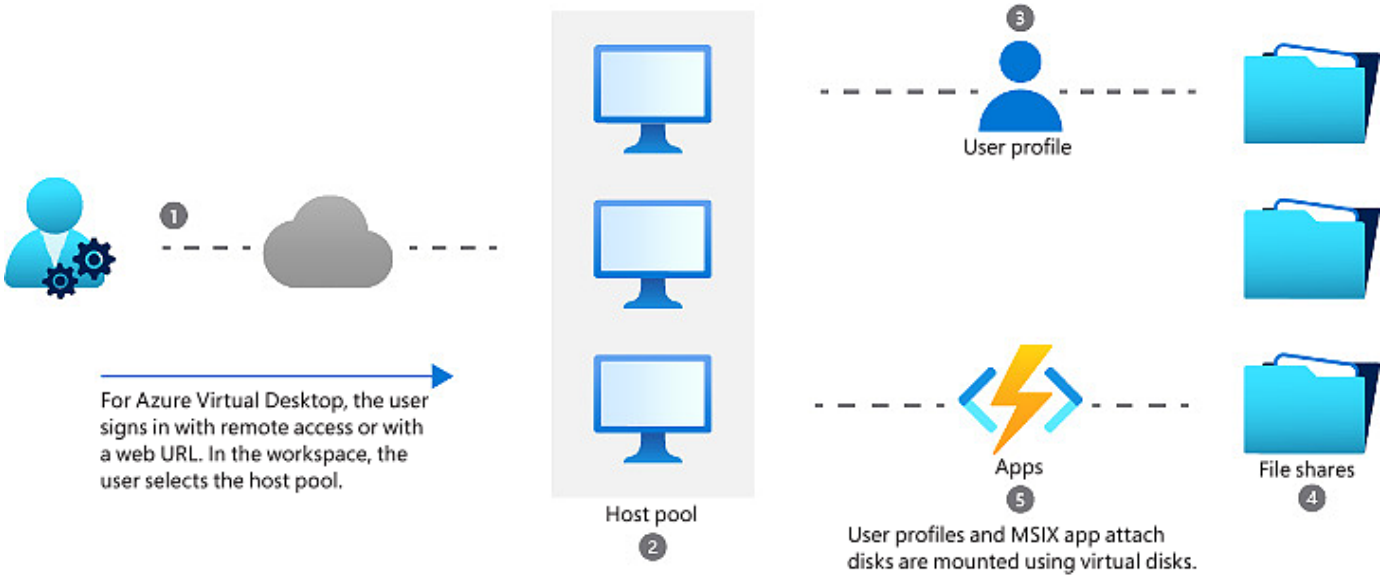


Figure 15: Steps for delivering MSIX app attach apps to a user

There are two areas that must be considered. First, you need to take care of the storage to ensure the MSIX images are accessible in the second location. Similar to profile containers, MSIX app attach requires network storage to store the MSIX images. This could be Azure Files, NetApp Files, or a file share. Depending on the option chosen, you should ensure that these MSIX images are available in a BCDR scenario.

The second consideration is that the MSIX image path may have changed if you have opted to use a new storage resource in the second region. By doing so, the storage paths have changed. This means you would need to reconfigure all your MSIX image paths via PowerShell or through the Azure management UI before users can access these applications through a host pool.

To avoid the complications of reconfiguring MSIX app attach and the MSIX image paths, use one of the following options.

- Create a separate host pool for the secondary region.
- Use Azure Files with GRS.
- Implement Azure NetApp Files cross-region replication.

Learn how you can set up MSIX app attach through the Azure portal with this documentation.

App dependencies

One final area to consider is any data or services running in the primary region, which should be failed over to prevent business application failure during an outage. Ensure that any business applications that rely on data located in the primary region can failover to the secondary location. This could be custom web services, SQL databases, or others.

It must also be ensured that the settings required are configured for the apps. You may be required to add additional configurations to these services once replication or high availability has been configured. One example is that if one of the apps depends on the SQL back-end, make sure to replicate SQL in the secondary location and configure the SQL high-availability connection strings.

You may configure the app to use the second region as either part of the failover process or as its default configuration. You can also model application dependencies on Azure Site Recovery plans.

Summary:

- If users of the Azure Virtual Desktop infrastructure need on-premises resource access, high availability of the network infrastructure that is required to connect is also critical and should be considered.
- The resiliency of authentication infrastructure needs to be assessed and evaluated.
- BCDR aspects for dependent applications and other resources need to be considered to ensure availability in the secondary disaster recovery location.

To learn more, see the documentation on recovery plans.

Testing disaster recovery

After you have finished setting up and configuring disaster recovery for Azure Virtual Desktop, you should test your plan to make sure it works and confirm that users can still access the required resources and services.

The following points should be considered when testing your Azure Virtual Desktop BCDR plan.

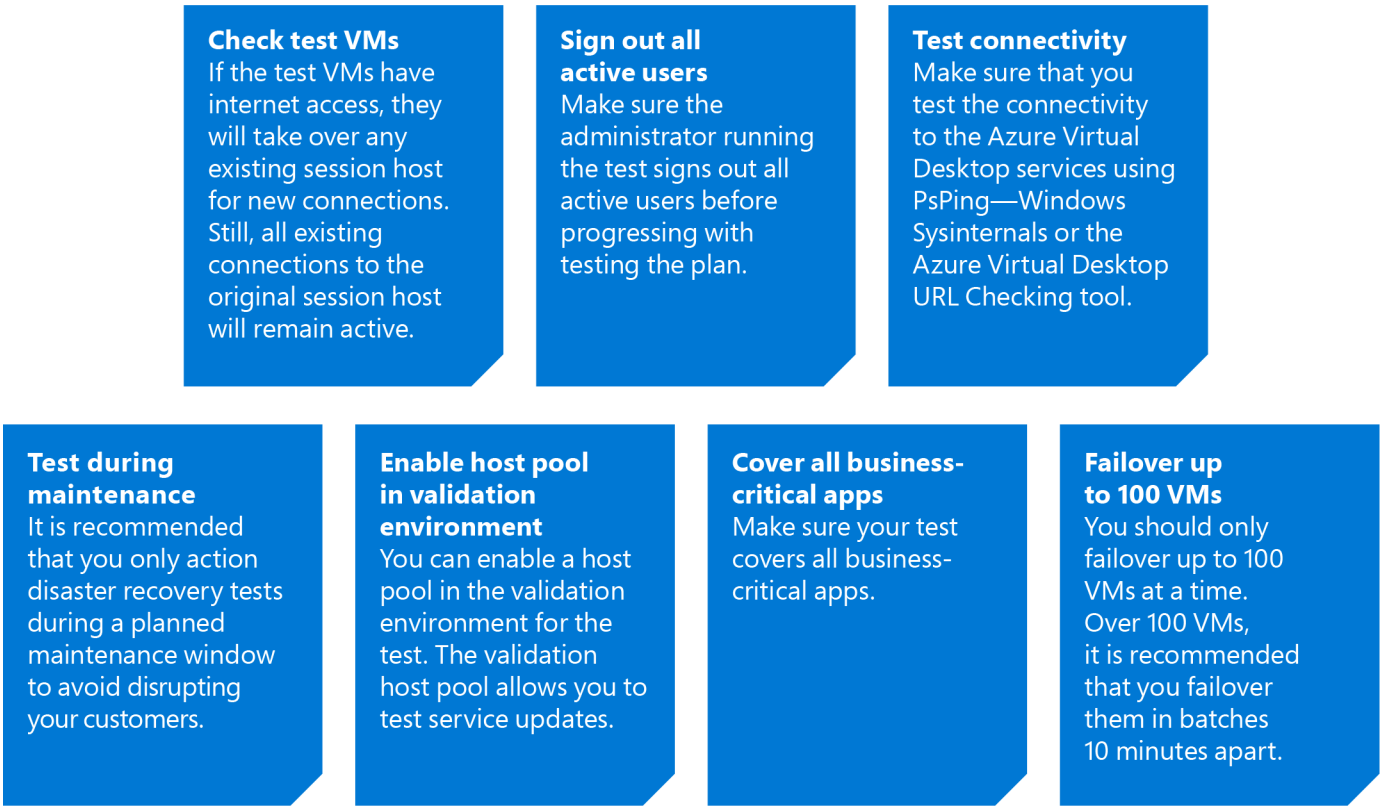


Figure 16: Considerations while testing the Azure Virtual Desktop BCDR plan

See the following guide for using the Required URL Check tool.

Tip: You can also test connectivity to Azure Virtual Desktop services using PsPing - Windows Sysinternals.

In the final chapter, we'll look at some of the key tools for optimization and best practices for Azure Virtual Desktop.

Optimizations and best practices

The following are best practices to consider for your disaster recovery design configuration:

Active Directory
AD authentication must be available in the disaster recovery region, or connectivity to the on-premises domain must be guaranteed.

Virtual machines
For Azure Virtual Desktop host pool compute deployment model BCDR, use the *active-passive* option if this will satisfy your requirements for RPO and RTO.

Azure Site Recovery
Azure Site Recovery is supported for Pooled (*shared*) host pools. This option can be evaluated and compared to the deployment of another host pool in the secondary disaster recovery region.

Note: Azure Site Recovery is recommended for Personal (*dedicated*) host pools. The target region should be aligned with the disaster recovery of the storage back-end used by FSLogix.

Availability zones
Availability zones should be used when maximum resiliency of the host pool is required in a single region. Customers should first verify the availability zone's feature availability in the required region and the availability of specific VM sizing type **stock keeping units (SKUs)** inside all the zones.

Azure Shared Image Gallery
Azure Shared Image Gallery should be used to replicate golden images to different regions. The storage used for image creation should be **zone replicated storage (ZRS)**, and at least two copies per region should be maintained.

FSLogix

We recommend storing FSLogix user Profile and Office containers on Azure Files or Azure NetApp Files for most customer scenarios.

Note: It is recommended to split user Profile and Office containers.

The recommended options for the FSLogix container storage types are detailed in *Figure 17*.

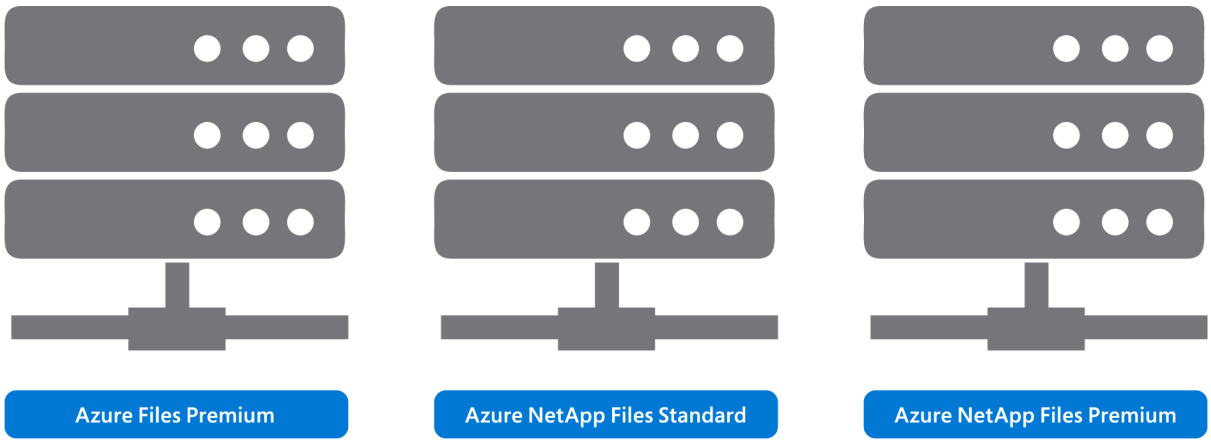


Figure 17: Recommended options for the FSLogix container storage type

The use of an Azure Files type depends on the resources and latency required by the specific workload. Large organizations would typically use Azure Files Premium or Azure NetApp Files Premium.

For optimal performance, FSLogix containers should be located on storage as close as possible to the VM to which the user is logged on, preferably in the same datacenter.

Azure storage built-in replication mechanisms should be used for BCDR when possible; for less critical environments, ZRS or GRS for Azure Files is recommended. Locally redundant storage (LRS) with local-only resiliency can be used if no zone/region protection is required.

Note: To get insights on designing, sizing, and implementing a Microsoft FSLogix Profile Container solution for large enterprises, refer this article.

Cloud Cache

Cloud Cache should be used only when:

- User Profile or Office containers data availability is required; high-availability SLA is critical and needs to be resilient to region failure.
- The selected storage option is not able to satisfy BCDR requirements. For example, with Azure Files share premium tier, or Azure Files share standard tier with large file support enabled, GRS is not available.
- When replication between disparate storage is required.

When Cloud Cache is used, it is recommended that an SSD is used for the managed disk of the Azure Virtual Desktop host pool VMs and a backup solution must be in place to protect user Profile and Office containers.

Azure Backup

You can use Azure Backup to protect critical user data from data loss or logical corruption when Azure Files share standard or premium tiers are used. Consider the following points when using Azure Backup:

- Use snapshots and policies when the Azure NetApp Files service is used.
- Even if supported, using Azure Backup to save a VM state in the host pool is not recommended since it should be stateless.
- Carefully review your resiliency and BCDR plans for dependent resources (networking, authentication, applications, and other internal services either in Azure or on-premises).
- Network infrastructure, as part of hub and spoke or virtual WAN architecture, must also be available in the secondary region.
- Hybrid connectivity must be highly available in both the primary and secondary regions.

All the best practices and tips on disaster recovery considerations shared in this chapter will help you ensure having strong and resilient BCDR.

Here are a few resources to help you with your disaster recovery plan

- Develop a business continuity and disaster recovery plan
- Use Azure Site Recovery as part of your BCDR plan
- Build resilient application services
- Set up a business continuity and disaster recovery plan

Conclusion and resources

Summary

We started this handbook with a brief overview of Azure Virtual Desktop and the importance of planning a disaster recovery strategy for your environment. It's quite important to have a good BCDR strategy. It is also essential to consider the key areas of Azure Virtual Desktop disaster recovery, including VNets, VMs, user identities, and user and app data.

Later in the handbook, we had a quick look at how to test an Azure Virtual Desktop disaster recovery implementation. Along with this, it is crucial to follow the best practices and guidance discussed regarding the design considerations when implementing a BCDR solution for Azure Virtual Desktop.

We hope this handbook helps you feel more prepared on how to plan, design, and deploy disaster recovery for Azure Virtual Desktop.

Check out the *Resources* section for additional reading and support to help you get started.

Resources

As you advance on your journey with Azure Virtual Desktop and BCDR, here are a few resources that can help:

- Read more about BCDR for Azure Virtual Desktop.
- Follow the Azure security baseline for Azure Virtual Desktop guidance.
- Start now with an Azure free account.
- Get in touch with an Azure sales specialist to get personalized guidance and discuss pricing, technical requirements, and solutions for secure remote work.
- Join the Azure Migration and Modernization Program to get guidance and expert help in migrating your on-premises VDI.

Glossary

The following table contains a glossary of the terminology used throughout this handbook.

Name	Description
Active Directory Domain	A directory is a hierarchical structure that stores information about objects on the network. A directory service, such as Active Directory Domain Services (AD DS), provides the methods for storing directory data and making this data available to network users and administrators.
Azure Active Directory (Azure AD)	Azure AD is Microsoft's cloud-based identity and access management service, which helps your employees sign in and access resources.
Azure Files	Azure Files offers fully managed file shares in the cloud, accessible via the Server Message Block (SMB) protocol or Network File System (NFS) protocol.
Azure NetApp Files	The Azure NetApp Files service is an enterprise-class, high-performance, metered file storage service. Azure NetApp Files supports any workload type and is highly available by default.
Azure Site Recovery	The Azure Site Recovery service manages the replication of Azure Virtual Desktop between regions.
FSLogix	FSLogix is designed to roam profiles in remote computing environments, such as Azure Virtual Desktop. It stores a complete user profile in a single container.
Windows 10 multi-session	Windows 10 Enterprise multi-session, formerly known as Windows 10 Enterprise for Virtual Desktops (EVD), is a new Remote Desktop session host that allows multiple concurrent interactive sessions.

About the author

Ryan Mangan is an end user computing (EUC) specialist, speaker, and presenter, who helps customers and technical communities with end user computing solutions, ranging from small to global, with 30,000+ user enterprise deployments in various fields. Ryan is the owner and author of ryanmangansitblog.com, which has over 3 million visitors and over 70+ articles on Remote Desktop Services and Azure Virtual Desktop. Some of Ryan's publications, and community and technical awards include the following:

- Author of:
  - *Quickstart Guide to Azure Virtual Desktop*
  - *An Introduction to MSIX App Attach*
- VMware vExpert, for eight consecutive years
- VMware vExpert EUC 2021
- Parallels RAS VIPP – three consecutive years
- LoginVSI Technology Advocate – two consecutive years
- Technical person of the year 2017 KEMP Technologies
- Parallels RAS EMEA Technical Champion 2018
- Microsoft Community Speaker
- Top 50 IT Blogs 2020 – Feed spot
- Top 50 Azure Blogs 2020 – Feed spot

Blog site: https://ryanmangansitblog.com
GitHub: https://github.com/RMITBLOG