TECHNICAL WHITE PAPER – **DECEMBER 2017**

NETWORKING AND ACTIVE DIRECTORY CONSIDERATIONS ON MICROSOFT AZURE FOR USE WITH VMWARE HORIZON CLOUD SERVICE

VMware Horizon Cloud Service

vmware®

Table of Contents

Executive Summary

This white paper provides details for the various options and best practices for using Active Directory for user identity and machine registration for VMware Horizon® Cloud Service™ on Microsoft Azure.

Horizon Cloud Service on Microsoft Azure provides a single platform for delivering virtualized Windows applications and shared desktop sessions from Windows Server instances using Microsoft Remote Desktop Services (RDS) running in Microsoft Azure. With Horizon Cloud, you can publish business-critical Windows apps alongside SaaS and mobile apps and desktops in a single digital workspace, easily accessed with single sign-on from any authenticated device or OS.

This white paper describes the use of the platform to meet key business requirements such as making standard Windows applications available to employees, while having common user identity management that meets your organizational security and operational needs.

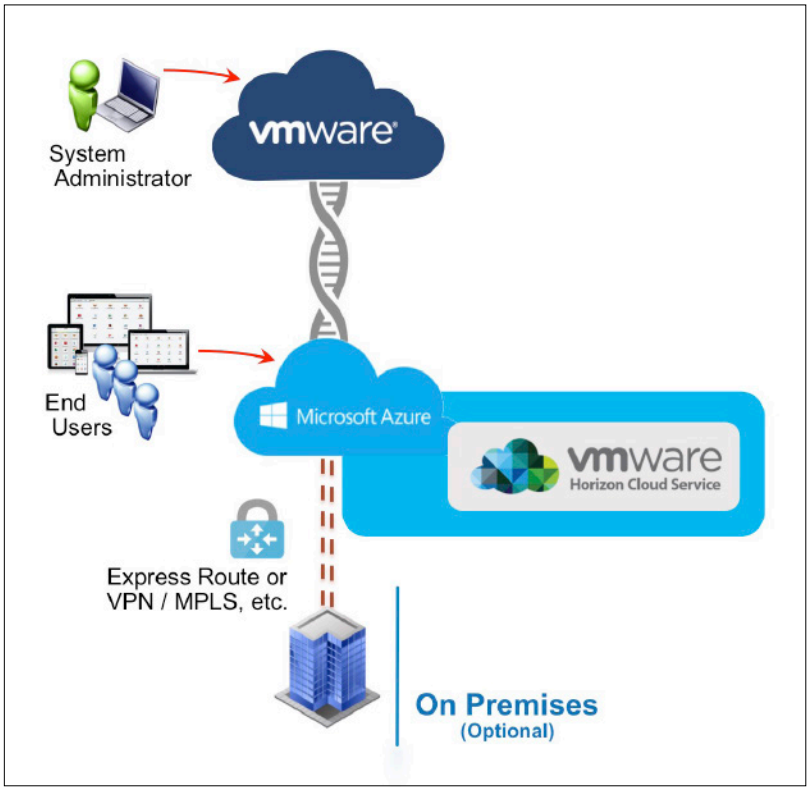
Most enterprises will already have Active Directory on premises for user identity. When delivering a cloud service, it is often important that the same identity (and credentials) are available for use in the cloud. This white paper introduces the key components involved in user identity in the cloud, along with presenting typical configuration options and identifying some best practices. A recommendation is made for various deployment types. The majority of administrators will find that a solution using Azure Active Directory Connect to replicate users into Azure Active Directory, and then Azure Active Directory Domain Services to connect Azure Active Directory to Horizon Cloud Service node, makes the simplest, most reliable, and usually lowest-cost solution.

Further to that, a short discussion regarding some salient networking considerations is presented to help your organization have success in deploying Horizon Cloud Service on Microsoft Azure.

Introduction

Horizon Cloud Service on Microsoft Azure provides a single platform for delivering virtualized Windows applications and shared desktop sessions from Windows Server instances using Microsoft Remote Desktop Services (RDS) running in Microsoft Azure. With Horizon Cloud, you can publish business-critical Windows apps alongside SaaS and mobile apps and desktops in a single digital workspace, easily accessed with single sign-on from any authenticated device or OS.

Administrative management of the RDS and desktop capacity is performed from the Horizon Cloud Service. It securely connects to the Azure capacity from which the RDS and desktop capacity is delivered. End users connect to this capacity via a secure access gateway allowing connection to desktops and applications over the Internet. Optionally, this Azure capacity can also connect back to on-premises environments to allow access to on-premises back-end systems, data, or other services. The following diagram shows a high-level overview of the Horizon Cloud Service on Microsoft Azure.



: Horizon Cloud Service on Microsoft Azure High-Level Overview

User identity is critical, because this defines how end users will connect to their enterprise resources. Typically, the connection is done using username and password. However with features such as two-factor authentication it doesn't need to be. What is essential for most organizations is that the user experience remain consistent between accessing resources on premises and cloud-delivered applications and services. That is, the username and password (or authentication flow) for a desktop accessed on premises would be identical to that served from the cloud.

To achieve this consistency, enterprises will often make use of one of the following approaches:

- Deploy a site-to-site VPN connection between workloads running in Azure Infrastructure and the corporate directory on premises.
- Extend the corporate AD domain/forest infrastructure by setting up replica domain controllers using Azure virtual machines.
- Deploy a stand-alone domain in Azure using domain controllers deployed as Azure virtual machines.
- Leverage native Azure Services to simplify a combination of the above.
- Or, some variant of the above.

All of these approaches have certain advantages and disadvantages, and there are special considerations needed for each. Each of these options is presented and discussed in this white paper.

Before we dive into the specific details, it is important to establish some definitions for key components that will be used throughout this document.

Definitions

Table 1 provides specifications for key components discussed in this paper.

TERM	DEFINITION
Active Directory (AD)	Active Directory manages network, user data, security, and distributed resources. Active Directory primarily uses an LDAP interface. In the context of Horizon Cloud Service, AD is used for user accounts and authentication, machine registration, and Group Policy for management thereof. See Active Directory for more detail.
Azure Active Directory (AAD)	Azure Active Directory is an identity and access management solution for the cloud. AAD is similar to Active Directory that runs on premises, but is specifically designed for the cloud and has a restricted feature set. It helps secure access to on-premises and cloud applications, including Microsoft web services like Office 365, and many non-Microsoft software-as-a-service (SaaS) applications. AAD is available with three service tiers: Free, Basic, and Premium. While Active Directory on premises uses LDAP, AAD uses a REST API to manage identity. Azure Active directory does not manage machines, and does not perform any domain services, for example, domain join or group policy. See Azure Active Directory Overview for more details.
Azure Active Directory Connect (AAD Connect)	Azure Active Directory Connect is a component that can be installed on premises in a Windows Server, which connects the on-premises Active Directory with Azure Active Directory. It does this without the need of a VPN, or similar connection. This allows identity to be synchronized between on premises and the cloud, and is typically used for users of Office 365 and other SaaS apps in AAD. See Integrate your on-premises directories with Azure Active Directory for more information.
Azure Active Directory Domain Services (AAD-DS)	Azure AD Domain Services provides managed domain services such as domain join, group policy, LDAP, and Kerberos/NTLM authentication that are fully compatible with Windows Server Active Directory. This is a fully managed paid service in Microsoft Azure that can be set up with a few configuration options, and requires no ongoing management or maintenance. Azure AD Domain Services synchronizes to Azure Active Directory, allowing Azure Active Directory–managed identity to be used, or synchronizes users and groups from on-premises Active Directory. Azure Active Directory Domain Services can be used to join Azure virtual machines to a domain and apply group policies, without having to deploy domain controllers. See Azure Active Directory Domain Services for more details.
Organizational unit (OU)	An organizational unit (OU) allows users, groups, and computers to be managed in a subdivision within an Active Directory. Typically, each domain will have its own organizational unit hierarchy, which often mirrors the enterprise functional or business structure. See Organizational Units for more information.

TERM	DEFINITION
VPN / ExpressRoute / MPLS	A Virtual Private Network (VPN) or Multiprotocol Label Switching (MPLS) link provides secure network connectivity between on-premises infrastructure and the cloud. ExpressRoute is a Microsoft Azure service that enables you to create private connections between Azure data centers and infrastructure on your premises or in a colocation environment. One key consideration when using a VPN (or an equivalent connection) is the reliability and availability of the link. If all user authentication for cloud services depends on the VPN connection, then if that link were to fail, users would be unable to authenticate. As such, it is often preferable for organizations to have a means to perform in-cloud authentication such that the VPN doesn't form a mission-critical part of daily operations.
Horizon Cloud Service on Microsoft Azure	Horizon Cloud Service on Microsoft Azure requires access to LDAP for user identity and authentication, and also requires AD to perform domain services such as domain join and group policy. As such, it cannot work natively with just Azure Active Directory. It can, however, interoperate with Azure Active Directory using Azure Active Directory Domain Services, and this is one of the configuration modes discussed in the following sections.

Table 1: Key Components

Active Directory Deployment Options

The following 6 scenarios are discussed:

1. Site-to-site link, using on-premises AD only
2. No site-to-site link, AD on one or more Azure-provisioned virtual machines
3. Active Directory replica controllers on one or more Azure-provisioned virtual machines (identity synchronized from on premises)
4. No site-to-site link, using Azure Active Directory-only sync to Azure Active Directory Domain Services
5. No site-to-site link, on-premises sync of AD to Azure Active Directory via Active Directory Connect
6. Site-to-site link, on-premises sync to Azure Active Directory via Active Directory Connect

In order to better understand the components used in each of the options outlined, Table 2 summarizes the components involved in each option. This may help you identify the options that are most suitable to your needs.

	ON-PREMISES AD	VPN	AZURE MANUALLY DEPLOYED/ MANAGED AD	AAD + AAD-DS	AZURE AD CONNECT
Option 1	✔	✔			
Option 2			✔		
Option 3		✔	✔		
Option 4				✔	
Option 5	✔			✔	✔
Option 6	✔	✔		✔	✔

Table 2: Key Components by Option

For each option, a configuration diagram is presented and some key pros and cons are discussed, along with a summary covering the features supported.

Let's get into it!

Option 1 – Use On-Premises AD Only via Site-to-Site Link

In this deployment mode, Active Directory is configured and running on premises. A VPN, or ExpressRoute, is configured to connect the on-premises network into the Azure environment. In effect, the on-premises network extends into the cloud. All authentication is done against the on-premises Active Directory.

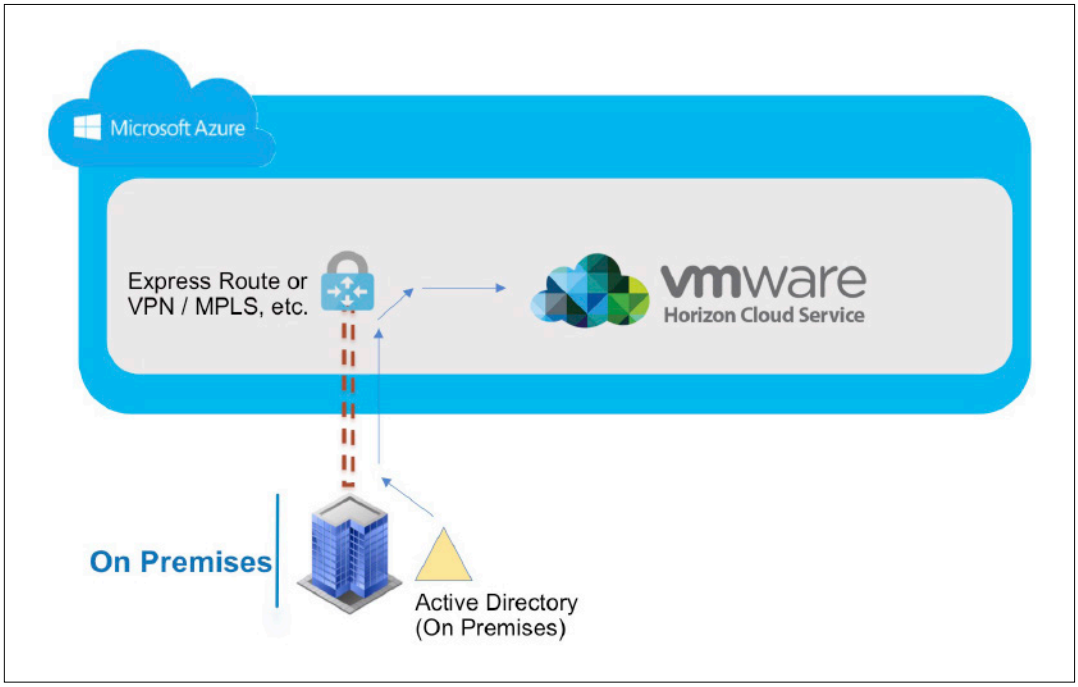


Figure 2: On-Premises AD Only via Site-to-Site Link

Because most enterprises already have Active Directory configured, this deployment mode leverages that infrastructure and requires no new Active Directory configuration. The downside, however, is that the deployment is dependent on the VPN link. The site-to-site link therefore becomes a point of failure: If the site-to-site link fails, then during that time of failure, users will be unable to log in to their desktops or apps in Microsoft Azure. Also, if there is significant latency between on premises and Horizon Cloud Service, then initial user authentication may be slower than is desirable.

Recommendations

If your organization has a very reliable and performant site-to-site link, then this can be a good mode of deployment. It also may be advantageous if your organization is concerned about placing Active Directory in the cloud. However, if you cannot guarantee the reliability of the site-to-site link, or latency may make performance a concern, then this is not the recommended solution.

VMware recommends against using this deployment mode if you can avoid it, because our experience shows that the site-to-site links will typically experience some issues, and when they do, all your users will be impacted.

SUMMARY	
Common identity from on premises	✔
Cloud identity managed in AAD	✘
Highly available (no site-to-site dependency)	✘
Connectivity for on-premises data and systems	✔
Easy ongoing management of cloud AD components	N/A

Option 2 – Active Directory on Azure-Provisioned Virtual Machine

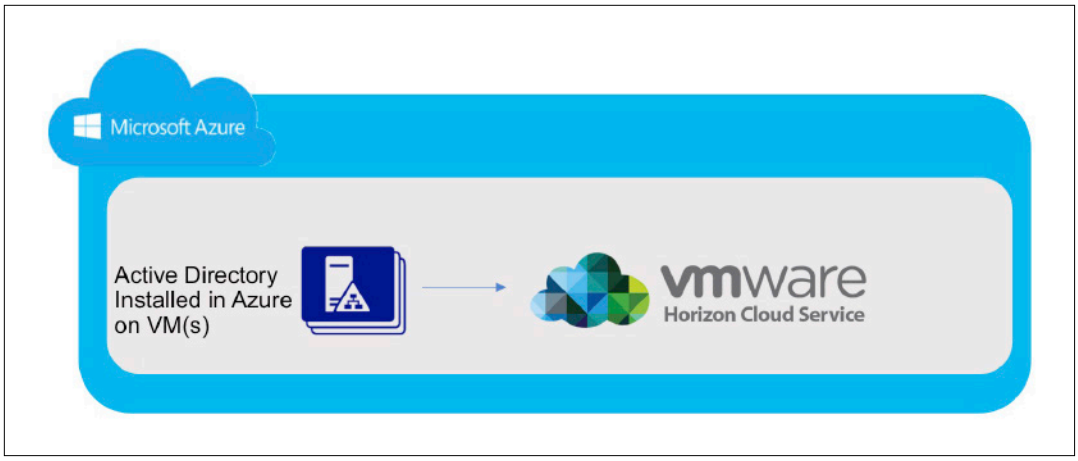


Figure 3: AD Sync on Azure-Provisioned VM

In this option, a virtual machine is provisioned in Azure, and configured to enable Active Directory. In order for this to be a highly available Active Directory implementation, more than one AD machine should be deployed and configured. However, more than one virtual machine incurs cost for compute 24x7 along with Windows Server licensing costs. Management of the Active Directory is done directly in Azure on these deployed VMs.

Approaches such as this one, which require virtual machines to be deployed into Azure, can suffer from administrative overhead and potentially high cost. Once the machines are deployed, administrators must perform any ongoing management of these VMs (for example, patching, monitoring, backing up, and more).

Recommendations

This deployment mode is typically used for quick proof-of-concept deployments where integration with corporate AD would be a time-consuming task requiring multiple teams to be involved in the process.

For a production environment using this sort of deployment, it is recommended to have more than one AD machine deployed, to allow for high availability in the event of a failure. As such, this deployment mode will require at least two machines to be patched, maintained, and updated, bringing an additional operational cost and burden.

While this *can* be used for production use of Horizon Cloud Service on Microsoft Azure, it is not recommended due to the additional overhead this brings as identified previously. An enhancement of this option is suggested in the following section.

SUMMARY	
Common identity from on premises	✘
Cloud identity managed in AAD	✘
Highly available (no site-to-site dependency)	✔
Connectivity for on-premises data and systems	✘
Easy ongoing management of cloud AD components	✘

Option 3 – Active Directory Replica Controllers on Azure-Provisioned Virtual Machine (Replicated Across Site-to-Site Link)

A variant of Option 2 that might provide a better experience is to configure the AD servers in Azure as replica controllers, whereby they replicate from an on-premises AD, as illustrated in Figure 3.

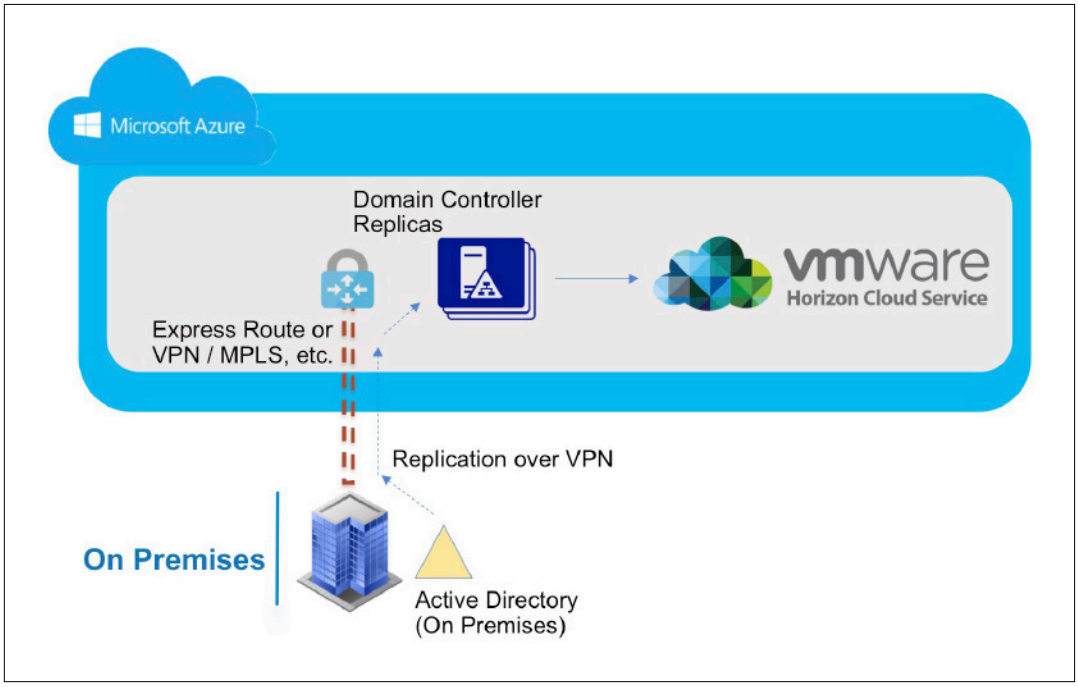


Figure 4: AD Replica Controllers on Azure-Provisioned Virtual Machine

In this scenario, the on-premises domain controller is replicated across the VPN to the domain controllers running in Microsoft Azure. This option has the benefit that the authentication for users in Horizon Cloud Service is *not* dependent on the VPN being connected, while ensuring that the users, groups, policy, and OU structure are all periodically replicated up to Azure. Install a replica Active Directory domain controller in an Azure virtual network provides some more information about this option. Typically, the on-premises domain controller acts as the master, but it is also possible to configure this in write-back mode such that changes made in the cloud replicate back to on premises.

Recommendations

This configuration likely requires multiple domain controllers to be stood up in Microsoft Azure (in separate fault domains in an availability set). This then starts to look very similar to the configuration options described in the following sections that use Azure Active Directory Domain Services (AAD-DS). With AAD-DS, the management, patching, and maintenance are automatically provided by Microsoft Azure. Also, the cost of the service is lower than that of a similarly sized set of virtual machines deployed manually. See configuration Option 4, Option 5, and Option 6 which discuss the use of AAD-DS in more detail.

SUMMARY	
Common identity from on premises	✔
Cloud identity managed in AAD	✘
Highly available (no site-to-site dependency)	✘
Connectivity for on-premises data and systems	✔
Easy ongoing management of cloud AD components	✘

Option 4 – Azure Active Directory Only Sync to Azure Active Directory Domain Services (No Site-to-Site Link)

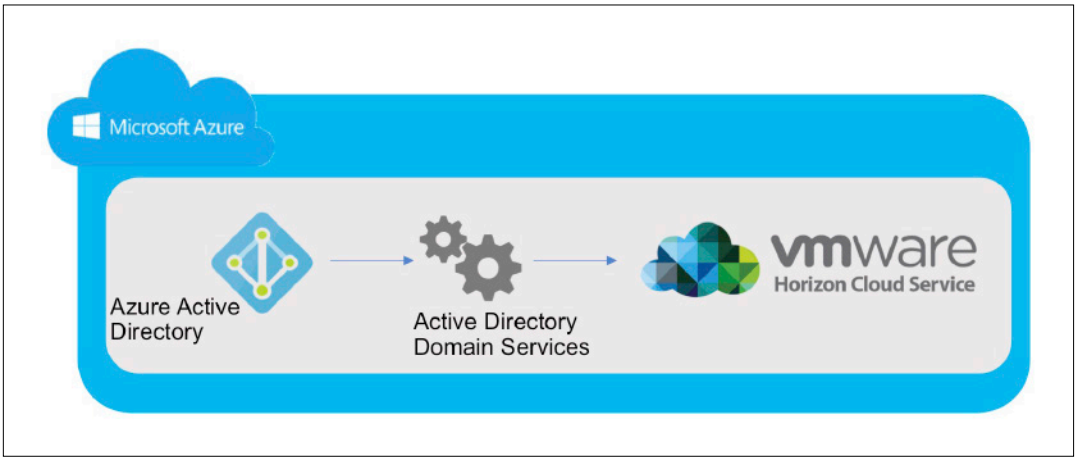


Figure 5: Azure AD Sync to AAD-DS (No Site-to-Site Link)

This mode of deployment might be a good one to use if your organization is already using Azure Active Directory and managing user identities directly in it. In this deployment, user identity is managed directly in Azure Active Directory, and Azure Active Directory Domain Services are synchronized from AAD, which allows Horizon Cloud Services to connect to it for user authentication and domain registration. There is no replication or connection back to on-premises Active Directory, and as such user identity is completely isolated and separate from anything that might be in use on premises.

Recommendations

It is critical that password hashing has been properly configured in Azure Active Directory. If it has not, in order to use Azure Domain Services, the password hashing must be enabled, and once enabled, all existing users in Azure Active Directory must reset their passwords so that the new hashes can be calculated.

Typically, most organizations will have Active Directory available on premises, and as such any user identity would likely need to be synchronized into Azure. This approach is therefore only good if the sync isn't needed. If the sync is required, configuration Option 5 or Option 6 will be a better approach.

SUMMARY	
Common identity from on premises	✘
Cloud identity managed in AAD	✔
Highly available (no site-to-site dependency)	✔
Connectivity for on-premises data and systems	✘
Easy ongoing management of cloud AD components	✔

Option 5 – On-Premises Sync to Azure AD via AD Connect with Azure Active Directory Domain Services

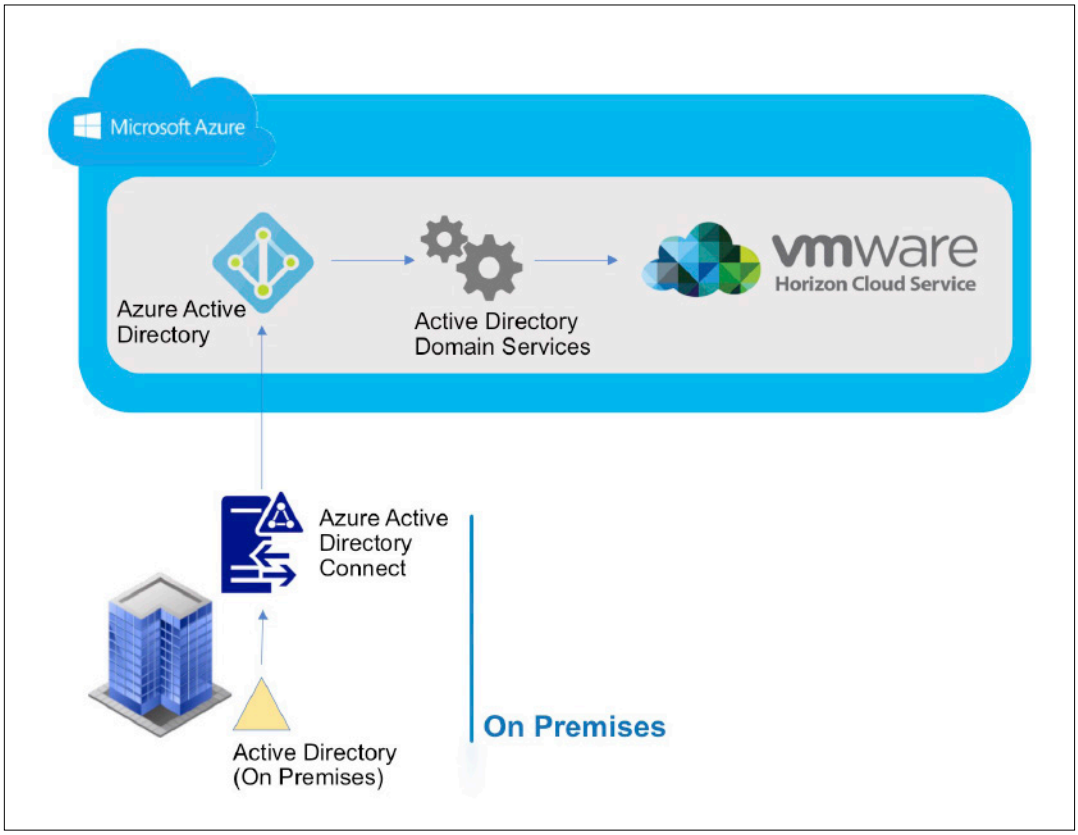


Figure 6: On-Premises Sync to Azure via AD Connect with AAD-DS

This mode of deployment is similar to Option 4, however this option has the advantage that all user identity is synchronized into Azure Active Directory from the organization's on-premises Active Directory. This is done without the need for a VPN link, and all authentication is done locally in the cloud. This then results in a much more highly reliable and performant solution.

In this deployment mode, the organization deploys an additional component on premises. This component is configured to sync from AD on premises, and given credentials to sync to Azure Active Directory. This is done over standard outbound ports without the need for a VPN. The sync does take several minutes, and can result in an updated password on premises taking several minutes before it is synced into the cloud; however, the reduced infrastructure overhead and reduced operational costs make this a good solution.

Recommendations

This is one of the optimal configurations for use with Horizon Cloud Service on Microsoft Azure. It benefits from a fully managed implementation of Domain Services in Azure, which costs less than the equivalent cost of deploying multiple VMs into Azure and managing them as virtual machines. In addition, this solution benefits from the ability to authenticate users and register machines directly in the cloud, and benefits from AD replication into the cloud providing common user identity.

SUMMARY	
Common identity from on premises	✔
Cloud identity managed in AAD	✔
Highly available (no site-to-site dependency)	✔
Connectivity for on-premises data and systems	✘
Easy ongoing management of cloud AD components	✔

Option 6 – On-Premises Sync to Azure AD via AD Connect with Azure Active Directory Domain Services with Additional Site-to-Site Link

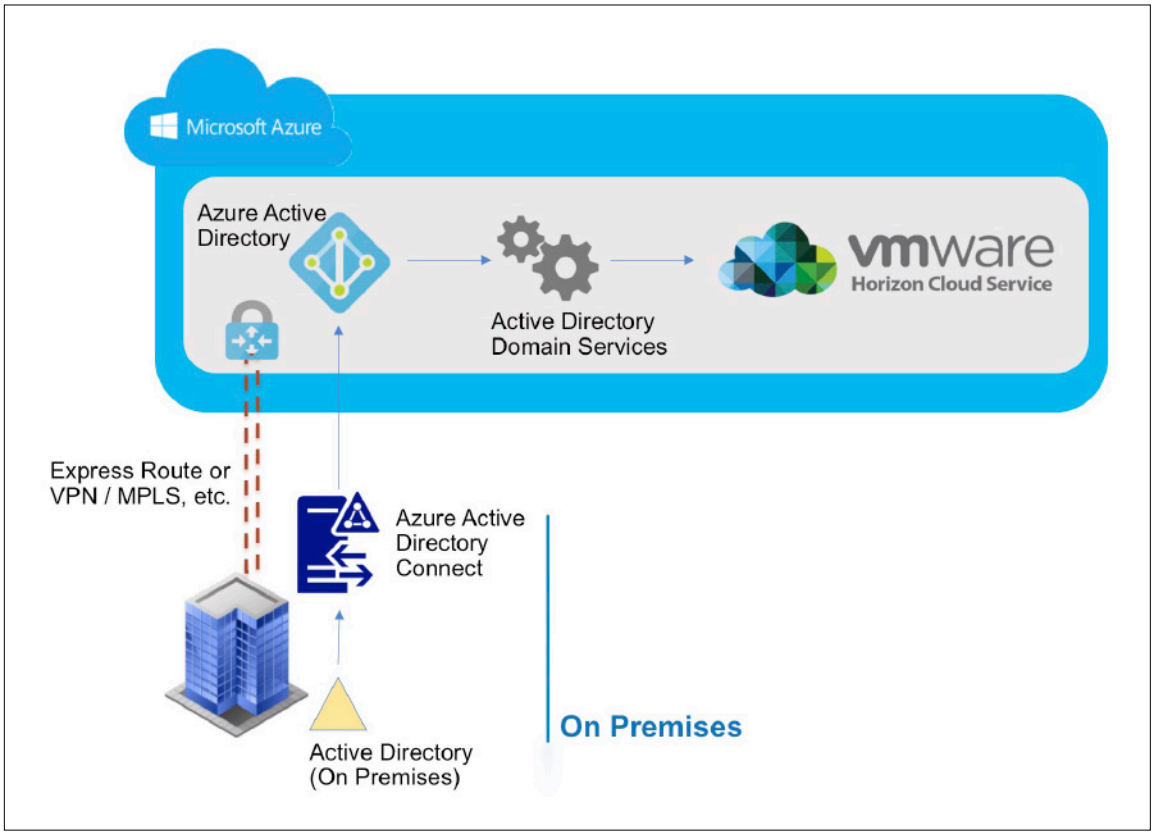


Figure 7: On-Premises Sync to Azure AD via AD Connect with AAD-DS with Additional Site-to-Site Link

This mode of deployment is almost identical to that of Option 5, however, it also includes a site-to-site link (VPN, ExpressRoute, or MPLS). The site-to-site link here, however, is not being used at all for the authentication or identity sync flows. Instead it can be used by users in Azure to connect back to on-premises systems (backend systems, databases, user data, and more). Because the site-to-site link is not required for authentication, primary use of Horizon Cloud Service will be highly reliable.

Recommendations

This is one of the optimal configurations for use with Horizon Cloud Service on Microsoft Azure when the organization wants to use common identity from Azure Active Directory.

For organizations that require connectivity back to on premises for specific applications, user data, or similar, this is the recommended approach. It benefits from Azure Active Directory Connect synchronization between on premises and the cloud (and optionally with write-back to sync any identity updates made into the cloud back to on premises), with the benefit of the ability to access on-premises data and applications securely.

SUMMARY	
Common identity from on premises	✔
Cloud identity managed in AAD	✔
Highly available (no site-to-site dependency)	✔
Connectivity for on-premises data and systems	✔
Easy ongoing management of cloud AD components	✔

Active Directory Deployment Options Summary

This paper identified and described six deployment configurations for managing Identity with Horizon Cloud Service on Microsoft Azure.

Which one is right for my organization?

Well, that depends! There is no one right answer: Just because Option 6 checks the most boxes in the summary, doesn't mean that it's the right solution for all organizations. For example, do you need common identity in the cloud and on premises? Do you need connectivity back to on premises for data? Do you want to use Azure Active Directory (AAD)? Is the ongoing cost and maintenance of infrastructure in the cloud something you want to avoid?

Each of the previous sections concluded with a summary of each of these key points. While a mini summary does mask some subtleties, it may help you narrow down the best options to consider for your needs.

The following table provides a side-by-side summary of each of the options:

1. Site-to-site link, using on-premises AD only
2. No site-to-site link, AD on Azure-provisioned virtual machine
3. Active Directory replica controllers on Azure-provisioned virtual machine (identity synchronized from on premises)
4. No site-to-site link, using Azure Active Directory-only sync to Active Directory Domain Services
5. No site-to-site link, on-premises sync of AD to Azure Active Directory via Active Directory Connect
6. Site-to-site link, on-premises sync to Azure AD via AD Connect

SUMMARY	OPTION 1	OPTION 2	OPTION 3	OPTION 4	OPTION 5	OPTION 6
Common identity from on premises	✔	✘	✔	✘	✔	✔
Cloud identity managed in AAD	✘	✘	✘	✔	✔	✔
Highly available (no site-to-site dependency)	✘	✔	✘	✔	✔	✔
Connectivity for on-premises data and systems	✔	✘	✔	✘	✘	✔
Easy ongoing management of cloud AD components	N/A	✘	✘	✔	✔	✔

Networking for Success

We now have a good idea of the architectures available. Let us now investigate some of the basics for how to configure Azure to set this up and get things working with Horizon Cloud Service.

Regardless of the configuration mode you select, before you can deploy Horizon Cloud Service, you must:

1. Decide on your network architecture within the Azure environment
2. Create a Virtual Network (VNet) onto which Horizon Cloud Service will be deployed
3. Create the AD infrastructure (whether on premises, locally managed in Azure, or via AAD-DS)
4. (Optional) Configure peering (if required) between VNets
5. Configure the Horizon Cloud Service VNet with DNS to point at the domain controller

Selecting Your Network Architecture

Network architecture is beyond the scope of this document, but here are a few things to consider and some questions that you will need to answer:

- In addition to Horizon Cloud Service, what other specific business applications or systems (if any) do you want to host in Azure?
- Are any of these 'shared services' such as DNS, AD, or user data?
- Some organizations like to isolate 'shared services' in their own subscription. This allows for a good security isolation for these mission-critical services, while allowing them to be 'shared' with other subscriptions using ExpressRoute, VPN, or similar. As such, there may be separate subscriptions for 'shared services,' 'devtest,' and 'production.'
- Do you plan to have isolation between 'dev/test' environments and 'production' environments? Or perhaps isolation between 'sales' and 'back office' and 'engineering'? Do you want to do this with different VNets or regions? Or use subscriptions to isolate as mentioned previously?

Most of the above questions will likely lead you to require more than one VNet, each in its own resource group (and possibly separate subscriptions too!). This will allow network-level polices to be applied. Many organizations choose to have a 'shared services' VNet, which hosts things like user data, DNS, and AD, and other VNets for each department or segment area of the organization (for example, dev/production).

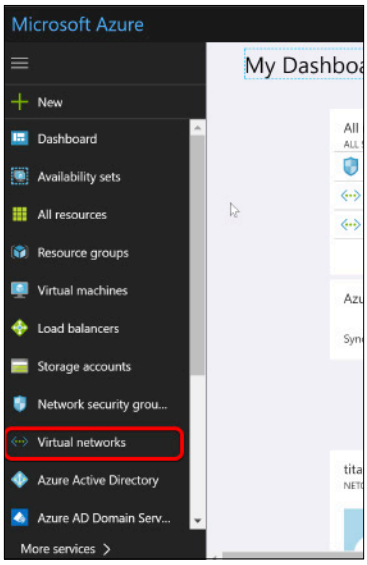
Some further considerations:

- In what region or regions are the consumers of the Azure service located? For Horizon Cloud Service, while it is optimized to work well over highly latent networks, the best user experience is achieved with low latency and reliable networks. As such, it is preferred that you deploy your Horizon Cloud Service node in an Azure region close to your user population.
- It is possible to deploy more than one Azure node, whereby each node can be deployed into a different Azure region. However, because VNets cannot span regions, any intra-region connectivity must be considered. Also, Microsoft charges for any inbound and outbound network ingress and egress between regions—another consideration into what services are placed where. If your needs require intra-region connectivity, then ExpressRoute or VPN is required to connect networks.

Once you have identified your required Azure network and infrastructure architecture design, you can start by creating the required VNets and other resources. The following sections are not intended to be absolute detailed step-by-step guides. They represent high-level guidance on the process to follow, with some important observations highlighted and some useful links for further reading. First, you need to create the required VNet(s).

Create a Virtual Network

Creating a Virtual Network (VNet) can be done simply from the main Virtual Networks menu / blade.



Considerations regarding VNet creation:

- When creating the VNet, you must decide on the address space. Horizon Cloud Service will automatically expand the VNet address space if needed.

  Note: If the VNet will be peered to another VNet, it is not possible to extend the address space. As such, it is highly recommended to make this address space as large as possible when creating the VNet (prior to applying the peering).

- Select the region in which you want to deploy Horizon Cloud Service.
  - **Note:** VNets cannot span multiple regions. You therefore must decide in which region you want to deploy the node.
  - It is recommended (but not mandatory) to place the node in a geographic region close to the end-user population that will be the primary users of the capacity. This yields the best results because those users will benefit from lower latency.

Create Active Directory

Option 1 – You Plan to Use On-Premises Active Directory via VPN

Setting up the on-premises AD and the VPN or site-to-site link is beyond the scope of this document. However, this ExpressRoute overview might prove useful for ExpressRoute learning and configuration.

These resources provide additional useful information pertinent for configuring VPNs in Azure:

- About VPN Gateway
- Planning and design for VPN Gateway
- Create a Site-to-Site connection in the Azure portal

One thing to remember is that when peering VNets, once a VNet is peered then its address space cannot be expanded. This is important to consider if you will be using ExpressRoute or a similar method to connect into Azure prior to adding the network peering.

Option 2 – Create Active Directory Machine(s) (If Required)

If you want to create and manage AD locally in Azure, you can create a virtual machine at this stage for this purpose. You could create a separate VNet (see Create a Virtual Network) or deploy the AD into the same VNet that you created. If using a new VNet, the new VNet must be peered to the existing VNet as described previously.

You can deploy a VM by going to the Virtual Machines blade, selecting 2012 Datacenter or 2016 Datacenter, and deploying it into the virtual network and subnet of choice.

Once deployed, make sure it is assigned a static IP address, and then configure the AD (and DNS) features in the server OS.

Option 3 – Create Azure Active Directory Domain Services

Azure Active Directory (AD) Domain Services provides an excellent overview to Azure Active Directory Domain Services (AAD-DS).

Setting up AAD-DS is really straightforward. At the time of writing this must be done using the Azure portal, however we understand from assorted internet forums that automation of this will be possible soon (using PowerShell). The Enable Azure Active Directory Domain Services using the Azure portal guide provides an easy-to-follow walkthrough of the process.

In summary, to set up AAD-DS:

- Provide a DNS domain name
- Provide a resource group / region
- Select a VNet (or create a new one) on which to run AAD-DS infrastructure
- Configure Admin group

Once these steps are complete, you can deploy. Deployment takes approximately 60 minutes.

Password Synchronization

Once deployed, it is **critical** that you configure password synchronization. Configuration should be done before any users are synchronized into the Azure Active Directory. If any user accounts were created prior to enabling the password hash synchronization, the accounts will need to have their passwords reset prior to being available for use. Enable password synchronization to Azure Active Directory Domain Services provides more information.

Managing the New Domain

Once deployed, you can manage the AAD-DS domain in the normal way. For example, by deploying a server OS you can then connect to the Domain and configure it. For more information, see Administer an Azure Active Directory Domain Services managed domain.

Key Considerations About Azure Active Directory Domain Services

- Once the AAD-DS is set up, Microsoft Azure takes care of the ongoing management of the underlying infrastructure (including patching, monitoring, and more).
- User account replication for the domain including user accounts, group memberships, and credentials from the Azure Active Directory tenant are automatically made available in AAD-DS.
- AAD-DS does however 'flatten' any OU structure in the Azure domain. That is, any complex hierarchy of OU will be flattened into a single level when synchronized. It is possible to manually create additional hierarchy in AAD-DS directly (see Managing the New Domain). However, if this is done, then structure is not reflected back on premises at all.
- Best practices suggest that custom OUs and Group Policies should be created for RDSH Servers. Create an Organizational Unit (OU) on an Azure AD Domain Services managed domain and Administer Group Policy on an Azure AD Domain Services managed domain provide more detail on how to configure this.
  - This is one of the (current) downsides to using AAD-DS: Specifically, the customer OU and GPs created in AAD-DS will not replicate back to on premises. If you require a complex domain structure, then replicating on-premises domain controllers into Microsoft Azure (Option 2) might be the best option. Option 2 maintains the complex OU hierarchy of Azure that is lost when using AAD-DS.

Configure Azure Active Directory Connect (Optional)

If you wish to synchronize the on-premises Active Directory to Azure Active Directory without requiring a site-to-site link (VPN, etc.), you can do so using Azure Active Directory Connect.

Integrate your on-premises directories with Azure Active Directory provides an excellent overview of Microsoft Azure Active Directory Connect, with a useful introduction and installation guide. In summary, you install the AAD-Connect application onto a server, configure it with AD credentials as well as credentials to access Microsoft Azure, configure some sync options, and that's it!

One consideration here is to decide if any of the write-back features (whereby changes made in Azure Active Directory are written back on premises, for example, password or group updates) are required. This can be configured here too, however, the configuration is dependent on the tier of Azure Active Directory selected. At the time of writing, write-back requires AAD Premium or higher.

Change the VNet Default DNS

Once your Active Directory is available, it is recommended to update the DNS configuration on your VNet(s) to point at that DNS infrastructure. Once this update is complete, any VMs added onto those VNets (in any subnet) inherit the default DNS information.

By default, VNet uses Microsoft Azure DNS, which cannot be used as the only DNS for Horizon Cloud Service. Change this value to point at your DNS so that machines can resolve internal addresses as well as external public addresses.

Peering VNets

If you wish to join multiple VNets together—for example your AD is in one VNet, and you require the VNet that will be used for the Horizon Cloud Service infrastructure to be in a different VNet—you will need to peer these networks so that AD can be accessed from Horizon Cloud Service. Remember that once VNets are peered, then their address space cannot be expanded. If you need to expand the address space after performing peering, you must un-peer, adjust space, and then re-peer the networks. (Of course, this might be impactful to your operations, so it is advised to make the address space as big as possible up front.)

When adding the new peering configuration, it is suggested to use a descriptive name for the peering using the name of the VNet so that other administrators are able to easily understand where it is peer to. Select the virtual network to peer to (for example, the Active Directory VNet) and ensure both **Allow forwarded traffic** and **Allow Gateway Transit** are selected.

Remember to also configure peering in the opposite direction.

Getting Started with Horizon Cloud Service Deployment

Once AD, DNS, and VNets are all configured, you can then create a Service Principal and deploy Horizon Cloud Service onto Microsoft Azure!

Follow the Getting Started Guide for more details.

Conclusion

This white paper introduced some key concepts about networking and Active Directory, and outlined some possible network infrastructure considerations when deploying Horizon Cloud Service on Microsoft Azure. The paper then detailed some high-level considerations around networking design and implementation to help make Horizon Cloud Service on Microsoft Azure deployments successful.

Authors

Peter Brown has been with VMware since 2012. Peter Brown is a Director of R&D in the End-User Computing Business unit, and is currently the engineering lead for the Horizon Cloud Service with Microsoft Azure. Peter has worked with Horizon 7 (on-premises) and Horizon Cloud Service, and has led engineering efforts for innovations such as True SSO, Linux desktops, USB redirection, RTAV, serial and scanner redirection, and much more.

Contributors

Nevon Brake is a Staff Engineer in the End-User Computing group at VMware. Prior to joining VMware, he was a Principal Engineer at Desktone. He has spent the last 6 years focused on delivering cloud-hosted virtual desktops and applications to customers. He is currently an engineering lead for Horizon Cloud on Microsoft Azure, with expertise in virtualization platforms and cloud-scale orchestration.

As Director of Architecture for Horizon Cloud at VMware, **Simon Le Comte** is focused on the Technology leadership with Cloud-Based Desktops and Applications including integration work across the VMware End-User Computing portfolio. As a veteran of Desktop and Application Virtualization, Simon has spent his entire career focused on the transformation of physical to virtual computing. In addition, he works closely with customers, partners, and the VMware community to evangelize desktop-as-a-service through the web, social, and events. Before joining VMware, Simon's career included positions at Citrix, Hewlett Packard, and Wyse Technology.

Jerrid Cunniff has been with VMware since 2013 and is a Sr. Architect for Horizon Cloud Services, in the End-User Computing business unit. Jerrid is focused on technical solution development for Cloud-Based Desktops and Applications along with integration of the VMware End-User Computing portfolio. In addition, Jerrid works closely with marquee customers and partners to ensure their success with Horizon Cloud.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com