Microsoft Azure

Virtual Machine Readiness Assessment

Ready – Are you still weighing the pros and cons of moving your virtual machines to Microsoft Azure? Do you understand the various migration scenarios that it supports? Have you thought about your identity provider? Are there any roles or features that are unsupported? This section runs you through all such questions to provide you with a better understanding of what is required to move your machines to Microsoft Azure.

Set - Do you know what hardware is available to use? Do you need to create your own virtual network? How much storage do you need? What items do you need to be aware of with regards to security? This section provides the answers to all these questions and prepares you for moving your machines to Microsoft Azure.

Move - Do you have an Azure subscription yet? Do you need help provisioning your virtual machine or moving your data? Do you need to monitor your new virtual machine? How do you get support once you have moved your machine? This section addresses these common questions and simplifies the process of moving your machines to Microsoft Azure.

What we checked

The checklist below provides an overall indicator of what has been done so far and what is still left to do. Use it as a roadmap to understand and identify the next steps.

Ready	Understand the benefits	✓
	Choose your scenario	⚠
	Determine identity provider needs	✓
	Review unsupported roles and features	⚠
Set	Evaluate hardware needs	✓
	Configure your network	⚠
	Plan for storage	⚠
	Prepare a disaster recovery plan	✓
	Secure your environment	✓
	Ensure a healthy environment	⚠
	Optimize your configuration	✓
Move	Get a subscription	✓
	Provision your virtual machine	✓
	Move your data	✓
	Monitor your environment	✓
	Get support	✓

✓ No work is required. You are good to go!
⚠ Planning or configuration is required before you move.

Ready

Understand the benefits

Windows Server AD DS running on Microsoft Azure virtual machines is well-suited as a branch office/perimeter network, a disaster recovery site, and for the deployment of network applications that require Active Directory.

- *Branch Office/Perimeter Network*.
  Many Windows Server AD DS deployment scenarios are well-suited for deployment as VMs on Microsoft Azure. For example, suppose you have a company in Europe that needs to authenticate users in a remote location in Asia. The company has not previously deployed Windows Server Active Directory DCs in Asia due to the cost to deploy them and limited expertise to manage the servers post-deployment. As a result, authentication requests from Asia are serviced by DCs in Europe with suboptimal results. In this case, you can deploy a DC on a VM that you have specified must be run within the Microsoft Azure datacenter in Asia. Attaching that DC to a Microsoft Azure virtual network that is connected directly to the remote location will improve authentication performance.
  In addition, it may be more cost effective than maintaining a secure facility to house the server, while keeping Microsoft Azure virtual machines under the direct control of your centralized IT staff.

  Users and computers on the corporate network in remote locations may see improved authentication and group policy application performance by creating a site-to-site VPN connection between the Microsoft Azure virtual network and the router at their location.

  Once the Microsoft Azure virtual network has a site-to-site VPN tunnel configured, you can promote a replica domain controller on a Microsoft Azure virtual machine in that region. Associating the subnet that the clients are on and that the Microsoft Azure domain controller is in to use the Microsoft

Azure site in Active Directory will allow that Dc to service those clients without traversing the globe.

- *Disaster Recovery Sites*.
  Microsoft Azure is also well-suited as a substitute to otherwise costly disaster recovery (DR) sites. The relatively low-cost of hosting a small number of domain controllers and a single virtual network on Microsoft Azure represents an attractive alternative.
  You can promote replica domain controllers for each domain in your forest by using Microsoft Azure virtual machines and a Microsoft Azure virtual network that connects to your on premises network. These virtual machines will run in a Microsoft Azure datacenter in any region of the globe that you choose. The Microsoft Azure virtual network allows these virtual machines to remain connected with your on premises network which helps keep Active Directory up-to-date.

- *Deployment of Active Directory Dependent Applications*.
  You may want to deploy a network application on Microsoft Azure, such as SharePoint, that requires Windows Server Active Directory but has no dependency on the on-premises network or the corporate Windows Server Active Directory. In this case, deploying an isolated forest on Microsoft Azure to meet the SharePoint server's requirements is optimal. Again, deploying network applications that do require connectivity to the on-premises network and the corporate Active Directory is also supported. If, at a later stage, you decide to extend connectivity to on premises clients, you could add a Site-to-Site VPN tunnel to the Microsoft Azure virtual network and establish a trust between forests or promote replica domain controllers in Microsoft Azure virtual machines for these on premises domains.

Key information

- Use AD DS on Microsoft Azure as a Branch Office/Perimeter Network, for Disaster Recovery Sites, or deployment of Active Directory Dependent Applications.
- Bring your own virtual machine from your on premises environment or build a new one from the Microsoft Azure image gallery.
- Quickly set up virtual machines in response to changing business needs.
- Pay only for what you use.

Read more

Scale on demand, only pay for what you use

Guidelines for Deploying Windows Server Active Directory on Azure Virtual Machines

Moving a development or test environment

Microsoft Azure enables you to develop and test applications faster, at reduced cost, and with the flexibility to deploy in the cloud or on-premises

Read more Development and Test Using Virtual Machines

Moving a production environment

Since you are deploying a production workload, you will want to make sure you review the Microsoft Azure SLAs (http://www.windowsazure.com/en-us/support/legal/sla/). Understanding the SLA for each of the various Azure services you are leveraging will help you decide how to best deploy your workload.

Read more Microsoft Azure Business Continuity Technical Guidance

Service Level Agreements

Choose your scenario

From virtualizing and then uploading an existing physical server to building an entirely new VM from a gallery image, there are lots of ways to go to the cloud.

- You can build a new virtual machine from the Microsoft Azure image gallery and migrate your data to it.
- You can migrate an existing VM from on-premises or another IaaS environment
- You can virtualize an existing physical server and upload it to Azure

Microsoft Azure Deployments Used

Windows Server AD DS or AD FS can be partly deployed on-premises and partly deployed on Microsoft Azure Virtual Machines. Depending on your business and technical requirements it is important to note that there are critical differences between running Windows Server AD DS and AD FS on Microsoft Azure virtual machines versus on-premises, and important decisions that affect design and deployment.

Read more

Install a new Active Directory forest in Microsoft Azure

Guidelines for Deploying Windows Server Active Directory on Microsoft Azure Virtual Machines

Move workloads virtualized in Hyper-V to Microsoft Azure

This workload is already running in Hyper-V. It should be portable directly to Microsoft Azure using CSUPload.

Read more CSUPload

Convert-VHD

Move workloads virtualized in VMWare to Microsoft Azure ✓

This workload is running in VMWare.

Read more CSUpload

Microsoft Virtual Machine Converter Solution Accelerator

Move workloads virtualized in Xen or AWS to Microsoft Azure ✓

This workload is running in XenServer or Amazon Web Services. You will need to migrate the virtualized servers to Microsoft Azure either directly or through Hyper-V.

Read more CSUPload

Only virtualized instances are allowed in Azure ✓

Microsoft Azure is a completely virtualized environment, so you will need to either virtualize the servers in your workload prior to migrating them to Microsoft Azure or plan on building new virtual machines from the Microsoft Azure image gallery.

Read more P2V with System Center Disk2VHD

If using VMWare, Solution Accelerator

Virtualized in Azure

One or more of your servers is already running in Microsoft Azure

Server AzureLab-DC01.AzureLab.com

Determine identity provider needs

Although you most likely have the machines in your on premises workload joined to the domain because it was convenient, you might find that you do not need to fully replicate that authentication model in Microsoft Azure. With Microsoft Azure, you can:

- **Deploy Active Directory on Microsoft Azure virtual machines in an isolated forest**.

  You can run applications, like SharePoint, which have dependencies on Active Directory with an isolated Active Directory forest that runs in Microsoft Azure for development, testing or proof-of-concept (POC) scenarios. You can also connect to an on-premises domain by configuring a site-to-site VPN connection on the virtual network.

- **Deploy Domain Controllers to Microsoft Azure VMs as a Branch Office solution**

  Microsoft Azure is well-suited as a substitute for a branch office solution. Running domain controllers in remote branch offices with minimal security may require deployment of Read-Only Domain Controllers (RODCs). Running domain controllers on Microsoft Azure virtual machines provides a greater level of control over the machine running in your Microsoft Azure subscription at a Microsoft Azure datacenter in a specific region. When extending your on premises Active Directory to Microsoft Azure, you might opt to deploy RODCs, not because of security risks typically associated with a branch office, but to keep the egress

network costs down. Deploying RODCs might prove to be more cost effective than a writable domain controller because RODCs do not replicate outbound.

- **Implement Trusts from Forests in Microsoft Azure on-premises Forests**

  Some organizations may not allow placing domain controllers for the on premises Active Directory in Microsoft Azure. Creating a Microsoft Azure virtual network with a site-to-site IPsec VPN tunnel to your on premises enables you to create a forest or domain trust between your on premises Active Directory and another forest in Microsoft Azure. Using a trust allows you to retain security isolation at the forest boundary, while providing on premises accounts to access resources running in your forest in Microsoft Azure.

- **Replicate File Content between Microsoft Azure VMs and on-premises Domain Controllers/File Servers**

  The Distributed File System Replication (DFSR) service can be used in Microsoft Azure either for replicating SYSVOL on domain controllers or for DFSR replicated folders on member servers. When a replicated folder replicates between one or more virtual machines in Microsoft Azure and on premises domain controllers or file servers, you must consider the need to create or modify content in the Microsoft Azure site. Deploying a read-only DFSR replica in Microsoft Azure (or a Read-only domain controller (RODC) if it is SYSVOL) will keep billable egress traffic from Microsoft Azure back to the on premises at a minimum.

FIPS is used on domain controllers 

Active Directory Domain Services (AD DS) that are configured for Federal Information Processing Standard (FIPS) are not compatible with the Password Sync feature.

Password Sync is a feature of the Windows Azure Active Directory Sync tool that synchronizes user passwords from your on premises Active Directory to Microsoft

Azure Active Directory ("Azure Active Directory"). This feature enables your users to log on to their Azure Active Directory services (such as Office 365, InTune, CRM Online, etc.) by using the same password that they use to log on to your on premises network.

Read more Implement Password Synchronization

Microsoft Azure Going to be Used as a Branch Office

Microsoft Azure is well-suited as a substitute for a branch office situation. Unlike a typical branch office, you will have physical control over the servers. However, in Microsoft Azure, egress traffic back to the on premises network is billable. Therefore, RODCs might prove to be more cost effective than a writable domain controller because RODCs do not have any outbound replication.

Read more

Differences Between an RODC and a Writable Domain Controller

SharePoint 2013 on Microsoft Azure Infrastructure Services

Read-Only Domain Controllers Application Compatibility Guide

Placing Several RODCs in the Same Site

Password Replication Policy Administration

Global Catalog Server Requirement for User and Computer Logon

Plan Global Catalog Servers

No RODCs Deployed or Planned to Deploy

This issue is raised only for informational purposes.

Regardless of whether you create a virtual network or not, Microsoft Azure charges for egress traffic but not ingress. Various Windows Server Active Directory design choices can affect how much egress traffic is generated by a deployment. For example, deploying an RODC limits egress traffic because it does not replicate outbound. You might deploy an RODC in the Microsoft Azure site, depending on your requirements for performing write operations against the DC and the compatibility of applications and services in the site with RODCs.

Suggested actions

Microsoft Azure does not present the physical security risk of a branch office, but RODCs might still prove to be more cost effective because the features they provide are well-suited to these environments albeit for very different reasons. For example, RODCs have no outbound replication and are able to selectively populate secrets (passwords). On the downside, the lack of these secrets might require on-demand outbound traffic to validate them as a user or computer authenticates. But secrets can be selectively prepopulated and cached.

RODCs provide an additional advantage in and around HBI and PII concerns because you can add attributes that contain sensitive data to the RODC filtered attribute set (FAS). The FAS is a customizable set of attributes that are not replicated to RODCs. You can use the FAS as a safeguard in case you are not permitted or do not want to store PII or HBI on Windows Azure. For more information, see RODC Filtered Attribute Set.

Make sure that applications will be compatible with RODCs you plan to use. Many Windows Server Active Directory-enabled applications work well with RODCs, but some applications can perform inefficiently or fail if they do not have access to a writable DC.

Read more Guidelines for Deploying Windows Server Active Directory on Microsoft Azure Virtual Machines

Will implement trusts from Microsoft Azure to on premises

Establishing a forest or domain trust back to one or more on premises forests will generate billable egress traffic whenever trusted accounts authenticate or perform name-to-SID lookups against on premises trusted domains.

Read more SharePoint 2013 on Microsoft Azure Infrastructure Services

Additional Configuration for Functionality Across Forests (Multiple Forest Considerations in Windows 2000 and Windows Server 2003)

Review unsupported roles and features

Microsoft supports several products running in Microsoft Azure virtual machines as well as many of the roles and features of Windows as documented in Microsoft server software support for Microsoft Azure Virtual Machines. Although many of the core Windows roles and features are fully supported in Windows virtual machines, not everything is supported today. Some of these roles and features do not have a Microsoft Azure equivalent, but many of them can be implemented using Microsoft Azure features. For example, the Windows Network Load Balancing feature is not supported; instead, you can use Microsoft Azure virtual networks to enable this. To learn more, refer to Load Balancing for Azure Infrastructure Services.

When using the Microsoft Azure image gallery, the unsupported roles and features are automatically not installed. If you are moving an existing virtualized machine, you must familiarize yourself with the above list to ensure that you are running a

supported configuration. As you review the unsupported roles and features, keep in mind that you may be able to modify the design of your workload and still be well-suited for a move to Microsoft Azure virtual machines.

Storing data on the volume labeled Temporary Storage in a Microsoft Azure virtual machine is not supported. Placing the AD DS database, AD DS Logs, or SYSVOL on this volume will result in a domain controller that will not boot after the next service healing *(the virtual machine is moved between Microsoft Azure hosts)* takes place because all data in that volume is lost when the virtual machine moves between Microsoft Azure hosts.

Key information

- Many of the most popular Microsoft products are supported.
- Notably, DHCP, Hyper-V, Remote Access (Direct Access) roles are not supported.
- Clustering, WINS, NLB, and SNMP features are not supported as well as a few others.
- Placing the AD DS database, AD DS Logs, or SYSVOL on the volume labeled Temporary Storage in a Microsoft Azure virtual machines is not supported.
- Microsoft Azure gallery images are available for use.

Hyper-V isn't supported in Microsoft Azure

Hyper-V hosts are not supported in Microsoft Azure, if you wish to run VM guests they should be configured to run in Microsoft Azure as independent virtual machines

Read more Microsoft server software support for Microsoft Azure Virtual Machines

Local volume must be NTFS

Just like for on-premises machines, Microsoft recommends that virtual machines running in Azure have their volumes formatted as NTFS.

Microsoft Azure doesn't support the use of Bitlocker on the operating system drive

While running Bitlocker is a recommended practice, Microsoft Azure does not support running BitLocker on the operating system drive. BitLocker on data disks is supported.

Read more Microsoft server software support for Microsoft Azure Virtual Machines

Move workload to server class operating system

Client operating systems are not supported in Microsoft Azure. All workloads must be composed entirely of server operating systems.

Read more How to Create a Custom VM

Virtual Machines Licensing FAQ

Move workloads to a 64-bit operating system

Although 32-bit applications are supported in Microsoft Azure, 32-bit operating systems are not. All workloads must run on 64-bit operating system.

Read more How to Create a Custom VM

Only server operating systems 2008 R2 and later are supported in Microsoft Azure

Server operating systems earlier than 2008 R2 are not supported in Microsoft Azure. Any workloads that contain Windows 2008 or earlier must be migrated to Windows 2008 R2 or later.

Suggested actions Since only server operating systems 2008 R2 and later are supported in Azure, we recommend you rebuild your server natively in Azure using a gallery image. This will ensure that you minimize the chances of configuring your OS such that it cannot migrate to Azure.

After building a new server OS, be sure to test your solution.

Read more How to Create a Custom Virtual Machine

Server AzureLab-DC01.AzureLab.com

Some Windows roles are not supported in Microsoft Azure 

Only certain Windows features are supported. They are outlined in the following knowledge base article (which is subject to change).
http://support.microsoft.com/kb/2721672

Read more Microsoft server software support for Microsoft Azure Virtual Machines

Set

Evaluate hardware needs

When you create your new virtualized servers in Microsoft Azure, you can choose from a variety of virtual machine sizes. Each size has a predefined amount of memory, cores, disk space, and so on. The virtual machine sizes are documented here:

http://msdn.microsoft.com/library/azure/dn197896.aspx

Your first instinct may be to choose the virtual machine size that most closely matches the hardware in the corresponding on premises server. But if your on premises server sits idle most of the time, it may make sense to scale down to a smaller virtual machine size. The smaller sizes cost less, and if you do need to size up in the future, it is as simple as making a configuration change in the portal and then restarting the machine.

You may also want to consider scaling out, that is adding more virtual machines to your environment, rather than scaling up, that is adding more resources to your existing machine(s). With Microsoft Azure, it is more effective to scale out by adding virtual machines to the farm. Provisioning new servers is faster, which enables quicker response to peak demands. Scale out also provides two other significant benefits, increased availability and reduced downtime (planned or unplanned.) From a high availability perspective, virtualization flexibility and cost makes it feasible to build server and service redundancy.

Key information

- Microsoft Azure supports between 768 MB and 112 GB of RAM, and up to 16 cores.
- Smaller virtual machine sizes cost less and are easy to size up in the future as your business needs change.
- Consider scaling out rather than scaling up, that is having multiple smaller virtual machines rather than just a few large ones.

Ensure appropriate domain controller sizing ✔

An on premises domain controller uses more than 14 GB of RAM.

In Microsoft Azure IaaS, each instance is hosted in a virtual machine, providing a guaranteed level of compute (cores, memory, and local disk space) to the instance. Based on your application requirements, you subscribe to a compute instance representing a virtual server with a given specification. Microsoft Azure offers various instance sizes from Small with one core to Extra-Large with eight cores. The other compute parameters scale similarly with instance size. The requirement to add more RAM on Windows Azure Active Directory is directly proportional to the compute instance type (A0-A9).

Read more Virtual Machines Pricing Details

Microsoft Azure has a limit of [448 currently] GB of RAM for a virtual machine ✔

The RAM available to Microsoft Azure machines ranges from 768 MB (ExtraSmall) to 448 GB (G5).

Read more Although focused on SQL Server, Performance Guidance for SQL Server in Microsoft Azure Virtual Machines includes a number of general performance recommendations for Microsoft Azure virtual machines.

Virtual Machine and Cloud Service Sizes for Microsoft Azure

Microsoft Azure virtual machines can have a maximum of 16 cores ✔

Microsoft Azure currently limits you to 32 cores for its largest virtual machine (G5)

Read more Virtual Machine and Cloud Service Sizes for Microsoft Azure

Microsoft Azure virtual machines have a minimum of 768 MB of RAM

The RAM available to Microsoft Azure machines ranges from 768 MB (ExtraSmall) to 448 GB (G5).

Read more Don't worry! Nothing is going to break if you get more RAM than expected. Just keep in mind that while the minimum RAM for Windows 2008 R2 is 512MB, the recommended amount is 2GB of RAM. For more details please visit Windows Server 2008 System Requirements

Understand the potential performance impact on workloads that are heavily I/O-dependent

Microsoft Azure virtual machines uses a combination of local drives and remote storage to provide data storage. The local drives are directly attached commodity disks and the remote storage is commodity disks abstracted by the storage layer. This means that by default your I/O won't be as fast as your on-premises SAN drives.
However, what you lose in raw performance you gain in redundancy. Microsoft Azure is built with the mindset that disks can fail at any time. This means that the ability to guarantee the preservation of your data is built into the core design of the system.

Suggested actions You can gain some level of performance by spreading your I/O over multiple disks. The "Performance Guidance for SQL Server in Microsoft Azure Virtual Machines" whitepaper includes information on how to configure this.

You will need to test your workload extensively to ensure that it performs at acceptable levels in the Microsoft Azure environment.

Read more

Microsoft Azure Business Continuity Technical Guidance (see Storage section)

Performance Guidance for SQL Server in Microsoft Azure Virtual Machines

Configure your network

Virtual machines multi NIC feature in Microsoft Azure lets you create and manage multiple virtual network interface cards (NICs) on your Azure virtual machines (VMs). New-AzureVMConfig should be used while configuring the feature. Microsoft Azure virtual networks provide for private communication amongst servers in the Microsoft Azure environment and/or servers in your on premises environment (via a traditional virtual private network link), separate from public communication with other servers via the Internet.

It is not mandatory to create a virtual network to use Microsoft Azure; you can simply communicate with your Microsoft Azure virtual machines via the public network. However, you must remember that virtual networks cannot be reconfigured after creation. In addition, machines in a virtual network will keep their internal IP (DIP) through reboots and shutdowns. Virtual networks also allow you to group your virtual machines together within a Microsoft Azure datacenter. Therefore, unless you are completely sure that you will not need it, you should consider creating a virtual network for your virtual machines, even if you do not see an immediate need for it.

When you set up a virtual network, you can divide it into one or more subnets. Be sure to allow for expansion. For example, even if you currently need to allow for 32

servers in a network, consider building your subnets with more IP addresses (/26 or /25) to ensure that you do not run out of room and have to rebuild your virtual network.

A Microsoft Azure virtual network is required for virtual machines hosting the AD DS role in Microsoft Azure because the default DNS in Microsoft Azure does not support CNAME and SRV records.

Before you create a Microsoft Azure virtual network, you must first create an Affinity group and a Storage group. Once a virtual network is created, simply deploy the first virtual machine in that virtual network.

Do NOT set static IP addresses in the virtual machines or this will result in loss of connectivity at some later date when the virtual machines move between Microsoft Azure hosts. The dynamically assigned IP address sticks with the virtual machine for the life of the machine. Azure offers the capability to configure reserved IPs onto IAAS VMs. When you reserve an IP address for the Azure VM, it is not entered into the VMs machine's TCP/IP configuration property sheet. Rather a reservation is created, so that DHCP hands out the desired address to the VM. If you look at the VM's NIC, it is still set as a DHCP client, but the DHCP server will honor the reservation that you configured.

Obtain the Host Name and Internal IP Address of the new virtual machine from the Dashboard of the virtual machine in the portal and use these properties to define it as a DNS Server on your virtual network. However, if you are promoting a replica domain controller for an on premises domain, then you must configure a site-to-site VPN on the virtual network and define an on premises DNS server on the virtual network to ensure a successful promotion. Reboot the virtual machine to assign the DNS Server that is defined on the virtual network to it.

Add the AD DS role and promote the server to be a domain controller. If this virtual network does not have the site-to-site connection, you will promote a new isolated forest with the DNS role. After the required reboot for domain controller promotion, RDP to the server and remove the statically defined DNS settings that were set when adding the DNS role.

Read more

Create a Virtual Network for Site-to-Site Cross-Premises Connectivity

Azure multiple network adapter requirements and constraints ✔

Azure allows multiple network adapters. This feature needs few requirements and constraints to be taken care of.
Refer to Read More section for additional information on those requirements.

Read More

Create a VM with multiple NICs

Multiple VM NICs and Network Virtual Appliances in Azure

Create a Multi-NIC VM with a Public IP in Azure

Configure connectivity to on-premises resources ✔

While Microsoft Azure virtual machines can talk amongst themselves via a Microsoft Azure virtual network, you will need to set up VPN tunnel to allow Microsoft Azure virtual machines to talk to on-premises machines.

Read more

Please see About Secure Cross-Premises Connectivity for an overview of the functionality.

Configure domain connectivity in Microsoft Azure ✔

If your Azure machines need to be members of a domain, you can either set up an isolated Active Directory domain in Microsoft Azure, or you can configure a VPN tunnel back to your on-premises domain.

Read more Please see Create a Virtual Network in Azure for a tutorial.

File Services role

The File Services role is completely supported in Microsoft Azure, but you need to ensure that on-premises clients have access to the virtual machine in some fashion.

Suggested actions The File Services role is completely supported in Microsoft Azure, but you need to ensure that on-premises clients have access to the virtual machine in some fashion. If servers exposing file shares are moved to Azure IaaS, a Microsoft Azure VPN tunnel must be created and Active Directory must be accessible to maintain access to those shares.

Read more Azure Site-to-Site VPN

You may want to consider looking at StorSimple. It is an appliance you install in your datacenter that uses cloud storage as its backing store and caches recently and frequently used content locally. This essentially gives a StorSimple device unlimited storage while minimizing access time.

Server AzureLab-DC01.AzureLab.com

Select a network configuration for a high bandwidth/low latency workload

If you are communicating between multiple Microsoft Azure virtual machines, they are all local to each other as long as you don't attempt to do cross-datacenter communications. In this scenario, you should have low latency, high bandwidth communications between machines. If you are communicating between on-

premises machines and Microsoft Azure virtual machines, you have to remember that the traffic is over the internet or a VPN and is thus likely to be much slower and with more retransmits.

Suggested actions You should definitely consider moving your entire workload to Microsoft Azure. If you only move part of it, you might not see the performance you would like due to latency issues.

Static IP address are not allowed in Azure 

IP Addresses cannot be statically configured on guest VMs. Windows Azure "owns" the address pool but will always assign the same address once the computer is provisioned. It is however possible to reserve IP addresses.
With Azure PowerShell, you have the capability to define and configure a specific internal IP address that can be statically assigned to an IaaS Virtual Machine deployed in a Virtual Network. This feature will allow you to directly configure the internal IP address for your Virtual Machine and maintain it even when stopping and starting the Virtual Machine. You can even delete the Virtual Machine and redeploy it months later and keep the same IP address.

Read More Static Internal IP Address for Virtual Machines

Setting Static IP Address in Windows Azure Virtual Machines

Plan for storage

Just like you attach physical hard drives to your on premises servers, you can attach virtual hard drives to your Microsoft Azure-based virtual machines. Each virtual hard drive can be up to 1 TB in size, and you can attach up to 16 virtual hard drives to each Microsoft Azure virtual machine.

Make sure you evaluate your storage from the perspective of what the workload needs and what Microsoft Azure supports, and not just the size of the on premises drives. If your application utilizes large amounts of data, you may want to consider designing your application so that it can spread that data across multiple virtual hard drives, or even multiple servers.

Since you pay for the storage that you use in Microsoft Azure, you will also want to ensure you only use the storage you need.

When deploying the domain controller role on Microsoft Azure virtual machines, the AD DS database, AD DS Logs, and SYSVOL *must* be deployed on Microsoft Azure Data Disks. Operating System disks on Microsoft Azure virtual machines have Write back caching enabled. Just like a physical computer, placing these components on a disk with Write back caching enabled could result in Jet database inconsistencies in the event of a dirty shutdown.

When creating DFSR replicate folder content on Microsoft Azure virtual machines, be sure to place the replicated folder on a Data Disk which has caching disabled (default). Data Disks have Write back cache disabled by default, whereas operating system drives do not.

Read more

Microsoft Azure Storage Pricing Details

DFSR Replication Halted on DC 

The DFSR service stops replication when a DFSR JET database is not shut down cleanly and AutoRecovery is disabled. Any domain controller attempting to replicate Sysvol content from this domain controller will fail. In addition, domain controllers running Windows Server 2008 R2 or later will record event ID 2213 in the DFSR event log when AutoRecovery is disabled.

Read more DFSR Event ID 2213 is logged on Windows Server 2008 R2 and Windows Server 2012

Event ID 4114 and Event ID 4008 are logged in the DFS Replication log in Windows Server 2008 R2

DFSR service is not running ✔

If the DFSR service is not running on the domain controller, review event logs on the domain controller to try and determine why it is stopped, and what error, if any was experienced. Resolve any issues found within the logs and then proceed to restart the service. Promotion of new domain controllers in Windows Azure, or on-premises, will not share out Sysvol if the DFSR service is stopped on direct replication partners.

Read more List of currently available hotfixes for Distributed File System (DFS) technologies in Windows Server 2008 and in Windows Server 2008 R2

Ensure replication of SYSVOL replication partners ✔

Domain controllers replicate data contained in the SYSVOL share using either the FRS or DFSR. Keeping this data consistent across domain controllers in the same domain ensures a predictable group policy and script processing experience for client machines and users.

When using FRS, two domain controllers use a process called a version vector join to perform comparisons of each other's SYSVOL structure. This allows them to determine differences that must be replicated. Domain controllers will report "never joined" for those partners that they have never successfully replicated with or have failed to replicate with for an extended period.

For DFSR replicated SYSVOL, failed replication will be reported in the event log and may be detected by querying the MicrosoftDfs\DfsrConnectionInfo WMI class and

examining the LastErrorCode assigned to replication connections. Any non-zero error code indicates failed replication.

FRS is in Journal Wrap 

File Replication Service (FRS) journal wrap refers to a condition where FRS is no longer able to track changes in the file system for replication. This can occur because too many changes are occurring, changes are occuring too fast, the FRS service has been stopped for too long, or the FRS database is in an invalid state. A domain controller will record event ID 13568 in the FRS event log if it enters a journal wrap state. Domain controllers being promoted in Windows Azure or on premises will not share out Sysvol (GPOs, Scripts) if FRS on their direct replication partner is in a journal wrap state.

Read more Use the BurFlags registry value to reinitialize File Replication Service replica set

Troubleshooting FRS Event 13568

FRS is Stopped or Disabled 

The FRS service is a critical component to a domain controller. It is the mechanism used to replicate the files and folders within the SYSVOL structure to other domain controllers in its domain. You should configure this service to start automatically and in a started state. An exception is when actively troubleshooting an FRS problem that requires the service be temporarily stopped. Inappropriately stopping the service will cause errors and eventually cause a journal wrap condition where FRS is unable to replicate. Domain controllers being promoted in Windows Azure or on premises will not share out Sysvol (GPOs, Scripts) if their direct replication partner has the FRS service stopped.

Make sure you don't currently use restricted drive letters 

If you have a volume that is using either D: or E:, be aware that it will be used in Azure for the pagefile

Suggested actions Build from gallery image and then make sure your workload doesn't have a hard-coded requirement to persist data on the D: or E: drives. Please test to ensure that doesn't negatively impact your workload.

Read more How to create a custom virtual machine

Server AzureLab-DC01.AzureLab.com

Microsoft Azure is currently limited to 64 data disks

Azure only supports 64 data disks currently (+ 1 OS disk), if you have more than that you will not be able to attach all of them to your VM

Read more How to Create a Custom Virtual Machine

SYSVOL, NTDS.DIT and/or NTDS Logs are on %SystemDrive%

In Microsoft Azure, Microsoft recommends that the SYSVOL, NTDS.DIT, and NTDS logs be placed on drives which are not the system drive.

Uploading existing domain controllers that have SYSVOL, NTDS.DIT, or NTDS logs on the system drive into a Microsoft Azure virtual machine could result in JET database inconsistencies at the time of service healing (the virtual machine is moved between Microsoft Azure hosts).

Suggested actions Consider promoting a replica domain controller in Microsoft Azure and place SYSVOL, NTDS.DIT, and NTDS logs on a

Data Disk instead of uploading the on premises domain controller.

If a custom configuration requires the virtual machine be uploaded to Microsoft Azure, consider changing the "Host Cache Preference" to "Read Only" for the operating system drive in the Microsoft Azure Management Portal or by using the Set-AzureDataDisk cmdlet.

Read more

Placement of the Windows Server AD DS database and SYSVOL

Manage Disks and Images

Exploring Microsoft Azure Drives, Disks, and Images

Domain Controller AzureLab-DC01.AzureLab.com

Used volume size may not exceed 1023 GB 

Microsoft Azure volumes are limited to 1023 GB. If you have a volume that is currently using more than 1TB, you will need to split out the data in this volume so it can be moved to Azure

Prepare a disaster recovery plan

Microsoft Azure is well-suited as a substitute to otherwise costly disaster recovery (DR) sites. Hosting a small number of Disaster Recovery domain controllers and a single virtual network on Microsoft Azure eliminates the overhead of maintaining an offsite facility in a different geographic region where there may not be any IT staff.

Disaster Recovery sites should be able to manage all the tasks in a forest/domain in the event all on premises domain controllers are destroyed. Therefore, DR sites should contain one or more writable domain controllers (RWDC) from each domain in the forest and these should have full writable copies of the Active Directory.

Will implement a cloud based Disaster Recovery site for on premises Active Directory

Microsoft Azure is well-suited as a substitute to otherwise costly disaster recovery Disaster Recovery sites. Hosting a small number of Disaster Recovery domain controllers and a single virtual network on Microsoft Azure eliminates the overhead of maintaining an offsite facility in a different geographic region where there may be no IT staff.

Suggested actions

Disaster Recovery sites should be able to manage all the tasks in the forest/domain in the event all on-premises domain controllers are destroyed. For this reason, Disaster Recovery sites should contain one or more writable domain controllers (RWDC) from each domain in the forest and these should have full writable copies of the domain they are domain controllers for.

The Global Catalog role should be added to Disaster Recovery domain controllers if more than one domain exists in the forest. This will enable the Disaster Recovery domain controllers to service authentication requests for on-premises users and computers in the event all on-premises domain controllers in the domain become unavailable.

Read-Only domain controllers (RODC) should not be used in Disaster Recovery sites because they cannot be converted to become RWDCs without being demoted and re-promoted.

It is important to understand the supported limitations of Disaster Recover Sites as well as the security implications

that a custom Active Directory replication schedules could introduce.

Promoting a RWDC in Microsoft Azure is not very different from doing it on-premises. However, some consideration should be given to the region where your azure data is located. Since this is a disaster recovery site you should consider creating an Affinity group that is in a different region of the globe than your datacenter. Next create a storage group and a virtual network that has a site-to-site VPN connection to your on-premises datacenter. Configure the virtual network to have an on-premises DNS Server. Add a VM in that virtual network and promote a RWDC for each domain in your forest and add the GC role.

When promoting the server the AD DS database, logs, and SYSVOL must be deployed on Microsoft Azure Data Disks. Placing these components on the Windows OS Disk is not recommended because Write back caching is enabled on these drives and can result in data inconsistencies after service healing takes place.

Configuration of Site/Subnet topology is crucial:

- Create a Site object specific to the Azure location in Active Directory Sites and Services

- Create a Subnet object for the Microsoft Azure virtual network and link it to the Azure site

- Create an IP Site Link under “Inter-Site Transports” in Active Directory Sites and Services

- In the new IP Site Link add the Azure site and the on-premises site with the fastest link that is the least number of

hops from the on-premises gateway under the "Sites in this site link" field.

- Define a higher Cost value on the new IP Site Link object to represent the more expensive transmission. By default the Cost is 100, so a number higher than 100 would reflect the higher cost. This setting will dissuade KCC from using GCs in the Azure site as a preferred replication route back to on-premises GCs.

If desired, you can increase the replication interval that the Disaster Recovery RWDC will use to contact on-premises domain controllers for updates. Do not set this for a value that is greater than tombstone lifetime. The greater the value the further out of convergence Active Directory will be in the Azure site from the rest of the forest.

You should not modify the replication schedule since the Microsoft Azure virtual network should always be online.

Read more

How Active Directory Replication Topology Works

Configure the Site Link Cost to Establish a Priority for Replication Routing

Disaster Recovery: Active Directory Users and Groups

Differences Between an RODC and a Writable Domain Controller

Windows Server 2008 Domain Controller Options That Are Not Supported on an RODC

Determining the Interval

Global Catalog Server Requirement for User and Computer Logon

Appendix B: Do Not Use a Lag Site as a Disaster Recovery Strategy

Placement of the Windows Server AD DS database and SYSVOL

Manage Disks and Images

Secure your environment

The Microsoft Azure platform environment is composed of computers, operating systems, applications and services, networks, operations and monitoring equipment, and specialized hardware, along with the administrative and operations staff required to run and maintain the services. The environment also includes the physical operations centers that house the services and which themselves must be secured against malicious and accidental damage.

Your organization may not allow you to place replica domain controllers from your on premises Active Directory on virtual machine hosts which are not under the direct control of your organization. Here are some options that you can choose from:

- **Isolated Forest.** Promote a new isolated forest in Microsoft Azure by using a Microsoft Azure virtual network that does not have site-to-site VPN connectivity back to your corporate network. This configuration is completely segmented from your on premises Active Directory and allows you to run applications such as SharePoint which require Active Directory.
- **Trusts:** Some organizations may not permit placing domain controllers for the on premises Active Directory in Microsoft Azure. You can retain isolation and still provide authentication from on premises accounts over a forest or domain

trust by using a Microsoft Azure virtual network which has a site-to-site IPsec VPN tunnel to your on premises network.

Once your Microsoft Azure virtual network has a connection back to the corporate network, you can promote a new forest in Microsoft Azure and establish the trust. Establishing a forest or domain trust back to one or more on premises forests will generate billable egress traffic each time a trusted account authenticates against on premises trusted domains.

To keep egress traffic down and improve authentication performance, it is best to promote replica domain controllers to virtual machines running in Microsoft Azure for your on premises Active Directory. If these domain controllers run in a separate forest, you should mirror the site and subnet for your Microsoft Azure subnet in both the on premises Active Directory and the forest running in Microsoft Azure so that clients can discover these domain controllers and get site-aware DFS referrals, as needed.

Key information

- The endpoint of your machine is accessible by all. Protect it!

Read more

- Microsoft Azure Trust Center

Allow RDP or remote PowerShell through your firewall 

Microsoft Azure does not currently provide console level access to the virtual machines. This means that you need to access and configure the machine with a combination of remote PowerShell and remoting into the virtual machine. If you don't have either enabled in Microsoft Azure, you won't be able to access your virtual machines.

Suggested actions You will need to enable remote PowerShell and/or RDP prior to migrating your workload to Microsoft Azure.

Remote Desktop must be enabled on Microsoft Azure virtual machines ✔

Console access is not enabled to Microsoft Azure Virtual Machines. In order to connect to Virtual machine you need to have Remote Desktop services (or other remote connection utility) enabled. In addition, for security purposes, RDP it is recommended that RDP be mapped to an endpoint that isn't 3389.

Read more Enable Remote Desktop

RODC Filtered Attribute Set (FAS) Defined in a forest with Windows Server 2003 domain controllers ✔

Traditionally RODCs are used in unsecure branch sites because sensitive data will not replicate to RODCs. In Microsoft Azure, you may deploy RODCs to primarily reduce egress network traffic over a Microsoft Azure virtual network, rather than for security reasons. If RODCs are deployed for security reasons and Windows Server 2003 domain controllers exist in the forest, then it is important to define RODC filtered attribute set (FAS).

The RODC filtered attribute set (FAS) is a dynamic set of attributes that are not replicated to any RODCs in the forest because they contain sensitive data. Therefore, a malicious user who has managed to compromise an RODC cannot expose these attributes. Applications that use AD DS as a data store may contain sensitive information (such as passwords, credentials, or encryption keys) that should not be stored on an RODC in case the RODC is stolen or compromised. The FAS can be extended (customized) to include any other attributes that you want to prevent from replicating to any RODC in the forest. If an RODC tries to replicate attribute in the FAS from a domain controller running Windows Server 2008 or later, the replication request is denied. However, if the RODC tries to replicate those attributes from a Windows Server 2003 domain controller, the replication request could succeed.

Read more RODC Filtered Attribute Set, Credential Caching, and the Authentication Process with an RODC

Ensure a healthy environment

Before migrating your on premises environment to Microsoft Azure, you should ensure that the environment is healthy and configured optimally. Any issues listed below may affect the current reliability or efficiency of your on premises environment. Please review them carefully, and consider addressing them before making the move to Microsoft Azure.

Automatic Updates Service need to be configured to run

Although the service may not need to be running when a 3rd party update application is used by stopping certain methods to track the installation of updates is lost. For example, the Microsoft Security Baseline Analyzer (MBSA) requires the service to be running in order to reliably scan a computer

Suggested actions Enable the Automatic Updates service and ensure it is set to start automatically.

Read more Azure Host OS Updates

Server AzureLab-DC01.AzureLab.com

Check inbound replication connection objects for naming contexts on domain controller

When a domain controller is missing an inbound replication connection object for one or more naming contexts, it means:

• This is the only domain controller replicating those naming contexts, which indicates a single point of failure for that naming context. In this scenario, consider adding additional replicas for redundancy.

OR

• The domain controller is failing to replicate changes for those naming contexts from its replication partners. In this scenario, you must further investigate the replication topology and replication failures.

Check outbound replication connection objects for naming contexts 

When a domain controller is missing an outbound replication connection object for one or more naming contexts, it means:

• This is the only domain controller replicating those naming contexts, which indicates a single point of failure for that naming context. In this scenario, consider adding additional replicas for redundancy.

OR

• The domain controller is failing to replicate changes for those naming contexts from its replication partners. In this scenario, you must further investigate the topology and replication failures.

Check the inbound replication links for naming contexts on a GC 

When a global catalog server (GC) is missing an inbound replication link for one or more naming contexts, it means:

1. This is the only GC replicating those naming contexts, which indicates a single point of failure for that naming context. In this scenario, consider adding additional replicas for redundancy.

2. That topology problems for those naming contexts from its replication partners exist preventing replication. In this scenario, you must further investigate the topology and replication failures.

Check to ensure any applications installed support Microsoft Azure ✓

Any application that runs on Windows or Linux should run just fine on a Microsoft Azure virtual machine. However, not every application vendor (including Microsoft) certifies every application to run on Microsoft Azure.

Configure valid DNS servers ✓

Incorrect DNS client configurations can lead to several issues within Active Directory. Therefore, you must ensure that all domain controllers are configured with valid DNS servers. Domain controllers running as Windows Azure virtual machines require a Windows Azure virtual network for their dynamically assigned IP and DNS server settings, while on premises domain controllers require static settings.

Read more Configure the DNS Client Settings of the First and Subsequent Domain Controllers.

Domain controller doesn't know all FSMO roles ✓

The DCDiag test returns the domain controller's knowledge of the five Flexible Single Master Operation (FSMO) roles. DCPROMO promotion will fail to install a writable domain controller if the RID FSMO role holder is not reachable

Domain in Windows 2000 Mixed Mode

Microsoft Azure currently supports Windows Server 2008 R2 and later operating systems. At least one domain in the forest is at Windows 2000 Native Domain Lunctional Level which means the Forest Functional Level is also Windows 2000. The minimum supported Domain and Forest Functional Level required to promote a Windows Server 2008 R2 or above domain controller is Windows Server 2003.

Read more

Understanding Domain and Forest Functional Levels

How to raise Active Directory domain and forest functional levels

DSA Not Writable value set to non-zero value

This issue requires immediate action! The DSA Not Writable flag being set typically means that the domain controller has experienced a USN rollback. KB875495 describes how to detect and recover from a USN rollback. However, this flag can also get set for other issues as described below. The domain controller will not honor originating writes until you perform the recovery steps listed in the KB.

Read more

How to detect and recover from a USN rollback in Windows Server 2003, Windows Server 2008, and Windows Server 2008 R2

Troubleshooting AD Replication error 8456 or 8457: "The source | destination server is currently rejecting replication requests"

Enable the Connection Translation option

Disabling the Connection Translation option will prevent the Knowledge Consistency Checker (KCC) from translating connections objects to replication links.

As a result, this will prevent the KCC from performing tasks such as creating new or cleaning up old connection objects.

Fix missing SPN registrations on domain controllers ✔

Domain controllers that are missing Service Principal Names (SPN) may lead to domain controller promotion failures with the "Target Account Name is incorrect" error.

Read more "Verify a Domain Computer Account"

Forest Zone has Dynamic Updates Disabled ✔

Microsoft DNS supports dynamic updates on standard primary and Active Directory-integrated zones. Although dynamic updates are not technically required by Active Directory, the feature is essentially a de facto requirement due to the tremendous administrative overhead in trying to manually create and maintain all of the DNS records required for Active Directory to function properly. Attempting to manually maintain the records is very prone to human error and is almost guaranteed to cause issues due to missing or incorrect records. The term "forest zones" refers to zones that contain records for an Active Directory domain within the forest. Promotion of a domain controller, on premises or in Windows Azure, will fail if the server being promoted cannot locate the DNS SRV or CNAME records for the source domain controller.

Read more Enable dynamic updates

How to Enable Dynamic Updates on UNIX BIND DNS Servers

Inbound Replication Disabled ✔

Active Directory replication is based on domain controllers pulling changes from other domain controllers. By default, Read-Write domain controllers allow both inbound and outbound replication while Read-only domain controllers only perform inbound replication. domain controllers that have inbound replication disabled will not learn of new domain controllers being promoted into the forest which will result in authentication failures and replication failures.

Microsoft Azure Virtual Machines are regularly updated via Windows Update ✓

The Automatic Updates service is primarily used to allow a computer to receive updates for the Windows operating system and certain Microsoft products. These updates can be downloaded from the Windows Update or Microsoft Update websites, a Windows Server Updates Services (WSUS) server, or SMS. 3rd party update deployment products may also interface with the Automatic Updates service.
If you disable the service by configuration you will need ensure the server is updated through other mechanisms.

Read more Azure Host OS Updates

NC failed to replicate past half of tombstone lifetime ✓

A domain controller has failed to replicate a naming context for greater than half the tombstone lifetime interval. If the domain controller continues to fail and exceeds the tombstone lifetime interval, it will have to be forcibly demoted and promoted again, or rebuilt.

NC failed to replicate past tombstone lifetime ✓

A domain controller has failed to replicate a naming context for greater than the tombstone lifetime interval. After a domain controller fails to replicate for greater

than the tombstone lifetime interval, it should never be allowed to replicate. For example, if a domain controller is encountered that was turned off or unable to communicate with the rest of the forest for whatever reason, that domain controller should remain in a non-communicating state. If the domain controller is allowed to communicate with other domain controllers, it can restore previously deleted objects. This can cause critical problems in the infrastructure.

Netlogon service is stopped or does not start automatically 

The Netlogon service on a domain controller performs multiple functions, including servicing network logon requests, dynamic DNS registration of SRV and GUID CNAME records, and automatic site coverage. The service should normally be started. Promotion of a domain controller, on premises or in Windows Azure, will fail if the only accessible source domain controller has its Netlogon service stopped.

No Global Catalogs in Site 

In a Windows 2000 native mode or later environment, a global catalog is required to service every authentication attempt. This is because Universal groups throughout a forest are only stored on global catalogs. In order to verify whether a user has access to a resource, all its groups must be evaluated. This is why the global catalog requirement exists. If a site has a domain controller that is not a global catalog, that domain controller must maintain a secure channel to a remote global catalog in order to service authentication requests. This can result in a complete service outage if the WAN link fails, because the domain controller will no longer be able to service authentications. In addition, Windows Azure sites with site-to-site VPN connections to an on premises domain should have a GC (or Universal Group Membership Caching (UGC) enabled) in the Windows Azure site. Otherwise, all authentication requests will generate egress network traffic back to on premises GCs. The on premises site that is in a sSite Llink with the Windows Azure site should have a GC to facilitate the GC role being added to domain controllers, or to service authentication if Universal Group Caching is enabled in the Windows Azure site.

Read more Enable or disable a global catalog

Enable Universal Group Membership Caching in a Site

Plan Global Catalog Servers

No site links found

Site links are leveraged by domain controllers and certain services to control actions such as replication flow, automatic site coverage, DFS referrals, Exchange mail flow, group membership caching, and so on. By default, each new forest has a site link named DEFAULTIPSITELINK. You can modify or even delete this site link, as necessary. However, in any forest that has two or more sites, at least one site link should exist to interconnect the sites. A failure to do so can impact any of the processes previously mentioned.

In Microsoft Azure, egress traffic back to the on premises network is billable. Therefore, you should define a higher Cost value on IP Site Links that link Microsoft Azure sites to their nearest on premises sites. This is especially important when Read-Write domain controllers (RWDCs) exist in a Microsoft Azure site that has a site-to-site connection with on premises domain controllers.Setting a numeric value for Cost on a Microsoft Azure Site Link that is higher than other Site Links reflects a more expensive transmission cost. This dissuades KCC from building replication links from Microsoft Azure domain controllers back to on premises GCs when more optimal on premises domain controllers exist.

Read more Understanding Sites, Subnets, and Site Links

Outbound replication disabled

Active Directory replication is based on domain controllers pulling changes from other domain controllers. By default, Read-Write domain controllers allow both inbound and outbound replication while Read-Only domain controllers only perform inbound replication. Domain controllers that have outbound replication disabled will prevent new domain controllers from being promoted into the domain.

Preferred bridgehead excluding a naming context ✔

Bridgehead servers are domain controllers that have inbound replication partners in other sites. By default, the selection of bridgeheads is automatic. Manually defining preferred bridgeheads is generally not recommended, because it incurs additional administrative overhead, can reduce the inherent redundancy of Active Directory, and can easily result in replication failures due to invalid configurations. Defining preferred bridgeheads that do not include all required naming contexts is also an invalid configuration that can result in replication failures. This is especially true if Bridge All Site Links (BASL) is disabled. In this case, domain controllers or global catalog servers are unable to fully replicate all their naming contexts. Promotion of domain controllers, or addition of the GC role, in Windows Azure and on premises could fail if Active Directory content is sourced from a manually defined bridgehead in this state.

Read more Determine Whether a Server is a Preferred Bridgehead Server

How Active Directory Replication Topology Works

Resolve host/glue registrations ✔

DNS Records checks every DNS server that hosts the _msdcs.<forestrootname> zone. It verifies that the DNS servers contain the GUID CNAME record of every domain controller in the forest, which can be resolved to their associated glue records. Glue records are the host (A) records of each domain controller.

Read more Fixing Replication DNS Lookup Problems (Event IDs 1925, 2087, 2088)

Schema has not been extended to support Windows Server 2008 R2 or higher

Microsoft Azure supports virtual machines running Windows Server 2008 R2 or higher. To support Windows Server 2008 R2 or later, you need to extend your Active Directory schema.

Read more Adprep.exe integration

Manage Disks and Images

Add a data disk to a new virtual machine

Set the Kerberos KDC service to start automatically

The Kerberos Key Distribution Center (KDC) service is a core component to the Kerberos infrastructure. Every Active Directory domain controller acts as a KDC to service Kerberos authentication requests. Stopping the service prevents a domain controller from servicing Kerberos authentications. Promotion of a new domain controller may fail if the KDC service on the only source domain controller that is reachable on the network is stopped.

Set the Server service to start automatically

The Server service is a component of the file and printer sharing features of a Windows computer. Domain controllers rely upon the Server service to allow clients to connect to the SYSVOL and Netlogon shares. The service should normally be started.

The Netlogon service requires the Server service to be running. Promotion of a domain controller, on-premises or in Microsoft Azure, will fail if the only accessible source domain controller has its Netlogon service stopped.

Set the Workstation service to start automatically ✓

The Workstation service is used to allow a computer to establish connections to another computer's Server service. This includes operations such as mapping a network drive or certain remote administrative tasks. The service should normally be started.

Windows Time service stopped or does not start automatically ✓

The Windows Time service is the default mechanism used to maintain time synchronization. The service should only be stopped if another service or functionality is used to ensure consistent time.

Optimize your configuration

Certain configuration optimizations are not as important for an on premises environment, but are much more important once you migrate to Microsoft Azure. For example, most on premises servers are configured to use the time zone of their physical location. This makes sense because physical servers rarely move locations and tend to be managed by local resources. In contrast, Microsoft Azure is a global service. To ensure that applications behave the same way regardless of their physical location, it is important for Microsoft Azure to have a consistent time zone across all geographies. UTC is a natural choice given the global customer base, and UTC is not subject to Daylight Saving Time (and the associated risk of bugs).

If you build a new virtual machine by using the Microsoft Azure image gallery, these configuration optimizations are set properly on your behalf, but if you plan to upload a virtual machine directly from your on premises environment, you will need

to explicitly configure them to be in line with recommendations for an Azure-based environment.

Even though you may create a secure site-to-site VPN connection, without name resolution, communication by hostname is not possible. There are multiple ways to provide name resolution for your Microsoft Azure Virtual Network. You can use the name resolution provided by Microsoft Azure, or you may use your own DNS server. Configuring your virtual network to use Microsoft Azure-provided name resolution is a relatively simple option. However, it does not meet the advanced name resolution needs of Windows Server AD DS. For example, it does not support dynamic SRV records, and so on. Name resolution is a critical configuration item for DCs and domain-joined clients. DCs must be capable of registering resource records and resolving other DC's resource records.

For fault tolerance and performance reasons, it is optimal to install the Windows Server DNS service on the DCs running on Microsoft Azure.

Your choice of a name resolution method should be based on one of the following scenario that it may support.

- Cross-premises: Name resolution between role instances or virtual machines in Microsoft Azure and on-premises computers
- Cross-premises: Name resolution between on-premises computers and role instances or virtual machines in Microsoft Azure
- Name resolution between role instances located in the same cloud service
- Name resolution between virtual machines located in the same cloud service
- Name resolution between virtual machines and role instances located in the same Virtual Network, but different cloud services
- Name resolution between virtual machines and role instances that are located in the same cloud services, not in a Microsoft Azure Virtual Network
- Name resolution between role instances located in different cloud services, not in a Microsoft Azure Virtual Network
- Name resolution between virtual machines located in the same Microsoft Azure Virtual Network
- Use name resolution to direct traffic between datacenters
- Control the distribution of user traffic to Microsoft Azure hosted services

Key information

- Disable any interactive boot policies prior to migrating a virtual machine to Azure. Otherwise, your virtual machine will be inaccessible in Azure and you will need to re-create it without an interactive boot policy.
- You should configure Azure virtual machines to utilize the UTC time zone and the RealtimeIsUniversal option in order to minimize the risk of time zone issues.
- Use only *Microsoft Azure Virtual* Machines for domain controllers (as opposed to Microsoft Azure "web" or "worker" role virtual machines). These machines are durable, which is must for a domain controller. Microsoft Azure Virtual Machines are designed for a domain controller workload.
- Configure subnets, sites, and site links (at appropriate costs) with Microsoft Azure Virtual Network to optimize traffic and minimize cost.
- The Windows Server AD DS database, logs, and SYSVOL must be deployed on Microsoft Azure Data Disks. *Data Disks* and *Operating System Disks* are two distinct virtual-disk drive types for Microsoft Azure. As a best practice for virtual domain controllers, store the database, logs, and SYSVOL on either the same data disk or separate data disks.
- On premises static IP addresses are assigned within the operating system to a specific NIC. Dynamic addresses are leased automatically from DHCP servers according to the scopes defined on the DHCP server.

  A third conceptual type of address is introduced by Microsoft Azure virtual networks and differs only slightly from DHCP address allocation. With Microsoft Azure virtual machines, the virtual machine must be configured to lease an IP address from DHCP. Unlike typical dynamic addresses, however, which may alter when a lease expires, the dynamic addresses on Microsoft Azure virtual networks are guaranteed.

  Microsoft recommends using a Microsoft Azure virtual network for IP address consistency because statically-assigned addresses are not supported. Configuring a static IP address within the virtual machine will eventually result in complete loss of

connectivity to it. Azure offers the capability to configure reserved IPs onto IAAS VMs.

- For name resolution, deploy your own (or leverage your existing) DNS server infrastructure; Microsoft Azure-provided DNS does not meet the advanced name resolution needs of Windows Server AD DS. For fault tolerance and performance reasons, it is optimal to install the Windows Server DNS service on the domain controllers running on Microsoft Azure.
- Avoid using the Microsoft Azure domain controllers for Active Directory administrative tasks. You will incur egress traffic costs due to the outbound replication traffic to on premises domain controllers

Read more

Moving to Coordinated Universal Time (UTC)
Windows Server Active Directory site topology
Placement of Windows Server AD DS database and Sysvol
Guidelines for Deploying Windows Server Active Directory on Microsoft Azure Virtual Machines
IP Addressing and DNS
Microsoft Azure Pricing at a glance
Microsoft Azure Name Resolution

Deploy an existing VHD to Azure with Time service set to autostart 

When you provision your VM from a gallery image, a number of custom operations are run to ensure smooth operations in Azure. You need to ensure these operations are also done manually if you use existing VHDs. Normally, setting the Windows Time service to autostart is done automatically as part of the provisioning process. If you are going to upload existing VHDs that do not currently have the Windows Time service set to autostart, be sure to modify the service start configuration prior to uploading your VHD.

Read more Creating and Uploading a Virtual Hard Disk that Contains the Windows Server Operating System

Registry entry RealtimeIsUniversal must be set ✔

When RealtimeisUniversal is not set, the virtual machine will attempt to sync its clock with the fabric host. In the absence of this value, the VM will attempt to sync its clock with the fabric host when it should use UTC (or timezone independent). You should set this value if you don't want to use the fabric host.

Read more

RealTimeIsUniversal is used to indicate if the CMOS clock is configured by using the local date/time (default) or UTC.

0 indicates that the CMOS clock is configured for local date/time.

1 indicates that the CMOS clock is configured by using UTC.

Server time zone needs to be UTC ✔

Azure VMs time zones are set to UTC, so your application may not behave the same way as it does with a different time zone.

Watch out for boot policies that prompt the user for input ✔

You won't have access to the console of a virtual machine running in Microsoft Azure. If there is a misconfiguration the boot policy should not wait for the user to take action because this will result in a hung Azure VM.

Read more Azure Business Continuity Technical Guidance

Server AzureLab-DC01.AzureLab.com

Move

Get a subscription

If you do not already have an Azure subscription, getting one is easy. Whether you are just learning the platform around or running a production deployment, there are many options available for creating an account.

- *Free Trial*. Microsoft Azure offers a free trial to everyone. You can sign up here:

  http://azure.microsoft.com/en-us/pricing/free-trial/

- *MSDN Subscription*. As an MSDN subscriber, you are entitled to free Azure credits. You can activate your account here:

  http://azure.microsoft.com/en-us/pricing/member-offers/msdn-benefits/

- *Purchase*. From pay as you go to monthly subscriptions, there are flexible options available for all. You can choose your package here:

  http://azure.microsoft.com/en-us/pricing/purchase-options/

Optimize for a geographically-limited user base

Microsoft Azure has data centers around the world and you can deploy your workload to any or all of them.

Suggested actions You should pick the datacenter that is closest geographically to your user base and deploy your application there.

Read more Virtual Machines Pricing Details (see Geographic Availability section)

Microsoft Azure Speed Test

Provision your virtual machine

Virtual machines deliver on-demand, scalable compute infrastructure when you need to quickly provision resources to meet your growing business needs. With virtual machines, you get the choice of Windows Server and Linux operating systems in multiple configurations on top of the trustworthy Microsoft Azure foundation.

In order to provision a virtual machine, simply choose your compute configuration (standard or high memory instances) and choose an image from the Microsoft Azure image gallery. In the gallery, you can either choose an existing template provided by Microsoft or you can select an image uploaded by you.

Using virtual machines enables you to move virtual hard disks (VHDs) back and forth between on premises and the cloud.

Creating a domain controller by using base images from the Microsoft Azure image gallery:

1. Create a Microsoft Azure virtual network as follows:
    a. If you are promoting the first domain controller, proceed to the next step.
    b. If you are promoting a replica domain controller for an existing domain in the Azure subscription or the on premises network, be sure to define a DNS server on the Microsoft Azure virtual network that has SRV records for the existing domain.
2. Create a virtual machine from the Microsoft Azure image gallery and attach an empty Data Disk with caching disabled (default).
3. Do *not* define Static IP or DNS settings in the virtual machine. Configure the reserved IP address for VM using Azure PowerShell.
4. In the virtual machine, mount the drive in Disk Management and format the volume as NTFS.
5. Add the AD DS role and promote the domain controller.
6. Ensure that SYSVOL, Active Directory Database, and Logs are on the Data Disk.

7. If the StopReplicationOnAutoRecovery value is present in the registry, ensure that it is set to zero to allow auto recovery of DFSR to take place, if needed. If the domain controllers are Windows Server 2008 R2, ensure that Microsoft KB 2780453 is installed first.
8. Once the newly promoted domain controller finishes rebooting, remove any Static DNS Server settings from the IP Properties of the network adapter that get added during the installation of the DNS Server role.

Uploading Existing On-Premises Hyper-V DCs Using Microsoft Azure PowerShell:

See "How to upload existing on-premises Hyper-V domain controllers to Azure by using Azure PowerShell"
http://support.microsoft.com/kb/2904015

Read more

Create a Virtual Machine Running Windows Server

DFSR Event ID 2213 is logged on Windows Server 2008 R2 and Windows Server 2012

Make sure you don't have unattend.xml configured ✔

Microsoft Azure virtual machines leverage the sysprep process. Having a custom unattend.xml can prevent your OS from being provisioned or starting up.

Read more Using answer files in Windows to automate setup

Server AzureLab-DC01.AzureLab.com

Move your data

Promoting domain controllers on Microsoft Azure virtual machines is essentially the same as doing it on premises. However, promoting a domain controller that uses a Microsoft Azure virtual network which has a site-to-site VPN connectivity back to the corporate network has egress network traffic costs which are typically not present in an on premises deployment.

Therefore, it is essential to properly configure the Active Directory replication topology if your Microsoft Azure virtual network has a site-to-site connection with your on premises Active Directory.

Monitor your environment

Although reboots are minimized in a Microsoft Azure environment as much as possible, they still do occur occasionally. While Microsoft Azure does guarantee that your virtual machine will come back up, you need to ensure that your application can handle unexpected reboots.

Expect to restart for host updates - It's been 30 days since the last reboot 

VMs running in Microsoft Azure will generally reboot at least once a month as the host computers apply security updates.

Read more Manage the Availability of Virtual Machines

Get support

Microsoft Azure offers a variety of support options, ranging from self-help via community forums to Premier support that offers the fastest response times and the highest level of contact with Microsoft support representatives who can assist you

with all your questions and issues regarding Azure. Carefully review the available support plans and choose the one that best meets the needs of your business.

Key information

- All Microsoft Azure subscriptions include free access to billing and subscription management, community forums, and the service dashboard.
- Microsoft Azure support plans start at just $29 per year and provide a higher level of service.

Read more

Microsoft Azure Support