



Ready



Set



Move

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



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 things 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 virtual machines.

Move - Do you have a Microsoft Azure subscription yet? Need help provisioning your virtual machine or moving your data? Is your virtual machine healthy? Do you need to monitor your new virtual machine? How do you get support once you've moved your machine? This section addresses these common questions and makes moving your machine a snap.



MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

© 2013 Microsoft Corporation. All rights reserved. Any use or distribution of these materials without express authorization of Microsoft Corporation is strictly prohibited.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, our provision of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The descriptions of other companies' products in this document, if any, are provided only as a convenience to you. Any such references should not be considered an endorsement or support by Microsoft. Microsoft cannot guarantee their accuracy and the products may change over time.

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**

Do you have a server that is underutilized most of the time but must be able handle the occasional spike in load? Do you want to run effective load tests but find that you are constrained by the amount of hardware that you can buy and configure? Have you ever waited days or weeks to procure new hardware for a simple development environment?

If so, you can benefit from Microsoft Azure Infrastructure as a Service (IaaS).

Microsoft Azure IaaS provides on-demand infrastructure that scales and adapts to your changing business needs.

To understand better, consider the following scenarios:

- *Do you need extra capacity to handle a spike in load on Monday morning, during the first week of school, or during the holiday shopping season?* Simply spin up some new virtual machines in Azure, tear them down once you are done, and pay for only what you use.
- *Do you want to do some load testing?* Create extra Microsoft Azure servers to generate and handle the load.
- *Do you need a simple development environment?* Upload a VM from your on premises environment, or use one from the Azure image gallery – even one that has other software pre-installed, such as Microsoft SQL Server or SharePoint Server. You can be up and running in minutes. When you're done developing your applications, you can decommission the environment or put it into production.

Azure IaaS gives you all the power and flexibility that you need to run your business optimally.

Key information

- Bring your own virtual machine from your on-premises environment or build a new one from the Azure image gallery.
- Quickly set up or tear down 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](#)

Moving a development or test environment

Windows 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 Windows Azure SLAs. 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 [Windows Azure Business Continuity Technical Guidance](#)
[Service Level Agreements](#)

Choose your scenario

From virtualizing and uploading an existing physical server to building an entirely new VM from the Microsoft Azure image gallery, there are lots of ways to go to the cloud. This section will explain the benefits and drawbacks of the various migration options and help you find the one that works best for your scenario.

- You can build a new VM from the 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

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 CSUUpload.

Read more

[CSUUpload](#)

[Convert-VHD](#)

Move workloads virtualized in VMWare to Microsoft Azure

This workload is running in VMWare.

Read more

[CSUupload](#)

[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](#)

Select appropriate gallery image



When they make sense, gallery images are a great way to make sure you use the latest and greatest versions of the Microsoft products supported in Windows Azure. You will need to install your custom software, but you can be assured that the default settings for the image are optimized for Windows Azure.

Read more [Create a Virtual Machine Running Windows Server](#)

Virtualized in Azure



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

Server AZURELAB-SQLSVR

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.

The simplest approach is to just leverage endpoint ACLs and local accounts to manage all of your authentication as described in the following reference:

<http://msdn.microsoft.com/en-us/library/windowsazure/dn376543.aspx>

In this configuration, you do not need any domain controllers in your Azure environment. You simply utilize the same usernames and passwords on all of your Azure VMs.

If you do find that you need domain authentication, you have a couple of options:

1. You can join your Microsoft Azure network to your on-premises domain via a virtual private network (VPN). This will require coordination with your on-premises Active Directory administrator, but is the best option if you want users to be able to authenticate using their current domain credentials.
2. You can build and configure a new remote domain controller in Azure. The resulting domain will be entirely disconnected from your on-premises domain.
3. You can leverage the single sign-on (SSO) capabilities of Microsoft Azure Active Directory.

Review unsupported roles and features

Microsoft supports several products running in Azure Virtual Machines as well as many of the roles and features of Windows as documented in [Microsoft server](#)

[software support for Windows Azure Virtual Machines](#). Most of the core Windows roles and features are fully supported in Windows Virtual Machines, but not every role or feature is supported in Microsoft Azure. Some of them don't have an Azure equivalent, but many roles and features can be implemented using Microsoft Azure features. For example, the Windows Network Load Balancing feature is not supported, instead you can use Azure Virtual Networks to enable similar functionality. To learn more, refer to [Load Balancing Virtual Machines](#). When using the Virtual Machines 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 supported roles and features 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 Azure Virtual Machines.

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.
- Gallery images are available for use.

Configure workloads to use Azure load balancing



When virtual machines run in Microsoft Azure and are added to a cloud services they should take advantage of the native load balancing features of Azure by being part of load balanced sets

Read more

[Microsoft server software support for Microsoft Azure Virtual Machines](#)

If you want to implement load balancing of an endpoint, see <http://www.windowsazure.com/en->

[us/manage/windows/common-tasks/how-to-load-balance-virtual-machines/](https://msdn.microsoft.com/en-us/magazine/ff872379.aspx).

If you are currently using a server in a load balanced role, you should consider evaluating if your application can be migrated to a Cloud Service. This would give you unlimited scalability that can be manually or automatically triggered.

<http://msdn.microsoft.com/en-us/magazine/ff872379.aspx>

<http://msdn.microsoft.com/en-us/library/windowsazure/jj156147.aspx>

Server

AZURELAB-SQLSVR

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-SQLSVR

Reconfigure existing failover clusters



Windows Server Failover Clustering isn't supported in Microsoft Azure

Read more

[Microsoft server software support for Microsoft Azure Virtual Machines](#)

[Manage the Availability of Virtual Machines](#)

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 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/en-us/library/windowsazure/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's 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, i.e. adding more resources to your existing machine. 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

- Azure supports between 768 MB and 448 GB of RAM, and up to 32 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.

Choose a virtual machine size matched to your workload (physical memory)

Microsoft Azure virtual machines are limited to 448 GB of RAM with an G5 virtual machine size. If SQL Server is using near 448 GB of RAM or more, you will not be able to migrate to a Microsoft Azure virtual machine without experiencing a decrease in performance. To migrate to Microsoft Azure VMs, you will need to either reduce the memory requirement of your workload or re-architect the solution to scale out across multiple Microsoft Azure virtual machines.

Read more

[Server Memory Server Configuration Options](#)

[Monitor and Tune for Performance](#)

[Virtual Machine and Cloud Service Sizes for Microsoft Azure](#)

[Performance Considerations for SQL Server in Microsoft Azure Virtual Machines](#)

[Performance Guidance for SQL Server in Microsoft Azure Virtual Machines](#)

Choose the best virtual machine size for your workload (CPU)

Microsoft Azure virtual machines support up to 32 logical processors with an extra-large or G5 virtual machine size. If SQL Server is fully utilizing more than 32 logical processors, you will not be able to migrate to the Windows Azure virtual machine without experiencing a decrease in performance. To migrate to Microsoft Azure virtual machines, you will need to either reduce the CPU consumption of your workload or re-architect the solution to scale out across multiple Microsoft Azure virtual machines.


Read more

[Monitor and Tune for Performance](#)

[Virtual Machine and Cloud Service Sizes for Microsoft Azure](#)

[Performance Considerations for SQL Server in Microsoft Azure Virtual Machines](#)

[Performance Guidance for SQL Server in Microsoft Azure Virtual Machines](#)

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



Windows 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. Windows 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 Windows 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 Windows Azure environment.

Read more [Windows Azure Business Continuity Technical Guidance](#) (see Storage section)

[Performance Guidance for SQL Server in Windows Azure Virtual Machines](#)

Configure your network

Virtual machines in Azure are limited to a single network interface card (NIC). Azure virtual networks provide for private communication amongst servers in the 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 Azure; you can simply communicate with your 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 an Azure data center. Therefore, unless you are completely sure you 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.

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 Applications and Firewalls to Allow TCP/IP Traffic

If you require external access to SQL Server running in a Microsoft Azure VM, you will need to enable the TCP/IP network protocol.

Read more

[Enable TCP/IP Network Protocol for SQL Server](#)

[Virtual Network FAQ](#)

[How to Set Up Communication with a Virtual Machine](#)

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.

Configure SQL Server to accept incoming connections



In Microsoft Azure virtual networking, Microsoft Azure assigns an IP address dynamically by using DHCP from a subnet that you specify. You cannot specify a static IP address. Microsoft Azure virtual machines are limited to one IP address each. The IP address is assigned to the virtual machine until it is stopped or de-allocated.

Accessing Microsoft Azure virtual machines from outside the same cloud service or virtual network requires an endpoint to be created in the Microsoft Azure portal.

Read more

[Configure a Server to Listen on a Specific TCP Port \(SQL Server Configuration Manager\)](#)

[How to Set Up Communication with a Virtual Machine](#)

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.

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.

If possible, design and plan to continue using Windows Authentication with Kerberos for the most secure environment in Windows Azure

Windows Authentication in SQL Server supports both Kerberos and NTLM and is more secure than SQL Server Authentication. In order to support Windows Authentication, SQL Server must have access to a domain controller in the domain where the security principal is a member.

Read more

[Choose an Authentication Mode](#)

[Recommendations and Guidelines on Configuring the Authentication Mode for SQL Server](#)

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

If you are communicating between multiple Windows 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 Windows 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 Windows 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

When planning to run SQL Server in Azure virtual machines, Microsoft recommends that you continue using the same database performance tuning options that are applicable to SQL Server in an on premises server environment. However, the performance of a relational database in a public cloud depends on several other factors such as the size of the virtual machine and the configuration of the data disks.

When you create a Azure virtual machine, the platform will attach at least one disk to the virtual machine for your operating system disk. This disk is a VHD stored as a page blob in storage. You can also attach additional disks to your virtual machine as data disks, and these will be stored in storage as page blobs. There is another disk present in Azure virtual machines called the temporary disk. This disk exists on the node that can be used for scratch space.

Operating system disk: An operating system disk is a VHD that you can boot and mount as a running version of an operating system and is labeled as the C: drive.

- **Data files:** The operating system disk has a limit of 1023 GB. Avoid using operating system or temporary disks for database storage or logging.
- **Caching:** By default, the operating system disk is configured with both read and write caching. If you place the database files on the operating system disk, Microsoft recommends that you disable write caching once the virtual machine has been provisioned. For instructions on configuring disk caching, refer to [Set-AzureOSDisk](#), [Set-AzureDataDisk](#) and [Managing Virtual Machines with the Windows Azure PowerShell Cmdlets](#).

Temporary disk: The temporary storage drive, labeled as the D: drive, is not persisted and is not saved in the Azure Blob storage. It is primarily used for the page file and its performance is not guaranteed to be predictable. Management tasks such as a change to the virtual machine size resets the D: drive. In addition, Azure erases the data on the temporary storage drive when a virtual machine fails over. Microsoft does not recommend using the D: drive for storing any user or system database files, including tempdb.

Data disk: Data disks in Azure virtual machines are limited to 1 TB in size. In order to migrate a database that is larger than 1 TB to SQL Server in a Azure virtual machine, you will need to either modify the database file layout to spread the data out over additional files by using one or more database filegroups or create a striped volume in the Azure virtual machine. Depending on the size, Azure virtual machines can support up to 64 data disks. You can use software-based striping or Windows Server 2012 Storage Spaces to combine these disks into one large storage location for large databases.

- Consider moving databases larger than 10 GB out of the system disk so that you can place the databases on data disks when moved to Azure virtual machines. By default, the operating system disk is configured with both read and write caching.

Key information

- Azure virtual machines use Azure Blob storage for storing the VHDs.
- Azure virtual machines can have a maximum of 64 attached disks.
- Data disks in Azure virtual machines are limited to 1 TB in size.

Read more

- [How to attach a data disk to the new virtual machine](#)

Consider moving the databases out of system disk so that you can place the databases on data disks when moved to Azure VMs

The operating system disk in a Microsoft Azure virtual machine has a limit of 127 GB and is configured with both read and write caching. You should not consider this disk for storing the data files.

Suggested actions By default, the operating system disk is configured with both read and write caching, avoid using operating system or temporary disks for database storage or logging.

Consider moving data files to a disk separate from the system disk. When moving to Microsoft Azure virtual machines, use a data disk for these data and transaction log files.

Read more [Performance Best Practices for SQL Server in Azure Virtual Machines](#)

Databases (3) AZURELAB-SQLSVR;master
AZURELAB-SQLSVR;model
AZURELAB-SQLSVR;msdb

Databases that are hosted on SSD drives on premises may experience disk I/O throughput changes when they move these databases to Windows Azure VMs

The IO response times of a Windows Azure virtual machine may be slower than that of SSD storage, which may decrease the overall performance. In Windows Azure virtual machines, the maximum throughput is 500 IOPS per data disk. To mitigate slower IO response times, you need to spread the IO out over additional files located on separate data disks in Windows Azure virtual machines. Alternatively, you can use multiple data disks with Storage Spaces in Windows Server 2012. Windows Server 2012 Storage Spaces does not impact performance and has been shown to have the same performance as the aggregated results of the individual data disks when comparing with traditional operating system striping.

Read more

[Virtual Machine and Cloud Service Sizes for Windows Azure](#)

[Storage Spaces Overview](#)

[SQL Server Best Practices Article](#)

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-SQLSVR

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](#)

Modify the database file layout for databases larger than 1 TB

Data disks in Microsoft Azure virtual machines are limited to 1 TB in size. To migrate a larger database to SQL Server in a Microsoft Azure virtual machine, you will need to either modify the database file layout to spread the data out over additional files by using one or more database filegroups or create a striped volume in the Microsoft Azure virtual machine. Depending on the size, Microsoft Azure virtual machines can support up to 16 data disks. You can combine these disks into one large storage location for large databases by using software-based striping or Windows Server 2012 Storage Spaces. Windows Server 2012 Storage Spaces does not impact performance and has been shown to have the same performance as the aggregated results of the individual data disks when comparing with traditional operating system striping.

Read more

[Virtual Machine and Cloud Service Sizes for Microsoft Azure](#)

[Performance Considerations for SQL Server in Microsoft Azure Virtual Machines](#)

[Performance Guidance for SQL Server in Microsoft Azure Virtual Machines](#)

[Storage Spaces Overview](#)

Move any user or system database files from the D: drive to other storage drives

The operating system disk (or the C: drive) in a Microsoft Azure virtual machine has a limit of 127 GB and is configured with both read and write caching. You should consider this disk only for storing the database files of databases that are 10 GB or smaller in size. Microsoft does not recommend using the D: drive for storing any user or system database files, including tempdb.

Suggested actions Move any data, log, or backup files stored on the D: drive to other storage drives before migrating the database to Microsoft Azure virtual machines.

Read more [Performance Best Practices for SQL Server in Azure Virtual Machines](#)

SqlServer AZURELAB-SQLSVR

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

Any critical application that stores its data in a database system must have a proper disaster recovery plan for business continuity purposes. The plan must be well designed and tested for recovering the databases in the event of a disaster. In addition, the recovery process must be tested frequently to ensure that all the IT

personnel who have been assigned tasks in the disaster recovery plan are well prepared with the execution of their tasks in the event of a real disaster.

There are several High Availability Disaster Recovery solutions that can be designed to address the Recovery Point Objective/Recovery Time Objective (RPO/RTO) requirements of a business. It is important to understand what each solution can address and prepare an appropriate disaster recovery plan.

Key information:

- Azure virtual machines support Always On Availability Groups in both full migration and hybrid scenarios.
- SQL Server 2012 SP1 CU2, enables SQL Server backup and restore directly to the Azure Blob service
- Azure virtual machines do NOT support Failover Clustering.
- Azure virtual machines support SQL Server Database Mirroring.
- Azure virtual machines support SQL Server Log Shipping.

Secure your environment

The 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. Azure virtual machines are subject to attack vectors that may be uncommon inside of corporate networks, including denial of service (DoS), user credential attacks, and unintended disclosure of data. Azure virtual machines need to be architected and built to handle these types of attacks that may not be common inside corporate networks.

Key information

- Your machine's endpoint is accessible to anyone. Protect it!

Read more

- Visit the [Windows Azure Trust Center](#) to learn more.

An unsecured SQL Server that has SQL logins with blank (NULL) password is vulnerable

A login without a password, or with password the same as login, provides an entry point for hackers and worms.

Read more

[Password Policy](#)

[PWDCOMPARE \(Transact-SQL\)](#)

[Microsoft Baseline Security Analyzer 2.2 \(for IT Professionals\)](#)

An unsecured SQL Server that has SQL logins with password same as logins allows vulnerability to a worms

A login without a password, or a password that is the same as the login, provides an entry point for hackers and worms.

Read more

[Password Policy](#)

[Understanding Password Policy for SQL Server Logins](#)

[PWDCOMPARE \(Transact-SQL\)](#)

[CREATE LOGIN \(Transact-SQL\)](#)

[ALTER LOGIN \(Transact-SQL\)](#)

[Microsoft Baseline Security Analyzer 2.2 \(for IT Professionals\)](#)

Configure SQL Server logins to adhere to strong password policy



Complex passwords can protect against brute force attacks by increasing the number of possible passwords. On an instance of SQL Server that is running on Windows Server 2003 or later, you can configure SQL Server logins to use Windows password complexity rules.

Suggested actions

- 1) Enforce password complexity rules on standard SQL logins. When using CREATE LOGIN to create a SQL Server login, set CHECK_POLICY and CHECK_EXPIRATION to ON.
- 2) Query master.sys.sql_logins for logins that have is_policy_checked or is_expiration_checked set to 0. Use ALTER LOGIN to set CHECK_POLICY and CHECK_EXPIRATION to on.

Read more

[Password Policy](#)

[Understanding Password Policy for SQL Server Logins](#)

[CREATE LOGIN \(Transact-SQL\)](#)

[ALTER LOGIN \(Transact-SQL\)](#)

SqlInstance

AZURELAB-SQLSVR

Local accounts with administrative rights shouldn't have common names



Azure virtual machines are exposed to the Internet by default. Therefore, you want to make it as difficult to guess the user names as possible.

Suggested actions Change the default administrator account to a non-default name

Use complex, uncommon passwords for administrative accounts

Server

AZURELAB-SQLSVR

Local Administrator accounts shouldn't have weak passwords

Although you can lock down RDP access via the public endpoint, it is very common to have the RDP endpoint exposed to the internet, so you want to ensure that none of your local administrator accounts use common passwords.

Make sure some local administrator accounts are enabled

You need be careful to maintain remote access to computers when uploading Virtual Machines to Microsoft Azure. If you disable the local administrator account you should ensure that you have credentials for another local account which has administrative access or that you have joined the computer to your domain and a domain controller is available to the virtual machine. Therefore, maintain credentials to allow access to uploaded virtual machines even in the event it does not have communication with an on-premises domain controller.

Read more

[Remote Desktop Services and Windows Firewall](#)

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](#)

Ensure a healthy environment

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

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.

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](#)

Optimize your configuration

Certain configuration optimizations are not as important for an on premises environment, but are much more important once you migrate to Azure. At the same time, several of the performance tuning options that are applicable for SQL Server in an on premises environment continue to apply to SQL Server on a Azure virtual machine as well.

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.
- Configure Azure virtual machine to utilize the UTC time zone and the RealtimeIsUniversal option in order to minimize the risk of time zone issues.
- Consider using database page compression as it can help improve the performance of I/O intensive workloads. However, the data compression might increase the CPU consumption on the database server.
- Consider compressing any data files when transferring in/out of Azure.

- Consider enabling instant file initialization to reduce the time that is required for initial file allocation. For more information, refer to [Database File Initialization](#).
- [Optimize tempdb for better performance](#).
- Enable auto-grow option, but do not rely on it for your database growth. Always manually grow the files during a downtime. The Auto-Grow should only come in during emergencies when monitoring fails. Change from a percentage-based growth to a fixed-size growth. Determine the fixed size based on your usage and the growth based on capacity planning. A 10 percent fixed size is a good number to start with for databases with a few hundred GBs of data.

Read more

- [Performance Considerations for SQL Server in Windows Azure Virtual Machines](#)
- [Performance Guidance for SQL Server in Windows Azure Virtual Machines](#)

Align the Max Degree of Parallelism option to the number of logical processors in Microsoft Azure virtual machine

In SQL Server, the Max Degree of Parallelism configuration option controls the number of processors used to execute a single statement. The value for this option should not exceed the number of physical processors or cores. The largest Microsoft Azure virtual machines, extra-large and G5 series machines, have 32 logical processors, so you should adjust the Max Degree of Parallelism option accordingly.

Read more

[Recommendations and guidelines for the "max degree of parallelism" configuration option in SQL Server](#)

[Configure the max degree of parallelism Server Configuration Option](#)

SqlInstance

AZURELAB-SQLSVR

Align the Max Server Memory option to the size of the Microsoft Azure virtual machine

Microsoft Azure virtual machines support up to 448 GB of RAM with an G5 virtual machine size. The Max Server Memory option in SQL Server helps you accommodate for memory needed by Windows and any other installed software. Because 448 GB of RAM is the largest virtual machine memory size, 444 GB is the largest recommended setting for Max Server Memory. If SQL Server is using more than 444 GB of RAM, you will not be able to migrate to a Microsoft Azure virtual machine without experiencing a decrease in performance. In this scenario, you will need to either reduce the memory requirement of your workload or re-architect the solution to scale out across multiple Microsoft Azure virtual machines.

Read more

[Virtual Machine and Cloud Service Sizes for Azure](#)

[Server Memory Server Configuration Options](#)

[Performance Best Practices for SQL Server in Azure Virtual Machines](#)

SqlInstance

AZURELAB-SQLSVR

Configure tempdb data files to minimize allocation bottlenecks and increase scalability

Use multiple data files for tempdb in order to optimize its performance and reduce allocation contention while increasing scalability. SQL Server uses a proportional fill algorithm when writing to data files of the same filegroup. Using identical initial size and growth increment for all data files helps the database engine optimally distribute allocations among all data files in the same filegroup.

Suggested actions

1) In an environment where tempdb is used heavily, consider keeping the number of tempdb data files between 0.25 to 1.0 times the number of physical cores.

2) On servers with more than 8 physical cores, start with 8 data files and then increase or decrease this number, as needed.

3) Modify properties of tempdb data files to have identical initial size and growth increment, leveraging the SQL Server proportional fill algorithm for file allocations.

Read more

[How to shrink the tempdb database in SQL Server](#)

[Optimizing tempdb Performance](#)

SqlInstance

AZURELAB-SQLSVR

Configure tempdb to scale allocation contention to improve SQL Server performance on Microsoft Azure virtual machines



When the trace flag 1118 is enabled, SQL Server allocates full extents to each database object, thereby eliminating the contention on SGAM pages. The pages within the extent are reserved and allocated singly from this extent, as needed. This helps reduce the contention.

Suggested actions Enable the Trace Flag 1118 as a startup parameter for the SQL Server instance and add additional data files matching the number of logical processors in the virtual machine. If the number of logical processors is more than 8, start with 8 data files and increase this number in multiples of 4 up to the number of logical processors.

Read more

[Concurrency enhancements for the tempdb database](#)

[Working with tempdb in SQL Server 2005 and above](#)

SqlInstance AZURELAB-SQLSVR

Consider the impact on SQL Server performance before enabling Lightweight Pooling

In a multi-processor system, sometimes the operating system moves process threads among different processors. This is called context switching, which can become a performance bottleneck. On a server where all processors are running at or near maximum capacity and there is a lot of context switching, enabling Lightweight Pooling, also known as Fiber mode, can improve performance by reducing context switching.

Note that some components of SQL Server such as SQLCLR and SQLMail do not support Fiber mode.

Read more [lightweight pooling Server Configuration Option](#)
[How to determine proper SQL Server configuration settings](#)

SqlInstance AZURELAB-SQLSVR

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](#)

Determine the appropriate initial size for tempdb in a production environment for optimal performance



With SQL Server 2005 and above, tempdb is responsible for managing temporary objects, row versioning, and online index rebuilds. Some of this processing has moved from the transaction log in SQL Server 2000 to tempdb in SQL Server 2005 onwards. Therefore, determining an appropriate initial size for tempdb in SQL Server 2005 and above is essential. Creating a tempdb file that is too small or leaving the default size set to 8 MB can trigger several autogrow operations during the peak times. As a result, the tempdb file may have to expand constantly, which will affect the server performance.

Suggested actions Determining the appropriate size for tempdb in a production environment depends on several factors, such as the existing workload and the SQL Server features being used. Microsoft recommends that you analyze the existing workload by performing the following tasks in a SQL Server test environment:

- 1) Set autogrow as ON for tempdb.
- 2) Run individual queries or workload trace files and monitor the tempdb space.
- 3) Run index maintenance operations, such as rebuilding indexes and monitor the tempdb space.
- 4) Use the space-use values from the previous steps to predict your total workload usage. Adjust this value for projected concurrent activity and then set the size of tempdb accordingly.

Read more

[Optimizing tempdb Performance](#)

SqlInstance AZURELAB-SQLSVR

Disable the Priority Boost option on both stand-alone and clustered SQL Server instances

The Priority Boost configuration option causes the operating system to run a SQL Server instance at a higher scheduling priority (priority base of 13) than other processes running on the same computer. By default, this option is disabled, which means that the operating system runs the SQL Server instance at priority base of 7.

Read more [priority boost Option](#)

[sp_configure \(Transact-SQL\)](#)

[How to determine proper SQL Server configuration settings](#)

SqlInstance AZURELAB-SQLSVR

Enable Instant File Initialization to allow faster execution of certain file operations

In SQL server, data and log files are initialized to overwrite any existing data left on the disk from previously deleted files. Data and log files are first initialized by filling the files with zeros when you perform one of the following operations:

- Create a database.
- Add files, log, or data to an existing database.
- Increase the size of an existing file (including autogrow operations).
- Restore a database or filegroup.

In SQL Server, data files can be initialized instantaneously which allows for fast execution of certain file operations. Instant File Initialization is available only if the SQL Server service account has been granted the Perform Volume Maintenance

Tasks privilege. Instant File Initialization reclaims used disk space without filling that space with zeros which allows the operations to execute faster.

Because the deleted disk content is overwritten only as new data is written to the files, the deleted content might be accessed by an unauthorized principal. While the database file is attached to the instance of SQL Server, this information disclosure threat is reduced by the discretionary access control list (DACL) on the file.

Note that Log files cannot be initialized instantaneously.

Read more [Database File Initialization](#)

Enable the backup compression default option in Microsoft Azure virtual machines running SQL Server

The backup compression default option determines whether the server instance creates compressed backups by default. Because a compressed backup is smaller than an uncompressed backup of the same data, compressing a backup typically requires less device I/O and therefore, usually increases the backup speed significantly.

Read more [View or Configure the backup compression default Server Configuration Option](#)

[Backup Compression \(SQL Server\)](#)

SqlInstance AZURELAB-SQLSVR

Modify properties of tempdb data files to have identical initial size and growth increments

Use multiple data files for tempdb in order to reduce allocation contention and increase scalability. SQL Server uses a proportional fill algorithm when writing to data files of the same filegroup. Using identical initial size and growth increment helps the database engine distribute allocations equally among data files in the same filegroup.

Read more

[How to shrink the tempdb database in SQL Server](#)

[Optimizing tempdb Performance](#)

Registry entry RealtimelsUniversal must be set



When RealtimelsUniversal 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

RealTimelsUniversal 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.

Review the SQL Server configurations that are set for different config and run values



Microsoft SQL Server configuration settings have two values: run_value and config_value. While run_value shows the currently effective value of a configuration setting, config_value shows the new value that is assigned to the setting by using sp_configure.

Read more [sp_configure \(Transact-SQL\)](#)
[Server Configuration Options \(SQL Server\)](#)

SqlInstance AZURELAB-SQLSVR

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.

Set the Affinity Mask and Affinity I/O MASK options to correct values ✓

In a multi-processor system, the Affinity Mask server configuration option is used to assign certain CPUs to an instance of SQL Server, and the Affinity I/O Mask is used to assign SQL Server disk I/O operations to specified CPUs. Assigning the same processor(s) to both the Affinity Mask and the Affinity I/O Mask, can slow performance by overloading the processor(s).

Read more [Correct Affinity Mask and Affinity I/O Mask Overlap](#)
[The 'affinity mask' and 'affinity I/O mask' configuration should not conflict](#)

SqlInstance AZURELAB-SQLSVR

SQL Server instance can be configured to use up to 32 logical processors on Microsoft Azure VMs ✓

Microsoft Azure virtual machines support up to 32 logical processors with an extra-large or G5 virtual machine size. If SQL Server is fully utilizing more than 32 logical processors, you will not be able to migrate to the Windows Azure virtual machine

without experiencing a decrease in performance. To migrate to Microsoft Azure virtual machines, you will need to either reduce the CPU consumption of your workload or re-architect the solution to scale out across multiple Microsoft Azure VMs.

Read more

[Monitor and Tune for Performance](#)

[Virtual Machine and Cloud Service Sizes for Microsoft Azure](#)

[Performance Considerations for SQL Server in Microsoft Azure Virtual Machines](#)

[Performance Guidance for SQL Server in Microsoft Azure Virtual Machines](#)

The SQL Server configuration setting, Affinity I/O Mask will be removed in a future version of Microsoft SQL Server. Avoid using this feature in new development work



In a multi-processor system, the Affinity I/O Mask server configuration option is used to assign SQL Server disk I/O to specified CPUs. The value of Affinity I/O Mask defines which CPUs can process SQL Server disk I/O operations. When the Affinity I/O Mask is at its default value of 0, the SQL Server instance can use all processors in the system for its disk I/O operations.


Read more

[affinity I/O mask Option](#)

[INF: Understanding How to Set the SQL Server I/O Affinity Option](#)

SQLInstance

AZURELAB-SQLSVR


The SQL Server configuration setting, Affinity Mask will be removed in a future version of SQL Server. Do not use this feature in new development work 

In a multi-processor system, the Affinity Mask server configuration option is used to assign certain CPUs to an instance of SQL Server. When the affinity mask is at its default value of 0, the SQL Server instance can use all processors in the system for its threads. Setting the Affinity Mask to a non-default value restricts SQL Server to using only the assigned CPUs.

Read more [affinity mask Server Configuration Option](#)

ALTER SERVER CONFIGURATION (Transact-SQL)


SqlInstance AZURELAB-SQLSVR

The SQL Server configuration setting, Affinity64 I/O Mask will be removed in a future version of Microsoft SQL Server. Avoid using this feature in new development work 

In a multi-processor system, the Affinity I/O Mask server configuration option is used to assign SQL Server disk I/O to specified CPUs. The value of Affinity I/O Mask defines which CPUs can process SQL Server disk I/O operations. When the Affinity I/O Mask is at its default value of 0, the SQL Server instance can use all processors in the system for its disk I/O operations.

Read more [affinity64 I/O mask Server Configuration Option](#)

SqlInstance AZURELAB-SQLSVR

The SQL Server configuration setting, Affinity64 Mask will be removed in the next version of Microsoft SQL Server. Avoid using this feature in new development work 

In a multi-processor system, the Affinity Mask server configuration option is used to assign certain CPUs to an instance of SQL Server. When the affinity mask is at its default value of 0, the instance of SQL Server can use all processors in the system for its threads. Setting the affinity mask to a non-default value, restricts SQL Server to using only the assigned CPUs.

On a server with more than 32 processors, "Affinity Mask" is used to bind the first 32 processors and "Affinity64 Mask" is used to bind the remaining processors to the instance of SQL Server. Affinity64 Mask is only available on the 64-bit version of SQL Server.

Read more [affinity64 mask Server Configuration Option](#)

SqlInstance AZURELAB-SQLSVR

The SQL Server configuration setting, allow updates, has been deprecated, do not use this feature for future development



The Allow Updates SQL Server configuration setting does not have any effect in SQL Server 2005 and later versions. However, when you enable this option in SQL Server 2000, it allows users to modify system tables by using ad hoc updates. This could result in major issues such as corruption, data loss, and service failure. Modifying system tables should only be done using system stored procedures.


Read more [allow updates Option](#)

[sp_configure \(Transact-SQL\)](#)

[SQL Server Requirements for System Center 2012 - Service Manager](#)

SqlInstance

AZURELAB-SQLSVR

Use Max Server Memory to control memory usage by the buffer pool, the operating system, and other applications running on the server 

The Max Server Memory configuration option sets a limit on the maximum size of the buffer pool. The buffer pool is the largest pool of memory in SQL Server that is used for caching data and indexes. When an instance of SQL Server starts, the buffer pool starts with only a limited amount of memory that it needs to initialize. As the workload increases, the buffer pool acquires more memory in order to support the workload. If the workload keeps increasing, the buffer pool keeps growing until it reaches the size defined by the Max Server Memory option. The default value for Max Server Memory is 2,147,483,647 MB. Leaving this option at its default value on an instance of SQL Server that is experiencing a heavy workload may result in the buffer pool consuming all the memory that it wants; thereby not leaving enough memory for other applications, the operating system, and other pools of SQL Server.

Read more[Server Memory Server Configuration Options](#)[Effects of min and max server memory](#)[Checklist: Configuring SQL Server \(BizTalk\)](#)

SqlInstance

AZURELAB-SQLSVR

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-SQLSVR

 Move

Get a subscription

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

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

<http://www.windowsazure.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://www.windowsazure.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://www.windowsazure.com/en-us/pricing/purchase-options/>

Optimize for a geographically limited user base

Windows Azure has data centers around the world and you can deploy your workload to any or all of them. This will allow you to better leverage the geographic diversity offered by Windows Azure.

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

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

Windows 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 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 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.

Read more

[Create a Virtual Machine Running Windows Server](#)

Enable RDP on the server



This rule fires if RDP is not enabled on the server.

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-SQLSVR

Review the currently available Microsoft Azure gallery images of the SQL Server instances

The Microsoft Azure image gallery provides pre-built images of SQL Server running on Windows for fast provisioning. Currently, there are several SQL Server images available in the gallery including the list, but not limited to.

- SQL Server 2014 SP1 standard on Windows Server 2012 R2
- SQL Server 2012 SP2 Enterprise on Windows Server 2012
- SQL Server 2008 R2 Service Pack 2 on Windows Server 2008 R2
- SQL Server 2012 Service Pack 1 on Windows Server 2008 R2
- SQL Server 2012 Service Pack 1 on Windows Server 2012

For other versions of SQL Server, you will need to create a custom image and upload it to Microsoft Azure.

Read more

[Provisioning a SQL Server Virtual Machine on Azure](#)

[Microsoft server software support for Microsoft Azure Virtual Machines](#)

[Creating and Uploading a Virtual Hard Disk that Contains the Windows Server Operating System](#)

[Microsoft Azure Powershell](#)

[Microsoft Azure SDK](#)

Move your data

This section of the assessment provides an overview of how to migrate your on premises SQL Server databases to the cloud via SQL Server in Azure virtual machines. Migrating existing SQL Server applications to Azure virtual machines requires minimal or no code changes. The very first step is to go ahead and get a Azure subscription and start exploring.

Once you have the subscription, the next step is to provision a SQL Server virtual machine on Azure. You can do this by using the Azure image gallery which contains several images that contain Microsoft SQL Server. You can select one of these images and with a few clicks, provision the virtual machine to your Azure environment.

You can copy or move the on premises SQL Server databases to SQL Server running in Azure virtual machines in several ways. Choosing the right method can ease the overall deployment into Azure. Copying or moving a database into Azure IaaS involves moving the data and all associated server objects such as user logins and SQL Server Agent jobs to the destination Azure virtual machine.

Review your requirements and select the easiest and most secure method to copy or move the database to Microsoft Azure

You can copy or move on premises SQL Server databases to SQL Server running in Microsoft Azure virtual machines in several ways. Choosing the right method can ease the overall deployment into Microsoft Azure. Copying or moving a database into Microsoft Azure Infrastructure as a Service (IaaS) involves moving the data and all associated server objects such as user logins and SQL Server Agent jobs to the destination Microsoft Azure virtual machine.

Suggested actions In most situations, the methods described below will be the most efficient and easiest. In some more complex scenarios, you may need to develop a custom solution that will meet your requirements.

Step 1: Back up the database

Perform a full backup of the database to the local drive. Be sure to use compression to reduce the amount of data being transferred to the Windows Azure virtual machine. For example:

```
BACKUP DATABASE [ADVENTUREWORKS2012] TO  
DISK=C:\TEMP\ADVENTUREWORKS2012_08152013.BAK  
WITH COMPRESSION, STATS = 5;
```

```
GO
```

Step 2: Copy the database backup to Microsoft Azure

Hybrid IT Architecture

When using a site-to-site VPN in a hybrid architecture, the on premises network and the virtual network in Microsoft Azure can communicate through the VPN tunnel. In this model, you may use Windows SMB shares in the form of \\ to move the file to the destination server at the other end of the VPN tunnel. Additionally, you can use the methods listed below under Full Migration.

Full Migration (no Site-to-Site VPN connection)

When a site-to-site VPN connection is not available, you will not be able to copy the file directly to the destination server in Microsoft Azure without additional steps or an intermediate storage location.

Method 1: Copy and paste through Remote Desktop session (smaller backup files)

1. Establish an RDP connection to the Microsoft Azure virtual machine. You can do this through the portal by selecting **Virtual Machines**, highlighting the correct virtual machine, and then clicking **Connect** at the bottom. This will download

an *.rdp file that will launch a Remote Desktop Connection. When the download starts, click **Open**. Click on the down arrow next to **Show Details** and verify that the **Clipboard** option is selected. Click **Connect** and provide your credentials when prompted.

If you are unable to connect, select the virtual machine under **Virtual Machines** and then click **Endpoints** from the menu across the top. Verify that an endpoint is defined for RDP. If not, you will need to add an endpoint for RDP.

2. Once the RDP connection is established, right-click the backup file that you created in Step 1 above and select **Copy**.

3. Through the RDP connection window, paste the backup file into the desired folder or on the desktop.

Method 2: Upload and download with PowerShell through Microsoft Azure Blob Storage (larger backup files)

1. Download and install the Microsoft Azure PowerShell tools on both the on premises server and the destination Microsoft Azure virtual machine. If you need help connecting to the Microsoft Azure virtual machine by using RDP, refer to Method 1 above.

2. In the Microsoft Azure Portal, you will need a storage account for uploading the backup file. If you do not have a storage account, you can create one by clicking **New** at the bottom left of the portal screen. Then, click **Data Services**, click **Storage**, and then click **Quick Create**. Provide a unique name to finish the storage URL, and select either an affinity group or datacenter region. Finally, click **Create Storage Account**.

3. In the Microsoft Azure Portal, select **Storage Accounts** on the left and select the storage account that you wish to use. Across the top menu, select **Containers**. At the bottom of the portal screen, click **Add** to create a new container in the storage account to hold the backup.

4. In the Microsoft Azure Portal, select **Storage Accounts** on the left and select the storage account that you will use to upload the backup file. At the bottom of the portal screen, click **Manage Access Keys**. In the Manage Access Keys pop-up window, click the **Copy** button to copy the Primary Access Key. Save this for later use. Close the screen.

5. Connect to the on premises server and launch the Microsoft Azure PowerShell environment. Run the following two commands by using the necessary information from your environment.

```
$context = New-AzureStorageContext StorageAccountName -  
StorageAccountKey
```

```
Set-AzureStorageBlobContent Container -File -Context  
$context
```

6. Once the upload completes, you will need to download the backup file to the Microsoft Azure virtual machine. Connect to the Microsoft Azure virtual machine by using an RDP session. Refer to Method 1 above for help connecting with RDP. Launch the Microsoft Azure PowerShell environment. Run the following commands to download the backup file to the Microsoft Azure virtual machine.

```
$context = New-AzureStorageContext StorageAccountName -  
StorageAccountKey
```

```
Get-AzureStorageBlobContent Blob -Container -Destination -  
Context $context
```

You may also download and install a Microsoft Azure Storage Explorer to use a GUI to accomplish the steps above.

Alternate methods

- 1) If you are running SQL Server 2012 SP1 CU2 or later, you can back up the database directly to Microsoft Azure Blob Storage from the on premises server and restore it from Microsoft Azure Blob Storage directly to the Microsoft Azure virtual machine.
- 2) You may also consider saving the file to a common storage service both servers have access to such as Windows Live OneDrive.
- 3) You may install an FTP server on the Microsoft Azure virtual machine. This will require an additional endpoint be setup for the FTP service in the Microsoft Azure Portal.
- 4) You can place the database backup file on a separate VHD drive and upload the drive to Microsoft Azure by using the CSUpload utility from the Microsoft Azure SDK. You can then attach this VHD drive to the Microsoft Azure virtual machine as a data disk.

Step 3: Restore the database

Restore the full backup to the SQL Server instance on the Microsoft Azure virtual machine. Be aware that you may need to relocate the database files by using the MOVE option of the TSQL RESTORE command if the drive layout in the virtual machine is different than that of the on premises server. For example:

```
RESTORE DATABASE [ADVENTUREWORKS2012] FROM  
DISK=C:\TEMP\AdventureWorks2012_08202013.bak
```

```
WITH MOVE AdventureWorks2012_Data TO  
M:\MSSQL\DATA\AdventureWorks2012_Data.mdf,
```

```
MOVE AdventureWorks2012_Log TO  
L:\MSSQL\LOG\AdventureWorks2012_Log.ldf;
```

```
GO
```

Important considerations:

- 1) After restoring the database, you may need to create additional objects in SQL Server on the Microsoft Azure virtual machine such as server level logins or SQL Server agent jobs. Additionally, you may need to re-map database users to the server level logins. More information can be found in the Read more section.
- 2) When using a third-party intermediate storage to move or copy the database into the Microsoft Azure virtual machine, consider the security risk involved and ensure that no unauthorized persons can access the backup file.
- 3) When using an FTP service or installing any additional services in the Microsoft Azure virtual machine, consider the security risk involved. Additional services will require you to create endpoints in the Microsoft Azure Portal to allow communication.
- 4) Make sure that Windows and SQL Server are up-to-date on all the latest security patches to prevent any unauthorized access.
- 5) Using SQL Server 2012 SP1 CU2 or later, or using the PowerShell method above can allow you to

programmatically move the database and automate regularly scheduled movements for environments where this is a requirement.

Read more

[Microsoft Azure PowerShell](#)

[Microsoft Azure Storage Explorers](#)

[CSUpload Command-Line Tool](#)

[How to move databases between computers that are running SQL Server](#)

[SQL Server Backup and Restore with Microsoft Azure Blob Storage Service](#)

[BACKUP \(Transact-SQL\)](#)

[RESTORE \(Transact-SQL\)](#)

SqlInstance

AZURELAB-SQLSVR

Monitor your environment

Although reboots are minimized in a Azure environment, they still do occur occasionally. While 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

Azure offers a variety of support options, ranging from self-help via community forums to Premier support that offers you 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 Azure subscriptions include free access to billing and subscription management, community forums, and the service dashboard.
- Azure support plans start at just \$29 per year and provide a higher level of service.

Read more

[Microsoft Azure Support](#)