Microsoft Azure - Starter Kits for Partners

Architecture

SharePoint in Azure Virtual Machines

Last Update: September 2015





**MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.**

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

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, the furnishing 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. Also, the descriptions are intended as brief highlights to aid understanding, rather than as thorough coverage. For authoritative descriptions of these products, please consult their respective manufacturers.

© 2015 Microsoft Corporation. All rights reserved. Any use or distribution of these materials without express authorization of Microsoft Corp. is strictly prohibited.

Microsoft and Windows are either registered trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Contents

[Overview 4](#_Toc404670192)

[This Starter Kit Selected Architecture 4](#_Toc404670193)

[Virtual Machine Components 5](#_Toc404670194)

[VHDs 5](#_Toc404670195)

[RDP and Remote PowerShell 6](#_Toc404670196)

[Azure Virtual Network 6](#_Toc404670197)

[Domain Controllers 7](#_Toc404670198)

[DNS 7](#_Toc404670199)

[Affinity Groups 7](#_Toc404670200)

[Firewalls and Endpoints 7](#_Toc404670201)

[Load balanced Endpoints 7](#_Toc404670202)

[High Availability and Availability Sets 8](#_Toc404670203)

[Operate and maintain SharePoint farm on Azure 9](#_Toc404670204)

[Monitoring 9](#_Toc404670205)

[Patching and updating 9](#_Toc404670206)

[Backup and Recovery 9](#_Toc404670207)

[Gold Images and Lab Environments 9](#_Toc404670208)

Architecture for SharePoint in Azure Virtual Machines

# Overview

The purpose of this document is to complement the lab document to include a broader discussion of concepts relevant to setting up a SharePoint 2013 farm with Azure Virtual Machines.

# This Starter Kit Selected Architecture

The scenario below is illustrated in the Cost Calculator and implemented in the Deployment Guidance (Hand on Labs). However, you may make changes in the architecture and topology as appropriate.

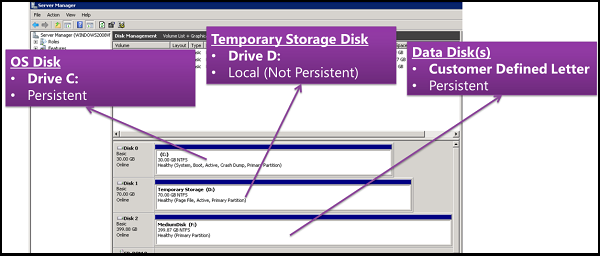


The rest of this document will discuss the other architecture aspects that you take into consideration for this scenario.

# Virtual Machine Components

## VHDs

All images and disks in Azure, except the temporary disk, are actually virtual hard disks (VHDs). The virtual hard disks are .vhd files stored as page blobs in a storage account in Azure. The temporary disk is not stored in Azure storage.



**Operating system disk** - Every [virtual machine](https://azure.microsoft.com/en-us/documentation/articles/virtual-machines-disks-vhds/) has one attached operating system disk. It’s registered as a SATA drive and labeled as the C drive. This disk has a maximum capacity of 127 GB. When Azure creates an operating system disk, three copies of the disk are created for high durability. Additionally, if you configure the virtual machine for geo-replication, your VHD is also replicated at a distance of greater than 400 miles. When troubleshooting issues on an operating system disk, you can attach the disk as a data disk to another running virtual machine to access the data on the disk and diagnose problems using the logs.

The **temporary disk** is automatically created for you. On Windows virtual machines, this disk is labeled as the D drive. Don’t store data on the temporary disk. This disk provides temporary storage for applications and processes and is used to store data that you don’t need to keep, such as page or swap files.

**Data disk** – A data disk is a VHD that can be attached to a running virtual machine to store application data, or other data that you need to keep. The maximum size of a data disk is 1 TB and you are limited in the number of disks that you can attach to a virtual machine based on the size of the machine. Data disks are registered as SCSI drives and are labeled with a letter that you choose. The size of the virtual machine determines the number of disks that you can attach to it.

**Disk Caching** - The operating system disk and data disk each have a host caching setting (sometimes called host-cache mode) that can improve performance under some circumstances. However, these settings can negatively affect performance in other circumstances, depending on the application. Host caching is OFF by default for both read operations and write operations for data disks. Host-caching is ON by default for read and write operations for operating system disks.

**Avoid use of stripped disk with geo-replication** - Data loss may occur if you use striped volumes (Windows or Linux) in geo-replicated storage accounts. If a storage outage occurs that requires restoring data from a replicated copy, there is no guarantee that the write order of the stripe disk set would be intact once restored.

When configuring SQL server virtual machine for your SharePoint Farm you should use data disks for your database files and logs.

## RDP and Remote PowerShell

You can access new virtual machines over the Internet through the Remote Desktop Protocol (RDP) and with remote Windows PowerShell sessions. By default, Azure adds inbound mappings, known as endpoints, for both types of traffic when you create the virtual machine. These endpoints allow incoming RDP and remote Windows PowerShell sessions with the appropriate user credentials.

## Azure Virtual Network

An [Azure Virtual Network](https://azure.microsoft.com/en-us/documentation/articles/virtual-networks-overview/) is a logical container that can host virtual machines grouped on subnets. Virtual machines on subnets in a virtual network can communicate directly with each other, just like on intranet subnets, without that traffic traversing the Internet. This is in contrast with Azure Virtual Machines that are not in a virtual network, which cannot communicate with each other without that traffic traversing the Internet. Whether you need a virtual network depends entirely on what you are trying to do. There are no one-size-fits-all virtual network designs. However, you’ll find that every solution falls into one of 3 basic configuration categories: No VNet, Cloud-Only VNet, or Cross-Premises VNet (which includes Hybrid solutions). You should always create a virtual network within Azure before deploying any new virtual machines. Creating a VNet will allow you to group your virtual machines together and allow you to divide and determine the ranges of IP addresses assigned to your virtual machines.

**Cross-premises VNet** is a virtual network that is connected to your organization network across the Internet through a site-to-site VPN connection. Virtual machines in a cross-premises virtual network act as an extension of your organization network, providing applications and services to intranet users, Internet users, or both. When you create a cross-premises virtual network, you define a private IPv4 address range unique to your organization network to use for all the subnets that the virtual network will contain. You also define an IPv4 address range for each subnet. When you create a virtual machine and add it to a subnet, Azure will assign an address from the IPv4 address range for the subnet through DHCP. The time on the DHCP lease is set to at least 100 years, providing a very stable address configuration. It is important to note that Azure itself uses several addresses from the IPv4 address range for each subnet. The first virtual machine you add to a subnet typically has the fourth IP address in the range. For example, for the subnet with the address range 10.0.0.0/24 (or 10.0.0.0 with the subnet mask 255.255.255.0), the IP address of your first virtual machine will be 10.0.0.4.

**Site to Site VPN Connections -** A [site-to-site VPN](https://azure.microsoft.com/en-us/documentation/articles/vpn-gateway-cross-premises-options/) allows you to create a secure connection between your on-premises site and your virtual network. To create a site-to-site connection, [a VPN device](https://azure.microsoft.com/en-us/documentation/articles/vpn-gateway-about-vpn-devices/) that is located on your on-premises network is configured to create a secure connection with the Azure Virtual Network Gateway. Once the connection is created, resources on your local network and resources located in your virtual network can communicate directly and securely. You must have an externally facing IPv4 IP address and a VPN device or RRAS to configure a site-to-site VPN connection.

## Domain Controllers

SharePoint 2013 requires AD DS domain membership for the server on which it runs. You cannot use Azure Active Directory (AD) as a substitute for AD DS domain membership for the SharePoint 2013 server. However, you can [use Azure AD to provide authentication](http://technet.microsoft.com/library/dn635311(v=office.15).aspx) for users accessing SharePoint resources. To minimize the latency of performing authentication of intranet user credentials for access to and administration of SharePoint farm sites and resources, you should [deploy Active Directory Domain Services (AD DS)](http://msdn.microsoft.com/library/azure/jj156090.aspx) domain controllers in the virtual network. For redundancy, you should deploy at least two.

## DNS

You can use your existing DNS servers on-premises if you define a cross-premises virtual network or you can DNS servers within the virtual network such as hosting them in ADDS domain controllers. You should not make any changes to network connections of virtual machines has this may render them unreachable.

## Affinity Groups

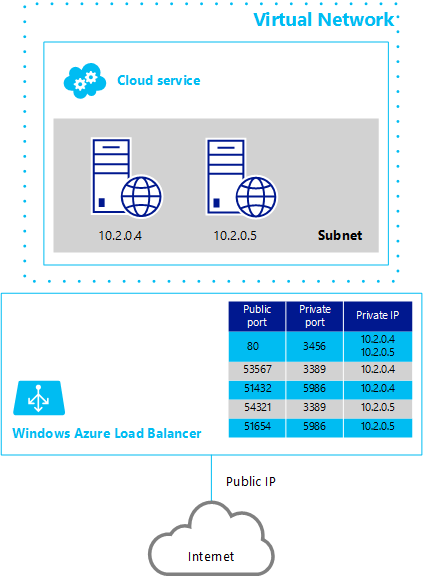
[Affinity groups](https://azure.microsoft.com/en-us/documentation/articles/virtual-networks-migrate-to-regional-vnet/) allow you to group your Azure services to optimize performance. All services and VMs within an affinity group will be located in the same region. Currently affinity groups are no longer required in order to create a virtual network. New virtual networks should now be associated with a Location (region).

## Firewalls and Endpoints

Virtual machines are accessible from other virtual machines inside the virtual network. You can use all TCP/IP protocols within the virtual network depending on the settings of the virtual machine firewall. For access from the Internet you will need to use the external name or public IP address of the cloud service. [Endpoints](http://azure.microsoft.com/en-us/documentation/articles/virtual-machines-set-up-endpoints/) can be configured for each individual virtual machine and are similar to port forwarding or mapping rules. Endpoints for both RDP and PowerShell are configured by default using random public port numbers that map to internal port numbers. You can remove these ports if you don’t want to administer the virtual machines from the Internet. For Internet traffic to your SharePoint farm, you must configure endpoints on the web server virtual machines. For example, you could configure an endpoint for the public TCP port 80 that maps to a private TCP port 80 (for standard web traffic), or to the TCP port on which the SharePoint server is listening.

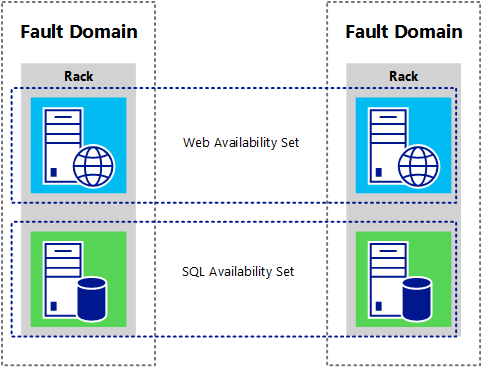
## Load balanced Endpoints

Azure also allows you to [load balance](https://azure.microsoft.com/en-us/documentation/articles/load-balancer-overview/) network traffic to a public address and a specific public port number across multiple virtual machines. The figure bellow shows an example with two web servers, both listening on private TCP port 3456 for incoming web traffic, in a configuration known as a load-balanced endpoint. Azure will randomly distribute the traffic between the nodes. You can have up 50 virtual machines behind a single load-balanced endpoint.



## High Availability and Availability Sets

For [High Availability](http://azure.microsoft.com/en-us/documentation/articles/virtual-machines-manage-availability/) you should deploy more than one single virtual machine of a particular role. This way you can avoid application stoppage due to local hardware or local network failures or any planned downtime, such as platform updates. When virtual machines are assigned to the same availability set, Azure assures that the machines are not taken all down together at the same time for servicing. It also minimizes the risk of the entire set failing for unforeseen reasons by placing them in separate update and fault domains (similar to a rack of physical servers) thus avoiding single points of failure.



# Operate and maintain SharePoint farm on Azure

## Monitoring

Azure provides a lot of flexibility and power to your SharePoint farm but having them running in Azure virtual machines (Iaas model) as opposed to using SharePoint Online (Saas model) means you still need to manage your Windows Server, SharePoint, SQL and any other dependencies. However, [administration tools and procedures](http://technet.microsoft.com/library/jj219701.aspx) are the same as an on-premises farm and you can leverage the use of System center for a centralized solution.

## Patching and updating

As in monitoring, you are still in control for [patching and updating](http://technet.microsoft.com/library/ff806329.aspx) and you can decide when, how it should happen. You can leverage Azure to test before updating your OS or SharePoint farm by creating a testing or staging environment when needed. Update only when you feel ready.

## Backup and Recovery

[Backing up and recovery of SharePoint](http://technet.microsoft.com/en-us/library/ee662536(v=office.15).aspx) farms in Azure is very similar to an on-premises SharePoint farm. One thing to consider is that you should suffer no significant down-time due to hardware failure. Because Azure will automatically repair and redeploy your virtual machine, there is no action to take on your part. You will get hardware downtime that would be automatically repaired. Ensure that any customizations you perform or applications you deploy can handle this automatic recovery. Azure makes it very easy to deploy more virtual machines, making it possible to create a highly available farm.

## Gold Images and Lab Environments

Although you can use the Microsoft-supplied SharePoint 2013 Trial image in the Azure Virtual Machine Image Gallery for your SharePoint servers, you can also create your own image. You might want to do this if you have different requirements or wish to preload other software, such as SharePoint applications or anti-malware software.

Azure allows you to [create gold images](http://azure.microsoft.com/en-us/documentation/articles/virtual-machines-capture-image-windows-server/) by creating a disk image from an existing VHD. This disk image contains both the operating system and any customizations you may require, such as the installation of software and custom Windows settings. This disk image can then be used to create new Azure virtual machines. Using a disk image means that you can quickly create multiple copies of the same server.

To create a gold image, you need a virtual machine on which to base the image. This virtual machine is just a standard Azure virtual machine that has been customized. To create a base image with SharePoint 2013 installed, it is recommended that you do not complete the entire SharePoint 2013 installation. This is due to incompatibilities with the SYSPREP tool, which is a required step to prepare the disk image.

**Additional Resource and Reference**: [Architecture for SharePoint in Azure Virtual Machines](https://technet.microsoft.com/library/dn635309(v=office.15).aspx)