Microsoft

Introducing Windows Azure

For IT Professionals

Mitch Tulloch with
the Windows Azure Team

PUBLISHED BY
Microsoft Press
A Division of Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052-6399

Copyright © 2013 Microsoft Corporation

All rights reserved. No part of the contents of this book may be reproduced or transmitted in any form or by any means without the written permission of the publisher.

Library of Congress Control Number: 2013949894
ISBN: 978-0-7356-8288-7

Microsoft Press books are available through booksellers and distributors worldwide. If you need support related to this book, email Microsoft Press Book Support at mspinput@microsoft.com. Please tell us what you think of this book at *http://www.microsoft.com/learning/booksurvey*.

Microsoft and the trademarks listed at *http://www.microsoft.com/about/legal/en/us/IntellectualProperty/Trademarks/EN-US.aspx* are trademarks of the Microsoft group of companies. All other marks are property of their respective owners.

The example companies, organizations, products, domain names, email addresses, logos, people, places, and events depicted herein are fictitious. No association with any real company, organization, product, domain name, email address, logo, person, place, or event is intended or should be inferred.

This book expresses the author's views and opinions. The information contained in this book is provided without any express, statutory, or implied warranties. Neither the authors, Microsoft Corporation, nor its resellers, or distributors will be held liable for any damages caused or alleged to be caused either directly or indirectly by this book.

Acquisitions Editor: Anne Hamilton
Developmental Editor: Karen Szall
Project Editor: Valerie Woolley
Editorial Production: Christian Holdener, S4Carlisle Publishing Services
Copyeditor: Andrew Jones

Contents

What do you think of this book? We want to hear from you!

Microsoft is interested in hearing your feedback so we can continually improve our books and learning resources for you. To participate in a brief online survey, please visit:

microsoft.com/learning/booksurvey

What do you think of this book? We want to hear from you!

Microsoft is interested in hearing your feedback so we can continually improve our books and learning resources for you. To participate in a brief online survey, please visit:

microsoft.com/learning/booksurvey

Introduction

The Windows Azure public cloud platform is one of the three pillars of Microsoft's Cloud OS vision that will transform the traditional datacenter environment, help businesses unlock insights in data stored anywhere, enable the development of a wide range of modern business applications, and empower IT to support users who work anywhere on any device while being able to manage these devices in a secure and consistent way. The other two pillars of the Cloud OS are, of course, Windows Server 2012 R2 and Microsoft System Center 2012 R2, and Microsoft Press will soon be releasing free Introducing books on these platforms as well.

What's really exciting to me personally as an IT pro is that this is all coming at once. General Availability (GA) of these latest versions of Windows Server and System Center is currently scheduled for October 18, 2013, which is less than two months away as this book is being written. In sync with these two releases, the Windows Azure platform has also been enhanced in recent months with preview releases of new services like Windows Azure BizTalk Services, Windows Azure Traffic Manager, and Windows Azure HDInsight. And in the same timeframe, services that were previously in preview like Windows Azure Web Sites and Windows Azure Mobile Services have now reached the GA milestone.

In fact, as I write this Introduction (it happens to be the last piece of the book that I'm writing) I just noticed that another new service, Windows Azure Store, has just entered preview. Fortunately, it turns out that my free Windows Azure subscription as an MSDN subscriber currently doesn't support purchasing from the Store in my geographical region, so I can't test this preview feature just yet. I'm actually glad about this because I just finished writing the last chapter and don't want to go back and have to revise it again!

My point of course is that Windows Azure, the public cloud portion of Microsoft's Cloud OS, is a constantly evolving platform with new features entering preview all the time. One has to draw a line somewhere though, so we've decided to title this book *Introducing Windows Azure for IT Professionals* as it tries to capture the essence of what Windows Azure can do for your business as Microsoft's Cloud OS vision becomes a reality with the release of Windows Server 2012 R2 and System Center 2012 R2.

Whether you're new to the Windows Azure platform or are already using it in your business, this book has something that should interest you. Most Windows Azure services are described in some detail, with screenshots used to demonstrate some of the multitude of capabilities of the platform. And for the experienced we have lots of under-the-hood insights and expert tips written by Microsoft insiders who develop, test, and use the Windows Azure platform.

So whatever your goals are in reading this book, you're going to find new things about the Windows Azure platform that will amaze and delight you. Because, as you'll soon see in Chapter 1, Windows Azure can be anything you want it to be!

About the companion content

The companion content for this book can be downloaded from the following page:

http://aka.ms/IntroAzure/files

The companion content includes the Windows PowerShell script and some code samples from sidebars in chapters 2 and 4 of this book.

Acknowledgments

Three groups of people have helped make this book possible, and as author I'd like to thank them all here.

First, the following experts at Microsoft have contributed sidebars that explain and demonstrate different aspects of the Windows Azure platform:

- Ashish Goyal
- Brian Hitney
- Clemens Vasters
- Eric Mattingly
- Hai Ning
- Hanu Kommalapati
- John Savill
- Mike Gaal
- Nikhil Sachdeva
- Paulo Almeida Tanaka
- Robert Nottoli
- Yuri Diogenes

Second, the following Microsoft insiders have peer reviewed the content of this book to help us ensure it's as accurate as possible:

- Hanu Kommalapati
- Ivan Aspillaga Velasco
- Manoj K Jain
- Simon Hart
- Steve Espinosa
- Tal Ben-Shalom

Finally, I'd also like to thank Valerie Woolley, Content Project Manager at Microsoft Press; Christian Holdener at S4Carlisle Publishing Services; and copyeditor Andrew Jones.

Errata & book support

We've made every effort to ensure the accuracy of this content and its companion content. Any errors that have been reported since this content was published are listed on our Microsoft Press site:

http://aka.ms/IntroAzure/errata

If you find an error that is not already listed, you can report it to us through the same page.

If you need additional support, email Microsoft Press Book Support at *mspinput@microsoft.com*.

Please note that product support for Microsoft software is not offered through the addresses above.

We want to hear from you

At Microsoft Press, your satisfaction is our top priority, and your feedback our most valuable asset. Please tell us what you think of this book at:

http://www.microsoft.com/learning/booksurvey

The survey is short, and we read every one of your comments and ideas. Thanks in advance for your input!

Stay in touch

Let's keep the conversation going! We're on Twitter: *http://twitter.com/MicrosoftPress*.

CHAPTER 3

Windows Azure network services

Windows Azure network services provide the foundation for building hybrid cloud solutions for your business. Windows Azure Virtual Network lets you securely connect your cloud infrastructure to your on-premises datacenter. Windows Azure Traffic Manager allows you to control how user traffic is distributed to cloud services. Windows Azure also includes a name resolution service you can use for internal hostname resolution within a cloud service. This chapter provides an overview of the different network services in Windows Azure and includes insights from product team experts concerning how these services relate to one another, what you can do with them, and how you can use them.

Virtual Network

In the past when you needed to add more servers to your datacenter to handle increasing demand, you had to obtain the necessary hardware and deploy operating systems and applications on your new systems. Such tasks were generally time consuming to perform—hardware procurement can particularly be a bottleneck because of your organization's budgeting process as well as vendor delivery timing.

With the Windows Azure platform, however, you can now easily extend your on-premises datacenter into the cloud, and Windows Azure Virtual Network is key to making this possible. For example, you can use Virtual Network to create and manage a virtual network that uses a private IPv4 address space in Windows Azure. You can also use Virtual Network to create a secure link between your on-premises IT infrastructure and your virtual network in Windows Azure. By creating a hybrid IT infrastructure that combines your on-premises network and your virtual networks in Windows Azure, you can securely connect your cloud-based applications to your on-premises information systems.

Virtual Network can be used with other Windows Azure services such as Virtual Machines. For example, you can use Virtual Network to provide connectivity between virtual machines provisioned using Windows Azure Virtual Machines. This approach is ideal—for example, if you want to run a Microsoft SharePoint farm in Windows Azure. Virtual Network can also be used with Cloud Services. By default, all virtual machines running in the same cloud service can already communicate with each other without

the need for you to create a virtual network for this purpose. By creating additional virtual networks, however, you can also enable virtual machines running in different cloud services to talk to each other.

Creating virtual networks

The best way to become familiar with Virtual Network is to start creating virtual networks. Begin by opening the Windows Azure Management Portal, select the Virtual Network tab on the left and then click the New button in the command bar at the bottom. The command bar expands, as shown in Figure 3-1, and displays the different options available for creating and configuring virtual networks.

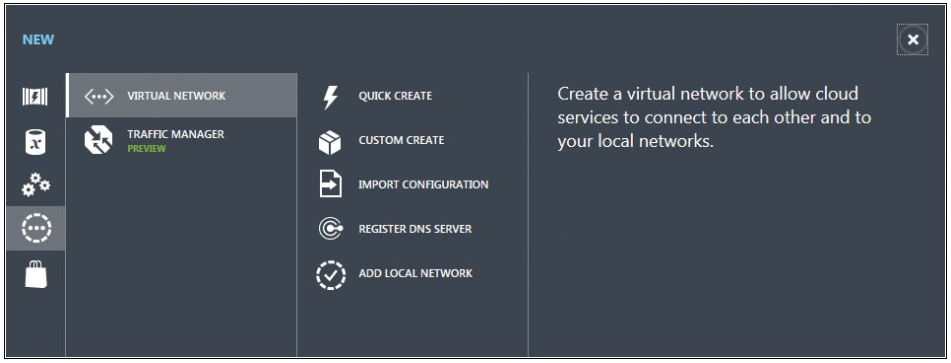


FIGURE 3-1 The command bar offers options for creating virtual networks.

The Quick Create option lets you create a basic virtual network which you can then further configure later on. Custom Create lets you configure your virtual network as you create it, while Import Configuration lets you configure a virtual network by importing an XML configuration file. The remaining options allow you to register DNS servers for your virtual network and add your local network for cross-premises connectivity.

Selecting the Custom Create option launches the Create A Virtual Network wizard. Figure 3-2 shows what the first page of this wizard looks like if this is the first virtual network you are creating. Because virtual networks must be associated with an affinity group, you must create a new affinity group if you haven't done so previously. An affinity group is a logical grouping of Azure services that tells Windows Azure where to locate the services in order to optimize the performance of cloud applications. When you create a new affinity group you must specify the geographical region where your affinity group will reside. For example, Figure 3-2 shows an affinity group being created in the "West US" region. Then if we later create a storage service in the same affinity group, Windows Azure will know that it should locate the storage in the "West US" location in order to optimize performance with other cloud services in the same affinity group.

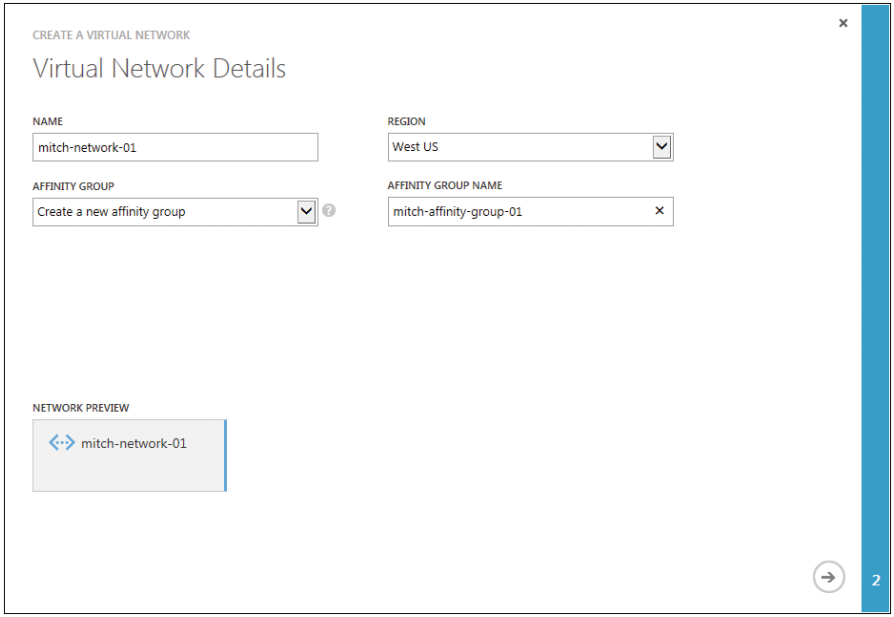


FIGURE 3-2 You can specify the Name and Affinity Group for the virtual network.

The next wizard page. shown in Figure 3-3, allows you to add DNS servers to your virtual network for name resolution. See the sidebar titled "Windows Azure and DNS name resolution" later in this section for more information on the different ways you can configure DNS name resolution for Windows Azure.

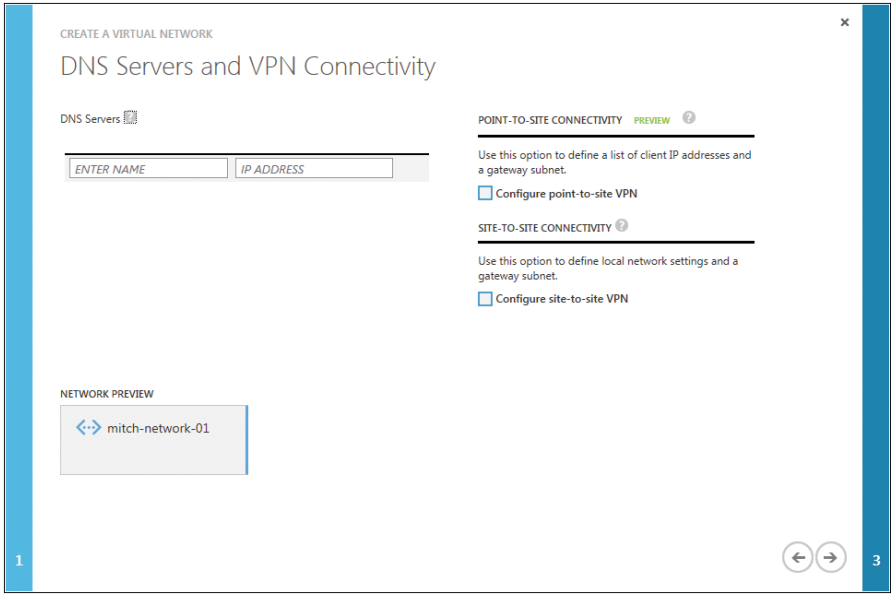


FIGURE 3-3 You can specify DNS servers and VPN connectivity options.

You can also use the wizard page shown in Figure 3-3 for configuring two kinds of VPN connectivity:

- **Point-To-Site Connectivity** Selecting this option displays an additional wizard page where you can define the address space for VPN clients that will connect to your virtual network from outside your virtual network space. This feature is currently in preview at the time of writing.
- **Site-To-Site Connectivity** Selecting this option displays an additional wizard page where you can define the VPN device IP address and address space used by clients connecting your virtual network from a remote site. You might use this option, for example, to establish a secure site-to-site VPN connection between your on-premises corporate network and your virtual network in the cloud. For more information on this feature and how to configure it, see the expert sidebar titled "The secure door to hybrid IT—Windows Azure site-to-site VPN" from a Microsoft insider later in this section.

If you haven't selected either of the two options above, the next and final wizard page shown in Figure 3-4 is where you can add address spaces and subnets to your virtual network. By default, the address space 10.0.0.0/8 is automatically added and the subnet 10.0.0.0/11 created, but you can edit both of these to change your virtual network addressing if desired, for example by changing the address space to 172.16.0.0/12 or 192.168.0.0/16 or something different. Only private IP address ranges can be specified as address spaces however.

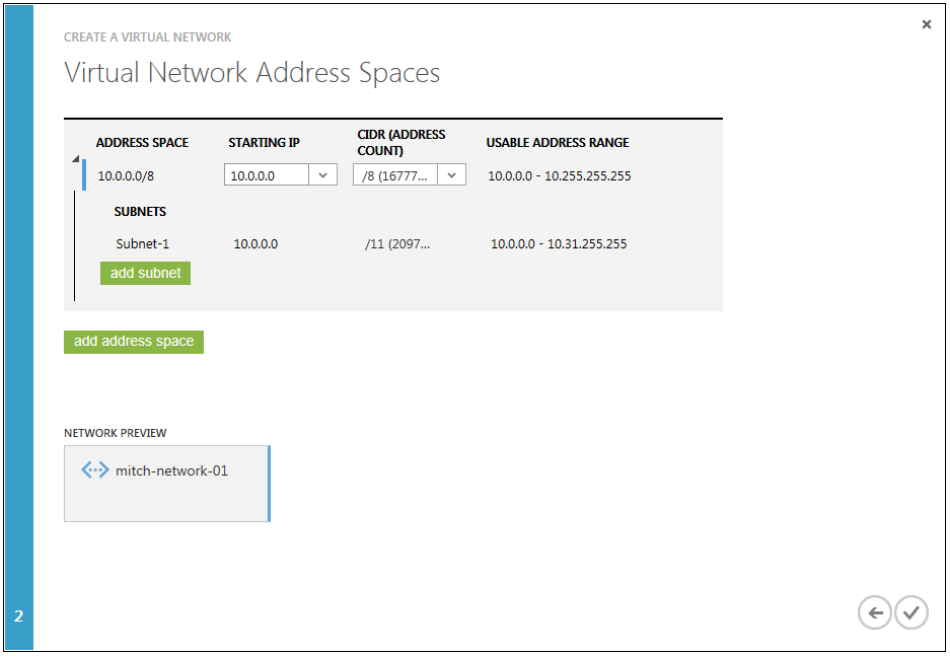


FIGURE 3-4 You can specify address spaces and subnets.

Windows Azure and DNS name resolution

Before you begin deploying virtual machines or role instances in Windows Azure, you need to consider and plan for how the DNS names of these virtual machines will be resolved from your on-premises network. Windows Azure provides its own name resolution service that can be used for resolving instance names within the same cloud service. For example, if you have two virtual machine instances named SRV-A and SRV-B running within the same cloud service named CLOUD-C, you don't need to deploy and configure a DNS server in order for each server to resolve the fully-qualified domain name of the other server.

If, however, your virtual machine instances are running in separate cloud services, Windows Azure name resolution won't suffice. You'll need to use a DNS solution of your choice for such purposes, for example a public DNS server, a DNS server belonging to your Internet service provider, or a DNS server on your corporate network.

For a comprehensive list of the different name resolution scenarios possible for Windows Azure and the solutions you can choose from, see *http://msdn.microsoft.com/en-us/library/windowsazure/jj156088.aspx*.

Once you've created one or more virtual networks in Windows Azure, you can associate a virtual network subnet with a virtual machine when you create the virtual machine using the procedure shown previously in Chapter 2, "Windows Azure compute services." For example, Figure 3-5 shows a new virtual machine being created and associated with a previously created cloud service named mitch-test-all and with the Subnet-1 (10.0.0.0/11) virtual network subnet.

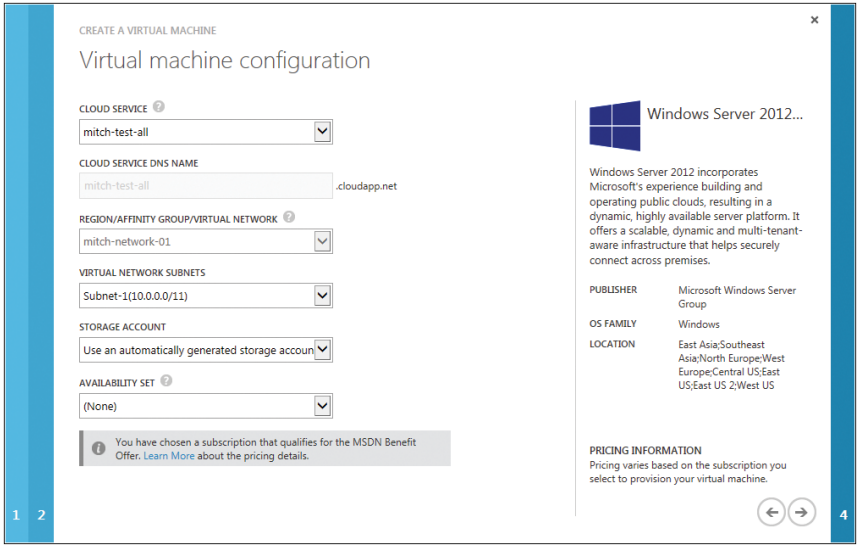


FIGURE 3-5 You can specify a virtual network to use when creating a new virtual machine.

Creating multiple virtual machines associated with the same cloud service and same virtual network subnet is a great way to quickly create a test network of servers in Windows Azure. Figure 3-6 shows three virtual machines associated with the mitch-test-all cloud service and the Subnet-1 virtual network subnet. To display this information, we first selected the Cloud Service tab on the left of the Management Portal. Next, we selected mitch-test-all from the list of cloud services displayed. Finally, we selected the Instances tab to show all virtual machine instances running in this cloud service.

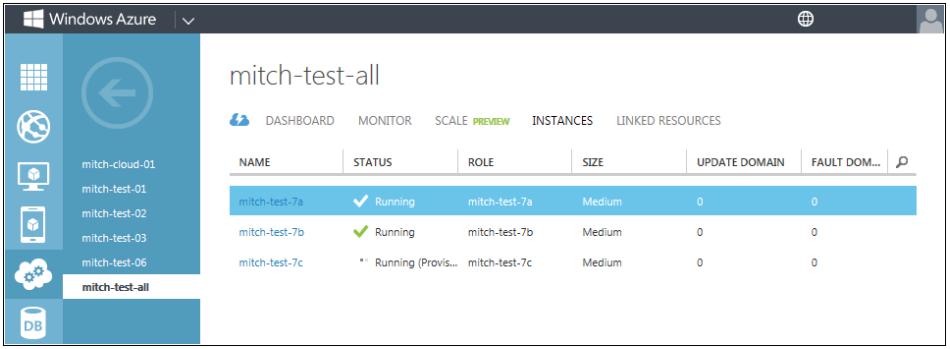


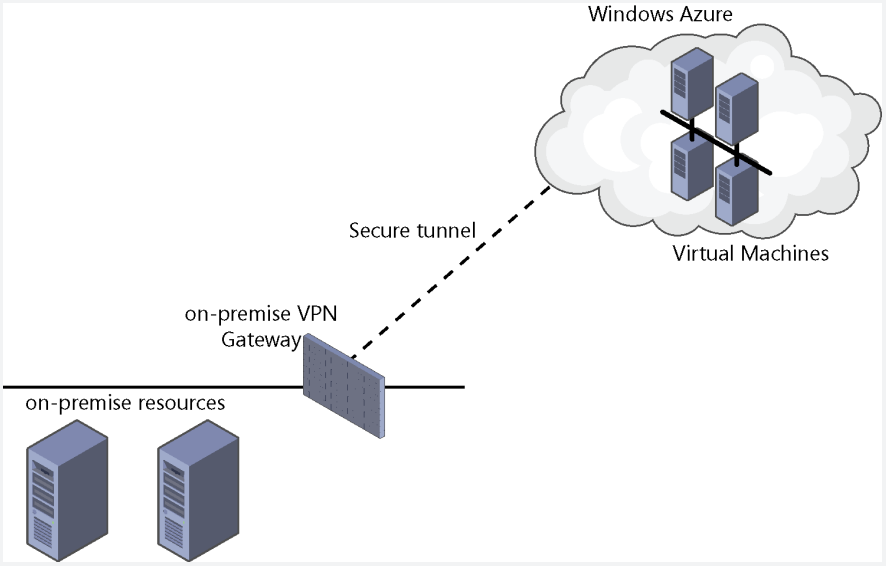
FIGURE 3-6 Three virtual machine instances are running in the same cloud service and on the same virtual network.

If we then selected each virtual machine in turn and displayed its dashboard page, we would see that Windows Azure has assigned the first three available IP addresses in Subnet-1 to the virtual machines, namely the addresses 10.0.0.4, 10.0.0.5, and 10.0.0.6.

The Secure door to hybrid IT—Windows Azure site-to-site VPN

Many companies have already realized the potential that cloud computing has to offer. However, some of these companies opted to invest more in building their own private cloud infrastructure in house. Many of these companies moved to this solution primarily because there were security concerns regarding moving their entire data to a public cloud provider. While private cloud is certainly a very good approach to take full advantage of the essential characteristics of cloud computing, there is more on the horizon for companies that are looking for agility, security, and elasticity. It is exactly on this context that hybrid cloud is turning into a great investment. Companies can now decide what data goes to a public cloud provider and what stays on-premises. What are the scenarios where the return on investment to have VMs in the cloud is better than having them on-premises? Hybrid cloud enables companies to have the best of both worlds: cloud computing and on-premises resources.

With Windows Azure IaaS, companies do not have the capability of instantiating VMs on Windows Azure and securely accessing these VMs from their resources onpremises. This is done using a site-to-site VPN between the on-premises VPN gateway and Windows Azure gateway, as shown in the following diagram:



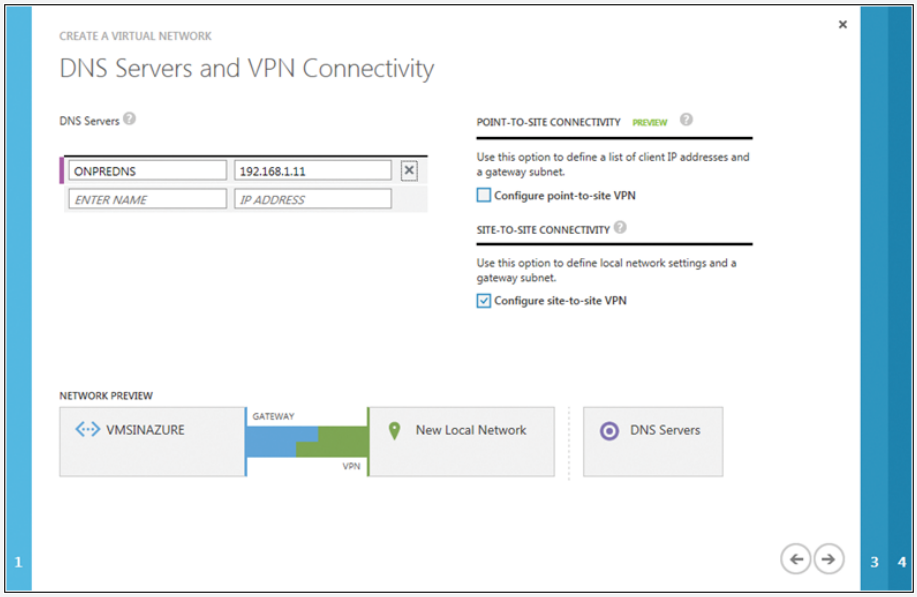
In order to set up a site-to-site VPN with Windows Azure gateway, the on-premises VPN device must support IKE v1 or IKE v2. Keep in mind that if you use IKE v1, Windows Azure will only support static routing. IKE v2 which uses dynamic routing is currently in preview at the time of writing. For a list of supported VPN devices and settings that must be used, see *http://msdn.microsoft.com/en-us/library/windowsazure/jj156075.aspx*.

This setup enables companies to rapidly and securely deploy VMs in Windows Azure. There are many scenarios that this setup can be used for such as development and testing. You can setup VMs in Windows Azure to be accessed from on-premises workstations to validate and test applications. The rapid instantiation of resources can assist you with quickly validating applications before they go to production.

Companies can also take advantage of the following capabilities in Windows Azure in order to make the solution highly available and enhance the overall security:

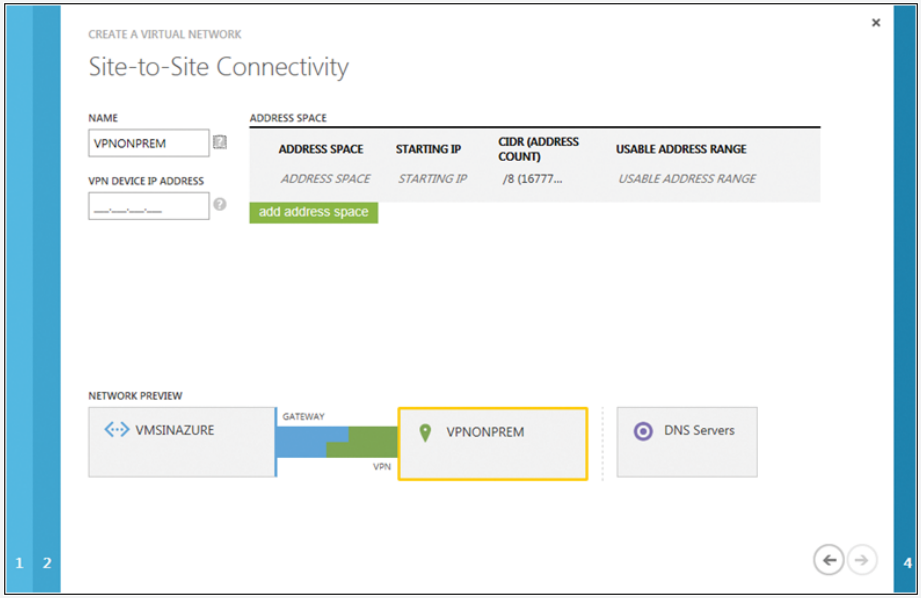
- Windows Azure Load Balancing
- Windows Azure Active Directory
- Windows Azure Autoscale

In order to implement the first step of this setup you will need to create a virtual network to host the VMs and the Windows Azure gateway. When you launch the Create A Virtual Network wizard, you will have the option to select Site-To-Site Connectivity, as shown here:



On this page you can also specify the DNS Server that will be used by the VMs that are instantiated on this virtual network. Since you want to have connectivity with the on-premises resources, you should type the DNS Server name and IP Address for the DNS located on-premises. The next step is to specify the On-Premises VPN Device name and IP address, as shown here:

It is very important that your on-premises device has the configuration and it is on the supported list of devices. For a list of supported VPN devices and settings that must be used, see *http://msdn.microsoft.com/en-us/library/windowsazure/jj156075.aspx*. Once you finish this setup, the Windows Azure gateway will be created and the public IP address of the device will be provided to you. At this point, you should start the configuration on your on-premises VPN device.



For a comprehensive scenario, considerations, and implementation of a hybrid IT solution, read the "Hybrid IT Infrastructure Solution for Enterprise IT" article set at *http://aka.ms/hybriditinfrastructuresolution*. In this document set, produced by our team (*http://technet.microsoft.com/en-us/cloud/private-cloud*), we describe in detail how to plan, design, and implement a solution that leverages all those capabilities and more.

Yuri Diogenes
Sr. Technical Writer

Learn more

For general information about Windows Azure Virtual Network and for purchase options and pricing details, see *http://www.windowsazure.com/en-us/services/virtual-network/*.

For more detailed information on what Windows Azure Virtual Network is and for tutorials on how to create and configure different kinds of virtual networks, see *http://www.windowsazure.com/en-us/documentation/services/virtual-network/*.

Additional documentation on Windows Azure Virtual Network can be found on MSDN at *http://msdn.microsoft.com/en-us/library/windowsazure/jj156007.aspx*.

Traffic Manager

Traffic Manager is another network service available with Windows Azure. Traffic Manager lets you load balance incoming traffic across multiple hosted Windows Azure services regardless of whether they're running in the same datacenter or in different ones at different geographical locations around the world. By using Traffic Manager, you can distribute users to the "best" location in your Windows Azure cloud solution to ensure high performance, availability, and resiliency for your cloud-based applications.

Traffic Manager is currently in preview at the time of writing and is free of charge.

Using Traffic Manager

Traffic Manager works by applying an intelligent policy engine to DNS queries for your domain names. To use Traffic Manager, you simply create configurations using the Management Portal. A Traffic Manager configuration consists of a profile, a definition, a policy, and monitors. A profile contains a domain name prefix that you create and is visible in the Management Portal. The definition contains the policy settings and monitor settings for the profile. Policy is where load-balancing methods and endpoints are specified. And monitors are where the DNS timeout, protocol, port, and relative path are specified. The process by which Traffic Manager routes traffic is explained in detail at *http://msdn.microsoft.com/en-us/library/windowsazure/hh744833.aspx*.

Traffic Manager provides you with a choice of three load-balancing methods: performance, failover, or round-robin:

- **Performance** This method directs traffic to the closest service based on network latency.
- **Round-robin** This method distributes traffic equally across all services.
- **Failover** This method directs traffic to the backup service if the primary service fails.

As Figure 3-7 shows, you can select the load-balancing method you want to use when you use the Quick Create option to create a new Traffic Manager profile using the Management Portal.

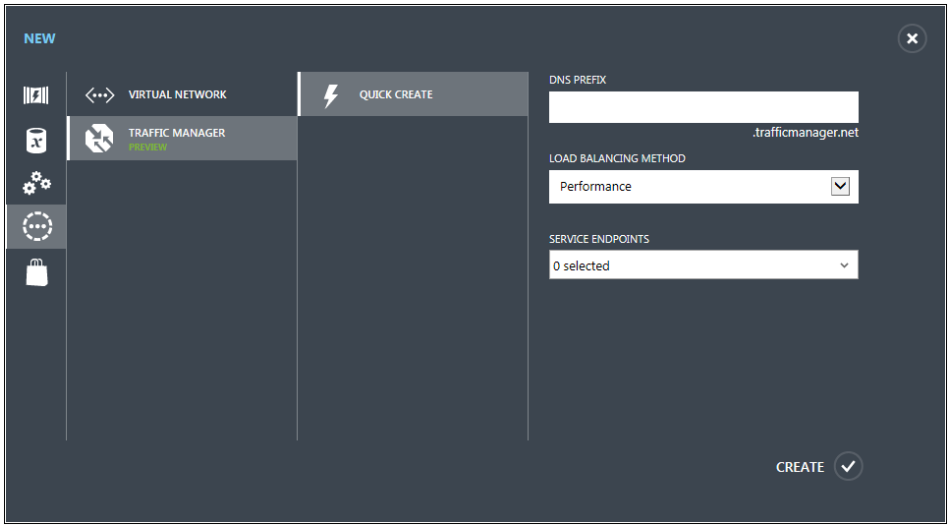


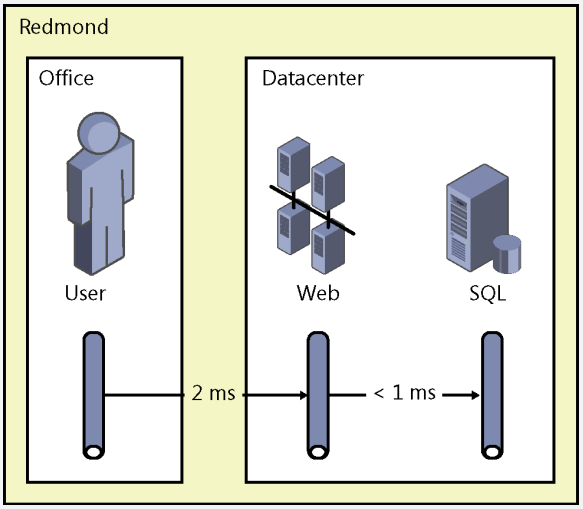
FIGURE 3-7 You can choose the load-balancing method when creating a new Traffic Manager profile.

For further information on how to plan and implement Traffic Manager for your cloudbased applications, see the links under "Learn more" at the end of this section. But first let's here from one of our insiders at Microsoft on why you need to consider network latency when planning your cloud-based applications.

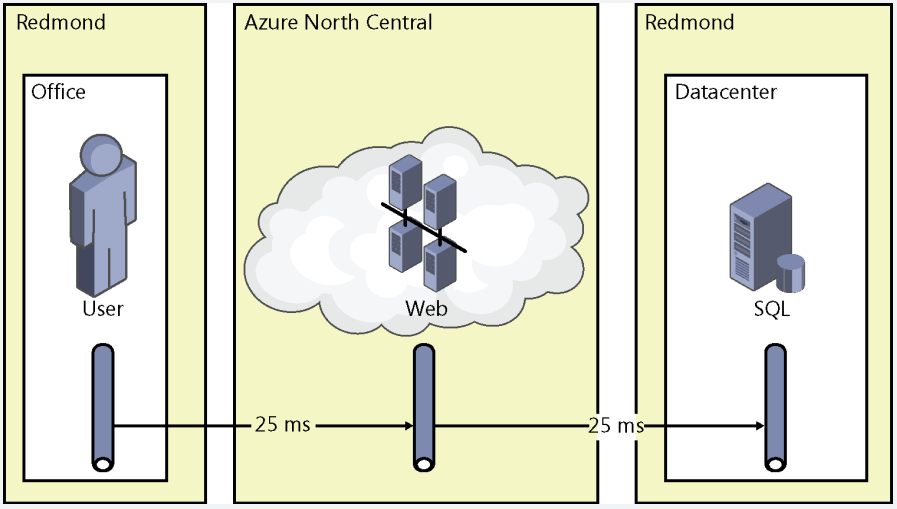
Impact of network latency on hybrid applications

When building hybrid applications, either by migrating an existing app or building net-new, it's important to understand the impact that network latency may have. When Microsoft IT began to explore migrating applications to a hybrid model, we realized quickly that our applications might not respond perfectly to going hybrid.

Take a classic two-tier application. In its original topology the users, web servers, and SQL servers were all within a few milliseconds of each other.



We wanted to move just the web servers into Windows Azure and keep SQL onpremises. By doing this, we suddenly introduced over 50 milliseconds of latency into a topology which previously was under 5 milliseconds! Needless to say, the application was never tested under these conditions....



How did our application react? Not well. We experienced a range of performance problems from general slowness to timeouts. Typically, the worst impact was seen when we were performing a high number of operations while passing large amounts of data.

We learned that the key is to be "chunky" instead of "chatty" over high-latency connections. Sometimes this may mean only a few changes while other times it

might mean a redesign. In our situation, we analyzed all the calls to SQL and noticed hundreds of redundant calls for a single page click due to Entity Framework. When fully on-premises, this was never noticed as the performance was still acceptable and the SQL calls took milliseconds.

Latency will also potentially impact on the "last mile" as well. Our application users sat within 1 millisecond of the datacenter but after migrating the web front ends to Windows Azure that changed to 25 milliseconds. This is thankfully more commonly tested as you are unable to completely control a user's latency to your application.

Now if it's a new hybrid application, we design with latency in mind. We try to use both Windows Azure Cache and the CDN to get data as close to users or the servers as possible. If migrating, we test the application using software network emulators beforehand so we know upfront what the experience may be.

While it's impossible to say exactly how latency might affect your application, it's something to look out for.

Eric Mattingly
Service Engineer, Microsoft IT – Enterprise Commerce

Learn more

For general information about Windows Azure Traffic Manager and for purchase options and pricing details, see *http://www.windowsazure.com/en-us/services/traffic-manager/*.

For more detailed information on what Windows Azure Traffic Manager is, how it works, and how to plan and implement its use, see *http://www.windowsazure.com/en-us/documentation/services/traffic-manager/*.

For a short walkthrough of configuring Traffic Manager to help make a cloud service highly available and reliable, see the post titled "Windows Azure July Updates: SQL Database, Traffic Manager, Autoscale, Virtual Machines" in Scott Guthrie's blog at *http://weblogs.asp.net/scottgu/archive/2013/07/23/windows-azure-july-updates-sql-database-traffic-manager-autoscale-virtual-machines.aspx*.

For a demonstration of Traffic Manager, see the Microsoft TechEd 2012 presentations titled "Overview of New Networking Features in Windows Azure," which is available for viewing and download from Channel 9 at *http://channel9.msdn.com/Events/TechEd/NorthAmerica/2012/AZR304*.