



# Windows Azure IaaS for Hybrid Cloud Fast-track

An approach to deliver hybrid cloud solutions

*Prepared for*  
**Windows Azure customers**  
**Monday, 20 May 2013**  
**Version 1**

*Prepared by*  
**Patrick Butler Monterde**  
Cloud Architect  
**Jim Priestley**  
Windows Azure TSP

*Contributors*  
*Martijn Hoogendoorn*  
*Cloud Architect*



## Revision and Signoff Sheet

### Change Record

Date	Author	Version	Change reference
2/18/2012	PBM	.1	Initial draft for review/discussion.
2/22/2013	PBM	.2	Added all sections. Ready for Review.
3/15/2013	PBM	.3	Added feedback and updated.
4/15/2013	PBM	1.0	Completed all sections. Verified.

### Reviewers

Name	Version approved	Position	Date
Martijn Hoogendoorn	.2	Cloud Architect	3/12/2013
Pete Schnettler	.7	Azure Architect	4/10/2013
Marc Mercuri	.8	Sr. Director ESWAT	4/12/2013
Mark Kottke	.9	Cloud Architect	4/13/2013

## Table of contents

<b>1</b>	<b>Abstract</b>	<b>1</b>
<b>2</b>	<b>Discovery</b>	<b>3</b>
2.1	Customer's network environment	3
2.2	Applications' servers and locations	4
2.3	Identifying target workloads	5
2.4	Backup procedures	5
2.5	Active Directory and security topology	5
<b>3</b>	<b>Education</b>	<b>7</b>
3.1	Windows Azure features	7
3.2	Managing and monitoring hybrid cloud	7
3.3	SharePoint deployments	8
<b>4</b>	<b>Planning</b>	<b>9</b>
4.1	Identity management (AD DS/other), DNS, and security	9
4.2	Network topology	11
4.3	Virtual machine templates	12
4.4	Windows Azure subscriptions and support	13
<b>5</b>	<b>Basic Implementation</b>	<b>15</b>
5.1	Sample deployment scenario	15
5.2	Deploy the network	16
5.2.1	Create an affinity group	16
5.2.2	Create the Virtual Network	17
5.2.3	Create the local network	19
5.2.4	Create the VPN gateway	20
5.2.5	Configure the customer router for the VPN	21
5.3	Deploy the first server	23
5.4	Testing virtual machine network connectivity	25
5.5	Management of public endpoints	26
5.6	Configure Active Directory and DNS	26
5.7	Create virtual machine images from a deployed virtual machine	27
5.8	Add customer VHD images to the Windows Azure Gallery	27
<b>6</b>	<b>Management of the IaaS Deployment</b>	<b>29</b>
6.1	Use the Windows Azure Management Portal	29
6.2	Use the Windows Azure PowerShell Cmdlets	30
6.2.1	Preparing to use Windows Azure PowerShell	30

6.2.2	Example Windows Azure PowerShell Cmdlets .....	31
6.3	System Center App Controller .....	34
6.4	System Center Orchestrator .....	34
6.5	Using the Windows Azure Service Management Rest API .....	35
<b>7</b>	<b>Appendix A: Educational resources .....</b>	<b>36</b>
7.1	Learning Windows Azure IaaS .....	36
7.2	Learning Windows Azure Virtual Networking .....	36
7.3	Disks, Images and VHDs Management .....	36
7.4	Active Directory, DNS and Security .....	37
7.5	Managing with Windows PowerShell and System Center .....	37
7.6	Understanding the Azure Billing Model for IaaS .....	38
7.7	SharePoint deployment on Windows Azure Virtual Machines .....	38
7.8	Deploying databases in Windows Azure IaaS.....	38
<b>8</b>	<b>Appendix B: Workshop opportunities .....</b>	<b>39</b>
8.1	3-day workshop .....	40
8.2	5-day workshop with an existing System Center 2012 SP1.....	40
8.3	5-day workshop without System Center .....	42
8.4	10-day workshop .....	43
<b>9</b>	<b>Appendix C: Checklists.....</b>	<b>46</b>
9.1	Discovery checklist.....	46
9.2	Planning checklist .....	49
<b>10</b>	<b>References and Bibliography.....</b>	<b>50</b>

# 1 Abstract

As our customers take on Windows Azure and other cloud technologies, they are realizing the multiple advantages and challenges of cloud computing. Cloud computing provides substantial return on investments (ROI), great agility, and reductions on services and operational costs. The decisions our customers had to make have been to port or migrate their applications to either Platform as a Service (PaaS) or Infrastructure as a Service (IaaS) cloud models.

PaaS is a very compelling cloud model, however for some scenarios like legacy applications, customers have found that there are a lot of challenges while migrating. Now, with the introduction of cloud features that enable customers to safely connect their private cloud to a public cloud and to run some tiers of those applications in an IaaS model, more opportunities are available to take advantage of the benefits that hybrid cloud solutions provide.

There is a continuum of opportunities from a lift and shift, bursting, to the ability to forklift the applications in IaaS and extend them into PaaS to get the maximum cost savings and return on investment.

Customers are attracted to hybrid cloud solutions because they provide the ability to extend their applications into the cloud to solve capacity planning, TCO, and time to market challenges. In addition, they also provide a greater sense of control because customers can use the same security controls and monitoring tools that they are currently using in their on-premise deployments.

Hybrid cloud also has its challenges, including the following most common challenges that customers face when implementing hybrid cloud solutions:

- Security and identity
- Data center distributed architectures
- Disaster recovery
- Business continuity
- Monitoring and application management
- Consolidating hardware/network/systems/software support
- Identifying technical resources with hybrid cloud know-how

To address the impact of these challenges, there is a need to provide a straightforward approach and to help customers implement hybrid cloud solutions using Windows Azure IaaS.

Based on the experiences of multiple customers and partners, this paper provides enterprise architects, consultants, and partners with a fast-track approach to deliver Windows Azure hybrid cloud solutions to customers. To make this approach more comprehensive it has been divided into the following steps:

Steps	Description
<b>Discovery</b>	The Discovery step enables us to understand the customer's infrastructure and environments used by the applications that we are going to move (partially) to Windows Azure and will also help to determine how we can better connect both environments to form the hybrid cloud. At the completion of the Discovery step you will have a series of artifacts (network diagrams, lists of assets that comprise the application, and so on) that will be used in next step.

Steps	Description
<b>Education</b>	The Education step provides time for knowledge transfer of Windows Azure and hybrid cloud best practices to the customer. The time spent on this step depends on the customer's knowledge. Appendix A contains a detailed list of resources for the relevant knowledge areas, and Appendix B could benefit the customer by providing them with practical and detailed insight.
<b>Planning</b>	The Planning step starts by defining and preparing the features needed to create the hybrid cloud environment. It focuses on the application's identity, DNS, security, network topology, Windows Azure Virtual Machine templates, and so on.
<b>Basic Implementation</b>	The Basic Implementation step provides best practices and checklists of the requirements for a successful application's hybrid cloud implementation.
<b>Management of the IaaS Deployment</b>	The Management step provides a list of common IaaS deployment scenarios with the tools and best practices required to properly manage and monitor the application's hybrid cloud implementation.

In addition, this paper includes the following information:

- **Appendix A: Educational resources.** This appendix provides an organized list of resources to educate the customer and to address most of the questions that they will have regarding Windows Azure, monitoring and management, security, and hybrid cloud.
- **Appendix B: Workshop opportunities.** Appendix B provides a list of templates and best practices to execute Windows Azure hybrid cloud workshops to customers.
- **Appendix C: Checklists.** This appendix provides checklists to facilitate the discovery and planning discussions with customers.

## 2 Discovery

The Discovery step provides insights into the customer's IT infrastructure and environments where the applications to be connected to the cloud exist. In this step the focus is on understanding the following areas:

- Customer's network environment
- Applications' servers and locations
- Identifying the target workloads
- Backup procedures and compliance requirements
- Identity (Active Directory) and security topology

At the end of the Discovery step, you will have a lot of information. This information will be used in the planning and implementation step. Check **Appendix C** for the Discovery checklist.

We also recommend to review the VRF Accelerator for Application Portfolio Assessment and Cloud Migration<sup>1</sup>. This tool will enable you to better identify and qualify target workloads.

### 2.1 Customer's network environment

The customer's network environment is key to enable connectivity between the on-premises environment and the public cloud. The following list defines the areas to explore and to obtain information from the customer:

- **Network diagrams.** Review, draw and collect the basic diagrams of the customer's network environment. The following are the key items to identify:
  - Router/firewall make and models
  - Edge firewall firmware Level
  - Edge IP address or range
  - Number and size of current Internet connections (primary, fail over, burstable)
  - Do ISP contracts allow bandwidth increase?
  - List of all network ranges in use on the customer's wide area network (WAN). For example, 10.0.0.0/16
  - Network policies around subnet assignments. How are subnets assigned now and will this policy extend to the Azure Virtual Network.
- **Perimeter network (also known as DMZ, demilitarized zone, and screened subnet).** Most customers have a perimeter network. Identify whether this perimeter network is relevant for the project and has any impact for the applications to be hybrid cloud-enabled. Identify
  - Firewall ports open
  - IP address range
- **Customer IT software stack bandwidth and port requirements.** Most customers will have an IT software stack to perform security, monitoring, and telemetry tasks for their applications. It is important to know what parts of the stack will be also installed in the IaaS virtual machines along with:

---

<sup>1</sup> Microsoft, , Application Portfolio Assessment and Cloud Migration Planning VRF Accelerator, <https://campus.partners.extranet.microsoft.com/esportal/Library/IP/Forms/Document%20Set/docsethomepage.aspx?ID=2014&FolderCTID=0x0120D520007E465FED93236A4F8535853D09D739A0&List=8b3507dc-f672-46bc-84c1-166758b96d95&RootFolder=%2Fesportal%2FLibrary%2FIP%2FVRF%2FVRF%20Accelerators%2FIT%20Led%20Change%2FApplication%20Portfolio%20Assessment%20and%20Cloud%20Migration%20Planning%20VRF%20Accelerator/>, 2013



- Understand purpose (development/public web hosting)
- IT software stack bandwidth requirements:
  - Syslog server
  - Diagnostics
  - Antivirus and security software
  - Any custom application loggers that they may be using
- Do they have a management system deployed, such as System Center?
- Software versions
- Memory Requirements
- Storage Requirements
- Hardware requirements. For example, the need of multiple NICs
- Components deployed

**Note:** It has been our experience with some customers that there is an uneasiness to disclose network information. Our recommendation is to clearly explain to the customer that the network information requested is to identify any possible issues regarding the connectivity and security of the application to be moved into the hybrid cloud model. For Windows Azure, we have two main ways to enable this connection: Windows Azure Service Bus and Windows Azure Virtual Network. Make sure to explain those options and their requirements in the Education step.

## 2.2 Applications' servers and locations

Identify the hardware on which the on-premises applications are running. Understand if those machines have been virtualized and if they are part of:

- **Physical or virtual servers.** Customers have a mix of physical and/or virtual servers running their applications. Take special note to the virtualization technologies utilized:
  - VMWare
  - Hyper-V
  - Others (such as Xen, OpenVZ, Virtual Box, and so on) because we need to be able to convert foreign images into Hyper-V later on
  - Static Address Required

**Note:** Understanding the virtualization layers used by the application will help streamline the movement of virtual machines to Windows Azure. In addition, review if the application needs to run in 32bit environment, since it may require specific hardware or/and drivers to properly function.

- **Server locations.** Where are the servers located? Are the applications distributed in multiple data centers? On the perimeter network?

**Note:** Applications that span multiple data centers bring more challenges. It is important to understand connectivity and latencies between data centers, security (VPN, direct patching), and the network gateways (routers/firewall) used.

## 2.3 Identifying target workloads

Identify the workloads and applications in those workloads that are going to be migrated to Windows Azure. Take special attention to understand all the applications involved in the workload, the network latency SLAs for each application and any required IT stack application:

- Identify workloads and applications:
  - Microsoft products
  - Third-party applications
  - Required customer's IT software stack to be installed in the Windows Azure Virtual Machines
  - Network latency SLA for the application(s) and components in the workloads?

**Note:** One of the great challenges of hybrid cloud is network latency. Understanding the latency requirements between components/applications inside a workload will determine what application's tiers can be migrated to the cloud and which ones need to stay on-premises. If network latency SLAs are not available, it would be helpful to perform tests to determine the network latencies. For some workloads, such as SharePoint latency and bandwidth, SLAs have been published.<sup>2</sup> Other workloads may require research.

In addition, identify the current physical or/and virtual servers that are targeted to be migrated into Windows Azure IaaS Virtual Machines. The following items need to be understood:

- List servers targeted for migration to Windows Azure
- Operating system
- Number of CPU cores and speed
- Amount of RAM
- Number and size of disk volumes
- Special I/O considerations, for example the number of IOPS needed

## 2.4 Backup procedures

The customer's backup and disaster recovery procedures will have an impact on how the application is configured. The main areas to inquire about include the following:

- How the workload's backups are currently performed?
- What are the data retention requirements?
- Are there any compliance requirements?
- What are the latency SLAs for the backup solution used?
- What disaster recovery and business continuity solutions/procedures are currently in place for the workloads to be moved to Windows Azure?

## 2.5 Active Directory and security topology

The last part of the Discovery step is to consider the identity solution used by the customer. Most Microsoft enterprise customers are using Active Directory Domain Services (AD DS) and Active Directory Federation Services (AD FS). Review with the customer both the AD DS and the security topology that is relevant for the workloads to be moved to Windows Azure:

---

<sup>2</sup> Roshan N. Y. "Guidance on Latency and Bandwidth for SharePoint 2010." MSDN Blogs, Sept. 20, 2012

- Active Directory Domain Services
  - Functional level
  - Number and location of AD DS servers
  - DNS topology. Is DNS deployed using AD DS integrated mode?
  - Are there any sub-domains?
- Are there corporate policies regarding the type of AD DS that can be deployed to the hybrid-cloud?
  - Core, limited trust, full, read-only?
  - What configuration can be deployed in Windows Azure?

**Note:** If the customer requires AD FS, gather specific information about how and where it needs to be configured.

### 3 Education

Hybrid cloud is a broad topic that touches multiple technologies, products, and architectures. Customers will come with very different levels of understanding about cloud and what it takes to move their workloads to Windows Azure. Therefore, it is critical to spend time with the customer to create a knowledge baseline regarding Windows Azure and the management and monitoring of hybrid clouds. This will provide a basis for highly productive and intelligent conversations when we address the planning and implementation step.

#### 3.1 Windows Azure features

Windows Azure is constantly adding new features. We recommend that you provide an overview of current and new features. The Windows Azure Team has done an excellent job supporting the Windows Azure Training Kit.

The Windows Azure Training Kit is the most complete and up-to-date training resource currently available. It includes hands-on labs, presentations, demos, and a training guide. One of the great features of this training is the quality of the labs and the PowerPoint presentations. We highly recommend using these presentations as a base for delivering specific content requested by the trainees.

- Windows Azure Training kit website available here: [Link](#)
- Windows Azure Training Kit presentations are available here: [Link](#)
- Windows Azure Training Kit Demos are available here: [Link](#)

In addition, the Windows Azure Training Kit contains a prebuilt training workshop agenda with multiple delivery choices that we will make use of:

Title	Content Type
<b>Day 1 - Introductory Day</b>	
<a href="#">Windows Azure Platform Overview</a>	Presentation
<a href="#">Windows Azure Compute</a>	Presentation
<a href="#">Windows Azure Storage</a>	Presentation
<a href="#">Intro to Windows Azure</a>	Hands-on Lab

Lead with The Windows Azure Training Kit and use the collateral in Appendix A to help you with Windows Azure features.

#### 3.2 Managing and monitoring hybrid cloud

Hybrid cloud includes multiple technologies, which makes the decision about what to spend time training on more difficult. The main areas that need to be understood if implementing a hybrid cloud solution in Windows Azure are the following:

Topic	Description	Resources
<b>Windows Azure Virtual Machines</b>	Understand how Windows Azure Virtual Machines are implemented and how they work.	Section 7.1
<b>Windows Azure Virtual Network</b>	Understand how to create and manage the network topologies that bridge between Windows Azure PaaS, Windows Azure IaaS, and on-premises deployments.	Section 7.2
<b>Windows Azure disks, images, and VHDs</b>	At the core of the Windows Azure Virtual Machines, Azure Storage blobs is the technology that supports the virtual machines, disks, images, and VHDs. It is fundamental to understand this technology to properly manage your virtual machines.	Section 7.3
<b>Windows Azure Active Directory and identity management</b>	Understanding how to provide single sign-on and to federate identity mechanics is key to transparently support the number of customers that will use the application. Also, understanding secure token services and how to integrate them in the hybrid cloud solution.	Section 7.4
<b>Windows Azure hybrid cloud management</b>	This step provides a list of common IaaS deployment scenarios with the tools and best practices required to properly manage and monitor the application's hybrid cloud implementation.	Section 7.5

### 3.3 SharePoint deployments

SharePoint farms are a very popular deployment that customers are interested in moving to a hybrid model. The reasons are quite diverse, but the most common scenarios that have been encountered in the field are as follows:

- **Disaster recovery / business continuity.** This scenario helps customers to use Windows Azure as a disaster recovery/business continuity site for their SharePoint farms. The scenario includes SharePoint farms in Active/Passive or Active/Active mode and also geo-distributed (deploying SharePoint farms in 2 Windows Azure data centers).
- **SharePoint development and test environments.** SharePoint development and test environments can be complex, expensive, and time-consuming to set up. Windows Azure hybrid model provides an automated way to create and re-create these SharePoint environments in a matter of minutes instead of days.
- **SharePoint farm growing pains.** A common scenario is successful SharePoint farms that grow faster than expected and need to support more users. The hybrid model provides a safe and secure way to extend those farms' resources.

The training resources for SharePoint deployments in Windows Azure hybrid clouds are not yet very extensive. However, the best resource to date is "SharePoint Deployment on Windows Azure Virtual Machines," which is available in Section 7.7 of this document.

## 4 Planning

The Planning step focuses on defining and preparing the features needed to create the hybrid cloud environment. In this step, we use the information gathered from the Discovery step and start planning the application's migration to Windows Azure. The main areas to address in this step are the following:

- **Identity management (Active Directory or other), DNS, and security.** The identity manager and provider(s) used, the DNS configuration and integration, the application's resiliency, the security configuration, and the software used that needs to be enabled in the hybrid cloud.
- **Network topology.** The network topology helps identify how to organize the application from a network traffic and visibility perspective. It defines the network isolation between application tiers. In addition, this area addresses the firewall and router configurations.
- **Virtual machine templates.** This area focuses on the virtual machine configuration, operating system, software (application servers, development server, and so on), the VHD attached to the virtual machines, and so on.

**Note:** For information regarding Windows Azure security and compliance, see the following site: [Windows Azure Security Guidance](#)

As a result of the Planning step you will have three artifacts (Appendix C: Planning Checklist):

- Document that describes the plan for identity management, DNS, and security
- Network topology diagram and associated documentation
- Virtual machine template list

### 4.1 Identity management (AD DS/other), DNS, and security

Verify with the customer the identity management system and providers that the application will support. Inquire about how the DNS will need to be configured, and also about security setup and resiliency requirements for the application. The following table identifies the main areas to plan for:

Topic	Description
<b>Active Directory</b>	Define whether the application's servers located in Windows Azure will be joined to the on-premises AD DS domain: <ul style="list-style-type: none"><li>○ Stand-alone forest</li><li>○ Sub-domain</li><li>○ Core-domain</li></ul> <p><b>Note:</b> If servers are Core or Sub-domain, plan for sites and subnets in AD DS.<sup>3</sup></p>

<sup>3</sup> Microsoft, Understanding Sites, Subnets, and Site Links, <http://technet.microsoft.com/en-us/library/cc754697.aspx>, TechNet, 2012.

Topic	Description
<b>Other identity providers</b>	<p>For other identity providers that need to be supported</p> <ul style="list-style-type: none"> <li>○ What trust relationships need to be set up?</li> </ul> <p><b>Note:</b> In Windows Azure, you can use Windows Azure Active Directory<sup>4</sup> and Windows Azure Access Control Service<sup>5</sup> to support other identity providers and set up trust relationships with third-party secure token servers (such as Ping Identity and Site Minder).</p>
<b>DNS</b>	<p>Determine the location of the DNS server—whether it’s going to be in Windows Azure or on-premises.</p> <p>Determine whether the application needs the DNS Server service integrated into the design and implementation of AD DS?<sup>6</sup></p>
<b>Security</b>	<p>Based on the customer’s IT security policies and procedures, determine:</p> <ul style="list-style-type: none"> <li>○ Development and test environments for the solutions been adequately isolated from production.</li> <li>○ Have the solutions deployed in the production environment been partitioned and reviewed for compliance, data protection, and security policies?</li> <li>○ If appropriate, select an antimalware solution.</li> <li>○ What will we implement as system loggers and monitors?</li> <li>○ Are security appliances (crypto boxes, honeypots, IDS) part of the application?</li> <li>○ Is there a current threat model for the application?<sup>7</sup> If not, we need to create one. If there is, we might need to get it updated given its new topology.</li> </ul> <p><b>Note:</b> In Windows Azure, you cannot deploy or install any hardware-based security devices in any of the Windows Azure data centers. Customers can install software-based security software in both PaaS and IaaS virtual machines.</p>

<sup>4</sup> Microsoft Corporation, Windows Azure Active Directory, Link: <http://msdn.microsoft.com/en-us/library/windowsazure/ji673460.aspx>, MSDN, 2013.

<sup>5</sup> Microsoft Corporation, Access Control Service 2.0, Link: <http://msdn.microsoft.com/en-us/library/windowsazure/hh147631.aspx>, MSDN, 2013.

<sup>6</sup> Microsoft Corporation, Active Directory Integration, [http://technet.microsoft.com/en-us/library/cc737383\(v=WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc737383(v=WS.10).aspx), TechNet 2005

<sup>7</sup> Microsoft, SDL Threat Modeling Tool, <http://www.microsoft.com/security/sdl/adopt/threatmodeling.aspx>, Microsoft.com, 2013

Topic	Description
<b>Resiliency</b>	<p>Determine the resilience needs for the application:</p> <ul style="list-style-type: none"> <li>○ Plan for data protection software/solutions that maybe required</li> <li>○ Review the resiliency requirements: <ul style="list-style-type: none"> <li>▪ Disaster recovery</li> <li>▪ Business continuity</li> <li>▪ Backups</li> </ul> </li> <li>○ Service level agreements (SLAs) for application availability and recovery.</li> </ul> <p><b>Note:</b> We recommend reviewing the “<a href="#">Failsafe: Guidance for Resilient Cloud Architectures</a><sup>8</sup>” paper for an overview of what is necessary to enable resilient cloud architectures.</p>

## 4.2 Network topology

This section will help you plan the network in which the application will be running. From the Windows Azure perspective, it’s important to consider two main areas:

- The Windows Azure Virtual Network<sup>9</sup> that will connect the application’s on-premises tier with the ones in the cloud. Also, we need to configure the network stack to tune the network performance.
- Firewall and router configuration and setup.

The following table identifies the main steps to follow:

Topic	Description
<b>Network</b>	<p>Verify and note the following items when planning the network topology for the application:</p> <ul style="list-style-type: none"> <li>○ Cloud service namespace</li> <li>○ Windows Azure subnets</li> <li>○ Gateway subnet</li> <li>○ DNS server</li> <li>○ Local network namespace(s)</li> <li>○ VPN gateway address</li> </ul>

<sup>8</sup> M. Mercuri, U. Homann, A. Townhill, Failsafe: Guidance for Resilient Cloud Architectures, <http://msdn.microsoft.com/en-us/library/windowsazure/jj853352.aspx>, Microsoft, 2012

<sup>9</sup> Microsoft Corporation, Networking, Link: <http://www.windowsazure.com/en-us/manage/services/networking>, WindowsAzure.com, 2013.



Topic	Description
<b>Firewall/router</b>	<p>From the information gathered in the Discovery step you should have the required information to verify whether the firewall/router that will be part of the VPN between the on-premises server and Windows Azure Cloud Services is a supported device.<sup>10</sup></p> <p>Planning is required to understand what changes need to be performed to configure and setup the VNP connectivity. Some of these tasks include:</p> <ul style="list-style-type: none"> <li>○ Sample firewall/router configuration script. This script should be examined by the customer and not conflict with the existing setup.</li> <li>○ Checking the following configuration settings: <ul style="list-style-type: none"> <li>▪ MTU max size 1350</li> <li>▪ NAT-T enabled</li> <li>▪ If in the Discovery step it was found that the firewall/router is behind another device, check that ports 500 and 4500 (for UDP and TCP, in and out) are open to the device.</li> <li>▪ Any special routing or ACLs required?</li> </ul> </li> </ul>

### 4.3 Virtual machine templates

The Planning step should have provided information regarding each one of the machine roles that will be part of the application. The application's roles/tiers that will be moved to Windows Azure will need to have virtual machines created. The following table provides pointers on the most relevant information you will need to plan for this process:

Topic	Description
<b>Planned Machines</b>	<p>For each application's tier, define the Virtual Machine's role:</p> <ul style="list-style-type: none"> <li>○ Active Directory/DNS?</li> <li>○ Database servers?</li> <li>○ Application servers?</li> <li>○ Development servers?</li> </ul>

<sup>10</sup> Microsoft Corporation, About VPN Devices for Virtual Network, Link: <http://msdn.microsoft.com/en-us/library/windowsazure/jj156075.aspx>, WindowsAzure.com, 2013.

Topic	Description
<p><b>For each virtual machine in the application's tier, provide the following information:</b></p>	<p>Verify and note the following items for each virtual machine:</p> <ul style="list-style-type: none"> <li>○ Number of cores (RAM implied)</li> <li>○ Number of Networking Interfaces (NICs) required</li> <li>○ Operating system – from the Windows Azure Gallery or custom</li> <li>○ Subnet the Virtual Machine will be connected to</li> <li>○ Number and size of data disks</li> <li>○ Products to be installed in the SYSPREP image</li> <li>○ Products to be installed after initialization</li> <li>○ Domain-joined?</li> <li>○ Post-initialization configuration</li> <li>○ Public ports (if any) to be exposed from Windows Azure <ul style="list-style-type: none"> <li>▪ RDP is on by default for Virtual Machines deployed from the portal</li> <li>▪ RDP port can be manually removed from the Windows Azure Management Portal. PowerShell <i>-noRDP</i> option allows deployment of Virtual Machines with this port closed.</li> </ul> </li> </ul>

#### 4.4 Windows Azure subscriptions and support

Windows Azure subscriptions are the mechanism used to manage access to Windows Azure resources. A customer may have multiple subscriptions depending on how they organize their billing, whether ownership is team-based (development, testing, operations, and so on), how they are managed, and so on. Therefore, it is very important to plan for support.

In addition, it is also important to understand the level of Windows Azure support that will be required by the customer. The following table provides pointers on the most relevant information you will need to plan for this step:

Topic	Description
<p><b>Windows Azure subscriptions</b></p>	<p>Plan what Windows Azure subscriptions will be used for the application. Also, verify that you have the following subscription data:</p> <ul style="list-style-type: none"> <li>• Owner</li> <li>• Billing type</li> <li>• Subscription name and ID</li> <li>• Level of Windows Azure support for the subscription</li> </ul>

Topic	Description
<b>Windows Azure support</b>	<p>Windows Azure has four main support options:</p> <p><b>Online forums.</b> Provides a free online forum to ask support questions. This forum is monitored by Microsoft Windows Azure support specialists and it has no SLA on the response times. Link: <a href="http://www.windowsazure.com/en-us/support/forums/">www.windowsazure.com/en-us/support/forums/</a></p> <p><b>Service dashboard.</b> Shows current health of all Windows Azure services running in all the data centers. Customers can subscribe to the RSS feed to get health status notifications. Link: <a href="http://www.windowsazure.com/en-us/support/service-dashboard/">www.windowsazure.com/en-us/support/service-dashboard/</a></p> <p><b>Windows Azure billing support.</b> Provides support for billing and Windows Azure resource quota increases. Link: <a href="https://manage.windowsazure.com/?getsupport=true">https://manage.windowsazure.com/?getsupport=true</a></p> <p><b>Windows Azure technical support.</b> Windows Azure offers flexible support options for customers of all sizes, from developers starting their journey in the cloud to enterprises deploying business-critical applications. Windows Azure support plans information is located at the following link: <a href="http://www.windowsazure.com/en-us/support/plans/">www.windowsazure.com/en-us/support/plans/</a></p> <p><b>Note:</b> Customers that already have an Enterprise Agreement (EA) or have Microsoft Premier hours could use these hours for Windows Azure support. Please contact the customer's TAM to confirm.</p>

## 5 Basic Implementation

In the Implementation step we use the information that was gathered in the Discovery and Planning step to migrate the customer application to Windows Azure. These are the steps of the implementation step:

1. Deploy the network
2. Deploy the VPN
3. Deploy the first server
4. Configure AD DS and the DNS
5. Create the virtual machine images for the application
6. Add virtual machine images to the gallery
7. Deploy and test the virtual machines and templates

**Note:** Configuring specific routers and best practices for router configuration security is beyond the scope of this document. Network edge devices are a critical part of network security and should only be configured by qualified personnel. The following sample configuration is for example purposes only.

### 5.1 Sample deployment scenario

For the purpose of this example, we will use the fictitious company Contoso as an example.

In the Discovery step, we learned that Contoso has the following network configuration:

- Namespace of 10.0.0.0/23
- Public router IP address 1.2.3.4 (note this is a sample and an intentionally fake IP)
- Edge device is a Cisco ASA 5510 using version 8.3 firmware
- Primary AD DS/DNS server IP address is 10.0.0.5 named CONTAD

In the Planning step, Contoso decided to configure a Windows Azure Virtual Network and VPN that connects directly to the corporate network and corporate AD DS domain.

**Note:** Some customers may choose to connect the VPN to a sub-domain located in a perimeter network. The decision is based upon what the IaaS deployment will be used for and the security requirements of the customer.

It was also decided that a domain controller with integrated DNS would also be deployed to Windows Azure as an extension of the on-premises domain.

In Windows Azure, it is required that a Virtual Network IP address space be a private address range, specified in CIDR notation as 10.0.0.0/8, 172.16.0.0/12, or 192.168.0.0/16 (as specified by RFC 1918). In the network setup process, we can use either CIDR or a base address and number of IPs to create when defining the namespace and subnets.

When creating a VPN, Windows Azure requires that a subnet be defined within the VNET namespace for the gateway subnet. The gateway subnet is the VPN network segment between the Windows Azure and customer routers.

Windows Azure requires that all addresses within the VNET be assigned by Windows Azure's DHCP server. These are permanent leases assigned in ascending order within the subnet's namespace. Windows Azure reserves the first 4 addresses in a subnet for internal use. Following this rule set, for a subnet 10.1.0.0/24, the first IP assigned will be 10.1.0.4. Because we want Windows Azure DHCP to tell all the servers the IP address of the planned DNS server, configure the Windows Azure DNS setting as 10.1.0.4 and be sure that the first server deployed is the domain controller. Please note that this behavior regarding network address assignments change with Azure environment changes, but this is the practice most often used today with customer deployments.

Customers can deploy multiple Windows Azure Virtual Networks, but each Virtual Network is required to exist in only one Windows Azure data center.

Windows Azure uses affinity groups to group services together on the same cluster within one Windows Azure data center. All Windows Azure Virtual Networks are required to exist within an affinity group. When creating a Virtual Network using the management portal, you can create an affinity group or select an existing one as part of the deployment. When importing a Virtual Network configuration to Windows Azure, the affinity group must be created first.

When deploying virtual machines, a storage account is required in the same affinity group to hold the virtual hard drives (VHD) files in blob storage.

Contoso has planned for the following Windows Azure VNET and VPN configuration:

- Data center - US East
- Affinity group name – ContosoAF
- Network name - ContosoAzNw
- Storage account for VHD files - contosostor
- Namespace of 10.1.0.0/23
- Subnet-1 10.1.0.0/24
- Gateway subnet 10.1.1.0/24
- DNS server 10.1.0.4 ContAZAD

The following sections will demonstrate the creation of the sample Virtual Network and VPN we have defined. See Chapter 7 for detailed documentation and best practices.

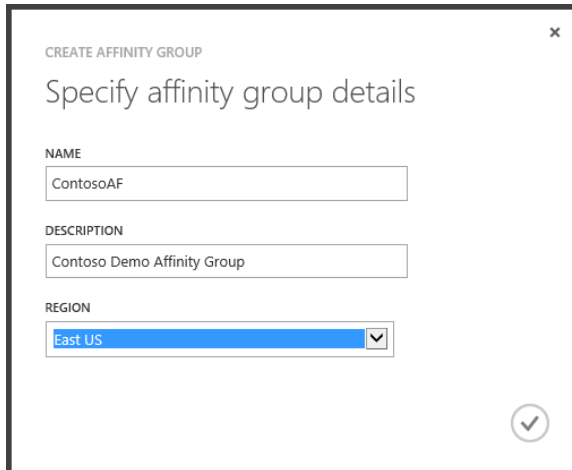
## 5.2 Deploy the network

Connect to the Windows Azure Management Portal [HTTP://manage.windowsazure.com](http://manage.windowsazure.com) and sign in using the Microsoft account that is associated to your Windows Azure subscription.

### 5.2.1 Create an affinity group

The first task is to create the affinity group in the desired data center. Affinity groups are managed in the "Settings" section of the Management Portal.

1. On the left menu bar, click **SETTINGS** and then click **AFFINITY GROUPS** at the top of the page.
2. Click **ADD** at the bottom of the page and enter the **Name**, **Description**, and **Location** for Contoso's affinity group.

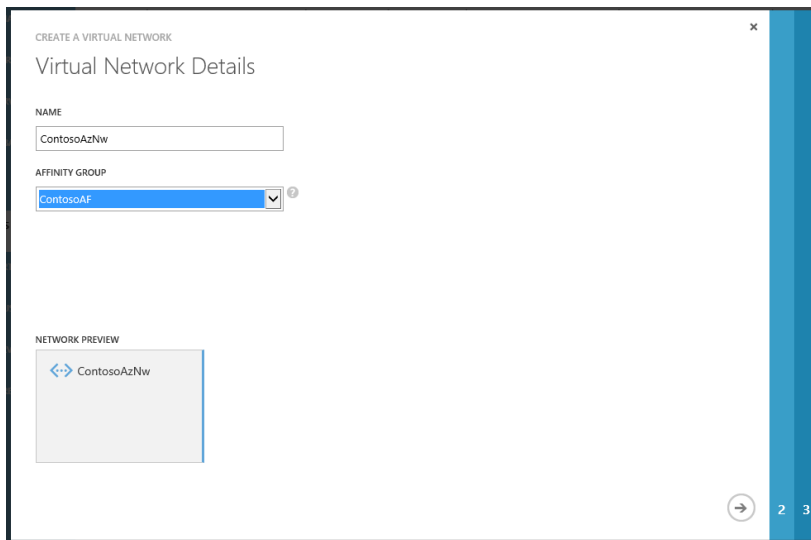


3. Click the **checkmark** button at the bottom of the window to save the affinity group.

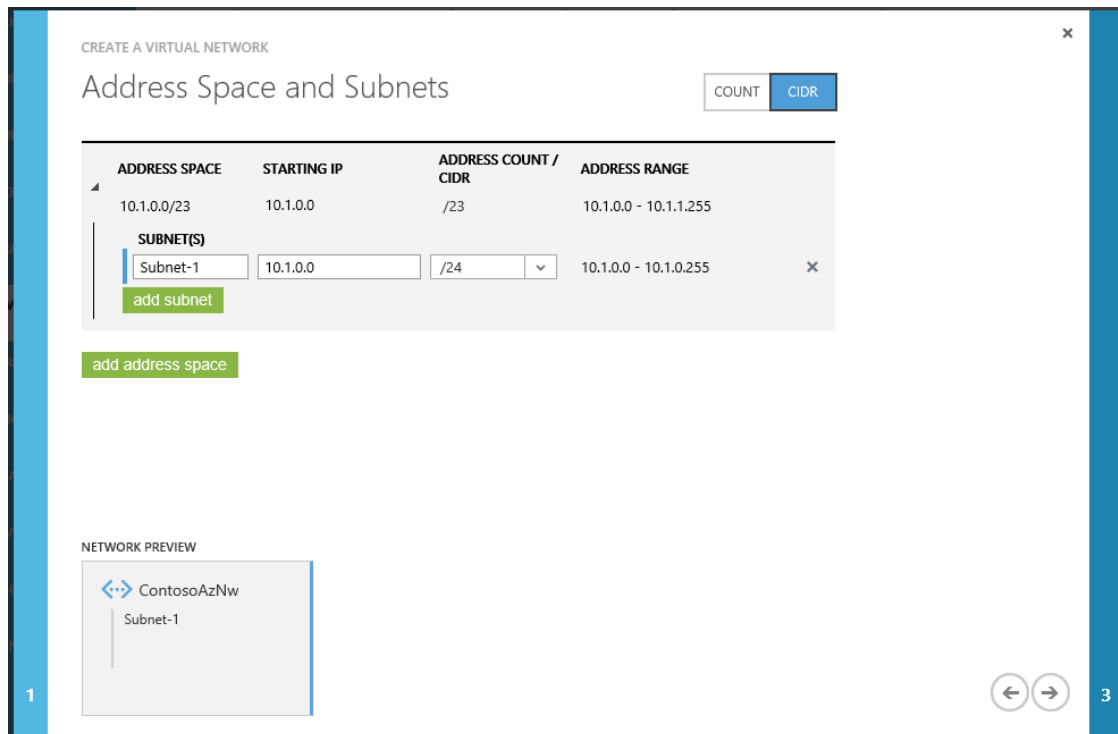
### 5.2.2 Create the Virtual Network

To create the Virtual Network:

1. Click **NETWORKS** on the left menu bar, then click **NEW** at the bottom, then **VIRTUAL NETWORK**, and then **CUSTOM CREATE** in the pop-up menu.
2. Enter the network name for Contoso (**ContosoAzNw**), select the Contoso affinity group **ContosoAF** from the affinity group drop-down box, and then click the **-> next** arrow at the bottom of the window.

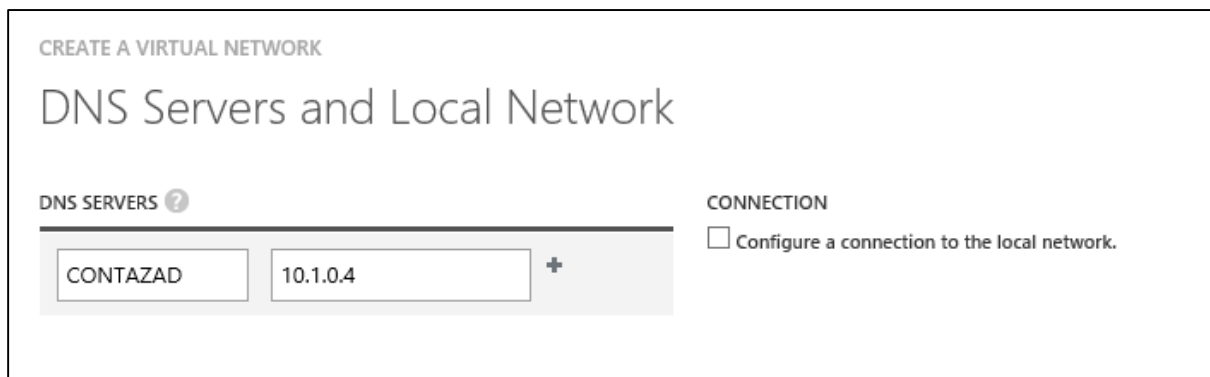


3. In the **Address Space and Subnets** window of the wizard, click **CIDR** at the top to enable entering addresses in CIDR notation.
  - Click **10.0.0.0** under **STARTING IP** in the "Address Space" section, and change it to **10.1.0.0**.
  - Click **/8** under **ADDRESS COUNT/CIDR** and change it to **/23** in the drop-down list.
  - Click **/26** under **ADDRESS COUNT/CIDR** on the **Subnet-1** line and change it to **/24**.

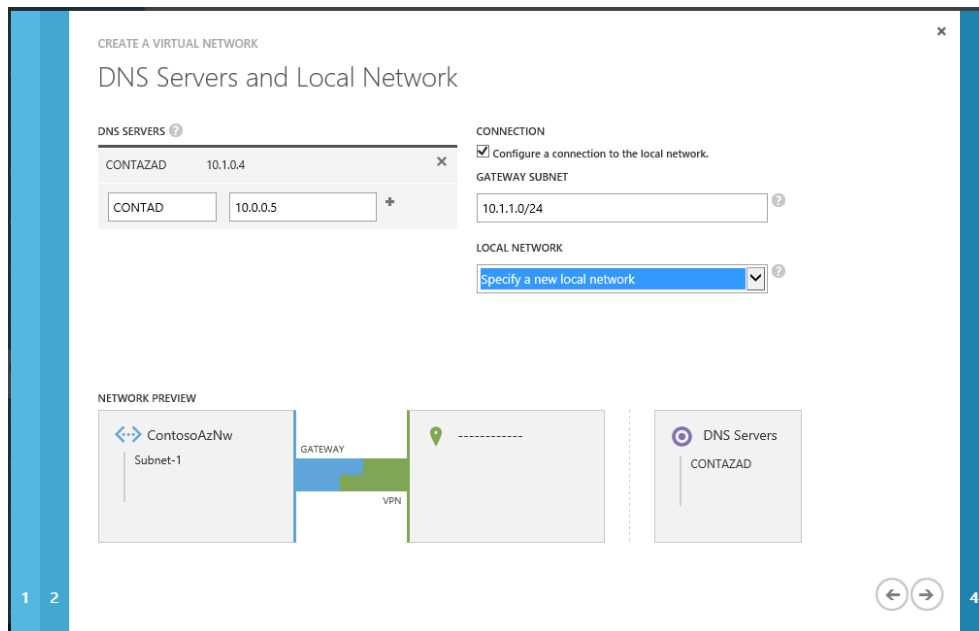


Then click the -> **next** arrow at the bottom of the window.

4. Enter the DNS server name that we will create in Windows Azure as **CONTAZAD** and the IP address **10.1.0.4**.
5. Check the box to **Configure a connection to the local network**.



6. Enter **CONTAD** and **10.0.0.5** for the on-premises secondary DNS server into the **DNS SERVERS** list.
7. Enter **10.1.1.0/24** as the **GATEWAY SUBNET**.
8. Select **Specify a new local network** in the **LOCAL NETWORK** drop-down list.

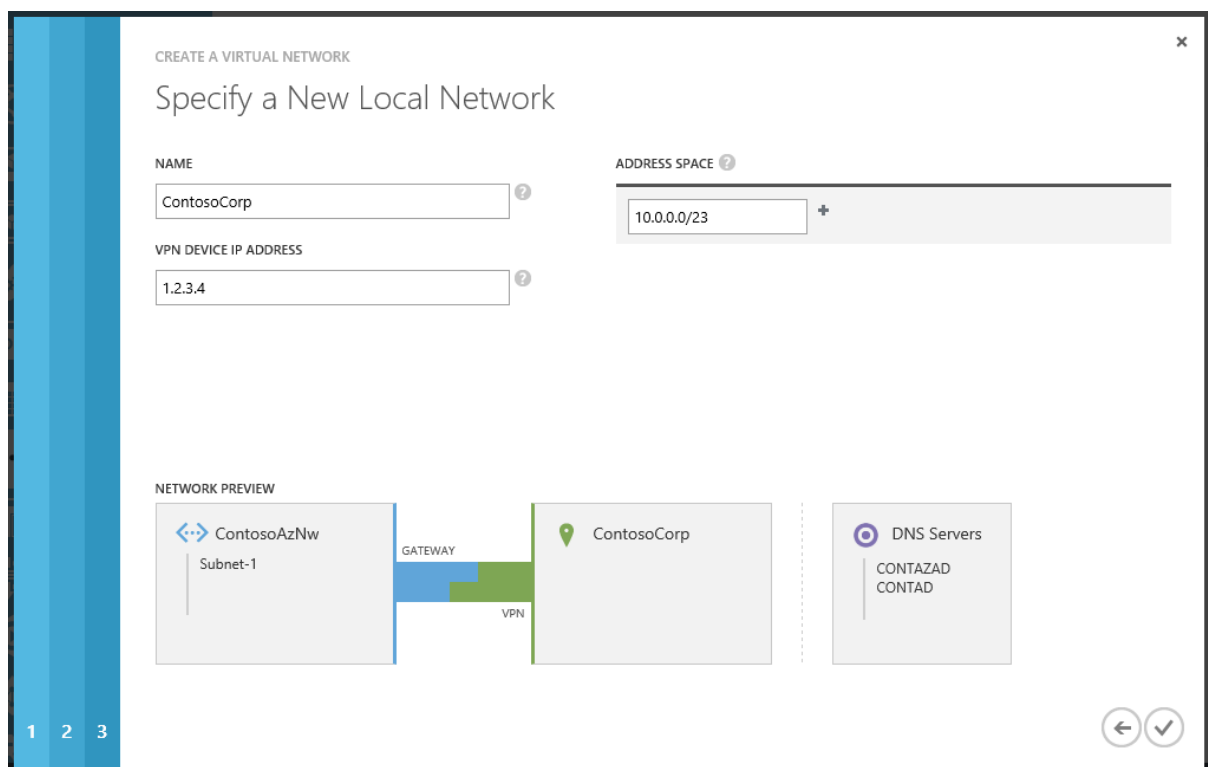


Then click the -> **next** arrow at the bottom of the window.

### 5.2.3 Create the local network

On the **Specify a New Local Network** page:

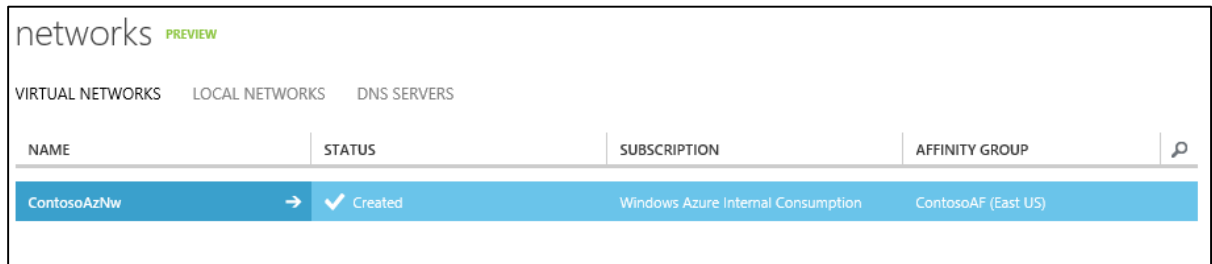
1. Enter **ContosoCorp** as the **NAME**.
2. Enter **1.2.3.4** as the **VPN DEVICE IP ADDRESS** (note this is a sample and an intentionally fake IP).
3. Enter **10.0.0.0/23** as the **ADDRESS SPACE**.





- Click the **done** symbol (check mark) at the bottom of the window to complete the wizard and deploy the network.

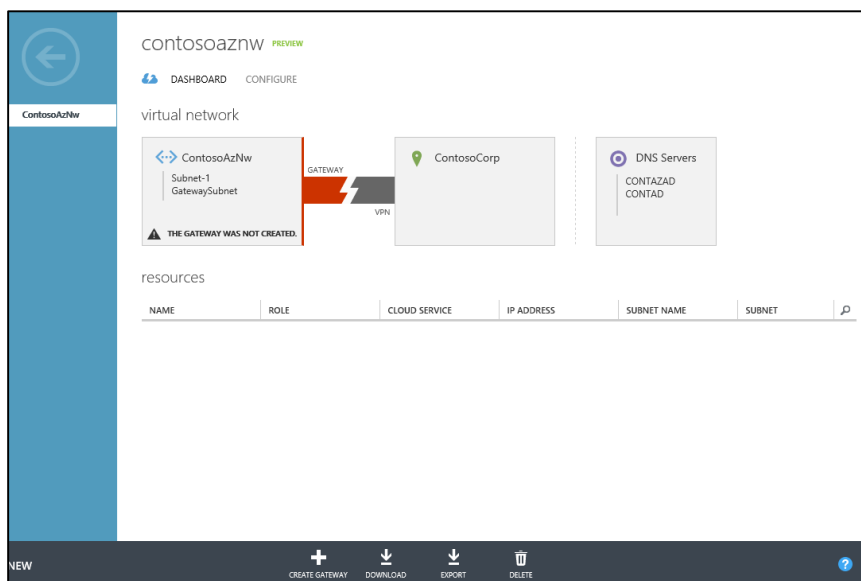
After a few moments, the creation will complete and look like the following screen shot:



NAME	STATUS	SUBSCRIPTION	AFFINITY GROUP
ContosoAzNw	Created	Windows Azure Internal Consumption	ContosoAF (East US)

### 5.2.4 Create the VPN gateway

- Click the network name, and then click **DASHBOARD** to see the details of the deployed network.

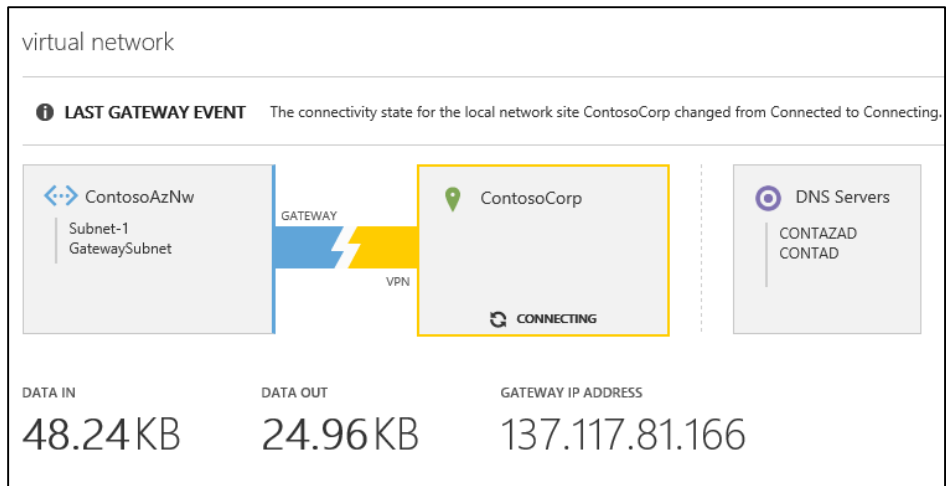


- Click **CREATE GATEWAY** at the bottom of the page to create the Windows Azure side of the VPN tunnel, and click **Yes** when prompted if you are sure you would like to deploy the gateway.

Deploying the gateway can take 5 to 15 minutes, and this process must complete before moving on to the next step. After the gateway deployment is completed:

- Click **CONNECT** at the bottom of the page to initialize the gateway.

The wizard display will look like the following screen shot when complete.



### 5.2.5 Configure the customer router for the VPN

**Note:** Configuring specific routers, and best practices for router configuration security is beyond the scope of this document. Network edge devices are a critical part of network security and should only be configured by qualified personnel. The sample configuration below is for example purposes only.

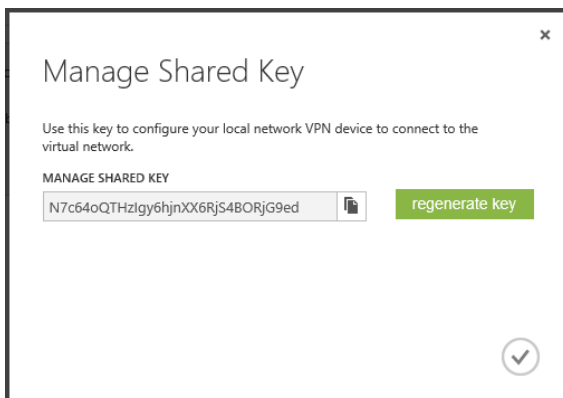
After the Virtual Network and gateway are deployed, the following three pieces of information are needed from the Windows Azure Management Portal to complete the configuration of the Cisco ASA 5510.

- Gateway IP address: 137.117.81.166
- The pre-shared IPsec key
- The sample Cisco ASA 5500 series configuration script

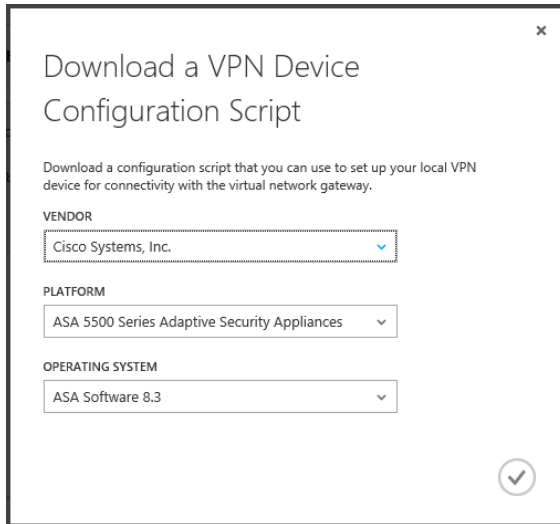
1. To obtain the IPsec key, click **MANAGE KEY** at the bottom of the window.

The key is displayed in a pop-up window and can be copied to the clipboard. If needed, a new key can be requested in this window by clicking **regenerate key**.

**Note:** Regenerating the key will reset the connection, and require reconfiguration of the customer router.



2. Click **DOWNLOAD** at the bottom of the window to download the sample configuration script for the ASA device as a text file.



3. Save the file to your computer and then open the file to edit it.
4. In the sample configuration file, each variable that needs to be edited with implementation specific details is in angle brackets. Variables that begin with **RP** are labels that you create. Variables that begin with **SP** are specific values from either the local or Windows Azure network configuration we have just completed.

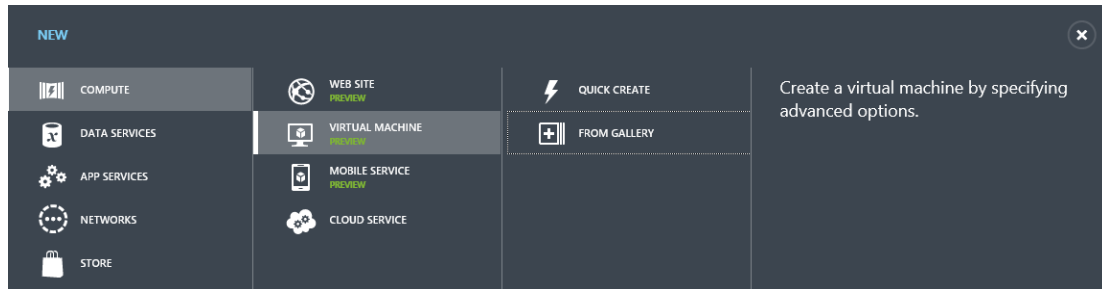
The following table lists the variables and values for the Contoso sample scenario.

Variable Name	Value
<RP_AzureNetwork>	ContAzNw
<SP_AzureNetworkIpRange>	10.1.0.0
<SP_AzureNetworkSubnetMask>	255.255.254.0
<RP_OnPremiseNetwork>	ContosoCorp
<SP_OnPremiseNetworkIpRange>	10.0.0.0
<SP_OnPremiseNetworkSubnetMask>	255.255.254.0
<RP_AccessList>	ContosoAZACL
<RP_IPSecTransformSet>	ContosoAZTS
<RP_IPSecCryptoMap>	ContosoCrypto
<SP_AzureGatewayIpAddress>	137.117.81.166
<SP_PresharedKey>	N7c64oQTHzIgy6hjnXX6RjS4BORjG9ed

## 5.3 Deploy the first server

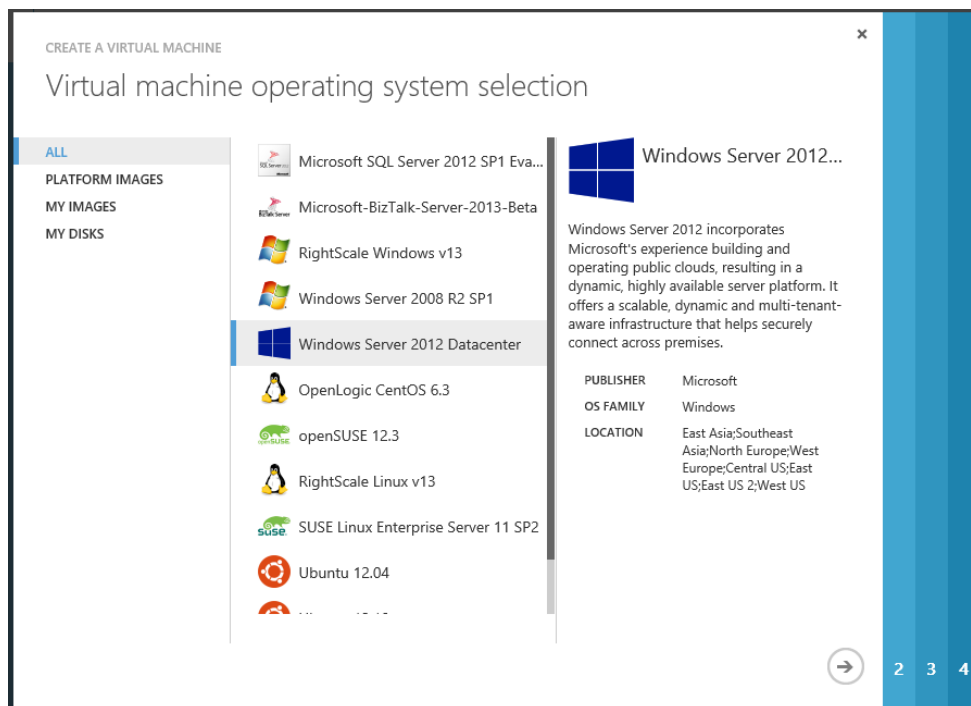
The first Windows Azure Virtual Machine to deploy is the Active Directory/DNS server for the Windows Azure network. To create the server using an image from the gallery:

1. Click **Virtual Machines** on the left menu bar, and then click **NEW** at the bottom of the window.
2. In the menu that pops up, click **COMPUTE**, then **VIRTUAL MACHINE**, then **FROM GALLERY**.



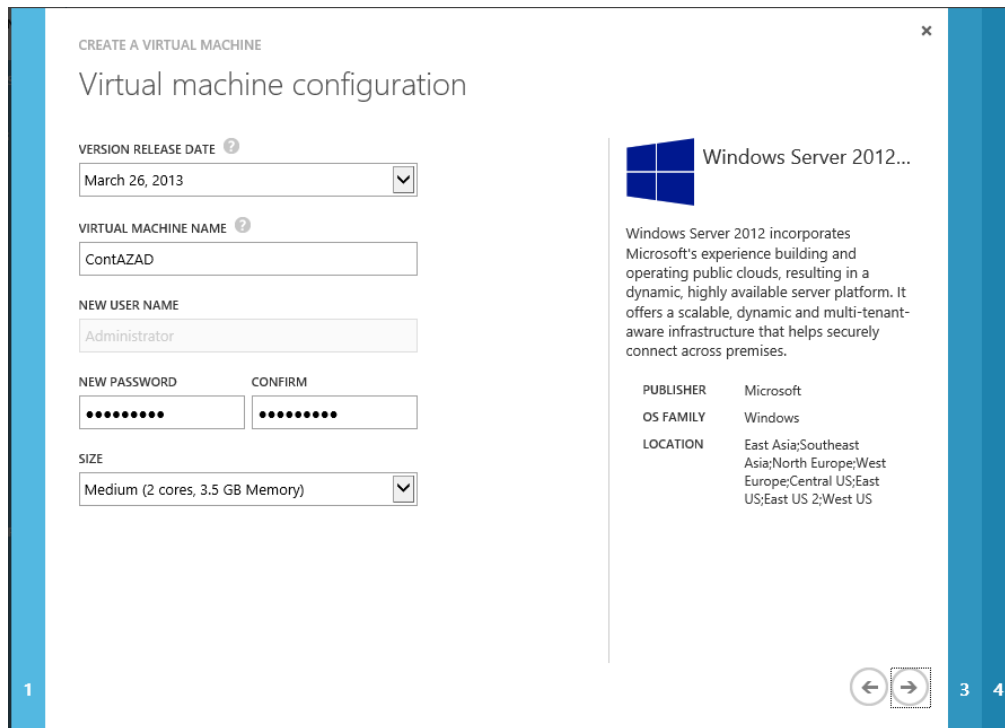
Contoso's plan is to deploy a Windows Server 2012 virtual machine as the Active Directory/DNS Server in Windows Azure.

3. Choose the **Windows Server 2012 Datacenter** image from the gallery, and then click the -> next arrow at the bottom of the window.



4. In the **Virtual Machine Configuration** window, do the following:
  - a. Choose the **VERSION RELEASE DATE**; use the newest release available.
  - b. Enter the **VIRTUAL MACHINE NAME**. This is the NetBios name for this Windows virtual machine.
  - c. Enter and confirm and strong password for the local Administrator account of the virtual machine.
  - d. Choose the **SIZE** of the machine to be deployed. Contoso has planned to deploy a Medium 2 core virtual machine for its AD DS server.

Then click the -> **next** arrow at the bottom of the window.



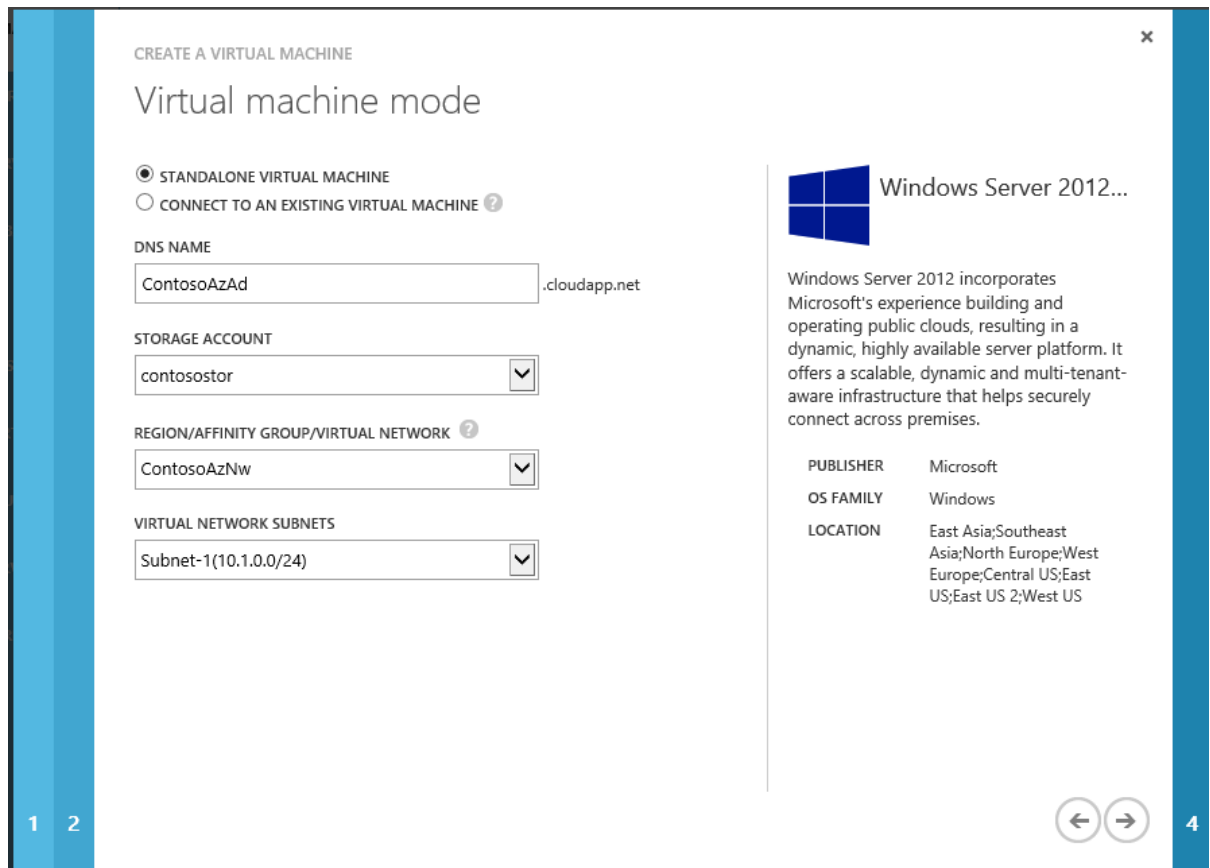
Servers in Windows Azure IaaS require two instances in an availability set connected to the same cloud service to have an availability SLA. For the purposes of the Contoso POC, the plan is to only deploy one AD DS server. In production, they will deploy at least two in an availability set to ensure high availability.

In the **Virtual Machine Mode** window, choosing **STANDALONE VIRTUAL MACHINE** creates a new cloud service with the DNS NAME provided and places this new Virtual Machine in the cloud service. Choosing **CONNECT TO AN EXISTING VIRTUAL MACHINE** would add the new virtual machine to an existing cloud service and enable the creation of an availability set on the next screen. In Windows Azure, two virtual machines in the same availability set will not be deployed to the same rack in the data center.

A storage account can be explicitly named to host the virtual hard drives for this virtual machine or the wizard can create one automatically. The storage account for the VHDs must be in the same affinity group as the virtual network and virtual machine.

Contoso has chosen to use the storage account **contosostor**, which was created in the affinity group **ContosoAF**.

5. Be sure to select the **ContosoAzNw** Virtual Network and **Subnet-1** as shown in the following screen shot so that the Virtual Machine is placed in the correct network.



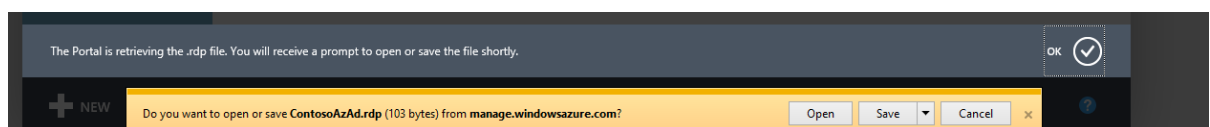
6. In the final (**Virtual Machine Options**) window, select **none** for the availability set as described previously and then click the **done** symbol (check mark) at the bottom of the window to start the creation of the virtual machine.

## 5.4 Testing virtual machine network connectivity

After the virtual machine deployment is completed, the status will update to Running.

Virtual machines deployed from gallery images using the Management Portal will have Remote Desktop enabled and the port (3389) for connecting to RDP exposed to the public Internet by default. To connect to the new virtual machine:

1. In the portal, highlight the virtual machine name in the list in the portal and then click the **CONNECT** button at the bottom of the screen. A file will be downloaded to your local computer with a “.rdp” extension. This file can be opened from the browser download or saved and opened.
2. Open the file to launch Windows Remote Desktop client with the proper connection settings to connect to the public IP of the new virtual machine.



3. Log in to the virtual machine using Administrator and your strong password. Leave the **Domain** blank.

After you are logged into the Virtual Machine, Windows will complete its first boot configuration.

Typical best practices for Windows deployment should be followed for setting up the VM in the Contoso environment.

4. After the virtual machine is up and running, test the VPN to verify that it is working by using the Ping command to communicate with computers on the corporate side of the VPN.

**Note:** Windows Firewall blocks Ping traffic by default. You will need to temporarily disable Windows Firewall or change the rule to allow Ping, both on the Windows Azure Virtual Machine and the on-premises computer that you use to do the testing.

## 5.5 Management of public endpoints

When deploying virtual machines using the Management Portal, the endpoint for RDP (Remote Desktop Protocol, 3389) is automatically created and opened to the public Internet. Because the Virtual Machines in this POC are connected to a Virtual Network with a VPN connection, we can close this port and still access the Virtual Machine via the IPsec VPN.

If there is a need to expose a public service like a website, add that port (example 80 for HTTP) as an endpoint.

To delete the default port 3389 RDP endpoint:

1. Click the virtual machine name in the list of machines in the Management Portal, and then click **ENDPOINTS** at the top of the window.
2. Highlight the port in the list that you wish to delete, and then click **DELETE ENDPOINT** at the bottom of the window. Click **YES** to confirm the deletion.

To add a port:

1. Click **ADD ENDPOINT** at the bottom of the window.
2. On the first screen, choose to **ADD ENDPOINT** or **LOAD BALANCE**. If there were two servers in the same cloud service, they would share a public IP and load balancer. You can configure load balancing of a port in this screen. However, for this example, we are just adding port 80 HTTP to one server.
3. Enter **HTTP** as the **NAME** of the port, **TCP** as the **PROTOCOL**, and **80** for both the **PUBLIC** and **PRIVATE** ports. Click the done symbol (check mark) to save.

## 5.6 Configure Active Directory and DNS

Configuration of AD DS in a multi-site environment is beyond the scope of this document.

Details of the process are located in the Windows Azure documentation “Guidelines for Deploying Windows Server Active Directory on Windows Azure Virtual Machines,” which is available at <http://msdn.microsoft.com/en-us/library/windowsazure/jj156090.aspx>

Key considerations for deployment on Windows Azure:

- All IP addresses for Windows Azure Virtual Machines are assigned by DHCP. Do not assign a static IP to a Windows Azure Virtual Machine.
- The operating system disk for Windows Azure Virtual Machines has write caching turned on by default. Write caching can cause AD DS corruption if changes are not flushed to storage

and the machine is failed over to a new deployment. Always add data disks with write caching turned off to a virtual machine that will host AD DS, and place the AD DS folder on the data disk.

- When deploying AD DS to a WAN that may have intermittent or high latency connections, it is important to properly create a sites topology within AD DS.
- Windows Azure charges for bandwidth that leaves the datacenter, for this reason, some customers may choose to deploy a Read Only Domain Controller <sup>11</sup>(RODC), which will cause the AD replication traffic to flow one-way from the corporate network to Azure, reducing bandwidth consumption.
- Best practices for AD deployment on Azure include using a Data Disk with no caching for the location of the AD database folders.
- Windows Azure requires two servers in the same Cloud Service, in an Availability Set to provide an Availability SLA of 99.95%.

**Note:** In Windows Azure there is no High Availability (HA) SLA for single instance for deployments.

## 5.7 Create virtual machine images from a deployed virtual machine

The Management Portal supports capturing an image of a virtual machine into the gallery. To capture a virtual machine as an image, the virtual machine should be prepared with Sysprep and must be shut down.

For an overview of Sysprep, refer to the following documentation on TechNet: <http://technet.microsoft.com/en-us/library/hh825209.aspx>

After the Virtual Machine has been prepared:

1. Highlight the virtual machine in the list on the Management Portal and click **Capture**.
2. Provide an **IMAGE NAME**, and indicate that the image has been Sysprepped.

**Note:** Virtual machines to be captured must be Sysprepped. Also, the virtual machine will be deleted as part of the capture process.

## 5.8 Add customer VHD images to the Windows Azure Gallery

Customers can create their own VHD files to upload as images to the Gallery.

Customer VHD images must:

- Be Hyper-V IDE format VHD files for OS Disks, and SCSI format for Data Disks
- No larger than 127 GB for OS Disks, and no larger than 1023 GB for Data Disks
- Be created as fixed size
- Be sysprepped(Windows) or generalized(Linux) to be added to the Gallery as an Image
- Only 64bit Server Operating Systems are supported as OS Disks

---

<sup>11</sup> Microsoft, Install a Windows Server 2012 Active Directory Read-Only Domain Controller (RODC) (Level 200), <http://technet.microsoft.com/en-us/library/jj574152.aspx>, 2013.



Microsoft provides a command-line tool CSUPLOAD with the Windows Azure SDK that performs the upload of images. The tool requires a management certificate be uploaded to the Windows Azure Management Portal and linked to the user's subscription.

Documentation for using CSUPLOAD is located at [www.windowsazure.com/en-us/manage/windows/common-tasks/upload-a-vhd/](http://www.windowsazure.com/en-us/manage/windows/common-tasks/upload-a-vhd/)

Using Windows PowerShell to manipulate images and disks will be covered in section 6.2.

## 6 Management of the IaaS Deployment

Depending upon the customer's operational maturity level, there are several options for the management of Windows Azure Virtual Machines. The table below lists five methods of managing IaaS deployments, in ascending order of operational maturity:

Management Method	Description
<b>Windows Azure Management Portal</b>	Customers who wish to manually deploy and manage IaaS can use the Windows Azure HTML5 web portal.
<b>Windows Azure PowerShell Cmdlets</b>	Windows Azure PowerShell Cmdlets <sup>12</sup> allow for manual execution of IaaS deployment and management commands. These commands can be parameterized and combined into powerful repeatable processes.
<b>System Center App Controller</b>	For customers that have deployed System Center 2012 SP1, App Controller provides an interactive management portal for IaaS. While this portal does not provide automation, it extends the management of IaaS by through Active Directory authenticated delegation of permissions.
<b>System Center Orchestrator</b>	Microsoft System Center Orchestrator 2012 SP1, includes an Integration Pack for Windows Azure that enables the rapid development of "RunBooks" for managing and deploying IaaS.
<b>Windows Azure Service Management REST API</b>	Customers who require the ability to integrate Windows Azure IaaS management and deployment into a custom or 3 <sup>rd</sup> Party management system can leverage the Windows Azure Service Management REST API.

### 6.1 Use the Windows Azure Management Portal

Windows Azure Virtual Machines can be managed manually via the web based portal. In Chapter 5 we detailed the deployment of a Virtual Network, site to site VPN, and Virtual Machines, and the management of disk images, using the portal and CSUPLOAD tool.

Customer who have not implemented any automation in their datacenters can use this method for deploying and managing Windows Azure Virtual Machines.

---

<sup>12</sup>Microsoft, Windows Azure PowerShell Cmdlets, <http://wappowershell.codeplex.com/>, 2012

## 6.2 Use the Windows Azure PowerShell Cmdlets

Windows Azure provides a full set of PowerShell Cmdlets for deploying and managing Virtual Machines and disk images.

A full tutorial on PowerShell or the Windows Azure PowerShell Cmdlets is beyond the scope of this document. The Windows Azure PowerShell Cmdlets Reference is documented here: <http://msdn.microsoft.com/en-us/library/jj152841.aspx>

### 6.2.1 Preparing to use Windows Azure PowerShell

#### Prerequisites:

- A computer that is running Windows 8, Windows 7, Windows Server 2012, or Windows Server 2008 R2.
- A Windows Azure subscription.
- A management certificate associated with the Azure Subscription

#### Installation Steps:

1. Download and install the Windows Azure PowerShell module:  
<http://go.microsoft.com/?linkid=9811175&clid=0x409>
2. Set the Execution Policy for PowerShell to *RemoteSigned*
  - a. Click Start, click All Programs, click Windows Azure, right-click Windows Azure PowerShell, and then select Run as administrator.
  - b. If this is the first time you have run the Windows Azure PowerShell command shell, run the following command, and type Y to finish the command:

```
PS C:\> Set-ExecutionPolicy RemoteSigned
```

*Note: You only need to use **Run as administrator** to set the execution policy. Future sessions can be run as a standard user. Because the Windows Azure PowerShell command shell is a 32-bit command shell, and execution policy is set separately for 32-bit and 64-bit shells, you must also set the execution policy for 64-bit Windows PowerShell to use the Windows Azure module in it.*

3. Import the Windows Azure Cmdlet module into Windows PowerShell
  - a. Type one of the following commands and then press Enter:
    - i. On a 64-bit version of the operating system, type:  
**PS C:\> Import-Module "C:\Program Files (x86)\Microsoft SDKs\Windows Azure\PowerShell\Azure\Azure.psd1"**
    - ii. On a 32-bit version of the operating system, type:  
**PS C:\> Import-Module "C:\Program Files\Microsoft SDKs\Windows Azure\PowerShell\Azure\Azure.psd1"**

## 6.2.2 Example Windows Azure PowerShell Cmdlets

### Connecting to Windows Azure

The PowerShell Cmdlets use a management certificate to authenticate connections to Windows Azure. The simplest way to associate your PowerShell session with your Azure Subscription is to import a *PublishSettings* file.

Executing the Cmdlet **Get-AzurePublishSettingsFile** will launch a browser session. Login when prompted using the Microsoft Account (Live ID) that is an administrator of the subscription(s) that you would like a *PublishSettings* file for. Note that all subscriptions that the Microsoft account is an administrator of will be included in the *PublishSettings* file. This web page runs a wizard that creates a new management certificate, associates it with your Azure Subscription, and then downloads a *PublishSettings* file that contains the Subscription name, ID, and certificate thumbprint, for each Subscription.

Choose **SaveAs** to save the PublishSettings file with a known name and location.

**Note: Possession of the PublishSettings file allows full control of an Azure Subscription.**

At the PowerShell prompt execute **Import-AzurePublishSettingsFile -PublishSettingsFile "C:\path\filename.publishsettings"** to connect your PowerShell session to Windows Azure.

Executing **Get-AzureSubscription** will list all of the Azure Subscriptions that are now connected.

Executing **Set-AzureSubscription -DefaultSubscription "<Subscription Name>"** will set the default subscription context for all following commands to the named subscription.

Executing **Set-AzureSubscription -SubscriptionName "<Subscription Name>" -CurrentStorageAccount "<Storage Account Name>"** will set the default Storage Account context for the named Subscription for all following commands.

### Deploy Networks

Azure Virtual Network configuration is managed with PowerShell by importing and exporting an XML file defining the Virtual Network. The schema for Virtual Networks is defined here: <http://msdn.microsoft.com/en-us/library/windowsazure/jj157100.aspx>

Executing **Get-AzureVNetConfig -ExportToFile "C:\PATH\FileName.XML"** will export the current Virtual Network configuration for the default Subscription to a XML file.

Executing **Set-AzureVNetConfig -ConfigurationPath "C:\PATH\FileName.XML"** will import a Virtual Network configuration file, and attempt to apply the configuration to the default Subscription.

Below is the exported Network Configuration created by following the sample in Chapter 5:

```
<?xml version="1.0" encoding="utf-8"?>
<NetworkConfiguration xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns="http://schemas.microsoft.com/ServiceHosting/2011/07/NetworkConfiguration">
  <VirtualNetworkConfiguration>
    <Dns>
      <DnsServers>
```

```

    <DnsServer name="CONTAD" IPAddress="10.0.0.5" />
    <DnsServer name="CONTAZAD" IPAddress="10.1.0.4" />
    <DnsServer name="onpremdns" IPAddress="192.168.37.3" />
  </DnsServers>
</Dns>
<LocalNetworkSites>
  <LocalNetworkSite name="ContosoCorp">
    <AddressSpace>
      <AddressPrefix>10.0.0.0/23</AddressPrefix>
      <AddressPrefix>192.168.37.0/24</AddressPrefix>
    </AddressSpace>
    <VPNGatewayAddress>24.0.142.51</VPNGatewayAddress>
  </LocalNetworkSite>
</LocalNetworkSites>
<VirtualNetworkSites>
  <VirtualNetworkSite name="ContosoAzNw" AffinityGroup="ContosoAF">
    <AddressSpace>
      <AddressPrefix>10.1.0.0/23</AddressPrefix>
    </AddressSpace>
    <Subnets>
      <Subnet name="Subnet-1">
        <AddressPrefix>10.1.0.0/24</AddressPrefix>
      </Subnet>
      <Subnet name="GatewaySubnet">
        <AddressPrefix>10.1.1.0/24</AddressPrefix>
      </Subnet>
    </Subnets>
    <DnsServersRef>
      <DnsServerRef name="CONTAZAD" />
      <DnsServerRef name="CONTAD" />
    </DnsServersRef>
    <Gateway>
      <ConnectionsToLocalNetwork>
        <LocalNetworkSiteRef name="ContosoCorp" />
      </ConnectionsToLocalNetwork>
    </Gateway>
  </VirtualNetworkSite>
</VirtualNetworkSites>
</VirtualNetworkConfiguration>
</NetworkConfiguration>

```

### Deploy Virtual Machines

Deploying a new Virtual Machine from a Gallery Image consists of four Cmdlets piped together to complete the task.

1. **New-AzureVMConfig** creates the configuration of the machine, specifying the name of the machine, instance size, and gallery image name to user.
2. **Add-AzureProvisioningConfig** allows us to set the local admin password. Additional options here allow for automatically joining a domain, and deploying without provisioning the default RDP endpoint.
3. **Set-AzureSubnet** is used to set the name of the subnet the machine should be joined to.

4. **New-AzureVM** creates the actual Virtual Machine. Options on this command allow us to choose the Virtual Network to join, and whether the VM should join an existing Cloud Service or create a new one.

Below is a sample script to create a second machine in the sample Virtual Network created in Chapter 5:

```
New-AzureVMConfig -Name "ContosoAzAd2" -InstanceSize "Small" -ImageName
"a699494373c04fc0bc8f2bb1389d6106__Windows-Server-2012-Datacenter-201303.01-en.us-
127GB.vhd" |

Add-AzureProvisioningConfig -Windows -Password "StrongAdminPass1" |

Set-AzureSubnet -SubnetNames "Subnet-1" |

New-AzureVM -ServiceName "ContosoAzAd2" -VNetName "ContosoAzNw" -AffinityGroup
"ContosoAF"
```

### *Manage Disks and Images*

**Add-AzureVHD** is used to copy VHD images from on premises to Azure using PowerShell. Parameters include the Local File Path, destination Storage Container, and Number of Threads to use for uploading.

**Add-AzureDisk** is used create an Azure Disk from a VHD. Parameters include Disk Name, VHD Location, and a flag to specify if the disk contains a bootable OS.

Beginning with the March 2013 release of the Windows Azure PowerShell Cmdlets, there are now commands for performing asynchronous copies between storage accounts and Azure Datacenters for the blob files used for storing VHD files. See the PowerShell documentation for details.

### *Deploy a Web Farm Template*

This sample deploys a simple web farm to the Virtual Network created in Chapter 5. Note that database server has two empty data disks being added, and the load balanced Endpoint created for the two web servers that are deployed to the same Cloud Service.

```
$adminPass = "StrongAdminPass1"

# Deploy Database Server
New-AzureVMConfig -Name "ContosoDB" -InstanceSize "Medium" -ImageName
"a699494373c04fc0bc8f2bb1389d6106__Windows-Server-2012-Datacenter-201303.01-en.us-
127GB.vhd" |
  Add-AzureProvisioningConfig -Windows -Password $adminPass |
  #add 2 new 100GB data disk on creation of VM.
  Add-AzureDataDisk -CreateNew -DiskSizeInGB 100 -DiskLabel "Data100a" -LUN 0 |
  Add-AzureDataDisk -CreateNew -DiskSizeInGB 100 -DiskLabel "Data100b" -LUN 1 |
  Set-AzureSubnet -SubnetNames "Subnet-1" |
  New-AzureVM -ServiceName "ACLiveDB1" -AffinityGroup "ContosoAF" -VNetName
"ContosoAzNw"

# Deploy Web 1
New-AzureVMConfig -Name "ContosoWeb1" -InstanceSize "Small" -ImageName
"a699494373c04fc0bc8f2bb1389d6106__Windows-Server-2012-Datacenter-201303.01-en.us-
127GB.vhd" |
  Add-AzureProvisioningConfig -Windows -Password $adminPass |
  Set-AzureSubnet -SubnetNames "Subnet-1" |
```

```

    New-AzureVM -ServiceName "ContosoWeb" -AffinityGroup "ContosoAF" -VNetName
    "ContosoAzNw"

# Deploy Web 2
New-AzureVMConfig -Name "ContosoWeb2" -InstanceSize "Small" -ImageName
"a699494373c04fc0bc8f2bb1389d6106__Windows-Server-2012-Datacenter-201303.01-en.us-
127GB.vhd" |
    Add-AzureProvisioningConfig -Windows -Password $adminPass |
    Set-AzureSubnet -SubnetNames "Subnet-1" |
    New-AzureVM -ServiceName "ContosoWeb"

# Create Load Balanced Port 80
Get-AzureVM -ServiceName "ContosoWeb" |
    Add-AzureEndpoint -Name "Web" -Protocol tcp -LocalPort 80 -PublicPort 80 -LBSetName "ACWEB"
-ProbePort 80 -ProbeProtocol "http" -ProbePath "/" |
    Update-AzureVM

```

### 6.3 System Center App Controller

Microsoft System Center App Controller provides a common self-service experience that can help you easily configure, deploy, and manage virtual machines and services across private and public clouds.

Configuration and deployment of App Controller is beyond the scope of this document. For details on App Controller, refer to the documentation here: <http://technet.microsoft.com/en-us/library/hh546834.aspx>

Support for Windows Azure Virtual Machines was added in App Controller 2012 SP1.

App Controller uses a management certificate to authenticate requests to the Windows Azure management API. Once App Controller has been configured to connect to a Windows Azure Subscription, users can be delegated to have deployment privileges to that Subscription using their Active Directory credentials.

Documentation for configuring App Controller to connect to a Windows Azure Subscription is located here: <http://technet.microsoft.com/en-us/library/hh221344.aspx>

### 6.4 System Center Orchestrator

Microsoft System Center Orchestrator is a workflow management solution for the data center. Orchestrator lets you automate the creation, monitoring, and deployment of resources in your environment.

Configuration and deployment of Orchestrator is beyond the scope of this document. For details on Orchestrator, refer to the documentation here: <http://technet.microsoft.com/en-us/library/hh237242.aspx>

Support for Azure Virtual Machines is provided via the Windows Azure Integration Pack for Orchestrator in System Center 2012 SP1. Download and installation details for the integration pack are located here: <http://technet.microsoft.com/en-us/library/jj721956.aspx>

With Orchestrator and the Windows Azure Integration Pack, complex automation scenarios can be created and run as scheduled or on demand tasks.

One key usage scenario is to use System Center Service Desk to create Self Provisioning Request Portals that advertise to users the availability of pre-defined virtual machine configurations like the web farm demonstrated in Section 6.2.2. Deploy a Web Farm Template. Consider the following scenario:

- A user requests the Web Farm test environment using Service Desk Provisioning Portal.
- Service Desk validates the request, including complex workflow, for instance requesting the user's manager approve the request first.
- Upon request validation and approval, Service Desk calls an Orchestrator RunBook passing in variables for the names, quantities and other deployment options for the Virtual Machines
- Orchestrator Executes the RunBook, and then notifies Service Desk the Task is complete.
- Service Desk notifies the user their machines are deployed and ready for use.

Assuming the manager approves the request immediately, this entire process can be completed in just a few minutes, from request to notification that the machines are available for use.

Additional logic can be developed to do tasks migrating VM's from on premises to the cloud and back, and de-provision test machines after a period of time, or on a scheduled basis to manage run rate costs.

## 6.5 Using the Windows Azure Service Management Rest API

For customers creating a custom or using a third party management solution, Windows Azure provides a REST API. The Service Management API provides programmatic access to much of the functionality available on Windows Azure. All API operations are performed over SSL and mutually authenticated using X.509 v3 certificates.

Custom development using the REST API is beyond the scope of this document. The Windows Azure Service Management REST API is documented here: <http://msdn.microsoft.com/en-us/library/windowsazure/ee460799.aspx>



## 7 Appendix A: Educational resources

### 7.1 Learning Windows Azure IaaS

#### Windows Azure IaaS documentation

- [Windows Azure Trust Center](#)
- [Windows Virtual Machines from the Gallery](#)
- [Linux Virtual Machines From the Gallery](#)
- [Virtual Machine Pricing](#)

#### Windows Azure Training

- [Windows Azure Training Kit](#)

#### Video recordings regarding Windows Azure IaaS

- [Introduction to Windows Azure Infrastructure as a Service \(IaaS\), Mark Russinovich](#)
- [Deep Dive into Running Virtual Machines on Windows Azure, Vijay Rajaopalan](#)
- [Windows Azure IaaS and How It Works, Corey Sanders](#)

### 7.2 Learning Windows Azure Virtual Networking

#### Windows Azure Virtual Networking documentation

- [Windows Azure Virtual Network](#)
- [Supported VPN Devices](#)
- [Establish a Site-to-Site VPN Connection](#)
- [Load Balancing Virtual Machines](#)

#### Video recordings regarding Windows Azure Virtual Networking

- [Overview of Windows Azure Networking Features, Ganesh Srinivasan](#)
- [Deep Dive: Extending Enterprise Networks to Windows Azure - Project "Brooklyn", Ganesh Srinivasan](#)
- [Hybrid Will Rule: Options to Connect, Extend and Integrate Applications in Your Data Center and Windows Azure, Yousef Khalidi](#)

### 7.3 Disks, Images and VHDs Management

#### Windows Azure disks, images and VHDs documentation

- [How to Attach a Data Disk to a Virtual Machine](#)
- [How to Detach a Data Disk from a Virtual Machine](#)
- [Creating and Uploading a Virtual Hard Disk that Contains the Windows Server Operating System](#)

- [Creating and Uploading a Virtual Hard Disk that Contains the Linux Operating System](#)
- [How to Capture an Image of an Azure Virtual Machine into the Gallery](#)

### **Troubleshooting**

- [Error deleting VHD: There is currently a lease on the blob and no lease ID was specified in the request](#)

## **7.4 Active Directory, DNS and Security**

### **Windows Azure AD, DNS, and security documentation**

- [Using Active Directory Service](#)
- [Active Directory Best Practices](#)
- [Managing Trusts](#)
- [Managing Sites](#)
- [Guidelines for Deploying Windows Server Active Directory on Windows Azure Virtual Machines](#)
- [Install a Replica Active Directory Domain Controller in Windows Azure Virtual Networks](#)
- [Install a new Active Directory forest in Windows Azure](#)
- [Windows Azure Security Guidance](#)

## **7.5 Managing with Windows PowerShell and System Center**

### **Windows Azure PowerShell Management documentation**

- [Introducing the Windows PowerShell ISE \(Scripting IDE\)](#)
- [Getting started with Windows Azure PowerShell](#)
- [Windows Azure Management Cmdlet Reference](#)

### **System Center App Controller SP1 documentation**

- [Connecting a Windows Azure Subscription to App Controller](#)
- [How to Add Windows Azure Virtual Machines to a Deployed Service in System Center 2012 SP1](#)
- [How to Upload a Virtual Hard Disk or Image to Windows Azure](#)
- [How to Add or Remove a Windows Azure Storage Account](#)

### **System Center Orchestrator SP1 documentation**

- [Using Runbooks in System Center 2012 - Orchestrator](#)
- [Windows Azure Integration Pack for Orchestrator in System Center 2012 SP1](#)

## 7.6 Understanding the Azure Billing Model for IaaS

### Windows Azure IaaS Billing Model documentation

- [Virtual Machines consume Compute, Storage, Storage Transaction and Bandwidth Resources](#)
- [VPN is Currently Free in Preview, \\$.05/VPN Connected Hour in GA](#)

## 7.7 SharePoint deployment on Windows Azure Virtual Machines

### Windows Azure SharePoint deployments documentation

- [SharePoint Deployment on Windows Azure Virtual Machines](#)

## 7.8 Deploying databases in Windows Azure IaaS

### Windows Azure IaaS Database deployment documentation

- [Getting started with SQL Server on a Windows Azure virtual machine](#)
- [Provisioning a SQL Server Virtual Machine on Windows Azure](#)
- [Install MongoDB on a virtual machine running Windows Server 2008 R2 in Windows Azure](#)
- [Install MySQL on a virtual machine running Windows Server 2008 R2 in Windows Azure](#)

## 8 Appendix B: Workshop opportunities

Workshops are excellent ways for customers to further their understanding of Windows Azure. The goal is to provide customers with a real example or proof of concept (POC) of the feasibility to move their applications to a Windows Azure hybrid environment. In this section we provide three examples of how workshops can be organized and delivered:

- **3-day workshop.** The 3-day workshop focuses on a basic Windows Azure IaaS migration. It directly dives into the discovery of the application, planning, and implementation.
- **5-day workshop.** This workshop includes the statement of work from the 3-day workshop and adds setup and training of Windows Azure management and automation. The 5-day workshop addresses Windows Azure management and automation options with the Windows Azure Management PowerShell Cmdlets and/or Microsoft System Center 2012 SP1.<sup>13</sup> This workshop enables customers to understand how to properly perform automated deployments and how to manage Windows Azure features and Windows Azure Virtual Networks. Installation and configuration of Microsoft System Center is a pre-requisite for this workshop.
- **10-day workshop.** This workshop includes the statement of work from the 3-day workshop and adds setup and training of Microsoft System Center 2012 SP1. This workshop enables customers to implement Systems Center components (Core System Center, AppController, and Orchestrator) to capture telemetry and monitoring information and manage the application(s) migrated to Windows Azure.

To have a successful workshop, customers need to agree to have resources committed to the project. The following customer teams should be involved in designing the POC:

- **Operations team.** Person(s) that are responsible for the IT operations of the application. Need to have a deep understanding of the customer's required IT stack of applications that would have to be installed in the Windows Azure Virtual Machines.
- **Security team.** Person(s) that have a deep knowledge of the customer's network security, customer network topology, security policies, procedures, and security configuration.
- **Development team.** Person(s) that have domain knowledge of the application selected to be migrated to Windows Azure.
- **Management team.** Person(s) belonging to the management team who have support from their leadership team and who can communicate with project stakeholders and help remove blockers.

**Note:** Depending on the size of the organization, you may have resources sharing multiple roles or full divisions dedicated to a single role.

---

<sup>13</sup> Microsoft, System Center 2012, [www.microsoft.com/en-us/server-cloud/system-center/default.aspx](http://www.microsoft.com/en-us/server-cloud/system-center/default.aspx), Microsoft 2013.

## 8.1 3-day workshop

The 3-day workshop enables migration of a customer's application to Windows Azure IaaS. The following table lists example tasks that would be performed in a 3-day workshop:

3-day workshop	
<b>Day 1</b>	
<input type="checkbox"/>	Assist customer in setting up an Enterprise Agreement or Trial Azure subscription for the project
<input type="checkbox"/>	Lead customer through the Discovery step; document customer's environment and goals
<input type="checkbox"/>	Educate customer about Windows Azure IaaS: <ul style="list-style-type: none"> <li>○ Windows Azure IaaS overview</li> <li>○ Windows Azure storage</li> <li>○ Windows Azure networking (VNETs, DNS, AD DS, and setting up the VPN)</li> </ul>
<b>Day 2</b>	
<input type="checkbox"/>	Windows Azure IaaS deployment planning
<input type="checkbox"/>	Perform initial Windows Azure IaaS implementation
<input type="checkbox"/>	Perform AD DS implementation, either by using Windows Azure Active Directory or integrating with the customer's on-premise AD DS
<input type="checkbox"/>	Educate customer about the following Windows Azure features: <ul style="list-style-type: none"> <li>○ Windows Azure identity services</li> <li>○ Windows Azure Active Directory</li> <li>○ Data management</li> </ul>
<b>Day 3</b>	
<input type="checkbox"/>	Windows Azure Virtual Machines planning and deployment
<input type="checkbox"/>	Windows Azure Virtual Machines backup and restore planning and deployment
<input type="checkbox"/>	(Linux) Support customer in creating and managing Linux VMs
<input type="checkbox"/>	Educate customer about the following Windows Azure features: <ul style="list-style-type: none"> <li>○ SQL Server on Windows Azure IaaS</li> <li>○ SharePoint on Windows Azure IaaS</li> <li>○ Monitoring and management with System Center</li> <li>○ Demonstrate how the customer can extend the deployment to include dynamic management with System Center App Controller and Orchestrator</li> </ul>

## 8.2 5-day workshop with an existing System Center 2012 SP1

The 5-day workshop with an existing System Center deployment builds on the 3-day training. It adds Windows Azure management and automation using the existing Microsoft System Center 2012 SP1 deployment. The following table lists tasks that would be performed in a 5-day workshop:

## 5-day workshop – with existing System Center 2012 SP1

5-day workshop – with existing System Center 2012 SP1	
<b>Day 1</b>	
<input type="checkbox"/>	Assist customer in setting up an Enterprise Agreement or Trial Azure subscription for the project
<input type="checkbox"/>	Lead customer through the Discovery step and document customer's environment and goals
<input type="checkbox"/>	Educate customer about Windows Azure IaaS: <ul style="list-style-type: none"> <li>○ Windows Azure IaaS overview</li> <li>○ Windows Azure storage</li> <li>○ Windows Azure networking (VNETs, DNS, AD DS, and setting up the VPN)</li> </ul>
<b>Day 2</b>	
<input type="checkbox"/>	Windows Azure IaaS deployment planning
<input type="checkbox"/>	Perform initial Windows Azure IaaS implementation
<input type="checkbox"/>	Perform AD DS implementation, either by using Windows Azure Active Directory or integrating with the customer's on-premise AD DS
<input type="checkbox"/>	Educate customer about the following Windows Azure features: <ul style="list-style-type: none"> <li>○ Windows Azure identity services</li> <li>○ Windows Azure Active Directory</li> <li>○ Data management</li> </ul>
<b>Day 3</b>	
<input type="checkbox"/>	Windows Azure Virtual Machines planning and deployment
<input type="checkbox"/>	Windows Azure Virtual Machines backup and restore planning and deployment
<input type="checkbox"/>	(Linux) Support customer in creating and managing Linux VMs
<input type="checkbox"/>	Educate customer about the following Windows Azure features: <ul style="list-style-type: none"> <li>○ SQL Server on Windows Azure IaaS</li> <li>○ SharePoint on Windows Azure IaaS</li> <li>○ Monitoring and management with System Center</li> <li>○ Demonstrate how the customer can extend the deployment to include dynamic management with System Center App Controller and Orchestrator</li> </ul>
<b>Day 4</b>	
<input type="checkbox"/>	Work with customer to create and install a management certificate in the Windows Azure Management Portal
<input type="checkbox"/>	Configure App Controller 2012 SP1
<input type="checkbox"/>	Educate customer about the following: <ul style="list-style-type: none"> <li>○ System Center App Controller</li> </ul>

	<ul style="list-style-type: none"> <li>○ Use of System Center App Controller for managing Windows Azure</li> </ul>
<b>Day 5</b>	
<input type="checkbox"/>	Install the Windows Azure Integration Pack for Orchestrator 2012 SP1
<input type="checkbox"/>	Co-author sample run books with the customer to demonstrate automated deployment and deletion of IaaS Virtual Machines
<input type="checkbox"/>	Educate customer about the following: <ul style="list-style-type: none"> <li>○ Use of the Windows Azure Integration Pack for Orchestrator</li> <li>○ Advanced automation scenarios that can be achieved by combining Service Manager provisioning portals with run books</li> </ul>

### 8.3 5-day workshop without System Center

The 5-day workshop without an existing System Center deployment. This workshop builds on the 3-day training and adds Windows Azure management and automation using Windows PowerShell scripts and the Windows Azure management's PowerShell cmdlets. The following table lists example tasks that would be performed in this 5-day workshop:

5-day workshop – without existing System Center 2012 SP1	
<b>Day 1</b>	
<input type="checkbox"/>	Assist customer in setting up an Enterprise Agreement or Trial Azure subscription for the project
<input type="checkbox"/>	Lead customer through the Discovery step and document customer's environment and goals
<input type="checkbox"/>	Educate customer about Windows Azure IaaS: <ul style="list-style-type: none"> <li>○ Windows Azure IaaS overview</li> <li>○ Windows Azure storage</li> <li>○ Windows Azure networking (VNets, DNS, AD DS, and setting up the VPN)</li> </ul>
<b>Day 2</b>	
<input type="checkbox"/>	Windows Azure IaaS deployment planning
<input type="checkbox"/>	Perform initial Windows Azure IaaS implementation
<input type="checkbox"/>	Perform AD DS implementation, either by using Windows Azure Active Directory or integrating with the customer's on-premise AD DS
<input type="checkbox"/>	Educate customer about the following Windows Azure features: <ul style="list-style-type: none"> <li>○ Windows Azure identity services</li> <li>○ Windows Azure Active Directory</li> <li>○ Data management</li> </ul>
<b>Day 3</b>	

<input type="checkbox"/>	Windows Azure Virtual Machines planning and deployment
<input type="checkbox"/>	Windows Azure Virtual Machines backup and restore planning and deployment
<input type="checkbox"/>	(Linux) Support customer in creating and managing Linux VMs
<input type="checkbox"/>	Educate customer about the following Windows Azure features: <ul style="list-style-type: none"> <li>○ SQL Server on Windows Azure IaaS</li> <li>○ SharePoint on Windows Azure IaaS</li> <li>○ Monitoring and management with System Center</li> <li>○ Demonstrate how the customer can extend the deployment to include dynamic management with System Center App Controller and Orchestrator</li> </ul>
<b>Day 4</b>	
<input type="checkbox"/>	Work with customer to create and install a management certificate in the Windows Azure Management Portal
<input type="checkbox"/>	Work with the customer to create scenarios that can be automated
<input type="checkbox"/>	Educate customer about the following: <ul style="list-style-type: none"> <li>○ Windows PowerShell tools such as ISE</li> <li>○ Windows Azure PowerShell Management cmdlets</li> </ul>
<b>Day 5</b>	
<input type="checkbox"/>	Work with the customer to co-author Windows PowerShell scripts to automate the planned scenarios

## 8.4 10-day workshop

The 10-day workshop builds on the 3-day training and adds information about end-to-end Windows Azure management and automation using the full suite of Microsoft System Center 2012 SP1 tools and features. The following table lists example tasks that would be performed in a 10-day workshop:

10-day workshop	
<b>Day 1</b>	
<input type="checkbox"/>	Assist customer in setting up an Enterprise Agreement or Trial Azure subscription for the project
<input type="checkbox"/>	Lead customer through the Discovery step and document customer's environment and goals
<input type="checkbox"/>	Educate customer about Windows Azure IaaS: <ul style="list-style-type: none"> <li>○ Windows Azure IaaS overview</li> <li>○ Windows Azure storage</li> <li>○ Windows Azure networking (VNETs, DNS, AD DS, and setting up the VPN)</li> </ul>
<b>Day 2</b>	



<input type="checkbox"/>	Windows Azure IaaS deployment planning
<input type="checkbox"/>	Perform initial Windows Azure IaaS implementation
<input type="checkbox"/>	Perform AD DS implementation, either by using Windows Azure Active Directory or integrating with the customer's on-premise AD DS
<input type="checkbox"/>	Educate customer about the following Windows Azure features: <ul style="list-style-type: none"> <li>○ Windows Azure identity services</li> <li>○ Windows Azure Active Directory</li> <li>○ Data management</li> </ul>
<b>Day 3</b>	
<input type="checkbox"/>	Windows Azure Virtual Machines planning and deployment
<input type="checkbox"/>	Windows Azure Virtual Machines backup and restore planning and deployment
<input type="checkbox"/>	(Linux) Support customer in creating and managing Linux VMs
<input type="checkbox"/>	Educate customer about the following Windows Azure features: <ul style="list-style-type: none"> <li>○ SQL Server on Windows Azure IaaS</li> <li>○ SharePoint on Windows Azure IaaS</li> <li>○ Monitoring and management with System Center</li> <li>○ Demonstrate how the customer can extend the deployment to include dynamic management with System Center App Controller and Orchestrator</li> </ul>
<b>Day 4</b>	
<input type="checkbox"/>	Work with the customer to plan and deploy a basic System Center Deployment, including Orchestrator and App Controller 2012 SP1
<input type="checkbox"/>	Work with customer to create and install a management certificate in the Windows Azure Management Portal
<b>Day 5</b>	
<input type="checkbox"/>	Configure App Controller 2012 SP1
<input type="checkbox"/>	Educate customer about the following: <ul style="list-style-type: none"> <li>○ System Center App Controller</li> <li>○ Use of System Center App Controller for managing Windows Azure</li> </ul>
<b>Days 6-7-8</b>	
<input type="checkbox"/>	Install the Windows Azure Integration Pack for Orchestrator 2012 SP1
<input type="checkbox"/>	Co-author sample run books with the customer to demonstrate automated deployment and deletion of IaaS Virtual Machines
<input type="checkbox"/>	Educate customer about the following: <ul style="list-style-type: none"> <li>○ Use of the Windows Azure Integration Pack for Orchestrator</li> </ul>

	<ul style="list-style-type: none"> <li>○ Advanced automation scenarios that can be achieved by combining Service Manager provisioning portals with run books</li> </ul>
<b>Days 9-10</b>	
<input type="checkbox"/>	Work with customer to plan and implement advanced automation scenarios
<input type="checkbox"/>	Verify and test advanced automation scenarios

## 9 Appendix C: Checklists

This sections contains discovery and planning checklists to help you work through the entire process.

### 9.1 Discovery checklist

Discovery checklist	
<b>Networking</b>	
<input type="checkbox"/>	<p><b>Network diagram:</b> Review, draw, and collect a basic diagram of the customer’s network environment that relates to the application(s) to be connected to the hybrid cloud.</p> <p><b>Reason:</b> Need to understand the current network topology and components to properly design and address changes to enable the hybrid cloud implementation.</p>
<input type="checkbox"/>	<p><b>Routers/firewalls:</b> Collect the following information:</p> <ul style="list-style-type: none"> <li>○ Makes and models</li> <li>○ Firmware version / level</li> </ul> <p><b>Reason:</b> Windows Azure Virtual Networks currently support a specific list of routers and firewalls. We need to verify whether the on-premises configuration will allow correct connectivity to the IaaS environment from a network perspective.</p>
<input type="checkbox"/>	<p><b>IP addresses:</b> Collect the following information:</p> <ul style="list-style-type: none"> <li>○ What is the edge network IP address or IP ranges?</li> <li>○ Network ranges in use on the customer WAN</li> </ul> <p><b>Reason:</b> Information needed to set up the Windows Azure Virtual Network.</p>
<input type="checkbox"/>	<p><b>Customer network:</b> Collect the following information about the customer network:</p> <ul style="list-style-type: none"> <li>○ Number and size of current Internet connection (primary, fail over, burstable)</li> <li>○ Does the ISP contract allow bandwidth increase?</li> </ul> <p><b>Reason:</b> Understanding what portion of the customer’s network will be used for the Windows Azure Virtual Network. In addition, the customer may see an increase in bandwidth consumption.</p>
<input type="checkbox"/>	<p><b>Perimeter network (also known as DMZ, demilitarized zone, and screened subnet):</b> Identify whether the perimeter network is relevant for the application to be hybrid cloud-enabled.</p> <p><b>Reason:</b> The <b>perimeter network</b> may have different network settings, firewall permissions, ACLs, and so on, which need to be taken into account when setting up the architecture for the hybrid cloud environment running the applications.</p>

<input type="checkbox"/>	<p><b>Customer IT software stack:</b> Identify the IT software stack that the customer may have installed in the environment as part of their IT policies and procedures. This stack may also need to be installed in the Windows Azure Virtual Machines. Check the following:</p> <ul style="list-style-type: none"> <li>○ Software to be installed and its purpose</li> <li>○ Software type (antivirus, management agent, security agent, and so on)</li> <li>○ Network requirements (bandwidth, ports)</li> </ul> <p><b>Reason:</b> Understand the extra software that would need to be installed in the virtual machines and ports to be open in the virtual machines' firewalls.</p>
<b>Application servers and locations</b>	
<input type="checkbox"/>	<p><b>Physical or virtual server:</b> Identify the servers used by the application and whether they are virtualized.</p> <ul style="list-style-type: none"> <li>○ Server name – usage</li> <li>○ Virtualization layer (such as Hyper-V, VMWare, Virtual Box)</li> <li>○ Application tier</li> </ul> <p><b>Reason:</b> Physical machines and virtual machines that are under Hyper-V and other supported virtualization layers maybe ported directly<sup>14</sup> to the Windows Azure IaaS environment.</p>
<input type="checkbox"/>	<p><b>Physical server locations:</b> Identify the physical location of each server in the application(s) landscape:</p> <ul style="list-style-type: none"> <li>○ Server location</li> <li>○ Multiple data centers</li> <li>○ Perimeter network</li> </ul> <p><b>Reason:</b> When the application is moved to a hybrid cloud environment, some tier will be placed in Windows Azure. In addition, applications that span multiple data centers bring more challenges. It is important to understand connectivity and latencies between data centers, security (VPN, direct patching), and the network gateways (routers/firewalls) that are used.</p>

<sup>14</sup> Microsoft, Adding Hyper-V Hosts and Host Clusters to VMM, <http://technet.microsoft.com/en-us/library/gg610605.aspx>, TechNet, 2013.

Identifying target workloads	
<input type="checkbox"/>	<p><b>Identify workloads and application(s):</b> Identify what workloads and application(s) are going to be deployed in the hybrid cloud:</p> <ul style="list-style-type: none"> <li>○ Microsoft products</li> <li>○ Third-party applications</li> <li>○ IT software stack required by customer's IT policies</li> <li>○ Network latency SLA for the application(s)</li> </ul> <p><b>Reason:</b> To ensure the customer will be successful in adopting the hybrid cloud model, we need to model the architecture in such a way that the workloads perform and operate at least equal to their performance/operation before the migration. To achieve this goal, we need to become concrete about the external dependencies of the applications within this architecture and ensure we know up front whether we are taking on something on which we can deliver.</p>
<input type="checkbox"/>	<p><b>List servers targeted for migration to Windows Azure:</b> Identify the following server information:</p> <ul style="list-style-type: none"> <li>○ Operating system</li> <li>○ Number of CPU cores and speed</li> <li>○ Amount of RAM</li> <li>○ Number and size of disk volumes</li> <li>○ Special I/O considerations, for example the number of IOPS needed</li> </ul> <p><b>Reason:</b> Sizing the virtual machines for a given workload is equally important on-premises as it is in Windows Azure. To ensure we can achieve our customer's goals, we need to identify how best to achieve them. If the specifications in this list exceed the current IaaS constraints, we might need to set up a mitigation plan for this workload or defer the migration to a moment in time in line with our roadmap.</p>
Backup procedures	
<input type="checkbox"/>	<p><b>Customer backup procedures:</b> Identify the backup procedures that apply to the workload and application(s) to be migrated to Windows Azure:</p> <ul style="list-style-type: none"> <li>○ How are the workload's backups currently performed?</li> <li>○ What are the data retention requirements?</li> <li>○ Are there any compliance requirements?</li> <li>○ What is the latency SLA for the backup solution that is used?</li> <li>○ What disaster recovery and business continuity solutions/procedures are currently in place for the workloads to be moved to Windows Azure?</li> </ul> <p><b>Reason:</b> The specifications from this list allow us to assess the feasibility of the migration and might lead to suggestions on changing procedures or setting up an architecture where some information stores continue to reside within the on-premises environment.</p>

Active Directory Domain Services (AD DS) and security topology	
<input type="checkbox"/>	<p><b>Customer AD DS:</b> Identify the AD DS instantiation that applies to the workload and application(s) to be migrated to Windows Azure:</p> <ul style="list-style-type: none"> <li>○ Functional level</li> <li>○ Number and location of AD DS servers</li> <li>○ DNS topology. What is AD DS integrated?</li> <li>○ Are there any sub-domains?</li> </ul> <p><b>Reason:</b> To determine if there is a need to deploy Domain Controllers as part of the deployment and if they have to be configured as Read-Write or Read Only. In addition, there is a need to determine if the primary domain will be extended, or a subdomain, or a standalone domain will be created.</p>
<input type="checkbox"/>	<p><b>Customer AD DS Security Topology:</b> Identify the AD DS topology that applies to the workload and application(s) to be migrated to Windows Azure:</p> <ul style="list-style-type: none"> <li>○ Are there corporate policies regarding the type of AD DS? <ul style="list-style-type: none"> <li>▪ Core, limited trust, full, read only?</li> <li>▪ What configuration can be deployed in Windows Azure?</li> </ul> </li> </ul> <p><b>Reason:</b> To determine if there is a need to deploy Domain Controllers as part of the deployment and if they have to be configured as Read-Write or Read Only. In addition, there is a need to determine if the primary domain will be extended, or a subdomain, or a standalone domain will be created.</p>

## 9.2 Planning checklist

Planning checklist	
<b>Planning step documents</b>	
<input type="checkbox"/>	<p><b>Identity management, DNS, and security plan:</b> This document describes the plan for the identity manager configuration and usage, DNS configuration and integration, the application's resiliency requirements, the security configuration, and software to be used by the application that is migrated to Windows Azure.</p>
<input type="checkbox"/>	<p><b>Network topology diagram</b></p>
<input type="checkbox"/>	<p><b>Network topology documentation:</b> Any additional information that complements the Network topology diagram.</p>
<input type="checkbox"/>	<p><b>Virtual machine templates document:</b> Collect all the information from the discovery step and the agreements with the customer and summarize it in a document.</p>
<input type="checkbox"/>	<p><b>Windows Azure subscriptions:</b> Define what subscription(s) will be used by the application. Gather the subscription information and who would be managing it at the customer.</p>

<input type="checkbox"/>	<p><b>Windows Azure support:</b> Define the level of Windows Azure support required by the application. This may be driven by the application SLA and business criticality. Also, verify whether the customer has already an Enterprise Agreement, because some of the resources could be used to provide Windows Azure support.</p>
--------------------------	--

## 10 References and Bibliography

Microsoft, Application Portfolio Assessment and Cloud Migration Planning VRF Accelerator, <https://campus.partners.extranet.microsoft.com/esportal/Library/IP/Forms/Document%20Set/docs/ethomepage.aspx?ID=2014&FolderCTID=0x0120D520007E465FED93236A4F8535853D09D739A0&List=8b3507dc-f672-46bc-84c1-166758b96d95&RootFolder=%2Fesportal%2FLibrary%2FIP%2FVRF%2FVRF%20Accelerators%2FIT%20Led%20Change%2FApplication%20Portfolio%20Assessment%20and%20Cloud%20Migration%20Planning%20VRF%20Accelerator/> , 2013

Roshan N Y, "Guidance on Latency and Bandwidth for SharePoint 2010" Retrieved from [http://blogs.msdn.com/b/sharepoint\\_cloud/archive/2012/09/20/guidance-on-latency-and-bandwidth-for-sharepoint-2010.aspx](http://blogs.msdn.com/b/sharepoint_cloud/archive/2012/09/20/guidance-on-latency-and-bandwidth-for-sharepoint-2010.aspx), MSDN Blogs, Sept. 20, 2012

Microsoft, "Understanding Sites, Subnets, and Site Links" <http://technet.microsoft.com/en-us/library/cc754697.aspx>, TechNet, 2012.

Microsoft, "Windows Azure Active Directory" <http://msdn.microsoft.com/en-us/library/windowsazure/jj673460.aspx>, MSDN, Apr. 9, 2013

Microsoft, "Access Control Service 2.0" <http://msdn.microsoft.com/en-us/library/windowsazure/hh147631.aspx> , MSDN, Feb. 28, 2013

Microsoft, "Active Directory Integration" [http://technet.microsoft.com/en-us/library/cc737383\(v=WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc737383(v=WS.10).aspx) ,TechNet, Jan. 21, 2005

Microsoft, "SDL Threat Modeling Tool" [www.microsoft.com/security/sdl/adopt/threatmodeling.aspx](http://www.microsoft.com/security/sdl/adopt/threatmodeling.aspx) , Microsoft.com, 2013

M. Mercuri, U. Homann, A. Townhill, "Fail-safe: Guidance for Resilient Cloud Architectures" <http://msdn.microsoft.com/en-us/library/windowsazure/jj853352.aspx>, MSDN, November, 2012

Microsoft, "Networking" [www.windowsazure.com/en-us/manage/services/networking/](http://www.windowsazure.com/en-us/manage/services/networking/) , WindowsAzure.com, 2013

Microsoft, "About VPN Devices for Virtual Network" <http://msdn.microsoft.com/en-us/library/windowsazure/jj156075.aspx> , WindowsAzure.com, 2013

Microsoft, "System Center 2012" [www.microsoft.com/en-us/server-cloud/system-center/default.aspx](http://www.microsoft.com/en-us/server-cloud/system-center/default.aspx), Microsoft.com, 2013

Microsoft, "Adding Hyper-V Hosts and Host Clusters to VMM" <http://technet.microsoft.com/en-us/library/gg610605.aspx>, TechNet, Jan. 15, 2013