XenDesktop 7 on Windows Azure

Design Guide

Contents

About This Design Guide

The Citrix Design Guide provides an overview of the XenDesktop 7 on Azure solution architecture and implementation. This design has been created through architectural design best practices obtained from Citrix Consulting Services and thorough lab testing, and is intended to provide guidance for solution evaluation and the introduction of proof of concepts.

The Design Guide incorporates generally available products into the design, and employs repeatable processes for the deployment, operation, and management of components within the solution.

Overview

With the introduction of Azure support for Remote Desktop Services Subscriber Access Licenses (RDS SALs) a broad set of opportunities to leverage Azure for hosted desktops and applications begin to unfold. As a platform Microsoft Azure provides a robust, state of the art infrastructure and global presence for enterprises and service providers.

Citrix customers wanting to leverage public cloud infrastructure as a service in order to expand their on premise datacenter capabilities, without investing in new capital resources, can now host desktops and applications using XenDesktop 7 within Azure. This capability enables faster proof of concept and pilot builds for migration to XenDesktop 7 for existing XenDesktop implementations, or as part of a new XenDesktop implementation where the leverage of public cloud infrastructure is preferred.

This document provides high level design guidance using a sample implementation of XenDesktop 7 Hosted Shared and Server VDI Flexcast models within the Microsoft Windows Azure cloud.

- Hosted Shared Desktops are built upon Windows Server 2008 R2 and Windows Server 2012 RDS Session Host servers where multiple user sessions execute on a single shared server instance.
- Server VDI Desktops are built upon Windows Server 2008 R2 and Windows Server 2012 for use cases where a single user requires a VDI-like dedicated or pooled server instance which provides an execution environment that is not shared.

Used in conjunction with the XenDesktop Modular Reference Architecture this document provides basic best practice guidance for companies looking to leverage Citrix and Microsoft cloud technologies to deliver a state of the art solution for their users.

Use Case

Let's assume "World-wide Co, Inc." (WWCo) plans to leverage Microsoft and Citrix products to deliver a hosted desktop solution for their accounting department. The solution will provide value to the department by enabling access to hosted desktops and applications from any device. The value of this solution for World-wide Co. is most evident in the ability to quickly bring new desktop services on line through a subscription to Azure infrastructure services rather than a protracted capital investment and datacenter build out project. Since the new desktops are an extension of the existing World-wide Co datacenter, the infrastructure already in place at World-wide Co. will be connected to Azure through a Site-to-Site VPN. This connectivity enables the Azure hosted XenDesktops to communicate with World-wide Co. corporate Active Directory and Back-office services like Microsoft Exchange or Microsoft Lync, as well as the corporate Secure Remote Access services Enabled through Citrix NetScaler Gateway.

The objective of this guide is to outline World-wide Co. business considerations, and how hosting their new XenDesktop 7 Windows Server based Flexcast models in Azure could address them.

Business Objectives

- Provide secure access to desktops and applications for the accounting team
- Avoid the need to build new infrastructure within the WWCo datacenter
- Leverage as much existing corporate infrastructure as possible to align with current IT practices and policies and to keep new expenses as low as possible.
- Use monthly programmatic funding instead of capital expenses for this project
- Manage the service within a public cloud environment in order to scale based on seasonal resource requirements
- Provide support for any device, enabling temporary contractors to "Bring your own Device"

Technical Objectives

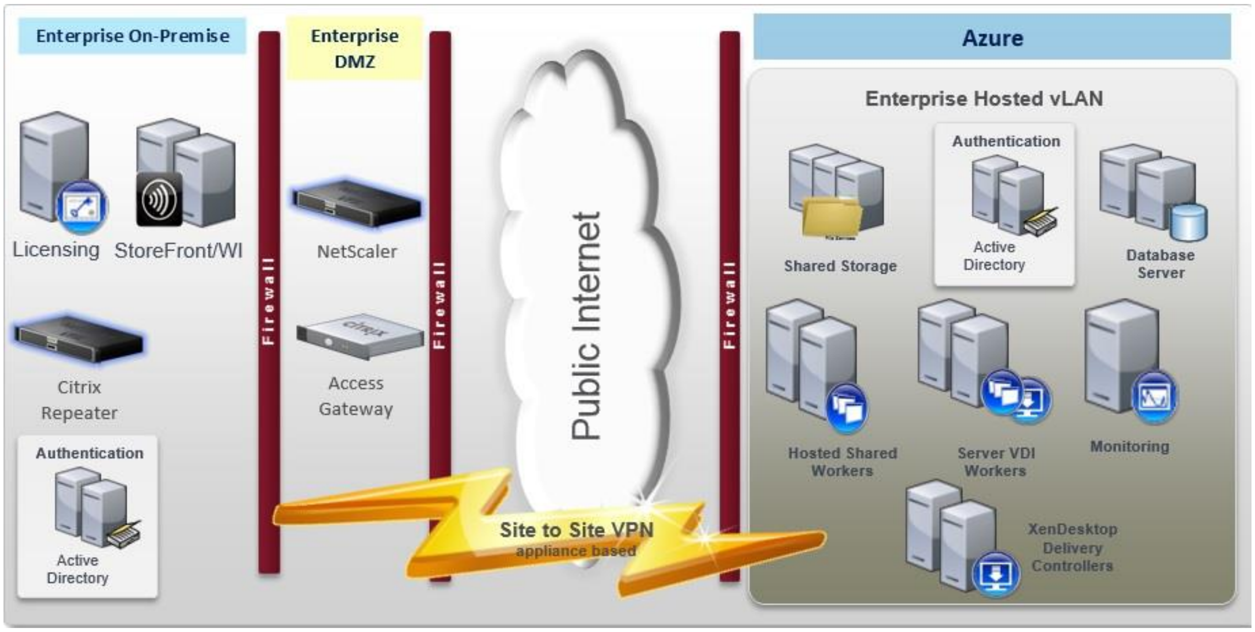
- Quickly design and implement environment to establish the value and metrics.
- Ensure high availability of critical components to ensure business continuity.
- Implement an "n+1" highly available solution to avoid any business interruption.
- Support access from user-owned devices that vary in form factor and operating system

Citrix XenDesktop 7 on Azure

World-wide Co. selected XenDesktop as their solution since it enables the best user experience across the public internet from any device according to independent analysis, and after reviewing the Citrix XenDesktop Modular Reference Architecture and Microsoft's Windows Azure IaaS capabilities, they believed they could build a solution without a large upfront capital investment.

The Citrix XenDesktop 7 solution hosted on Azure consisted of a small number of components,

- Citrix XenDesktop 7 Delivery controllers
- Hosted Shared workers (Windows Server RDS Session Host enabling "Session Isolation")
- and Server VDI Workers (Windows Server pooled or dedicated "VDI-like" VM Isolation)
- An Azure local Active Directory DC that is a member of the World-wide Co. Corporate Forest.
- An Azure local SQL Server VM Instance
- An Azure local File Server for the storage of XenDesktop Roaming User Profiles.



The remaining components were already in place in the World-wide Co. on premise corporate datacenter.

A brief description of key Citrix components follows:

- **Citrix Receiver.** Citrix Receiver is an easy-to-install client software that lets you access your docs, applications and desktops from any of your devices including smartphones, tablets and PCs.
- **Citrix XenDesktop Delivery controllers.** These XenDesktop 7 Servers are used to manage and deliver dedicated the Windows applications and desktops.
- **Hosted Shared Workers.** These XenDesktop 7 workloads, leveraging Windows Server Remote Desktop Services Session Host as the foundation, are used to deliver shared hosted applications and desktops for most users.
- **Server VDI Workers.** These XenDesktop 7 workloads, using Windows Server without the Remote Desktop Services Session Host role, provide "VDI-like" VM or Server level isolation of an individual server instance for those users that require more customization or administrative control of their virtual desktop.
- **Citrix License Server.** The Citrix License Server hosts all of the licenses that enable Citrix products and features.
- **NetScaler Gateway.** NetScaler Gateway is a secure application and data access solution that provides administrators granular application- and data-level control while empowering users with remote access from anywhere.

- **StoreFront Services.** StoreFront Services provides authentication and resource delivery services for Citrix Receiver, enabling you to create centralized enterprise stores to deliver desktops, applications, and other resources to users on any device, anywhere.

XenDesktop 7 on Azure Architecture

Once World-wide Co. had completed their assessment and concluded that a Citrix XenDesktop 7 solution on Microsoft Azure could meet their objectives, they quickly moved into the design phase. World-wide Co. wanted a simple, easy process to determine the hardware and storage sizing to support their individual implementation based on the needs of their subscribers. World-wide Co. used Citrix Project Accelerator- an open, web-based application where you can manage your move to virtualized desktops and applications based on best practices of Citrix's top consultants - to assist with the user assessment and environment design. In conjunction with project accelerator guidance, World-wide Co. made the following design decisions:

- Although Project Accelerator was currently designed for XenApp 6.5 and XenDesktop 5.6 versions of the Citrix products, World-wide Co. decided that its output could be used as a foundational design to work from in conjunction with their own testing to determine the final requirements when they went to production. Please Note: Although in order to remain consistent with the true ouputs of the Project Accelerator tool we have left the original graphic outputs of the Project Accelerator by showing "Windows 7" as one of the desktop images to deploy, the actual implementation on Azure must use Windows Server 2008 R2 or Windows Server 2012 instances to enable "Server VDI" for these desktops. Windows Client operating systems are not licensed for hosting on Azure at this time. The output of the Project Accelerator is only part of the data used to design the complete solution and some Azure specific adjustments must be made in order to remain compliant with Microsoft licensing. More detail is available in the "Solution Capabilities and Constraints" section of this guide.

- For a robust solution high availability is important, so an "N+1" configuration was chosen to ensure that the solution sizing included a spare server to handle user capacity in the event of a failure.

- All users would need to connect to Azure over an encrypted connection through a Site-to-Site VPN between Azure and the World-wide Co. corporate network. Secure remote access would be provided by NetScaler Gateways within the corporate network.

- Active Directory, DNS/DHCP, and SQL Server would be provisioned in Azure to reduce login times for this solution.

- A variety of financial applications, as well as MS Office would be made available as part of the standard desktop image for this group of users.

The following architecture is a visual representation of the solution as recommended by Citrix Project Accelerator. Additional considerations that leverage this output as the base are documented later in this guide. The following diagram represents World-wide Co.'s projected hardware, and infrastructure requirements based on a team of 100 users, spread over the 2 types of users; task workers and content creators.

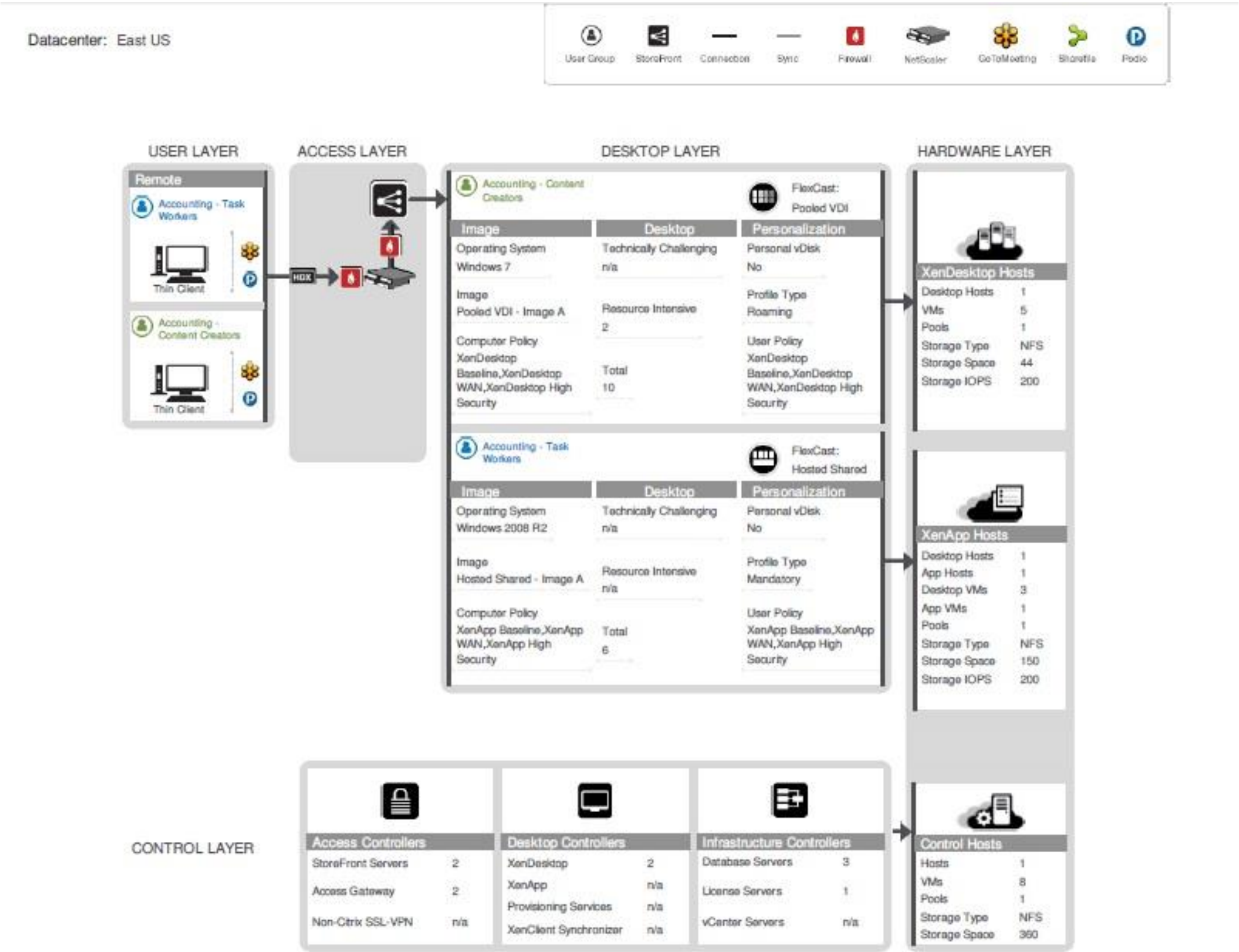
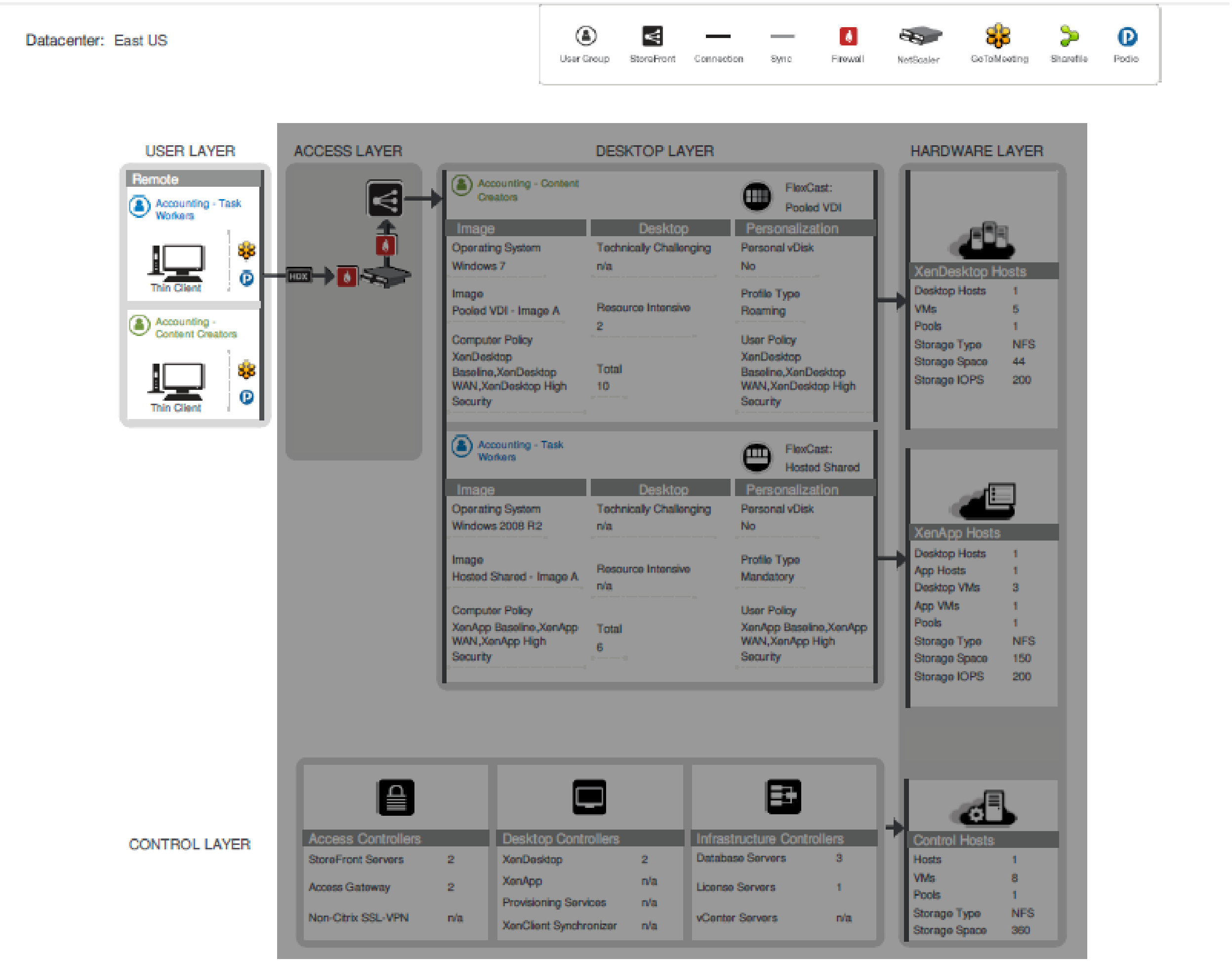


Figure 1: Project Accelerator Output for World-wide Co. XenDesktop 7 on Azure Project

Each layer of the architecture diagram is discussed in detail below:

User Group

The User Group layer represents the subscriber types that will access the Azure hosted desktops from their own end-point devices. Although the graphic represents these devices as "Thin Clients" these devices can be anything from a SmartPhone, Tablet, PC, Mac, or Linux desktop or laptop. These user groups represent the use cases of "Task Worker" or "Content Creator". The details of what is delivered to these different user groups is enabled within the Desktop layer which address after the Access Layer section below.



Datacenter: East US

USER LAYER

Remote

Accounting - Task Workers

Accounting - Content Creators

ACCESS LAYER

DESKTOP LAYER

Accounting - Content Creators

FlexCast: Pooled VDI

Image	Desktop	Personalization
Operating System Windows 7	Technically Challenging n/a	Personal vDisk No
Image Pooled VDI - Image A	Resource Intensive 2	Profile Type Roaming
Computer Policy XenDesktop Baseline,XenDesktop WAN,XenDesktop High Security	Total 10	User Policy XenDesktop Baseline,XenDesktop WAN,XenDesktop High Security

Accounting - Task Workers

FlexCast: Hosted Shared

Image	Desktop	Personalization
Operating System Windows 2008 R2	Technically Challenging n/a	Personal vDisk No
Image Hosted Shared - Image A	Resource Intensive n/a	Profile Type Mandatory
Computer Policy XenApp Baseline,XenApp WAN,XenApp High Security	Total 6	User Policy XenApp Baseline,XenApp WAN,XenApp High Security

HARDWARE LAYER

XenDesktop Hosts	
Desktop Hosts	1
VMs	5
Pools	1
Storage Type	NFS
Storage Space	44
Storage IOPS	200

XenApp Hosts	
Desktop Hosts	1
App Hosts	1
Desktop VMs	3
App VMs	1
Pools	1
Storage Type	NFS
Storage Space	150
Storage IOPS	200

CONTROL LAYER

Access Controllers	
StoreFront Servers	2
Access Gateway	2
Non-Citrix SSL-VPN	n/a

Desktop Controllers	
XenDesktop	2
XenApp	n/a
Provisioning Services	n/a
XenClient Synchronizer	n/a

Infrastructure Controllers	
Database Servers	3
License Servers	1
vCenter Servers	n/a

Control Hosts	
Hosts	1
VMs	8
Pools	1
Storage Type	NFS
Storage Space	360

Figure 2: User Group

World-wide Co. requires the following Citrix components on each end-point device:

- **Citrix Receiver.** Citrix Receiver is an universal thin client that runs on virtually any device operating platform, including Windows, Mac®, Linux®, iOS® and Android®. This is the one client users need to access business-critical apps and data from today's latest tablet and smartphone devices and improve their mobility. Citrix Receiver can be downloaded and installed by each employee on their personal devices.

Access Layer

The access layer consists of the servers responsible for providing connectivity to the XenDesktop 7 on Azure environment.

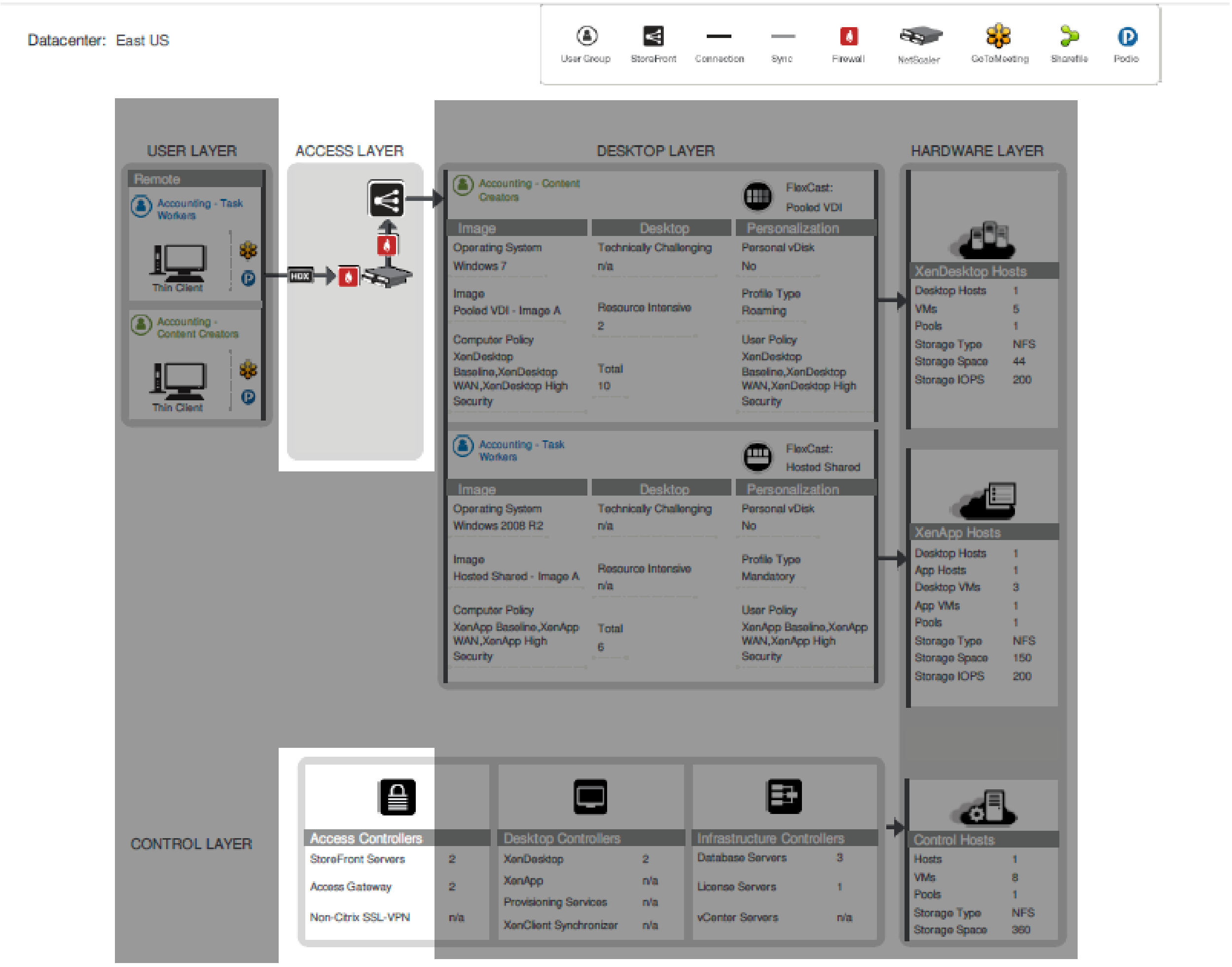


Figure 3: Access Layer

WWCO's solution required the following Citrix components to provide secure remote access:

- **StoreFront Services.** StoreFront Services provides a self-service subscription service to desktops and applications via an enterprise app store, giving users convenient access to all the resources they need. WWCO created a centralized enterprise app store with StoreFront Services within their on-premise datacenter to enumerate and aggregate the resources available for each user. WWCO deployed a pair of StoreFront servers to ensure high availability.

StoreFront Services Servers	
Instances	2 StoreFront Server VMs
Virtual Machine Configurations	
Memory	4 GB RAM

StoreFront Services Servers	
Processor	2 vCPUs
Hard Drive	60 GB
Installed Software [1]	
Web Interface	StoreFront 2.0
Windows Server	Windows Server 2012
IIS	7.5 or greater
Microsoft .NET Framework	4.0
Ports Utilized	
StoreFront	80, 443, 808

- **NetScaler Gateway.** NetScaler Gateway is a secure application and data access solution that gives administrators granular application and data-level control while empowering users with remote access from anywhere. IT administrators gain a single point of management for controlling access and limiting actions within sessions based on user identity and the endpoint device. The results are better application security, data protection and compliance management.

  NetScaler Gateway works in conjunction with StoreFront Services to authenticate the user and create an SSL tunnel between the end-user and NetScaler Gateway to ensure secure remote access from any device. NetScaler Gateway requires either a physical or virtual NetScaler appliance. WWCO selected two physical NetScaler MPX appliances to host NetScaler Gateway in an active/active mode to ensure secure access is highly available and maximum capacity.

NetScaler Gateway	
Instances	
NetScaler MPX	2 physical NetScaler MPX-5500
Build	9.3
Throughput	500 Mbps
Ports Utilized	
DMZ	80, 443
Internal	80, 443, 1494, and 2598

  Citrix recommends installing NetScaler Gateway in the network DMZ. When installed in the DMZ, NetScaler Gateway participates on two networks: a private network and the Internet with a publicly routable IP address. NetScaler Gateway can be used to partition local area networks internally in the organization for access control and security by creating partitions between wired or wireless networks and between data and voice networks.

  The NetScaler Gateway MPX appliance supports Versions 9.2, 9.3, and 10 of the NetScaler Gateway software. Click here for detailed specifications of NetScaler Gateway MPX appliance.

Desktop Layer

The Desktop layer represents the separate use cases that WWCO will service. As you can see, plans for 95 users to access Task Worker resources, and 5 users to access Content Creator resources.

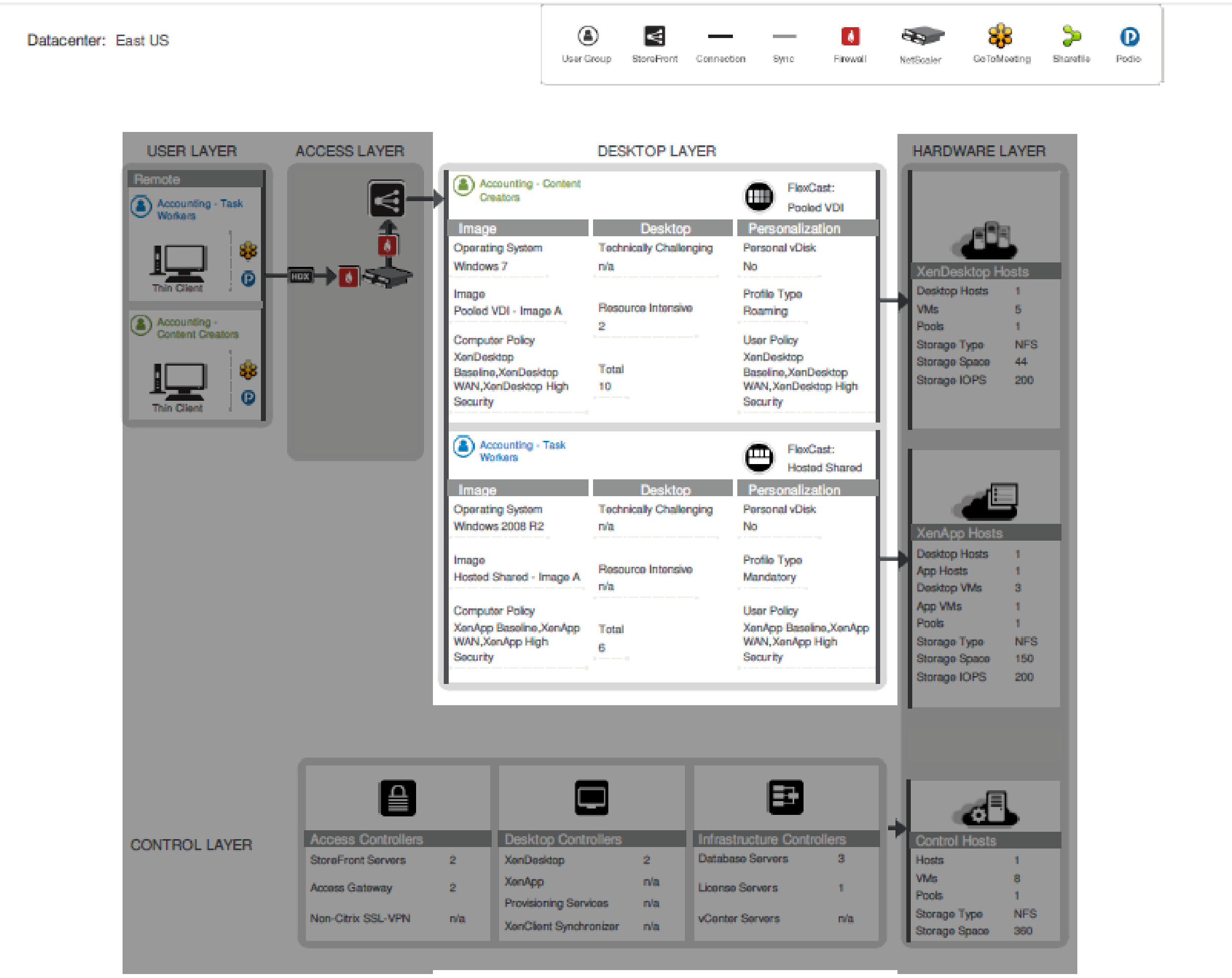


Figure 4:Desktop Layer

The WWCO solution required the following Citrix components to provide the Desktop Layer,

- **Citrix XenDesktop Delivery controllers.** These XenDesktop 7 Servers are used to manage and deliver dedicated the Windows applications and desktops.
- **Hosted Shared Workers.** These XenDesktop 7 workloads, leveraging Windows Server Remote Desktop Services Session Host as the foundation, are used to deliver shared hosted applications and desktops for most users.
- **Server VDI Workers.** These XenDesktop 7 workloads, using Windows Server without the Remote Desktop Services Session Host role, provide “VDI-like” VM or Server level isolation of an individual server instance for those users that require more customization or administrative control of their virtual desktop.

XenDesktop Controller Servers[2]	
Instances	2 XenDesktop Controller VMs
Virtual Machine Configurations	
Memory	4 GB RAM
Processor	2 vCPUs
Disk	60 GB HD
Installed Software	
XenDesktop Version	7
Windows Server	Windows Server 2012
Ports Utilized	
XenDesktop Controller	8080

Control Layer

The control layer contains all the infrastructure components required to support the access and desktop layers. The Access Controllers and Desktop Controllers were previously discussed in their respective sections. This section outlines WWCO's implementation of the Infrastructure Controllers and Control Hosts placed in Microsoft Windows Azure to decrease WAN traffic for logon and the potential increased logon times that can result.

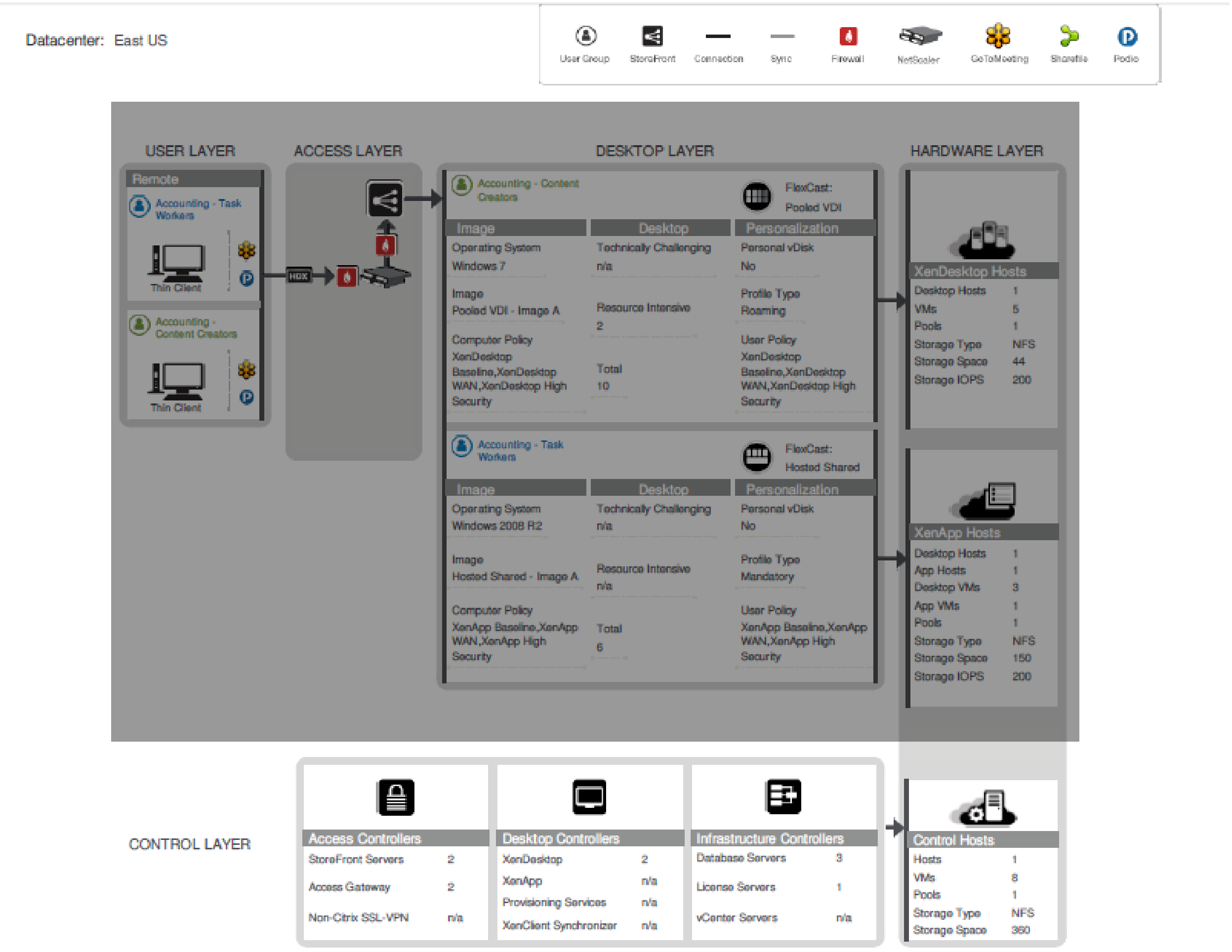


Figure 5: Control Layer

According to the Project Accelerator WWCO's solution required the following Citrix and Microsoft infrastructure components within the control layer:

- **Active Directory.** Citrix leverages Active Directory for authentication and policy setting enforcement on both users and computers.

Active Directory Controller	
Instances	2 Active Directory Controller VMs
Virtual Machine Configurations	

Memory	4 GB RAM
Processor	2 vCPUs
Disk	60 GB HD
Installed Software	
Windows Server	Windows Server 2008 R2 SP1
Windows PowerShell	2.0
Ports Utilized	
Active Directory	

- **SQL Server Database**. Provides the Database Services used by XenDesktop 7.

SQL Server Requirements	
Instances	3 SQL Server VMs
Virtual Machine Configurations	
Memory	16 GB RAM
CPU	4 vCPUs
Disk	60 GB
Installed Software	
SQL Server version	SQL 2008 R2
Authentication	Mixed
TCP/IP	Enabled
Named Pipes	Enabled
IP Address	10.250.18.50
Port	1436
Disk space data files	60Gb
Disk space log files	20Gb
Windows Server	Windows Server 2008 R2
Microsoft .NET Framework	3.5
Ports Utilized	
	1436

Management and Operations

For day to day administration Desktop Director was leveraged to manage and support the environment. Support staff and administrators were granted access to the console.

Administrators manage the site using Desktop Studio. This console handles all site level responsibilities including policies, device and user allocations. Only senior administrators are granted access to the Desktop Studio. The console was installed on each XenDesktop controller for high availability.

Additional tools are available to support managing the environment:

The Project Accelerator outputs provide the base sizing and architecture for AzureCSP's CSP on Azure solution. The following sections provide additional considerations, tools and optimizations specific to CSP multi-tenancy and the Azure IaaS platform itself. Taken into consideration together a complete solution was implemented in Azure.

SOLUTION CAPABILITIES AND CONSTRAINTS

PROJECT ACCELERATOR ARCHITECTURE MODIFICATIONS WITHIN AZURE

The following sections outline some of the considerations within Azure that have influenced this design beyond the recommendations from the Project Accelerator.

AZURE AS AN IAAS PLATFORM

The Azure platform has evolved to include several Infrastructure as a Service enabling technologies. This section provides a brief overview of those technologies that are leveraged as a part of the Citrix solution on Azure.

More information about Azure IaaS and Windows VM Instance capabilities can be found at http://www.windowsazure.com/en-us/manage/windows/ .

NETWORKING

Windows Azure Virtual Networking enables a secure environment for each Azure tenant. The example in this guide uses a single virtual network for all Azure hosted XenDesktop 7 workloads. An Azure Site-to-Site VPN connection was used between WWCO's on premise corporate datacenter and the Azure hosted virtual network.

More information regarding Azure Networking can be found at http://www.windowsazure.com/en-us/manage/services/networking/

STORAGE

The scenario in this document leverages Azure shared storage as provided to the VM instances provisioned within Azure. In addition a Windows Server 2012 File Server has been configured within Azure as a shared file service for the storage of user profiles and data. Additional storage can be allocated within the environment as required for other workloads not documented in this guide.

More information about Azure storage can be found at http://www.windowsazure.com/en-us/manage/services/storage/

Important!: Due to the fact that Citrix Provisioning Service is not supported with Azure at this time the storage calculations from the Project Accelerator can differ significantly from the storage actually used. Please confirm your storage requirements as part of your cost models.

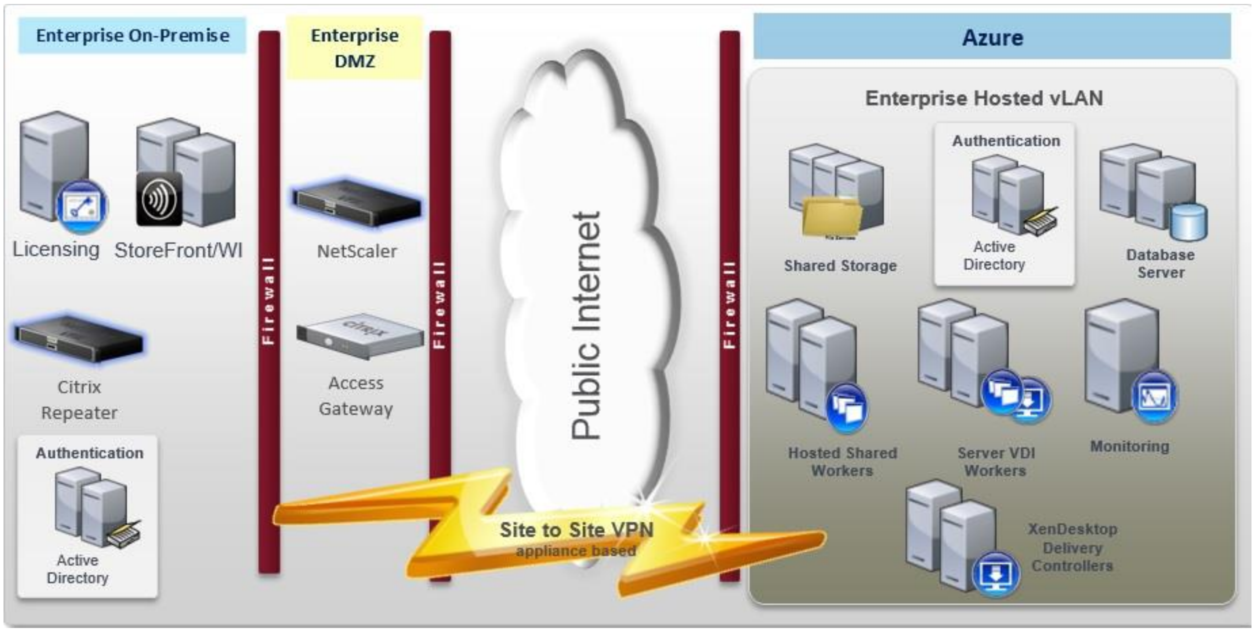
PROVISIONING

The provisioning of VM Instances within Azure is accomplished through manual creation of the instances through the Azure portal. Larger scale environments can be provisioned using Azure PowerShell scripting. The appendix of this guide provides some sample scripts used to provision various instances and workloads within Azure. The portal UI examples in this guide are used for the sake of clarity, while it is generally recommended that a CSP leverage the Azure PowerShell scripts to ensure continuity when provisioning instances over time or at larger scale.

More information about Azure PowerShell and other command line tools can be found at http://www.windowsazure.com/en-us/downloads/#cmd-line-tools

SECURE ACCESS

For the scenario in this guide, secure access to desktops and applications within Azure is provided through the WWCO on premise NetScaler Gateway when connecting to Azure hosted workloads. The connections made through the NetScaler Gateway are then passed through the Azure Site-to-Site VPN to the Azure hosted desktops and applications



More information about Citrix NetScaler Gateway can be found at http://www.citrix.com/edocs

MICROSOFT INSTANCES AND SERVICES USED FOR THIS GUIDE

Microsoft Windows Server 2012 Datacenter Instances were used for all Windows Servers in this Guide. Some of the Roles and Services enabled on various servers include…

- Active Directory Services
- File Services
- Internet Information Services
- Microsoft SQL Server 2010 Service Pack 2

- .NET 3.5
- .NET 4.0
- Remote Desktop Services
- Remote Desktop Service License Server

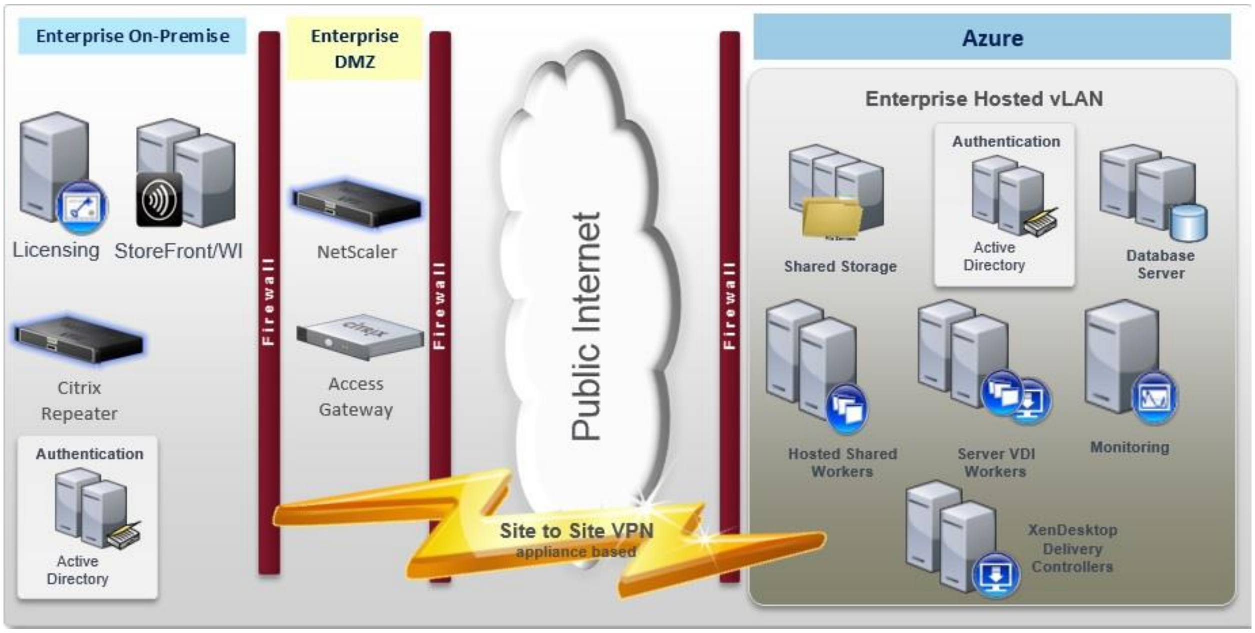
CITRIX COMPONENTS SUPPORTED IN AZURE FOR THIS SOLUTION

The following Citrix components are currently supported within Azure.

- Citrix XenDesktop 7 Delivery controllers, Hosted Shared Workers and Server VDI Workers

SCENARIO: AUGMENTING ON PREMISE SERVICES WITH XENDESKTOP 7 CONTROLLERS AND WORKERS HOSTED IN AZURE

SAMPLE ARCHITECTURE



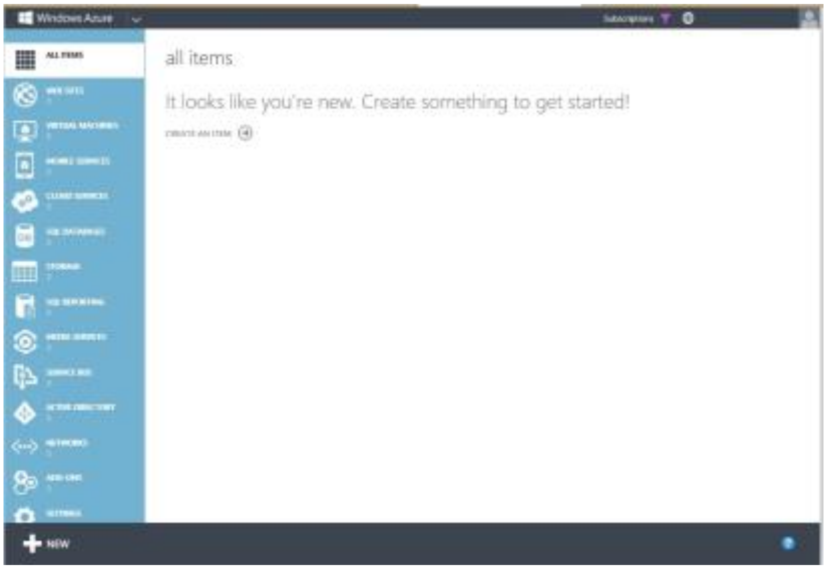
CREATING THE AZURE VIRTUALNETWORK AND CONNECTING IT TO THE ON PREMISE WWCO NETWORK

In the following section we will walk through the creation of an Azure Virtual Network to be connected to the WWCO on premise datacenter via an Azure Site-to-Site VPN.

CONSIDERATIONS WHEN BUILDING THE BASE AZURE VIRTUAL NETWORKS AND ACTIVE DIRECTORY VM INSTANCES.

As stated earlier, a single virtual network is used for this scenario. Below is a brief walk-through of how a Virtual Network would be created for this scenario using the Azure Portal.

Starting with a blank Azure Subscription…

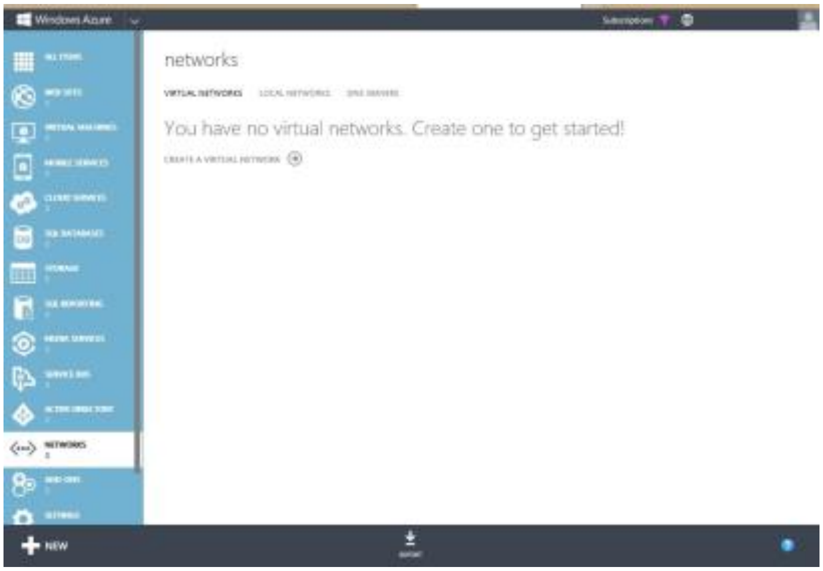


all items

It looks like you're new. Create something to get started!

CREATE AN ITEM

Create a Network

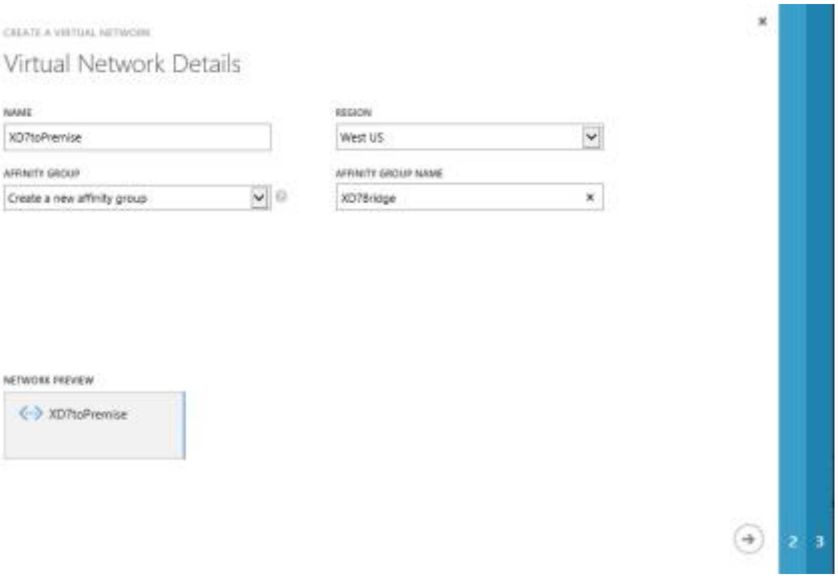


networks

VIRTUAL NETWORKS   LOCAL NETWORKS   DNS SERVERS

You have no virtual networks. Create one to get started!

CREATE A VIRTUAL NETWORK



CREATE A VIRTUAL NETWORK

Virtual Network Details

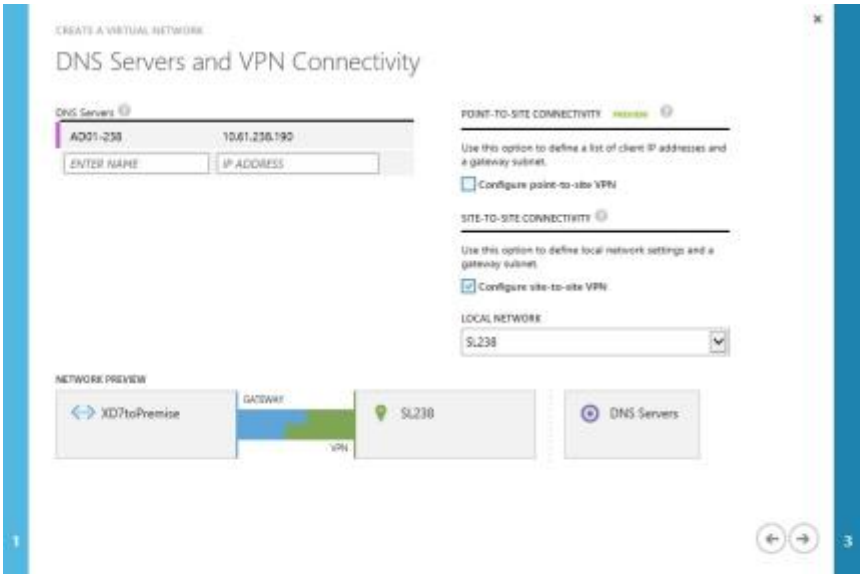
NAME: XD7toPremise

REGION: West US

AFFINITY GROUP: Create a new affinity group

AFFINITY GROUP NAME: XD7Bridge

NETWORK PREVIEW



CREATE A VIRTUAL NETWORK

DNS Servers and VPN Connectivity

DNS Servers

AD01-238	10.61.238.190
ENTER NAME	IP ADDRESS

POINT-TO-SITE CONNECTIVITY PREVIEW

Use this option to define a list of client IP addresses and a gateway subnet.

☐ Configure point-to-site VPN

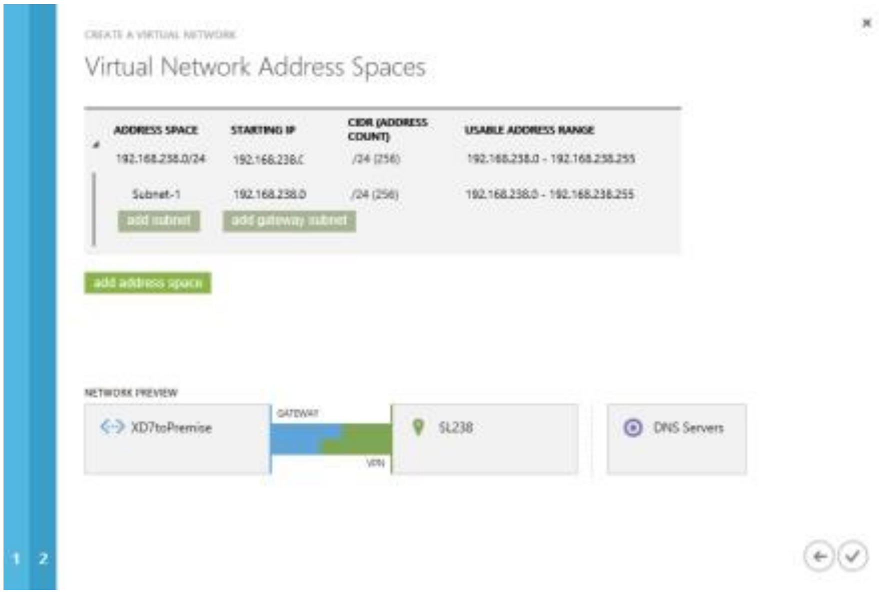
SITE-TO-SITE CONNECTIVITY

Use this option to define local network settings and a gateway subnet.

☑ Configure site-to-site VPN

LOCAL NETWORK: SL238

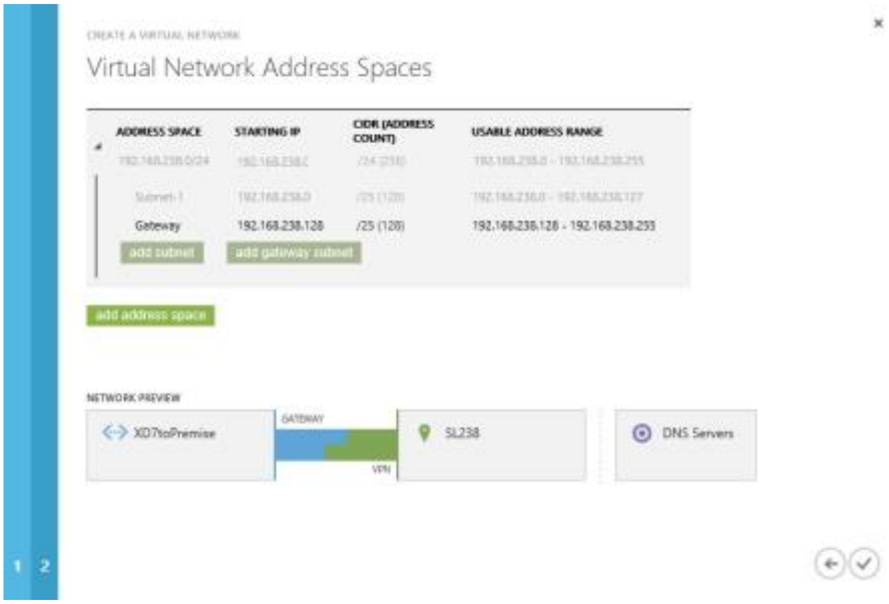
NETWORK PREVIEW



CREATE A VIRTUAL NETWORK

Virtual Network Address Spaces

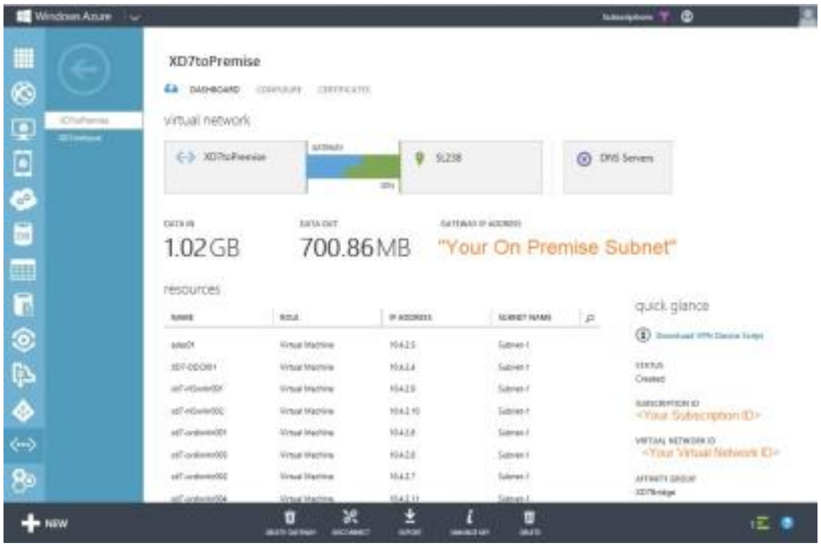
ADDRESS SPACE	STARTING IP	CIDR (ADDRESS COUNT)	USABLE ADDRESS RANGE
192.168.238.0/24	192.168.238.(	/24 (256)	192.168.238.0 - 192.168.238.255
Subnet-1	192.168.238.0	/24 (256)	192.168.238.0 - 192.168.238.255



CREATE A VIRTUAL NETWORK

Virtual Network Address Spaces

ADDRESS SPACE	STARTING IP	CIDR (ADDRESS COUNT)	USABLE ADDRESS RANGE
192.168.238.0/24	192.168.238.(	/24 (256)	192.168.238.0 - 192.168.238.255
Subnet-1	192.168.238.0	/25 (128)	192.168.238.0 - 192.168.238.127
Gateway	192.168.238.128	/25 (128)	192.168.238.128 - 192.168.238.255



XD7toPremise

DASHBOARD CONFIGURE CERTIFICATES

virtual network

DATA IN 1.02GB

DATA OUT 700.86MB

GATEWAY IP ADDRESS "Your On Premise Subnet"

resources

NAME	ROLE	IP ADDRESS	SUBNET NAME
[illegible]	Virtual Machine	10.4.2.5	Subnet-1
[illegible]	Virtual Machine	10.4.2.4	Subnet-1
[illegible]	Virtual Machine	10.4.2.9	Subnet-1
[illegible]	Virtual Machine	10.4.2.10	Subnet-1
[illegible]	Virtual Machine	10.4.2.8	Subnet-1
[illegible]	Virtual Machine	10.4.2.6	Subnet-1
[illegible]	Virtual Machine	10.4.2.7	Subnet-1
[illegible]	Virtual Machine	10.4.2.11	Subnet-1

quick glance

Download VPN Device Script

STATUS
Created

SUBSCRIPTION ID
<Your Subscription ID>

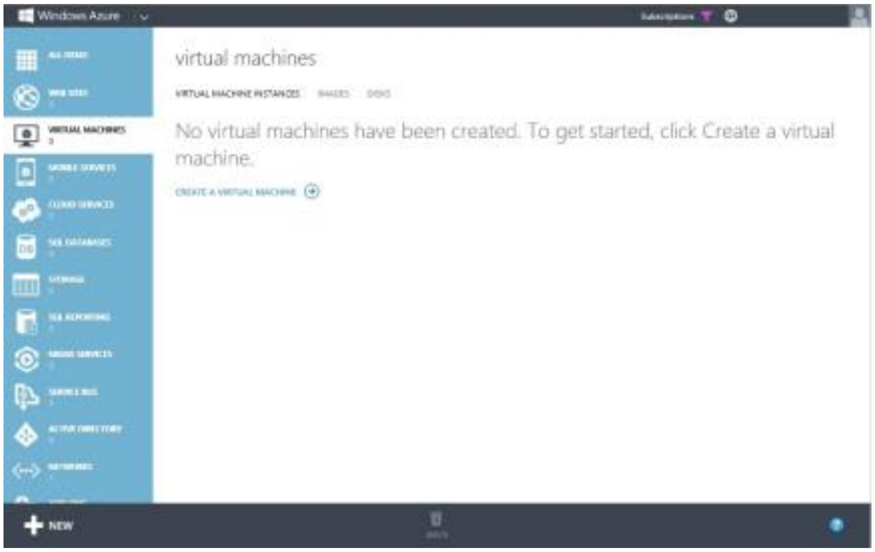
VIRTUAL NETWORK ID
<Your Virtual Network ID>

AFFINITY GROUP
XD7Bridge

Once the virtual network is in place the Azure AD Controllers must be created and joined to the on premise Forest…

Creation of the Active Directory Servers can be accomplished through either manually provisioning the instances through the Azure Portal or by using the Azure PowerShell.

In the Portal, click on Virtual Machines, then click “Create a virtual machine” …



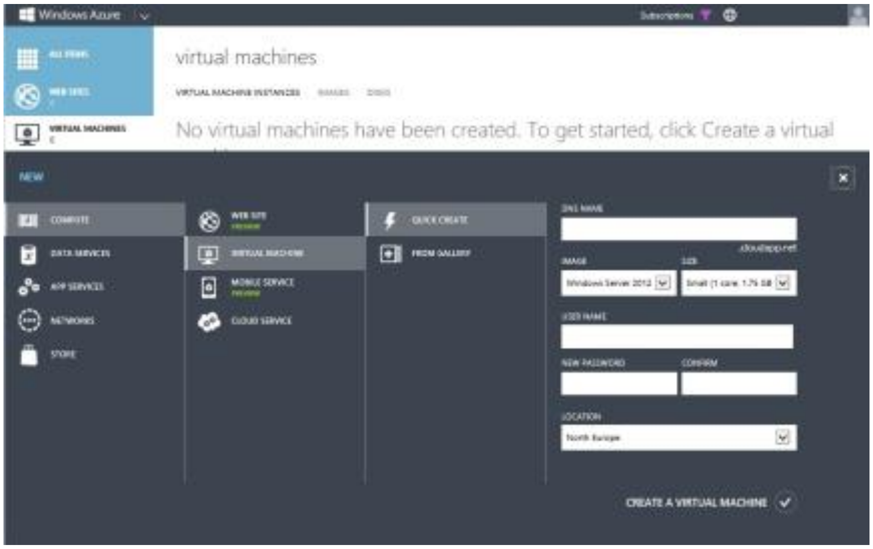
virtual machines

VIRTUAL MACHINE INSTANCES IMAGES DISKS

No virtual machines have been created. To get started, click Create a virtual machine.

CREATE A VIRTUAL MACHINE

Click “From Gallery”



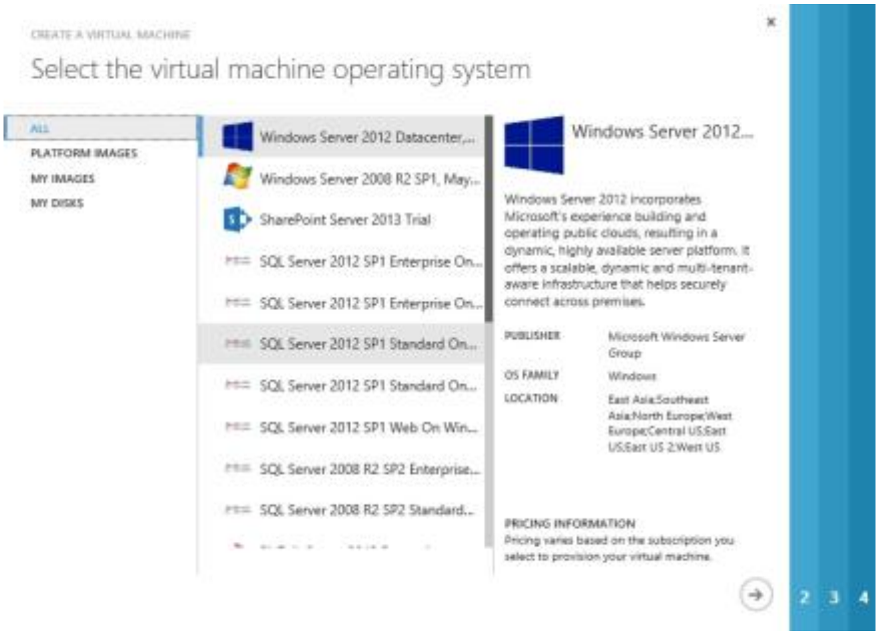
No virtual machines have been created. To get started, click Create a virtual

IMAGE Windows Server 2012

SIZE Small (1 core, 1.75 GB)

LOCATION North Europe

For this example we will use the Windows Server 2012 Datacenter Template from the Azure Gallery..


CREATE A VIRTUAL MACHINE
Select the virtual machine operating system
ALL
PLATFORM IMAGES
MY IMAGES
MY DISKS
Windows Server 2012 Datacenter,...
Windows Server 2008 R2 SP1, May...
SharePoint Server 2013 Trial
SQL Server 2012 SP1 Enterprise On...
SQL Server 2012 SP1 Enterprise On...
SQL Server 2012 SP1 Standard On...
SQL Server 2012 SP1 Standard On...
SQL Server 2012 SP1 Web On Win...
SQL Server 2008 R2 SP2 Enterprise...
SQL Server 2008 R2 SP2 Standard...
2
3
4

Windows Server 2012...

Windows Server 2012 incorporates Microsoft's experience building and operating public clouds, resulting in a dynamic, highly available server platform. It offers a scalable, dynamic and multi-tenant-aware infrastructure that helps securely connect across premises.

PUBLISHER Microsoft Windows Server Group

OS FAMILY Windows

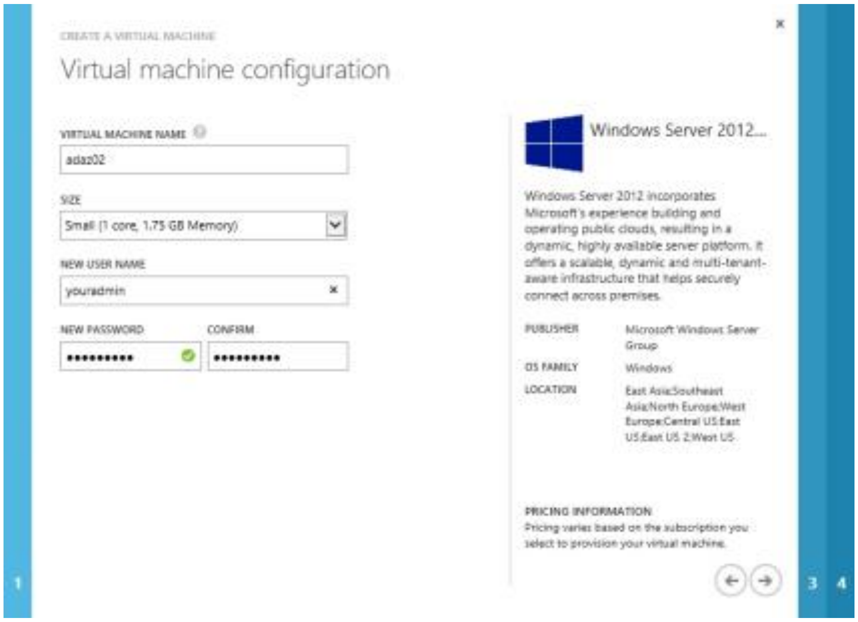
LOCATION East Asia;Southeast Asia;North Europe;West Europe;Central US;East US;East US 2;West US

PRICING INFORMATION

Pricing varies based on the subscription you select to provision your virtual machine.

Click the right facing arrow to indicate you are ready to proceed…

Next we will name this VM instance adaz01 and choose the small instance type. You may choose a larger instance depending upon the scale of you offering…



CREATE A VIRTUAL MACHINE

Virtual machine configuration

VIRTUAL MACHINE NAME: adaz02

SIZE: Small (1 core, 1.75 GB Memory)

NEW USER NAME: youradmin

NEW PASSWORD: •••••••••• CONFIRM: ••••••••••

Windows Server 2012...

Windows Server 2012 incorporates Microsoft's experience building and operating public clouds, resulting in a dynamic, highly available server platform. It offers a scalable, dynamic and multi-tenant-aware infrastructure that helps securely connect across premises.

PUBLISHER	Microsoft Windows Server Group
OS FAMILY	Windows
LOCATION	East Asia;Southeast Asia;North Europe;West Europe;Central US;East US;East US 2;West US

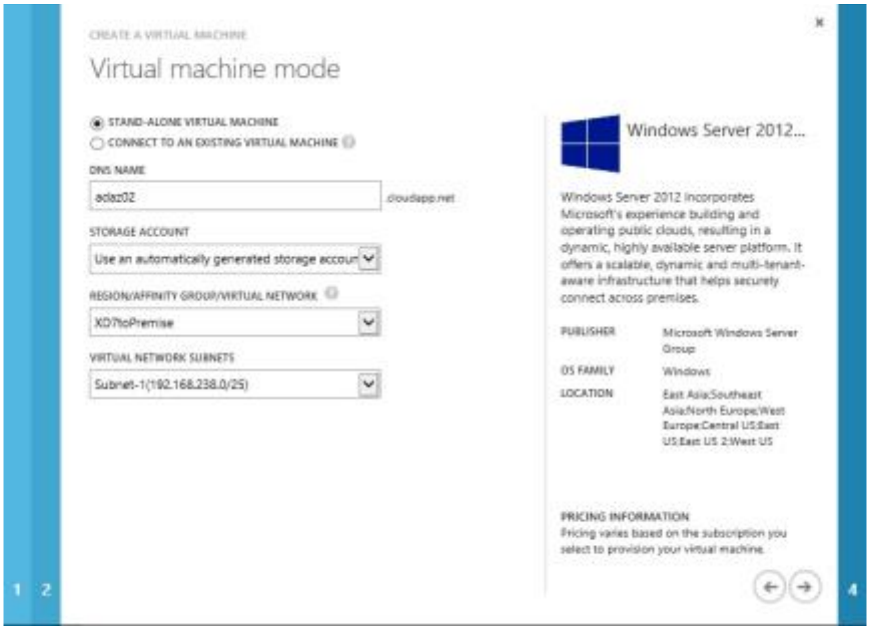
PRICING INFORMATION

Pricing varies based on the subscription you select to provision your virtual machine.

Provide a unique administrator name for this instance. Once it is running you will want to disable the default administrator account to provide a higher level of security for this VM.

Click the right facing arrow to indicate you are ready to proceed…

Provide the DNS name for this instance and assign it to the Affinity Group that was created within your Virtual Network.



CREATE A VIRTUAL MACHINE

Virtual machine mode

● STAND-ALONE VIRTUAL MACHINE

○ CONNECT TO AN EXISTING VIRTUAL MACHINE

DNS NAME: adaz02 .cloudapp.net

STORAGE ACCOUNT: Use an automatically generated storage accoun

REGION/AFFINITY GROUP/VIRTUAL NETWORK: XD7toPremise

VIRTUAL NETWORK SUBNETS: Subnet-1(192.168.238.0/25)

Windows Server 2012...

Windows Server 2012 incorporates Microsoft's experience building and operating public clouds, resulting in a dynamic, highly available server platform. It offers a scalable, dynamic and multi-tenant-aware infrastructure that helps securely connect across premises.

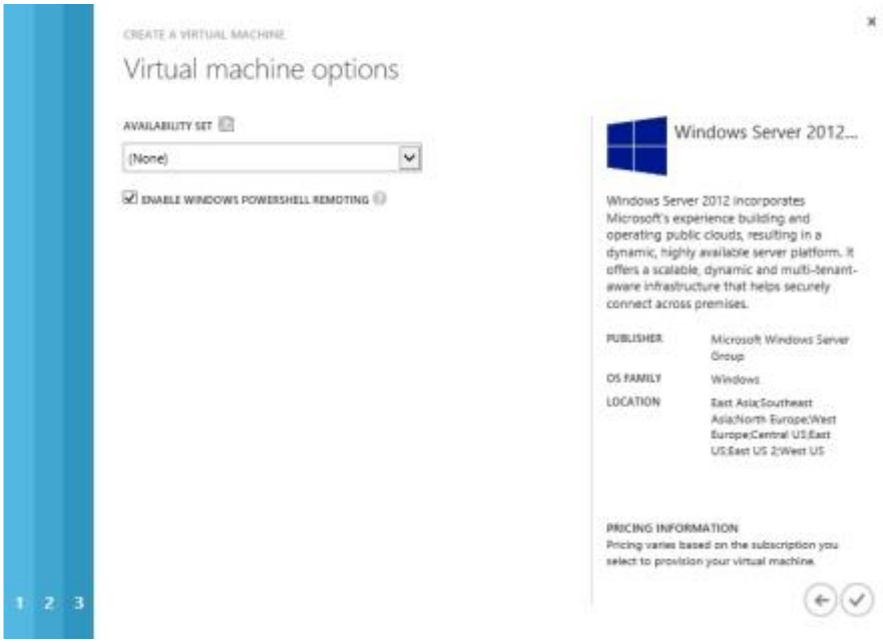
PUBLISHER	Microsoft Windows Server Group
OS FAMILY	Windows
LOCATION	East Asia;Southeast Asia;North Europe;West Europe;Central US;East US;East US 2;West US

PRICING INFORMATION

Pricing varies based on the subscription you select to provision your virtual machine.

Click the right facing arrow to indicate you are ready to proceed…

Accept the defaults for the next panel and Click the check mark to complete the wizard.



CREATE A VIRTUAL MACHINE

Virtual machine options

AVAILABILITY SET

(None)

☑ ENABLE WINDOWS POWERSHELL REMOTING

Windows Server 2012...

Windows Server 2012 incorporates Microsoft's experience building and operating public clouds, resulting in a dynamic, highly available server platform. It offers a scalable, dynamic and multi-tenant-aware infrastructure that helps securely connect across premises.

PUBLISHER	Microsoft Windows Server Group
OS FAMILY	Windows
LOCATION	East Asia;Southeast Asia;North Europe;West Europe;Central US;East US;East US 2;West US

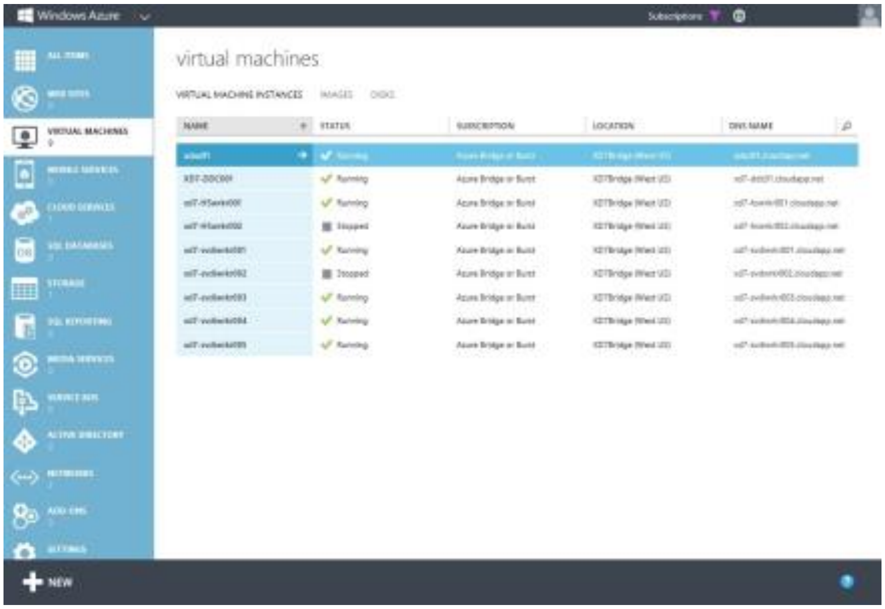
PRICING INFORMATION

Pricing varies based on the subscription you select to provision your virtual machine.

This same basic procedure can be followed to provision all of the VM instances required for the environment. As an AD controller you will next need to install the AD roles for your environment.

A great Microsoft blog post on how to create AD controllers in Azure through PowerShell can be found at http://www.windowsazure.com/en-us/manage/services/networking/active-directory-forest/

Once the provisioning of a VM has finished you will see the instance in a running state. A screen shot of the complete set of VM instances provisioned in Azure for this sample design demonstrates the state of these VMs.



virtual machines

VIRTUAL MACHINE INSTANCES | IMAGES | DISKS

NAME	STATUS	SUBSCRIPTION	LOCATION	DNS NAME
[illegible]	✓ Running	[illegible]	[illegible]	[illegible]
XD7-DDC001	✓ Running	Azure Bridge or Burst	XDTBridge (West US)	[illegible]
[illegible]	✓ Running	Azure Bridge or Burst	XDTBridge (West US)	[illegible]
[illegible]	■ Stopped	Azure Bridge or Burst	XDTBridge (West US)	[illegible]
[illegible]	✓ Running	Azure Bridge or Burst	XDTBridge (West US)	[illegible]
[illegible]	■ Stopped	Azure Bridge or Burst	XDTBridge (West US)	[illegible]
[illegible]	✓ Running	Azure Bridge or Burst	XDTBridge (West US)	[illegible]
[illegible]	✓ Running	Azure Bridge or Burst	XDTBridge (West US)	[illegible]
[illegible]	✓ Running	Azure Bridge or Burst	XDTBridge (West US)	[illegible]

Once the networking and VM instances are in place the standard XenDesktop installation procedures as outlined in the product documentation were followed. There are no special considerations when implementing XenDesktop delivery controllers or worker servers within Azure as proposed in this sample design.

A FEW SUGGESTIONS FOR SECURING AZURE IAAS VM INSTANCES.

- Rename the local administrator account.
- Disable the local administrator account and create some uncommonly named user account for administrative access.
- Choose strong plus complex passwords, or passphrases. Not simply one or the other. The OS can enforce complexity but not strength.
- A dictionary attack is likely to hit "P@ssw0rd" but it is unlikely to hit "Just a city boy, born and raised in South Detroit".
- Denying user access after X failed logon attempts (lock the account). This is a Local security policy if not domain joined, or a Domain policy if joined. Consider an automatic (timed) unlock as well, or you could have no recourse but to destroy your machine.
- Do not allow the creation of the default RDP public endpoint. This is only possible through the API / PowerShell. Or delete the auto created endpoint after creating the machine in the Portal.
- Only create the RDP endpoint when remote administration is necessary, and removing it after. But remember that we are human, and unless you have some interface doing this for you, you will probably forget at some point.
- Remove the RDP endpoint and use the Virtual Network Gateway feature of the Azure Virtual Network for secured remote administration without public endpoints. This requires some ground based router, and the VPN is slow, but your ports are closed.
- Remove RDP endpoint & use Azure Connect. This is limited to IPv6 TCP traffic only, but that should cover anything required to manage the OS.
- Avoid 3389 as the public port (I noticed my compromised machine specifically scanning for this port to spread itself) by using a port in the ephemeral range.
- Use the Windows Advanced Firewall rules and define them appropriately.
- Use Windows IP Security Policies and tightly define the sources from which RDP traffic can be accepted from. This is highly effective, but a pain to set up.
- Monitor the machine. Azure provides metrics through the portal and API. Discover a baseline. Use an agent within the machine. This only detects the compromise after it happens and is not preventative.
- Take a snapshot of the clean state. This is not a point and click thing in Azure today, but you can work this out using the Storage cmdlets through destroying your machine, making the diff disk, and reincarnating the machine.

Conclusion

By cross referencing the Citrix Project Accelerator and XenDesktop Modular Reference Architecture WWCO was able to implement a XenDesktop solution within Microsoft's Azure IaaS environment.

Leveraging public cloud infrastructure such as Azure virtually eliminated any need for a new WWCO capital investment, allowing them to bring their new service online quickly in a globally available, state of the art cloud hosted infrastructure.

By leveraging Citrix XenDesktop 7 WWCO was capable of providing an industry leading desktop virtualization solution, ensuring the best user experience across any device, in as enabled by Citrix technologies like HDX.

ADDITIONAL RESOURCES

CITRIX XENDESKTOP PRODUCT WEB SITE

XENDESKTOP MODULAR REFERENCE ARCHITECTURE

SAMPLE VIDEOS ON CITRIXTV

CITRIX PROJECT ACCELERATOR

MICROSOFT WINDOWS AZURE SITE

Revision History

Number	Change Description	Updated by	Date
0.1	Document Created	Kurt Moody	June 18, 2013
1.0	Final Draft	Kurt Moody	June 25, 2013
1.1	Revised to clarify server instances	Kurt Moody	July 11, 2013

Appendix

SAMPLE AZURE POWERSHELL SCRIPTS

This section includes some basic information for using Azure PowerShell scripts to build a Hosted Desktop environment within Azure. The "Basics" section provides some of the useful cmdlets you will use to configure and discover resources within your Azure subscription, the "Examples" section contains versions of scripts used by Citrix in testing the published scenario.

Note: The Azure PowerShell cmdlets are a work in progress.

They are currently a community contribution that is being folded into the product lifecycle and enhanced by MSFT and properly released.

You can find the cmdlets here:

https://www.windowsazure.com/en-us/manage/downloads/

The primary information source on using the cmdlets is this blog:

http://michaelwasham.com/ (Azure Evangelist as MSFT)

Be sure to have your Azure management certificate properly stored in your Personal certificate store prior to connecting to your subscription.

BASICS:

Here are some useful commands to use the cmdlets to drive machine and service creation.

These commands must be used to configure your Azure PowerShell session to communicate with your specific Azure subscription.

Import the module:

```
import-module 'C:\Program Files (x86)\Microsoft SDKs\Windows Azure\PowerShell\Azure\Azure.psd1'
```

Import a settings file (this speeds up as it lists all subscriptions you have access to - to create this file perform

```
Export-AzurePublishSettingsFile (Visual Studio also uses this))
```

Then import the settings file into your environment:

```
Import-AzurePublishSettingsFile 'C:\Users\Public\Documents\<your subscription>-credentials.publishsettings'
```

Choose the subscription that you will interact with for your session:

```
Select-AzureSubscription -SubscriptionName "<your subscription>"
```

Set the default Storage account that will be used (it must be in the same subscription)

```
Set-AzureSubscription -SubscriptionName "< your subscription>" -CurrentStorageAccount <your storage account>
```

Useful cmdlets for Finding an Image from which to create Virtual Machines

The filters can be changed to focus on Gallery images or images that have been user created.

List all available images:

```
Get-AzureVMImage
```

List all available in a table:

```
Get-AzureVMImage | Format-Table
```

Find images that have been uploaded to your Storage account ('user' images):

```
Get-AzureVMImage | where { ($_.Category -eq "user") }
```

Creating Virtual Machines from Images

Note: by default a new service is created and the VM added, unless an existing Service name is defined.

This same image will be used for both examples:

```
$svr2012Image = Get-AzureVMImage | where { ($_.Category -eq "Microsoft") -and ($_.Label -match "Server 2012" ) -and ($_.ImageName -match "Datacenter") }
```

Apply a customization configuration to the image:

```
$myImage = New-AzureVMConfig -Name <Your Image Name> -InstanceSize ExtraSmall -ImageName $svr2012Image.ImageName

Add-AzureProvisioningConfig -VM $myImage -Windows -Password P@ssw0rd

New-AzureVM -ServiceName "<Your Service Name>" –VMs $myImage
```

A more advanced configuration that also creates endpoints and sets a Virtual Network, DNS Settings, Affinity Group, and creates a new IaaS service:

```
$myImage = New-AzureVMConfig –Name <Your Image Name> -InstanceSize ExtraSmall -ImageName $svr2012Image.ImageName
```

Add-AzureProvisioningConfig -VM $myImage -Windows -Password P@ssw0rd -NoRDPEndpoint

Add-AzureEndpoint -Protocol tcp -LocalPort 3389 -PublicPort 3389 -VM $myImage -Name RDP

Add-AzureEndpoint -Protocol tcp -LocalPort 5986 -PublicPort 5986 -VM $myImage -Name WinRM

Set-AzureSubnet -VM $myImage -SubnetNames IaaSSubnet

$dns = New-AzureDns -Name <Your Image Name> -IPAddress 10.104.2.4

(# This is the IP that the VM that is providing DNS within my Service)

New-AzureVM -ServiceName "<Your Image Name> " –VMs $myImage -VNetName VNetOne -DnsSettings $dns -AffinityGroup <Your Affinity Group>

Defining a custom DNS setting (for your DNS server, necessary for AD domain join)

As seen above New-AzureDns created a configuration XML object that is applied to a Virtual Network or to a Service when the first Virtual Machine is added. This setting can only be added with the first Virtual Machine in the Service.

$dns = New-AzureDns -Name <Your Name> -IPAddress 10.104.2.4

New-AzureVM -ServiceName "<Your Name> " –VMs $myImage -VNetName VNetOne -DnsSettings $dns -AffinityGroup <Your Affinity Group Name>

Defining joining to an AD on provisioning

Here the -JoinDomain section is added to the Provisioning Configuration and -WindowsDomain is used instead of -Windows

$myImage = New-AzureVMConfig -Name $role -InstanceSize ExtraSmall -ImageName $svr2008Image.ImageName

Add-AzureProvisioningConfig -WindowsDomain -VM $myImage -Password P@ssw0rd -JoinDomain "brianeh.local" -Domain "<Your Domain Name> " -DomainUserName "administrator" -DomainPassword "P@ssw0rd" -MachineObjectOU 'OU=TenantTwo,OU=XenApp,DC=<Your Domain>,DC=local'

New-AzureVM -ServiceName "<Your Service Name>" –VMs $myImage

EXAMPLES:

These are some script samples that were created to enable working through scenarios with Azure Virtual Machines (IaaS). As the Azure platform continues to evolve some cmdlets and parameters may change. Please work through the Azure help and documentation to ensure your scripts provide you with the correct configurations.

Creating XenApp infrastructure Virtual Machines Using the July 2012 Azure Gallery Server 2008 R2 image

If the Gallery image has been updated, this will need to be modified to select the proper one. This particular image is Server 2008 R2 SP1 Datacenter. Note the hardcoded Virtual Network, Subnet, and Affinity Group settings; as well as passwords and domain and OU. The Affinity Group and the Virtual Network settings must align.

The assumption here is that Azure will name the OS of the VMs with the Machine Name specified and join them to my Domain Control in Azure. The Domain Controller is located through DNS, so you must provide your own DNS. This can be done by adding the DNS on the new AD controllers to your Azure virtual network.

This script should create images that are ready for App Orchestration 1.0 to provide the Citrix Hosted Desktop Services installation and configuration.

This Creates the IaaS Service:

```
$svr2008Image = Get-AzureVMImage | where { ($_.Category -eq "Microsoft") -and ($_.Label -match "Server 2008" ) -and ($_.ImageName -match "Datacenter") }

# Deploy the Primary Zone Data Collector and Backup Zone Data Collector and other Windows OS infrastructure
$roles = @()
$roles += "CSPPDC", "CSPBDC", "CSPCSG", "CSPWI"

$dns = New-AzureDns -Name <yourDNS> -IPAddress <IPADDR>

$infraVms = @()

foreach ($role in $roles){
    $myImage = New-AzureVMConfig -Name $role -InstanceSize <AppropriateSizeForYourScale> -ImageName $svr2008Image.ImageName
    Add-AzureProvisioningConfig -WindowsDomain -VM $myImage -Password P@ssw0rd -JoinDomain "brianeh.local" -Domain "brianeh.local" -DomainUserName "administrator" -DomainPassword "P@ssw0rd" -MachineObjectOU 'OU=TenantTwo,OU=XenApp,DC=brianeh,DC=local'
    Set-AzureSubnet -VM $myImage -SubnetNames Infra

$infraVms += $myImage
}
    New-AzureVM -ServiceName "CSPXenApp" –VMs $infraVms -VNetName <YourVirtualNetwork> -DnsSettings $dns

    Get-AzureVM -ServiceName CSPXenApp -Name CSPCsg | Add-AzureEndpoint -Protocol tcp -LocalPort 443 -PublicPort 443 -Name ClientFrontEnd | Update-AzureVM
```

Create a number of Servers from a gallery image for XenApp session hosts:

This is similar to the above except for the naming scheme, OU, and create is slightly different. This adds machines to an existing IaaS Service. This uses the same Gallery server image as the above script.

```
#Choose the image and set the number of session hosts.
[int32]$numXaSessionHosts = Read-Host "How many XenApp Session Hosts?"

$sessHostVms = @()

Do {
    $myImage = New-AzureVMConfig -Name ("bjeXenApp3" + $numXaSessionHosts) -InstanceSize ExtraSmall -ImageName $svr2008Image.ImageName
    Add-AzureProvisioningConfig -WindowsDomain -VM $myImage -Password P@ssw0rd -JoinDomain "<YourDomainName>" -Domain "<YourDomain>" -DomainUserName "administrator" -DomainPassword
"P@ssw0rd" -MachineObjectOU
'OU=SessionHosts,OU=TenantOne,OU=XenApp,DC=<YourDomain>,DC=<YourSuffix>'
   Set-AzureSubnet -VM $myImage -SubnetNames Three
$sessHostVms += $myImage
--$numXaSessionHosts
} Until ( $numXaSessionHosts -eq 0 )
   New-AzureVM -ServiceName "bjeXenApp" –VMs $sessHostVms -VNetName VNetTwo -DnsSettings $dns
# doing one big create and passing in multiple VM configurations is more reliable than placing New-Azure VM
within the loop.
```

Deleting all the Virtual Machines within a Service:

This does delete the VHDs. If you want to leave the VHDs comment the Remove-AzureDisk line.

```
# Total Clean Up.
$vms = get-azurevm -ServiceName bjeXenApp

foreach ($vm in $vms){
$osDisk = get-azureosdisk -VM $vm.vm
Remove-AzureVM -ServiceName $vm.DeploymentName -Name $vm.InstanceName
Remove-AzureDisk -DiskName $osDisk.DiskName -DeleteVHD
}
```

Deleting OS VHDs that are not associated with a Virtual Machine:

This is a clean up script to prevent leaving a bunch of OS disks in your Azure Storage account.

# or clean up all the disks that are not attached to a VM (all that are not attached), test for OS declaration.

```
Get-AzureDisk | where { ($_.AttachedTo -eq $null) -and ($_.OS -ne $null) } | Remove-AzureDisk -DeleteVHD
```

In both of these examples -DeleteVHD was added as a flag to the command. IF this is not added then the VHD registration is removed, but the VHD is not deleted.

Removing all the endpoints with a particular name from all Virtual Machines in a Service

This is one of those that happened while I was trying to figure out why the RDP port forwarding was not working.

```
get-azurevm -ServiceName bjeTest | Remove-AzureEndpoint -Name RDP
```

About Citrix

Citrix, Inc. (NASDAQ:CTXS) is a leading provider of virtual computing solutions that help companies deliver IT as an on-demand service. Founded in 1989, Citrix combines virtualization, networking, and cloud computing technologies into a full portfolio of products that enable virtual workstyles for users and virtual datacenters for IT. More than 230,000 organizations worldwide rely on Citrix to help them build simpler and more cost-effective IT environments. Citrix partners with over 10,000 companies in more than 100 countries. Annual revenue in 2011 was $2.20 billion.