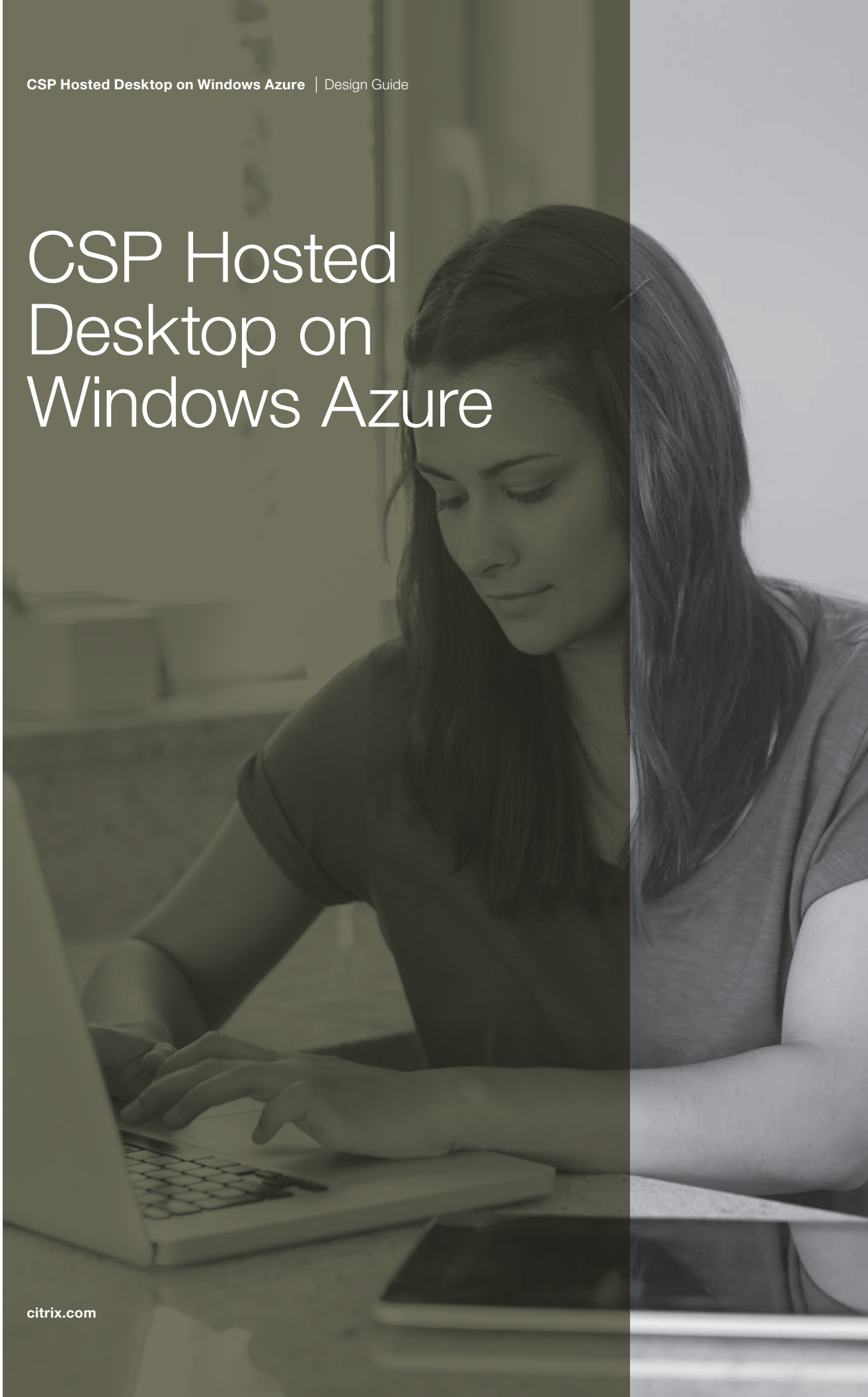
CSP Hosted Desktop on Windows Azure



CITRIX®

citrix.com

About this design guide

The Citrix Design Guide provides an overview of the Citrix Service Provider Hosted Desktops 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.

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 Windows desktops and applications begin to unfold. As a platform Microsoft Azure provides a robust, state of the art infrastructure and global presence for service providers.

Citrix Service Providers, enabled through the implementation of the Citrix Service Provider Reference Architecture for Multi-tenant hosted desktops, and the Citrix Service Provider subscription licensing program now have the opportunity to rapidly grow their business within a region or globally by leveraging Citrix hosted capabilities on the Azure platform.

This document provides high-level design guidance using a sample implementation of XenApp 6.5 within the Microsoft Windows Azure cloud. Used in conjunction with the Citrix Service Provider Reference Architecture these documents provide basic best practice guidance for service providers looking to leverage Citrix and Microsoft cloud technologies to deliver a state of the art solution for their subscribers.

Use Case

Let's assume "AzureCSP" is a Citrix Service Provider with plans to leverage Microsoft and Citrix products to deliver a Hosted Desktop solution to multiple small and medium businesses across several vertical markets, including; accounting firms, legal practices, real estate, and healthcare. The AzureCSP hosted solution will provide value to the customers (tenants) by enabling access to Windows desktops and applications from any device. Another compelling benefit of this service is that it can remove the tenants' in-house human resource and capital investment requirements for the installation, configuration, maintenance and support of Windows desktops and applications, replacing it with a month-to-month hosted subscription managed by AzureCSP.

The objective of this guide is to outline AzureCSP's business considerations, and how hosting their hosted Service in Azure could address them.

Business objectives

- Provide a month-to-month hosted desktop subscription service for 5000 subscribers
- Manage the service within a multi-tenant environment to gain economies of scale
- Start this service with minimal to no capital investment by AzureCSP

- Provide tenants with access to cloud hosted desktops and applications managed by AzureCSP
- Tenants will use their own devices
- Provide a degree of IT self-service for some tenants
- Provide a tiered selection of; Basic, Premium and Dedicated hosted desktop services

Technical objectives

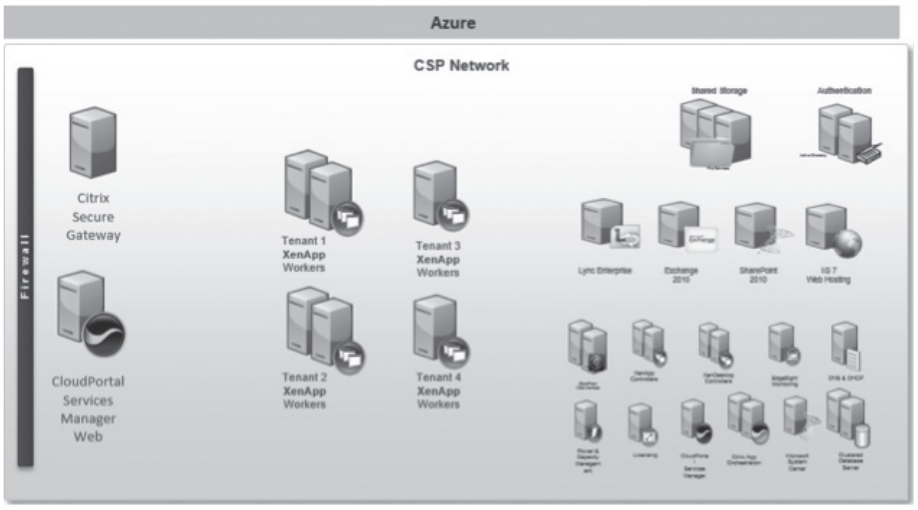
- Quickly design and implement environment to establish the value and metrics.
- Ensure high availability of critical components to ensure business continuity.
- Implement an “n+1” highly available solution to avoid any business interruption.
- Support access from subscriber-owned devices that vary in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

Citrix Service Provider Hosted Desktops on Azure

AzureCSP selected a combination of XenApp and XenDesktop as their solution since they enable the best user experience across the public internet from any device according to independent analysis, and after reviewing the Citrix Service Provider Reference Architecture and Microsoft’s Windows Azure IaaS capabilities, they believed they could build a solution without a large upfront capital investment.

The Citrix Hosted Desktop solution on Azure consisted of many components.

- Citrix XenApp 6.5 Delivery controllers and Hosted Shared Workers
- Citrix XenDesktop 5.6 Delivery controllers and Server VDI Workers
- Citrix License Server
- Citrix CloudPortal Services Manager 10
- Citrix EdgeSight 5.2.1
- Citrix Web Interface 5.4
- Citrix Secure Gateway
- Citrix Service Provider Automation Pack
- Citrix Cloud Provider Pack (Includes App Orchestration)
- Citrix Receiver



- **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 XenApp 6.5 Delivery controllers and Hosted Shared Workers** – The XenApp components are used to deliver shared hosted applications and desktops within the multi-tenant Hosted desktop solution.
- **Citrix XenDesktop 5.6 Delivery controllers and Server VDI Workers** – The XenDesktop components are used to manage and deliver dedicated “Server VDI” Windows desktops within the multi-tenant Hosted Desktop solution.
- **Citrix License Server** – The Citrix License Server hosts all of the licenses that enable the CSP environment as well as providing the tools to enable CSP reporting of month-to-month usage back to Citrix.
- **Citrix CloudPortal Services Manager 10** – Citrix CloudPortal Services Manager will be used to provision applications, back-office services and desktops to multiple tenants from a single interface. This component also enables a CSP to provide self-service provisioning capabilities for their tenants that may require this level of service.
- **Citrix EdgeSight 5.2.1** – Citrix EdgeSight provides a detailed, end-to-end view of the hosted desktop environment for pro-active support and maintenance, as well as re-active troubleshooting of the complete Hosted desktop system.
- **Citrix Web Interface 5.4** – Citrix Web Interface provides a web-based logon point that enables subscribers to view and access their application and desktop resources as published by AzureCSP.
- **Citrix Secure Gateway** – Citrix Secure Gateway is installed on Windows Servers to provide a SSL secured proxy from subscriber end-point device, through the public internet to AzureCSP hosted applications and desktops.

- **Citrix Service Provider Automation Pack** – The Citrix Service Provider Automation Pack streamlines the installation and configuration of the Citrix XenApp Farm, providing a consistent and relatively hands-free build of a Citrix best practices XenApp solution for CSPs.
- **Citrix Cloud Provider Pack (Includes App Orchestration)** – The Citrix Cloud Provider Pack enables many of the latest available CSP specific technologies, including; App Orchestration, Local App Access, and the Citrix Mobility Pack.

These Citrix components communicated with each other in order to deliver a secure remote access connection to the Hosted desktop, for an in-depth technical explanation of component communication please review the Citrix Service Provider Reference Architecture.

Citrix Service Provider Hosted Desktop on Azure Architecture

Once AzureCSP had completed their assessment and concluded that a Citrix hosted desktop solution on Microsoft Azure could meet their objectives, they quickly moved into the design phase. AzureCSP needed a simple, easy process to determine the hardware and storage sizing to support their individual implementation based on the needs of their subscribers. AzureCSP 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, AzureCSP made the following design decisions:

- Although Project Accelerator was designed for Enterprise deployments of Citrix technologies its output could be used as a foundational design to work from in conjunction with the Citrix Service Provider Reference Architecture.
- 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 subscribers would need to connect to AzureCSP over an encrypted connection.
- In addition to the Citrix hosted desktop enabling products, Active Directory, DNS/DHCP, and SQL Server would need to be provisioned in Azure for this solution.
- A variety of healthcare, legal and financial applications, as well as MS Office would be made available as a part of the monthly subscription.
- Four different pricing tiers for services, requiring three different base desktop types would be offered to tenants;
  - **A Basic Desktop** – consisting of a Windows desktop, anti-virus, Microsoft Word, Excel and Internet Explorer, plus Adobe Acrobat Reader.

- **A Premium Desktop** – consisting of the Basic Desktop, plus the appropriate LOB applications for a particular vertical market as available and manage by AzureCSP.
- **A Dedicated Desktop** – consisting of a Windows VDI desktop that would enable virtually any application to be installed and managed either by AzureCSP or the subscriber if agreed. These desktops are most usually allocated to a niche of users within an organization, typically an application developer or a multi-media content developer or team.
- **Custom Hosted Desktop** services for larger organizations with complex application and self-service IT needs. This tier of services is not covered in this guide although Citrix hosted desktop on Microsoft Azure could certainly be used as a part of the custom solution.

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 AzureCSP's projected hardware, and infrastructure requirements based on a total subscriber base of 5000, spread over the 3 primary pricing tiers as discussed above.

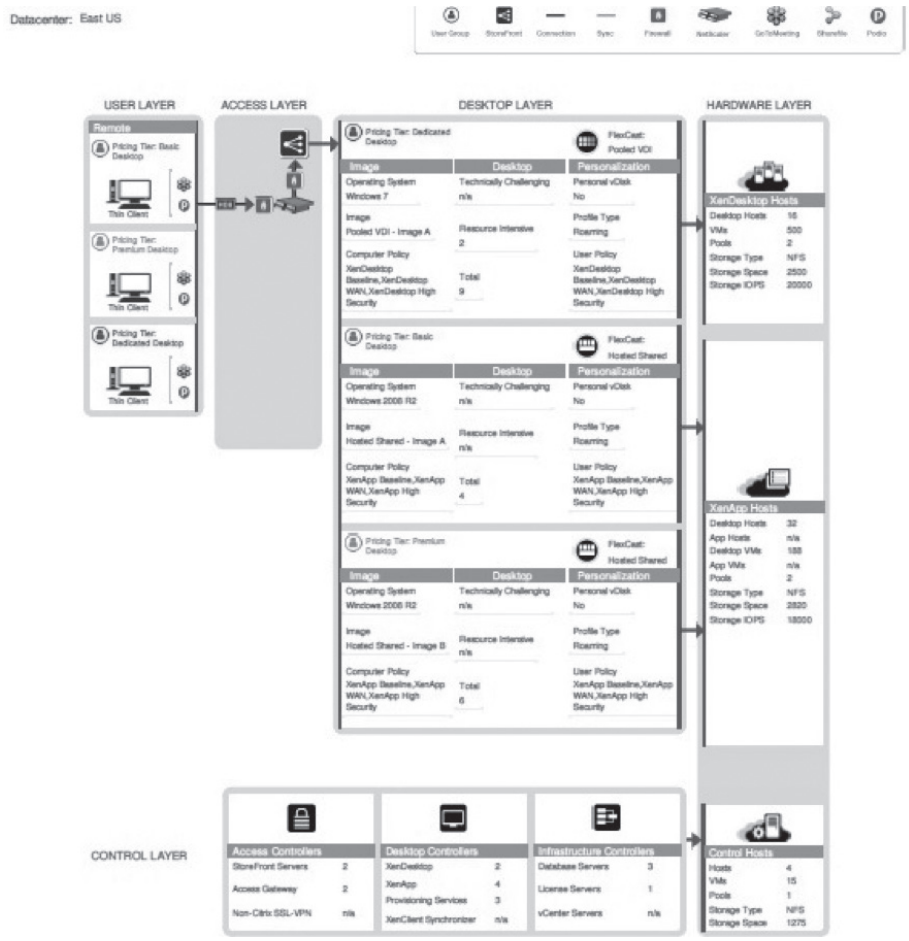


Figure 1: Project Accelerator OutPut for AzureCSP

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 AzureCSP services 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 subscriber requirements and use cases across multiple tenants. 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.

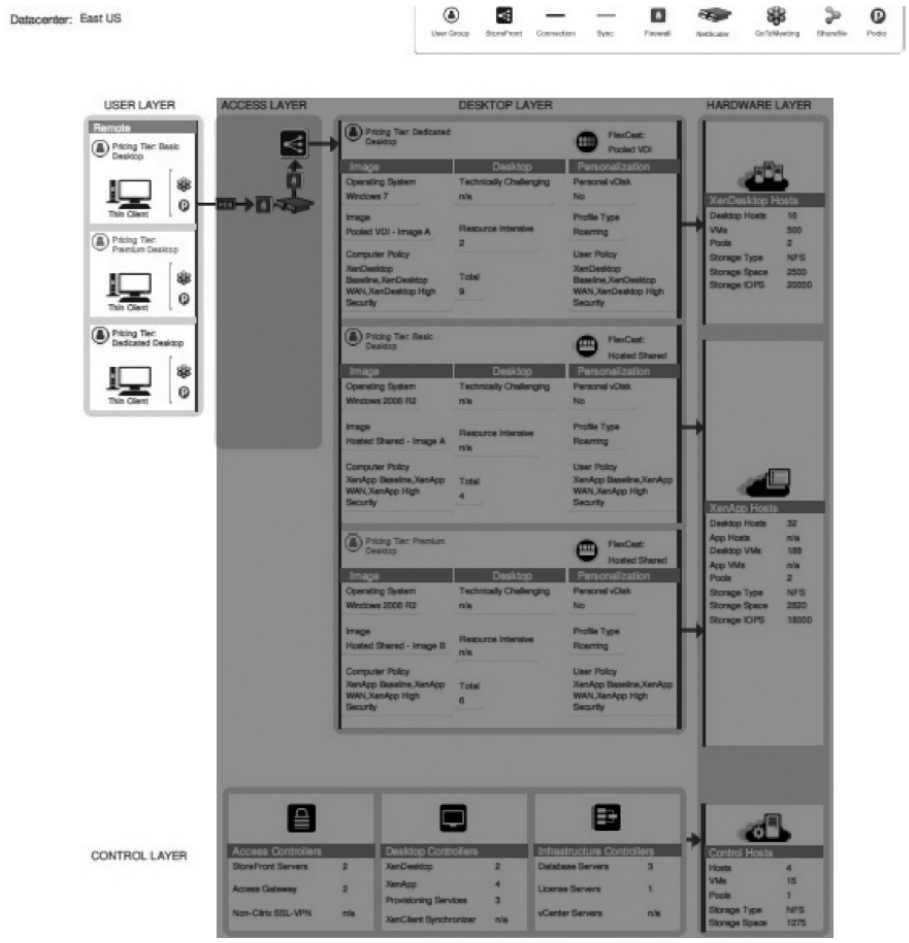


Figure 2: User Group

AzureCSP requires the following Citrix components on each subscriber's 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 CSP on Azure environment.

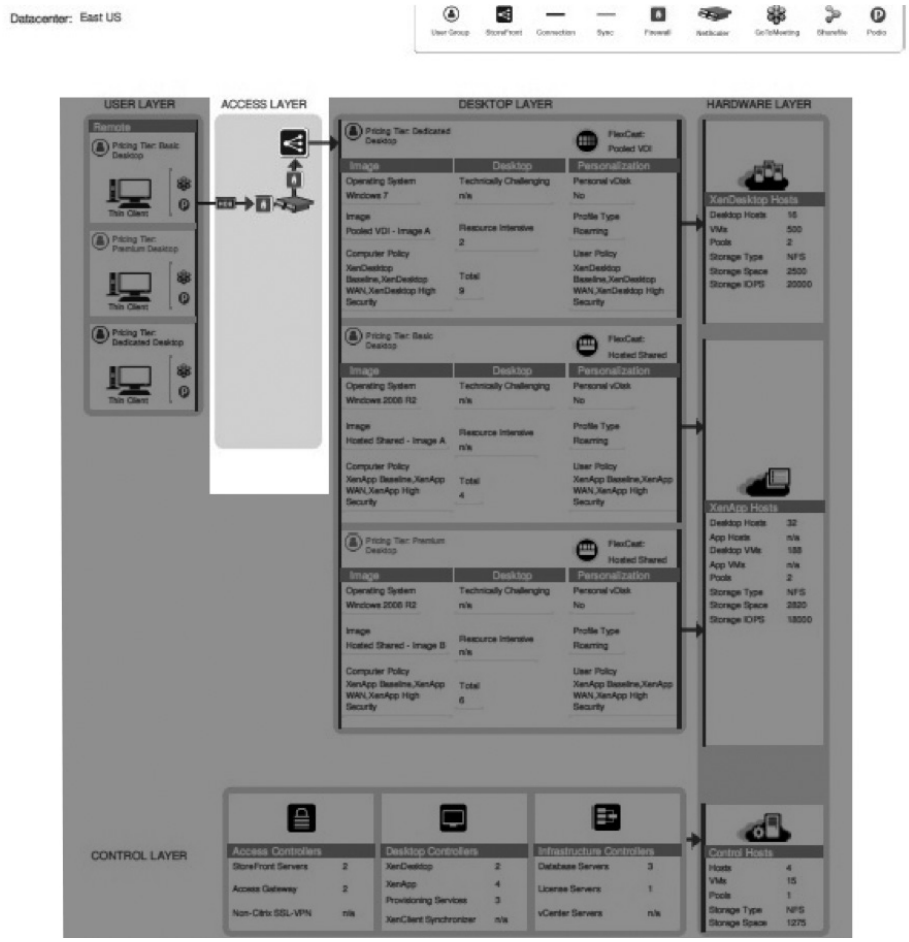


Figure 3: Access layer

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

- **Web Interface and Secure Gateway Services** – Web Interface is combined with Citrix Secure Gateway to provide secure access to advertised desktop and application services from Azure provisioned Windows Server instances. Web Interface sites can be aggregated to present both XenDesktop and XenApp resources in a single view from a single logon point for subscribers. Another advantage of using Web Interface in this scenario is that the App Orchestration technology currently available in the XenApp 6.5 Cloud Provider Pack can also orchestrate the provisioning of multi-tenant Web Interface sites based on pre-configured App Orchestration catalog parameters.

Web interface services	
Instances	2 Web Interface Server VMs
Virtual Machine configurations	
Memory	4 GB RAM
Processor	2 vCPUs
Hard Drive	60 GB
Installed software	
Web Interface	Web Interface 5.4
Windows Server	Windows Server 2008 R2 SP1
IIS	7.5
Microsoft .NET Framework	3.5 Service Pack 1
Windows PowerShell	2.0
MSFT Management Console	3.0
SQL Database	SQL Server 2008 R2 Enterprise
Ports utilized	
Web Interface	80, 443

Citrix Secure Gateway	
Instances	2 Secure Gateway Server VMs
Virtual Machine configurations	
Memory	4 GB RAM
Processor	2 vCPUs
Hard Drive	60 GB
Installed software	
Web Interface	Citrix Secure Gateway
Windows Server	Windows Server 2008 R2 SP1
IIS	7.5
Microsoft .NET Framework	3.5 Service Pack 1
Windows PowerShell	2.0
MSFT Management Console	3.0
Ports utilized	
Citrix Secure Gateway	443

Desktop layer

The Desktop layer represents the separate pricing tiers that AzureCSP plans to make available to tenants. As you can see, Azure CSP has assumed that the majority of Hosted desktop subscribers will use the Basic Desktop offering (3000 projected), half that many will use the Premium offering, and only 500 will require a Dedicated Desktop subscription.

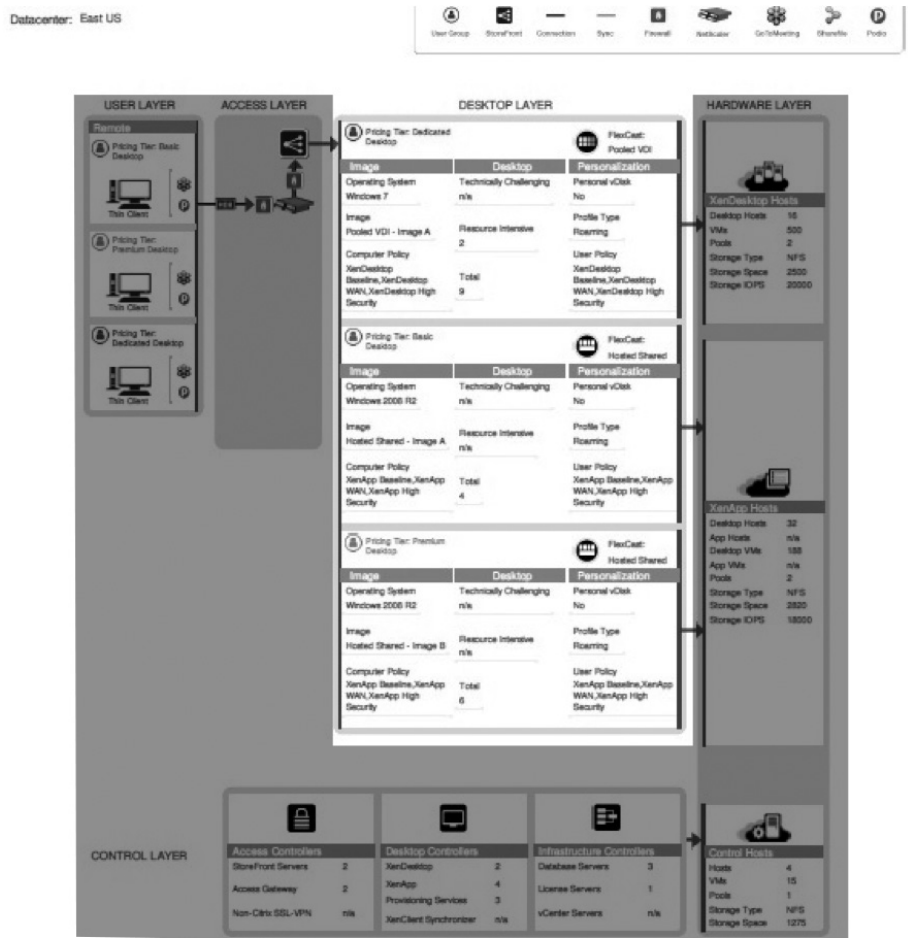


Figure 4: Desktop layer

AzureCSP's solution required the following Citrix components to provide the Desktop Layer, this layer is similar to the Multi-tenant Hosted desktop and Management modules within the Citrix Service Provider Reference Architecture, as a result AzureCSP cross referenced the output of the Project Accelerator with the CSP Reference Architecture, and the VM Instances available on Azure to determine the proper VM sizes for each component:

- **Citrix XenApp 6.5 Delivery controllers and Hosted Shared Workers** – The XenApp components are used to deliver shared hosted applications and desktops within the multi-tenant Hosted desktop solution.
- **Citrix XenDesktop 5.6 Delivery controllers and Server VDI Workers** – The XenDesktop components are used to manage and deliver dedicated "Server VDI" Windows desktops within the multi-tenant Hosted desktop solution.

- **Citrix License Server** – The Citrix License Server hosts all of the licenses that enable the CSP environment as well as providing the tools to enable CSP reporting of month-to-month usage back to Citrix.
- **Citrix CloudPortal Services Manager 10** – Citrix CloudPortal Services Manager will be used to provision applications, back-office services and desktops to multiple tenants from a single interface. This component also enables a CSP to provide self-service provisioning capabilities for their tenants that may require this level of service.
- **Citrix EdgeSight 5.2.1** – Citrix EdgeSight provides a detailed, end-to-end view of the Hosted desktop environment for pro-active support and maintenance, as well as re-active troubleshooting of the complete Hosted desktop system.

XenDesktop Controller Servers	
Instances	2 XenDesktop Controller VMs
Virtual Machine configurations	
Memory	4 GB RAM
Processor	2 vCPUs
Disk	60 GB HD
Installed software	
XenDesktop Version	5.6 Feature Pack 1 • XenDesktop Controller • Desktop Studio • Desktop Director
Windows Server	Windows Server 2008 R2 SP1
Microsoft .NET Framework	3.5 Service Pack 1
Internet Information Services (IIS) and ASP.NET	2.0
Visual J#	2.0 Redistributable Package, Second Edition
Visual C++	2008 Service Pack 1 Redistributable Package
Windows PowerShell	2.0
SQL Database	SQL Server 2008 R2 Enterprise
Ports utilized	
XenDesktop Controller	8080

XenDesktop Controller Servers	
Instances	4 XenApp Controller VMs
Virtual Machine configurations	
Memory	4 GB RAM
Processor	2 vCPUs
Disk	60 GB HD
Installed software	
XenDesktop Version	6.5 Feature Pack 1 • XenApp • Service Provider Automation Pack • Cloud Provider Pack
Windows Server	Windows Server 2008 R2 SP1
Microsoft .NET Framework	3.5 Service Pack 1
Internet Information Services (IIS) and ASP.NET	2.0
Visual J#	2.0 Redistributable Package, Second Edition
Visual C++	2008 Service Pack 1 Redistributable Package
Windows PowerShell	2.0
SQL Database	SQL Server 2008 R2 Enterprise
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 AzureCSP's implementation of the Infrastructure Controllers and Control Hosts on Microsoft Windows Azure IaaS.

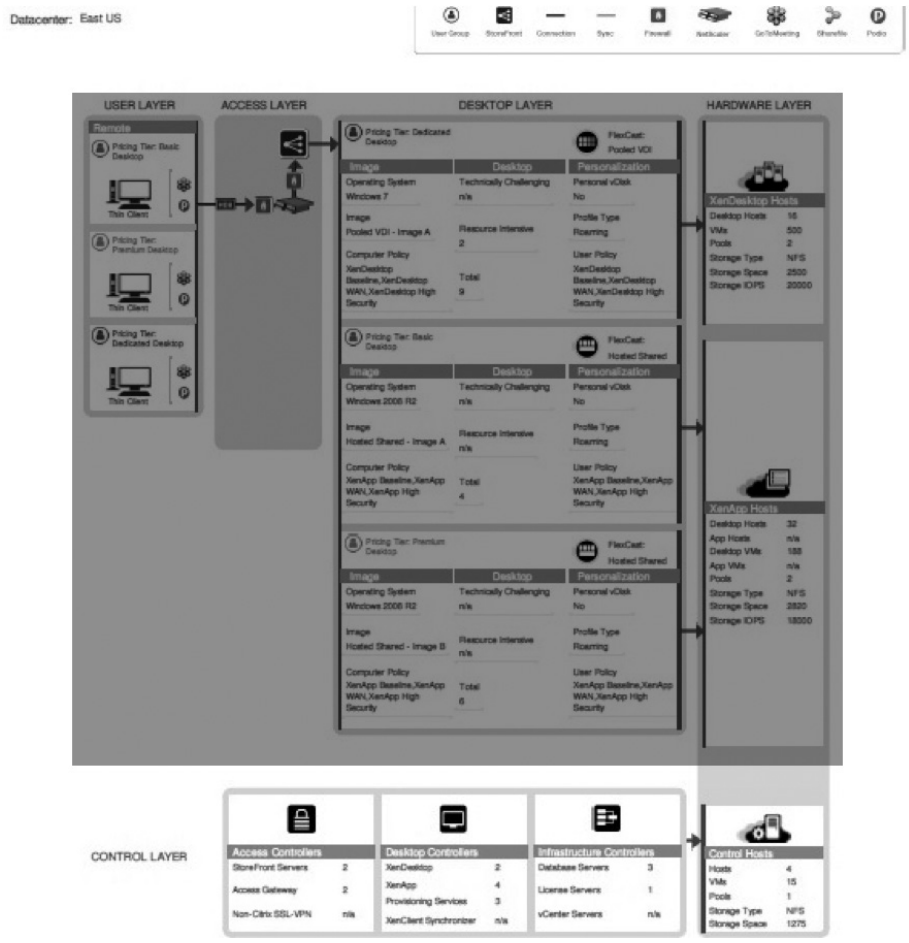


Figure 5: Control layer

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

- **Active Directory** – Citrix hosted desktops 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 foundation for the overall hosted desktop solution by storing all configurations, desktop and utilization information. EdgeSight and CloudPortal Service Manager also depend upon SQL Server Database Services.

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

- **License Server** – The license server manages all of the Citrix licenses required to support the environment.

License Server requirements	
Instances	1 License Server VM
Virtual Machine configurations	
Memory	4 GB RAM
CPU	2 vCPUs
Disk	60 GB
Installed software	
Citrix License Server	11.10.0
Windows Server	Windows Server 2008 R2
Microsoft .NET Framework	3.5
Ports utilized	
Citrix License Server	2700, 7279

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 for the Dedicated Desktops 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:

- **Delivery Services Console** – The Delivery Services Console is a tool that snaps into the Microsoft Management Console (MMC) and enables you to perform a number of XenApp management functions. With Delivery Services Console AzureCSP can set up and monitor servers, server farms, published resources, and sessions. They can set up policies and printers, configure Citrix Receiver client application access, and find troubleshooting information. In addition, AzureCSP can manage load balancing, diagnose problems in their farms, view hotfix information for their Citrix products, and track administrative changes.
- **License Administration Console** – Use this console to manage and track Citrix software licenses.
- **SpeedScreen Latency Reduction Manager** – Use this tool to configure local text echo and other features that improve the user experience on slow networks.

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

Citrix Service Provider Reference Architecture modifications within Azure

The solutions and capabilities outlined in this section influenced the CSP Reference Architecture when implemented in the Azure environment. All three multi-tenant isolation models from the CSP Reference Architecture (Farm Isolation, Server Isolation, and Session Isolation) can be hosted within Azure, although there are some networking specifics within Azure today that require a simplification of the firewall and networking scheme as documented in the CSP Reference Architecture. As a result single-farm multi-vLAN solutions are not recommended within a pure Azure environment today. Citrix will continue to work with Microsoft to investigate various multi-tenancy opportunities and alternatives as both of our service provider roadmaps evolve. The diagram of this modified architecture below illustrates the recommended design within Azure while maintaining the core practices documented in the CSP Reference Architecture.

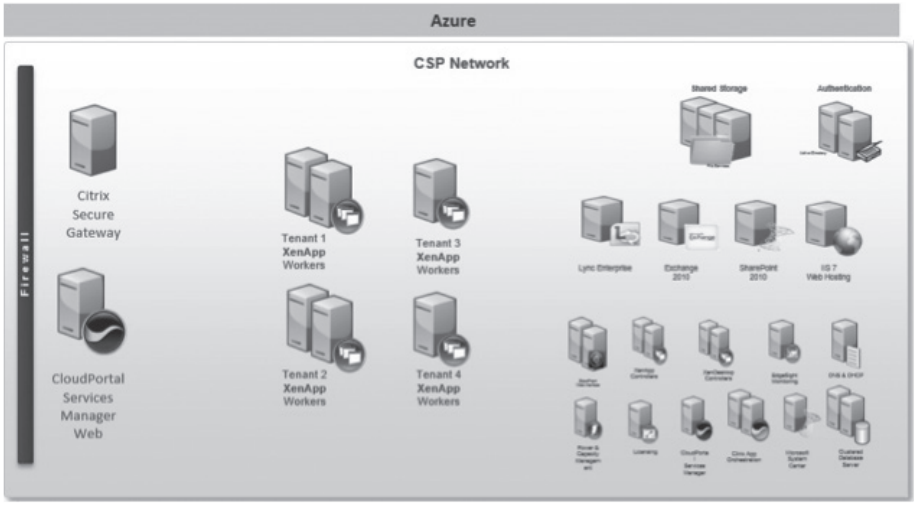


Fig A1.1

The following sections outline some of the considerations within Azure that have influenced this design.

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 CSP management and tenant workloads.

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 2008 R2 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 CSP workloads within Azure is provided through the Citrix Secure Gateway when connecting directly across the public internet to Azure hosted workloads.

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

Microsoft instances and services used for this guide

Microsoft Windows Server 2008 R2 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

The following Citrix components are currently supported within Azure.

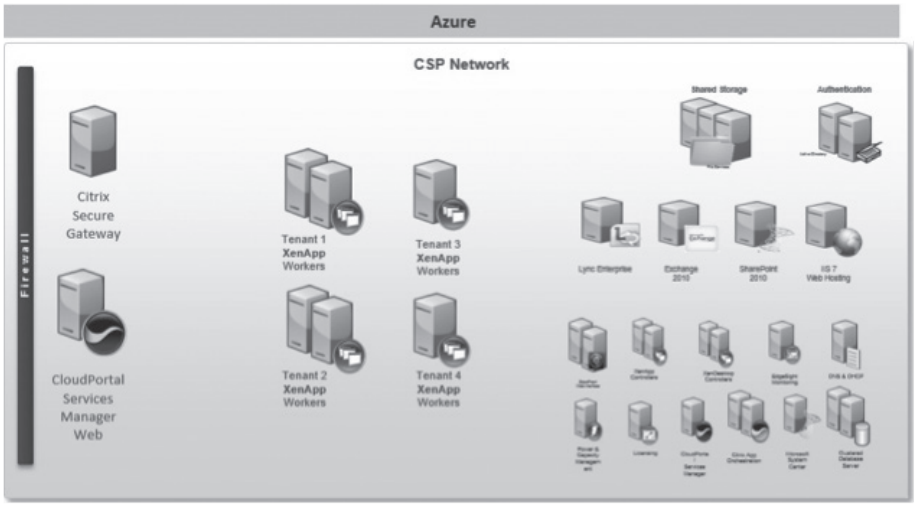
- Citrix XenApp 6.5 Delivery controllers and Hosted Shared Workers
- Citrix XenDesktop5.6 Delivery controllers and Server VDI Workers
- Citrix License Server
- Citrix CloudPortal Services Manager 10
- Citrix EdgeSight 5.2.1
- Citrix Web Interface 5.4
- Citrix Secure Gateway
- Citrix Service Provider Automation Pack
- Citrix Cloud Provider Pack (Includes App Orchestration)

Automation and orchestration

Automation and Orchestration of Citrix XenApp 6.5 Farms within the Azure environment is enabled through Citrix App Orchestration 1.0 from the March 2011 Citrix Cloud Provider Pack. All XenDesktop 5.6 Server VDI Farms and workloads must be manually provisioned at this time. All VM instances are manually created for this guide but Azure PowerShell scripting should be used for continuity at larger scale. Sample scripts as used by Citrix are provided in the Appendix.

Scenario: Azure as the CSP's primary datacenter

Sample architecture



The management network

The CSP Active Directory Forest

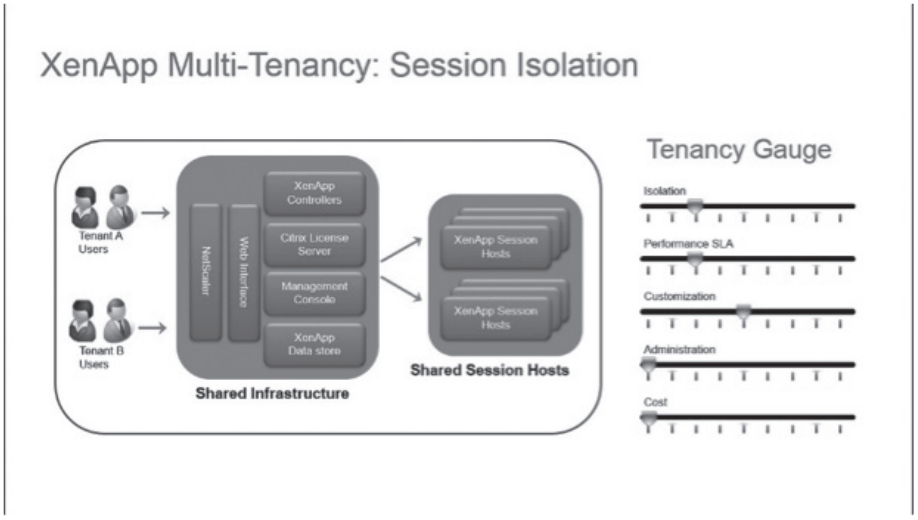
The Citrix Service Provider Reference Architecture leverages Microsoft Active Directory and Group Policy for several key capabilities. Leveraging Active Directory enables standards based, streamlined provisioning and management of tenant and subscriber environments, configuration and orchestration of Citrix workloads, and the provisioning of various back office services such as; Microsoft Exchange and Microsoft Lync Services, all of which should be managed through Citrix CloudPortal Services Manager. It is recommended that a pair of Active Directory servers be provisioned within Azure to provide high availability of AD services as well as to provide the best performance when larger scale environments are anticipated.

Shared storage services

Shared Storage within the design is enabled through Windows Server 2008 R2 with the File Services Role installed. User's Roaming Profile paths and a user home drive are mapped to this file server for basic functionality. Additional shares can be created as necessary.

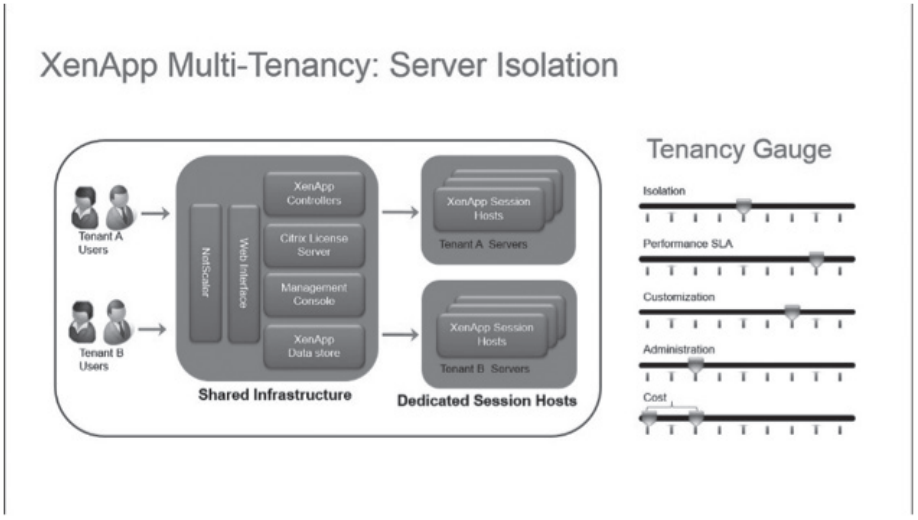
Hosted shared desktops and the shared XenApp 6.5 Farm

For this scenario a single XenApp 6.5 Farm is used to deliver Hosted Shared Desktops and Applications. XenApp Session Host Workers can be shared across multiple tenants when using the Session Isolation mode…



(Figure A2.1)

… or groups of XenApp Worker Servers can be isolated for each tenant within the same farm using Citrix Worker Groups to enable Server Isolation mode.



(Figure A2.2)

These modes of isolation and others are detailed in the CSP Reference Architecture document. Both of these multi-tenant modes provide the greatest density of Hosted desktop services available in the market today while also providing appropriate levels of isolation and security for different target tenant markets. These two modes represent a large percentage of current production Hosted desktop deployments and have proven cost effective for businesses from the micro scale of 2-5 users, to much larger organizations that may require Windows desktop and application services for more than a thousand users per tenant.

Server VDI and the shared XenDesktop 5.6 Farm

A single XenDesktop 5.6 Farm can be used to deliver Server VDI desktops from Azure. These desktops provide many of the benefits of Client based VDI while using the Windows Server Operating System Instances that are available through Azure. More detail on Citrix XenDesktop Server VDI capabilities can be found in the Citrix Cloud Provider Pack documentation available to Citrix Service Providers and on the XenApp 6.5 Downloads page at http://www.citrix.com/downloads.

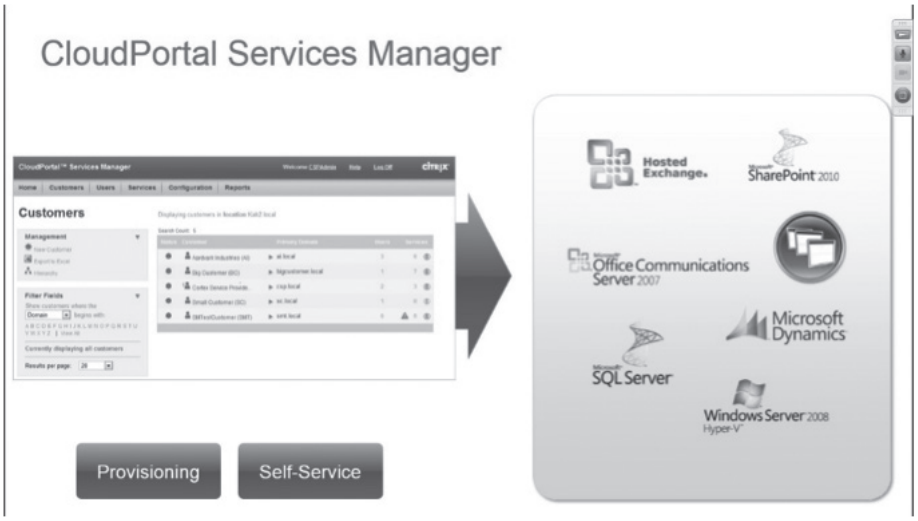
The shared web interface server

For this scenario Web Interface is combined with Citrix Secure Gateway to provide secure access to advertised desktop and application services from Azure provisioned Windows Server instances. Web Interface sites can be aggregated to present both XenDesktop and XenApp resources in a single view from a single logon point for subscribers. Another advantage of using Web Interface in this scenario is that the App Orchestration technology currently available in the XenApp 6.5 Cloud Provider Pack can also orchestrate the provisioning of multi-tenant Web Interface sites based on pre-configured App Orchestration catalog parameters.

Provisioning with Citrix CloudPortal Service Manager

CloudPortal Services Manager provides a single pane of glass for provisioning and management of Desktops, Applications and Back Office Services such as Microsoft Exchange and Microsoft Lync across multiple tenants. There are no special considerations when implementing CPSM within an Azure hosted CSP environment.

More information on CloudPortal Services Manage can be found at http://www.citrix.com/products/cloudportal-services-manager/overview.html.



Monitoring with Citrix EdgeSight

EdgeSight integration provides HDX monitoring and troubleshooting capabilities. Use of EdgeSight can also simplify Citrix CSP License reporting, for use in CSP billing systems as well as for their monthly license reporting.

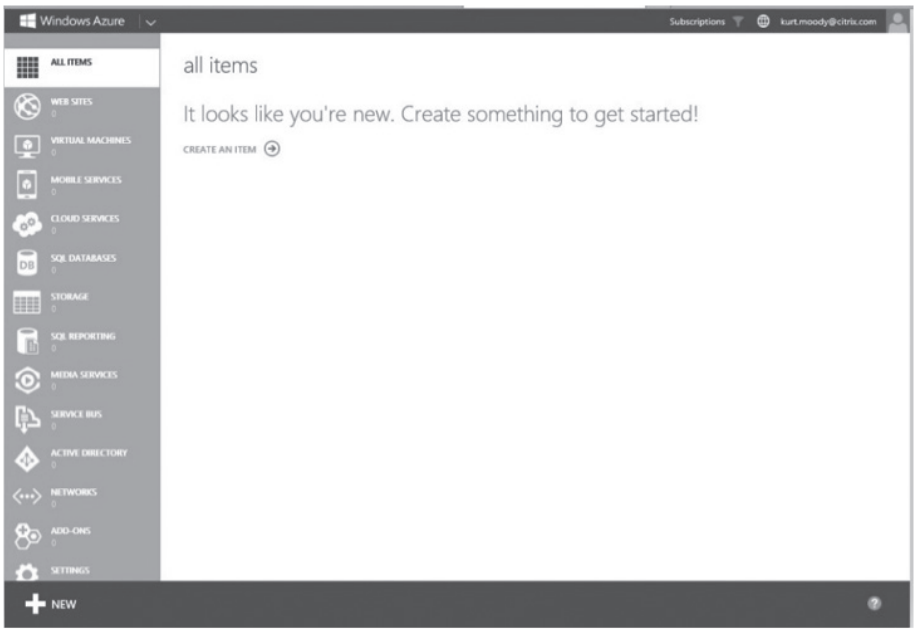
The EdgeSight inherent multi-tenant architecture enables CSPs to delegate certain reporting and monitoring capabilities to their tenants. There are no special considerations when implementing EdgeSight within an Azure hosted CSP environment.

Building the multi-tenant Hosted Desktop Network

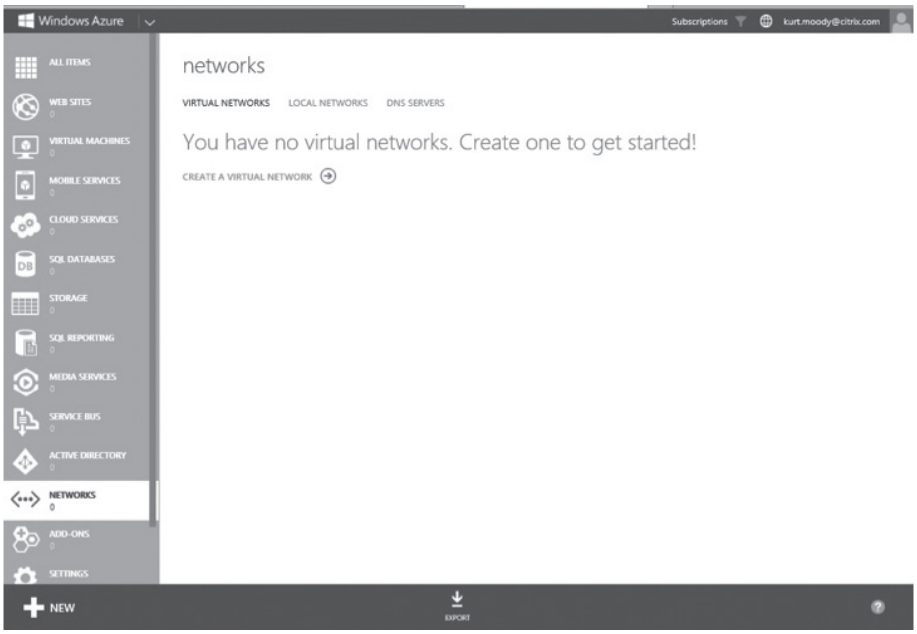
Considerations when building the base Azure virtual networks and active directory VM instances

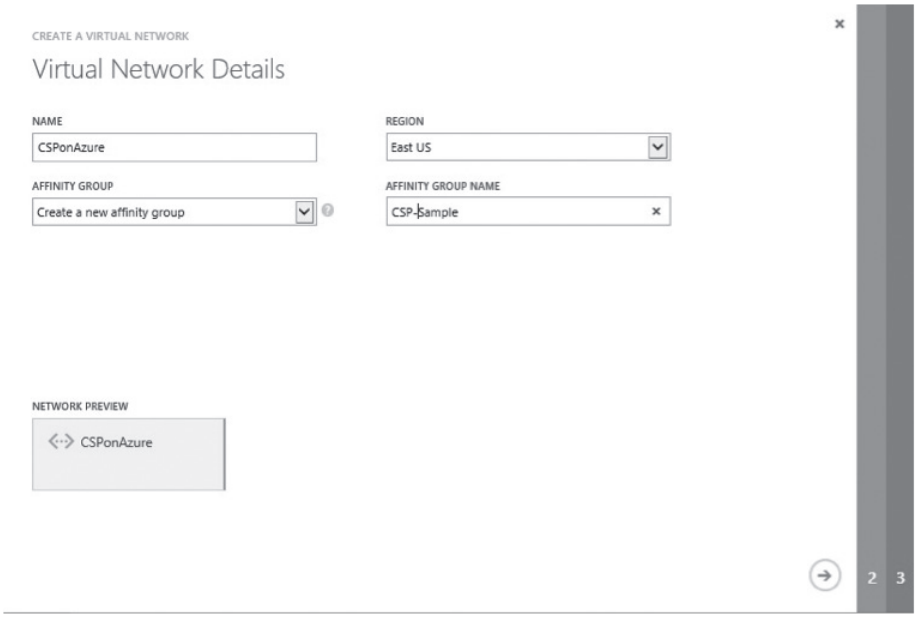
As stated earlier, a single virtual network is used for this scenario. Below is a brief walk-through of how a Virtual Network would be created for this scenario using the Azure Portal.

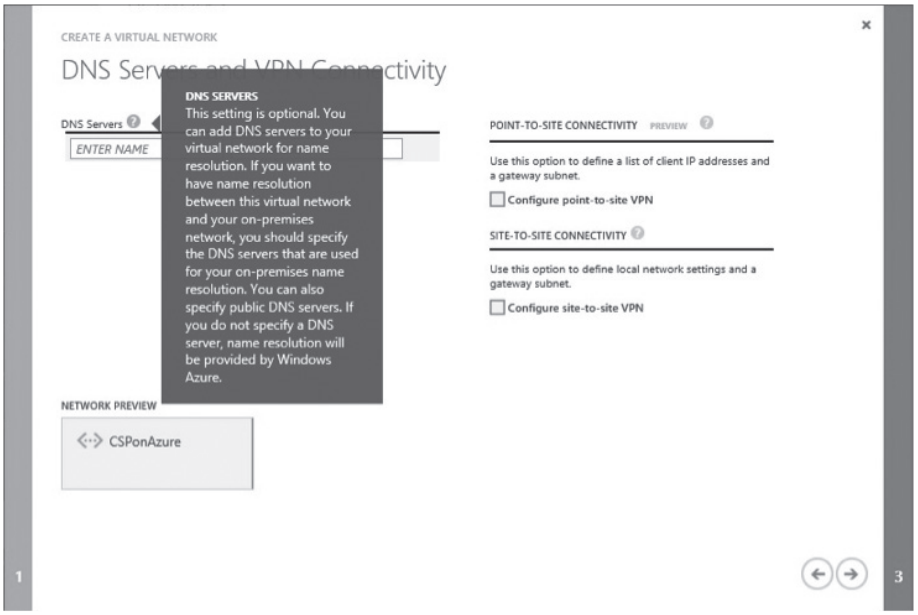
Starting with a blank Azure Subscription…

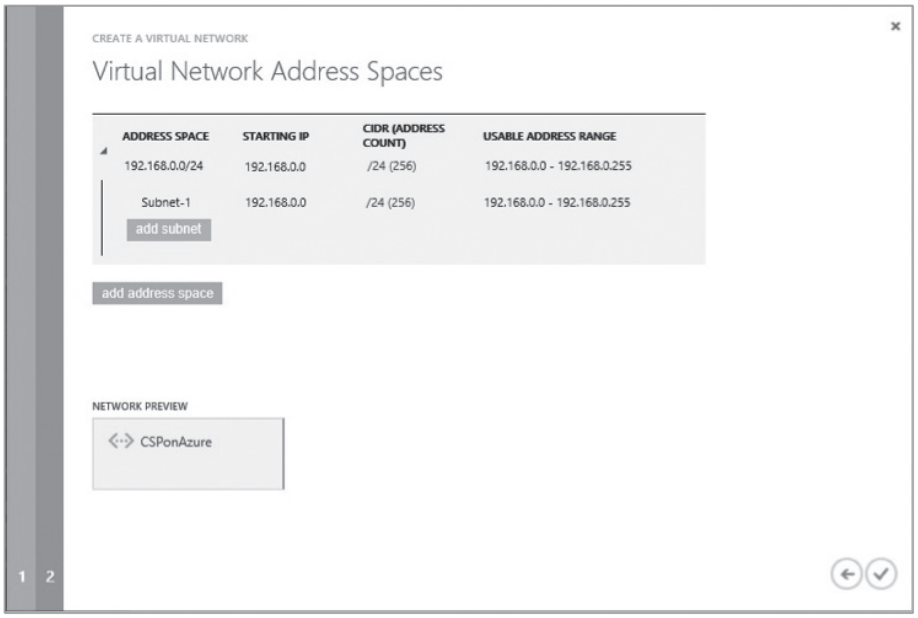


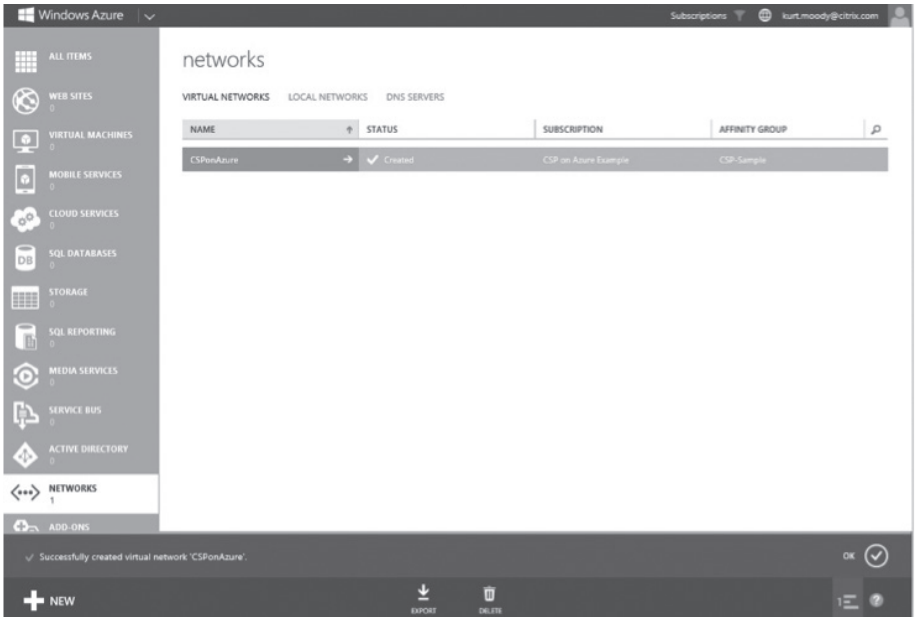
Create a network




CREATE A VIRTUAL NETWORK
Virtual Network Details
NAME
CSPonAzure
REGION
East US
AFFINITY GROUP
Create a new affinity group
AFFINITY GROUP NAME
CSP-Sample
NETWORK PREVIEW
CSPonAzure
2
3


CREATE A VIRTUAL NETWORK
DNS Servers and VPN Connectivity
DNS Servers
ENTER NAME
DNS SERVERS
This setting is optional. You can add DNS servers to your virtual network for name resolution. If you want to have name resolution between this virtual network and your on-premises network, you should specify the DNS servers that are used for your on-premises name resolution. You can also specify public DNS servers. If you do not specify a DNS server, name resolution will be provided by Windows Azure.
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
NETWORK PREVIEW
CSPonAzure
1
3

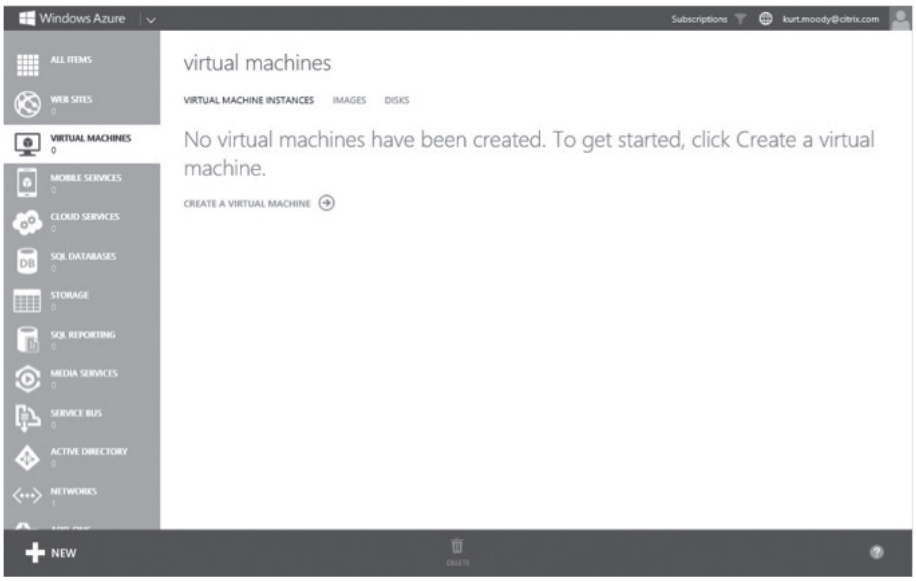




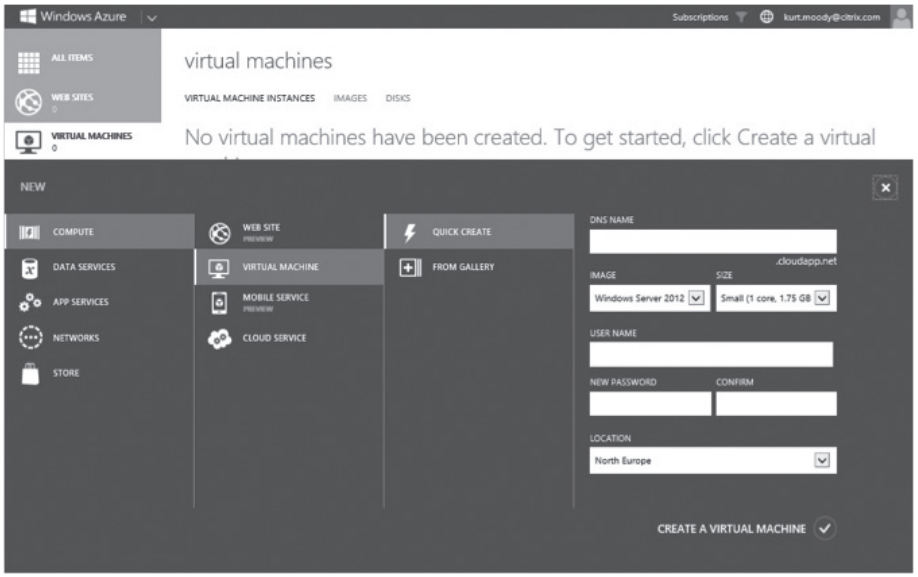
Once the virtual network is in place the Active Directory Forest and Controllers must be created…

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” …



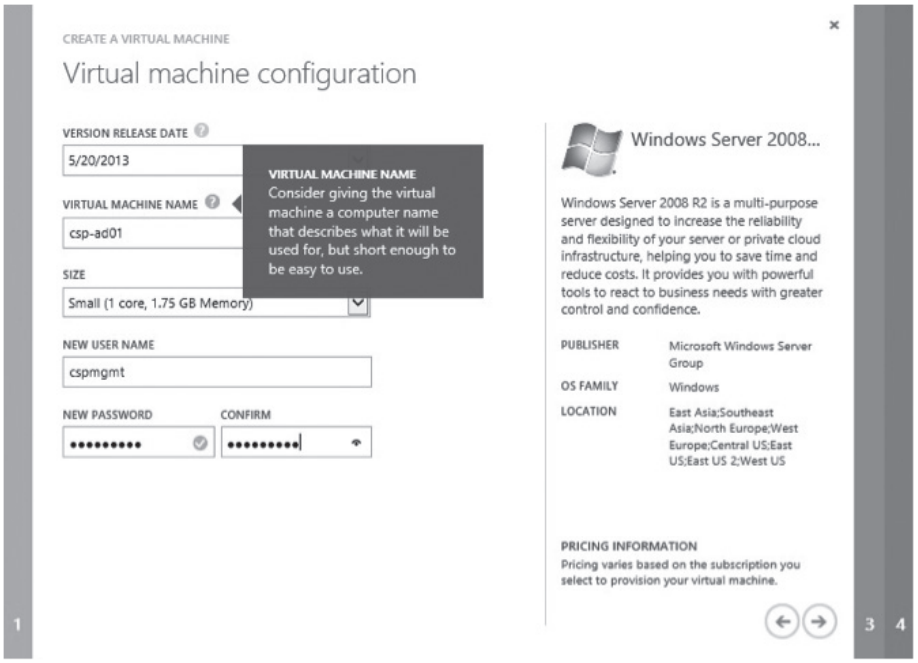
Click “From Gallery”



For this example we will use the Windows Server 2008 R2 SP1 Template from the Azure Gallery.

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

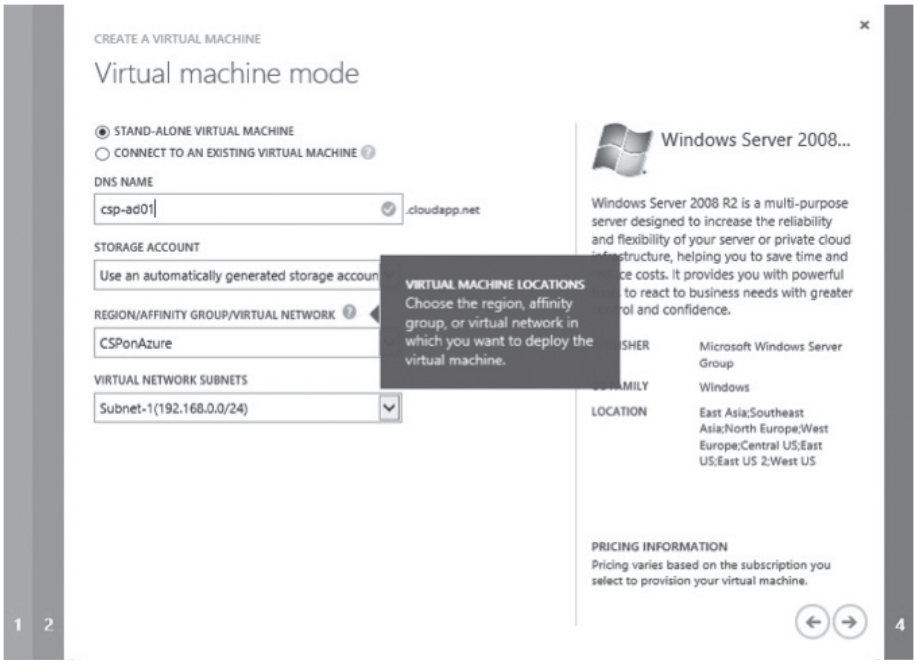
Next we will name this VM instance csp-ad01 and choose the small instance type. You may choose a larger instance depending upon the scale of you offering…



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.

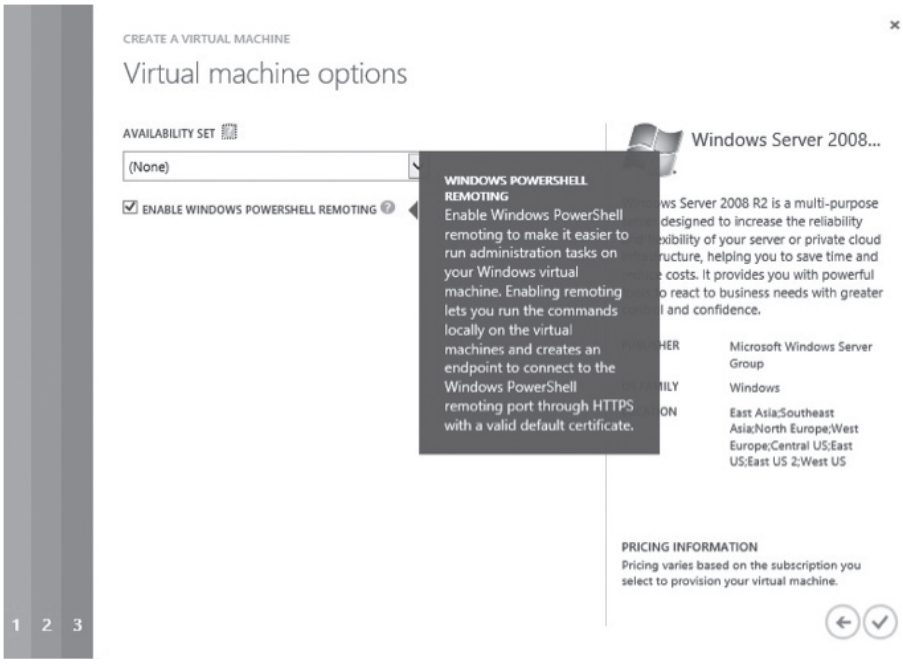
Click the right facing arrow to indicate you are ready to proceed…

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

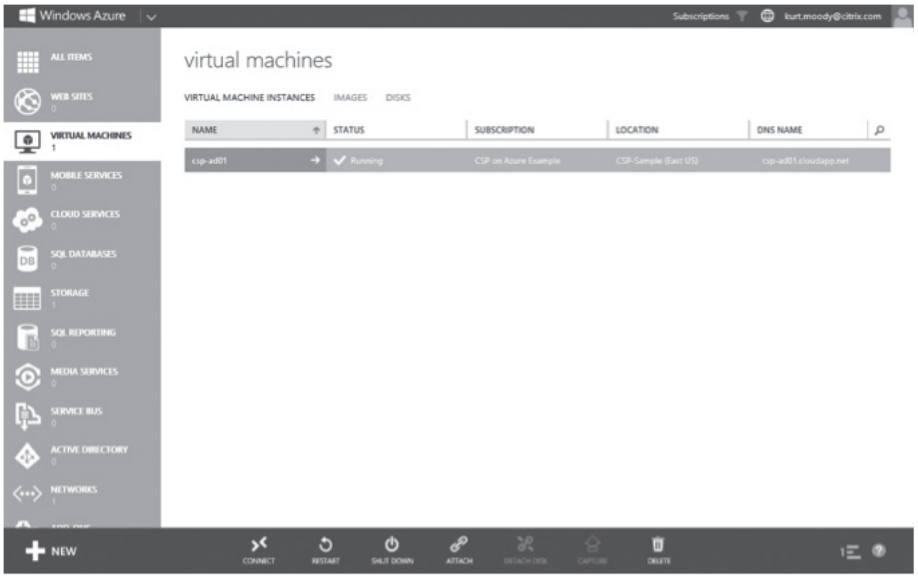


Click the right facing arrow to indicate you are ready to proceed…

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



Once the provisioning of the VM has finished you should see the instance in a running state.



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 networking and VM instances are in place the standard XenApp and XenDesktop installation procedures as outlined in the product documentation and CSP implementation guides should be followed. There are no special considerations when implementing XenApp and XenDesktop delivery controllers or worker servers within an Azure hosted CSP environment.

Citrix Multi-tenant Farm creation is accomplished through the use of the App Orchestration technology available in the Citrix Cloud Provider Pack. The initial environment configured by the CSP Automation Pack and the Citrix Cloud Provider Pack enables the basic Hosted desktop service that can then be customized and expanded based on your business needs.

The CSP Automation Pack will create a basic environment within Azure as shown in Fig A3.1.

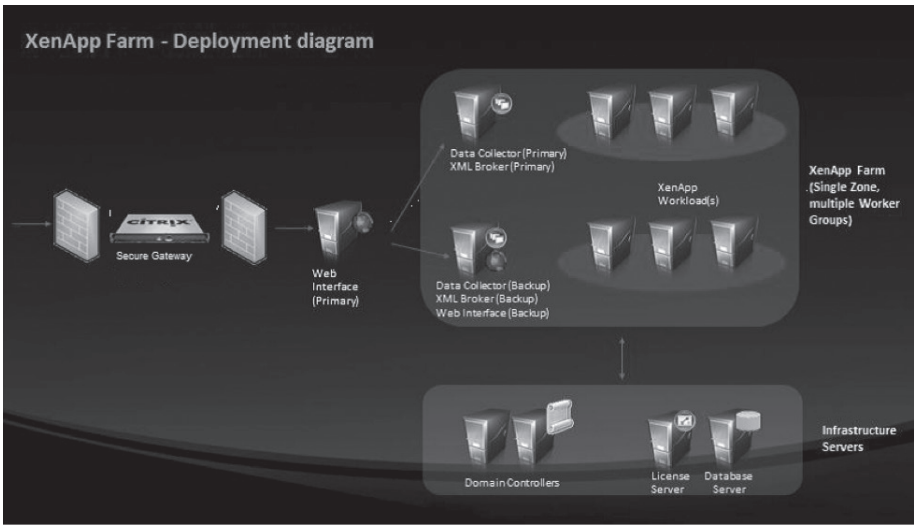


Fig A3.1

Once this first XenApp Farm is created additional farms and workloads can be provisioned within the environment using Citrix App Orchestration. The complete environment will reflect the Citrix products in Fig A3.2.

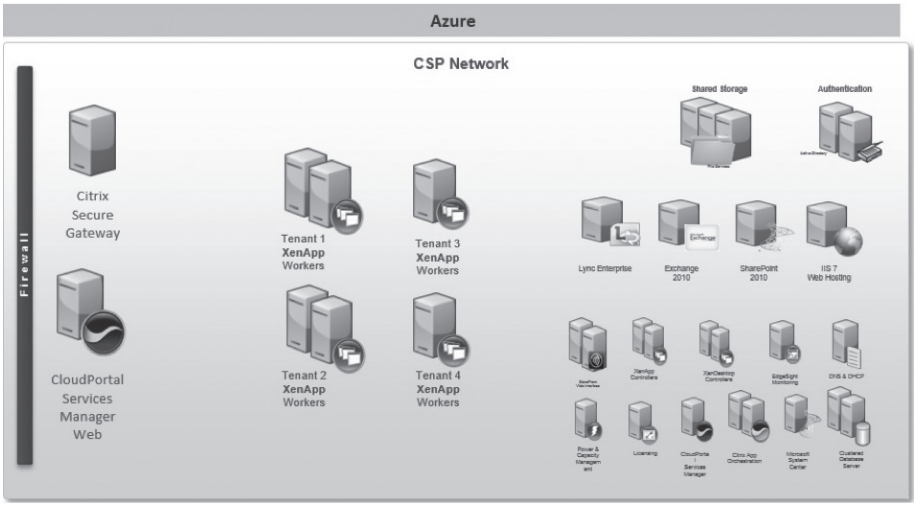


Fig A3.2

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 Citrix Service Provider Reference Architecture AzureCSP was able to create a Hosted desktop solution within Microsoft's Azure IaaS environment. Leveraging public cloud infrastructure such as Azure virtually eliminated AzureCSP's initial capital investment, allowing them to bring their new Hosted desktop service online quickly in a globally available, state of the art cloud hosted infrastructure.

By leveraging Citrix products AzureCSP was capable of building a Hosted desktop offering that provided tiered pricing levels based on different use cases and multi-tenancy requirements, including self-service, at multiple layers of the virtualization stack, while also delivering the best subscriber experience in the market as enabled by Citrix technologies like HDX.

Additional resources

Citrix service provider web site

The CSP Toolkit

Citrix Service Provider Reference Architecture

CSP Sample Videos On CitrixTV

Citrix Project Accelerator

Microsoft Windows Azure Site

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

CITRIX®

Corporate Headquarters
Fort Lauderdale, FL, USA

Silicon Valley Headquarters
Santa Clara, CA, USA

EMEA Headquarters
Schaffhausen, Switzerland

India Development Center
Bangalore, India

Online Division Headquarters
Santa Barbara, CA, USA

Pacific Headquarters
Hong Kong, China

Latin America Headquarters
Coral Gables, FL, USA

UK Development Center
Chalfont, United Kingdom

About Citrix
Citrix (NASDAQ:CTXS) is the cloud company that enables mobile workstyles—empowering people to work and collaborate from anywhere, easily and securely. With market-leading solutions for mobility, desktop virtualization, cloud networking, cloud platforms, collaboration and data sharing, Citrix helps organizations achieve the speed and agility necessary to succeed in a mobile and dynamic world. Citrix products are in use at more than 260,000 organizations and by over 100 million users globally. Annual revenue in 2012 was $2.59 billion. Learn more at www.citrix.com.