

Microsoft Azure Desktop Hosting Reference Architecture Guide

Session Desktops and Remote Applications Running On Microsoft Azure Infrastructure Services

Published: November 2014  
Microsoft Corporation

**Copyright information**

This document is provided "as-is". Information and views expressed in this document, including URL and other Internet website references, may change without notice.

Some examples depicted herein are provided for illustration only and are fictitious. No real association or connection is intended or should be inferred.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

Microsoft, Active Directory, Hyper-V, SQL Server, Windows PowerShell, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. All other trademarks are property of their respective owners.

© 2014 Microsoft Corporation. All rights reserved.

Contents

[1 Desktop Hosting Service Logical Architecture 5](#_Toc403487837)

[2 Desktop Hosting Service 7](#_Toc403487838)

[2.1 Tenant Environment 7](#_Toc403487839)

[2.2 Remote Desktop Web Access 7](#_Toc403487840)

[2.3 Remote Desktop Gateway 8](#_Toc403487841)

[2.4 Active Directory Domain Services 8](#_Toc403487842)

[2.5 Remote Desktop Connection Broker 9](#_Toc403487843)

[2.6 RD License 10](#_Toc403487844)

[2.7 Remote Desktop Session Host 11](#_Toc403487845)

[2.7.1 User Profile Disks 11](#_Toc403487846)

[2.8 File Server 12](#_Toc403487847)

[3 Azure Infrastructure Services 12](#_Toc403487848)

[3.1 Azure Management Portal 12](#_Toc403487849)

[3.2 Azure Load Balancer 12](#_Toc403487850)

[3.3 Azure Virtual Private Networking (VPN) 13](#_Toc403487851)

[3.4 Security Considerations 13](#_Toc403487852)

[3.5 Design Considerations 14](#_Toc403487853)

[4 Tenant On-Premises Components 14](#_Toc403487854)

[4.1 Clients 14](#_Toc403487855)

[4.2 Active Directory Domain Services 15](#_Toc403487856)

This document defines a set of architectural blocks for using Remote Desktop Services (RDS) and Microsoft Azure Virtual Machines to create multitenant, hosted Windows® desktop and application services, referred to in this document as “desktop hosting.” The primary goal is to help customers create highly secure, scalable, and reliable desktop hosting solutions for small- and medium-sized organizations with 5 to 5000 users.

The primary audience for this reference architecture are hosting providers who want to leverage Microsoft Azure Infrastructure Services to deliver desktop hosting services and Subscriber Access Licenses (SALs) to multiple tenants via the [Microsoft Service Provider Licensing Agreement](http://www.microsoft.com/hosting/en/us/licensing/splabenefits.aspx) (SPLA) program. A second audience for this reference architecture are end customers who want to create and manage desktop hosting solutions in Microsoft Azure Infrastructure Services for their own employees using [RDS User CALs extended rights through Software Assurance](http://download.microsoft.com/download/6/B/A/6BA3215A-C8B5-4AD1-AA8E-6C93606A4CFB/Windows_Server_2012_R2_Remote_Desktop_Services_Licensing_Datasheet.pdf) (SA).

To deliver a desktop hosting solutions, hosting partners and SA customers leverage Windows Server® and the Windows Desktop Experience feature to deliver Windows users an application experience that is familiar to business users and consumers. **Although Windows 8.1, Windows 7, and earlier Windows client versions are not licensed for hosting environments with shared hardware, the Desktop Experience feature in Windows Server 2012 R2 provides a similar user experience and application support.**

The scope of this document is limited to:

* Architectural design guidance for a desktop hosting service.   
  Detailed information, such as deployment procedures, performance, and capacity planning is explained in separate documents. For more general information about Azure Infrastructure Services, see [Microsoft Azure Virtual Machines](http://www.windowsazure.com/en-us/documentation/services/virtual-machines/).
* Session-based desktops, RemoteApp applications, and server-based personal desktops that use Windows Server 2012 R2 Remote Desktop Session Host (RD Session Host).   
  Windows client-based virtual desktop infrastructures are not covered because there is no Service Provider License Agreement (SPLA) for Windows client operating systems. Windows Server-based virtual desktop infrastructures are allowed under the SPLA, and Windows client-based virtual desktop infrastructures are allowed on dedicated hardware with end-customer licenses in certain scenarios. However, client-based virtual desktop infrastructures are out-of-scope for this document.
* Microsoft® products and features, primarily Windows Server 2012 R2 and Microsoft Azure Infrastructure Services.
* Desktop hosting services for tenants ranging in size from 5 to 5000 users.   
  For larger tenants, this architecture may need to be modified to provide adequate performance. The Server Manager RDS graphical user interface (GUI) is not recommended for deployments over 500 users. PowerShell is recommended for managing RDS deployments between 500 and 5000 users.
* The minimum set of components and services required for a desktop hosting service.  
  There are many optional components and services that can be added to enhance a desktop hosting service, but these are out-of-scope for this document.

After reading this document, the reader should understand:

* The building blocks that are necessary to provide a secure, reliable, multitenant desktop hosting solution based in Microsoft Azure Infrastructure Services.
* The purpose of each building block and how they fit together.

There are multiple ways to build a desktop hosting solution based on this architecture. Throughout the document, variations are noted to address different requirements for scale and capability.

# Desktop Hosting Service Logical Architecture

A logical architecture diagram of the software components for a basic desktop hosting service in Microsoft Azure is shown in Diagram 1.



Diagram 1: Azure-based basic desktop hosting service logical architecture

The logical architecture diagram shows a two-layer architecture with the following layer definitions:

* **Desktop Hosting Service**: Virtual machines, networks, and storage that make up the functional service for each tenant.
* **Infrastructure Services**: Consists of the Azure Management Portal, Load Balancer, VPN gateway, Windows Server operating system instances running the Hyper-V role used to virtualize the physical servers, storage units, networks switches, routers, and so on that make up the Azure Infrastructure Services. The Azure Infrastructure Services allow the VMs, networks, storage, and applications to be created independently from underlying hardware.

The basic desktop hosting service can be extended by adding both desktop and RemoteApp collections and by duplicating the components to add higher availability and allow the service to scale out to larger numbers of users. A logical architecture diagram of the software components for an extended desktop hosting service in Microsoft Azure is shown in Diagram 2.



Diagram 2: Azure-based extended desktop hosting service logical architecture

Duplicated role services run in virtual machines assigned to same availability set in Azure to increase availability. The logical architecture diagram of the extended desktop hosting service shows a SQL Server AlwaysOn Availability Group that is required to create a Remote Desktop (RD) Connection Broker cluster.

# Desktop Hosting Service

## Tenant Environment

The provider’s desktop hosting service is implemented as a set of isolated tenant environments. Each tenant’s environment consists of one or more Azure Cloud Services, a storage container, and a set of virtual machines, all communicating over an isolated virtual network. Each virtual machine contains one or more of the components that make up the tenant’s hosted desktop environment. The following subsections describe the components that make up each tenant’s hosted desktop environment.

## Remote Desktop Web Access

The Remote Desktop Web Access (RD Web Access) component allows the tenant’s employees to have a single website where they can authenticate and then access Windows desktops and applications that are hosted in Microsoft Azure. By using RD Web Access, Windows desktops and applications can be published to a variety of Windows and non-Windows client devices, and they can be selectively published to specific users or groups.

The RD Web Access component requires installation of Internet Information Services (IIS). A Hypertext Transfer Protocol Secure (HTTPS) connection is used to provide an encrypted communications channel between the clients and the RD Web server. The RD Web Access virtual machine must have an Azure TCP endpoint with a private and public port of 443 to allow the tenant’s users to connect from the Internet using the HTTPS communications transport protocol.

Matching digital certificates must be installed on the server and clients. For development and testing purposes, this can be a self-generated and self-signed certificate. For a released service, the digital certificate must be obtained from a trusted certification authority. The name of the certificate must match the Fully Qualified Domain Name (FQDN) that is used to access RD Web Access whether that be the externally facing DNS name for the Azure Cloud Service or the CNAME DNS record pointing to the Azure Cloud Service.

For tenants with small numbers of users, the RD Web Access and Remote Desktop Gateway workloads may be combined in a single virtual machine to reduce cost. To provide a highly available service and to scale-out to larger numbers of users, additional RD Web virtual machines may be added to an RD Web Access farm. When a RD Web Access farm has been implemented in a multiple VMs for high availability and scale out, the HTTPS endpoints must be configured in a load-balanced set.

**Additional information:**

[Deploying and Configuring RD Web Access](http://social.technet.microsoft.com/wiki/contents/articles/10758.deploying-and-configuring-rd-webaccess-in-windows-server-2012.aspx)

[Publishing RemoteApps in Windows Server 2012 R2](http://social.technet.microsoft.com/wiki/contents/articles/10817.publishing-remoteapps-in-windows-server-2012.aspx)

[Distribution of Remote Apps and Desktops in Windows Server 2012 R2](http://social.technet.microsoft.com/wiki/contents/articles/14488.distribution-of-remote-apps-and-desktops-in-windows-server-2012.aspx)

## Remote Desktop Gateway

The Remote Desktop Gateway (RD Gateway) component enables tenant employees who are using client devices on the public Internet to securely access Windows desktops and applications that are hosted in a Cloud Service in Microsoft Azure.

The RD Gateway component uses Secure Sockets Layer (SSL) to provide an encrypted communications channel between the clients and the server. The RD Gateway virtual machine must have an Azure HTTPS endpoint with a private and public port of 443 to allow the tenant’s users to connect from the Internet using the HTTPS communications transport protocol. The RD Gateway virtual machine should also have an Azure UDP endpoint with a private and public port of 3391 to allow users to connect using the UDP protocol for improved performance. Matching digital certificates must be installed on the server and client. For development and testing purposes, this can be a self-generated and self-signed certificate. For a released service, the digital certificate must be obtained from a trusted certification authority. The name of the certificate must match the FQDN that is used to access RD Gateway whether that be the externally facing DNS name for the Azure Cloud Service or the CNAME DNS record pointing to the Azure Cloud Service.

For tenants with small number of users, the RD Web Access and RD Gateway can be combined on a single virtual machine to reduce cost. To provide a highly available service and to scale-out to larger numbers of users, additional RD Gateway virtual machines may be added to an RD Gateway farm. When an RD Gateway farm has been implemented in multiple VMs for high availability and scale out, the HTTPS and UDP endpoints must be configured in a load-balanced set and the Azure load balancer must be configured with client IP affinity so that all HTTPS connections from a client connect through the same RD Gateway virtual machine.

**Additional information:**

[Deploying and Configuring RD Gateway](http://social.technet.microsoft.com/wiki/contents/articles/10974.deploying-and-configuring-rd-gateway-in-windows-server-2012.aspx)

[What’s New In Windows Server 2012 R2 RD Gateway](http://blogs.msdn.com/b/rds/archive/2013/03/14/what-s-new-in-windows-server-2012-remote-desktop-gateway.aspx#loadbalancing)?

[RD Gateway Capacity Planning in Windows Server 2012 R2](http://download.microsoft.com/download/D/3/0/D308F3B6-5B4D-434C-AEDF-6E5B20B9746A/RD%20Gateway%20Capacity%20Planning%20in%20Windows%20Server%202012.docx)

## Active Directory Domain Services

The tenant’s network includes an Active Directory® Domain Services (AD DS) server for the tenant’s forest and domain. A stand-alone AD DS server may be provided by the hosting provider and located in the tenant’s virtual networking environment in Azure. Alternatively, an AD DS server can be located on the tenant’s premises and connected to the tenant’s virtual networking environment using a site-to-site VPN connection through the Azure Load Balancer. In the latter case, a replica domain controller can be provided in the tenant’s virtual networking environment to improve performance and reliability. All the virtual machines in the tenant’s virtual subnet are joined to the tenant’s domain. All the tenant’s users have user accounts in the tenant’s domain.

The VM used to deploy AD DS must have an Azure data disk attached and configured for the AD DS database and SYSVOL. An Azure data disk uses write-through caching which guarantees that writes to the disk persist across restarts of the VM.

If the provider is deploying AD DS in the Cloud Service for the tenant, then the DNS role will be deployed with AD DS and will serve as the primary DNS server for the other virtual machines in the tenant’s Cloud Service. To resolve names on the public Internet, the tenant’s DNS server forwards requests to a public DNS server.

To provide a continuously available service, two AD DS server virtual machines can be configured and assigned to the same availability set. The first AD DS domain controller deployed creates the tenant’s domain and the forest. By default, it holds the DNS role, and it is the operations master for all five operations master roles. A second domain controller is promoted as a replica in the tenant’s domain. The second domain controller’s preferred DNS server must be configured to point to the IP address of the first domain controller before running the promotion user interface.

The tenant’s forest does not require any trust relationship with the provider’s management forest. A domain administrator account may be set up in the tenant’s domain to allow the provider’s technical personnel to perform administrative tasks in the tenant’s environment (such as monitoring system status and applying software updates) and to assist with troubleshooting and configuration.

For small tenants, the cost can be reduced by combining AD DS, the file server, RD Connection Broker, and Remote Desktop Licensing (RD Licensing) on a single virtual machine on the tenant’s virtual network.

**Additional information:**

[What is Active Directory?](http://www.microsoft.com/en-in/server-cloud/windows-server/active-directory-overview.aspx)

[Windows Server 2012 R2: What’s new in Active Directory Domain Services?](http://technet.microsoft.com/en-us/library/hh831477)

[Microsoft Azure: Guidelines for Deploying Windows Server Active Directory on Microsoft Azure Virtual Machines](http://msdn.microsoft.com/en-us/library/windowsazure/jj156090.aspx)

[Microsoft Azure: How to Attach a Data Disk to a Virtual Machine](http://www.windowsazure.com/en-us/manage/windows/how-to-guides/attach-a-disk/)

[Manage the Availability of Virtual Machines](http://www.windowsazure.com/en-us/manage/windows/common-tasks/manage-vm-availability/)

[Microsoft Azure Virtual Network Overview](http://msdn.microsoft.com/library/windowsazure/jj156007.aspx)

## Remote Desktop Connection Broker

Remote Desktop Connection Broker (RD Connection Broker) manages incoming remote desktop connections to the servers in Remote Desktop Session Host (RD Session Host) server farms, known as collections. RD Connection Broker handles connections to collections of full desktops and to collections of RemoteApps. For new connections, RD Connection Broker can balance the load across the servers in the collection. For a session that was disconnected, RD Connection Broker reconnects the user to the correct RD Session Host server and the disconnected session, which already exists in the RD Session Host farm.

To support single sign-on and application publishing, matching digital certificates must be installed on the RD Connection broker server and the client. For development and testing purposes, this can be a self-generated and self-signed certificate. For a released service, the digital certificate must be obtained from a trusted certification authority. The name of the certificate must be the internal Fully Qualified Domain Name (FQDN) of the RD Connection Broker virtual machine.

The Windows Server 2012 R2 RD Connection Broker can be installed on the same virtual machine as AD DS to reduce cost. To provide a highly available service and to scale-out to larger numbers of users, additional RD Connection Broker virtual machines in the same availability set can be added for create an RD Connection Broker cluster. To create an RD Connection Broker cluster, a Microsoft SQL Server AlwaysOn Availability Group must also be deployed in virtual machines.

**Additional information:**

[Overview of Remote Desktop Connection Broker (RD Connection Broker)](http://technet.microsoft.com/en-us/library/cc772245.aspx)

[RD Connection Broker Performance and Scalability](http://download.microsoft.com/download/C/8/D/C8DB9F38-660E-4C2A-8312-04EDB5114B9E/RD%20Connection%20Broker%20Performance.docx)

[RD Connection Broker High Availability in Windows Server 2012](http://blogs.msdn.com/b/rds/archive/2012/06/27/rd-connection-broker-high-availability-in-windows-server-2012.aspx)

[Create a SQL AlwaysOn Availability Group in Microsoft Azure End-to-End](http://blogs.msdn.com/b/sqlalwayson/archive/2013/01/23/test-lab-create-an-alwayson-availability-group-in-windows-azure-end-to-end.aspx)

## RD License

Each tenant’s environment includes an activated Remote Desktop License server to allow users to connect to the Remote Desktop Session Host (RD Session Host) servers that host the tenant’s desktops and applications. For hosted environments, the licensing server is configured in “per user” mode.

The service provider must acquire the proper number of RDS Subscriber Access Licenses (SALs) based on the number of unique (not concurrent) users authorized to log on to the service each month. Service providers who offer hosted desktops must purchase Microsoft Azure Infrastructure Services directly and the SALs through the Microsoft Service Provider Licensing Agreement (SPLA) program.  End customers who purchase a hosted desktop solution from a service provider must purchase the complete hosted solution (Azure and RDS) from the service provider.

For small tenants, the cost can be reduced by combining the AD DS, the file server, and RD Licensing components on a virtual machine in the tenant’s environment. To provide a higher availability service, two RD License server virtual machines can be deployed in the same availability set. All the RD servers in the tenant’s environment are associated with both RD license servers to ensure that users will be able to connect to new sessions even if one of the license servers is unavailable.

**Additional information:**

[Overview of Remote Desktop Licensing](http://technet.microsoft.com/en-us/library/cc725933.aspx)

[Deploying Remote Desktop Licensing Step-by-Step Guide](http://technet.microsoft.com/en-us/library/dd983943(WS.10).aspx)

[Managing RDS Licensing Using PowerShell on Windows Server 2012 R2](http://social.technet.microsoft.com/wiki/contents/articles/13293.managing-rds-licensing-using-powershell-on-windows-server-2012.aspx)

[Generate Per User CAL Report](http://gallery.technet.microsoft.com/ScriptCenter/9739eaee-fb8a-4cb8-8456-7f138d175934/)

[Microsoft Volume Licensing: Licensing Options for Service Providers](http://www.microsoft.com/licensing/licensing-options/spla-program.aspx#tab=1)

## Remote Desktop Session Host

The Remote Desktop Session Host (RD Session Host) component provides a tenant’s users with session-based desktops and RemoteApp programs. The desktops and applications can be accessed over the Internet from any device running a capable remote desktop connection client. For more information, see the [Client section](#_Clients) later in this document.

The remote desktops and applications can be organized into collections of one or more RD Session Host servers. The collections can be customized for specific groups of users within each tenant. For example, a collection could be created so that a tenant’s accounting group can access accounting applications but the engineering group cannot access them.

The applications can be installed directly on the RD Session host servers. For larger deployments, streaming applications to the RD Session Host from an App-V server is recommended to reduce the maintenance costs.

To provide higher availability of the collections and to increase scale to support more users or applications that use more computer resources, each collection can be expanded by adding RD Session Host server virtual machines to a collection farm with each RDSH virtual machine within a collection assigned to same availability set.

In most cases, the R Session Host servers are shared by multiple users simultaneously. This is the most efficient way to utilize the Azure resources for a desktop hosting solution. In this configuration, users must sign in to collections by using non-administrative accounts. In certain cases, some users want full administrative access to their remote desktop. This can be achieved by creating a collection with 1 RDSH virtual machine for each user who wants administrative access.

When the user signs in to a desktop collection, by default, the user sees a server desktop. Administrators can install the Desktop Experience feature and customizing the default profile to provide a more client-like experience for the end user. We strongly recommend leveraging the Desktop Experience feature as part of a desktop hosting solution. Additional customizations can be made by creating and uploading a virtual hard disk that contains the Windows Server operating system to be used as a template for creating RD Session Host virtual machines.

### User Profile Disks

User profile disks allow users to save personal settings and files when they are signed in to a session on an RD Session Host server in a collection, and then have access to the same settings and files when signing in to a different RD Session Host server in the collection. When the user first signs in, a user profile disk is created on the tenant’s file server, and that disk is mounted to the RD Session Host server to which the user is connected. For each subsequent sign-in, the user profile disk is mounted to the appropriate RD Session host server, and with each sign-out, it is un-mounted. The contents of the profile disk can only be accessed by that user.

**Additional information:**

[Remote Desktop Services Overview](http://technet.microsoft.com/en-us/library/hh831447.aspx)

[Windows Server 2012 R2: What’s New in Remote Desktop Services](http://technet.microsoft.com/en-us/library/hh831527.aspx)?

[Using PowerShell to install, configure and maintain RDS in Windows Server 2012 R2](http://social.technet.microsoft.com/wiki/contents/articles/12835.using-powershell-to-install-configure-and-maintain-rds-in-windows-server-2012.aspx)

[Easier User Data Management with User Profile Disks in Windows Server 2012 R2](http://blogs.msdn.com/b/rds/archive/2012/11/13/easier-user-data-management-with-user-profile-disks-in-windows-server-2012.aspx)

[Desktop Experience Overview](http://technet.microsoft.com/en-us/library/cc772567.aspx)

[Install Desktop Experience on an RD Session Host Server](http://technet.microsoft.com/en-us/library/cc742809.aspx)

[Getting Started With App-V 5.0](http://technet.microsoft.com/en-us/library/jj713418.aspx)

[Microsoft Azure: Creating and Uploading a Virtual Hard Disk that Contains the Windows Server Operating System](http://www.windowsazure.com/en-us/manage/windows/common-tasks/upload-a-vhd/)

## File Server

The file server provides shared folders by using the Server Message Block (SMB) 3.0 protocol. The shared folders are used to create and store user profile disk files (.vhdx), to backup data, and to allow users a place to share data with other users in the tenant’s Cloud Service.

The VM used to deploy the file server must have an Azure data disk attached and configured with shared folders. Azure data disks use write-through caching which guarantees that writes to the disk persist across restarts of the VM.

For small tenants, the cost can be reduced by combining the AD DS, the file server, and RD Licensing components on a single virtual machine in the tenant’s environment.

**Additional information**

[File and Storage Services Overview](http://technet.microsoft.com/en-us/library/hh831487.aspx)

[How to Attach a Data Disk to a Virtual Machine](http://www.windowsazure.com/en-us/manage/windows/how-to-guides/attach-a-disk/)

# Azure Infrastructure Services

## Azure Management Portal

After the provider creates an Azure subscription, the Azure Management Portal can be used to manually create each tenant’s environment. This process can also be automated using PowerShell Scripts.

**Additional information:**

[Microsoft Azure](http://www.windowsazure.com/en-us/)

[Microsoft Azure Infrastructure Services](http://www.windowsazure.com/en-us/solutions/infrastructure/)

## Azure Load Balancer

The tenant’s components run on virtual machines that communicate with each other on an isolated network. During the deployment process, these virtual machines can be accessed externally through the Azure Load Balancer using Remote Desktop Protocol endpoints or Remote PowerShell endpoint. Once a deployment is complete, these endpoints will typically be deleted to reduce the attack surface area. The only endpoints will be the HTTPS and UDP endpoints created for the VM running the RD Web and RD Gateway components. This allows clients on the Internet to connect to sessions running in the tenant’s desktop hosting service. If a user opens an application that connects to the Internet, such as Internet Explorer Web browser, the connections will be passed through the Azure Load Balancer.

When a RD Gateway farm has been implemented in a multiple VMs for high availability and scale out, the HTTPS and UDP endpoints must be configured in a load-balanced set and the Azure load balancer must be configured with client IP affinity so that all HTTPS connections from a client connect through the same RD Gateway virtual machine.

**Additional information:**

[Microsoft Azure: Load Balancing Virtual Machines](http://www.windowsazure.com/en-us/manage/windows/common-tasks/how-to-load-balance-virtual-machines/)

## Azure Virtual Private Networking (VPN)

Site-to-site virtual private networking (VPN) connections between the tenant’s on-premises network and the tenant’s network in Microsoft Azure can be supported using the Azure VPN service and Azure virtual networks. This allows the hosted desktops to access the on-premises resources.

**Additional information:**

[Microsoft Azure Virtual Network Overview](http://msdn.microsoft.com/library/windowsazure/jj156007.aspx)

[Microsoft Azure: Virtual Network](http://www.windowsazure.com/en-us/documentation/services/virtual-network/)

## Security Considerations

This Azure Desktop Hosting Reference Architecture Guide is designed to provide a highly secure and isolated environment for each tenant. The security of the system also depends on safeguards taken by the provider during deployment and operation of the hosted service. Following is a list of some mitigations that the provider must consider to help ensure the security of a desktop hosting solution based on this reference architecture.

* All administrative passwords must be strong, and ideally randomly generated, changed frequently, and saved in secure central location that is only accessible by a select few provider administrators.
* Care must be taken when replicating the tenant environment for new tenants to avoid using the same or weak administrative passwords.
* The RD Web Access site URL, name, and certificates must be unique and recognizable to each tenant to mitigate spoofing attacks.
* During the normal operation of the desktop hosting service, all endpoints should be deleted for all VMs except the for the HTTPS and UDP endpoints for the RD Web and RD Gateway VM that allow users to securely connect to the tenant’s desktop hosting cloud service. Endpoints may be temporarily added to allow management tasks to be performed but should always be deleted

**Additional information:**

[Security and Protection Overview](http://technet.microsoft.com/en-us/library/hh831778.aspx)

[Strong Passwords](file:///C:\Users\v-diree\AppData\Local\Microsoft\Windows\Temporary%20Internet%20Files\Content.Outlook\KIJA96HO\Strong%20passwords)

[Security Best Practices for IIS 8](http://technet.microsoft.com/en-us/library/jj635855.aspx)

[Secure Windows Server 2012 R2](http://technet.microsoft.com/en-us/library/hh831360.aspx)

## Design Considerations

Microsoft Azure Infrastructure Services have a number of constraints that must be considered when designing a multitenant desktop hosting service. The following is a list of some constraints that the provider must consider to achieve a functional and cost effective desktop hosting solution based on this reference architecture.

* An Azure subscription has a maximum number of virtual networks, VM cores, and Cloud Services that can be used. Consequently, providers may need to create multiple subscriptions.
* An Azure Cloud Service has a maximum number of VMs that can be used. Consequently, providers may need to create multiple Cloud Services for larger tenants.
* The cost of Azure deployments are based partially on the number of VMs and the size of the VMs. Consequently, the provider should optimize the number and size of the VMs for each tenant to provide a functional and highly secure Desktop Hosting environment at the lowest cost.
* The physical computer resources in the Azure data center are virtualized by using Hyper-V. The Hyper-V hosts are not configured in host clusters so the availability of the virtual machines is dependent on the availability of the individual servers used in the Azure infrastructure. To provide higher availability, multiple instances of each role service VM can be created in an availability set and then guest clustering can be implemented within the VMs.
* In a typical storage configuration, a service provider will have a single storage account with multiple containers (e.g. one for each tenant), and multiple disks within each container. However, there are constraints on the total storage and performance that can be achieved for a single storage account. For service providers that support large numbers of tenants or tenants with requirements for large storage capacity and/or high performance, the service provider may need to create multiple storage accounts.

**Additional information:**

[Virtual Machine and Cloud Service Sizes for Microsoft Azure](http://msdn.microsoft.com/library/dn197896.aspx)

[Microsoft Azure Virtual Machine Pricing Details](http://www.windowsazure.com/en-us/pricing/details/virtual-machines/)

[Hyper-V Overview](http://technet.microsoft.com/library/hh831531)

[Manage the Availability of Virtual Machines](http://www.windowsazure.com/en-us/manage/windows/common-tasks/manage-vm-availability/)

[Microsoft Azure Storage Abstractions and their Scalability Targets](http://blogs.msdn.com/b/windowsazurestorage/archive/2010/05/10/windows-azure-storage-abstractions-and-their-scalability-targets.aspx)

# Tenant On-Premises Components

## Clients

To access the hosted desktops and applications, the tenant’s users must use Remote Desktop Connection (RDC) clients that support Remote Desktop Protocol (RDP) 7.1 or higher. In particular, the client must support Remote Desktop Gateway and Remote Desktop Connection Broker. To deliver applications to the local desktop, the client must also support the RemoteApp feature. To achieve highest gateway scale, the client must support the pure HTTP transport connections to RD Gateway. Examples include the RDC clients that are available in computers running Windows 7 with SP1 with latest updates or Windows 8.1 and the Microsoft Remote Desktop apps for non-Windows operating systems.

**Additional information:**

[RemoteFX Enabled Devices](http://social.technet.microsoft.com/wiki/contents/articles/14534.remotefx-enabled-devices.aspx)

[What’s new in Windows Server 2012 R2 Remote Desktop Gateway](http://blogs.msdn.com/b/rds/archive/2013/03/14/what-s-new-in-windows-server-2012-remote-desktop-gateway.aspx#transport)

[Remote Desktop app for Windows in the Windows Store](http://apps.microsoft.com/windows/en-us/app/remote-desktop/051f560e-5e9b-4dad-8b2e-fa5e0b05a480)

[Microsoft Remote Desktop - Android Apps on Google Play](https://play.google.com/store/apps/details?id=com.microsoft.rdc.android)

[Mac App Store - Microsoft Remote Desktop](https://itunes.apple.com/us/app/microsoft-remote-desktop/id715768417?mt=12)

[Microsoft Remote Desktop on the App Store on iTunes](https://itunes.apple.com/us/app/microsoft-remote-desktop/id714464092?mt=8)

## Active Directory Domain Services

Some larger and more sophisticated tenants may choose to host an Active Directory Domain Services (AD DS) server on their premises. In this case, the AD DS server in the Azure Cloud Service will typically be a replica of AD DS server that is on the tenant’s premises. This is supported by creating a virtual network in the tenant’s Cloud Service and using the Azure VPN to create a site-to-site connection from the tenant’s on-premises network to the tenant’s virtual network in the Azure data center.

**Additional information:**

[Microsoft Azure Virtual Network Overview](http://msdn.microsoft.com/library/windowsazure/jj156007.aspx)

[Microsoft Azure: Virtual Network](http://www.windowsazure.com/en-us/documentation/services/virtual-network/)