

Microsoft Azure: Desktop Hosting Deployment Guide

Basic Desktop Hosting Implementation 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 Prerequisites 6](#_Toc400095528)

[2 Create tenant’s networking environment 6](#_Toc400095529)

[3 Create tenant’s virtual machines 6](#_Toc400095530)

[4 Configure the DNS address for the virtual network 7](#_Toc400095531)

[5 Deploy AD DS and DNS roles 7](#_Toc400095532)

[6 Prepare virtual machines for Remote Desktop Services deployment 9](#_Toc400095533)

[7 Create Remote Desktop Services deployment 9](#_Toc400095534)

[8 Connect to deployment from the client computer over the Internet 13](#_Toc400095535)

[9 Secure the Deployment 13](#_Toc400095536)

This document provides guidance for deploying a basic desktop hosting solution based on the [Microsoft Azure Desktop Hosting Reference Architecture Guide](http://msdn.microsoft.com/en-us/library/windowsazure/dn451351.aspx). This document is intended to provide a starting point for implementing a Desktop Hosting service on Microsoft Azure virtual machines. A production environment will need additional deployment steps to provide advanced features such as high availability, customized desktop experience, RemoteApp collections, etc.

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:

* Deployment guidance for a basic desktop hosting service based on Remote Desktop Services (RDS).   
  Advanced deployment guidance for desktop hosting is not covered in this document.
* Session-based desktops that use Windows Server Remote Desktop Session Host (RDSH).   
  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 or Windows Server 2012 and Microsoft Azure infrastructure Services.
* Basic availability provided by Microsoft Azure Infrastructure Services.  
  Additional levels of high availability can be provided by guest clustering, but a general high availability solution is out-of-scope for this document.
* 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.
* Standalone desktop hosting cloud service that does not have Virtual Private Network links to an on premises network.  
  This can be added optionally but is out-of-scope for this document.
* Self-signed certificates

For a production deployment, certificates should be obtained from a trusted root certificate authority and alternative deployment procedures used to install these certificates on the servers and client devices.

After reading this document, the reader should understand:

* How to deploy a basic desktop hosting service in Microsoft Azure virtual machines using Windows Server 2012 R2 and Windows Server 2012.

There are multiple ways to deploy a desktop hosting solution. Throughout the document, specific examples are given that can be used as a starting point for a basic deployment. These examples are identified with the *e.g.* notation.

# Prerequisites

This document assumes that the reader has already performed the following tasks.

1. Create a Microsoft Azure subscription. See [Microsoft Azure Free Trial](http://www.windowsazure.com/en-us/pricing/free-trial/).
2. Launch and sign in to the [Microsoft Azure Management Portal](https://manage.windowsazure.com/).
3. Create a storage account. See [How to Create a Storage Account](http://www.windowsazure.com/en-us/manage/services/storage/how-to-create-a-storage-account/).

# Create tenant’s networking environment

The following steps create the tenant’s networking environment within Microsoft Azure.

1. Create a Virtual Network
   1. In the Microsoft Azure Management Portal select **NETWORKS, +NEW, VIRTUAL NETWORK,** and **CUSTOM CREATE**.
   2. Enter a **NAME** for the tenant’s virtual network, e.g. Contoso-VNET
   3. Under **LOCATION** select a location that is near the tenant’s users, e.g. **West US**
   4. Skip the **DNS servers** setting for now.
   5. Configure the **ADDRESS SPACE** and a **SUBNET**, e.g. 192.168.0.0/26 (64) and subnet-1 192.168.0.0/26 (64).
2. Create a Cloud Service
   1. In the Microsoft Azure Management Portal select **CLOUD SERVICES**, **+NEW, CLOUD SERVICE,** and **CUSTOM CREATE**
   2. Enter a **URL**, e.g. Contoso-CS1
   3. Under **REGION OR AFFINITY GROUP** select the region used for the virtual network.

# Create tenant’s virtual machines

The following steps create the virtual machines in the tenant’s environment that will be used to run the Windows Server 2012 R2 roles, services, and features required for a desktop hosting deployment. For this example of a basic deployment, the minimum of 3 virtual machines will be created. One virtual machine will host the Active Directory Services (AD DS) role, DNS role, the Remote Desktop Connection Broker and License Server role services, and a file share for the deployment. A second virtual machine will host the Remote Desktop Gateway and Web Access role services. A third virtual machine host the Remote Desktop Session Host role service. If using Windows Server 2012, the RD Connection Broker role service cannot be installed with AD DS role so an additional virtual machine must be created to host the RD Connection Broker role service. For larger deployments, the various role services may be installed in individual virtual machines to allow better scaling.

1. Create virtual machine to host the Active Directory Domain Services (AD DS)
   1. In the Microsoft Azure Management Portal select **VIRTUAL MACHINES**, **+NEW, COMPUTE, VIRTUAL MACHINE,** and **FROM GALLERY**
   2. Select Platform Images, **Windows Server 2012 R2 Datacenter**
   3. Select the most recent **VERSION RELEASE DATE**
   4. Enter a **VIRTUAL MACHINE NAME**, e.g. Contoso-AdCb1
   5. Select the **SIZE,** e.g. **Small**
   6. Enter a **NEW USER NAME** and a **NEW PASSWORD** to be added to the local administrators group
   7. Select the **CLOUD SERVICE** created above
   8. Accept the **REGION/AFFINITY GROUP/VIRTUAL NETWORK** for this Cloud Service.
   9. Select the **STORAGE ACCOUNT** created above.
   10. Set **AVAILABILITY SET** to **(None).** (Note: This can be changed later if a replica AD DS server is added for high availability.)
   11. Accept the default **ENDPOINTS**, i.e. Remote Desktop and PowerShell.
2. Attach 2 Azure data disks to AD DS virtual machine for the shares and AD database.
   1. In the Microsoft Azure Management Portal select **VIRTUAL MACHINES**
   2. Select the VM created above for AD DS
   3. Select **DASHBOARD, ATTACH** and **Attach empty disk**
   4. Accept the defaults for **VIRTUAL MACHINE NAME**, **STORAGE LOCATION**, and **FILE NAME**
   5. Enter the **SIZE (GB)** to be large enough to hold the NTDS databases, logs, and SYSVOL, e.g. 32GB (For more information, see [Guidelines for Deploying Windows Server Active Directory on Microsoft Azure Virtual Machines](http://msdn.microsoft.com/en-us/library/windowsazure/jj156090.aspx).)
   6. Set the **HOST CACHE PREFERENCE** to **NONE**
   7. Repeat steps c. through f. and enter a size large enough to hold network shares for the tenant’s environment, including AD backups, user disks, etc., e.g. 140GB
3. Repeat step 1. for the other two virtual machines entering appropriate names for each, e.g. Contoso-WebGw1 and Contoso-RDSH1

# Configure the DNS address for the virtual network

1. Get IP address of AD DS virtual machine
   1. Open and sign-in to the Microsoft Azure Management Portal
   2. Select **VIRTUAL MACHINES,** the AD DS virtual machine, and **DASHBOARD**
   3. Scroll down and copy the **INTERNAL IP ADDRESS**
2. Set the DNS server name and address for the virtual network
   1. Select **NETWORKS,** the virtual network for this tenant**,** and **CONFIGURE**
   2. Paste the IP address of the DNS server VM into the IP ADDRESS field, e.g. 192.168.0.4
   3. Enter the name of the DNS server, e.g. Contoso-AdCb1
   4. Select **SAVE**
   5. Wait for the operation to complete successfully
3. Restart the virtual machines
   1. Select **VIRTUAL MACHINES,** the AD DS virtual machine**,** and **DASHBOARD**,and **RESTART**
   2. Repeat step a for the other two virtual machines
   3. Wait for the operation to complete successfully.

# Deploy AD DS and DNS roles

This section provides the steps to create a stand-alone domain controller (DC) for Active Directory Domain Services (AD DS). Alternatively, virtual private networking (VPN) could be configured to connect the tenant’s Azure networking environment to the tenant’s on-premises network. In this alternative configuration, the DC in the Microsoft Azure environment would be configured as a replica of the on-premises DC.

1. Connect to the AD virtual machine using Remote Desktop Connection (RDC) client
   1. In the Microsoft Azure Management Portal select **VIRTUAL MACHINES**
   2. Select the virtual machine created above for AD DS
   3. Select **DASHBOARD, CONNECT,** and **OPEN** to open the RDC client
   4. On the RDC client, select **Connect**, **Use another user account**, and enter the user name and password for the local administrator account created above.
   5. Select **Yes** when warned about the certificate.
2. Enable Remote Management
   1. From **Server Manager,** select **Local Server,** andthe **Remote management** current setting (disabled).
   2. Check the box to **Enable remote management for this server**
   3. Select **OK**
3. Optional: Temporarily set Windows Update to not automatically download and install updates.  
   (This avoids changes and reboots while deploying system.)
   1. From **Server Manager, s**elect **Local Server** and the **Windows Update** current setting
   2. In the **Windows Update** dialog select **Change Settings** and **Check for updates but let me choose whether to download and install them**
4. Initialize the data disks
   1. From **Server Manager,** select **Tools**, **Computer Management**, and **Disk Management**
   2. Initialize disks as Master Boot Record (**MBR**) partition style
   3. Right click the attached disk for the AD DS files and select **New Simple Volume…**
   4. Accept the default size, driver letter, etc.
   5. Enter an appropriate **Volume label**, e.g. AD-DB-LOGS-SYSVOL
   6. Repeat steps c. – e. on the attached disk for shared folders entering an appropriate **Volume label**, e.g. Shares
5. Install AD DS DNS Server and associated Features
   1. From **Server Manager,** select **Manage** and **Add Roles and Features**
   2. Page through the wizard accepting defaults until the Server Roles page
   3. Check **Active Directory Domain Services**, **DNS Server**, and add the associated Features
   4. Select **Continue** to ignore a warning about no static IP addresses.
   5. Page to the end of the wizard and select **Install** (Note: A restart is not required.)
6. Promote the virtual machine to a domain controller
   1. From **Server Manager,** select the notification warning icon and **Promote this server to a domain controller**
   2. Select **Add a new forest** and enter the **Root domain name**, e.g. Contoso.com
   3. Enter a **Restore Mode** **Password**
   4. Enter **The** **NetBIOS domain name**, e.g. Contoso
   5. Change the location of the **Database folder**, **Log files folder**, and **SYSVOL folder** to the attached data disk by creating new folders, e.g. F:\NTDS, F:\NTDS, and F:\SYSVOL, respectively.
   6. Select **Install**
   7. The server will restart to complete the promotion to a domain controller.
7. Create domain users and administrators
   1. Connect to the AD DS virtual machine using RDC client (step 1 above)
   2. From Server Manager, select **Tools** and **Active Directory Users and Computers**
   3. Select the newly created domain, e.g. Contoso.com
   4. Select **Action**, **New**, and **User**
   5. Create standard domain users and domain administrators
   6. Select the domain administrator account, **Action**, **Add to a group…** , and add the account to the **Domain Admins** group.
8. Create a file shares for the user disks and certificates
   1. Launch **File Explorer**
   2. Select **This PC** (or **Computer** on Windows Server 2012) and open the disk that was added for file shares, e.g. Shares (F:)
   3. Select **Home** and **New Folder**
   4. Enter a name for the user disks folder, e.g. UserDisks
   5. Right click the new folder and select **Properties**, **Sharing**, and **Advanced Sharing…**
   6. Check the **Share this folder** box and select **Permissions**
   7. In the **Permissions** dialog select **Everyone, Remove, Add…, e**nter **administrators,** andselect **OK**
   8. Check the **Allow Full Control** check box and select **OK, OK,** and **Close**
   9. Repeat steps c. – h. to create a shared folder for certificates to be shared, e.g. Certificates.

# Prepare virtual machines for Remote Desktop Services deployment

1. Connect to the virtual machine using Remote Desktop Connection (RDC) client
   1. In the Microsoft Azure Management Portal select **VIRTUAL MACHINES**
   2. Select the RD RDSH virtual machine, e.g. Contoso-RDSH1
   3. Select **DASHBOARD, CONNECT,** and **OPEN** to open the Remote Desktop Connect client
   4. On the RDC client, select **Connect**, **Use another user account**, and enter the user name and password for the local administrator account.
   5. Select **Yes** when warned about the certificate.
2. Enable Remote Management
   1. From **Server Manager,** select **Local Server** and the **Remote management** current setting
   2. In the **Configure Remote Management** dialog, check the box labeled **Enable remote management for this server from other computers.**
   3. Select **OK**
3. Optional: Temporarily set Windows Update to not automatically download and install updates to avoid changes and reboots while deploying the system.
   1. From **Server Manager**, select **Local Server** andthe **Windows Update** current setting
   2. In the **Windows Update** dialog, select **Change Settings** and **Check for updates but let me choose whether to download and install them**
   3. Select **OK**
4. Add the virtual machine to the domain
   1. From **Server Manager,** select **Local Server and** the **Workgroup** current setting
   2. In the **System Properties** dialog, select **Change…** , **Domain**, and enter the domain name, e.g. Contoso.com
   3. Enter domain administrator credentials
   4. Restart the computer
5. Repeat steps 1 through 4 for the RD Web and GW virtual machine, e.g. Contoso-WebGw1

# Create Remote Desktop Services deployment

Note: The virtual machine created to run the Remote Desktop Connection Broker (RD Connection Broker) role service will also run the Remote Desktop Management Services (RDMS). This virtual machine, referred to as the RDMS server, will be used to deploy and manage the rest of the servers in the tenant’s hosted desktop environment.

1. Connect to the RDMS server using Remote Desktop Connection (RDC) client
   1. In the Microsoft Azure Management Portal select **VIRTUAL MACHINES**
   2. Select the RDMS server virtual machine, e.g. Contoso-AdCb1
   3. Select **DASHBOARD, CONNECT,** and **OPEN** to open the Remote Desktop Connect client
   4. On the RDC client, select **Connect**, **Use another user account**, and enter the user name and password for a domain administrator account.
   5. Select **Yes** when warned about the certificate.
2. Add all servers to Server Manager
   1. From **Server Manager,** select **Manage** and **Add Servers**
   2. In the **Add Servers** dialog select **Find Now**
   3. Select all the servers and **OK**
3. Create a session-based deployment
   1. From **Server Manager,** select **Manage** and **Add Roles and Features**
   2. In the **Add Roles and Features** wizard select **Remote Desktop Services Installation, Standard Deployment,** and **Session-based desktop deployment**
   3. Select the appropriate virtual machines for the **RD Connection Broker server**, **RD Web Access server**, and **RD Session Host server**, e.g. Contoso-AdCb1, Contoso-WebGw1, and Contoso-RDSH1, respectively.
   4. Check the box labeled **Restart the destination server automatically if required** and select **Deploy**
   5. Wait for the deployment to complete successfully
4. Add RD License Server
   1. From **Server Manager,** select **Remote Desktop Services**, **Overview,** and **+ RD Licensing**
   2. In the **Add RD Licensing Servers** wizard, select the virtual machine that the RD license server is installed on, e.g. Contoso-AdCb1
   3. Select **Next** and **Add**
   4. Wait for the RD License server to be added successfully.
5. Activate the RD License Server and add to the License Servers group
   1. From **Server Manager,** select **Tools**, **Terminal Services**, and **Remote Desktop Licensing Manager**
   2. In **RD Licensing Manager**, select the server name, **Action** and **Activate Server**
   3. Page through the **Activate Server Wizard** accepting defaults until the Company information page and enter your **Company Information**.
   4. Page through the remaining pages accepting defaults until the final page then uncheck the **Start Install Licenses Wizard now** box and select **Finish**.
   5. Select **Review, Add to Group,** and **Register as SCP**
6. Add RD Gateway server and certificate name
   1. From **Server Manager, s**elect **Remote Desktop Services**, **Overview,** and **+ RD Gateway**
   2. In the **Add RD Gateway Servers** wizard, select the virtual machine with the RD Gateway server installed on it, e.g. Contoso-WebGw1
   3. Enter the **SSL certificate name** for the RD Gateway server using the external fully qualified DNS Name (FQDN) of the RD Gateway server. In Azure, this will be of the form <cloudservice>.cloudapp.net, e.g. Contoso-CS1.cloudapp.net.
   4. Select **Next** and **Add**
   5. Wait for the RD Gateway server to be added successfully.
7. Create and install self-signed certificates for the RD Gateway and RD Connection Broker servers

Note: This procedure will be different if using certificates from a trusted certificate authority.

* 1. From **Server Manager,** select **Remote Desktop Services**, **Overview, Tasks** and **Edit Deployment Properties**
  2. In the **Deployment Properties** dialog and expand **Certificates**
  3. Scroll down to the table and select **RD Gateway** and **Create new certificate…**
  4. In the **Create New Certificate** dialog, enter the **Certificate name** using the external FQDN of the RD Gateway server, e.g. Contoso-CS1.cloudapp.net, and a **Password**.
  5. Check the box labeled **Store this certificate and** select **Browse …,**
  6. In the **Save As** dialog**,** navigate to the sharedfolder for certificates created above, e.g. \\Contoso-AdCb1\Certificates
  7. Enter a **File name**, e.g. ContosoRdGwCert
  8. Select **Save**.
  9. Check the box labeled **Allow the certificate to be added to the Trusted Root Certificate Authorities certificate store on the destination computers**.
  10. Select **OK**
  11. In the **Deployment Properties** dialog select **Apply**.
  12. Wait for the certificate to be successfully applied to the RD Gateway server.
  13. Select **RD Web Access** and **Select existing certificate…**
  14. In the **Select Existing Certificate** dialog, select **Browse…**
  15. In the **Open** dialog, select the certificate created for the RD Gateway server, e.g. ContosoRdGwCert, and **Open**.
  16. In the **Select Existing Certificate** dialog, enter the **Password**, check the box labeled **Allow the certificate to be added to the Trusted Root Certificate store on the destination computers,** andselect **OK**
  17. In the **Deployment Properties** dialog, select **Apply**
  18. Wait for the certificate to be successfully applied to the RD Web Access server.
  19. Repeat steps c. - r. for the **RD Connection Broker – Enable Single Sign On** and **RD Connection Broker - Publishing** services using the internal FQDN of the RD Connection Broker server for the new certificate’s name, e.g. Contoso-AdCb1.Contoso.com

1. Export self-signed public certificates and copy to a client computer

Note: This procedure is not required if using certificates from a trusted certificate authority.

* 1. Launch certlm.msc
  2. In the left-hand pane, expand **Personal** and select **Certificates**
  3. In the right-hand pane right click the RD Connection Broker certificate intended for **Client Authentication**, e.g. Contoso-AdCb1.Contoso.com
  4. Select **All Tasks >** and **Export …**
  5. In the **Certificate Export Wizard** accept defaults until the **File to Export** page.
  6. Select **Browse…**
  7. In the **Save As** dialog, navigate to the sharedfolder for certificates created above, e.g. \\Contoso-AdCb1\Certificates
  8. Enter a **File name**, e.g. ContosoCbClientCert
  9. Select **Save**, **Next,** and **Finish**
  10. Repeat steps c. through i. for the RD Gateway and Web certificate, e.g. Contoso-CS1.cloudapp.net, giving the exported certificate an appropriate file name, e.g. ContosoWebGwClientCert
  11. Open **File Explorer** and navigate to the folder where the certificates were stored, e.g. \\Contoso-AdCb1\Certificates
  12. Select the two exported client certificates, right click on them, and select Copy
  13. On the local client computer, launch **File Explorer**, navigate to an appropriate folder, right click and select **Paste** to copy the certificates to the client computer’s hard drive.

1. Configure the RD Gateway and RD Licensing deployment properties
   1. From **Server Manager,** select **Remote Desktop Services**, **Overview, Tasks** and **Edit Deployment Properties**
   2. In the **Deployment Properties** dialog and expand **RD Gateway** and uncheck the box labeled **Bypass RD Gateway server for local addresses**
   3. Expand **RD licensing** and select **Per User**
   4. Select **OK**
2. Create a session collection
   1. From **Server Manager,** select **Remote Desktop Services**, **Collections, Tasks,** and **Create Session Collection**
   2. In the **Create Collection** wizard, enter a **Collection Name**, e.g. ContosoDesktop, select an **RD Session Host Server**, e.g. Contoso-RDSH1, accept the default **User Groups,** e.g. Contoso\Domain Users, and enter the Universal Naming Convention (UNC) **Path** to the user profile disks created above**,** e.g. \\Contoso-AdCb1\UserDisks**,** and a **Maximum size,** and **Create.**
   3. Wait for the collection to be created successfully.
3. Install Desktop Experience and set the audio service to start automatically on the RDSH server
   1. From **Server Manager,** select **All Servers**, right click the RDSH server, and select **Computer Management**
   2. In the **Computer Management** window, expand **Services and Applications**, and select **Services**
   3. Scroll down, right click **Windows Audio**, and select **Properties**
   4. In the **Windows Audio Properties** dialog, set the **Startup type**: to **Automatic,** and select **OK**
   5. In **Server Manager**, right click the RDSH server, and select **Add Roles and Features**
   6. In the **Add Roles and Features Wizard**, click through accepting defaults until reaching the **Features** page
   7. Scroll down, expand the **User Interfaces and Infrastructure** feature, select **Desktop Experience**, **Add features**, **Next**, **Restart the destination server automatically if required**, and **Install**.
   8. Wait for the Feature to install successfully and the RDSH server to restart.
4. Add the server running AD DS and RD Connection Broker to the RD Gateway server’s Resource Authorization Policies (RAP)  
   Note: This step is only required if the RD Connection Broker role service has been installed on the same server as AD DS role.
   1. From **Server Manager** on the RDMS server, select **All Servers**, right click the RD Gateway server, and select **Remote Desktop Connection**
   2. Logon to the RD Gateway server using a domain admin account
   3. From **Server Manager** on the RD Gateway server, select **Tools**, **Terminal Services**, and **RD Gateway Manager**
   4. In the RD Gateway Manager’s left pane, expand the **Local** computer (e.g. Contoso-WebGw1) and expand **Policies**
   5. Right click **Resource Authorization Policies,** select **Create New Policy,** and **Custom**
   6. In the **New RD RAP** dialog**,** enter a **Policy name**,e.g. AllowAdCbConnections
   7. Select the **User Groups** tab and **Add…**
   8. In the **Select Group**s dialog, enter **Domain Users** and select **OK**
   9. In the **New RD RAP** dialog, select the **Network Resources** tab, the **Select an existing RD Gateway-managed group or create a new one** radio button, and **Browse…**
   10. In the **Select a RD Gateway-managed computer group** dialog, select **Create New Group…**
   11. In the **New RD Gateway-Managed Computer Group** dialog, enter a group **Name,** e.g. AdCbGroup
   12. Select the **Network resources** tab, enter the fully qualified domain name of the server running RD Connection Broker and AD DS, e.g. Contoso-AdCb1.Contoso.com, and select **Add**, **OK**, **OK**, and **OK**

# Connect to deployment from the client computer over the Internet

1. Add https (443) and UDP (3391) endpoints for RD Web and Gateway virtual machine
   1. In the Microsoft Azure Management Portal, select **VIRTUAL MACHINES**, the virtual machine running RD Web Access and RD Gateway, e.g. Contoso-WebGw1, **ENDPOINTS**, **+ ADD**
   2. In the **ADD ENDPOINT** wizard, select **ADD STANDALONE ENDPOINT**, **HTTPS**, and accept the default ports (**443**).
   3. Repeat step b. and add a **UDP** endpoint with ports set to **3391**.
2. Install the self-signed client certificates on the client computer

This procedure is not required if a certificate has been obtained from a trusted root certificate authority.

* 1. Logon to the client computer with an administrative account, navigate to the folder where the certificates were copied, right click one of the certificate files, and select **Install certificate**.
  2. In the **Certificate Import Wizard,** select **Local Machine, Place all certificates in the following store**, **Browse…, Trusted Root Certification Authorities, OK, Next, Finish,** and **OK.**
  3. Repeat steps a. and b. for the other certificate.

1. Connect to the deployment through RD Web Access and RD Gateway

Note: There are multiple ways to connect from a client computer to the desktop hosting deployment. These are described in the TechNet Wiki article titled [Distribution of Remote Apps and Desktops in Windows Server 2012](http://social.technet.microsoft.com/wiki/contents/articles/14488.distribution-of-remote-apps-and-desktops-in-windows-server-2012.aspx). The steps in this section connect using the RD Web Access site.

* 1. Launch **Internet Explorer**
  2. In the address field, enter the FQDN of the cloud service, e.g. https://Contoso-CS1.cloudapp.net/RDWeb
  3. Sign in with a domain user account, e.g. Contoso\u1
  4. Under **RemoteApp and Desktops** select one of the collections created for this deployment, e.g. ContosoDesktop
  5. Select **Connect**

# Secure the Deployment

1. Delete unused endpoints for the RD Web Access and RD Gateway virtual machine, e.g. Contoso-WebGw1

Hint: If later you choose to recreate these endpoints, use port numbers from the ephemeral port range (49152 to 65535) for the external port numbers.

* 1. In the Microsoft Azure Management Portal, select **VIRTUAL MACHINES**, the RD Web Access and RD Gateway virtual machine (e.g. Contoso-WebGw1), and **ENDPOINTS**
  2. Select an endpoint (except the HTTPS and UDP endpoints) and **DELETE**
  3. Wait for the endpoints to delete successfully.
  4. Repeat steps b. and c. for each endpoint (except the HTTPS and UDP endpoints)

1. Repeat step 1 for each virtual machine in the tenant’s deployment, e.g. Contoso-AdCb1 and Contoso-RDSH1