

Microsoft Azure: Remote Desktop Web Access and Gateway Farm Deployment

Desktop Hosting with Improved Availability and Scale

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 4](#_Toc403402468)

[2 Configure the current RD Web and Gateway virtual machine for high availability and load balancing 4](#_Toc403402469)

[3 Create an additional RD Web and Gateway virtual machine 5](#_Toc403402470)

[4 Prepare virtual machine for RDS deployment 5](#_Toc403402471)

[5 Add RD Web and Gateway server to the RDS deployment 6](#_Toc403402472)

[6 Configure the RD Web and Gateway virtual machines for load balancing 8](#_Toc403402473)

[7 Connect to deployment from the client computer over the Internet 9](#_Toc403402474)

[8 Secure the deployment 9](#_Toc403402475)

This document provides guidance for deploying a Remote Desktop Web Access (RD Web Access) and Remote Desktop Gateway (RD Gateway) farm to improve the availability and scale of a Windows Server 2012 R2 Remote Desktop Services (RDS) deployment in Microsoft Azure Infrastructure Services. This document assumes, as a starting point, a basic desktop hosting deployment based on the [Microsoft Azure Desktop Hosting Reference Architecture Guide](http://msdn.microsoft.com/en-us/library/windowsazure/dn451351.aspx) and the [Microsoft Azure Desktop Hosting Deployment Guide](http://msdn.microsoft.com/en-us/library/windowsazure/dn451351.aspx).

The scope of this document is limited to:

* Deployment guidance for adding a second RD Web Access and RD Gateway virtual machine to a basic desktop hosting deployment.  
  For higher scale, additional virtual machines running RD Web Access and RD Gateway can be added by repeating the steps in this document.

After reading this document, the reader should understand:

* How to deploy a second RD Web Access and RD Gateway virtual machine within a basic desktop hosting deployment in a single Microsoft Azure Cloud Service.

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 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/).
4. Create a basic desktop hosting service deployment in Azure Infrastructure Services. See [Microsoft Azure Desktop Hosting Reference Architecture Guide](http://msdn.microsoft.com/en-us/library/windowsazure/dn451351.aspx) and the [Microsoft Azure Desktop Hosting Deployment Guide](http://msdn.microsoft.com/en-us/library/windowsazure/dn451351.aspx).

# Configure the current RD Web and Gateway virtual machine for high availability and load balancing

1. Create an availability set for the RD Web and Gateway virtual machine
   1. In the Microsoft Azure Management Portal select **VIRTUAL MACHINES**, the RD Web and Gateway virtual machine created in the basic deployment (e.g. Contoso-WebGw1), and **CONFIGURE**
   2. Under the AVAILABILITY SET drop down select **Create an availability set**
   3. Enter a name (e.g. WebGwAvSet) and select **SAVE**
2. Create a load-balanced set for the endpoints
   1. In the Microsoft Azure Management Portal select **VIRTUAL MACHINES**, the RD Web and Gateway virtual machine created in the basic deployment (e.g. Contoso-WebGw1), and **ENDPOINTS**
   2. Select the HTTPS endpoint and **EDIT**
   3. In the **EDIT ENDPOINT** wizard select **CREATE A LOAD-BALANCED SET**
   4. Enter a **LOAD-BALANCED SET NAME** (e.g. WebGwHttpsLbSet) and accept the defaults
   5. Repeat steps b. through d. for the UDP endpoint using an appropriate name for the load balanced set (e.g. WebGwUdpLbSet) and setting the **PROBE PORT** to 443

# Create an additional RD Web and Gateway virtual machine

1. Create a virtual machine to host the RD Web Access and RD Gateway role services
   1. In the Microsoft Azure Management Portal select **VIRTUAL MACHINES**, **+NEW, COMPUTE, VIRTUAL MACHINE,** and **FROM GALLERY**
   2. Select **Windows Server 2012 R2 Datacenter**
   3. Select the most recent **VERSION RELEASE DATE**
   4. Enter a **VIRTUAL MACHINE NAME**, e.g. Contoso-WebGw2
   5. Select the **SIZE,** e.g. **A1**
   6. Enter a **NEW USER NAME** and a **NEW PASSWORD** to be added to the local administrators group
   7. Select the new **CLOUD SERVICE** created in the prerequisites
   8. Accept the **REGION/AFFINITY GROUP/VIRTUAL NETWORK** for this Cloud Service.
   9. Select the **STORAGE ACCOUNT** created above
   10. In the **AVAILABILITY SET** list**,** select the availability set created above (e.g. WebGwAvSet)
   11. Accept the default **ENDPOINTS**, i.e. Remote Desktop and PowerShell.

# Prepare virtual machine for RDS deployment

1. Connect to the new RD Gateway virtual machine using Remote Desktop Connection (RDC) client
   1. In the Microsoft Azure Management Portal select **VIRTUAL MACHINES**
   2. Select the RD Gateway virtual machine, e.g. Contoso-WebGw2
   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.
   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. 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 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**
4. Add the server 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 server

# Add RD Web and Gateway server to the RDS deployment

1. Create a Remote Desktop endpoint for the virtual machine running Remote Desktop Management Services (RDMS). The RDMS virtual machine will typically be the virtual machine running the first instance of RD Connection Broker deployed.

Note: This procedure is not necessary if a Remote Desktop endpoint already exists for the RDMS virtual machine.

* 1. In the Microsoft Azure Management Portal select **VIRTUAL MACHINES**
  2. Select the RDMS server’s virtual machine, e.g. Contoso-AdCb1
  3. Select **DASHBOARD, ENDPOINTS,** and **ADD** to open the **ADD ENDPOINT** wizard
  4. In the **ADD ENDPOINT** wizard, select **ADD A STAND-ALONE ENDPOINT**, set the **NAME** to **Remote Desktop,** andaccept the default values for the **PROTOCOL** and **PORTS**

1. Connect to the RDMS server using Remote Desktop Connection 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 the new RD Web Access and RD Gateway server to Server Manager
   1. From **Server Manager,** select **Manage** and **Add Servers**
   2. In the **Add Servers** dialog select **Find Now**
   3. Select the newly created RD Web Access and RD Gateway server and **OK**
3. Add the new RD Web Access and RD Gateway servers to the deployment
   1. From **Server Manager,** select **Remote Desktop Services**, **Overview, DEPLOYMENT SERVERS, TASKS,** and **Add RD Web Access Servers**
   2. In the **Add RD Web Access Servers** wizard, select the newly created server, e.g. Contoso-WebGw2
   3. Select **Next** and **Add**
   4. Wait for the RD Web Access role service to be installed successfully.
   5. Repeat steps a. through d. but use **Add RD Gateway Servers**
4. Add the RD Gateway servers to a farm
   1. From **Server Manager** on the RDMS server, select **All Servers,** right click one of the RD Gateway servers 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, select the **Local** computer (e.g. Contoso-WebGw1)
   5. In the RD Gateway Manager’s center pane, select **Add RD Gateway Server Farm members**
   6. In the Gateway properties dialog, select the **Server Farm** tab, enter the name of each RD Gateway server, then select **Add** and **Apply**
   7. Repeat steps a. through f. for each RD Gateway server
5. Add the server running AD DS and RD Connection Broker to the new 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 an 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-WebGw2) 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 RD Connection Broker server (e.g. Contoso-AdCb1.Contoso.com), and select **Add**, **OK**, **OK**, and **OK**
6. Add the RD Web Access servers to a farm

The steps below configure the Validation and Decryption Machine Keys to be the same on both RDWeb sites.

* 1. From **Server Manager** on the RDMS server, select **All Servers,** right click one of the RD Web Access servers, and select **Remote Desktop Connection**
  2. Logon to the RD Web Access server using a domain admin account
  3. From **Server Manager** on the RD Web Access server, select **Tools**, **Terminal Services**, and **Internet Information Services (IIS) Manager**
  4. In the IIS Manager’s left pane, expand the local computer (e.g. Contoso-WebGw1), **Sites**, and **Default Web Site** and then select **RDWeb**
  5. In the IIS Manager’s center pane, right click **Machine Key** and select **Open Feature**
  6. On the **Machine Key** page **Actions** pane, select **Generate Keys** and **Apply**
  7. Double click the **Validation Key** field, right click and select **Copy**
  8. Minimize the RD Connection window to this RD Web server
  9. Repeat steps b. through e. for the second RD Web Access server
  10. For the **Validation Key**, uncheck the box **Automatically generate at runtime**, double click the **Validation Key** field, right click, and select **Paste**.
  11. Under **Actions**, select **Apply**
  12. Minimize the RD Connection window to the second RD Web Access server
  13. Maximize the RD Connection window to the first RD Web Access server
  14. Repeat steps g. through k. for the **Decryption Key**
  15. After the **Validation Key** and **Decryption Key** are identical on both RD Web Access servers, sign out of all RD Connection windows to the RD Web Access servers

1. Re-install certificates for the RD Gateway servers
   1. From **Server Manager** on the RDMS server**,** 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 the **RD Gateway Role Service** and **Select existing certificate…**
   4. In the **Select Existing Certificate** dialog, select **Choose a different certificate** and **Browse…**
   5. In the **Open** dialog, navigate to the location of the certificates (e.g. \\Contoso-CB1\Certificates), select the certificate file for the RD Web and Gateway server created during the prerequisites (e.g. ContosoRdGwCert) and select **Open**
   6. Enter the **Password** for the certificate, check the box labeled **Allow the certificate to be added to the Trusted Root Certificate Authorities certificate store on the destination computers**, and select **OK**.
   7. In the **Deployment Properties** dialog select **Apply**.
   8. Wait for the certificate to be successfully applied to the RD Gateway server.
   9. Repeat steps c. through h. for the **RD Web Access Role Service**.

# Configure the RD Web and Gateway virtual machines for load balancing

1. Configure the additional RD Gateway virtual machine’s endpoints
   1. In the Microsoft Azure Management Portal select **VIRTUAL MACHINES**, the name of the RD Gateway server virtual machine added to the original deployment (e.g. Contoso-WebGw2),select **ENDPOINTS,** and **ADD**
   2. In the **ADD ENDPOINT** wizard, select **ADD AN ENDPOINT TO AN EXISTING LOAD-BALANCED SET,** accept the load balanced set created above, and enter the name HTTPS
   3. Repeat steps a. and b. for the UDP endpoint using the load balanced set for the UDP port created above.
2. Configure the Azure Load Balancer to use IP affinity
   1. Install the Microsoft Azure PowerShell Module on your computer (version 0.8.10.1 or later) by running the [Microsoft Web Platform Installer](http://go.microsoft.com/fwlink/p/?linkid=320376&clcid=0x409). Click **Run and Install when prompted.**
   2. Run **the Microsoft Azure PowerShell** command prompt as administrator
   3. Execute the following:

Add-AzureAccount

Set-AzureLoadBalancedEndpoint -ServiceName "Contoso-CS1" -LBSetName "WebGwHttpsLbSet" -Protocol tcp -LocalPort 443 –ProbeProtocolTCP -ProbePort 443 -LoadBalancerDistribution "sourceIP"

Set-AzureLoadBalancedEndpoint -ServiceName "Contoso-CS1" -LBSetName "WebGwUdpLbSet" -Protocol UDP -LocalPort 3391 –ProbeProtocolTCP -ProbePort 443 -LoadBalancerDistribution "sourceIP"

# Connect to deployment from the client computer over the Internet

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

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
  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 new RD Web Access and RD Gateway virtual machine (e.g. Contoso-WebGw2)
   1. In the Microsoft Azure Management Portal, select **VIRTUAL MACHINES**, the newly created virtual machine for this deployment (e.g. Contoso-WebGw2), **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).
2. Repeat step 1 for the RDMS server virtual machine, e.g. Contoso-AdCb1