Step-by-step guide for High Availability Setup of the RDS Gateway Server

Prepared for

Service Providers

Prepared by

Manish Dhall – Cloud Solutions Strategist
Microsoft OCP

People Tech Group (SI Partner)

MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, our provision of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The descriptions of other companies' products in this document, if any, are provided only as a convenience to you. Any such references should not be considered an endorsement or support by Microsoft. Microsoft cannot guarantee their accuracy, and the products may change over time. Also, the descriptions are intended as brief highlights to aid understanding, rather than as thorough coverage. For authoritative descriptions of these products, please consult their respective manufacturers.

Revision and Signoff Sheet

Change Record

Date	Author	Version	Change Reference
March 16, 2018	Manish Dhall	1.0	Initial draft for review/discussion

Reviewers

Name	Version Approved	Position	Date

Table of Contents

Introduction

You can deploy 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 Remote Desktop Services (RDS) deployment.

Prerequisites

1. A VM created for RD Gateway and configured in an Availability Set in Azure.
2. The VM should be configured with RD Gateway and have the Web Access Role.
3. A second VM created in Azure and added to the same Availability Set as in the Step 1.
4. Join the servers to the domain and enable remote management.

Deployment Steps

Step 1: Configure the new server to be part of the RDS environment

1. Connect to the RDMS server in the Azure portal, using the Remote Desktop Connection client
2. Add the new RD Web and Gateway server to Server Manager:
   a. Launch **Server Manager**, then click **Manage > Add Servers**
   b. In the **Add Servers** dialog, click **Find Now**
   c. Select the newly created Gateway Server - for example, **Contoso-WebGw2** and click **OK**
3. Add RD Web and Gateway servers to the deployment Launch Server Manager
   a. Click **Remote Desktop Services** > **Overview** > **Deployment Servers** > **Tasks** > **Add RD Web Access Servers**
   b. Specify the newly created server - for example, **Contoso-WebGw2**, and then click **Next**
   c. On the **Confirmation** page, click **Restart remote computers as needed**, and then click **Add**
   d. Repeat these steps to add the RD Gateway server, but choose **RD Gateway Servers** in step b
4. Re-install certificates for the RD Gateway servers:
   a. In **Server Manager** on the RDMS server, click **Remote Desktop Services** > **Overview** > **Tasks** > **Edit Deployment Properties**
   b. Expand **Certificates**
   c. Scroll down to the table. Click **RD Gateway Role Service** > **Select existing certificate**
   d. Click **Choose a different certificate** and then browse to the certificate location. For example, **Contoso-CB1\Certificates**. Select the certificate file for the RD Web and Gateway server created during the prerequisites – for example, **ContosoRdGwCert**, and then click **Open**
   e. Specify the password for the certificate, select **Allow the certificate to be added to the Trusted Root Certificate Authorities certificate store on the destination computers**, and then click **OK**
   f. Click **Apply**. (**Note:** You may need to manually restart the TSGateway service running on each RD Gateway server, either through **Server Manager** or **Task Manager)**
   g. Repeat steps 4a-4f for the **RD Web Access Role Service**

Step 2: Configure RD Web and RD Gateway properties on the new server

1. Configure the server to be part of an RD Gateway farm
    a. In Server Manager on the RDMS server, click All Servers. Right-click one of the RD Gateway servers, and then click Remote Desktop Connection
    b. Login to the RD Gateway server using a domain admin account
    c. In Server Manager on the RD Gateway server, click Tools > Remote Desktop Services > RD Gateway Manager
    d. In the navigation pane, click the local computer – for example, Contoso-WebGw1
    e. Click Add RD Gateway Server Farm members
    f. On the Server Farm tab, specify the name of each RD Gateway server, then click Add and Apply
    g. Repeat steps 1a-1f on each RD Gateway server so that they recognize each other as RD Gateway servers in a farm. Do not be alarmed if there are warnings, as it might take time for DNS settings to propagate

2. Configure the server to be part of an RD Web Access farm. Use the following steps to configure the Validation and Decryption Machine Keys to be the same on both RDweb sites
    a. In Server Manager on the RDMS server, click All Servers. Right-click the first RD Web Access server – for example, Contoso-WebGw1 and then click Remote Desktop Connection
    b. Login the RD Web Access server (RD Gateway Server) using a domain admin account
    c. In Server Manager on the RD Web Access server (RD Gateway Server), click Tools > Internet Information Services (IIS) Manager
    d. In the left pane of IIS Manager, expand the Server – for example, Contoso-WebGw1 > Sites > Default Web Site, and then click RDweb
    e. Right-click Machine Key, and then click Open Feature
    f. On the Machine Key page, in the Actions pane, click Generate Keys, and then click Apply
    g. Copy the validation key. Right-click the key and then click Copy
    h. Minimize the RD Connection window for this RD Web server
    i. Login into the Gateway HA Server

j. In **Server Manager** on the RDMS server, click **All Servers** and add **CBVM, Gateway and Session host servers**

k. In **Server Manager** go to the **Manage** panel > **Add Roles and Features**

l. Click **Enable Remote Desktop Services**

m. Repeat steps 2 through 5 for the second RD Web Access server, ending on the feature view of **Machine Key**

n. For the Validation Key, clear the checkbox for **Automatically generate at runtime**, and then paste the key you copied in step 2g

o. Click **Apply**

p. Minimize the **RD Connection** window to the second RD Web Access server, and then maximize the **RD Connection** window to the first RD Web Access server

q. Repeat steps 7-11 to copy over the Decryption Key

r. When validation keys and decryption keys are identical on both RD Web Access servers, sign out of all RD Connection windows

Step 3: Configure load balancing for the RD Web and RD Gateway servers

If you are using Azure infrastructure, you can create an external Azure load balancer; if not, you can set up a separate hardware or software load balancer. Load balancing is key so that traffic will be evenly distributed across the long-lived connections from Remote Desktop clients, through the RD Gateway, to the servers where users will be running their workloads

Note: If your previous server running RD Web and RD Gateway was already set up behind an external load balancer, skip ahead to step 4, select the existing backend pool, and add the new server to the pool.

1. Create an Azure Load Balancer:
   a. In the **Azure portal** click **Browse** > **Load balancers** > **Add**
   b. Enter a name - for example **WebGwLB**
   c. Specify **Public** for the **Scheme**, **Public IP address**, and a **Public IP address**. You can specify an existing Public IP address or create a new one

   d. Specify the appropriate **Subscription**, **Resource Group**, and **Location**
   e. Click **Create**

2. Create a probe to monitor which servers are alive
   a. In the **Azure portal** click **Browse > Load Balancers** for the load balancer you just created – for example, **WebGwLB**, and **Settings**
   b. Click **Probes** > **Add**
   c. Specify a name - for example, **HTTPS**, for the probe. Specify **TCP** as the **Protocol**, and enter **443** for the **Port**, then click **OK**
3. Create the HTTPS and UDP load balancing rules
   a. In **Settings**, click **Load balancing rules**
   b. Specify **Add** for the **HTTPS rule**
   c. Specify a name for the rule - for example, **HTTPS**, and specify **TCP** for the **Protocol**. Specify **443** for both **Port** and **Backend port**, then click **OK**
   d. In **Load balancing rules**, click **Add** for the **UDP rule**
   e. Specify a name for the rule - for example, **UDP**, and select **UDP** for the **Protocol**. Specify **3391** for both **Port** and **Backend port**, and click **OK**
4. Create the backend pool for the RD Web and RD Gateway servers
   a. In **Settings**, click **Backend address pools** > **Add**
   b. Specify a name - for example, **WebGwBackendPool** , then click **Add a virtual machine**
   c. Specify an availability set - for example, **WebGwAvSet**, then click **OK**
   d. Click **Choose the virtual machines**, specify each virtual machine, and then click **Select** > **OK** > **OK**