Configuring Remote Desktop Services on Windows Server 2012 R2® with The Sanbolic Platform®
About this guide

This guide walks system administrators through the process of setting up highly available and highly scalable Remote Desktop Services on Windows Server 2012 R2 with the Sanbolic SDS Scale-out Platform.
Prerequisites

Note: Although the following instructions pertain to a two-node Remote Desktop Services (RDS) implementation, the same steps should be followed for larger RDS implementations.

- **Operating Systems** – Windows Server 2012 R2 Enterprise or Datacenter edition
- **Hardware** – One Domain Controller and at least two RDS servers with the following (minimum) specifications:
  a) CPU – Intel Xeon E5310 @ 1.6 GHz or equivalent
  b) RAM – 2 GB
  c) HDD – 50GB
- **Software** – The following must be installed on each RDS server:
  a) SQL Server 2012 SP1 Express x64 With tools
  b) SQL Server 2012 SP1 Native Client
  c) .NET Framework 3.5 as a feature (install before setting up Remote Desktop Services)
  d) A digitally signed certificate. This certificate needs to contain the FQDN you will use as the RD Web Access URL (e.g. gateway.domain.net). It needs to be in .pfx format and you need to have the private key in it.
  e) The latest version of the Sanbolic Platform available on our site. You should install it on all domain members (not the domain controller) and create a volume that can be accessed (read-and-write) by all domain members concurrently. This should be done prior to Remote Desktop Services setup.
- **Networking** – A minimum of two network adapters with TCP/IP connectivity to the LAN. Sanbolic recommends using one network adapter connected to a stand-alone (private) network for Sanbolic cluster administration (i.e., exchanging heartbeat and locking information between/amongst all nodes)
Installing Remote Desktop Services

Log on to the Domain Controller. In Server Manager, right-click the All Servers node and add all other servers using the “Add Servers” command (or select the All Servers node, click “Manage” and click “Add Servers”).

Once all servers needed for the deployment are present, click “Manage” and then click “Add Roles & Features”. Click “Next” to continue.

Select Installation Type
Select Remote Desktop Services installation. Click “Next”.

Select Deployment Type
Select Standard deployment. Click “Next”.

Select Deployment Scenario
Select Session-based desktop deployment. Click “Next”.

Review Role Services
Review the services that will be installed. Click “Next”.

Specify RD Connection Broker server
Click the preferred server and click the “Add” button. Click “Next”.

Specify RD Web Access server
Click the preferred server and click the “Add” button or select “Install the RD Web Access role service on the RD Connection Broker server” if you want to install on the Broker server. Click “Next”.

Specify RD Session Host server
Click the preferred server and click the “Add” button. Click “Next”.

Confirm selections
Keep in mind that you can install all the services on one server and add the rest later. Check “Restart the destination server automatically if required”. Click “Deploy”.

View progress
Wait until all role services are deployed and the RD Session Host server has restarted. Click “Close”.

In **Server Manager**, click “Remote Desktop Services” and scroll down to the overview. Note the deployment is missing a RD Gateway server and a RD Licensing server. Click the “Add RD Licensing server” button.

*Select a server*
Click the domain controller and click the “Add” button. Click “Next”.

*Confirm selections*
Click “Add”.

*View progress*
Wait until the role service is deployed. No restart is needed. Click “Close”. Click the “Add RD Gateway server” button.

*Select a server*
Click the correct server and click the “Add” button. This can be any domain member server but the domain controller. Click “Next”.

*Name the self-signed SSL certificate*
The wizard creates a self-signed certificate. We will deal with certificates in this deployment in a little bit. Enter the external Fully Qualified Domain Name for the Gateway URL (e.g. gateway.testdomain.org). Click “Next”.

*Confirm selections*
Click “Add”.

*View progress*
Wait until the role service is deployed. No restart is needed. Note that “gateway.testdomain.org” was configured for the deployment as a FQDN. Also notice that certificate configuration is needed. (We’ll get to this in a moment.)

In **Server Manager > Remote Desktop Services > Overview**, click “Tasks” and click “Edit Deployment Properties”.

*Configure the deployment*
Review the RD Gateway settings and notice what settings are available. Server name should be gateway.testdomain.org. You can leave the setting as they are. Click “RD Licensing”.
Configure the deployment
Notice that a RD License server is available, but no license type is selected yet. Select Per User. Also notice the licensing server has already been set to the domain controller. No further changes are needed here. Click “RD Web Access”.

Configure the deployment
By default the RD Web Access IIS application is installed in /RdWeb. You can leave this on default. Click “Certificates”.

Configure the deployment
Notice that the certificate level currently has a status of Not Configured. The RD Gateway certificate is used for Client to gateway communication and needs to be trusted by the clients. Either install the self-signed certificate on all clients, or use a certificate for which the complete certificate chain is already trusted by all clients. As it said in the wizard, the external FQDN should be on the certificate.

The RD Web Access certificate is used by IIS to provide a server identity to the browser clients.

The RD Connection Broker actually has two goals for which it needs certificates - to enable single sign on (server to server authentication), and for publishing (signing RDP files). If you look in the deployment you’ll see that the Connection Broker is now configured to use the server we installed the feature on earlier, so we have to change it to use an external FQDN as well. If we use the same FQDN for all goals described above, we need only one certificate, and only one external IP address.

We’ll come back to this wizard later to assign the certificate. First order of business is to change the internal FQDN for the Connection Broker to an external FQDN. Click “OK”.

Open DNS Manager on the domain controller and browse to Forward Lookup Zones. Right click “Forward Lookup Zones” and click “New Zone”. Go through this wizard accepting the defaults until you have to enter a Zone Name. Enter the external FQDN, which will also be used by the Connection Broker (e.g. gateway.testdomain.org). Finish the rest of the wizard accepting the defaults. Browse to the newly created zone.
**New Host**

Leave the Name field blank, but enter the member server’s (holding the RD Connection Broker role) IPv4 address. Click “Add Host”. You should do this for all the other nodes as well as we will add them to the RD Connection Broker later.

Create a new Global Security Group called “RDS Connection Brokers” and add the computer accounts for the member servers to it as group members. We need this group to be able to convert the RD Connection Broker to a highly available RD Connection Broker. Reboot the member servers to let them know they are members of the RDS Connection Brokers security group.

Install SQL Express on the Domain Controller (or use an existing SQL Server if you already have one). Here’s a list of the required features:

- Database Engine Services
- Client Tools Connectivity
- Management Tools – Basic, Management Tools – Complete

You must have .NET Framework 3.5 already installed in order to complete.

Use the Default Instance and continue with the defaults.

When the installation is done, open SQL Configuration Manager and browse to Client Protocols under SQL Native Client 11.0 Configuration. Check if TCP/IP is enabled under Client Protocols. SQL Express install enables this by default, but check to be sure, especially if you use an existing SQL Server.

Under SQL Server Network Configuration, browse to Protocols for MSSQLSERVER. Enable TCP/IP. If this is a new SQL installation, this will be disabled by default. Restart the SQL Server service if you changed this setting.

On the SQL Server, make sure port 1433 is not being blocked by Windows Firewall. Open SQL Server Management Studio and browse to Logins under Security. Right click “Logins” and click “New Login”.

**Login – New**
Click Search. Select User, Service Account, or Group. Click “Object Types” and select “Group”. Type the RDS Connection Brokers security group name and click “Check Names”. Click “OK”.

**Login – New**
Click “Server Roles” and select “dbcreator”. Click “OK”.
We have just effectively granted the RDS Connection Broker server the right to create databases.
We need this because the RDS Connection Broker service will try to migrate from WID (Windows Internal Database to a (high available) SQL Server instance when we convert the Broker to a highly available broker.

Install the SQL Native Client on the member servers (Client Components only).

Log on to the RD Connection Broker server. In **Server Manager**, click “Remote Desktop Services” and scroll down to the overview. Right-click “RD Connection Broker” and click “Configure High Availability”.

**Before you begin**
Look at the pre-requisites. Click “Next”.

**Configure RD Connection Broker for High Availability**
Database connection string:
- DRIVER=SQL Server Native Client 11.0;SERVER="Domain Controller name";Trusted_Connection=Yes;APP=Remote Desktop Services Connection Broker;DATABASE="DB name" ("Domain Controller name" and "DB name" are the names of the domain controller and database, type them without the quotes)
Folder to store database files:
- C:\Program Files\Microsoft SQL Server\MSSQL11.MSSQLSERVER\MSSQL\DATA (instance default folder)
DNS round robin name:
- The DNS Zone name we configured in DNS earlier.
Click Next.

**Confirmation**
If you get an error before this page:
- Check if TCP/IP is enabled in client protocols and for your instance
- Check if you can reach port 1433 on the SQL Server from the member server
Click “Configure”.

Progress
If you get an error on this page:
- Check SQL permissions for the security group
- Check if the database path you entered is correct
Click “Close”.

The RD Connection Broker is now in High Availability Mode and we are finally ready to complete the configuration.

In Server Manager > Remote Desktop Services > Overview, click “Tasks” and click “Edit Deployment Properties,” then click “Certificates”.
Click “RD Connection Broker – Enable Single Sign On” and click “Select Existing certificate”. Browse to the .pfx file, enter its password, and check “Allow the certificate”. Click “OK”. Click “Apply”. This may take a little while.
Click “RD Connection Broker – Publishing” and click “Select Existing certificate”. Browse to the .pfx file, enter its password, and check “Allow the certificate”. Click “OK”. Click “Apply” and wait for the process to complete.
Click “RD Web Access” and click “Select Existing certificate”. Browse to the .pfx file, enter its password, and check “Allow the certificate”. Click “OK”. Click “Apply” again. This may also take some time.
Click “RD Gateway” and click “Select Existing certificate”. Browse to the .pfx file, enter its password, and check “Allow the certificate”. Click “OK”. Click “OK” to finish the certificate configuration.

Now we need to tell the gateway that external users are allowed to connect to it.

On the RD Gateway server, open Server Manager. Click “Remote Desktop Services” (if it says it’s missing servers, ignore this message), click “Servers” and then right-click the “RD Gateway server”. Click “RD Gateway Manager”.

RD Gateway Manager
Navigate to Policies – Resource Authorization Policies. There’s the default policy. Right-click the default policy and disable it. In the Actions pane to the right, click “Manage Local Computer Groups”.

Manage locally stored computer groups
Click “Create group”. Name the new group. On the Network Resources tab, add the RD Session Host(s) and the DNS external name of the broker. We will add the rest of the servers as hosts later. Click “OK”.
**RD Gateway Manager**
Right-click the “Resource Authorization Policies” node and click “Create New Policy”. Click “Custom”. Name the policy.

Click “User Groups,” add Domain Users, or any group you wish to grant access. Click “Network Resource”. Click “Select an existing RD Gateway-managed group” or create a new one and browse to select the group you created a few steps back. Notice that upon selecting the group, the RD Gateway-managed group members box shows the members of the group. Add all the servers that will comprise the cluster.

Review the Allowed Ports tab and make changes if necessary. Click “OK”.

Before publishing resources we should add the rest of the servers in the cluster to RD Gateway, RD Connection Broker and RD Session Host. We can add only RD Session Host servers to the setup and the users will still be able to login in case the initial host server fails, but no changes to the environment will be possible until the original host holding the Gateway and Connection Broker services is restored.

In Overview, right-click “RD Session Host” and click “Add RD Session Host Servers”. Note that the Remove RD Session Host servers option is used to remove one or more Session Host servers from the deployment. This will not uninstall the RD Session Host role service from the selected server(s), unless you choose to do so in the wizard.

Click the newly added server and click the “Add” button. Click “Next”.

**Confirm selections**
Check “Restart the destination server automatically if required”. Click “Add”.

**View progress**
Wait until the RD Session Host role service is deployed and the new RD Session Host server has restarted. Click “Close”.

If you want Web Access users to be able to log on to this server, you need to add this server to the Resource Group for which we configured a policy on the RD Gateway server a bit earlier. In case you did not add the servers then, this is how you do it.

Open the RD Gateway Manager tool and expand the server node, expand the Polices node and click the "Resource Authorization Policies” node. (If in your setup you chose a different server for each RD Connection service, you’ll need to log on to the RD Gateway server first).
**RD Gateway Manager**
Click “Manage Local Computer Groups”. Make sure the Resource group is selected and click “Properties”. Type the name of the new server and click “Add”. The note you see here refers to the Remote Desktop Session Host server farm principle in case you also publish Windows 2008(R2) Remote Desktop deployments. In Windows 2012(R2) the farm concept is handled by the RD Broker and the RD Session Collections. Click “OK” to apply the settings to the resource group and click “Close” to close the group manager.

At this point we are ready to publish a Remote Desktop environment, but as stated earlier, we should also add the rest of the cluster nodes as RD Gateway and RD Connection Broker servers.

In Overview, right-click on “RD Gateway” and add RD Gateway Servers.

**Server Selection**
Select the servers you wish to add as RD Gateway servers and click “Next”.

**Confirmation**
Review the settings and click “Add”.

**Results**
Wait for the process to complete. Click “Close”.

In case this server is the one holding the RD Connection Broker service, go to Overview. Otherwise you will need to log on to the RD Connection Broker server. Right-click on “RD Connection Broker” and add RD Connection Broker Server.

**Before You Begin**
Review the requirements, click “Next”.

**Server Selection**
Select the servers you wish to add as RD Connection Broker servers and click “Next”.

**Confirmation**
Review the settings and click “Add”.

**Results**
Wait for the process to complete. Click “Close”.
I. Publishing Remote Desktop Sessions

We are now ready to publish a Remote Desktop environment. We will publish full desktop
sessions.

In **Server Manager > Remote Desktop Services > Session Collections**, click “Tasks” and
then click “Create Session Collection”. You can do this on any Host server in the
environment.

*Before you begin*
Review the requirements. Click “Next”.

*Name the collection*
Enter a descriptive name. This name will be displayed under its icon in the Web Access
interface. Click “Next”.

*Specify RD Session Host servers*
Click the member servers that have the RD Session Host role and click the “Add” button. You
can only add servers that do not have a Collection set yet and have added RD Session Host
role. Click “Next”.
You can limit access here. Add one or more groups to restrict access to these groups only.
Click “Next”.

*Specify user profile disks*
As stated at the beginning of this guide, you should already have a Sanbolic volume
configured on all servers in this cluster. You can create a folder on the volume that will hold
the user disks. Ex. `Z:\userprofiledisks\rds`

Check “Enable user profile disks” and enter “Z:\userprofiledisks\rds” as location below.
Since the Sanbolic volume will be visible as the same drive letter on all nodes, you do not
need to set a share. You can change the maximum size for each user disk. Click “Next”.

*Confirm selections*
Review the information and click “Create”.

*View Progress*
Wait until the collection is created and the server is added to the collection. Click “Close”.
To see how we can influence the load balancing properties, go back to **Server Manager** and
click “Remote Desktop Services,” then click the desktop collection you just created. Click
“Tasks” and then select “Edit Properties”.

**Session Collection**
In this load balancing setup both servers are equally weighted for sessions. You could rebalance this if hardware resources are not the same across all servers in the collection. While you’re in this screen, review the other properties of this session collection. You can leave them as they are or change them depending on the specifics of your environment.

Load balancing a collection makes it possible to do maintenance on your servers without disrupting your users. You can put a server in maintenance mode without disrupting functionality. In the Host Servers section for the collection, right-click the server for which you want to perform maintenance. Select “Do not allow new connections”. Of course, you will have to wait until existing sessions are completed or instruct users to log off and log back on, in which case they will be redirected by the RD Broker to the other server. Note this is a new session; there is currently no way to migrate sessions to other hosts without disrupting users.

**II. Testing the setup**

On a server that has access to your test setup, open an RDP connection to the gateway (e.g. gateway.testdomain.org) or open https://gateway.testdomain.org/rdweb. If you are using an RDP connection enter a valid username and password (DOMAIN\username) and you will be presented with a certificate confirmation window. Click “Yes”.

After the user identity is confirmed you will be logged on to one of the host servers.

If you are using the web access, enter a valid username and password (DOMAIN\username or username@domain). Click “Sign in”. After logging in, you’ll be presented with the full desktop session collection we created. After clicking the collection named icon (e.g. Desktop), you’ll get the warning that devices are going to be redirected. Click “Connect”.

This concludes our guide to setting up a RDS environment with the Sanbolic Platform.