**[Tech-Coffee](https://www.tech-coffee.net/)**

* [CLOUD](https://www.tech-coffee.net/category/cloud/)
* [SOFTWARE-DEFINED](https://www.tech-coffee.net/category/software-defined/)
* [STORAGE](https://www.tech-coffee.net/category/sto/)
* [SQL SERVER](https://www.tech-coffee.net/category/sql-server/)
* [SYSTEM CENTER](https://www.tech-coffee.net/category/systemcenter/)
* [WINDOWS SERVER](https://www.tech-coffee.net/category/windows-server/)





RDS 2016 farm: RDS Final configuration

Posted by: [Romain Serre](https://www.tech-coffee.net/author/romain-serre/" \o ") in [Microsoft Azure](https://www.tech-coffee.net/category/cloud/microsoft-azure/) May 24, 2017 [2 Comments](https://www.tech-coffee.net/rds-2016-farm-rds-final-configuration/#comments) 38,598 Views

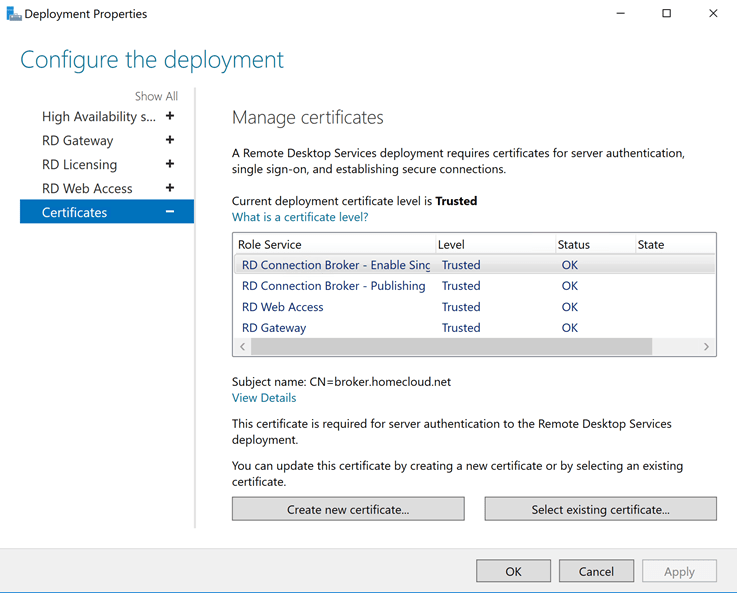
This article is the final topic about how to deploy a Remote Desktop Service in Microsoft Azure with Windows Server 2016. In this topic, we will apply the RDS Final configuration, such as the certificates, the collection and some custom settings. Then we will try to open a remote application from the portal.

* [Deploy a Windows Server 2016 RDS Farm in Microsoft Azure](https://www.tech-coffee.net/deploy-a-windows-server-2016-rds-farm-in-microsoft-azure/)
* [Create Microsoft Azure networks, storage and Windows image](https://www.tech-coffee.net/rds-2016-farm-create-microsoft-azure-networks-storage-and-windows-image/)
* [Deploy the Microsoft Azure Virtual Machines](https://www.tech-coffee.net/rds-2016-farm-deploy-the-microsoft-azure-vm/)
* [Configure Domain Controllers](https://www.tech-coffee.net/rds-2016-farm-configure-domain-controllers/)
* [Deploy the RDS farm](https://www.tech-coffee.net/rds-2016-farm-deploy-the-farm-in-azure/)
* [Configure File Servers for User Profile Disk (UPD)](https://www.tech-coffee.net/rds-2016-farm-configure-file-servers-for-user-profile-disks/)
* **RDS final configuration**

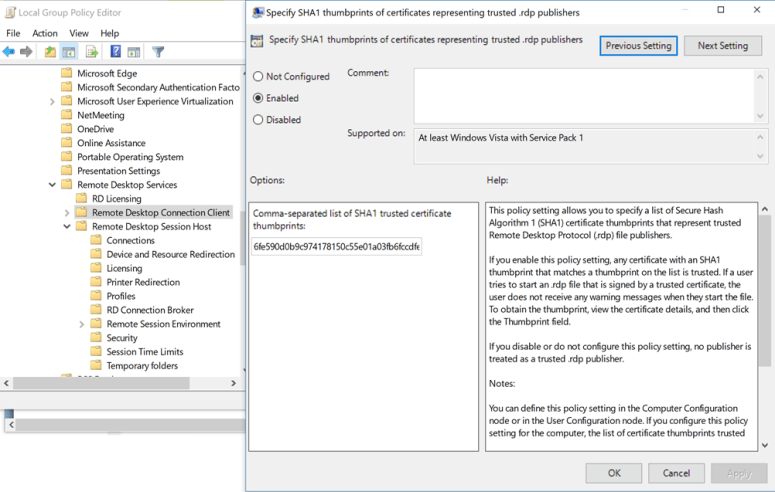
Certificates

Before creating the collection, we can configure the certificates for RD Web Access, RD Gateway and the brokers. You can request a public certificate for this or you can use your own PKI. If you not use your own PKI, you have to distribute the certificate authority certificates to all clients. You have also to provide the CRL/OCSP responder. If you use a public certificate, there is almost no client side configuration. You can get more information about required certificates [here](https://technet.microsoft.com/en-us/library/dn781533%28v=ws.11%29.aspx?f=255&MSPPError=-2147217396).

Once you have your certificate(s), you can open the properties of the RDS Farm from the server manager. Then navigate to certificates. In this interface, you can add the certificate(s) for each role.



On client side, you should add a setting by GPO or with local policy editor. Get the RD Connection Broker – Publishing thumbprint and copy it. Then edit this setting **(Specify SH1 thumbprint of certificates representing trusted .rdp publishers**) and add the certificate thumbprint without spaces. This setting enable to remove a pop-up for the clients.

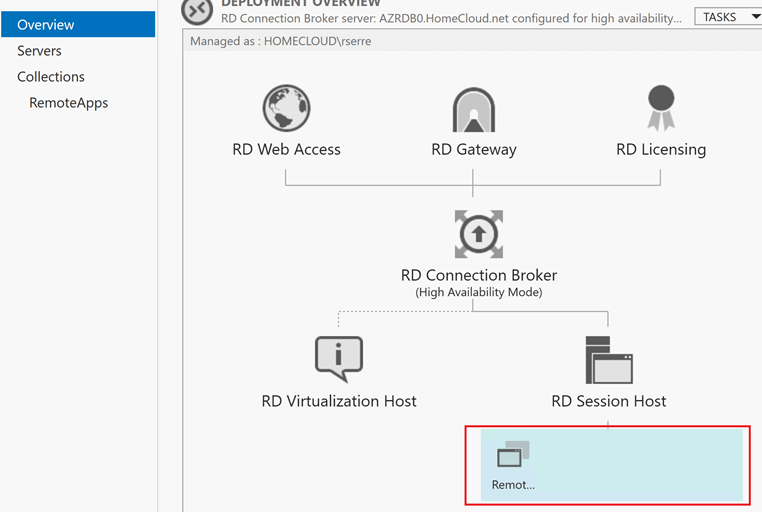


Create and configure the collection

To create the collection, I use the following PowerShell cmdlet:

|  |  |
| --- | --- |
| 1  2  3  4 | New-RDSessionCollection –CollectionName RemoteApps `                          –SessionHost azrdh0.homecloud.net, azrdh1.homecloud.net `                          –CollectionDescription "Remote application collection" `                          –ConnectionBroker azrdb0.homecloud.net |

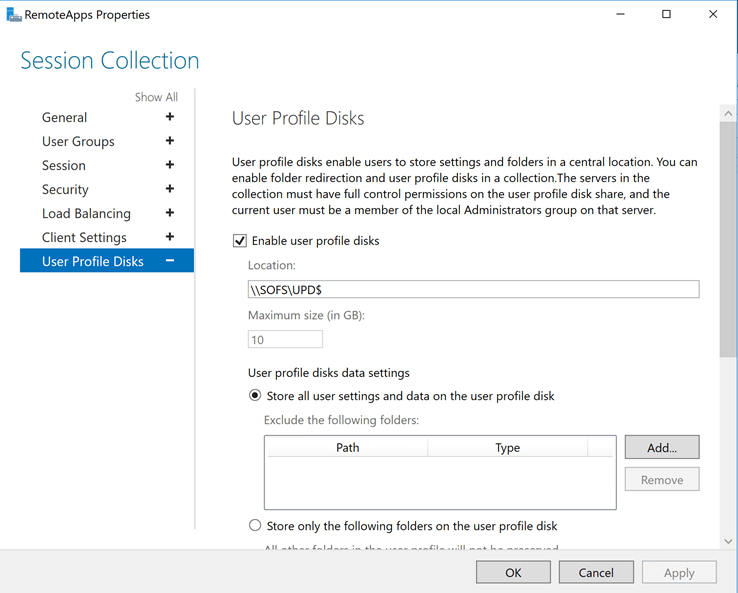
Once you have created the collection, the RDS farm should indicates a new collection:



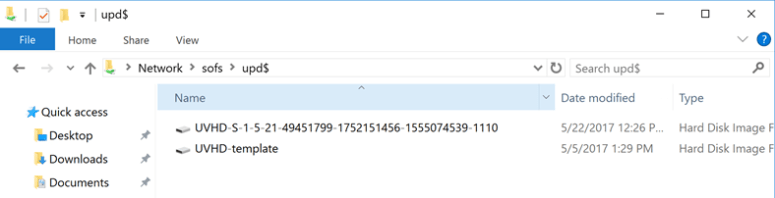
Now we can configure the User Profile Disks location:

|  |  |
| --- | --- |
| 1  2  3  4  5 | Set-RDSessionCollectionConfiguration -CollectionName RemoteApps `                                       -ConnectionBroker azrdb0.homecloud.net `                                       -EnableUserProfileDisk `                                       -MaxUserProfileDiskSizeGB 10 `                                       -DiskPath \\SOFS\UPD$ |

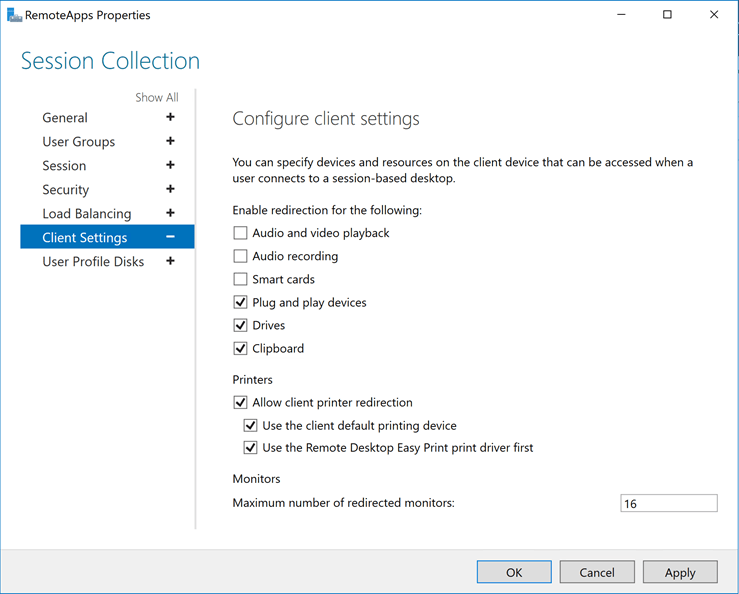
If you edit the properties of the collection, you should have this User Profile Disk configuration:

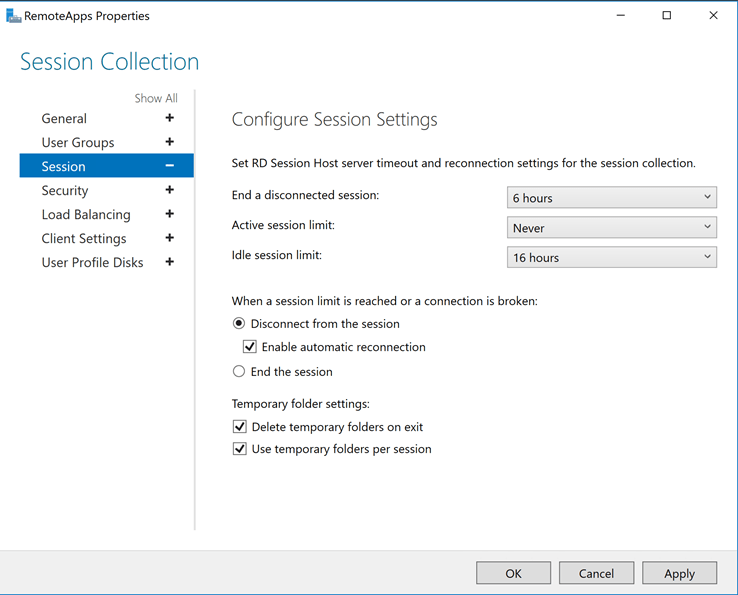


In the **\\sofs\upd$** folder, you can check if you have new VHDX files as bellow:



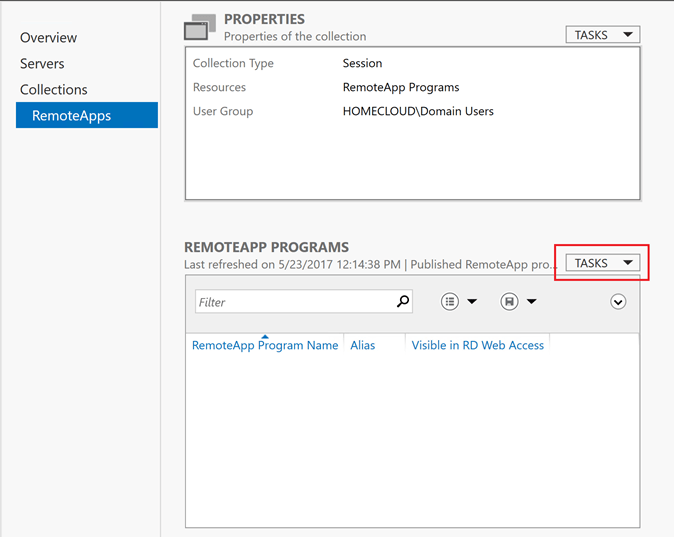
From the Server Manager, you can configure the collection properties as below:



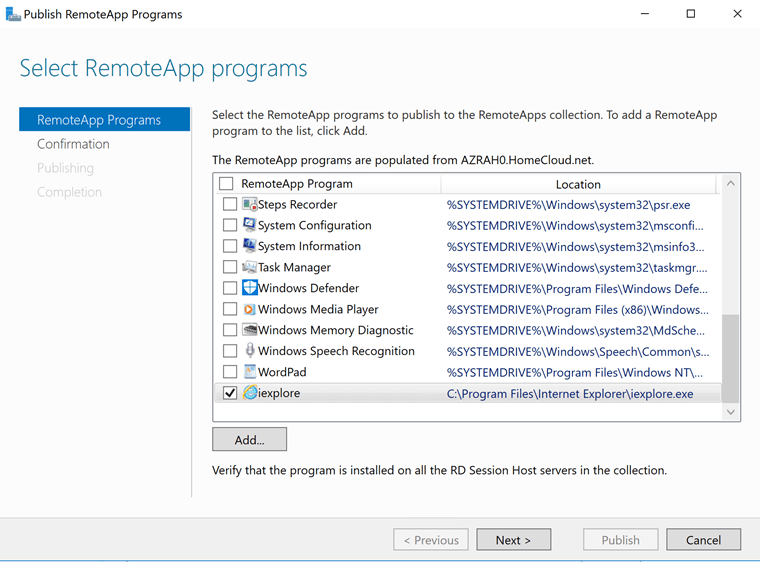


Add applications to the collection

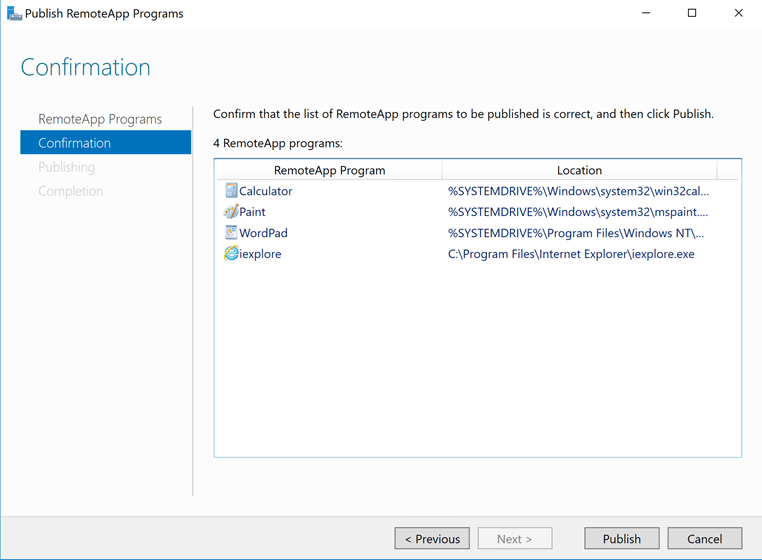
The collection that we have created is used to publish applications. So, you can install each application you need in all RD Host servers. Once the applications are installed you can publish them. Open the collection properties and click on add applications in RemoteApp Programs part.



Then select applications you want to publish. If the application you want to publish is not available in the list, you can click on **add**.

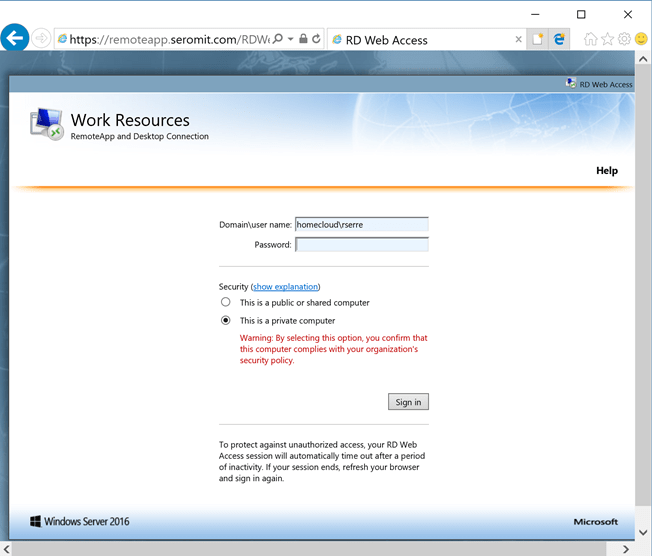


Then the wizard confirms you the application that will be published.

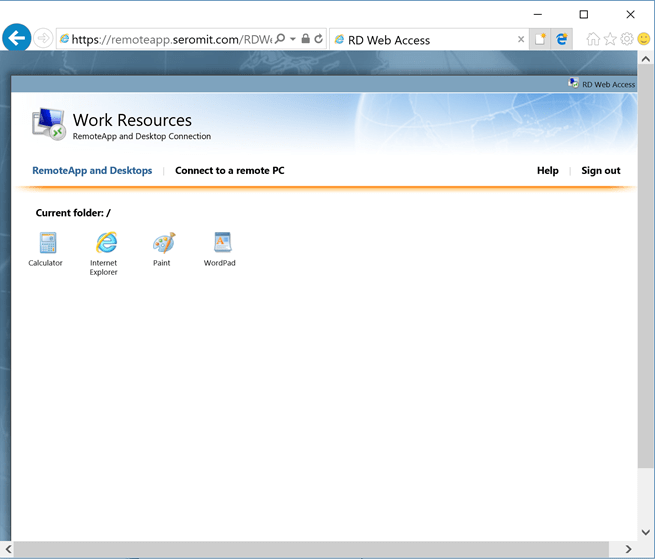


Test

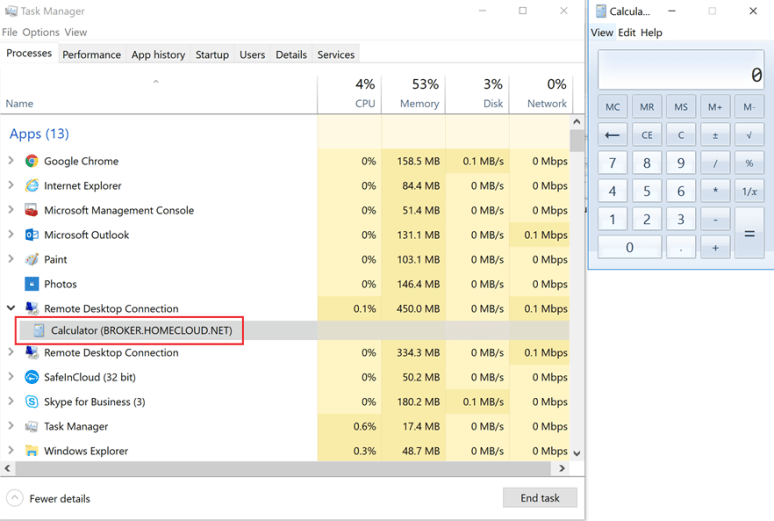
Now that applications are published, you can browse to the RD Web Access portal. In my configuration, I have added a DNS record which is bound to the Azure Load Balancer public IP. Specify your credential and click on Sign In.



Click on the application of your choice.



I have chosen the calculator. As you can see in the task manager, the calculator is run through a Remote Desktop Connection. Great, it is working.



Conclusion

This series of topics about Remote Desktop Services shown you how to deploy the farm in Azure. We saw that Windows Server 2016 brings a lot of new features that ease the deployment in Azure. However, you can also deploy the RDS Farm On-Prem if you wish.