Flexible Windows Server 2019 Azure Stack HCI Virtual Desktop Infrastructure Hybrid Solution

Written by Bono Hsueh

Last Update: 3/23/2020
Version: 2.1

Abstract

Windows Server 2019 brings about tremendous changes and improvements to the Windows Server architecture. There are great improvements in the realm of hybrid cloud, Storage Spaces Direct (S2D), security, HCI, and many others that help to take the enterprise data center to the next level when running on top of the Windows Server architecture.

Azure Stack HCI and the Windows Server Software Defined (WSSD) Program are both invitation-only programs in which solution providers are requested by Microsoft to design hyper-converged infrastructures with Windows Server technologies.

One of the enhanced areas of functionality with Windows Server 2019 is the new Remote Desktop Services (RDS) features and functionality found in Windows Server 2019. RDS has been a staple component of the Windows Server operating system for quite some time and Windows Server 2019 takes those features and capabilities to the highest level.

Azure Stack HCI offers the optimal platform for VDI. Leveraging a validated HCI solution and Microsoft's mature Remote Desktop Services (RDS), customers can create highly available and highly scalable architectures.

There are two types of virtual desktop solutions in the Microsoft ecosystem – Session Virtualization with Remote Desktop Services Host and Virtual Desktop Infrastructure served out by Hyper-V. You can use either solution or mix them effectively to meet the demands of most use cases presented to your business for remote connectivity.

In addition, Azure Stack HCI VDI solutions provide unique cloud-based capabilities for protecting VDI workloads and clients:

- Manage updates centrally using Azure Update Management
- Unified security management and advanced threat protection for VDI clients.

REVISIONS

Version	Date	Description	Author
1.0	11/13/2019	First Publish	Bono Hsueh
1.1	11/21/2019	Add Materials	Bono Hsueh
1.2	12/23/2019	Finished	Bono Hsueh

CONTENTS

Overview of Virtual Desktop Infrastructure (VDI) and Windows Server RDS

Virtual Desktop Infrastructure, or VDI, uses server hardware to run desktop operating systems and software programs on a virtual machine. For as long as operating system virtualization existed, VDI offered the flexibility of running traditional desktop workloads, on centralized servers.

Leveraging VDI in a business setting has a wide range of advantages, including keeping sensitive company applications and data in a secure datacenter, accommodating a bring-your-own-device policy without worrying about personal data getting mixed with corporate assets, reducing liability when corporate assets are lost - covering both data loss prevention and exposure of sensitive data to potential corporate espionage and/or hackers. In addition, VDI has become the de-facto standard for supporting remote and branch workers as well as for providing access to contractors and partners.

Today's businesses are empowering their employees to work from anywhere and from multiple devices. With Virtualization and Virtual Desktop Infrastructure (VDI) technologies driving the modern workforce, employees now have more connectivity and productivity options than ever before.

When it comes to utilizing Microsoft technologies for remote access to satisfy business needs, Windows Server Remote Desktop Services offer a wide range of features and capabilities. When used with underlying virtualization technologies, it provides a powerful platform for remote access.

Common Use Cases for Virtual Desktops

There are certain common use cases that are generally cited by many businesses as the primary reasons for configuring a virtual desktop solution

- Bring Your Own Device (BYOD) Environments – BYOD can introduce a lot of complexity, especially around security and other concerns. Controlling BYOD with all company policies can be difficult. However, having a virtual desktop that can be accessed from the BYOD device with all the company restrictions and policies in place is much more feasible

- Remote Contractors/Teleworkers – This is one extremely common scenario that drives virtual desktops so remote contractors or teleworkers can "remotely" connect into a corporate environment no matter where they are located or which networks they are coming from

- Running Windows applications on non-Windows devices – This allows flexibility in running your Windows applications. Since published applications are actually running on the Windows Server backend, this allows them to be presented on non-Windows devices for consumption

- Performance and Resiliency Demands – Certain desktops are critical enough in nature that they need to be housed in data center environments and on server class hardware and storage. Virtual desktop environments make this possible as the virtual desktop instance physically resides on in the data center. Workloads housed in the data center environment are afforded the protection of the data center, including backups and other fail-safes that are available. Additionally, performance may dictate that the desktop environment is as close as possible to the actual data. By placing the desktop in the same data center as the backend data, this reduces latency and other performance affecting variables

- Disaster Recovery – Disaster recovery is a strong use case for virtual desktops. Virtual desktops allow your workforce to be in a totally different location from where your infrastructure is located. If there are situations that keep workers from coming into the office, or if there is a widespread disaster where workloads may fail over to a different environment, virtual desktops allow provisioning of desktop resources for productivity and business applications

Types of VDI Virtual Desktop Implementations

Two types of VDI deployments exist in the Windows VDI world: pooled and personal desktops. What is the difference?

- Pooled – In this configuration, you set up a "pool" of virtual machines. When a user connects, they are automatically assigned a virtual machine that is not in use. When the user disconnects, the VM is reset to a default state and the VM is added back to the pool to be available for connection from other users

- Personal – A personal desktop allows the same VM to be assigned to a specific user to cater to individual requirements. Such a VM may have a particular configuration or software that the specific user needs.

Pooled desktops hold certain advantages over the personal desktops in terms of maintenance and other administrative duties. The pooled desktops are generated from a "Gold" image VM. Since the data is reset each time a user logs off, there is no need to maintain specific VMs. You simply patch and update the Gold VM and all the other VMs will be updated upon their next generation.

Personal desktops are convenient for dealing with end-user data. Since they are persistent, end-user data are maintained locally. Therefore, system administrators do not have to worry as much about how to save users' data.

The Enhancements with Windows Server 2019 RDS

RDS web client – as part of the RD web client in the browser, you can use the single-sign-on experience to allow authentication to be passed on to desktops you have access to from the RDS web client. RDS web client is a little limited in what it can redirect. You can create a PDF of the printout and then print when you are connected.

GPU virtualization is a big part of user experience. More and more applications today are requiring graphics acceleration. Discrete device assignment has been continually improved in Windows Server 2019 including RDSH scalability with GFX HW acceleration, use of all available GPUs, and improvements on video detection and handling.

Moving onto the Discrete Device Assignment or DDA functionality, let's compare DDA and Remote vGPU in Windows Server 2019.

DDA:

- Primary story for GPU acceleration in WS2019
- Enhanced security and isolation
- Guaranteed GPU performance
- API compatibility (DirectX 12, OpenGL)
- We are continuing to evaluate GPU-P drivers for VDI and RDSH

Remote vGPU:

- Deprecated in WS2019
- Clean OS installation cannot share RemoteFX vGPUs with new Hyper-V VMs
- Upgrade warning if RemoteFX vGPU is enabled in the upgraded OS
- If you had a Remote FX vGPU-enabled VM it will continue to work after upgrade
- Admins can remove RemoteFX vGPU after upgrade to WS2019

RDSH (Remote Desktop Session Host) Improvements

When we look at the RDSH improvements found in Windows Server 2019, there are several areas where improvements can be seen, including:

- **Video playback**
  - Hardware acceleration applied at any time
  - Supports smooth playback while moving the video window
  - Supports 4K downsampling

- **Device redirection**
  - High-level redirection of built-in or attached video camera
  - Less network bandwidth compared to USB camera
  - Increased video framerate, up to 30 fps
  - Redirect multiple cameras

- **Improved printing messages**
  - Message queuing that is built-into the Windows client

- **User Input Delay performance counters**
  - Another measure to troubleshoot poor application performance
  - Correlate with other performance counters (Active Sessions, CPU, etc.)
  - Enabled by default in WS2019 RDSH and Windows 10, version 1809

QCT Deployment Lab

Hardware and Software for this Guide

Server Hardware BOM:

QuantaGrid D52BQ-2U (2~4 nodes) (Alias name: S5BQ)				
SKU	Description	Qty per unit	Total	Version
Server Platform	D52BQ-2U	1	4	BIOS: S2P_3B10 BMC: 3.33
CPU	Intel Xeon Gold 5118 CPUs (2.3GHz, 12-core, 16.5MB cache)	2	8	
Memory	Samsung 32GB DDR4 2666MHz ECC-Register DIMMs	16	64	
Cache	Samsung 1.92TB 2.5” SATA SSD	4	16	104Q
Storage	Seagate 8TB 3.5” SATA HDD (ST8000NM0055)	8	32	PN01
Boot Drive	Intel 480G 2.5” SATA SSD	1	4	G2010140
HBA Card	QCT LSI SAS 9305-16i - IT firmware mode	1	4	FW: 1B03
NIC Card	Mellanox Quanta OCP Mezz CX4, Dual Port 25G	1	4	FW: 14.24.1000

Network:

Switch: 2x TOR QuantaMesh T4048-IX8D and 1x BMC QuantaMesh T1048-LY4R

Hardware:
The four servers were interconnected using Mellanox based 25GbE Ethernet RDMA cards that also support DCB/PFC/ETS Ethernet switches.

The SSD (cache tier) + HDD (capacity tier) drives were added to a single S2D pool with multiple volumes based on the number of QCT S2D server nodes.

Software:
Each server ran Windows Server 2019 Datacenter Edition and participated in a Windows Failover Cluster (required for S2D).

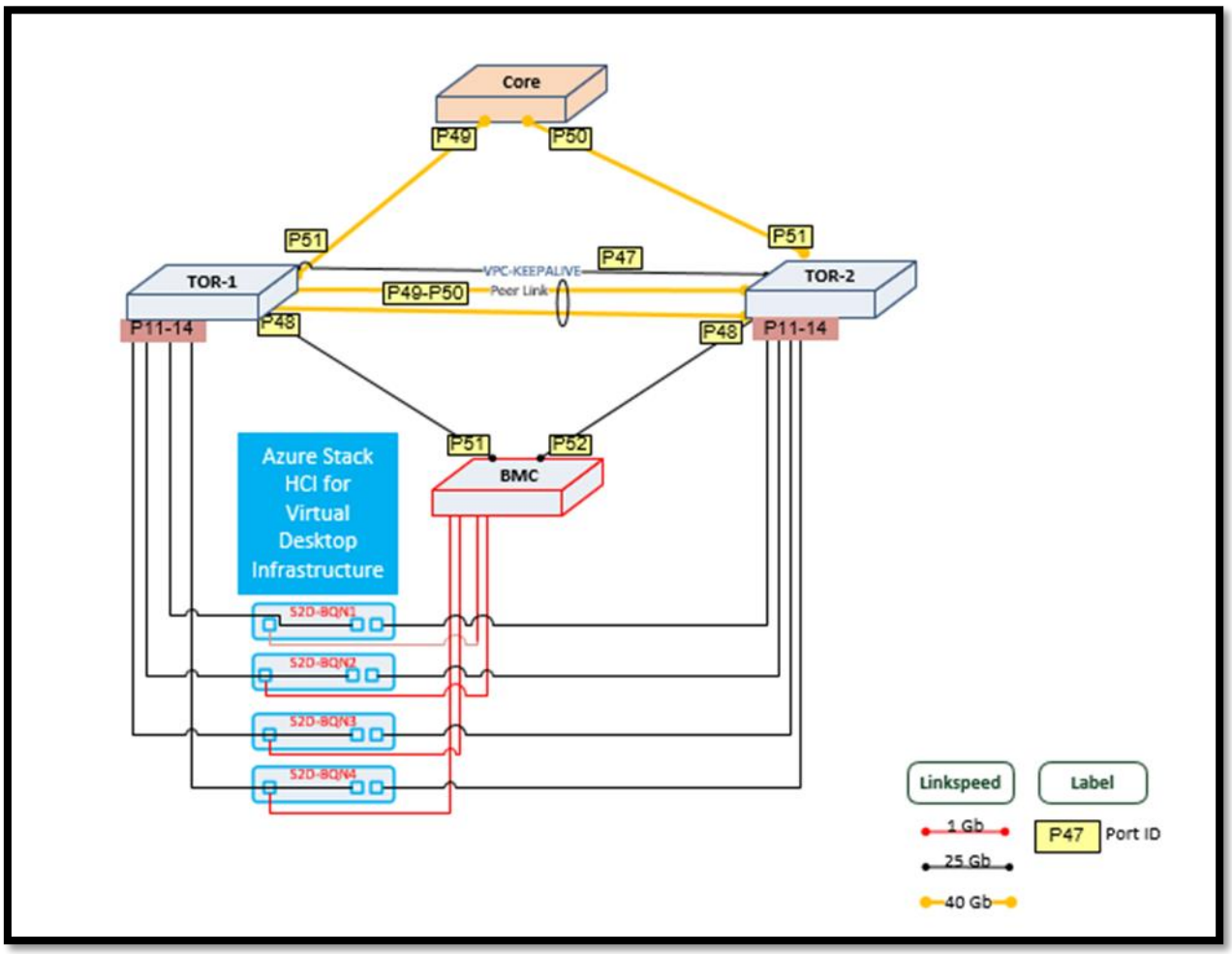
The volumes were configured for the operating system (OS) and data drives as 2-way mirrored volumes, resulting in one local copy of data and one remote copy on other nodes.

Client user workloads were run in Hyper-V virtual machines, with Windows 10 adopted as the guest OS and a few apps installed on windows 10 Enterprise Edition. Each VM was configured with 2 virtual cores (mapped to 1 physical core) and 8GB of RAM.

The disks included are as shown below:

Drive	Size(GB)	Purpose	Note
C:	40	Windows OS	Windows 10 client VM installed with Sysprep and other apps
D:	100	User Data	Client user data file

Server Nodes / Network Diagram



Prepare the QCT physical server node

Best practices dictate that with every new server deployment, the first task is to review the system firmware and drivers relevant to the incoming operating system. If the system has the latest firmware and drivers installed it will expedite tech support calls and may reduce the need for such calls.

https://qct.io/product/index/Server/rackmount-server/2U-Rackmount-Server/QuantaGrid-D52BQ-2U#download

In this tutorial, we will show how to set up an RDS farm in Windows 2016/2019 with the following features:

- Remote Desktop Session Host (x2)
- Service broker for the distribution of connections
- Setting up a collection
- Publishing RemoteApp on a web portal
- Remote Desktop Gateway
- User Profile Disk (UPD)

For the establishment of a complete RDS farm, it takes at least 4 servers without counting the domain controller and file server and print. All the servers on the farm must be in the field.

Composition:

Name	IP	Roles
RDS-DKP-153.ws19demo.qct	10.106.5.153	Remote Desktop Session Host 1
RDS-DKP-155.ws19demo.qct	10.106.5.155	Remote Desktop Session Host 2
RDS-BRK-152.ws19demo.qct	10.106.5.152	Service Broker / License Manager
RDS-WEB-154.ws19demo.qct	10.106.5.154	Gateway Remote Desktop / Web Access
RDS-APP-151.ws19demo.qct	10.106.5.151	Remote APP Publish Host

For the realization of this tutorial, we used an AD server, dc01.ws19demo.qct with the IP address 10.106.48.100. DC is used for storing UPDs.

Server role definitions that are part of an RDS farm.

Remote Desktop Session Host: On these servers, the user sessions are open which allows them to work.

Service broker: This is the circulation agent for sessions in an environment with multiple remote desktop session hosts.

Remote Desktop Gateway: Its primary role is to enable secure access to the RDS infrastructure from the Internet. It connects to the farm using HTTPS and filter connections using access policy.

Web Access: Publishes a web portal that allows access to applications via RemoteApp via an Internet browser. This role is also used for RemoteApp access for Windows clients. Through this portal, it is also possible to include password change for the users.

License Manager: This service is used for license distribution (CAL RDS).

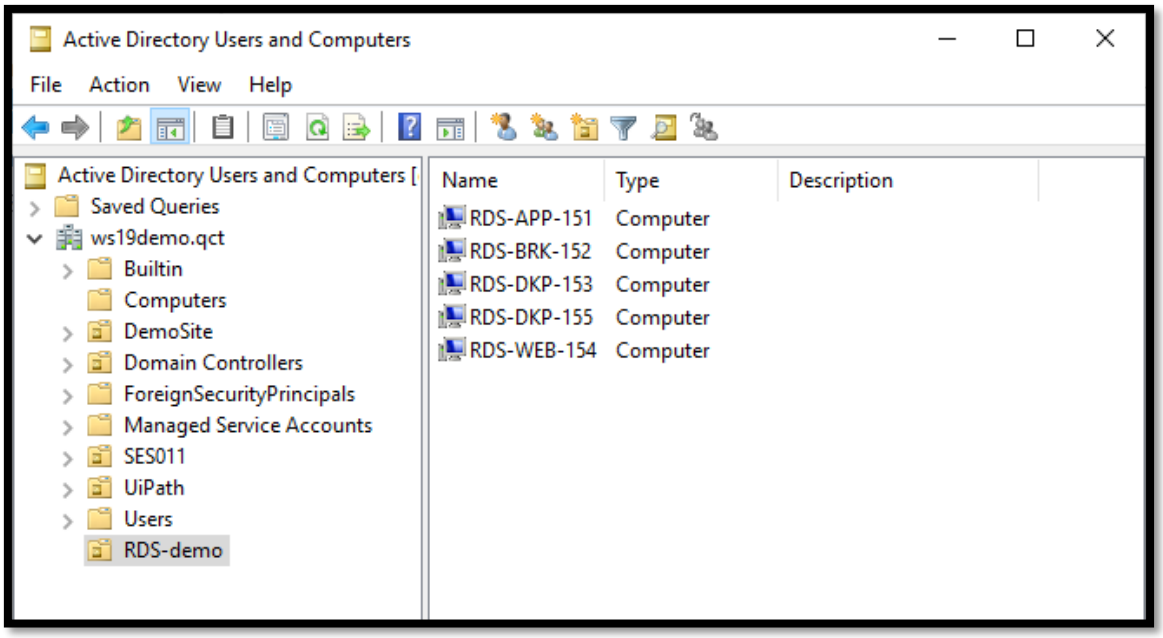
The tutorial was made under Windows 2012R2. The deployment of an RDS farm under Windows 2016 and 2019 is almost identical.

Preparation of the environment

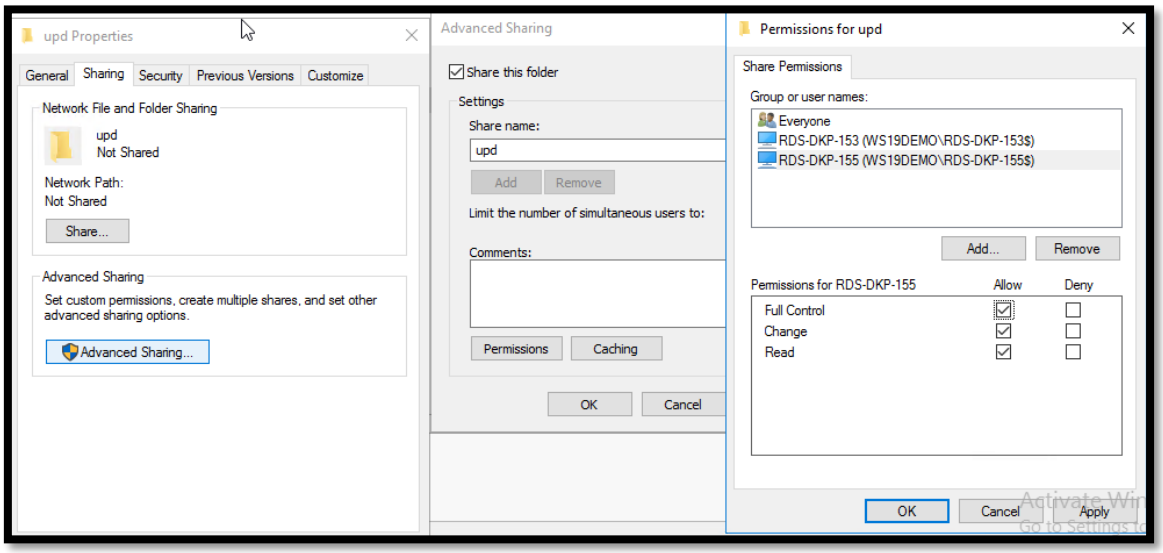
1. Move the Remote Desktop Session Host Servers to an OU

This operation will allow subsequently apply specific GPO at the RDS environment using a loopback policy for user parameters.

Open the Active Directory Users and Computers console, create a specific OU for the Remote Desktop Session Host servers, and move them in.

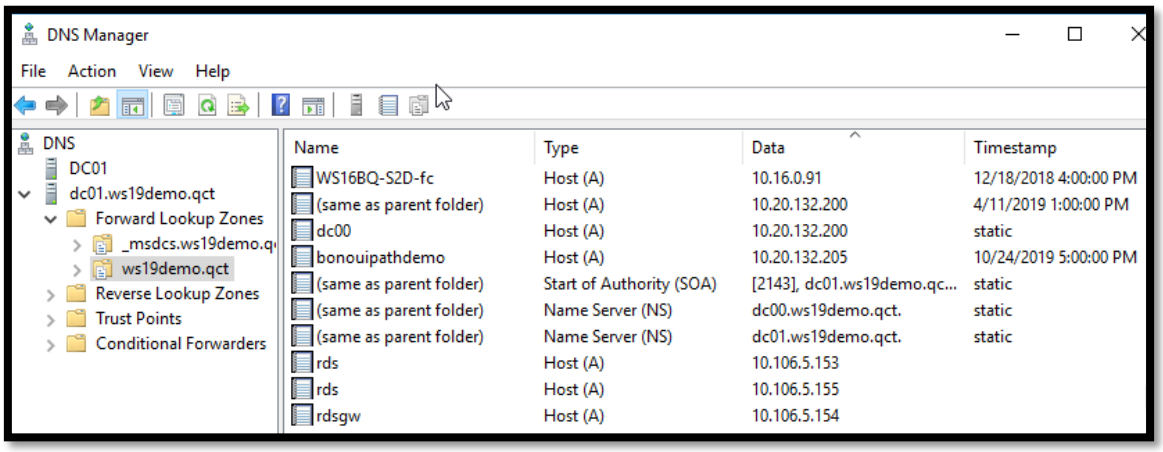


2. On a file server (DC01), create a folder for storing UPDs, share the folder, the accounts of the computers having the remote desktop session host role (RDS-DKP-153$ and RDS-DKP-155$) must have full control.



3. Add DNS records

Create a type A record with the same name that will point to the IPs of your remote desktop session host, as shown below.



I added a record of type A RDS Gateway pointing to the IP of the server RDS-WEB-154 to be able to use the gateway internally.

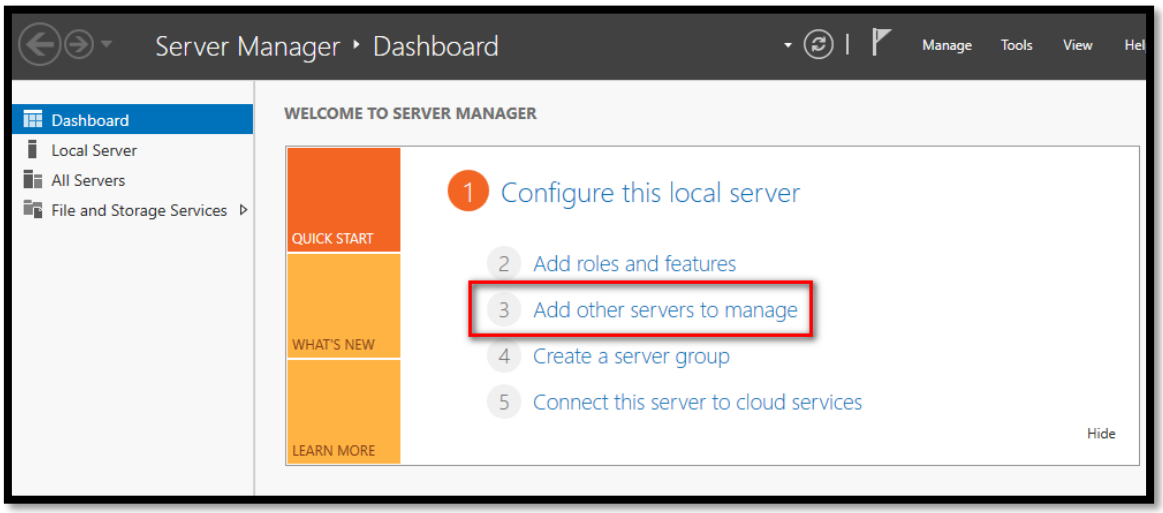
In production, it will be necessary to provide a recording on a domain accessible from the Internet of type A on a public IP and to set up a rule on router / firewall to authorize the traffic on the port 443.

4. Server Manager - Add Servers in One Console

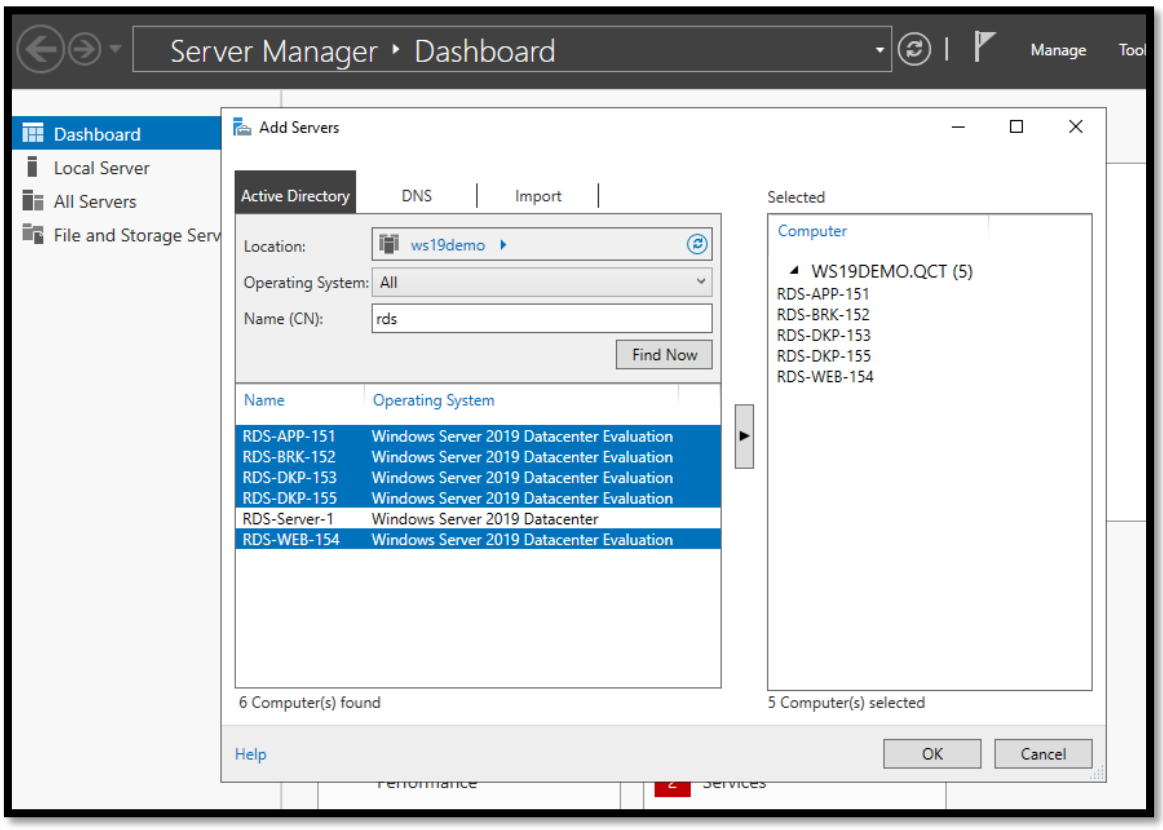
To use the Windows Deployment Tool, you must add the servers that make up the RDS environment in one console.

The following operations are to be done on the server RDS-BRK-152.ws19demo.qct.

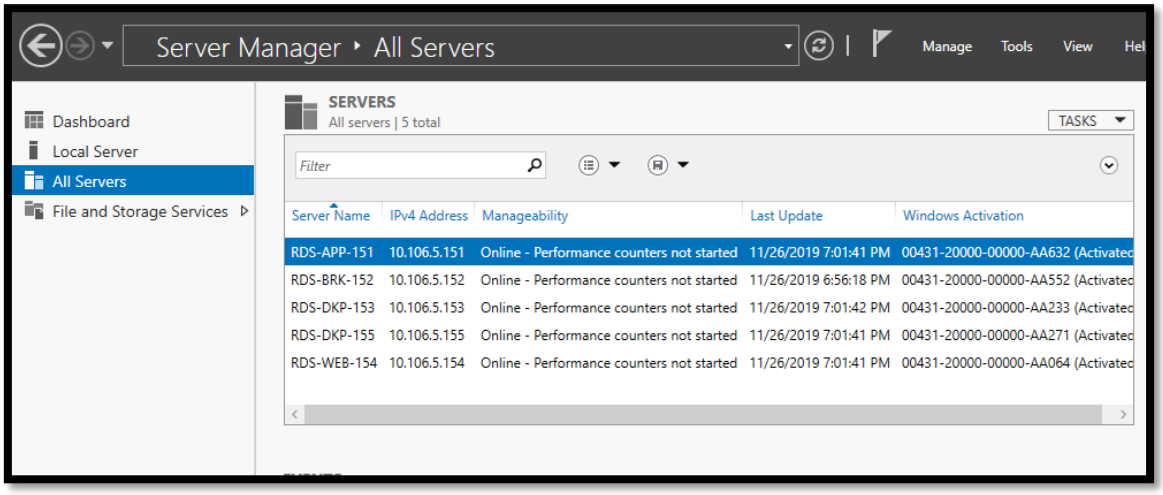
1. From the server manager, click Add more servers to manage:



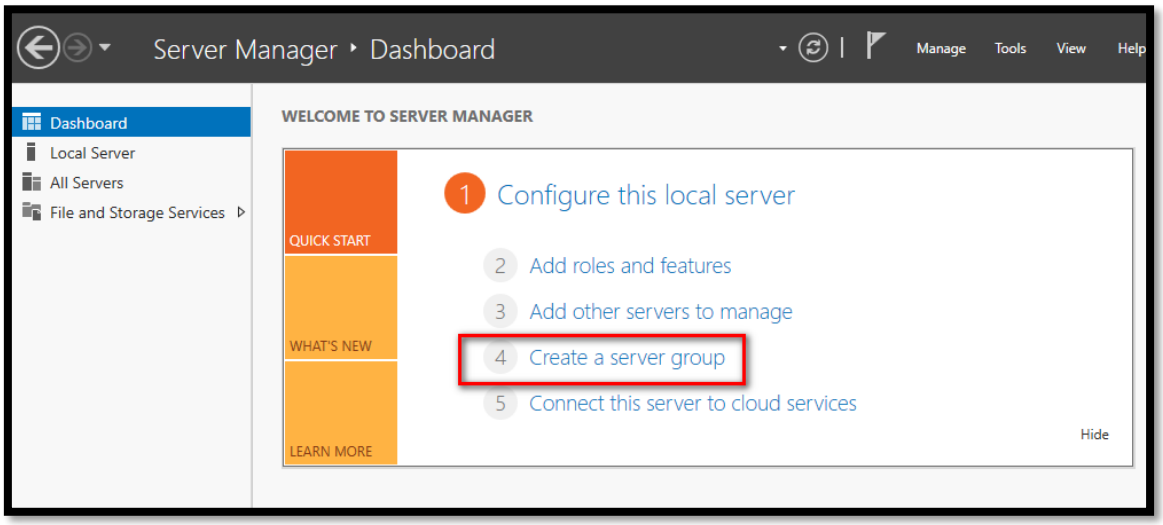
2. Search in the Active Directory to view the available computers. Select the computers that make up the RDS 2 infrastructure and click on the 3 arrows to add them.



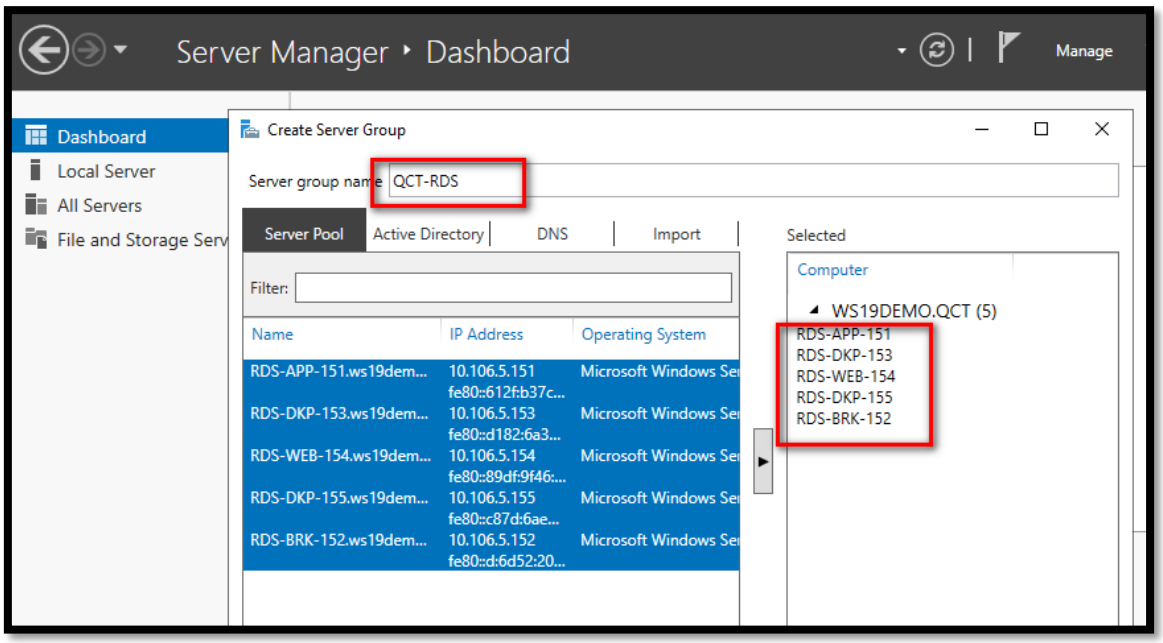
3. On the server manager, go to [All Servers] to view them.

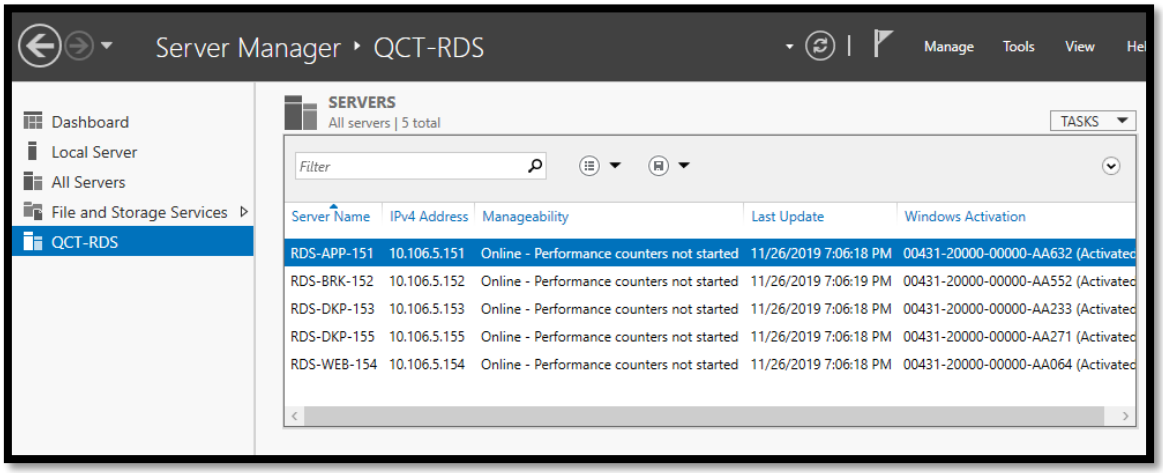


4. From the Server Manager Dashboard, click Create Server Group



5. Name the group, select the servers, and click on the arrow to add them.





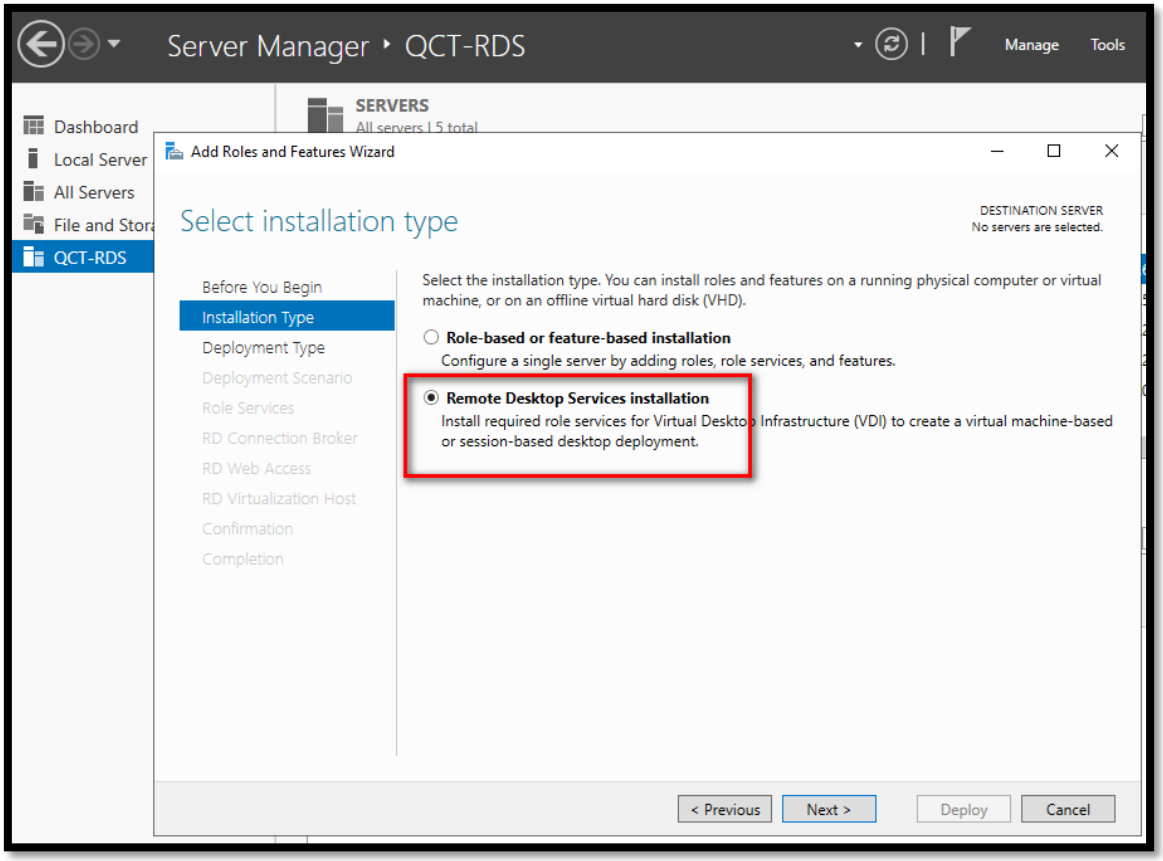
Deploying RDS roles

The deployment of an RDS infrastructure is facilitated by the tool built into the server managers, in a single manipulation the following roles will be installed:

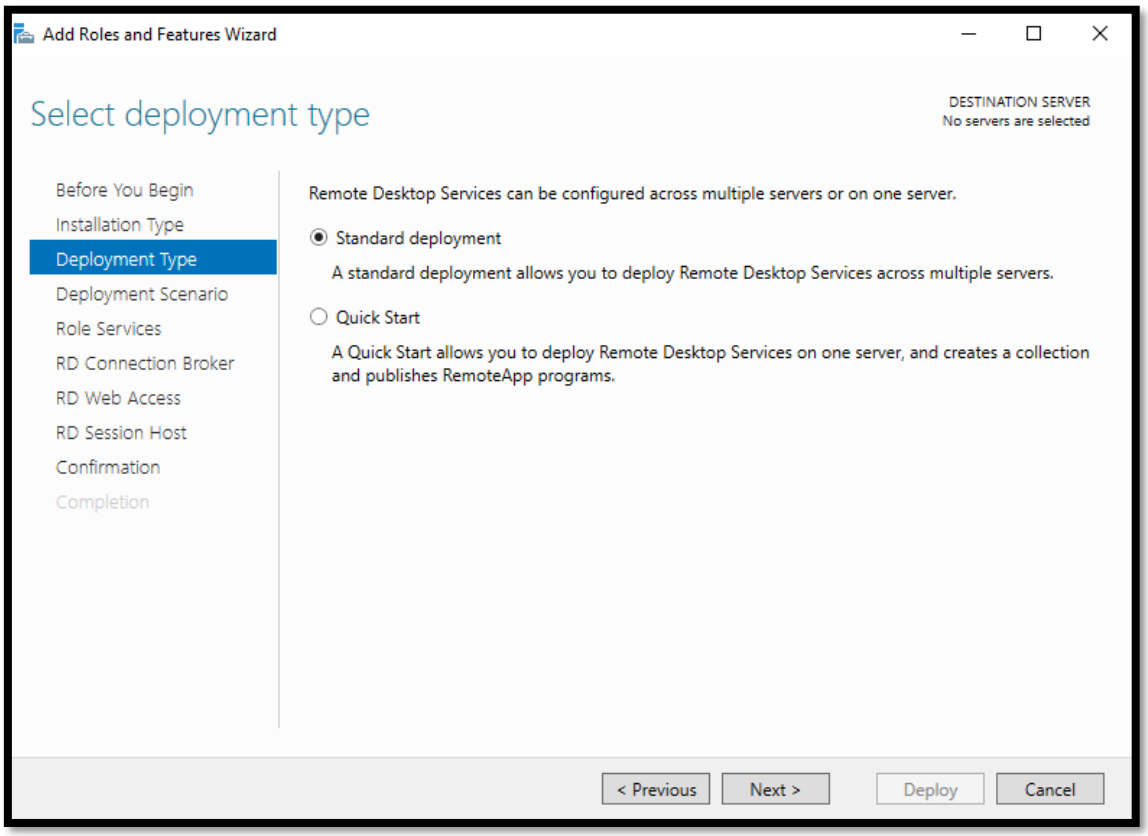
- Remote Desktop Session Host
- Broker
- Remote Desktop Access via the Web

1. From the Server Manager, click Manage → Add Roles and Features

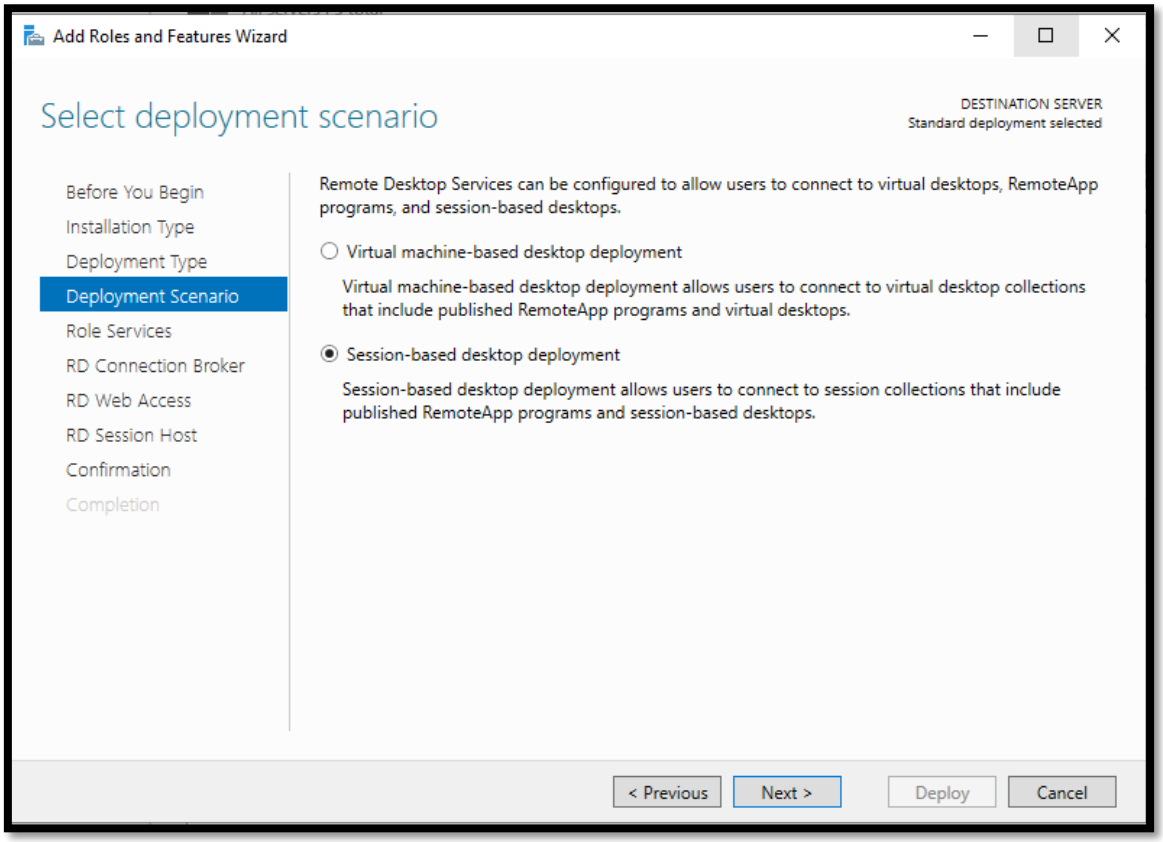
Installation Type: Select Remote Desktop Services Installation



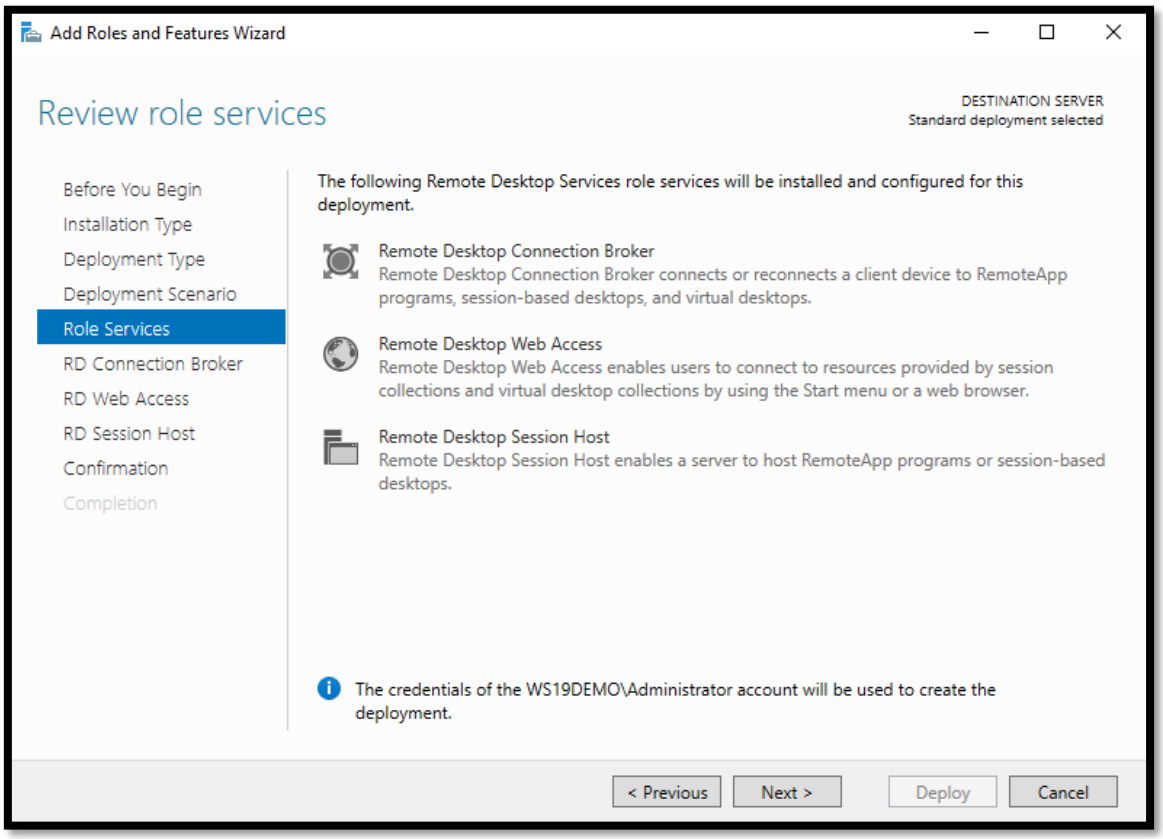
2. Deployment Type: select Standard Deployment



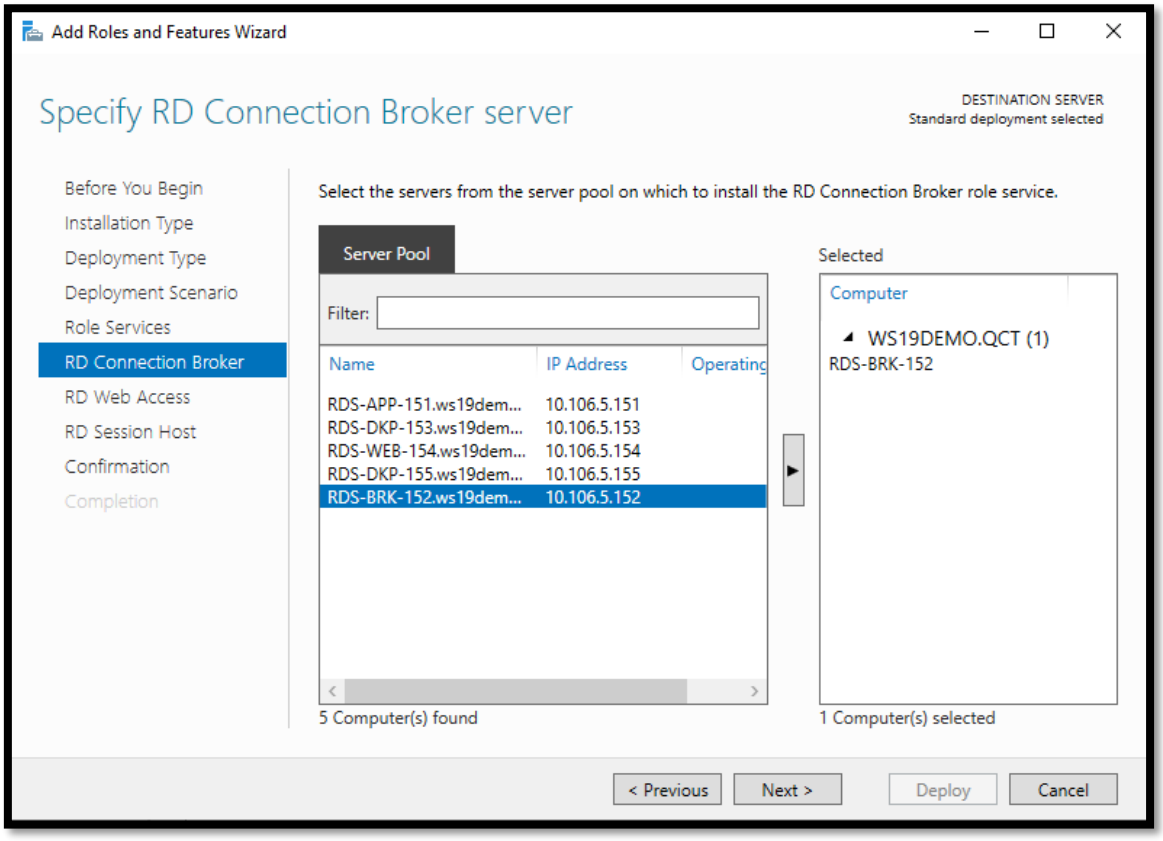
3. Deployment Scenario: Session-based desktop deployment



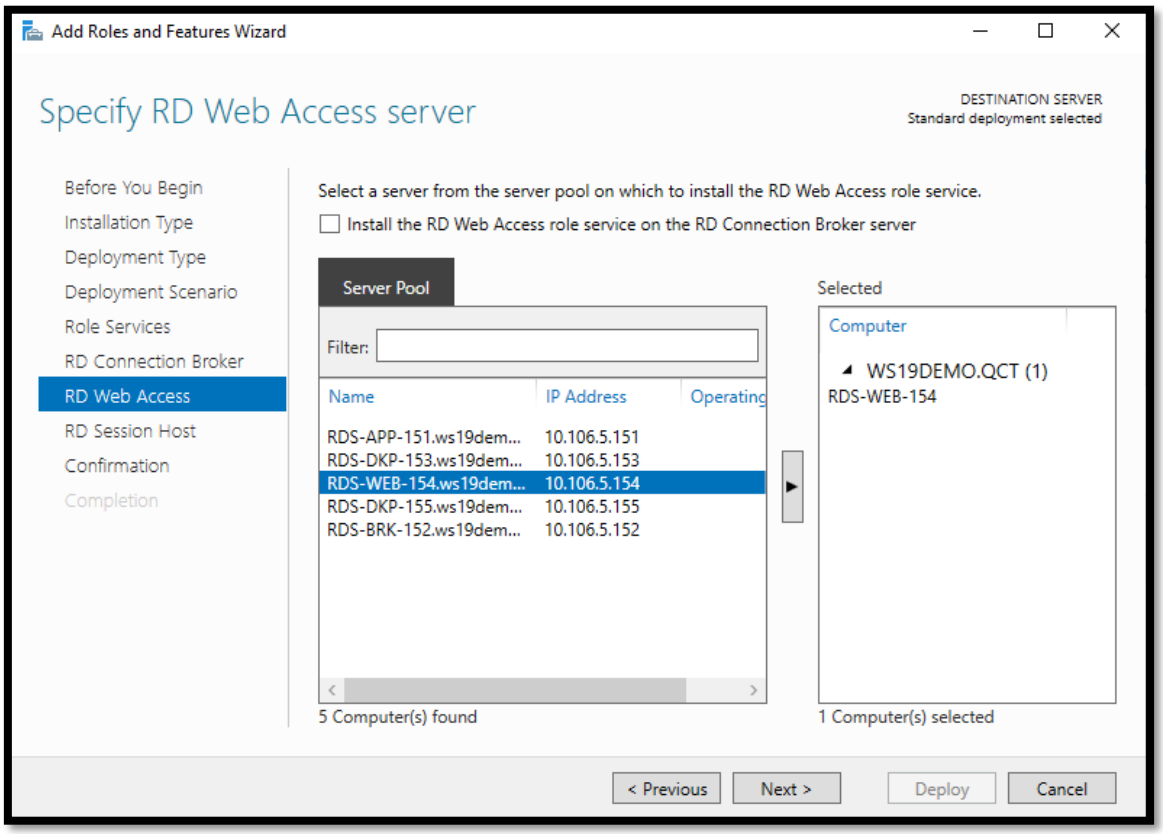
4. The wizard summarizes the roles that will be deployed.



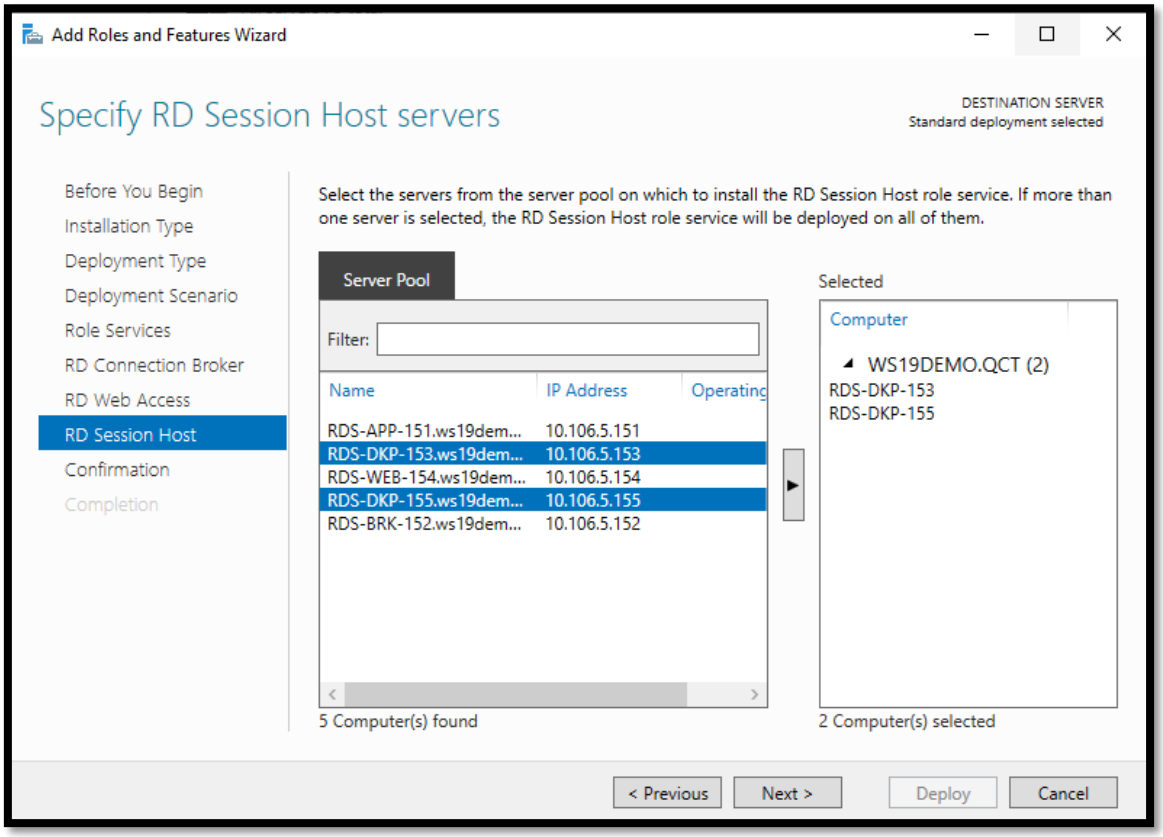
5. Service broker: Select the server that will have the role, click on the arrow to add



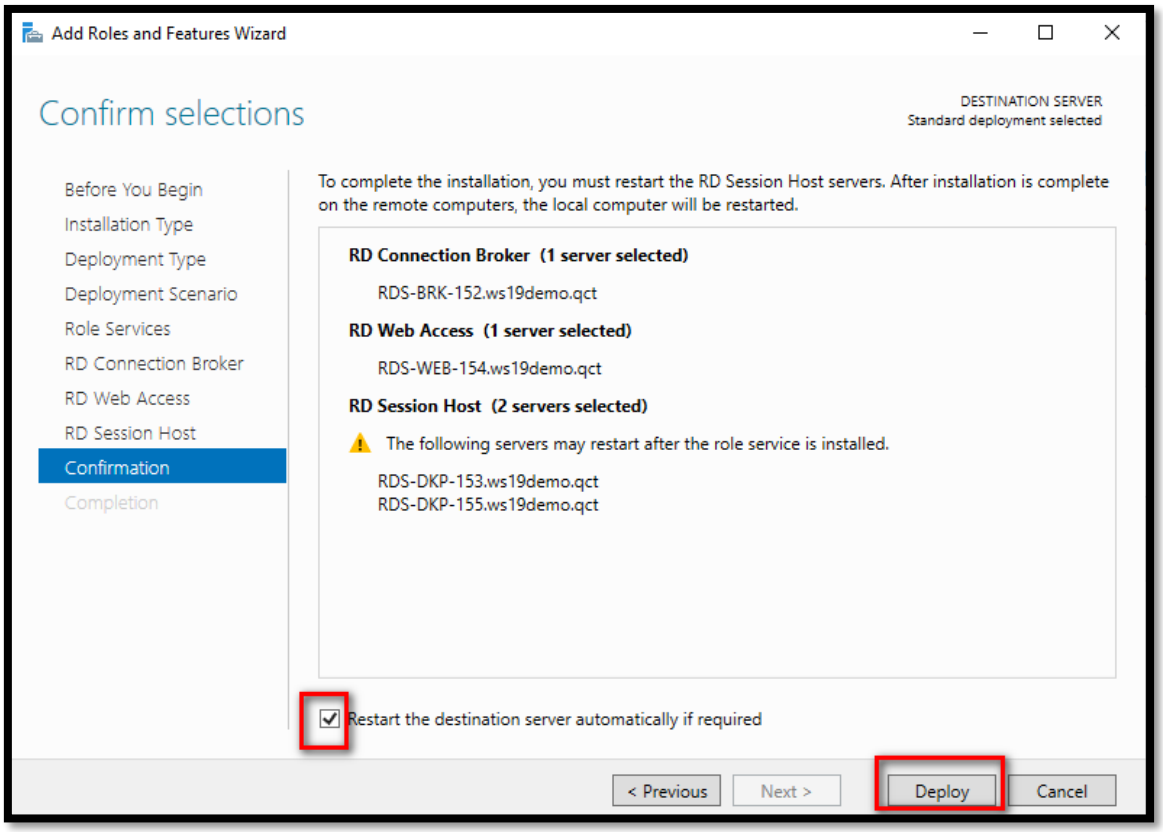
6. Remote Desktop Web Access: Select the server that will have the role



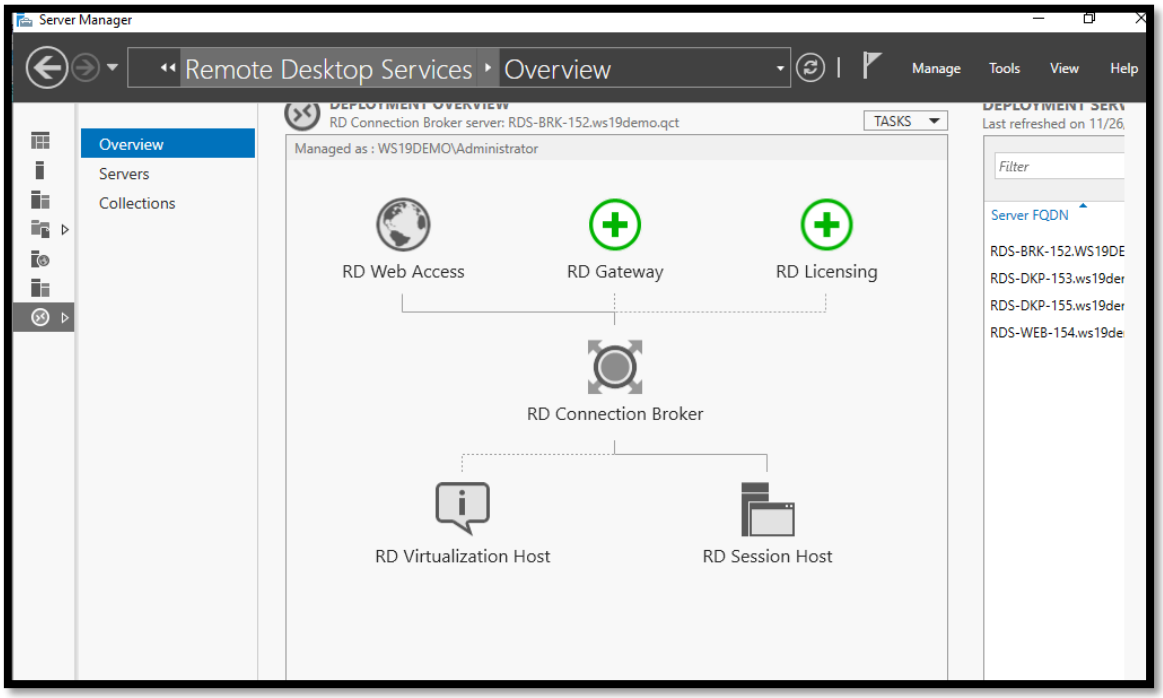
7. Remote Desktop Session Hosts: Select the servers that will have the role

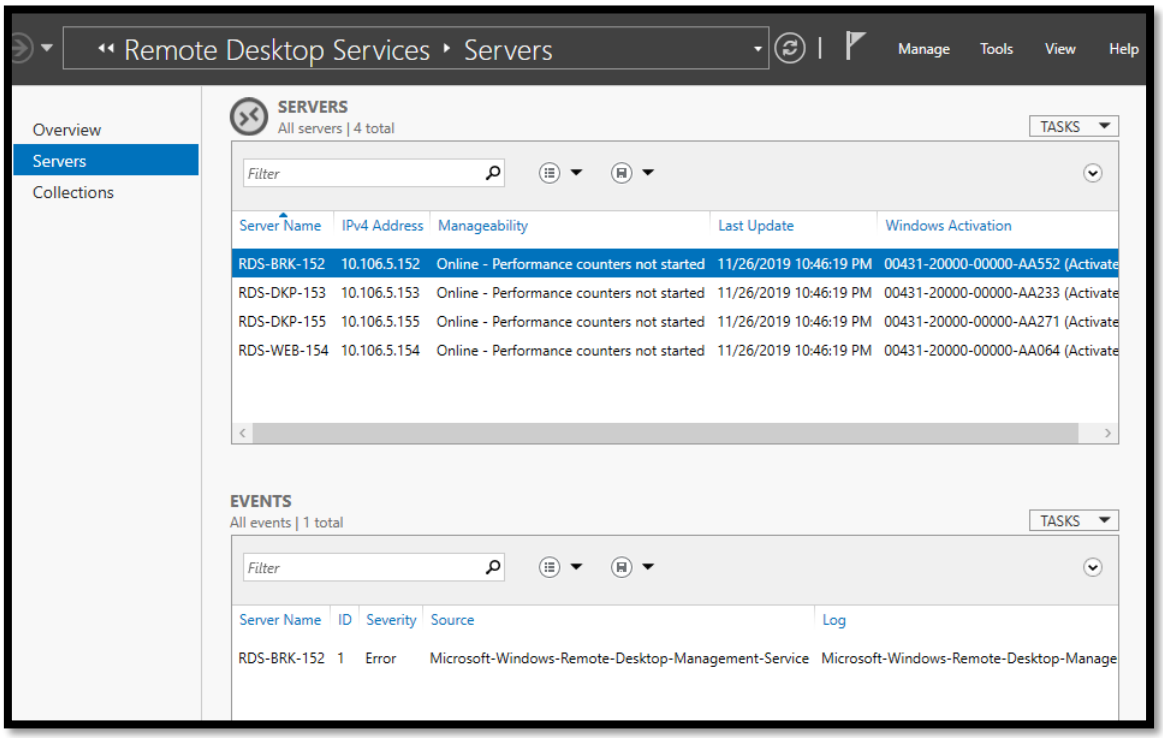


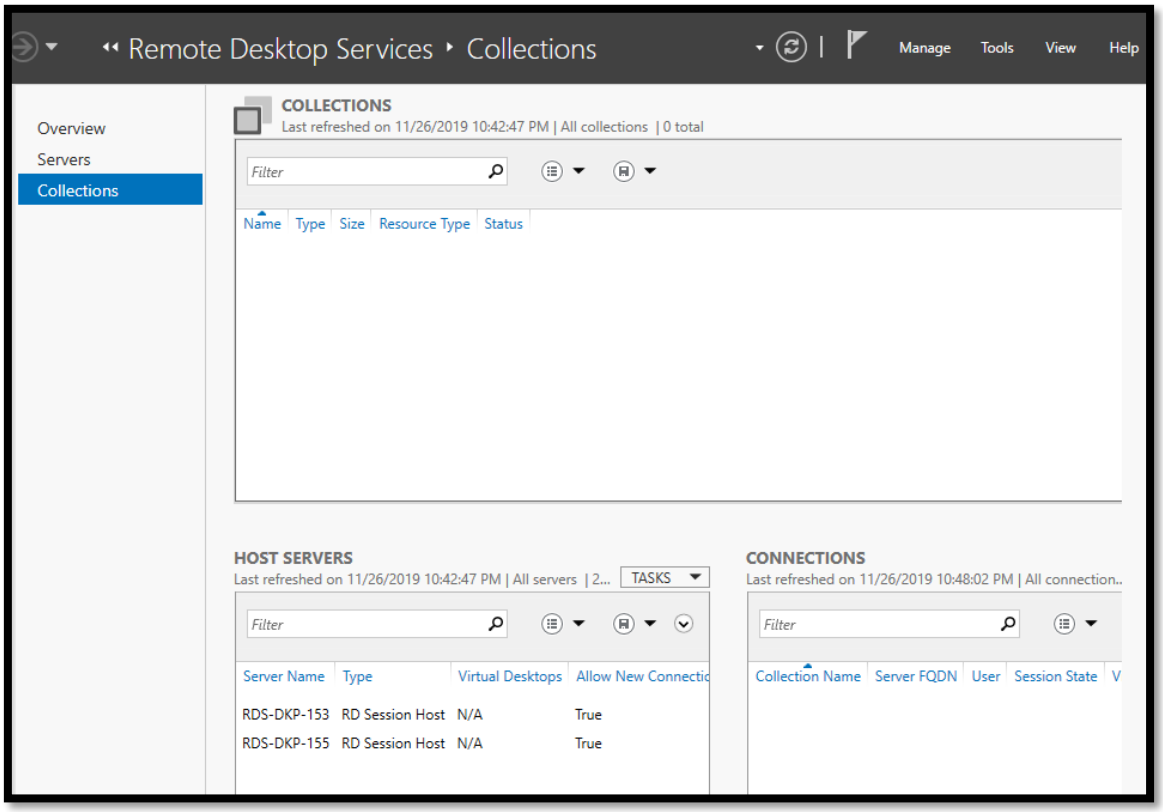
8. Check the box [Restart the destination server automatically if required], then click on [Deploy]



9. From the server manager, go to Remote Desktop Services. From this view, an overview of the deployment is visible.




Remote Desktop Services ‣ Servers
Manage
Tools
View
Help
Overview
Servers
Collections
SERVERS
All servers | 4 total
TASKS
Filter
Server Name
IPv4 Address
Manageability
Last Update
Windows Activation
RDS-BRK-152 10.106.5.152 Online - Performance counters not started 11/26/2019 10:46:19 PM 00431-20000-00000-AA552 (Activate
RDS-DKP-153 10.106.5.153 Online - Performance counters not started 11/26/2019 10:46:19 PM 00431-20000-00000-AA233 (Activate
RDS-DKP-155 10.106.5.155 Online - Performance counters not started 11/26/2019 10:46:19 PM 00431-20000-00000-AA271 (Activate
RDS-WEB-154 10.106.5.154 Online - Performance counters not started 11/26/2019 10:46:19 PM 00431-20000-00000-AA064 (Activate
EVENTS
All events | 1 total
TASKS
Filter
Server Name
ID
Severity
Source
Log
RDS-BRK-152 1 Error Microsoft-Windows-Remote-Desktop-Management-Service Microsoft-Windows-Remote-Desktop-Manage


Remote Desktop Services ‣ Collections
Manage
Tools
View
Help
Overview
Servers
Collections
COLLECTIONS
Last refreshed on 11/26/2019 10:42:47 PM | All collections | 0 total
Filter
Name
Type
Size
Resource Type
Status
HOST SERVERS
Last refreshed on 11/26/2019 10:42:47 PM | All servers | 2...
TASKS
Filter
Server Name
Type
Virtual Desktops
Allow New Connectic
RDS-DKP-153 RD Session Host N/A True
RDS-DKP-155 RD Session Host N/A True
CONNECTIONS
Last refreshed on 11/26/2019 10:48:02 PM | All connection..
Filter
Collection Name
Server FQDN
User
Session State

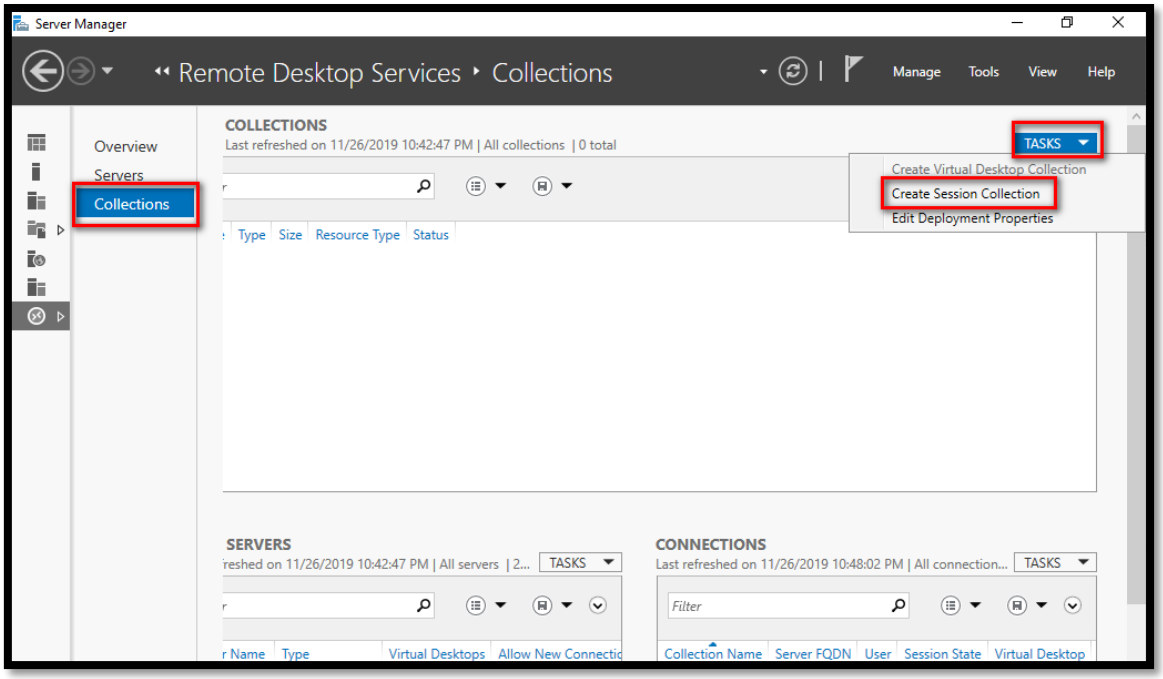
Setting up a collection

A collection allows remote desktop configuration by specifying the hosts that make up the collection and who can access it.

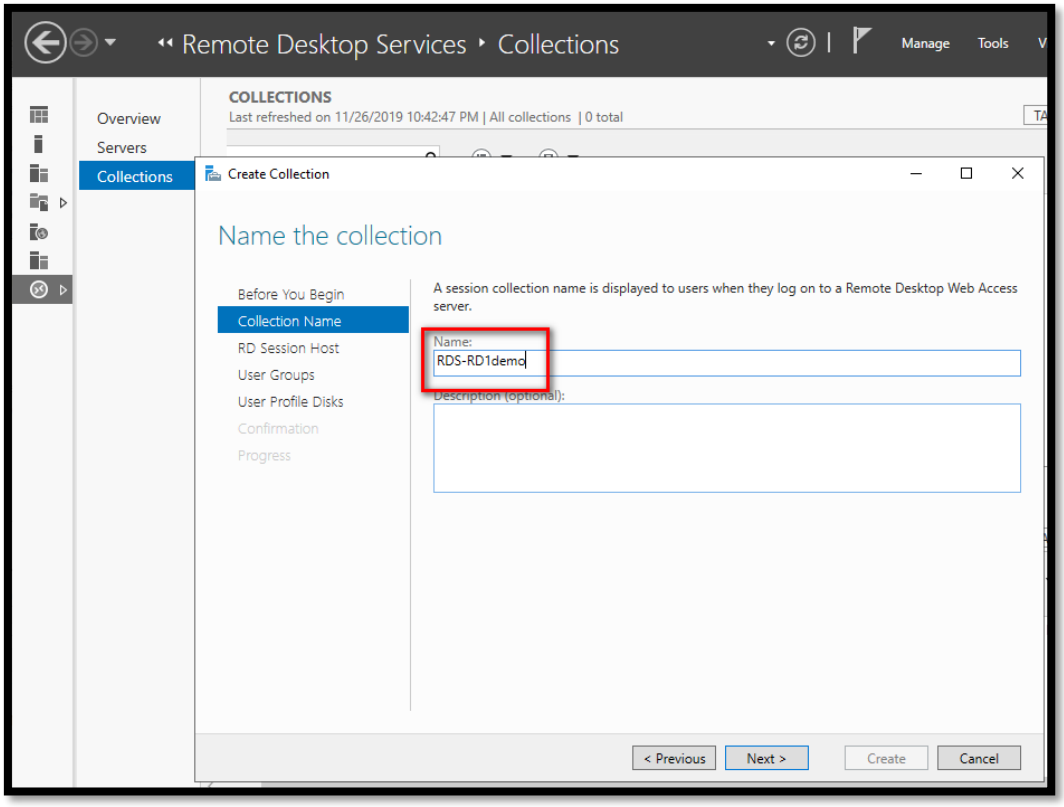
It is at the collection level that the use of User Profile Disks (UPDs) and applications published in RemoteApp via Web Access is configured.

Create a collection

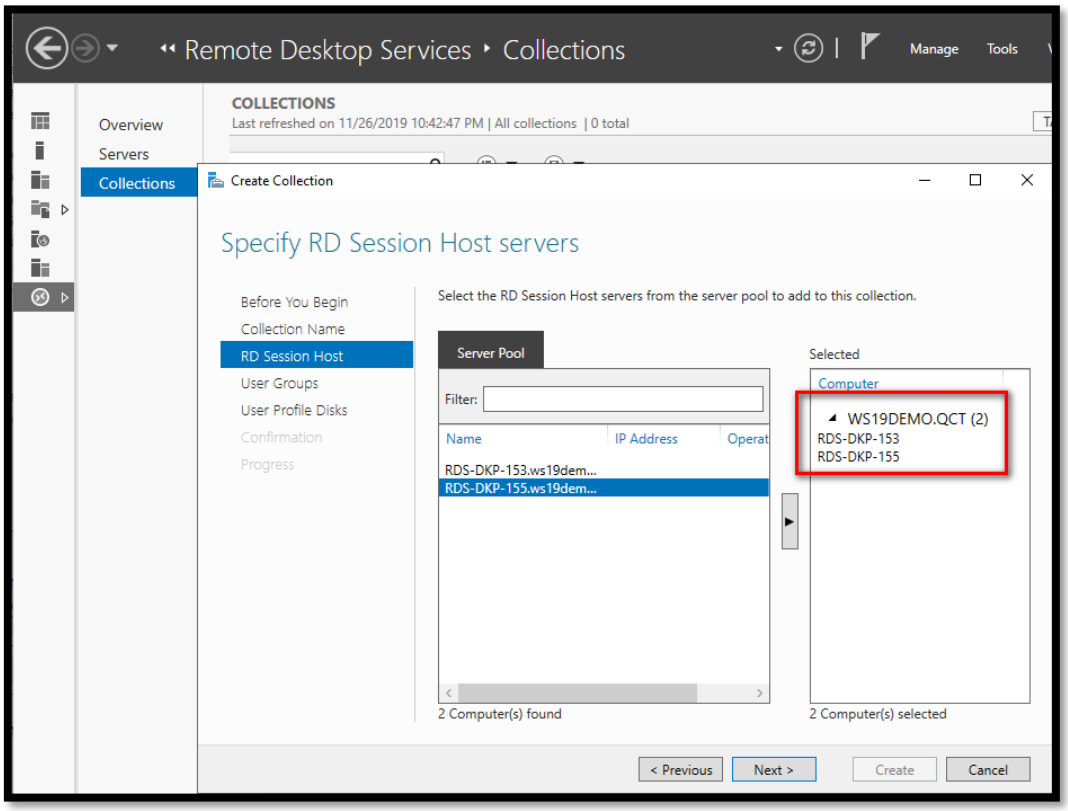
1. From the Server Manager on the collection management page, click on TASKS and Create a collection of sessions.



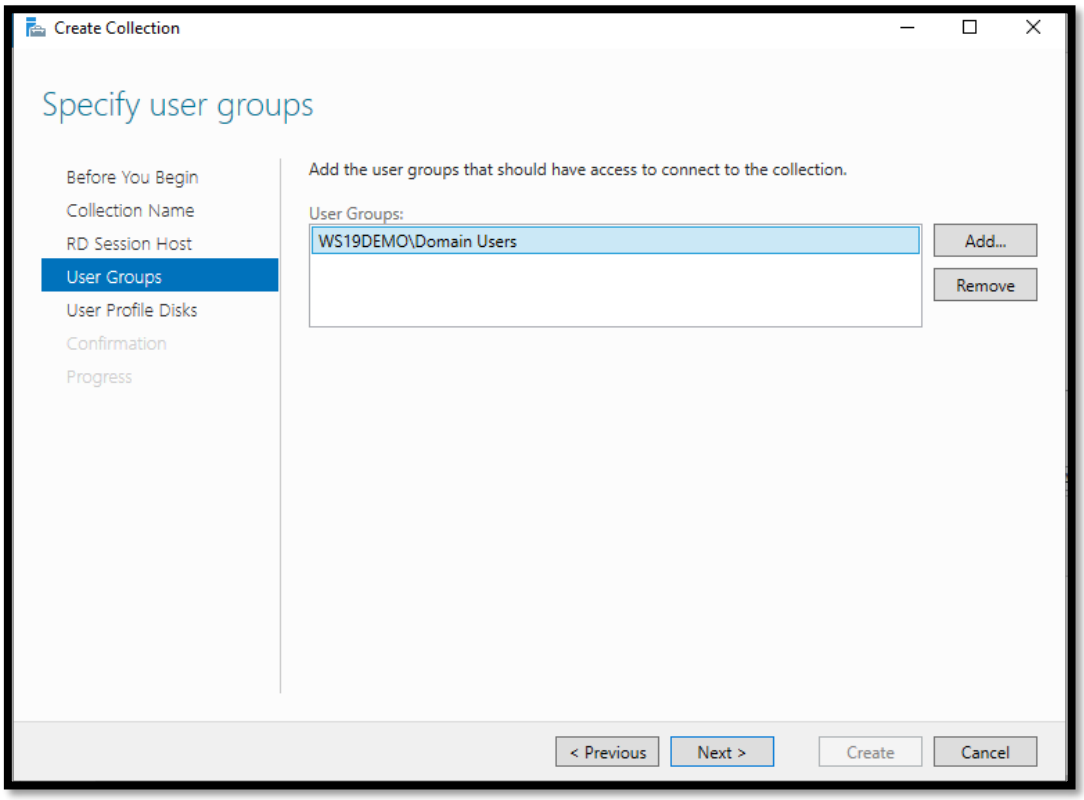
2. Enter the name of the collection and click Next.



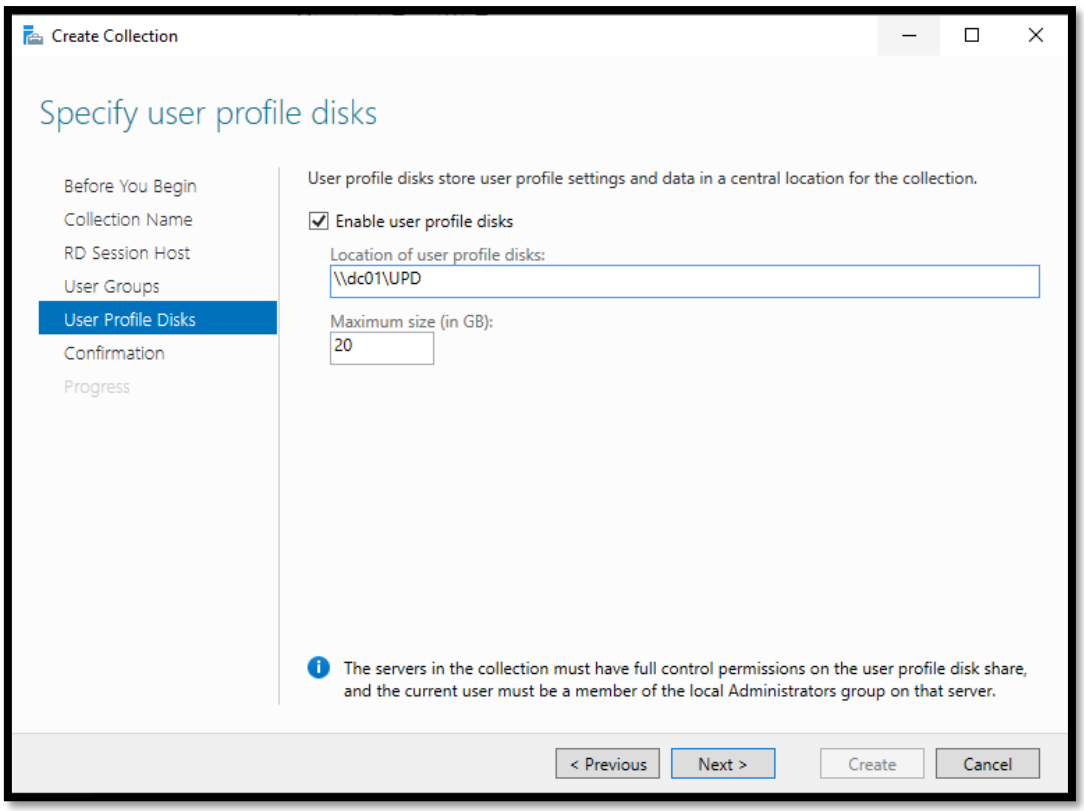
3. Add the Remote Desktop Session Host servers from the collection and click Next.



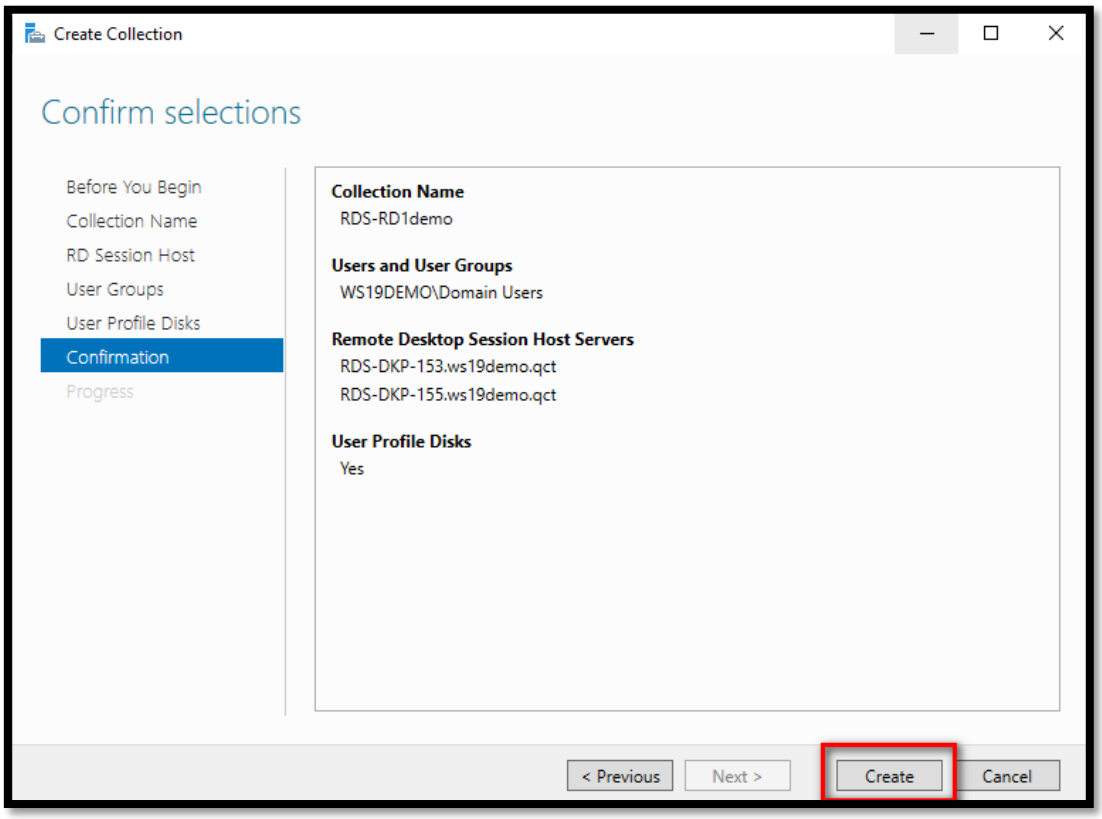
4. Specify the allowed user group(s) to connect to the collection and click Next.



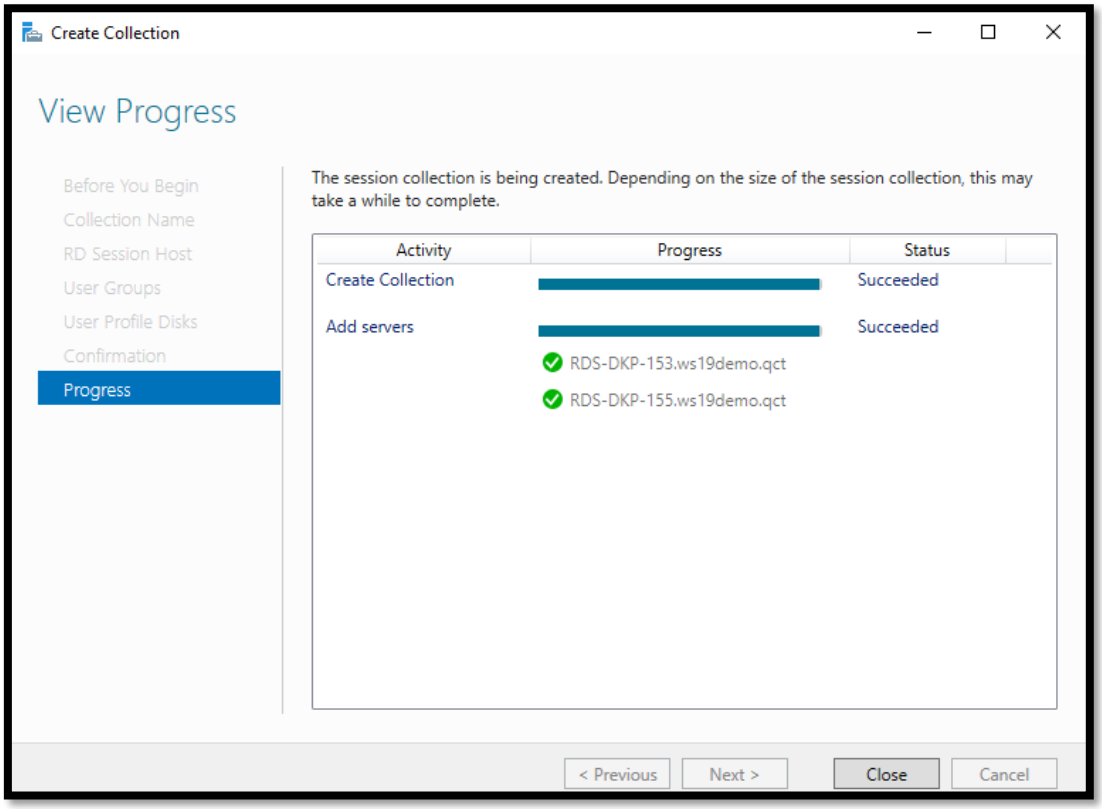
5. Check the [Enable user profile disks] box, specify the share for storing UPD, enter the maximum size of a disk and click Next.



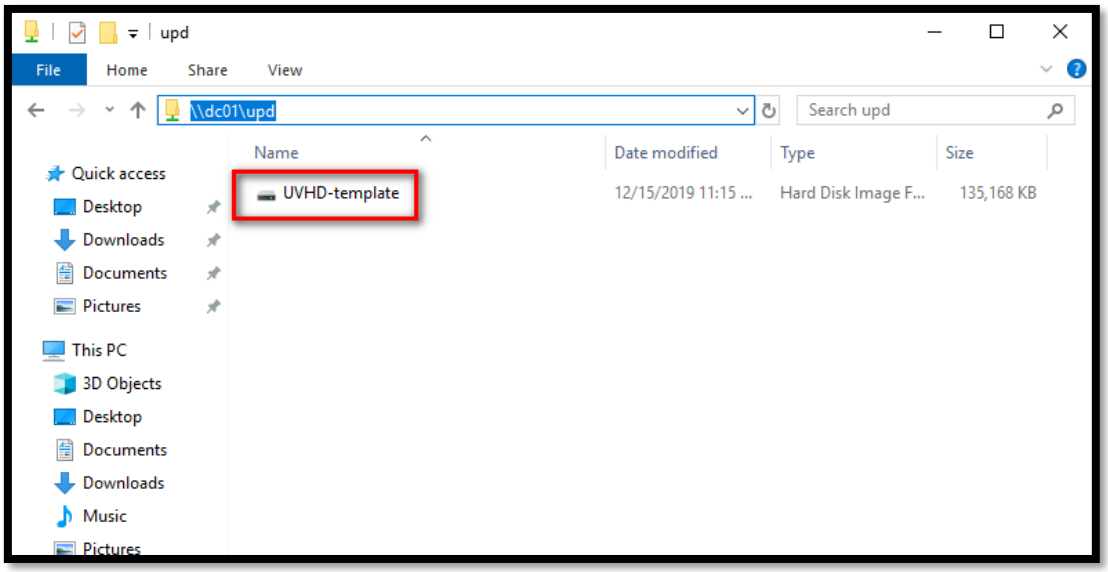
6. Click Create.



7. Check that the collection is ready, and click on Close.

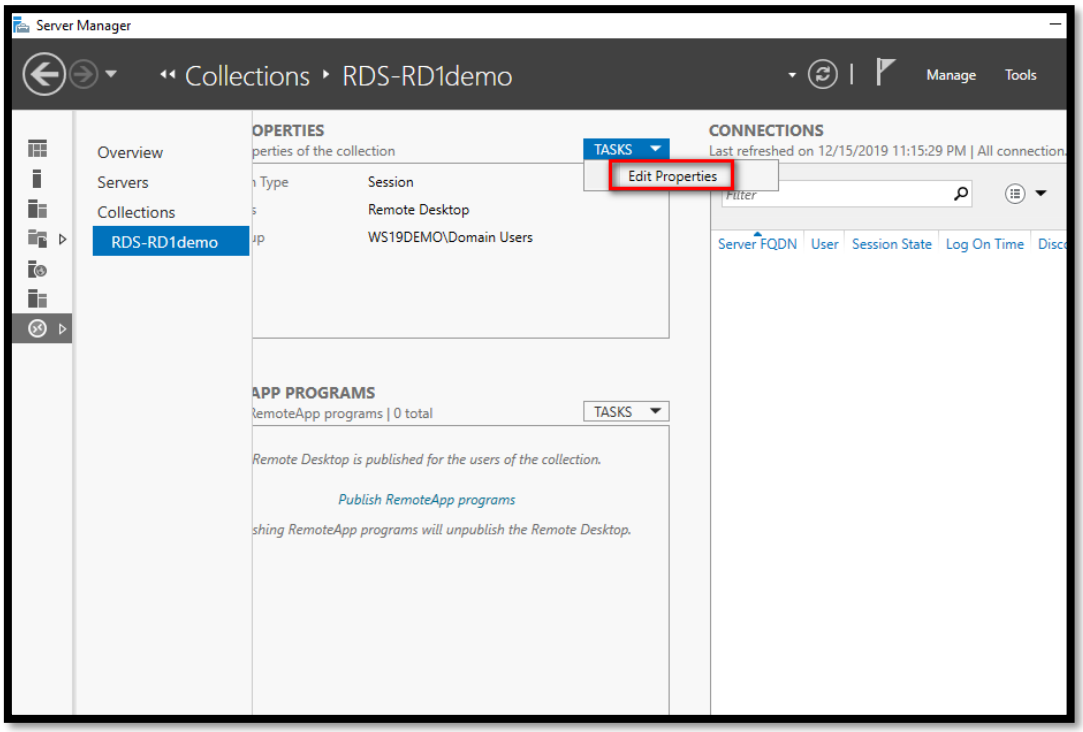


8. Open the parameter folder for storing UPD, a disk named UVHD-template.vhdx is created. It corresponds to the Default Profile folder on a computer.

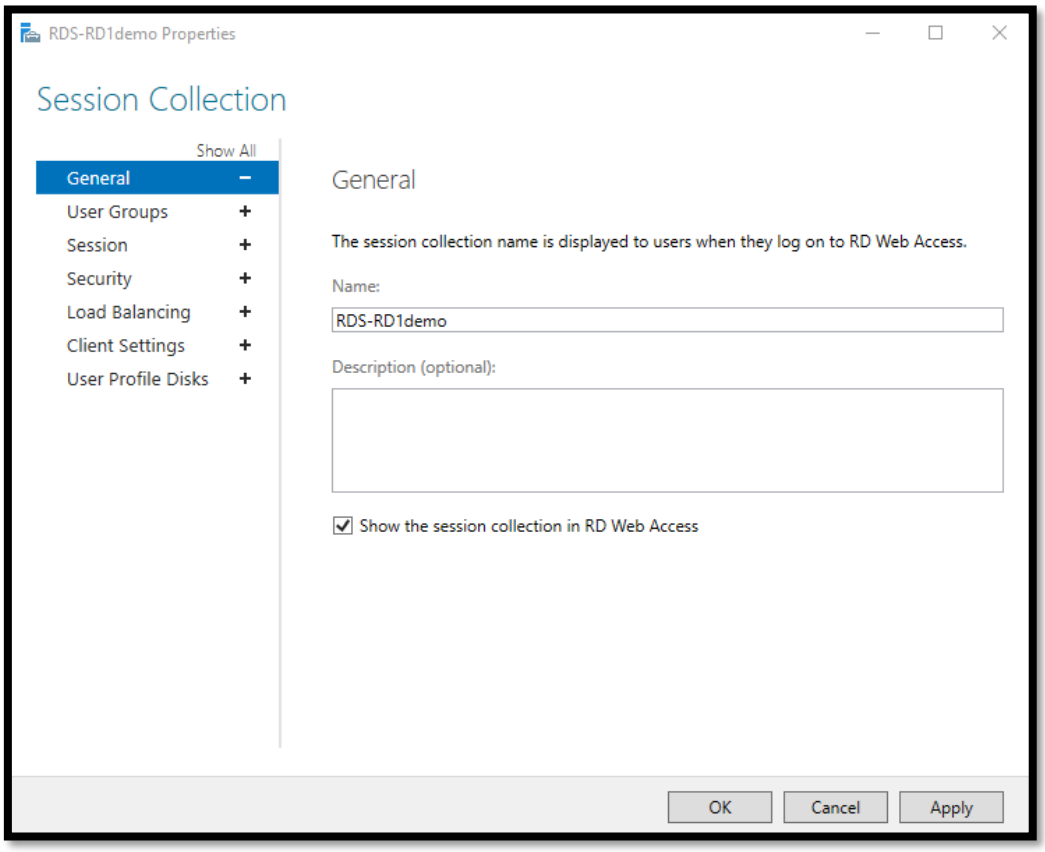


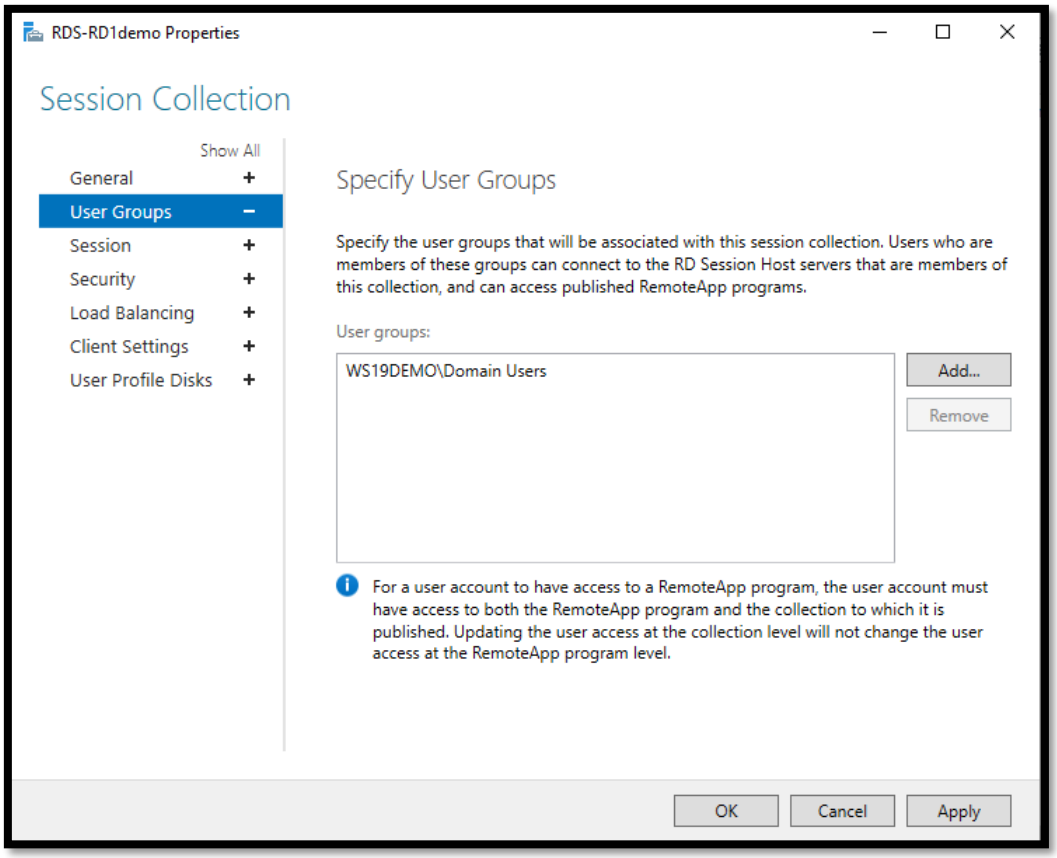
Edit a collection

1. From the page of the collection, on the page PROPERTIES insert, click on TASKS / Edit Properties.

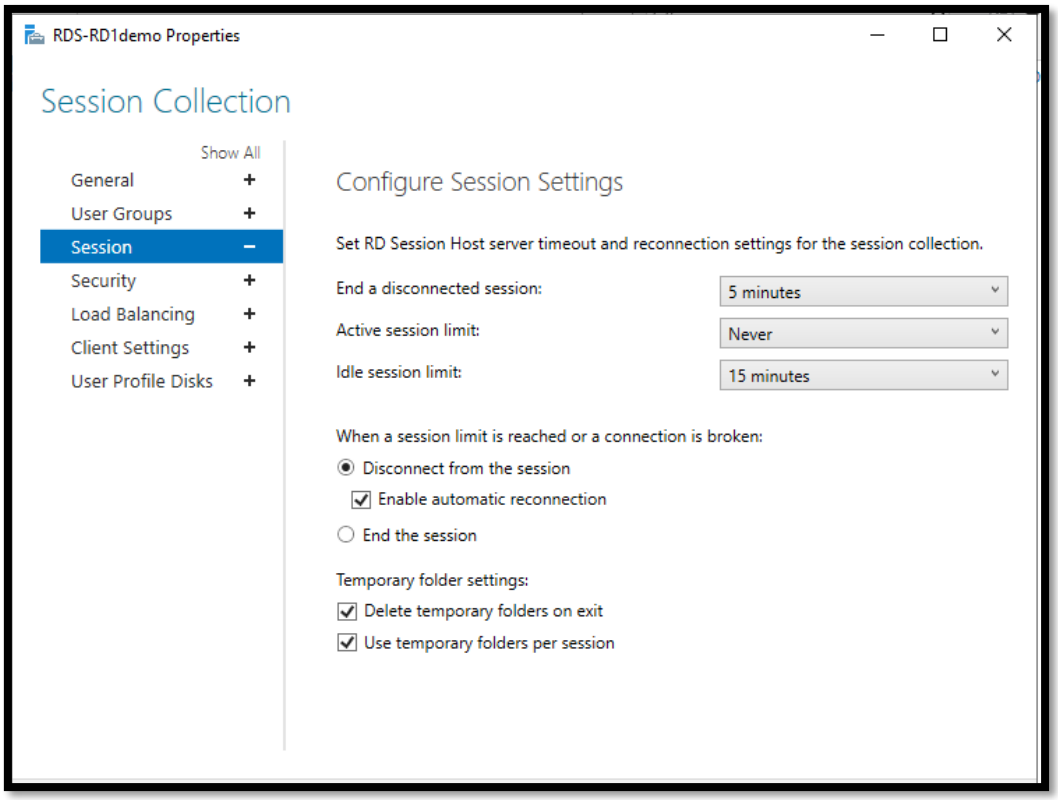


2. You can change the name the user groups are allowed to connect to.

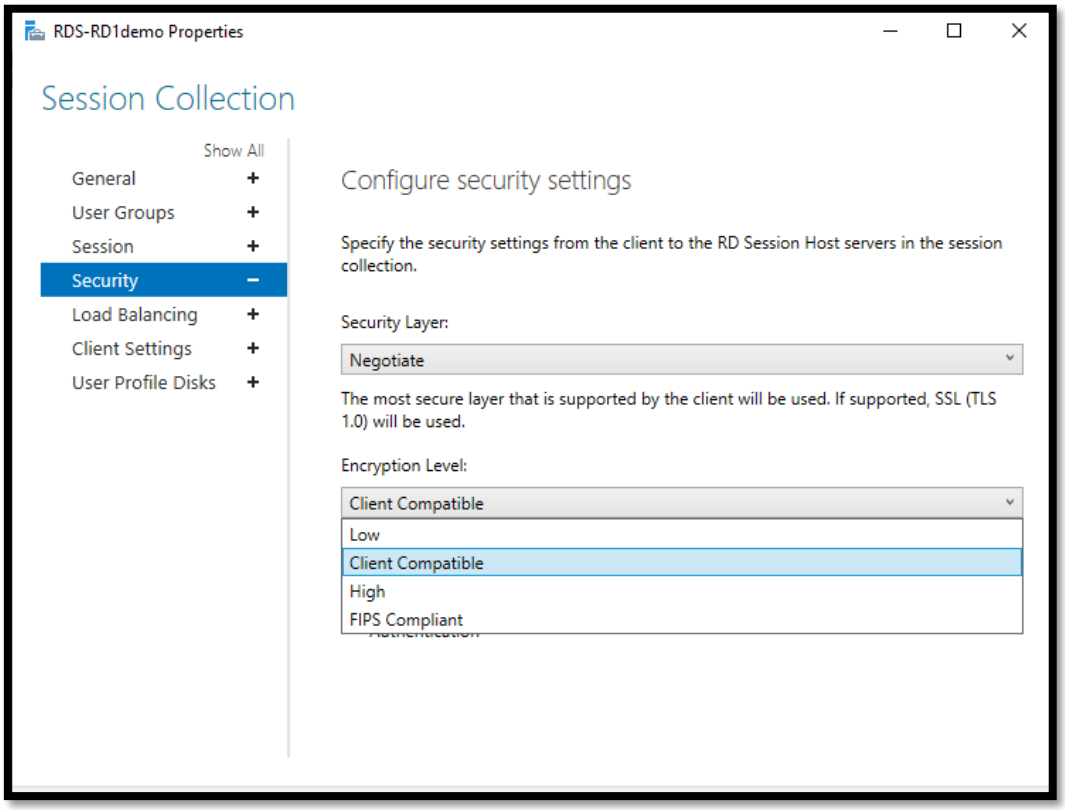

RDS-RD1demo Properties
Session Collection
Show All
General
User Groups
Session
Security
Load Balancing
Client Settings
User Profile Disks
General
The session collection name is displayed to users when they log on to RD Web Access.
Name:
RDS-RD1demo
Description (optional):
Show the session collection in RD Web Access
OK
Cancel
Apply


RDS-RD1demo Properties
Session Collection
Show All
General
User Groups
Session
Security
Load Balancing
Client Settings
User Profile Disks
Specify User Groups
Specify the user groups that will be associated with this session collection. Users who are members of these groups can connect to the RD Session Host servers that are members of this collection, and can access published RemoteApp programs.
User groups:
WS19DEMO\Domain Users
Add...
Remove
For a user account to have access to a RemoteApp program, the user account must have access to both the RemoteApp program and the collection to which it is published. Updating the user access at the collection level will not change the user access at the RemoteApp program level.
OK
Cancel
Apply

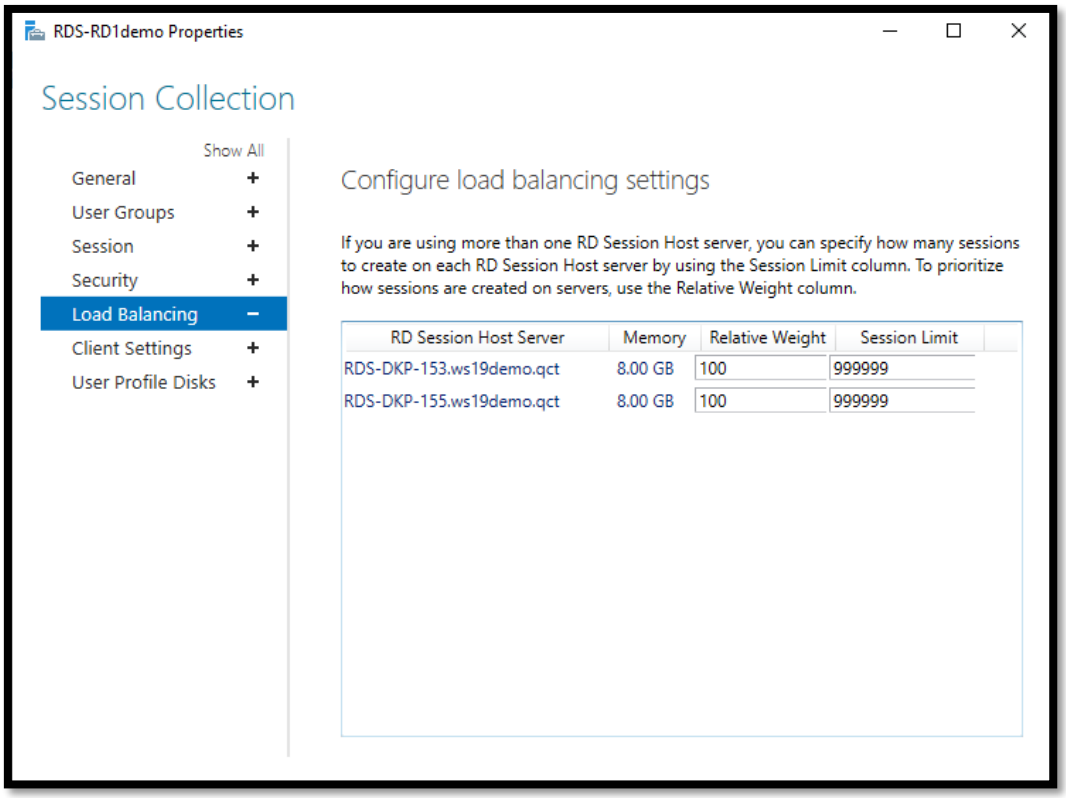
3. Session Section: Setting the Expiration and Reconnection Time on Collection Hosts, Setting Temporary Folder Behaviour.



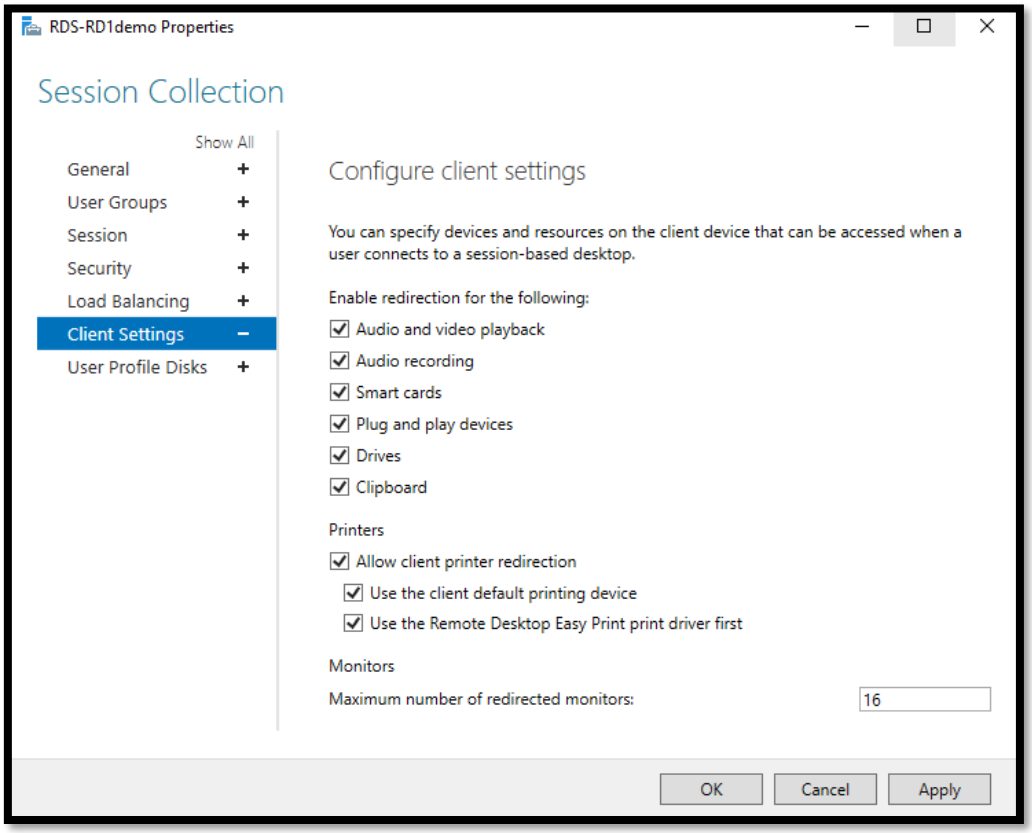
4. Security Section: Configuration of security layers between the RDP client and the servers.



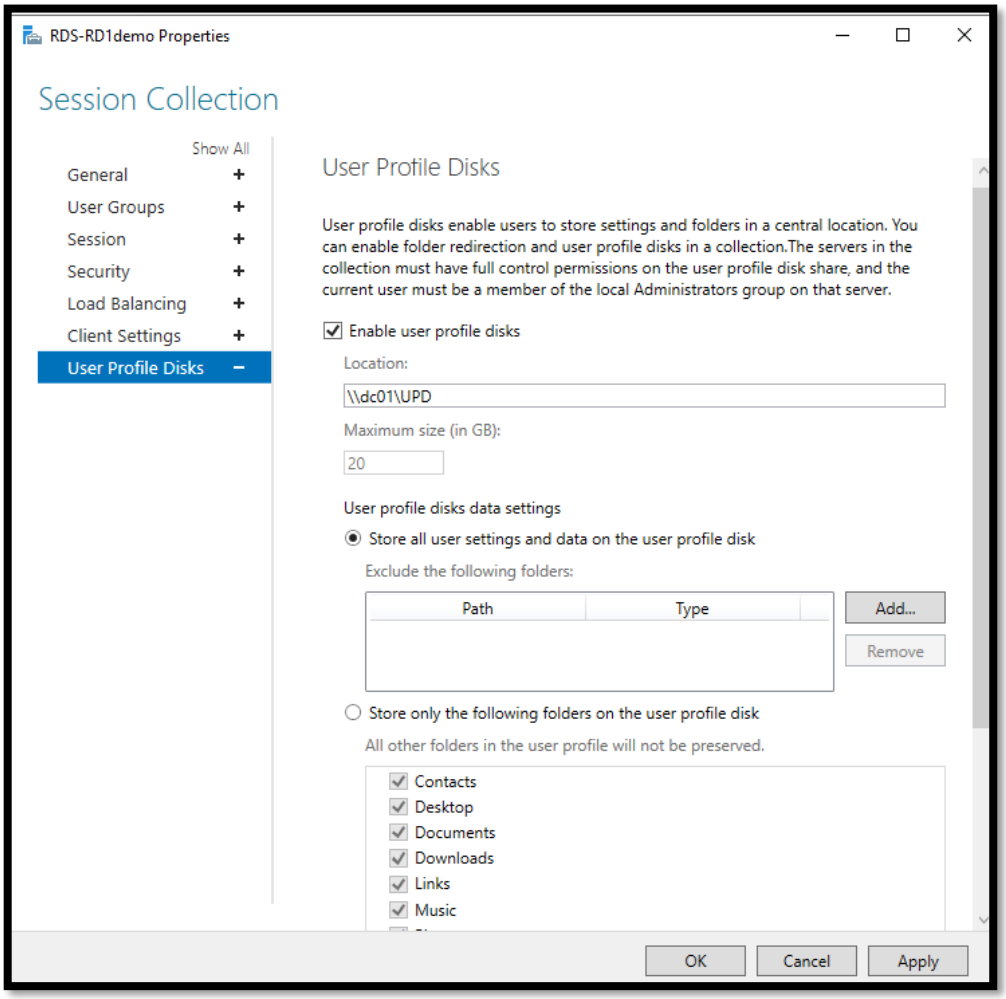
5. Load Balancing Section: In case of different power server usage, it is possible to prioritize a server and set a session limit.



6. Client Setting Section 1: Configuring Device and Printer Redirection.



7. User Profile Disks Section: Configuring UPDs (Size, Folder Exclusions, Location …).



The RDS farm is now usable.

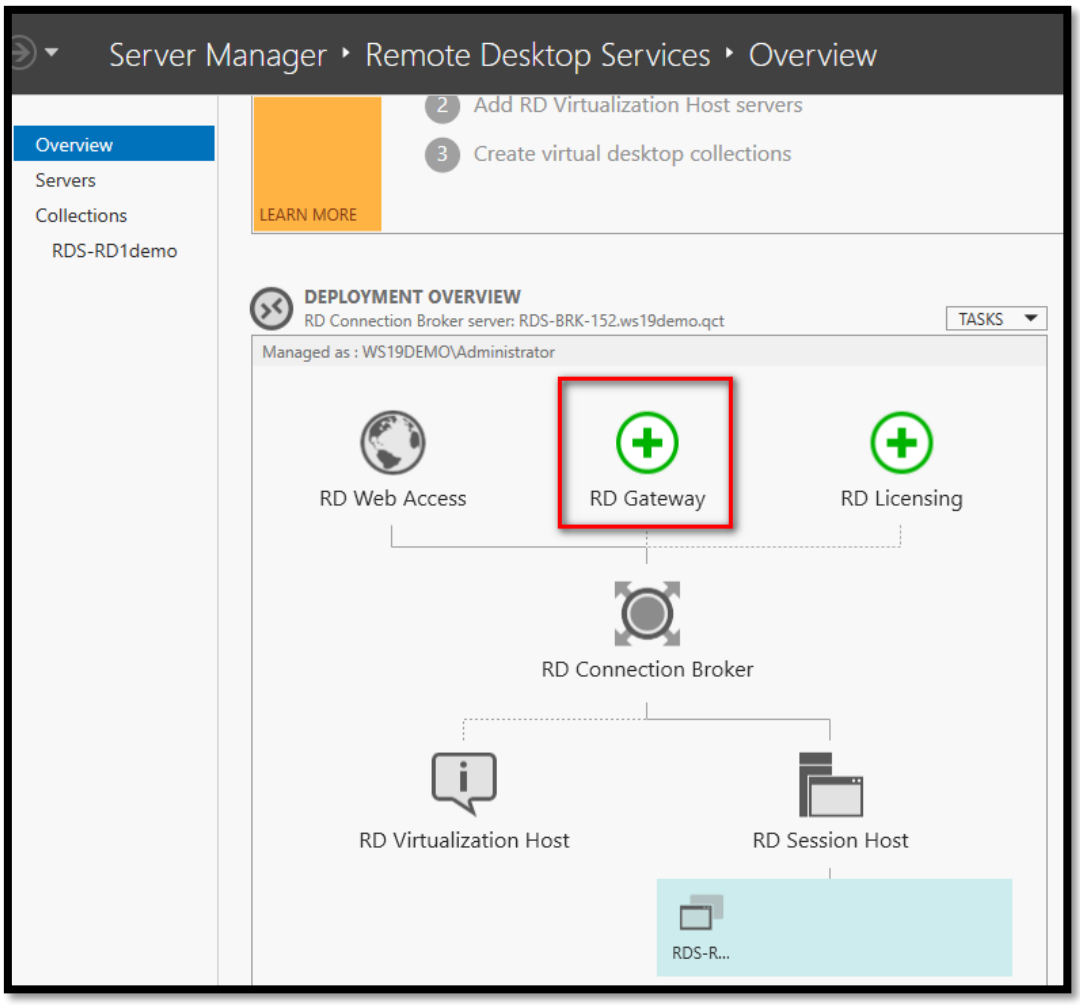
It is possible to deploy several collections on the same RDS deployment, which allows pooling broker services, web access. The remote desktop session hosts are dedicated to a collection.

Remote Desktop Gateway – Gateway RDS

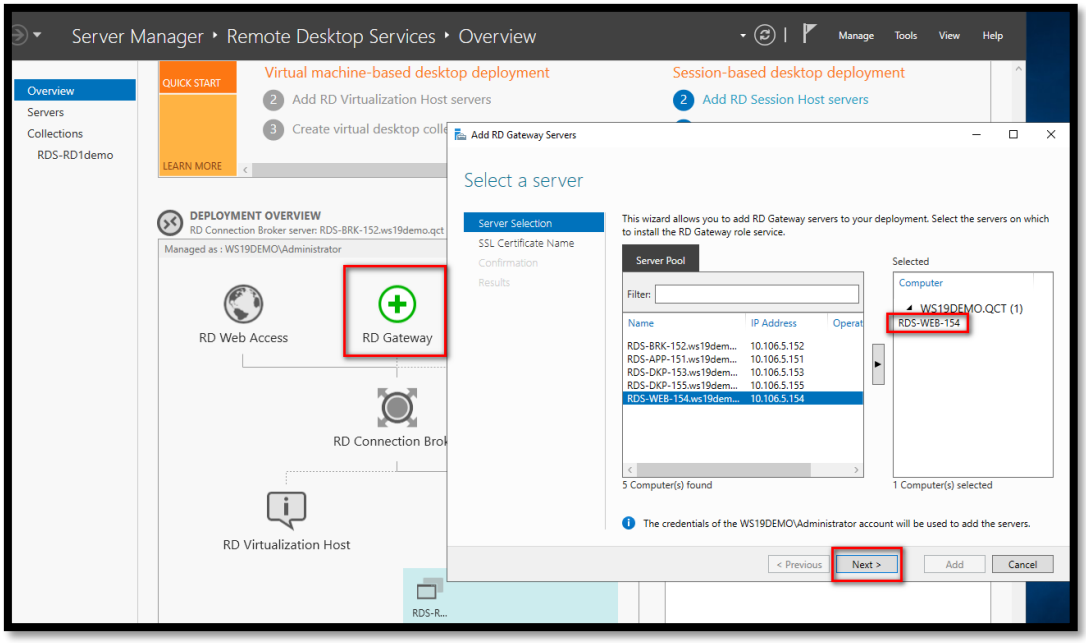
The Remote Desktop Gateway allows access to resources (servers / computers) accessible from outside the enterprise on port 443 (https) without the need to establish a VPN connection and applying security strategies.

Remote Desktop Services Gateway Installation

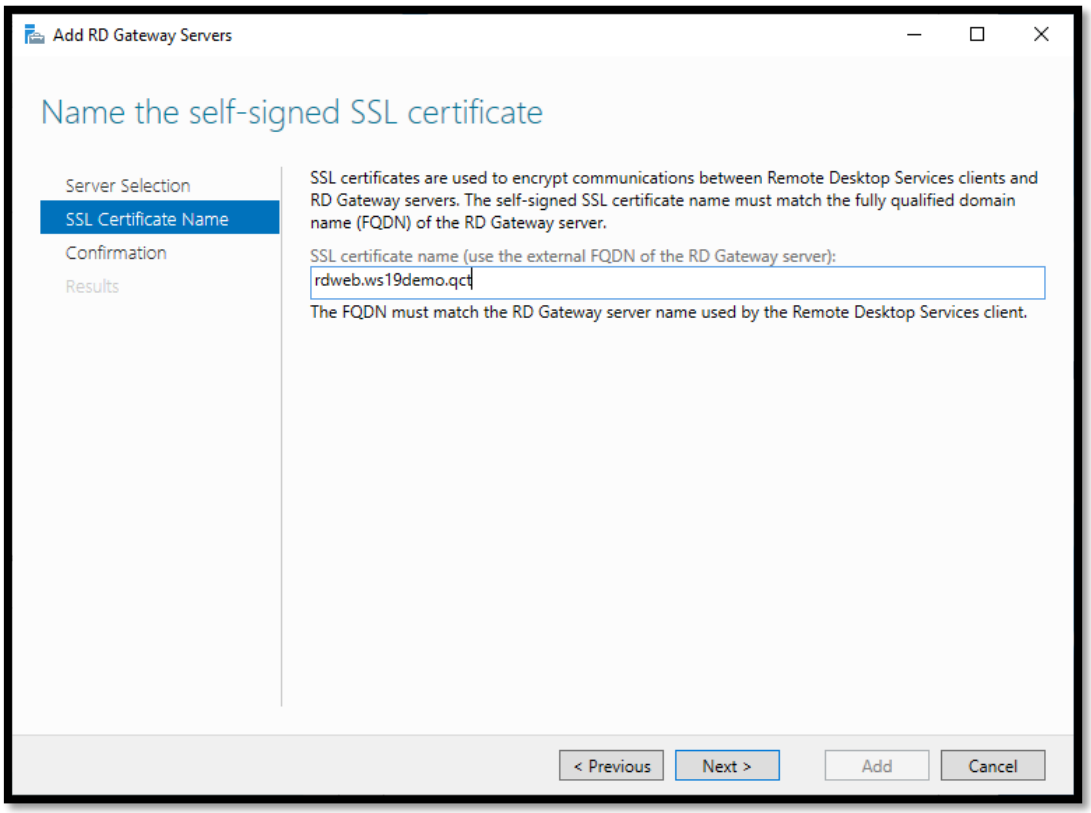
1. Go to Overview of Remote Desktop Services and click on Service Gateway. This will open the role installation wizard for the RDS farm.



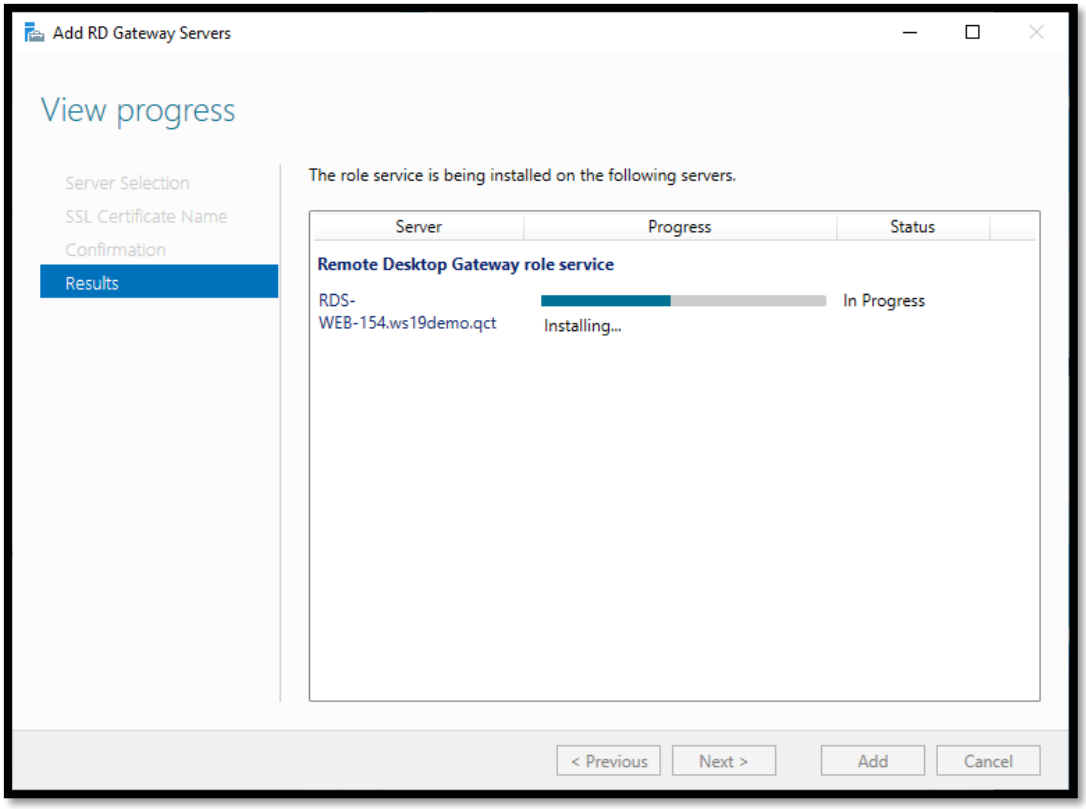
2. Select server where the role is to be installed and click Next.



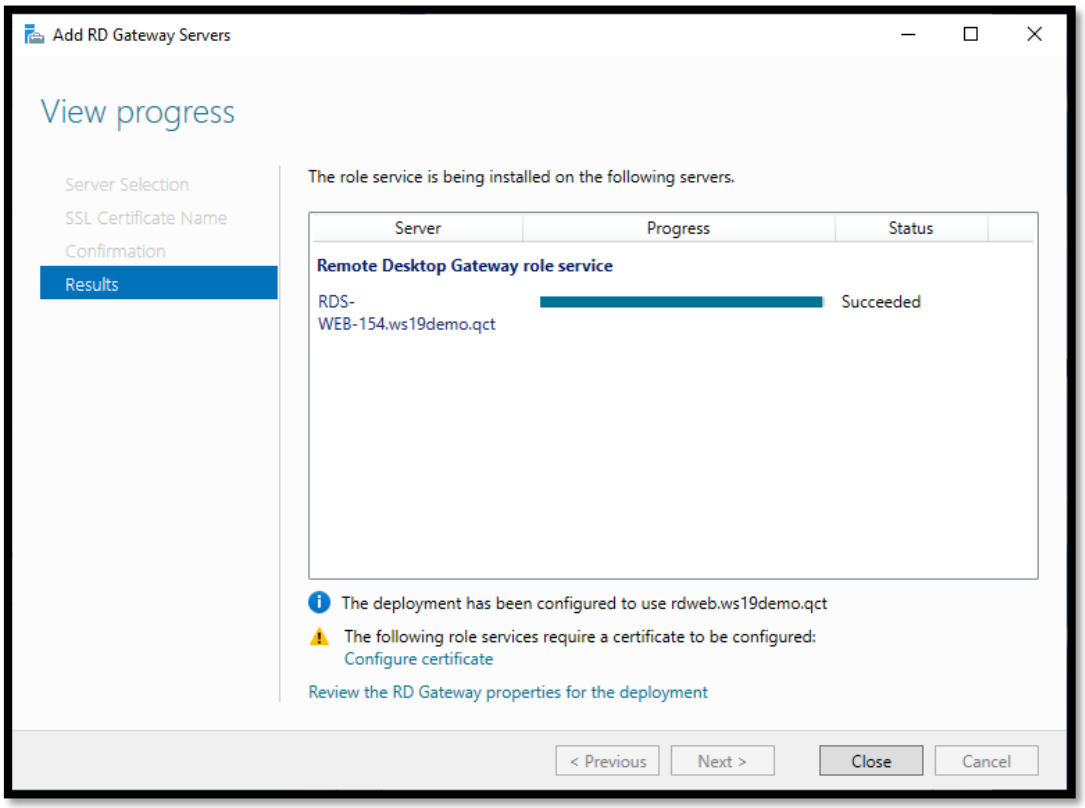
3. Enter the name of the SSL certificate (usually the publication name on the internet) and click Next.



4. Click Add to start the installation.



5. Installation completed, click Close.



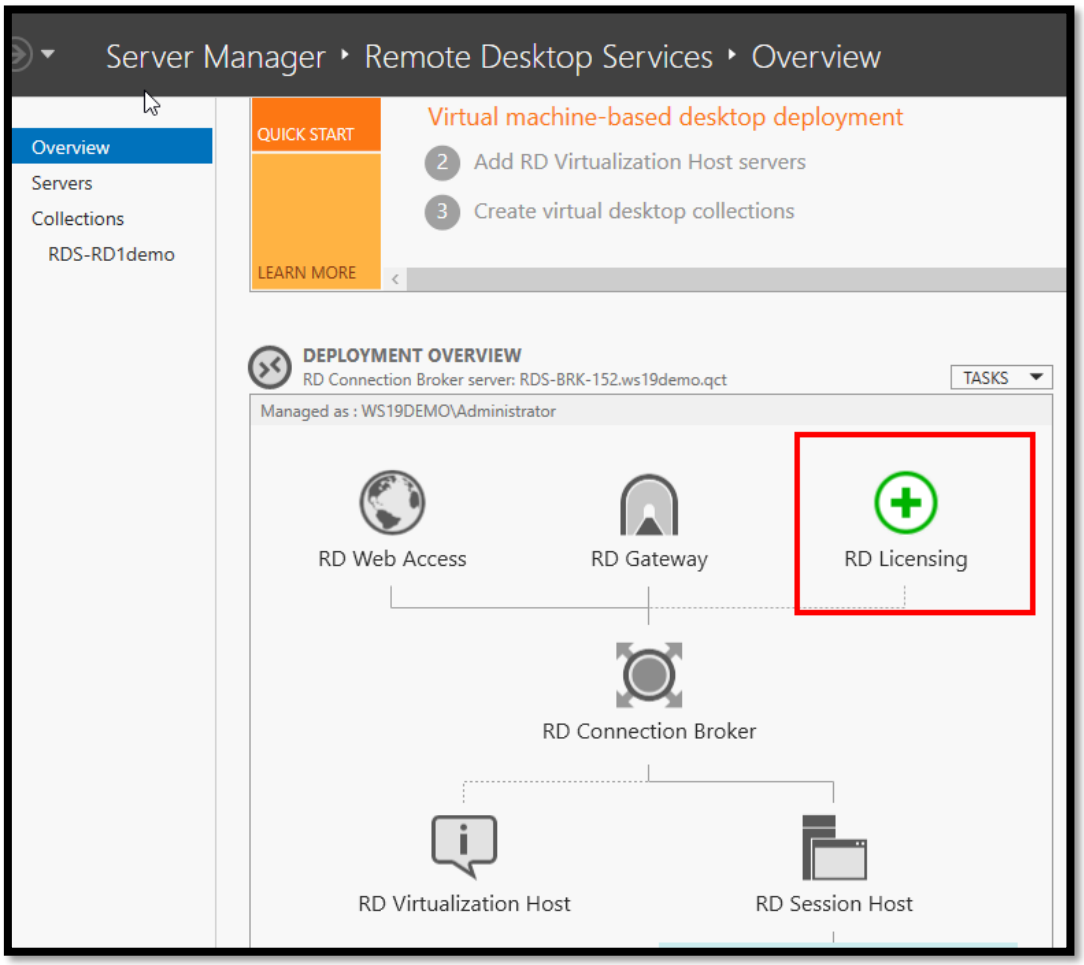
Remote Desktop Services License Manager

The license manager allows users or devices that connect to the RDS farm to issue an access license (CAL).

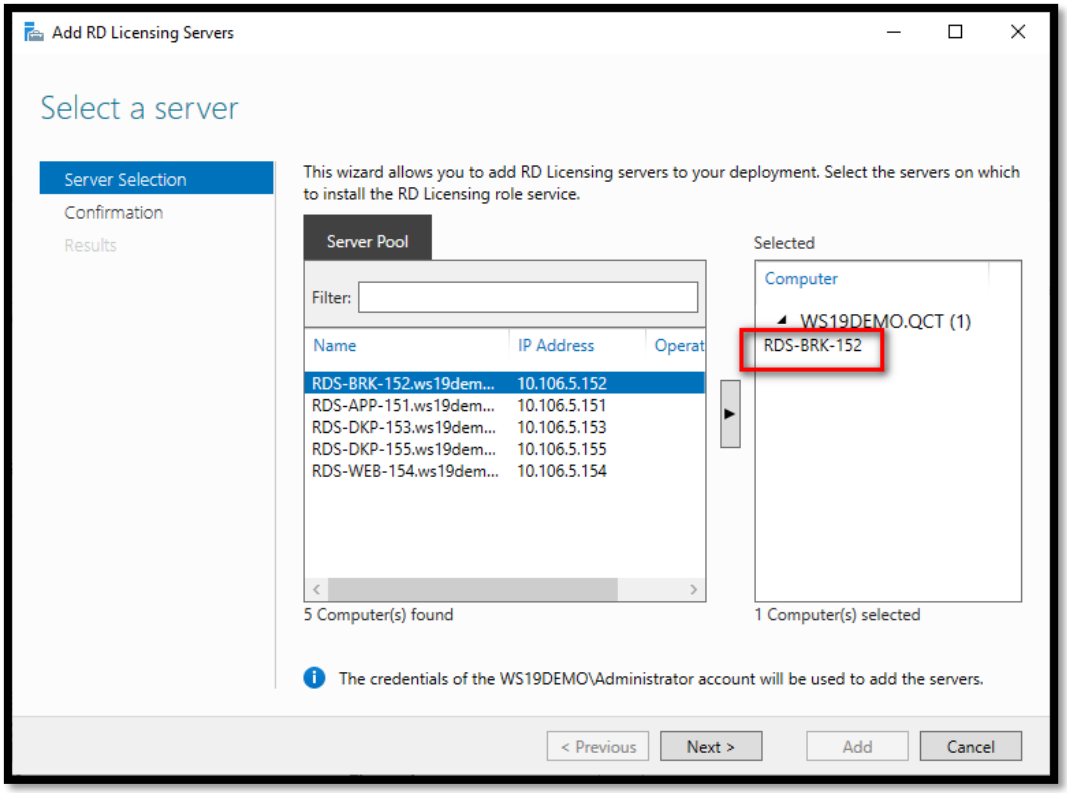
Only one licensing mode for the RDS farm can be configured: users or devices. A licensed server can distribute several types of licenses and different versions (2008/2012 …).

Installation

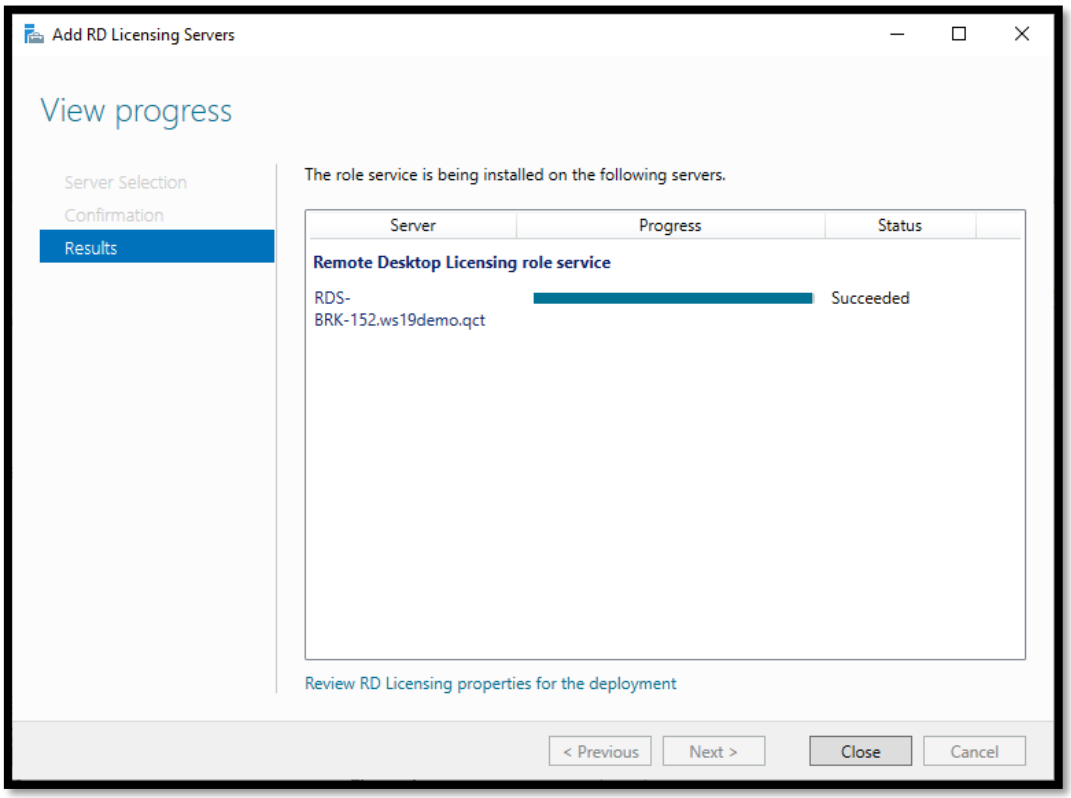
1. From Server Manager, on the RDS farm overview, click License Manager to open the wizard.



2. Add the server that will receive role and click Next.

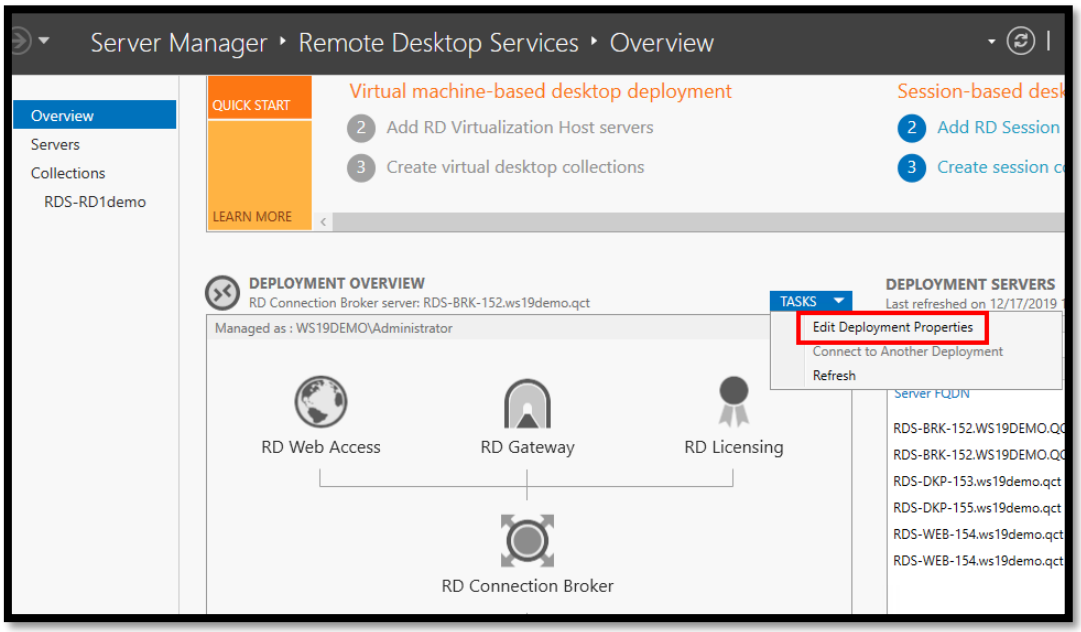


3. The installation is complete, click Close to exit the wizard.

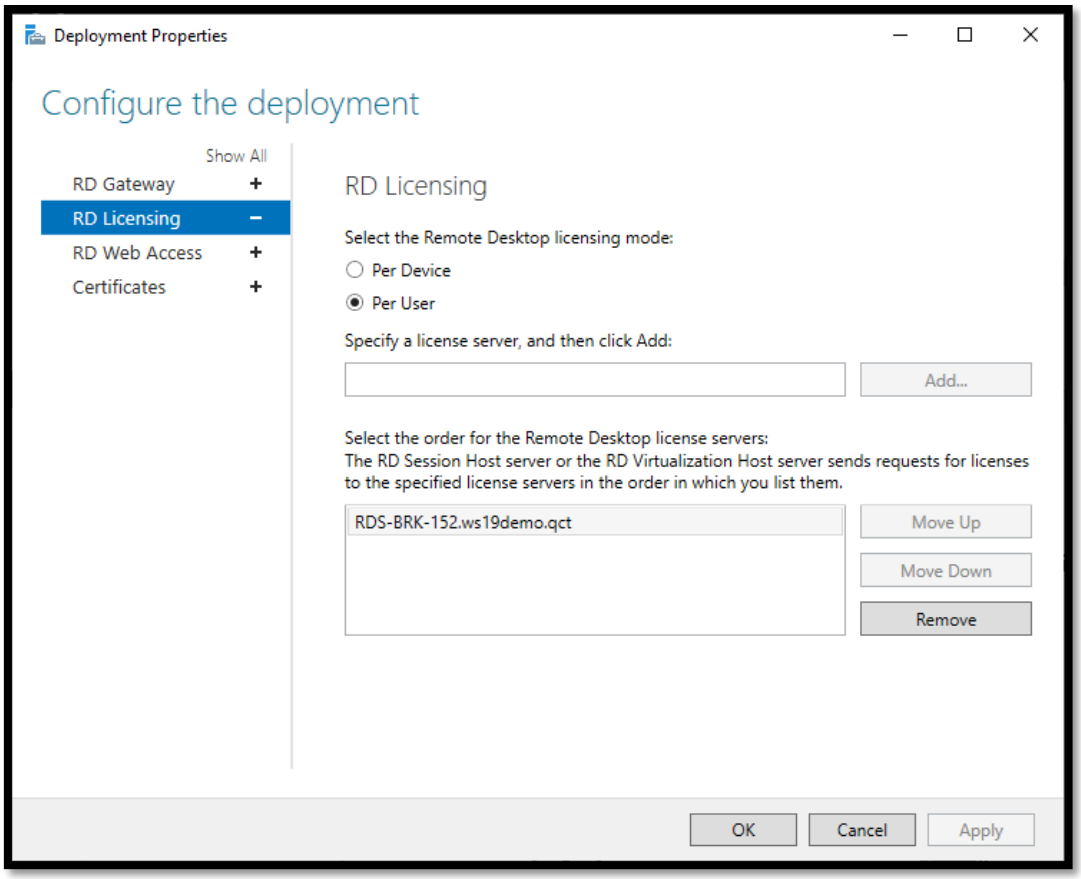


Configuring the Remote Desktop Services Licensing Mode

1. From the overview, deployment, click on TASKS / Edit Deployment Properties.

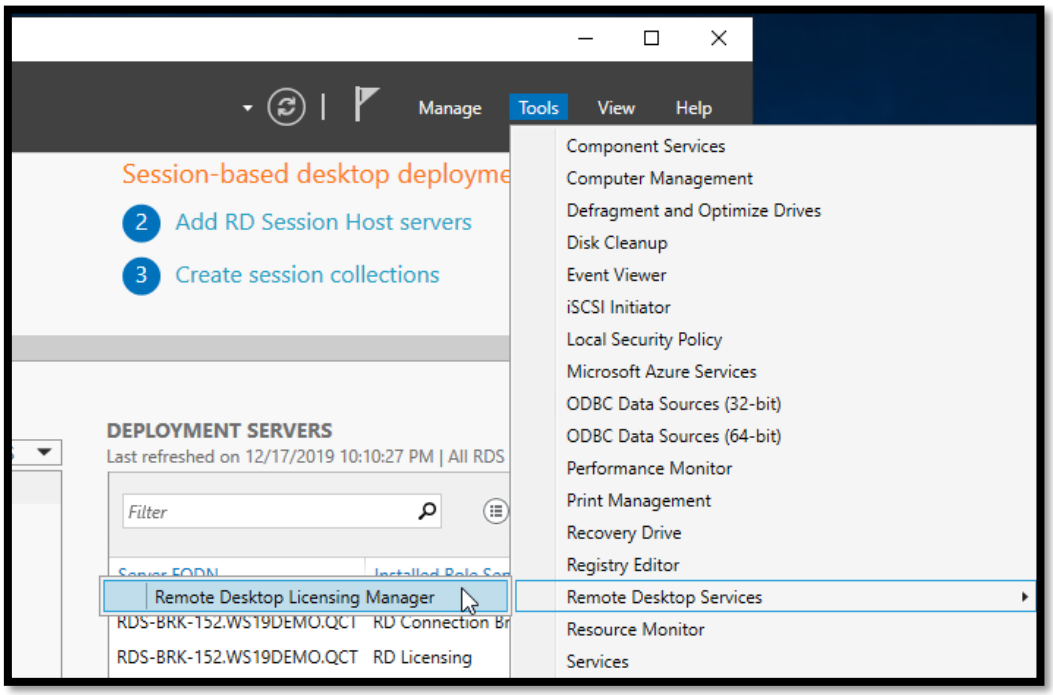


2. Select the license mode then click on Apply and OK.

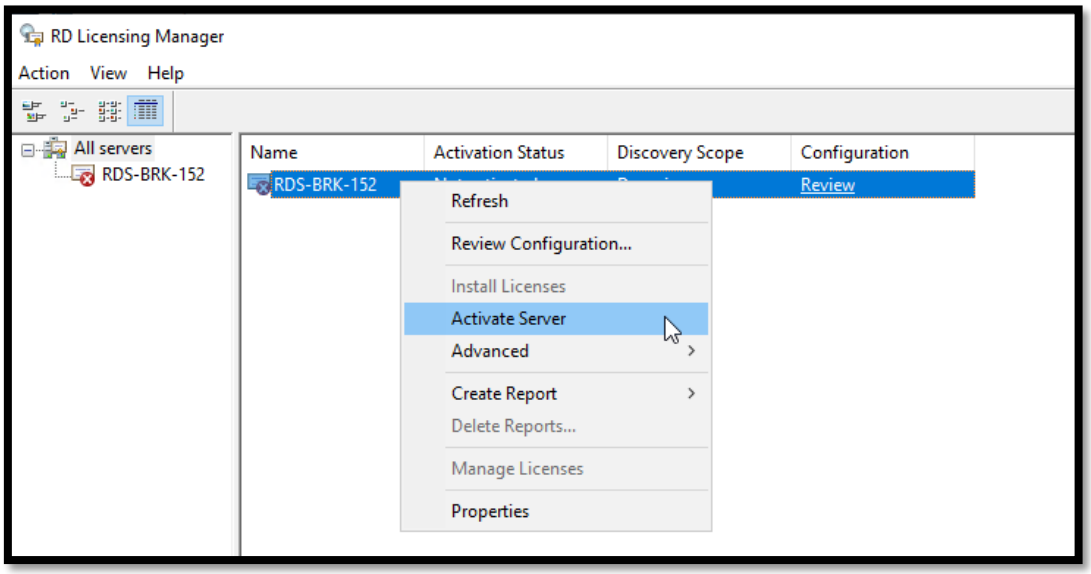


Add licenses

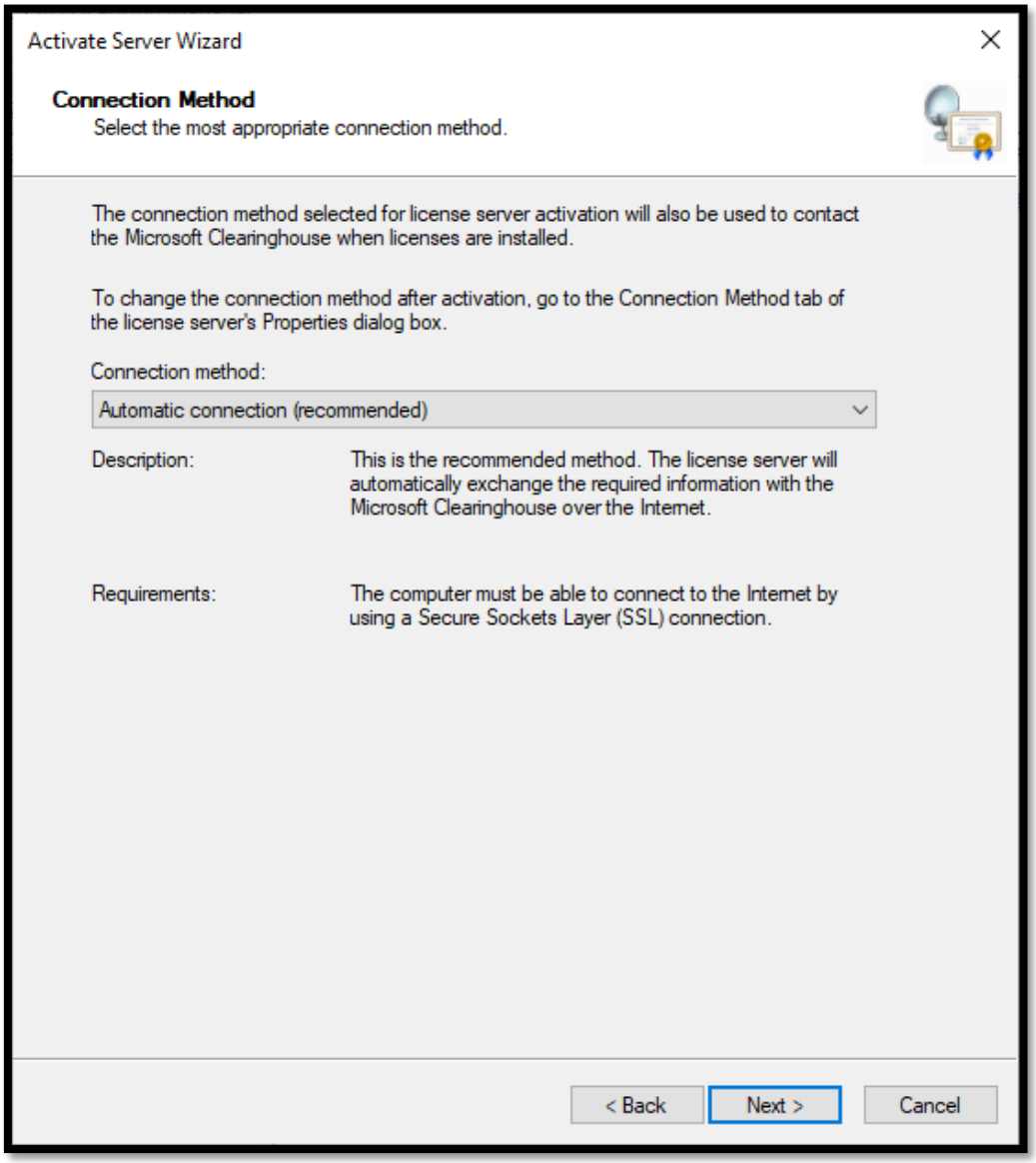
1. Open the console, from Server Manager, click Tools / Remote Desktop Services / Remote Desktop Licensing Manager.



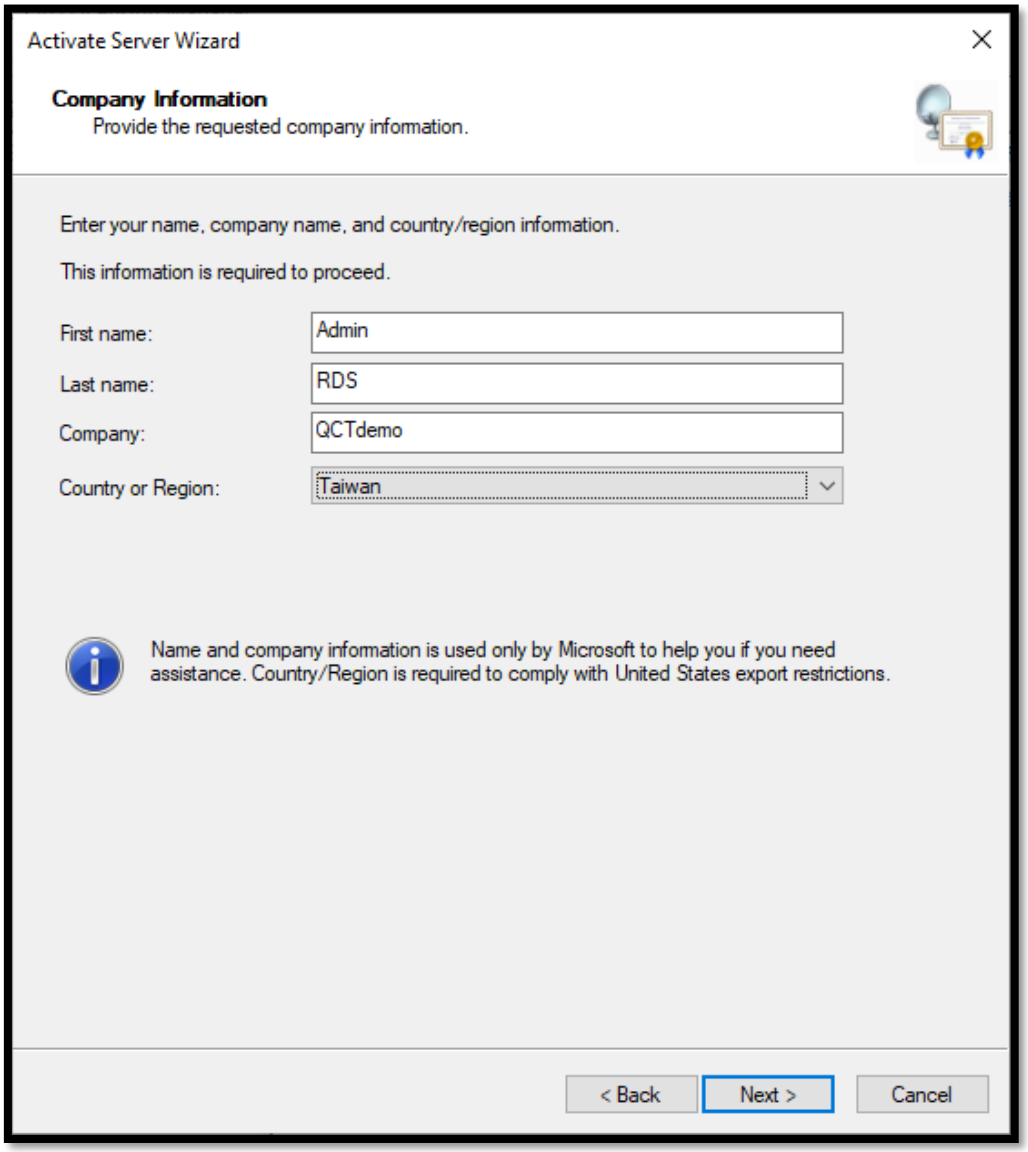
2. Before adding licenses, activate the server by right clicking on the server and clicking [Activate Server].



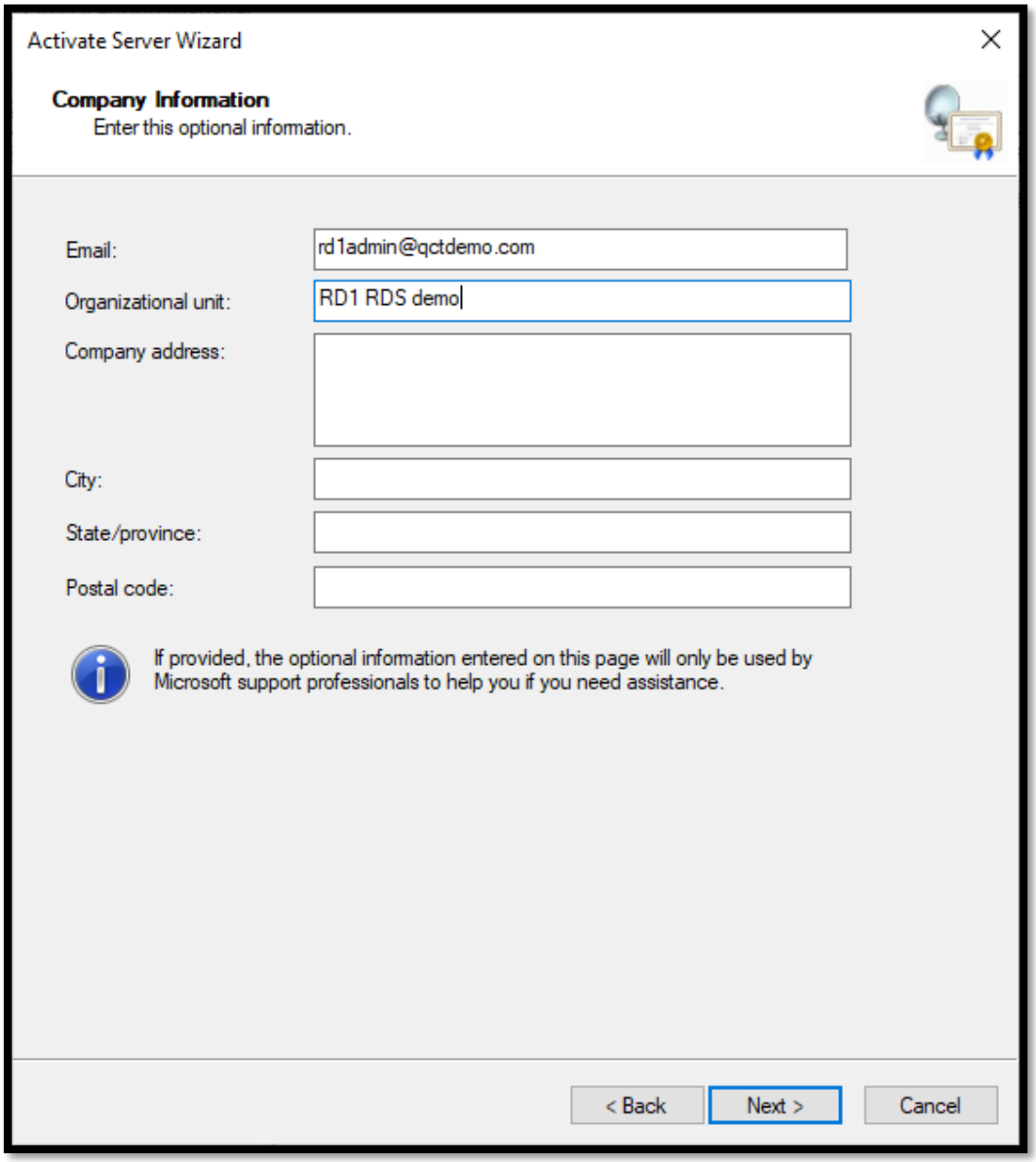
3. To leave the Connection Method screen, click Next.



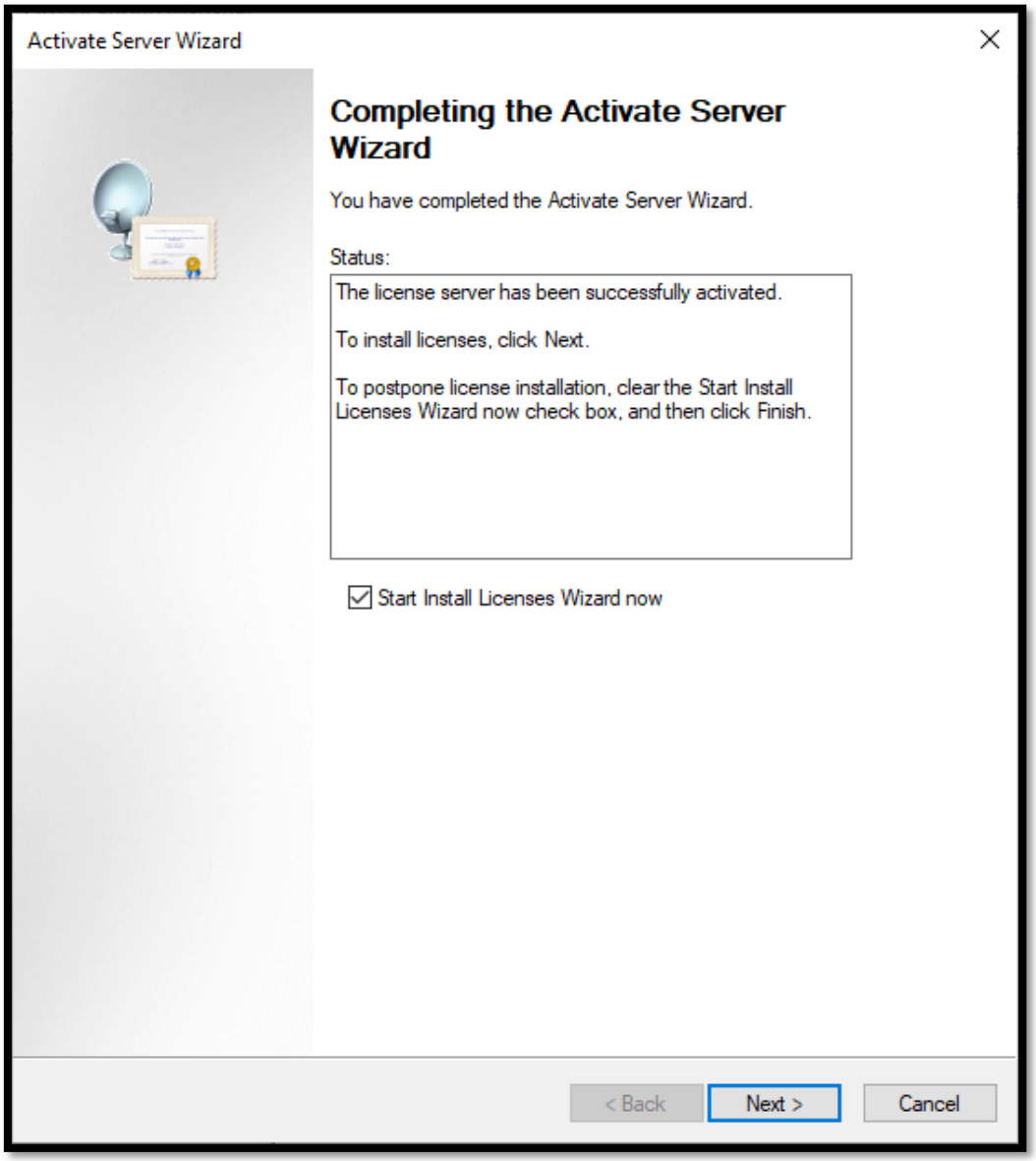
4. Enter Company Information and click Next.



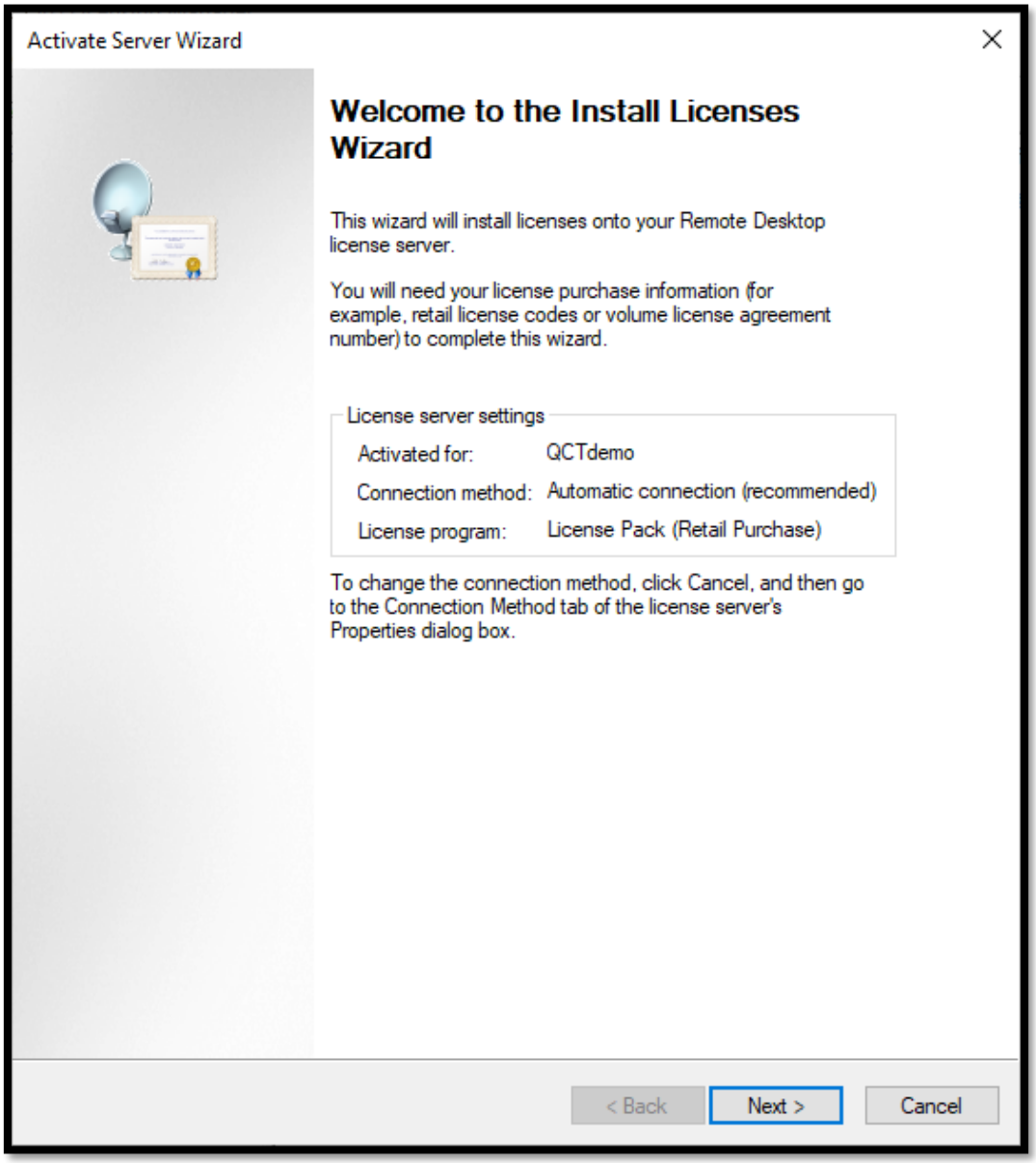
5. Enter contact information (optional) and click Next.



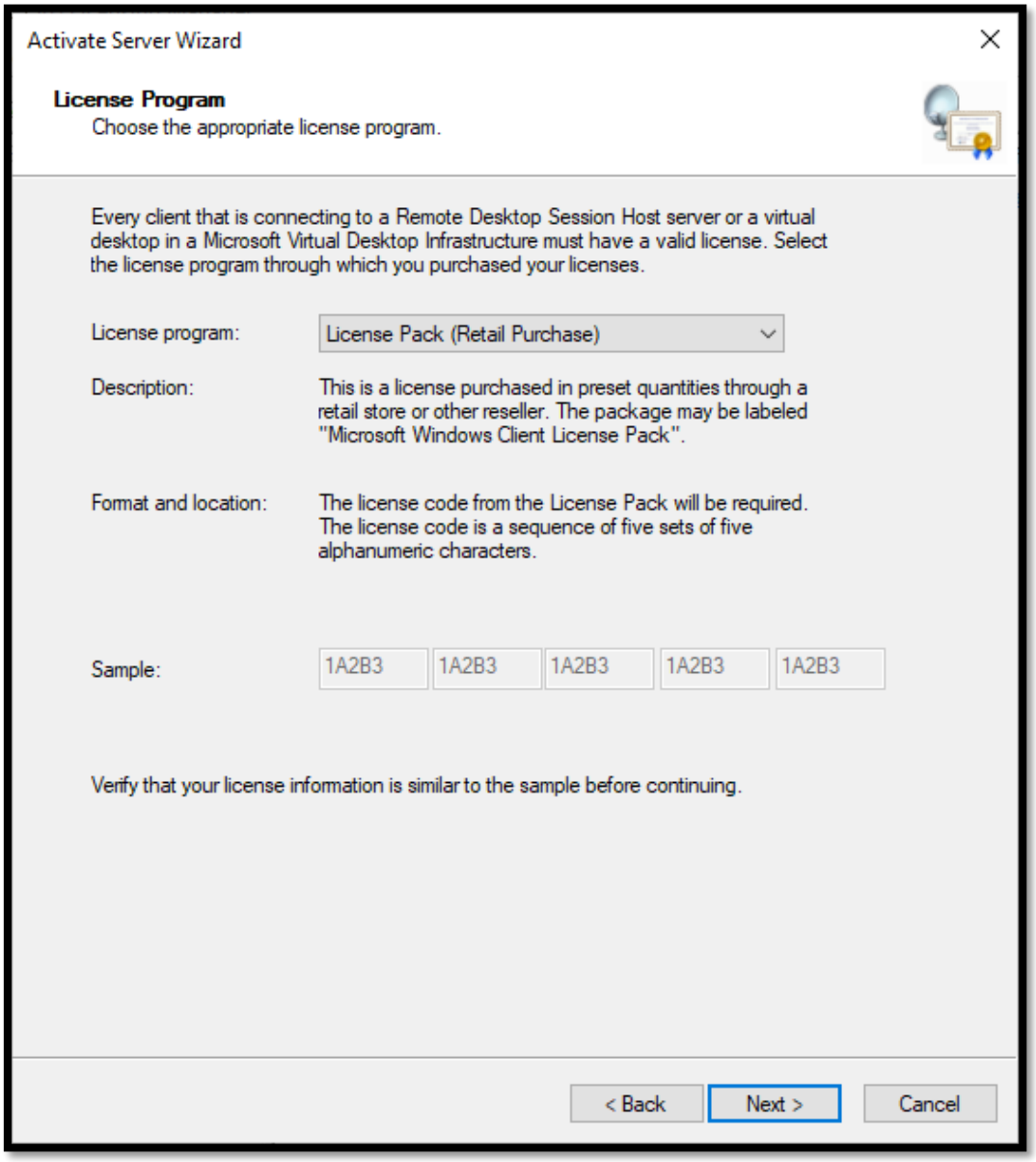
6. The server is now activated. When you click Next, the Install License Wizard will launch.



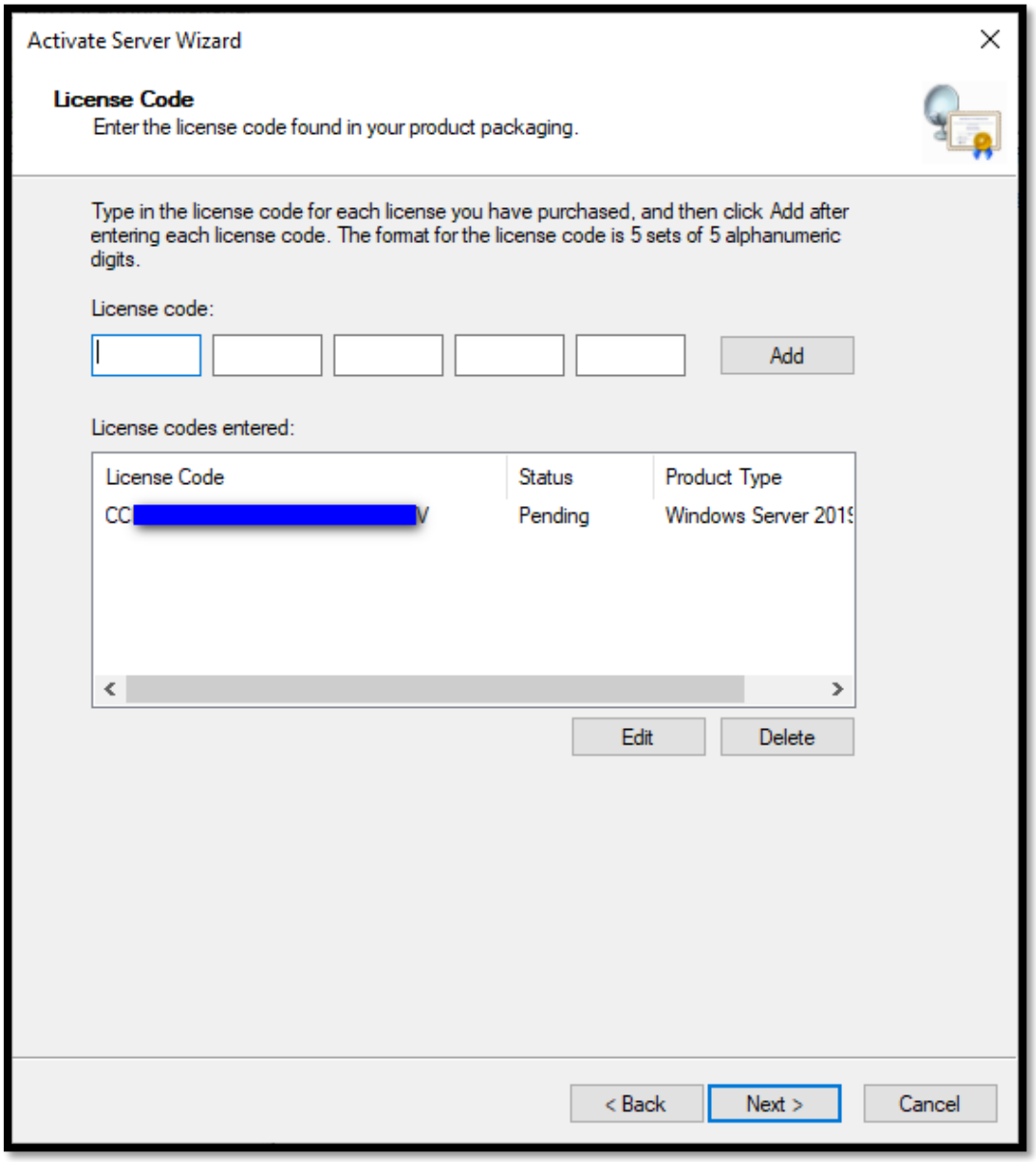
7. When the Install Licenses Wizard launches, click Next.



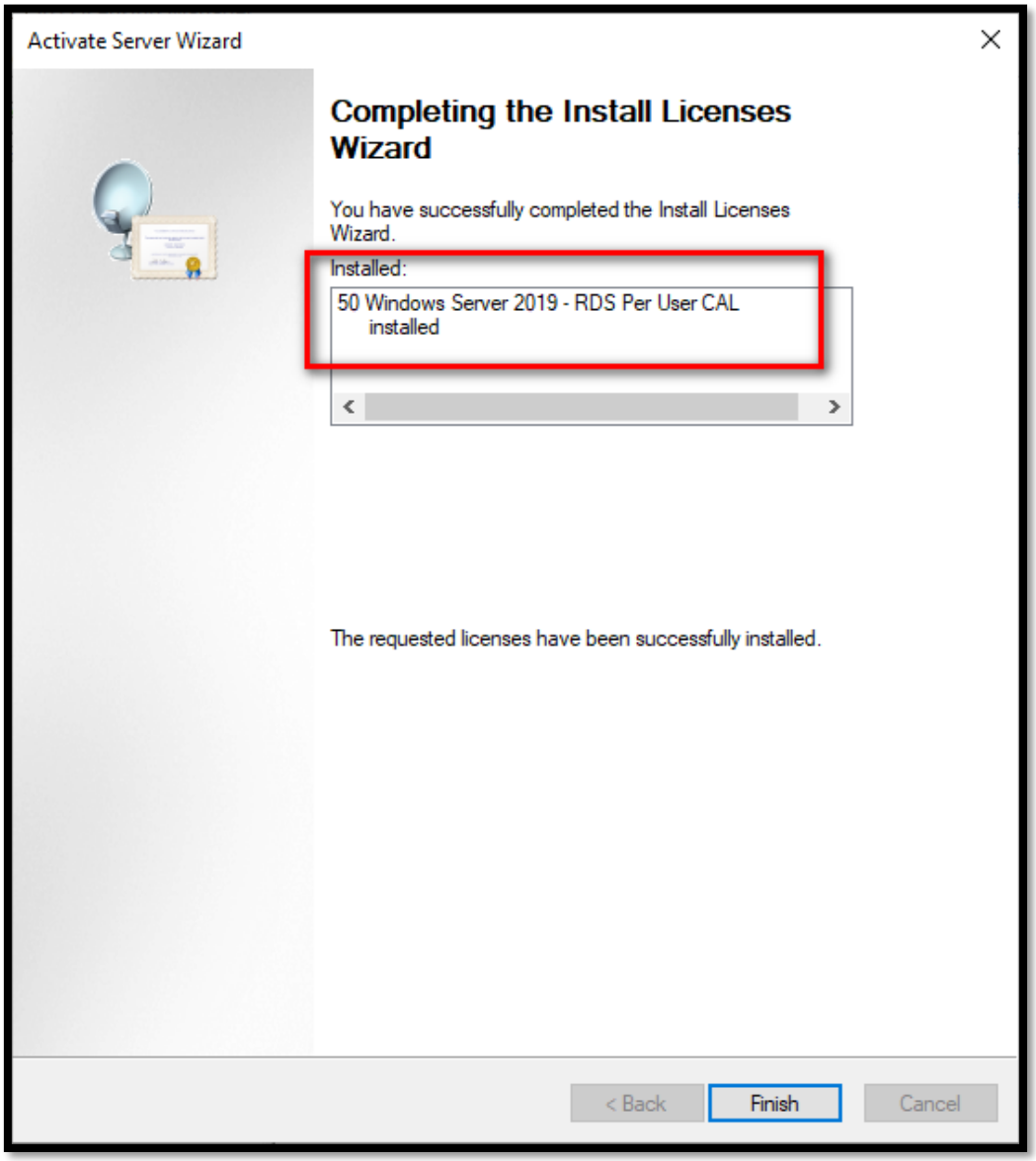
8. Select license type and click Next.



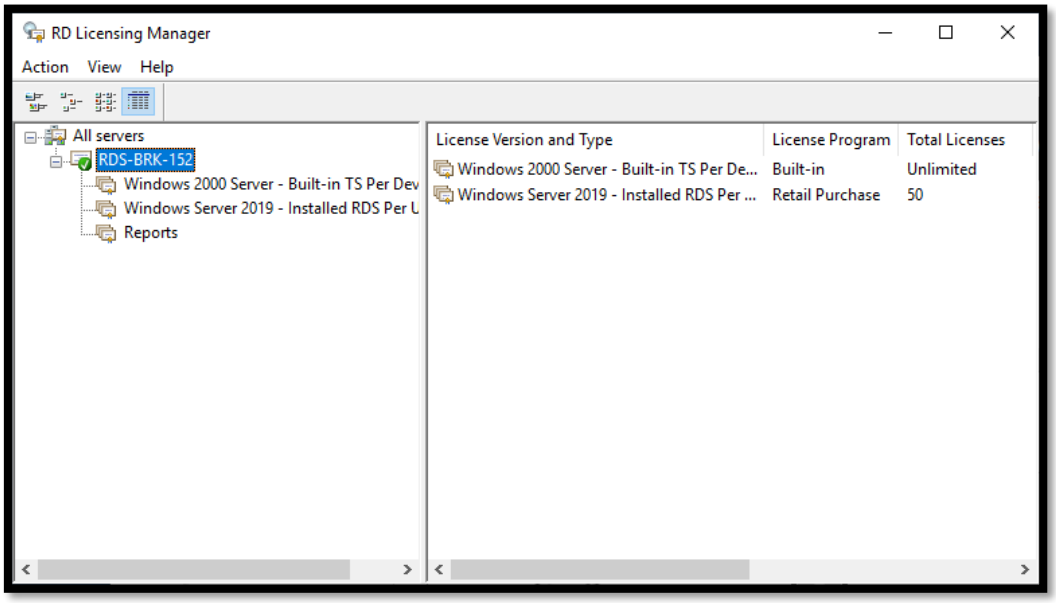
9. Enter the license information and click Next.



10. Click Finish to close the wizard.



11. The licenses are now visible on the server.



HTML5 client for Microsoft Remote Desktop Service

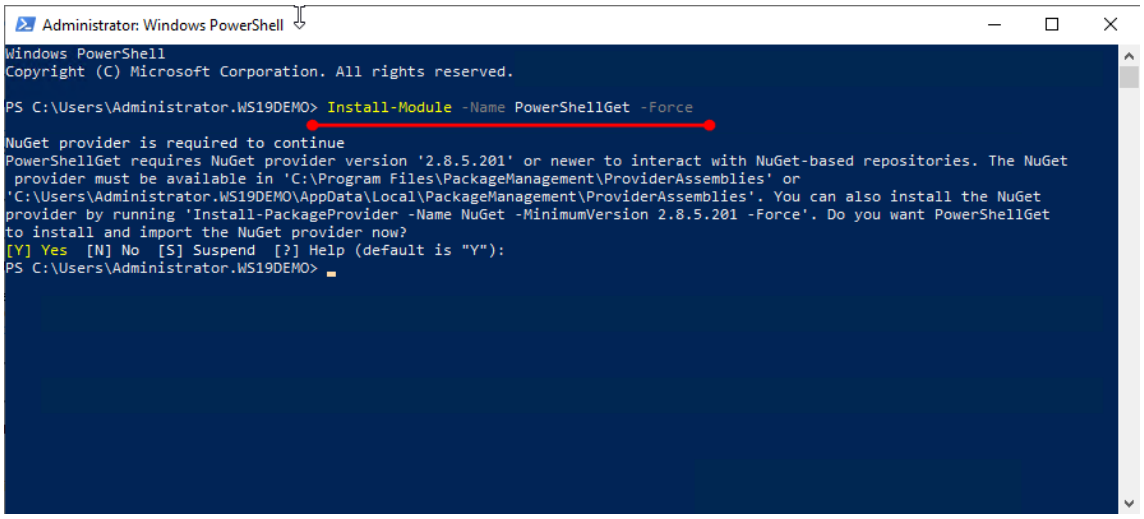
Until now to connect to Remote Desktop or RemoteApp, it was necessary to have a heavy RDP client. Since March 2018, Microsoft has previewed an HTML5 client that installs on the server with the RD Web Access role, which allows you to connect to desktops and applications without the need for a heavy client.

The installation is to be done on the server having the role of Web Access.

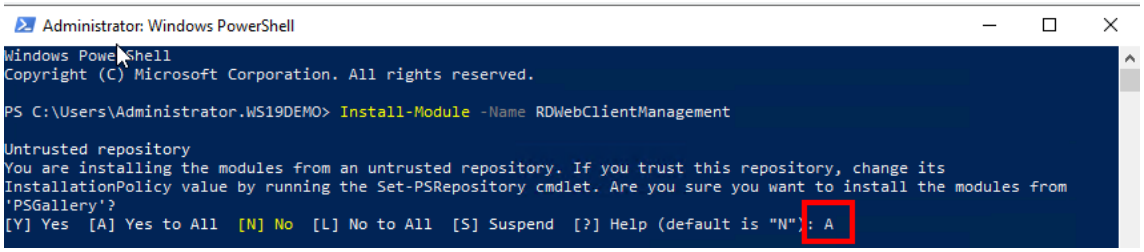
- Servers with Remote Desktop, Service Broker, and Remote Desktop Gateway Web Access roles must be running Windows Server 2016/2019.
- The https://support.microsoft.com/en-us/help/4025334/windows-10-update-kb4025334 update must be installed on the Remote Desktop Gateway server.
- Broker / Gateway / Web Access certificates should not be self-signed. (They can come from a private Authority)
- The license mode must be per user.

Installation

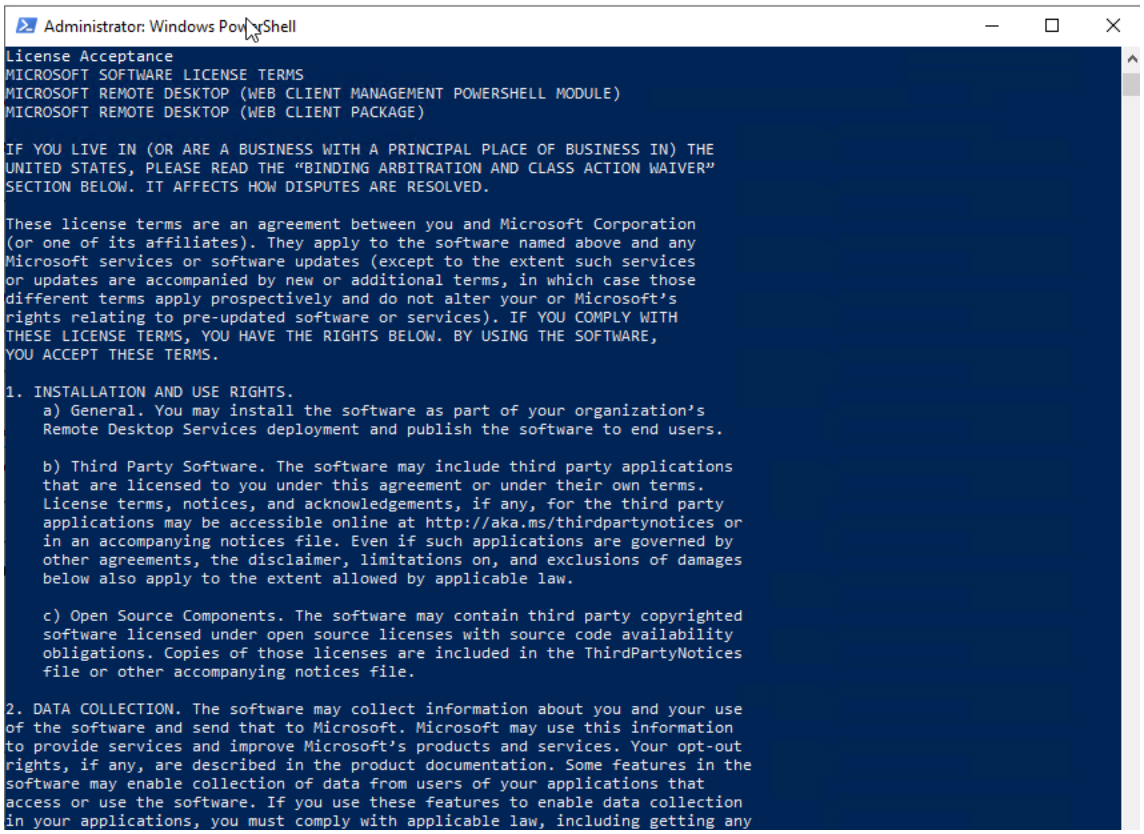
1. Open a PowerShell window and enter the following command to install PowerShellGet. Confirm the installation by entering Y.



2. Enter the following command to install Remote Desktop Web Client Management:



3. Accept the license.



4. Enter the following command to install Remote Desktop Web Client:

5. Install-RDWebClientPackage

6. Import the broker server certificate:

7. Import-RDWebClientBrokerCert c:\cert-file\BRK-154.cer

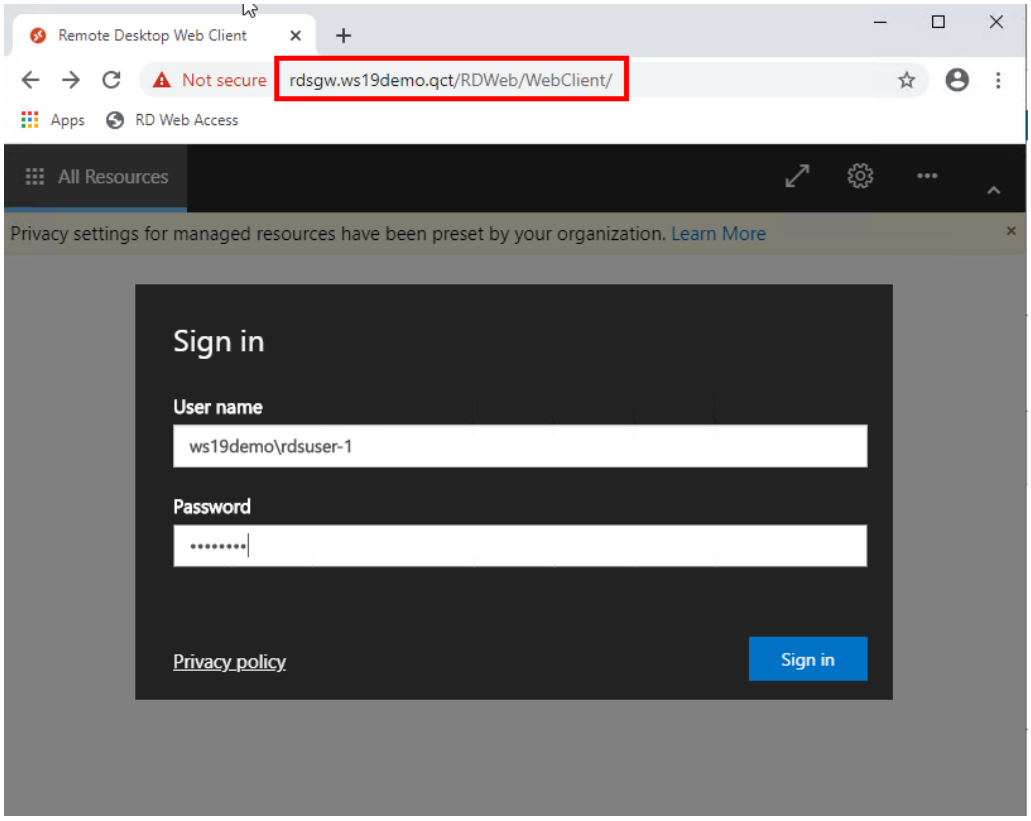
8. Publish the RDWC HTML 5 client:

9. Publish-RDWebClientPackage -Type Production -Latest

Now that the client is installed and configured on the server

USE

To test the HTML5 web client, open a browser (currently Edge, IE 11, Google Chrome browsers are all officially supported) and browse to **https://<publicdomain>/RDWeb/Pages/webclient**.



The RDS session will now process the logon.

~ End

About QCT

Quanta Cloud Technology (QCT) is a global data center solution provider. We combine the efficiency of hyperscale hardware with infrastructure software from a diversity of industry leaders to solve next-generation data center design and operation challenges. QCT serves cloud service providers, telecoms and enterprises running public, hybrid and private clouds.

Product lines include hyperconverged and software-defined data center solutions as well as servers, storage, switches and integrated racks with a diverse ecosystem of hardware component and software partners. QCT designs, manufactures, integrates and services cutting-edge offerings via its own global network. The parent of QCT is Quanta Computer, Inc., a Fortune Global 500 corporation. www.QCT.io.

United States

QCT LLC., Silicon Valley office
1010 Rincon Circle, San Jose, CA 95131
TOLL-FREE: 1-855-QCT-MUST
TEL: +1-510-270-6111
FAX: +1-510-270-6161
Support: +1-510-270-6216

QCT LLC., Seattle office
13810 SE Eastgate Way, Suite 190, Building 1,
Bellevue, WA 98005
TEL: +1-425-633-1620
FAX: +1-425-633-1621

China

云达科技, 北京办公室（Quanta Cloud Technology）
北京市朝阳区东三环中路 1 号，环球金融中心东楼 1508 室
Room 1508, East Tower 15F, World Financial Center
No.1, East 3rd Ring Zhong Rd., Chaoyang District, Beijing, China
TEL: +86-10-5920-7600
FAX: +86-10-5981-7958

云达科技, 杭州办公室（Quanta Cloud Technology）
浙江省杭州市西湖区古墩路浙商财富中心 4 号楼 303 室
Room 303，Building No.4，ZheShang Wealth Center
No. 83 GuDun Road, Xihu District, Hangzhou, Zhejiang, China
TEL: +86-571-2819-8660

Japan

Quanta Cloud Technology Japan 株式会社
日本国東京都港区芝大門二丁目五番八号
牧田ビル 3 階
Makita Building 3F, 2-5-8, Shibadaimon,
Minato-ku, Tokyo 105-0012, Japan
TEL: +81-3-5777-0818
FAX: +81-3-5777-0819

Taiwan

雲達科技（Quanta Cloud Technology）
桃園市龜山區文化二路 211 號 1 樓
1F, No. 211 Wenhua 2nd Rd., Guishan Dist.,
Taoyuan City 33377, Taiwan
TEL: +886-3-286-0707
FAX: +886-3-327-0001

Other regions

Quanta Cloud Technology
No. 211 Wenhua 2nd Rd., Guishan Dist.,
Taoyuan City 33377, Taiwan
TEL: +886-3-327-2345
FAX: +886-3-397-4770