IMPLEMENTATION OF REMOTE DESKTOP SERVICES

Lab 08 – Windows Services

Andrea Girotto | Guilherme Videira Marques
GirAn570@school.lu | vidgu017@school.lu

1. Overview

This lab simulates a small educational IT environment where multiple students need secure and centralized access to a Windows desktop environment from their personal devices.

The objective is to deploy a Remote Desktop Services (RDS) infrastructure that allows students to log in using domain credentials and access applications hosted on a central Windows Server, without requiring local software installation or high-performance client hardware.

The scenario reflects a real-world use case such as a school computer lab, training center, or small organization. RDS provides centralized management, user isolation, and simplified maintenance, allowing administrators to manage users and control access through Active Directory groups while providing remote access via full desktop sessions or RemoteApp programs.

The implemented solution demonstrates how Remote Desktop Services, combined with Active Directory and DNS, delivers controlled, scalable, and secure remote access from physical client machines in a mixed network environment.

1.1 Target result

A Windows Server 2022 VM (RDS-SRV01) deployed with Active Directory Domain Services (AD DS) and DNS Server provides Remote Desktop Services to two Windows 11 client machines (LAB-PC-1, LAB-PC-2). The session-based desktop deployment enables students to authenticate with domain credentials and access a full Windows desktop environment from their personal devices without local software installation.

Infrastructure components:

- Active Directory Domain Services (AD DS) for user and group management
- DNS Server for name resolution within the domain
- Remote Desktop Services Session-based deployment for centralized desktop hosting

1.2 Naming used in this implementation

Component	Value
Server hostname	RDS-SRV01
Domain	lab8.local
RDS collection name	QuickSessionCollection
Student group	LAB8\RDS_Students
Server IP address	10.0.97.61
Subnet mask	255.255.255.0

2. Prerequisites

2.1 Required Resources

- VirtualBox installed on the host machine
- Windows Server 2022 ISO
- Two Windows 11 client PCs on the same LAN
- Local admin rights on the server and the clients
- Sufficient network connectivity between all machines

2.2 Hardware Recommendations

Server VM (RDS-SRV01):

- RAM: 4-6 GB (minimum 4 GB)
- Disk: 40-60 GB
- Network: Bridged Adapter

Client PCs:

- Standard Windows 11 hardware requirements
- Network connectivity to server

2.3 Network Topology

All on the same Network

3. Build the server VM (RDS-SRV01)

3.1 Create the VirtualBox VM

1. ***Open VirtualBox***
2. ***Create a new VM with the following settings:***
    - Name: RDS-SRV01
    - Type: Microsoft Windows
    - Version: Windows 2022 (64-bit)
    - RAM: 4-6 GB (depending on your host machine capabilities)
    - Disk: 40-60 GB (dynamically allocated)
3. ***Configure networking:***
    - Adapter 1: Bridged Adapter
    - Select the correct host NIC (the network interface connected to your LAN)

Note: Bridged networking allows the VM to appear as a separate machine on your physical network, enabling client PCs to connect directly to it.

3.2 Install Windows Server 2022

1. ***Boot the VM from the Windows Server 2022 ISO***
2. ***Follow the installation wizard:***
    - Select language and keyboard preferences
    - Click "Install now"
    - Choose Windows Server 2022 Standard (Desktop Experience)
    - Accept the license terms
    - Select Custom: Install Windows only (advanced)
    - Select the virtual disk and proceed with installation
3. ***Set the local Administrator password when prompted***
    - Use a strong password
    - Document this password securely

Important: The server will restart automatically after installation.

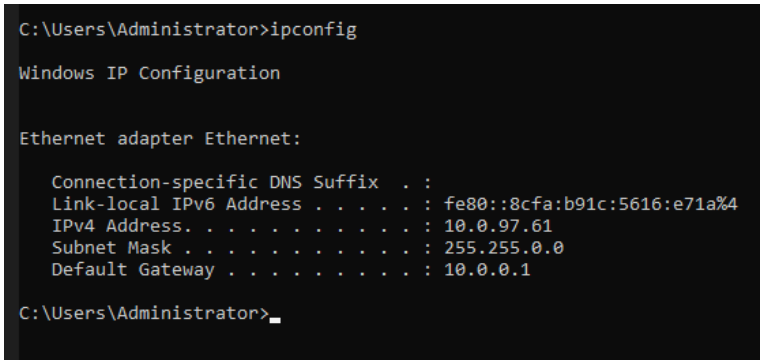
3.3 Rename the server

1. ***After first login, open Server Manager (launches automatically)***
2. ***Click Local Server in the left pane***
3. ***Click the current computer name (e.g., WIN-XXXXXXXXXXX)***
4. ***Click Change... button***
5. ***Enter the new name:***
   - Computer name: RDS-SRV01
6. ***Click OK, then OK again to confirm restart***
7. ***Click Restart Now***

Result: Server hostname is now RDS-SRV01

3.4 Configure a static IP address

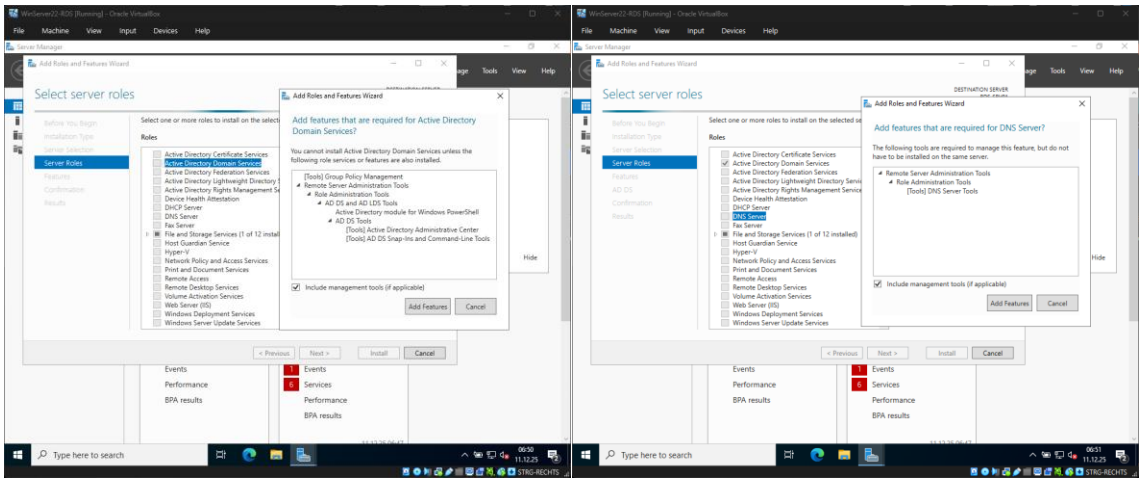
1. ***Open Network and Sharing Center***
   - Right-click the network icon in the system tray
   - Select "Open Network and Sharing Center"
2. ***Click Change adapter settings (left sidebar)***
3. ***Right-click the Ethernet adapter → Select Properties***
4. ***Select Internet Protocol Version 4 (TCP/IPv4) → Click Properties***
5. ***Select Use the following IP address and configure:***
   - Obtain an IP address automatically (DHCP) - should already be selected
   - Obtain DNS server address automatically - should already be selected
6. ***Click OK to close***
7. ***Open Command Prompt and run:***



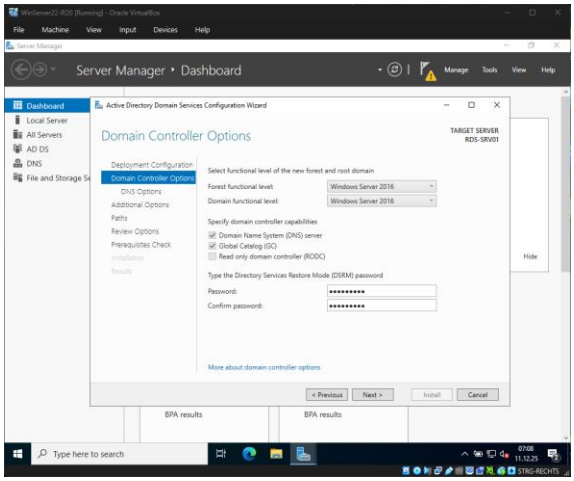
4. Install AD DS and DNS (Domain Controller)

4.1 Add the server roles

1. ***Open Server Manager (if not already open)***
2. ***Click Manage → Add Roles and Features***
3. ***In the wizard, click Next on the "Before You Begin" page***
4. ***Select Role-based or feature-based installation → Click Next***
5. ***Ensure RDS-SRV01 is selected from the server pool → Click Next***
6. ***On the "Server Roles" page, select:***
   - Active Directory Domain Services
   - DNS Server

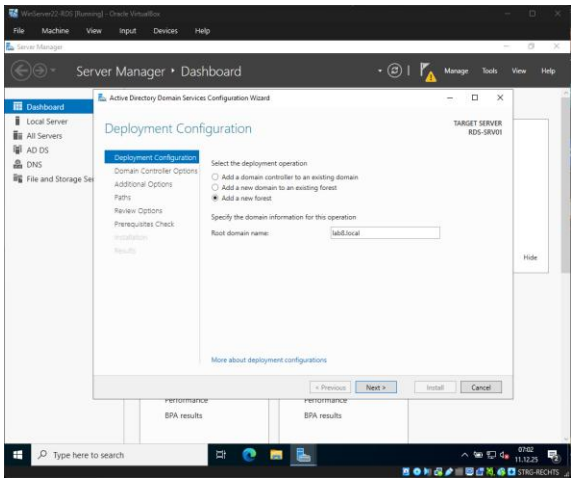


7. ***On "Confirmation", click Install***

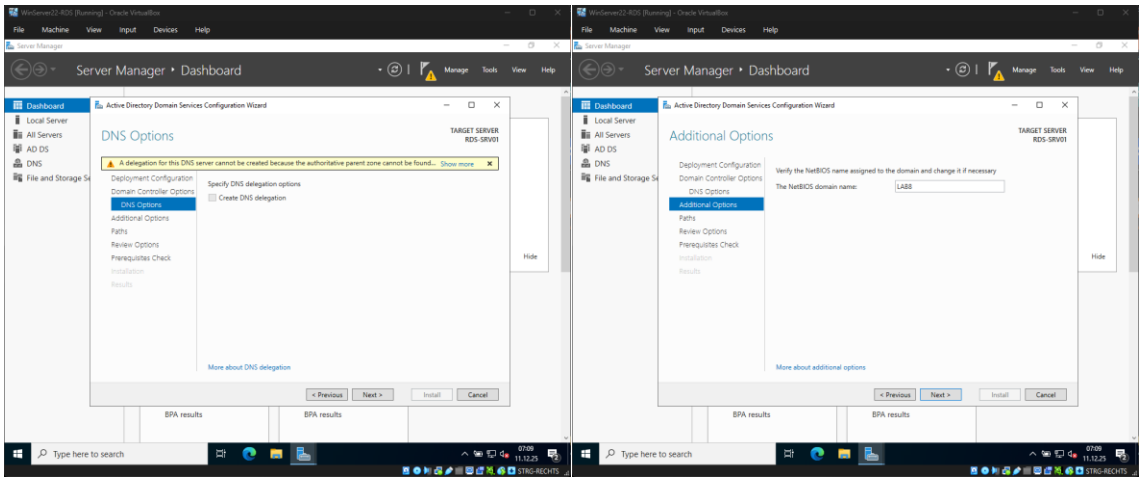


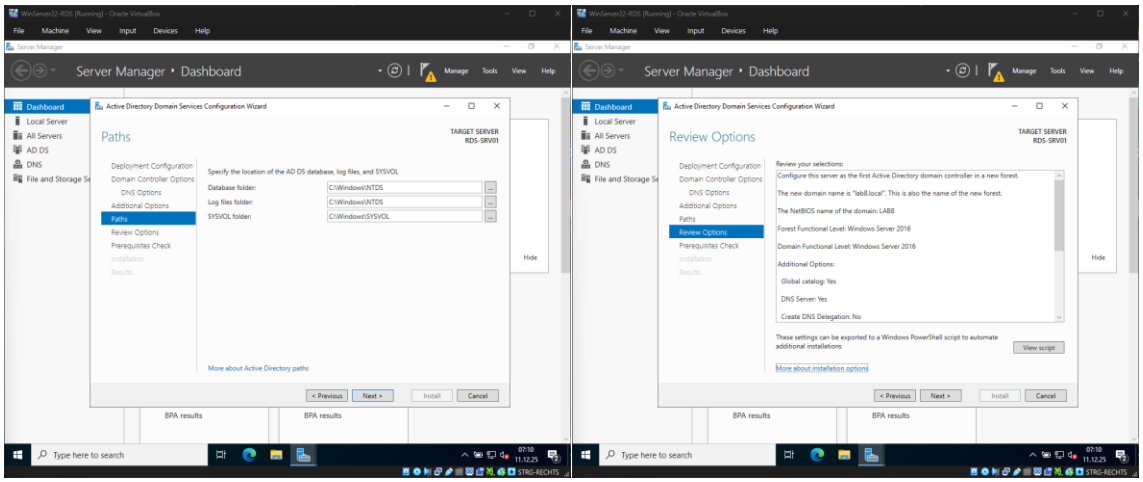
4.2 Promote to Domain Controller

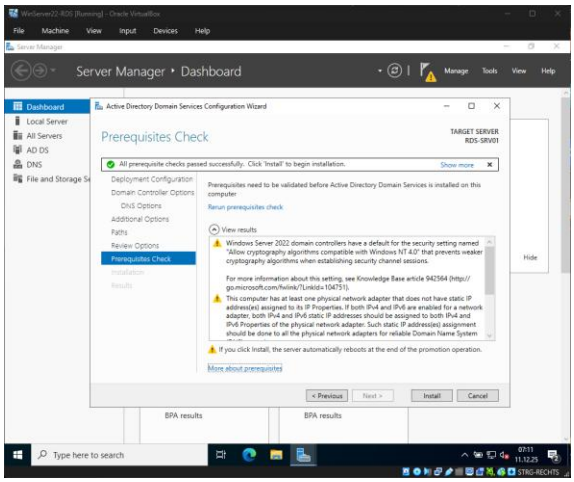
1. ***In Server Manager, click the notification flag (yellow triangle icon in the top-right)***
2. ***Click Promote this server to a domain controller***
3. ***In the Deployment Configuration:***
    - Select Add a new forest
    - Root domain name: lab8.local



4. ***In Domain Controller Options:***
    - Leave Domain Name System (DNS) server checked
    - Leave Global Catalog (GC) checked
    - Forest functional level: Windows Server 2016 (or higher)
    - Domain functional level: Windows Server 2016 (or higher)
    - Enter a Directory Services Restore Mode (DSRM) password
    - Document this password securely







5. Complete the wizard and reboot.

5. Create users and group for students

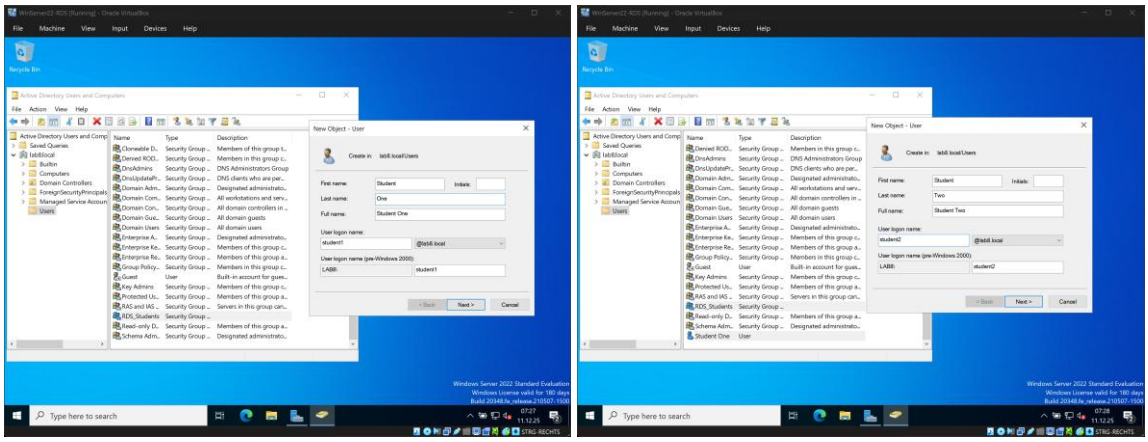
5.1 Open Active Directory Users and Computers

1. ***Ensure you're logged in to RDS-SRV01 as LAB8\Administrator***
2. ***Open Server Manager → Tools → Active Directory Users and Computers***
3. ***In the left pane, expand lab8.local***

5.2 Create student user accounts

1. ***Open Active Directory Users and Computers.***
2. ***Expand lab8.local***
3. ***In Users, create:***
    - student1
    - student2

Assign passwords according to your lab rules.

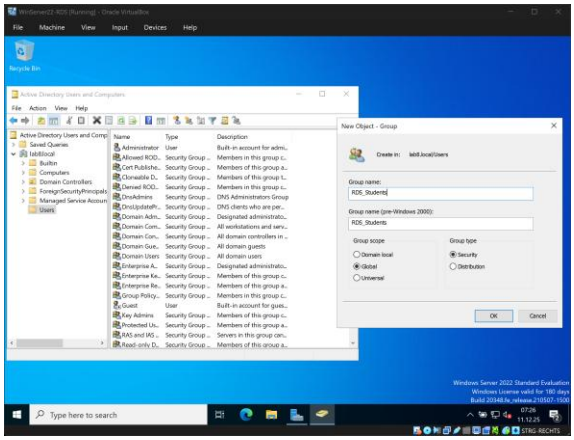


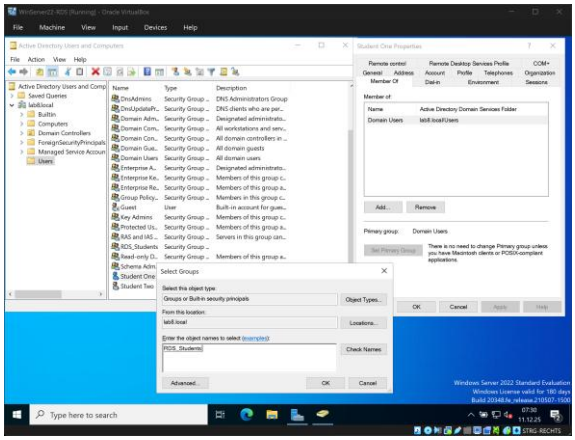
5.3 Create the RDS access group

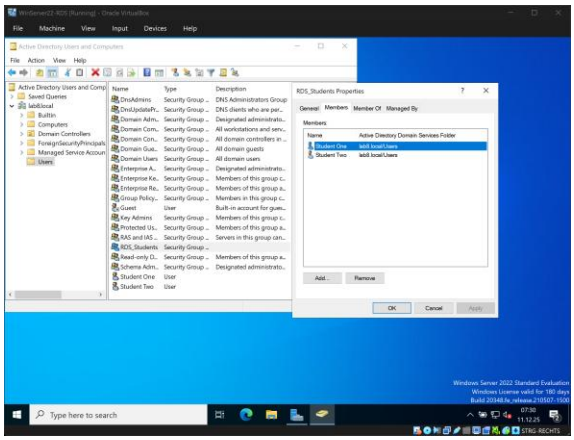
1. ***In Users, create a new group:***

   - Name: RDS_Students
   - Scope: Global
   - Type: Security

2. ***Add student1 and student2 as members.***



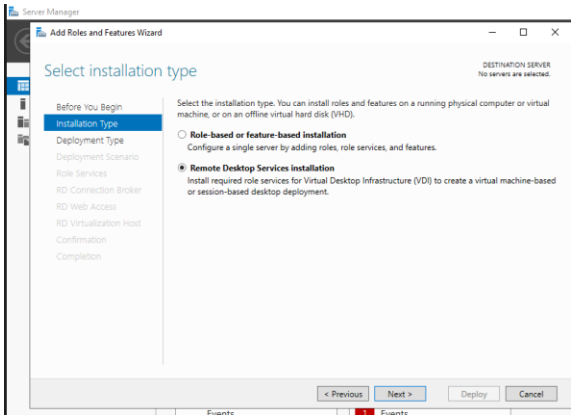




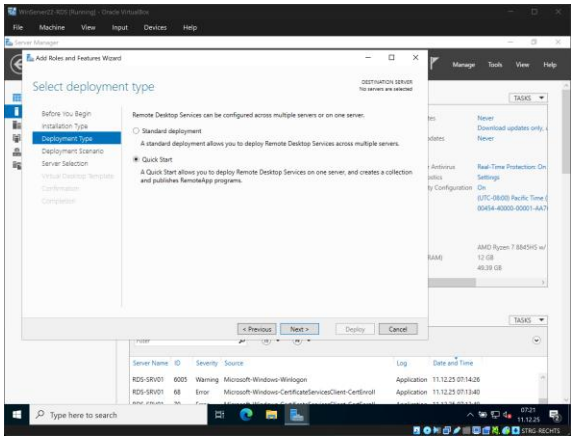
6. Install Remote Desktop Services (RDS)

6.1 Install the RDS deployment

1. ***In Server Manager, click Manage →Add Roles and Features.***
2. ***Choose Remote Desktop Services installation.***

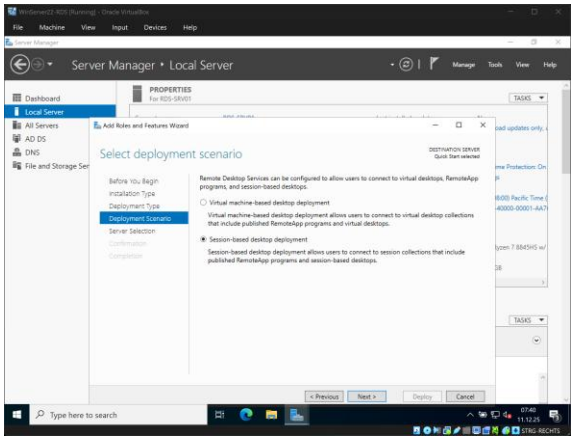


3. ***On "Deployment Type", select Quick Start →Click Next***

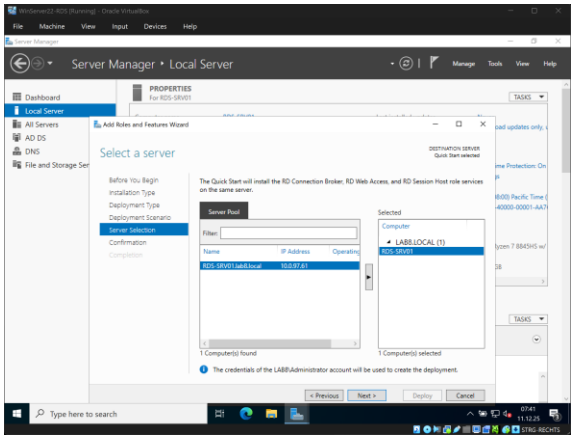


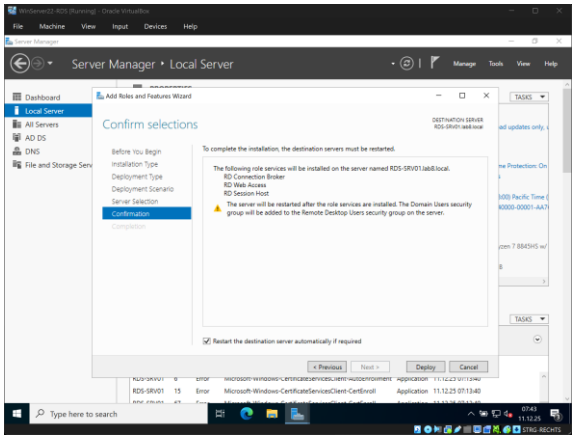
Note: Quick Start is ideal for lab environments with a single server. Standard deployment is used for multi-server production environments.

4. *On "Deployment Scenario", select Session-based desktop deployment.*

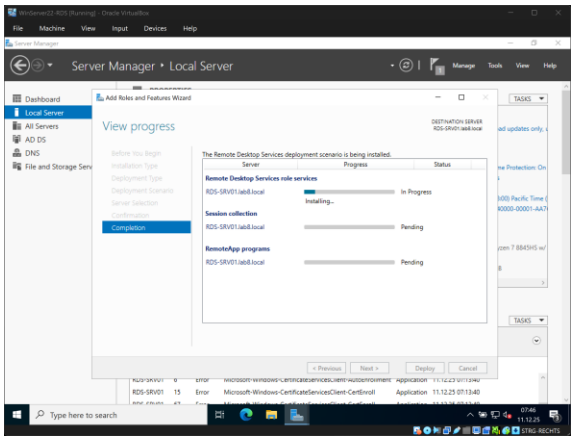


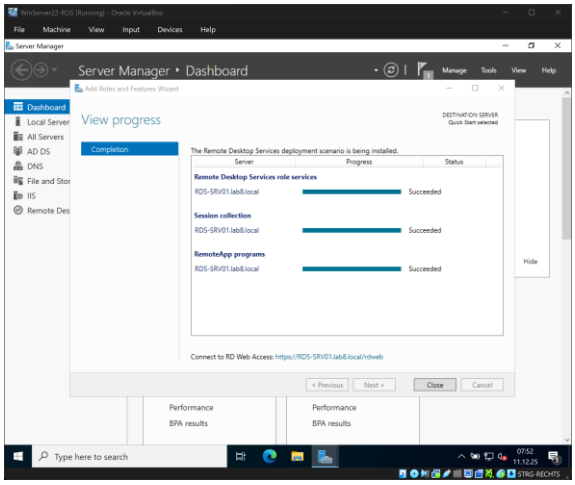
5. *On "Server Selection", ensure RDS-SRV01.lab8.local is selected*





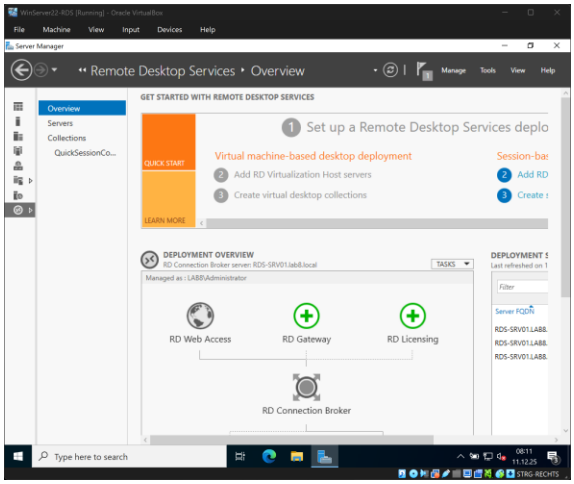
6. *Complete the wizard (restart if prompted).*





6.2 Verify the Session Collection

1. ***In Server Manager, click Remote Desktop Services in the left navigation pane***



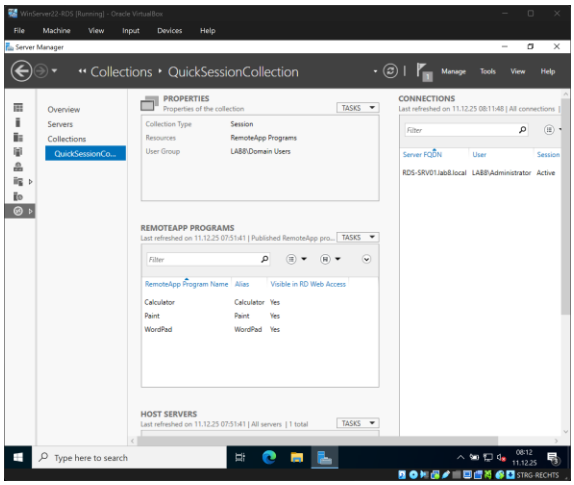
2. ***Click Collections under Remote Desktop Services***

3. ***Verify that QuickSessionCollection appears in the collections list***

Note: This collection was automatically created by the Quick Start deployment. If you want to create a custom collection with a different name, you can do so, but QuickSessionCollection works perfectly for this lab.

6.3 Configure User Group Access

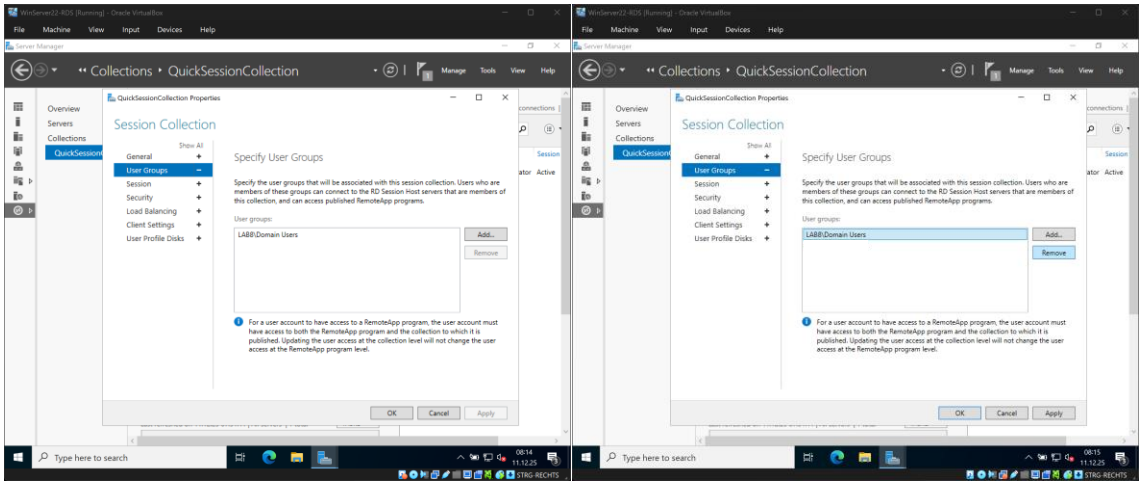
1. ***Click on QuickSessionCollection in the collections list***



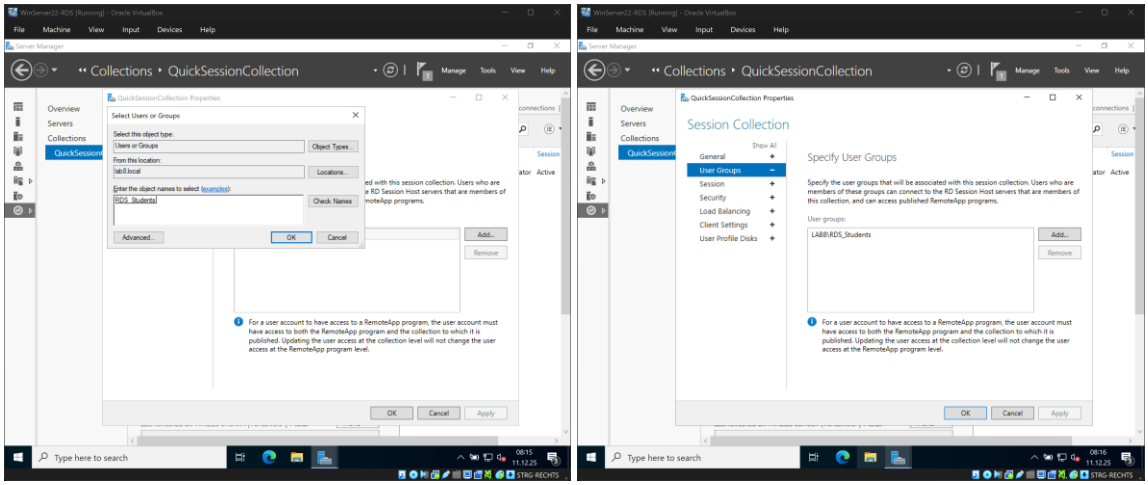
2. ***In the Properties section (Middle pane), click TASKS → Edit Properties***

3. ***In the left menu, click User Groups***

4. ***Review the current user groups listed***
   - If Domain Users or other broad groups are listed, select them and click Remove



5. ***Click Add → Type RDS_Students in the object name field → Check Names → OK***



Result: Only members of the RDS_Students group can now launch sessions in this collection.

7. Application Configuration and Certificate Setup

7.1 Understanding Application Access Methods

In Remote Desktop Services, there are two ways users can access applications:

Full Desktop Sessions:

- Users connect to a complete Windows desktop environment
- All applications installed on the server are accessible via the Start menu
- Users can launch any program just like on a local computer

RemoteApp Programs:

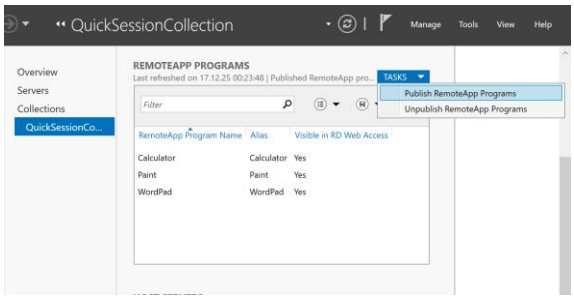
- Individual applications are published and appear as separate icons
- Users launch specific applications without seeing the full desktop
- Only published applications are available to users

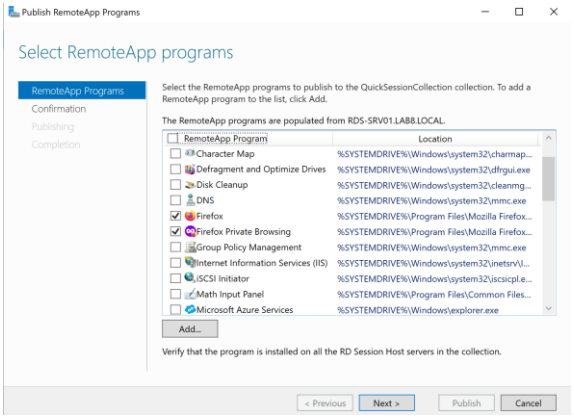
Note: *In our session-based desktop deployment, users get full desktop access by default, meaning they can use all installed applications without additional configuration.*

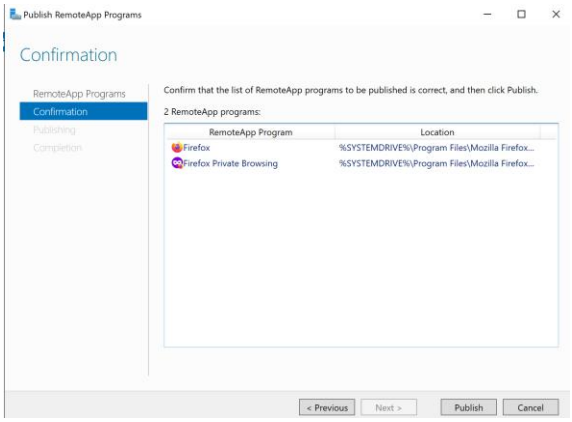
7.2 (Optional) Publishing RemoteApp Programs

If you want to publish specific applications:

1. ***Remote Desktop Services → Collections → QuickSessionCollection***
2. ***RemoteApp Programs → Click TASKS → Publish RemoteApp Programs***







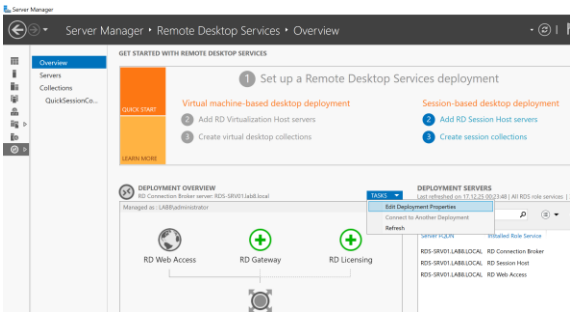
1. ***Click Publish***

Result: *Published RemoteApp programs appear in the RD Web Access portal and can be downloaded as .rdp files for direct launching.*

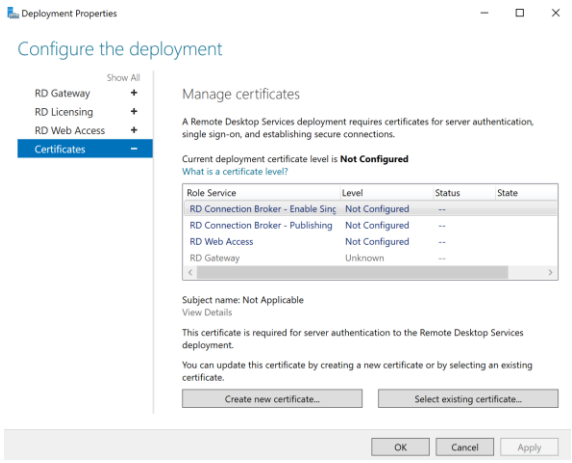
7.3 Configure RD Web Access Certificate

To secure the RD Web Access portal and eliminate certificate warnings:

1. ***In Remote Desktop Services → Overview***
2. ***In the Deployment Overview section, locate TASKS → Click Edit Deployment Properties***

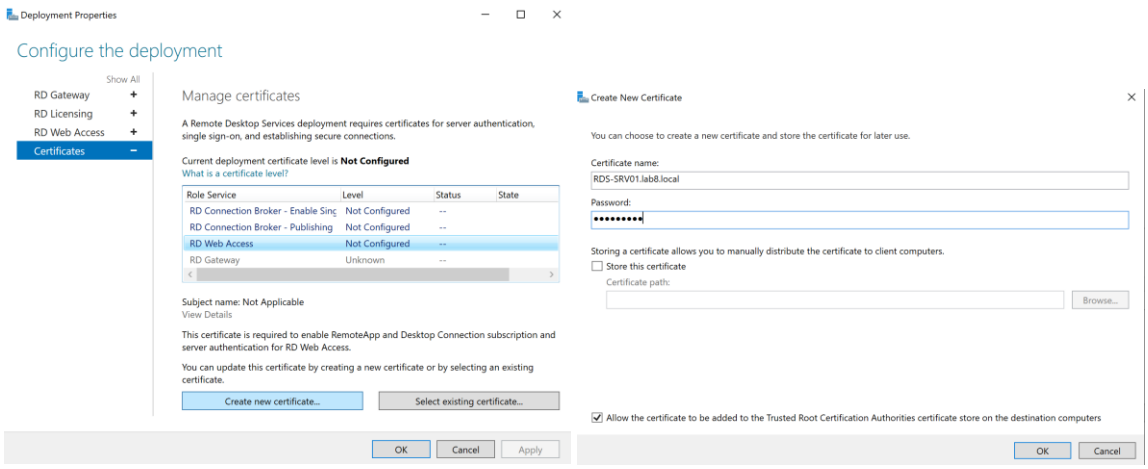


3. *In the left menu, select Certificates*



4. *Select RD Web Access → Click create a new certificate*

- Certificate name: RDS-SRV01.lab8.local
- Password: (set a password for certificate export)
- Check: "Allow the certificate to be added to the Trusted Root Certification Authorities certificate store on the destination computers"



5. *Apply*

7.4 Accessing RD Web Access with School Network DNS

Challenge: The certificate is issued for RDS-SRV01.lab8.local, but the school's DNS doesn't recognize this name. When you download an .rdp file from RD Web Access, it references the hostname RDS-SRV01.lab8.local, not the IP address.

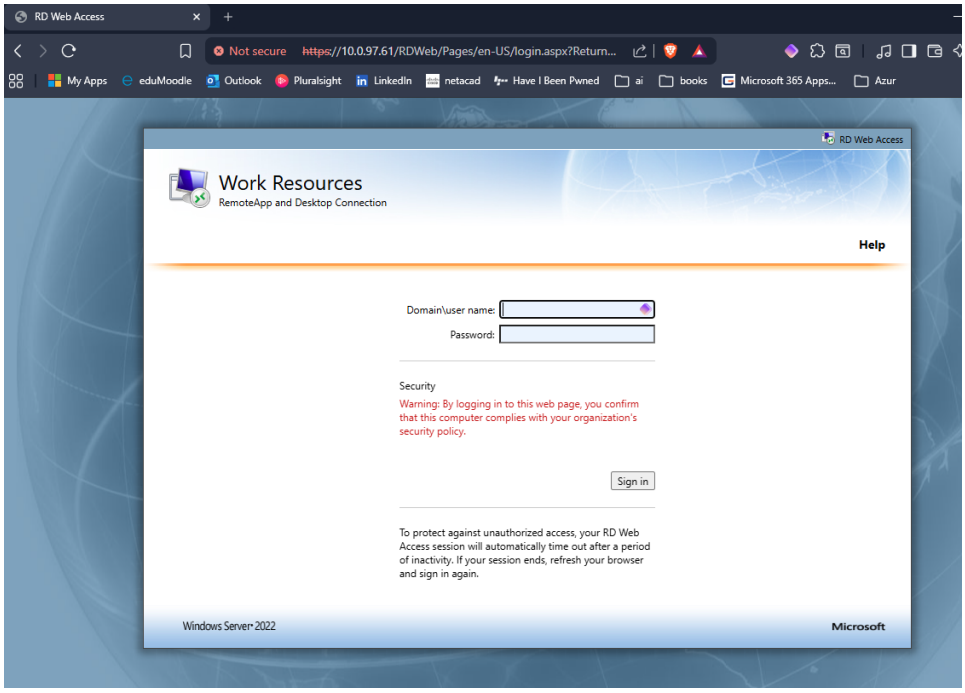
Critical Issue: Even if you access the RD Web Access portal using the IP address (https://10.0.97.61/rdweb), the downloaded .rdp files will still fail to connect because they contain the hostname, which your client cannot resolve.

Required Solution: Modify the Hosts File

You MUST map the hostname to the IP on every client machine that will use RD Web Access or RemoteApp:

1. ***On your client PC, open Notepad as Administrator***
2. ***In Notepad, open the hosts file:***
   - C:\Windows\System32\drivers\etc\hosts
3. ***Add the following line at the end of the file:***
   - 10.0.97.61 RDS-SRV01.lab8.local
4. ***Save the file and close Notepad***
5. ***Now you can access RD Web Access using either method:***

https://RDS-SRV01.lab8.local/rdweb or https://10.0.97.61/rdweb



7.5 Disclaimer

Why this is REQUIRED:

- The RD Web Access portal generates .rdp files that contain the server hostname (RDS-SRV01.lab8.local)
- Client computers outside the domain cannot resolve this hostname by default
- Without proper name resolution, launching RemoteApp results in the error:
- "Remote Desktop can't find the computer"
- To ensure correct hostname resolution, a hosts file entry is required
- This configuration must be applied on every client machine that accesses RD Web Access or RemoteApp

Alternative Solution (Not implemented in this lab):

Using Internal Network with Client VMs: If you want to avoid hosts file modifications, you could set up an isolated virtual environment:

1. Change the server's network adapter from Bridged to Internal Network in VirtualBox
2. Configure the server to act as a DHCP server for the internal network
3. Create Windows 11 client VMs and set their network adapters to the same Internal Network
4. The clients would receive IP addresses from the server's DHCP
5. The clients would use the server's DNS (which knows about lab8.local)
6. Everything would work without hosts file modifications because DNS resolution would be handled internally

Why we didn't use this approach:

We intentionally avoided setting up a fully isolated internal network. The goal was to keep the setup simple while still allowing access from real, physical machines.

By using bridged networking, the server is directly reachable from external devices. This allowed users—such as Andrea—to connect from their own PCs without being part of an internal virtual network, simply by using the server's IP address.

To handle name resolution in this mixed physical/virtual environment, we used a hosts file entry as a lightweight workaround.

8. Configure the clients (LAB-PC-1, LAB-PC-2)

From the beginning of the lab (LAB 1 and LAB 2), personal physical machines were used as client devices. This approach was maintained throughout the entire lab to ensure consistency and to simulate real-world client access rather than relying on virtualized test clients.

8.1 Name Resolution Configuration (Reference to Section 7.4)

Hostname resolution for RDS-SRV01.lab8.local was configured earlier as described in Section 7.4 by modifying the hosts file on each client machine.

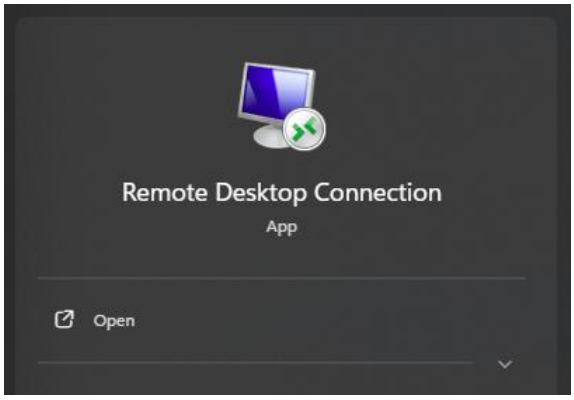
Expected result:

- The client can resolve RDS-SRV01.lab8.local
- RD Web Access and RemoteApp .rdp files function correctly

8.2 Full Remote Desktop Session Test

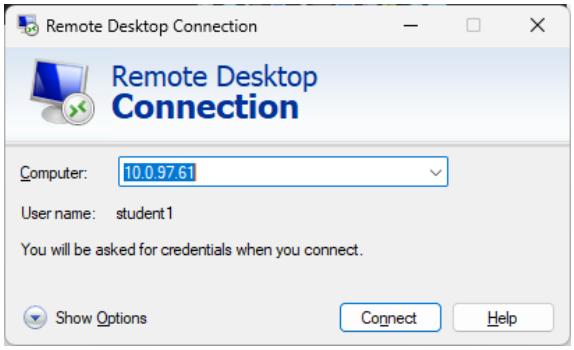
On the client machine, open Remote Desktop Connection by either:

1. ***Press Win + R and type mstsc, or***
2. ***Typing Remote Desktop Connection / mstsc directly in the Windows search bar***

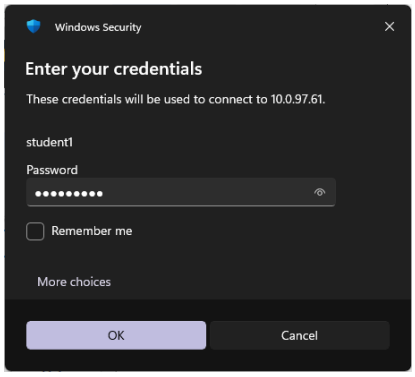


3. *Enter:*

RDS-SRV01.lab8.local or server IP address

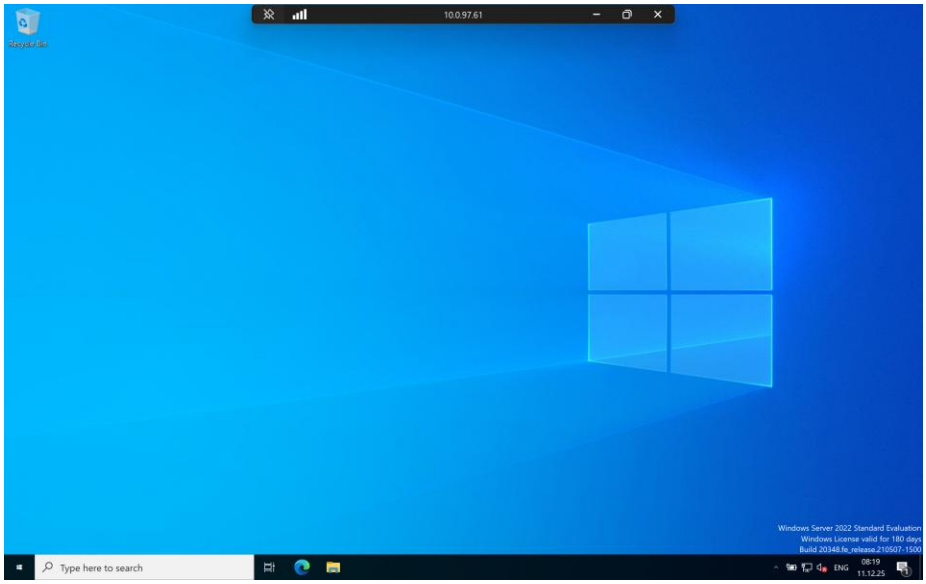


4. *Log in using domain credentials*



5. *Expected result:*

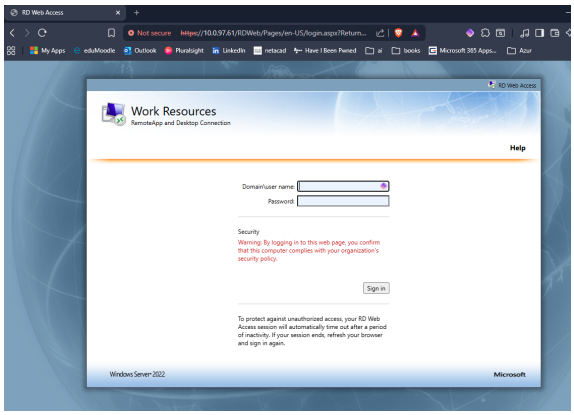
- ***A full Remote Desktop session opens successfully***



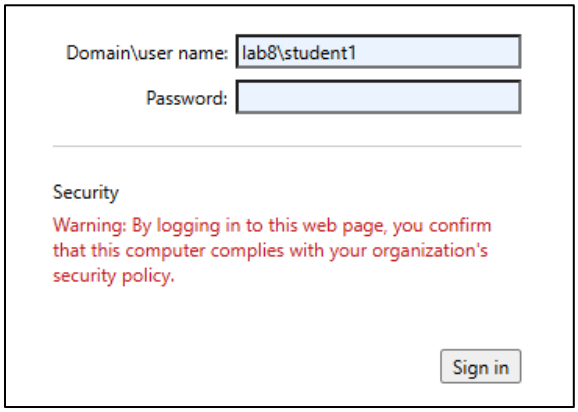
8.3 RemoteApp Access via RD Web Access

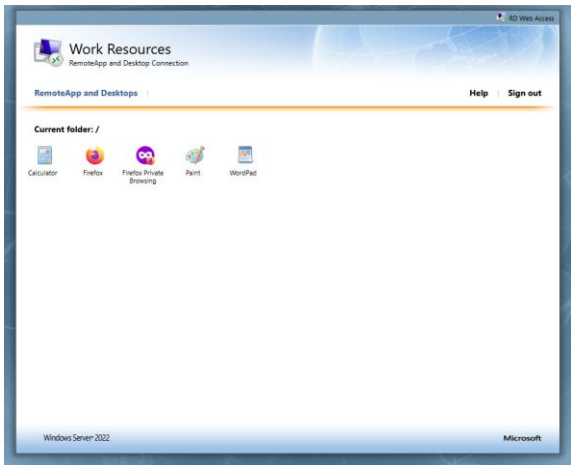
This step validates RemoteApp functionality from a personal client device.

1. ***Open a web browser***
2. ***Navigate to the server using the IP address or domain name:***

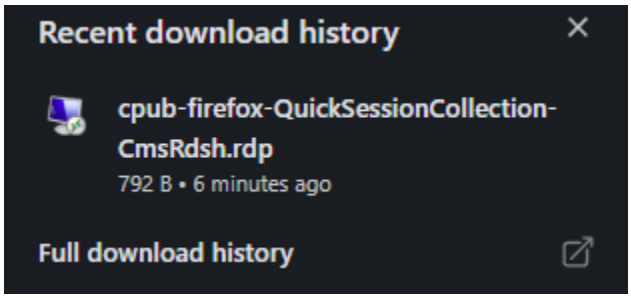


3. ***Authenticate using domain credentials***

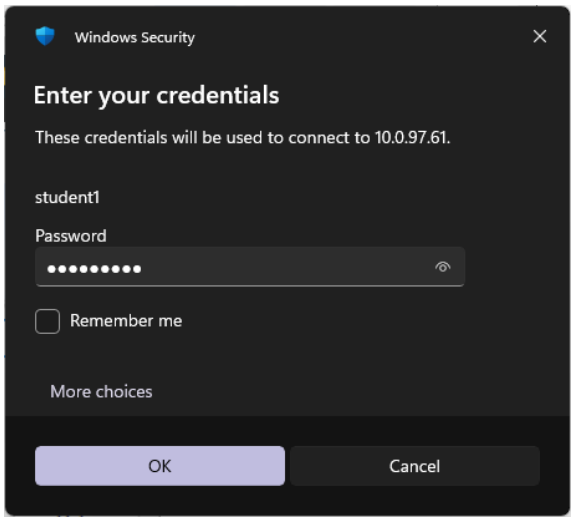




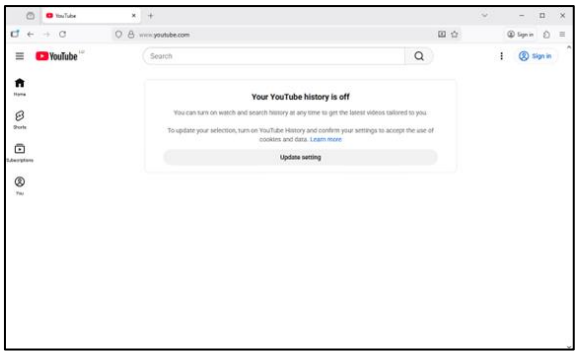
4. ***Launch a published RemoteApp, and open the downloaded .rdp file.***



5. ***Login***



6. ***The RemoteApp opens successfully, showing the Remote Desktop icon overlay. Functionality was verified by opening YouTube.***



9. Troubleshooting

9.1 Common issues

- **Client cannot resolve the server name:**
  Verify that the client's DNS settings point to the RDS server IP address or that the hosts file entry for RDS-SRV01.lab8.local exists.
- **Connection refused:**
  Ensure the RDS_Students group is added to the Remote Desktop Users group on the server.
- **RDS services not starting:**
  Verify that all required RDS roles are installed correctly and that the server was restarted after role installation.

Conclusion

This implementation provides a complete Remote Desktop Services (RDS) environment for lab purposes. A functional Active Directory domain was deployed, users and groups were configured, and Remote Desktop and RemoteApp access were successfully delivered to students.

The solution supports access from personal client machines using bridged networking, allowing real devices to connect without an isolated internal network. Full Remote Desktop sessions and published RemoteApp applications were verified to function correctly.

All components (RDS-SRV01, LAB-PC-1, LAB-PC-2) are fully configured and operational.