Windows Server:
RDS Deployment

By Miriam Ferreira

Contents

Overview

In this project I implemented a Remote Desktop Services (RDS) environment on Windows Server to provide centralized application access using RemoteApp. The goal was to design, deploy, and validate a secure RDS setup integrated with Active Directory and DNS, simulating a real world small enterprise scenario.

Scenario

A midsized architectural firm (ArchiPlan) needs to provide employees access to resource heavy applications from multiple locations without deploying high end workstations. Applications are hosted centrally, while users connect using lightweight client machines.

Architecture

The lab environment consists of:

- Active Directory Domain Services (AD DS)
- DNS
- Domain: `archiplan.local`
- RD Session Host
- RD Web Access
- RD Connection Broker
- Client Machine
- Windows 11 domainjoined workstation used for validation

All systems were deployed as virtual machines using Oracle VirtualBox on a NAT network.

Core Features Implemented

- Active Directory domain creation and centralized authentication
- RDS Quick Start deployment for smallscale environments
- RemoteApp publishing instead of full desktop access
- Rolebased access using Active Directory security groups
- Webbased access to applications through RD Web Access

Access Control Model

An Organizational Unit (OU) was created for ArchiPlan users, a security group (RDS_Users) was used for RemoteApp access, only members of this group can launch published applications. This enforces access and centralized permission management.

Applications Published

- Paint (simulating design tools)
- WordPad (simulating office productivity tools)
- Calculator

Applications are launched through the RD Web Access portal rather than exposing a full remote desktop session.

Validation and testing

The deployment was validated by joining a Windows 11 client to the domain and verifying DNS resolution and network connectivity, accessing the RD Web portal via HTTPS and successfully launching RemoteApps from the browser.

Troubleshooting highlights

- Incorrect role installation (AD CS instead of AD DS)
- Domain login failures due to incorrect username formats
- RD Web Access HTTPS errors caused by missing certificates
- Client connectivity issues caused by DNS misconfiguration

These issues were resolved through role correction, proper domain configuration, certificate deployment, and DNS alignment.

What I Learned

- How RDS integrates tightly with Active Directory and DNS
- Why groupbased access control is critical in enterprise environments
- The importance of certificate management for secure remote access
- How small configuration mistakes can break authentication and connectivity
- How to troubleshoot Windows Server services systematically

Limitations and future improvements

- Licensing services were not fully implemented
- No RD Gateway was deployed for external access

Future work could include a RD gateway with certificates, load balanced multisession RDS deployment or/and security hardening.

Disclaimer

This project was built in a controlled lab environment for educational purposes.