**Final Assignment Overview (AWS Deployment)**

**Objective:**

Deploy and manage a secure, scalable file-sharing system using DFS Replication on Windows Server 2022 in AWS for a simulated company with 3 departments (HR, Finance, Marketing).

**VM Infrastructure (5 Instances)**

|  |  |  |  |
| --- | --- | --- | --- |
| VM Name | **R**ole | OS | Suggested IP: |
| SRV-DC01 | Domain Controller | Windows Server 2022 | 10.0.0.10 |
| SRV-FILE01 | Primary File Server | Windows Server 2022 | 10.0.0.11 |
| SRV-FILE02 | Secondary File Server (DFS) | Windows Server 2022 | 10.0.0.12 |
| CLIENT1 | Test Client | Windows 10 Pro | 10.0.0.20 |
| CLIENT2 | Test Client | Windows 10 Pro | 10.0.0.21 |

**Step-by-Step Guide on AWS**

STEP 1: AWS Account and IAM Setup

1. Log in to AWS Console

2. Create IAM Users

\* Go to IAM → Users → Add Users

\* Assign EC2 and VPC permissions.

\* Enable MFA.

3. Create a Key Pair

\* Go to EC2 → Key Pairs → Create Key Pair

\* Save `.pem` file for RDP access later.

STEP 2: VPC and Network Setup

1. Go to VPC Dashboard → Create VPC

\* Name: `Fileshare-vpc`

\* CIDR block: `10.0.0.0/24`

2. Create 1 Subnet

\* Name: `Fileshare-subnet`

\* Subnet: `10.0.0.0/25`

3. \*\*Internet Gateway\*\*

\* Create and attach it to your VPC

4. \*\*Route Table\*\*

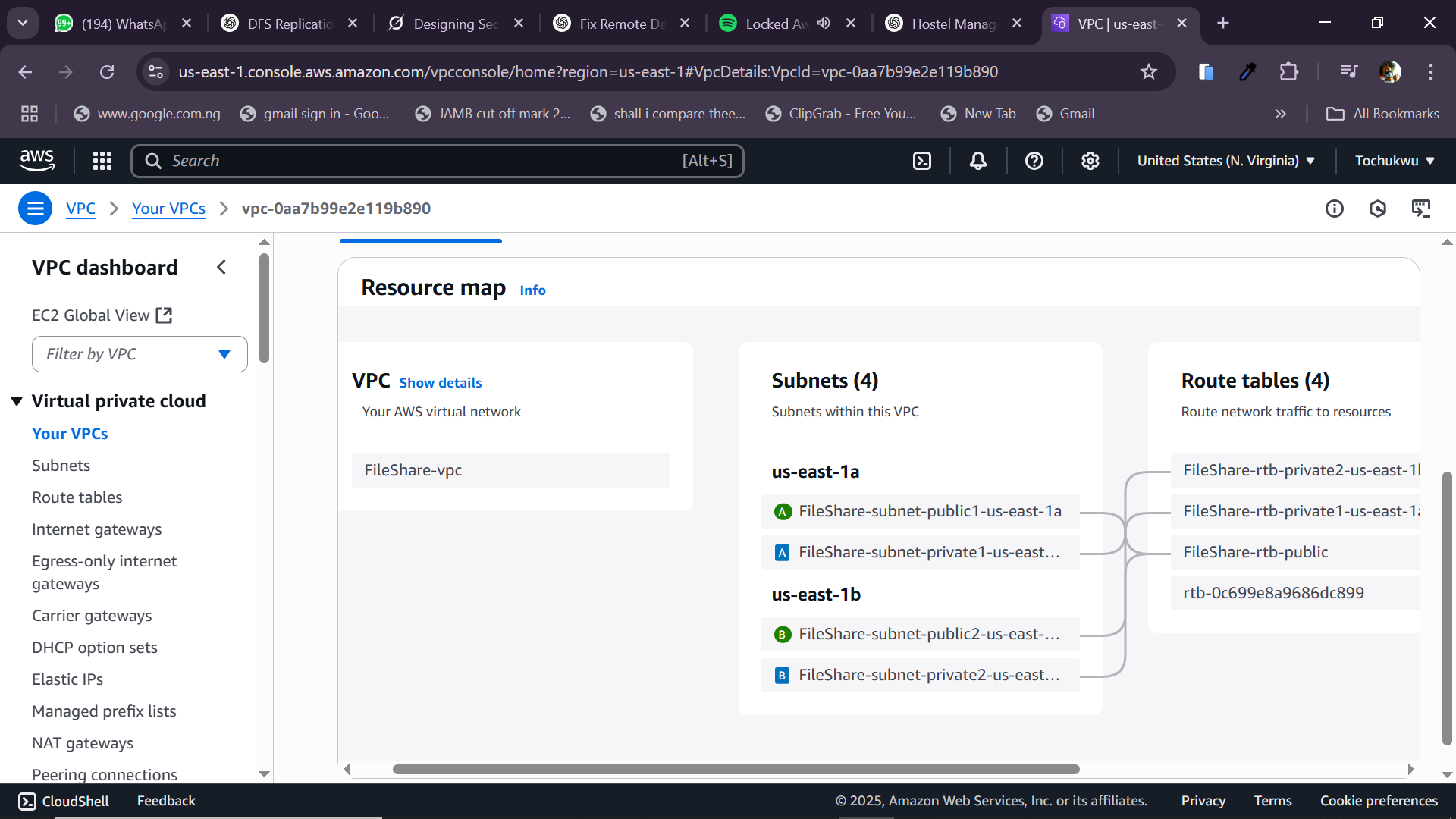
\* Edit main route table → add route `0.0.0.0/0 → Internet Gateway`

\* Associate with `Fileshare-subnet`

5. \*\*Security Group\*\*

\* Allow RDP (TCP 3389) from your IP

\* Allow all traffic between instances inside the same VPC



STEP 3: Launch EC2 Instances (5 Times)

Repeat this for each of the 5 instances below:

Example: SRV-DC01 (Domain Controller)

1. Launch EC2 → Select Windows Server 2022 Base

2. Instance Type: `t3.medium`

3. Network: Select `Fileshare-vpc`, `Fileshare-subnet`

4. Storage: 30 GB (GP3)

5. Add Tag: `Name = SRV-DC01`

6. Security Group: Select the one created above

7. Key Pair: Use the `.pem` file you saved earlier

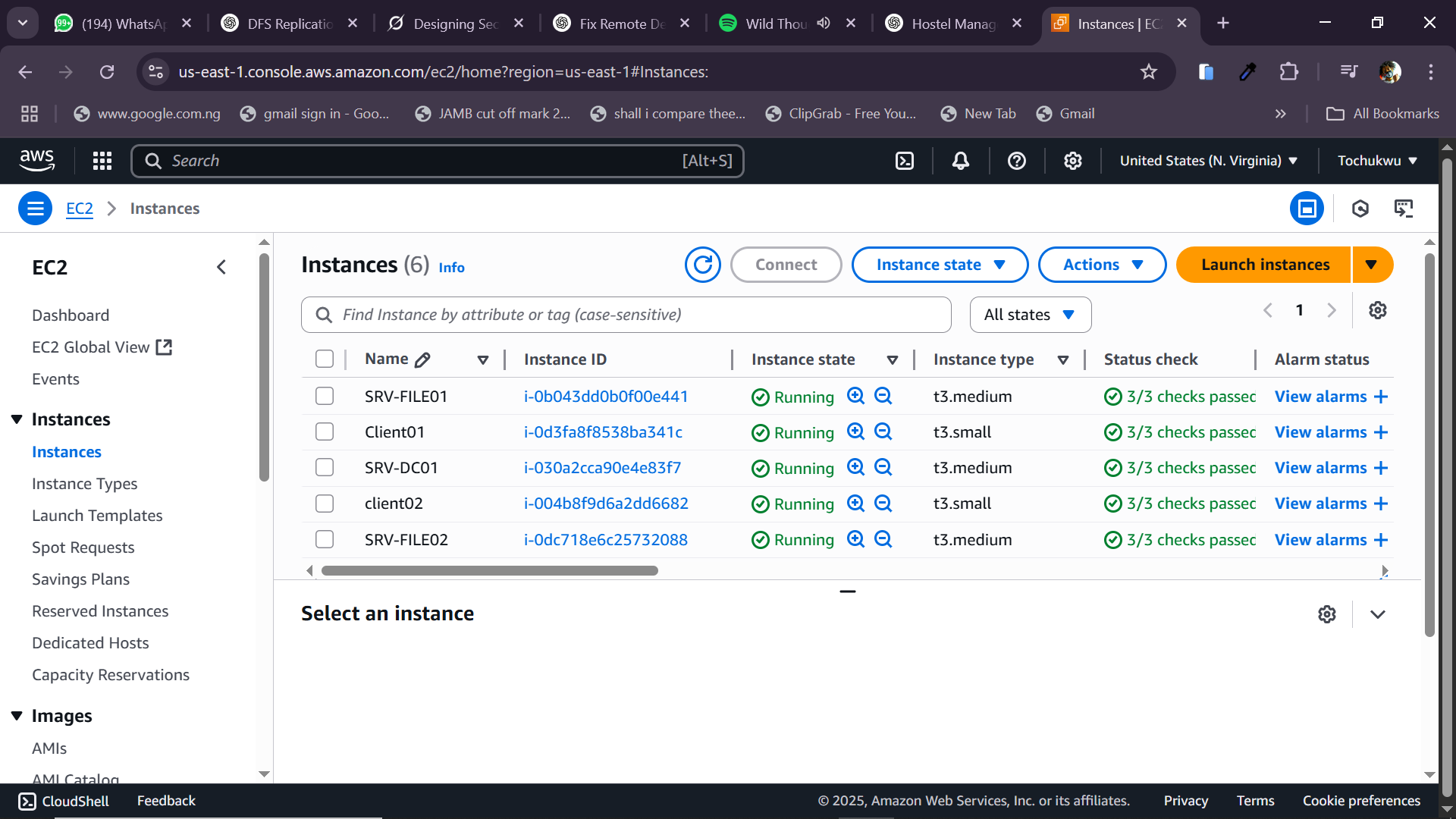
Repeat this for:

\* `SRV-FILE01` (Add extra 20GB disk for D:)

\* `SRV-FILE02` (Same)

\* `CLIENT1` (Windows 10 Pro)

\* `CLIENT2` (Windows 10 Pro)



STEP 4: Configure SRV-DC01 (Domain Controller)

1. Connect via RDP using `.pem` file

2. Open PowerShell:

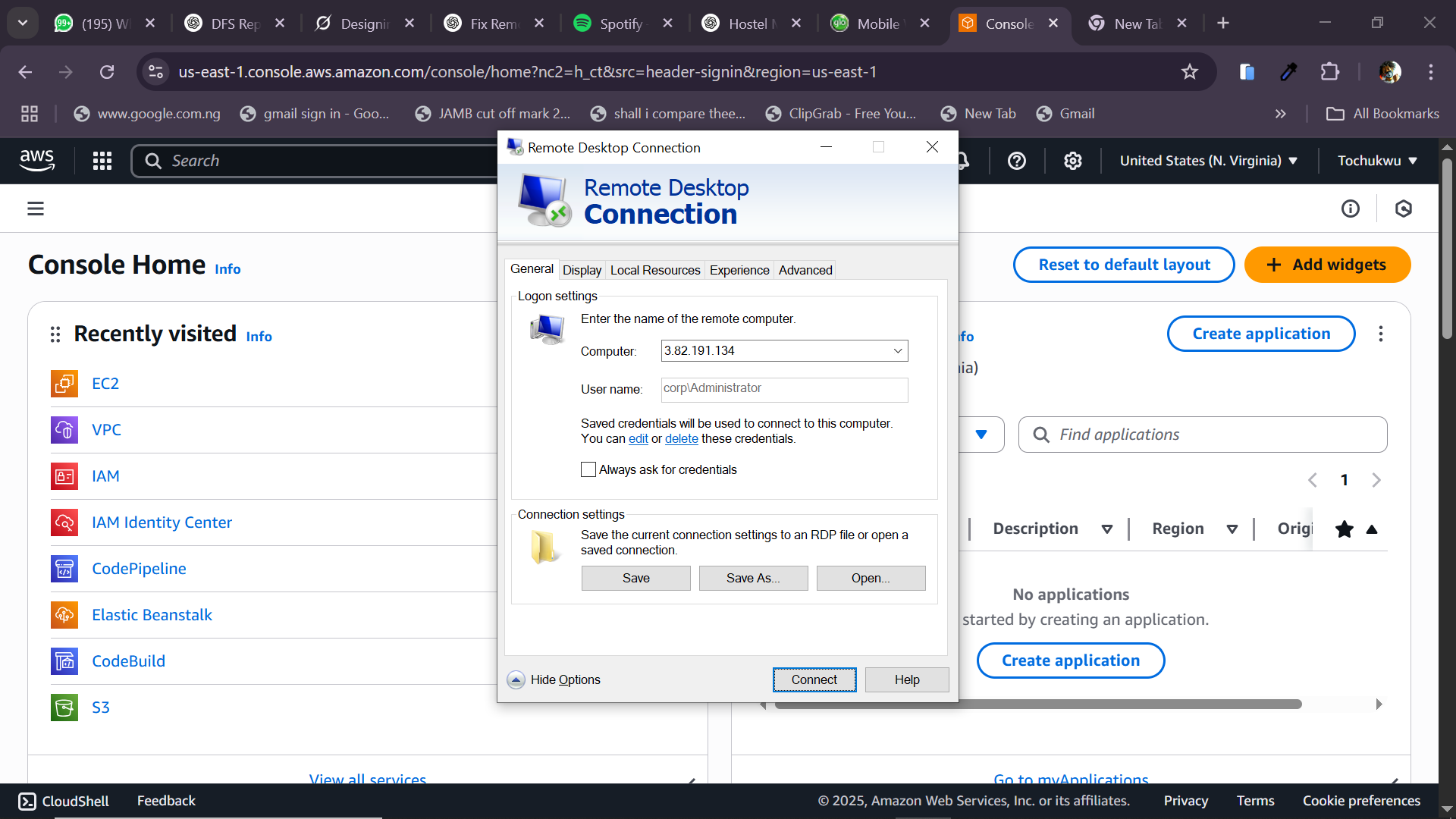
```powershell

Install-WindowsFeature AD-Domain-Services -IncludeManagementTools

Install-ADDSForest -DomainName "corp.local"

```

3. Reboot and log in as domain admin.



4. In Active Directory Users and Computers:

\* Create OUs: `HR`, `Finance`, `Marketing`

\* Create groups: `HR-Users`, `Finance-Users`, etc.

\* Create users: `hr\_user1`, etc.

STEP 5: Configure File Servers (SRV-FILE01 & SRV-FILE02)

On both:

1. Join Domain

\* System Settings → Join `corp.local`

2. Install DFS Roles:

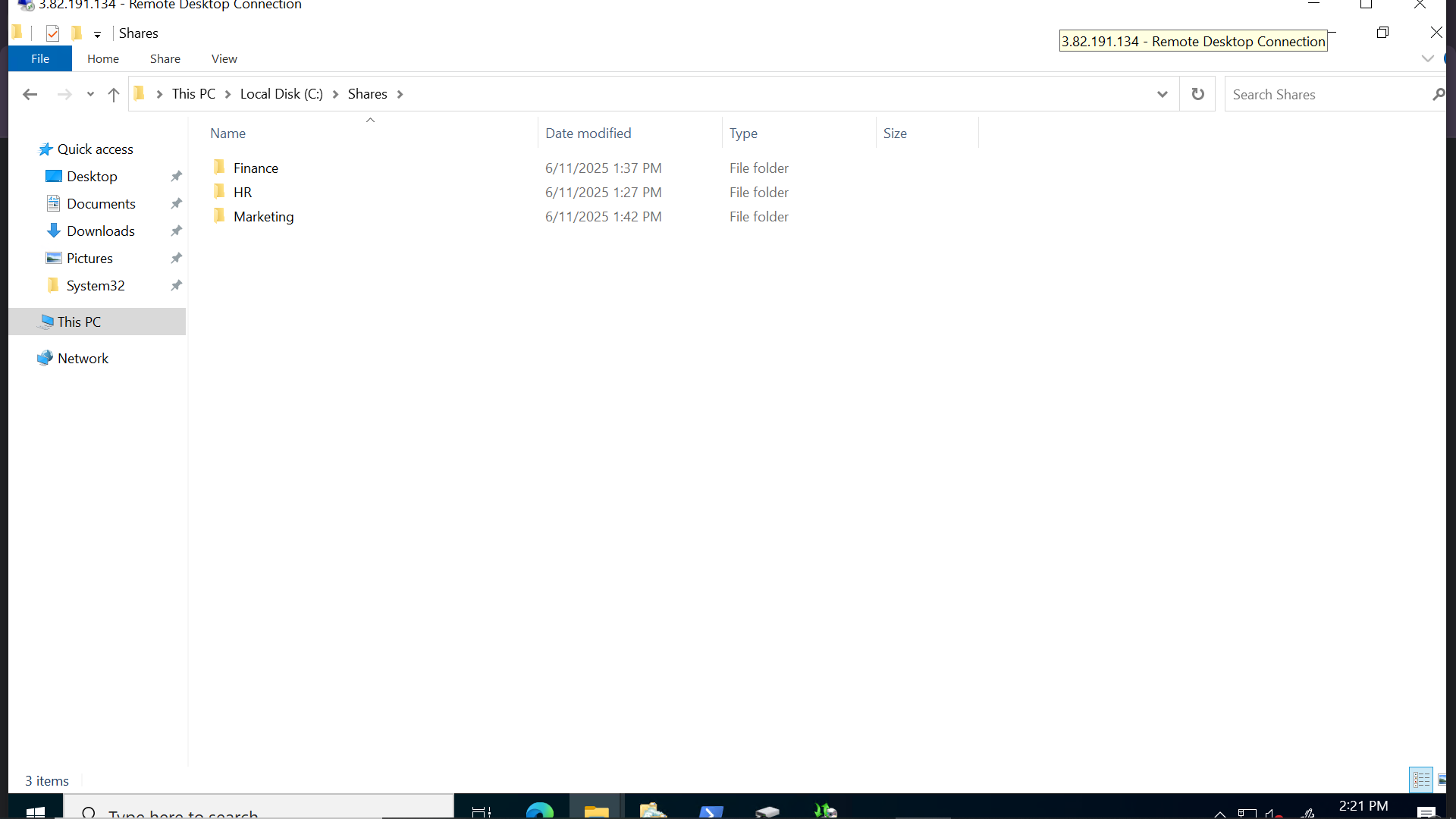
```powershell

Install-WindowsFeature FS-DFS-Namespace, FS-DFS-Replication -IncludeManagementTools

```

3. Create Folders and Shares:

\* D:\HR, D:\Finance, D:\Marketing

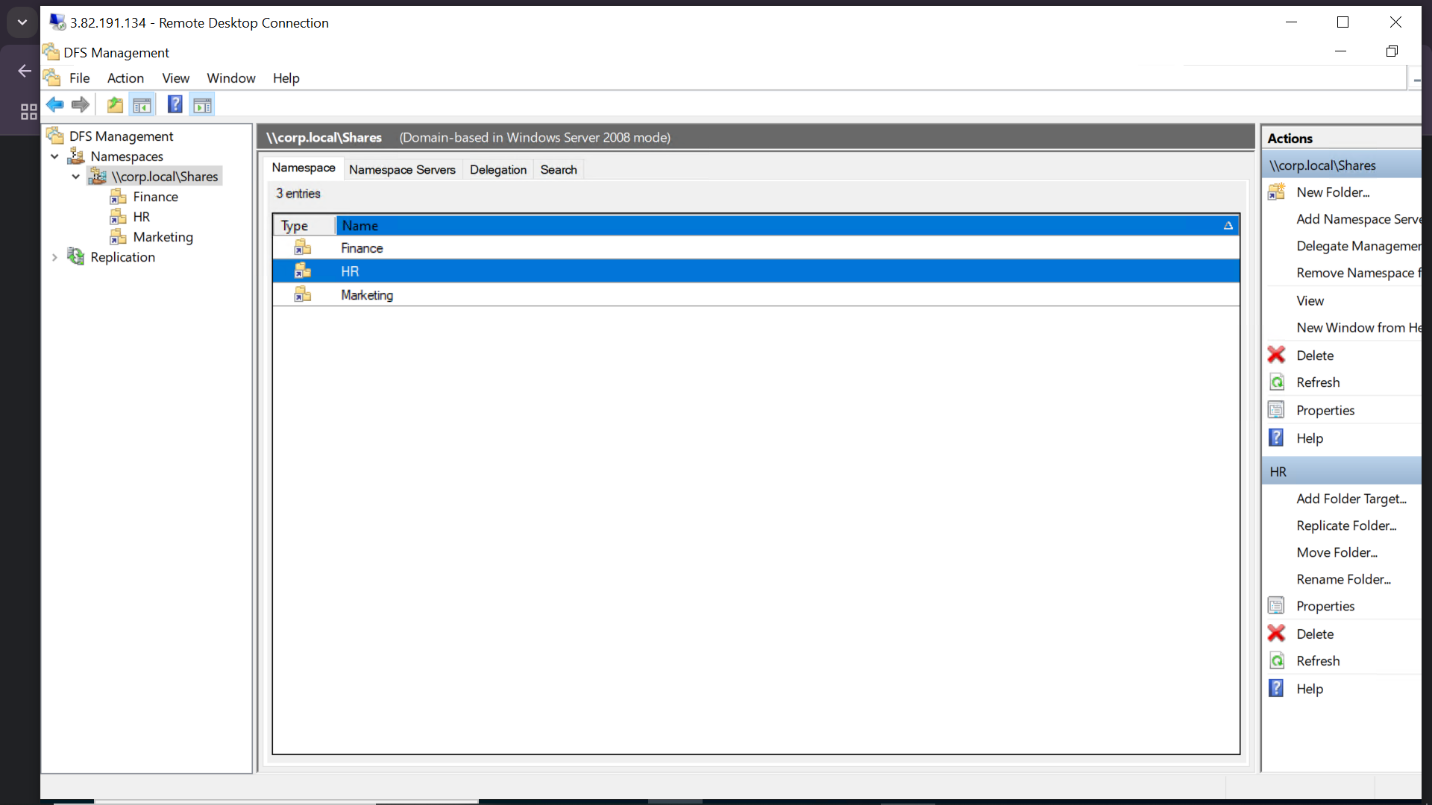


\* Share each and assign NTFS + Share permissions

4. Set Up DFS Namespace

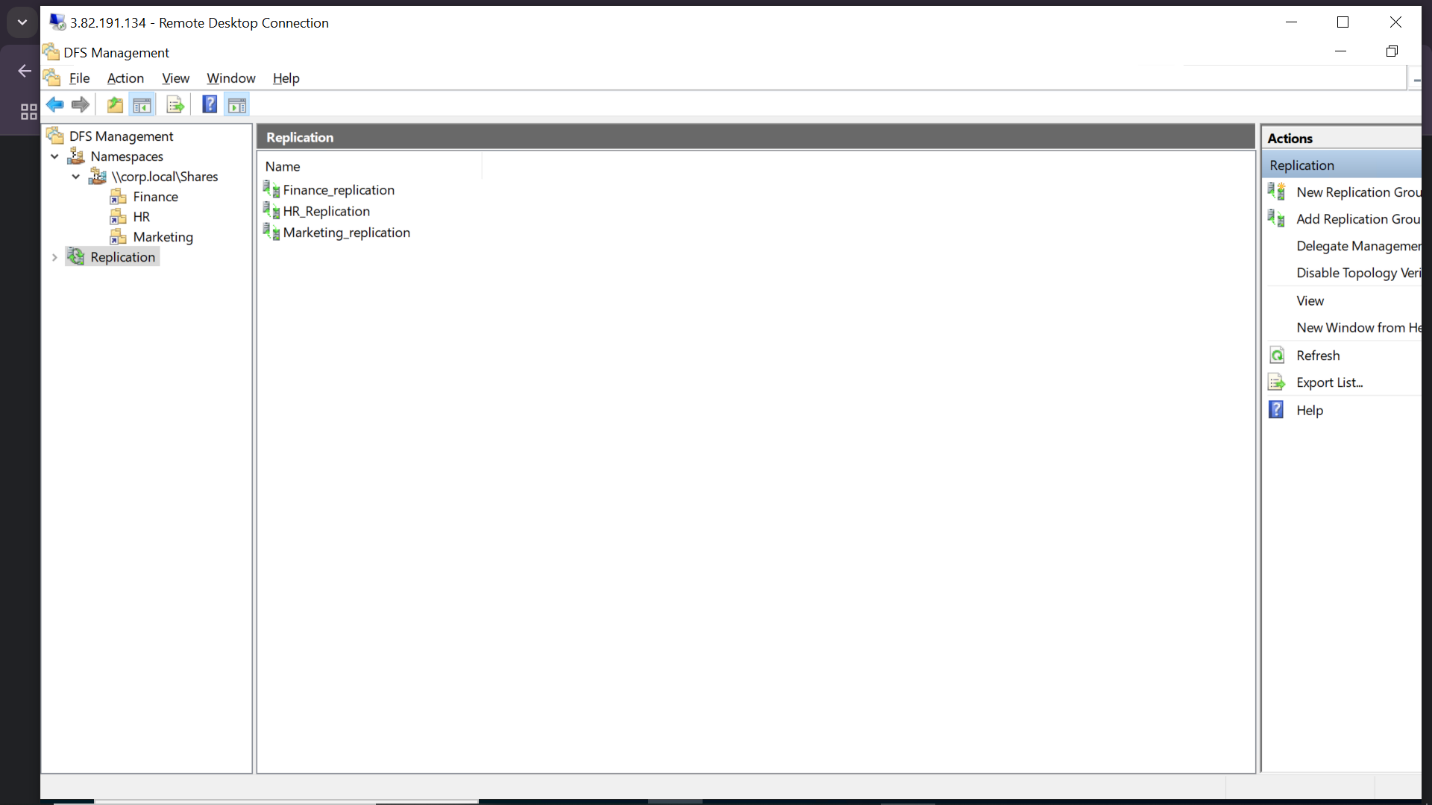
\* Open DFS Management

\* Create Namespace: `\\corp.local\Shares`



\* Add folders from both servers

\* Create Replication Group for each share



STEP 6: Configure Clients (CLIENT1 & CLIENT2)

1. Join Domain

2. Login with test users like `hr\_user1`

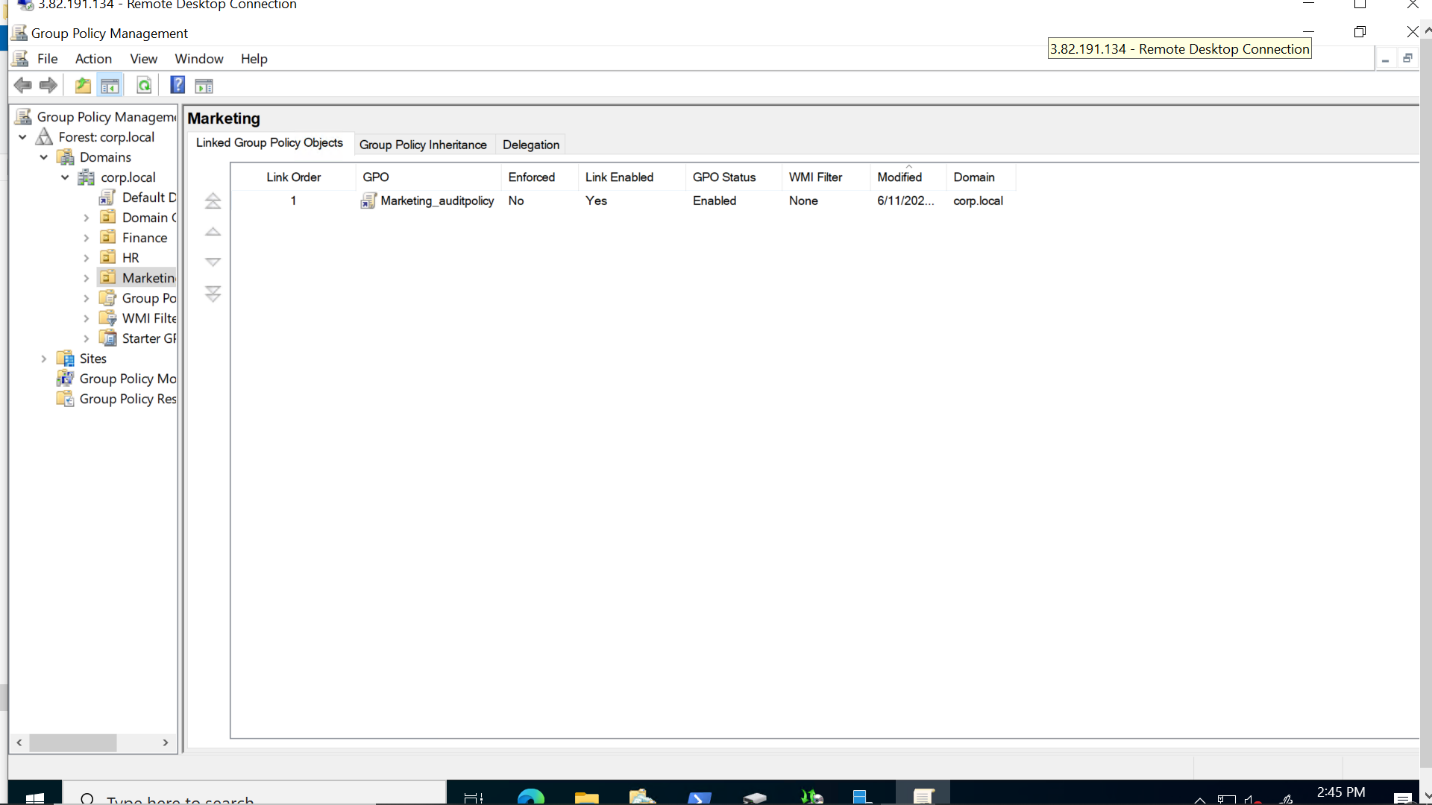
3. Test Access to `\\corp.local\Shares\HR`

STEP 7: Auditing and Backup

A. Auditing:

\* Group Policy:

\* `Computer Config → Policies → Security Settings → Audit Object Access`



\* Enable auditing on folders

B. Backup:

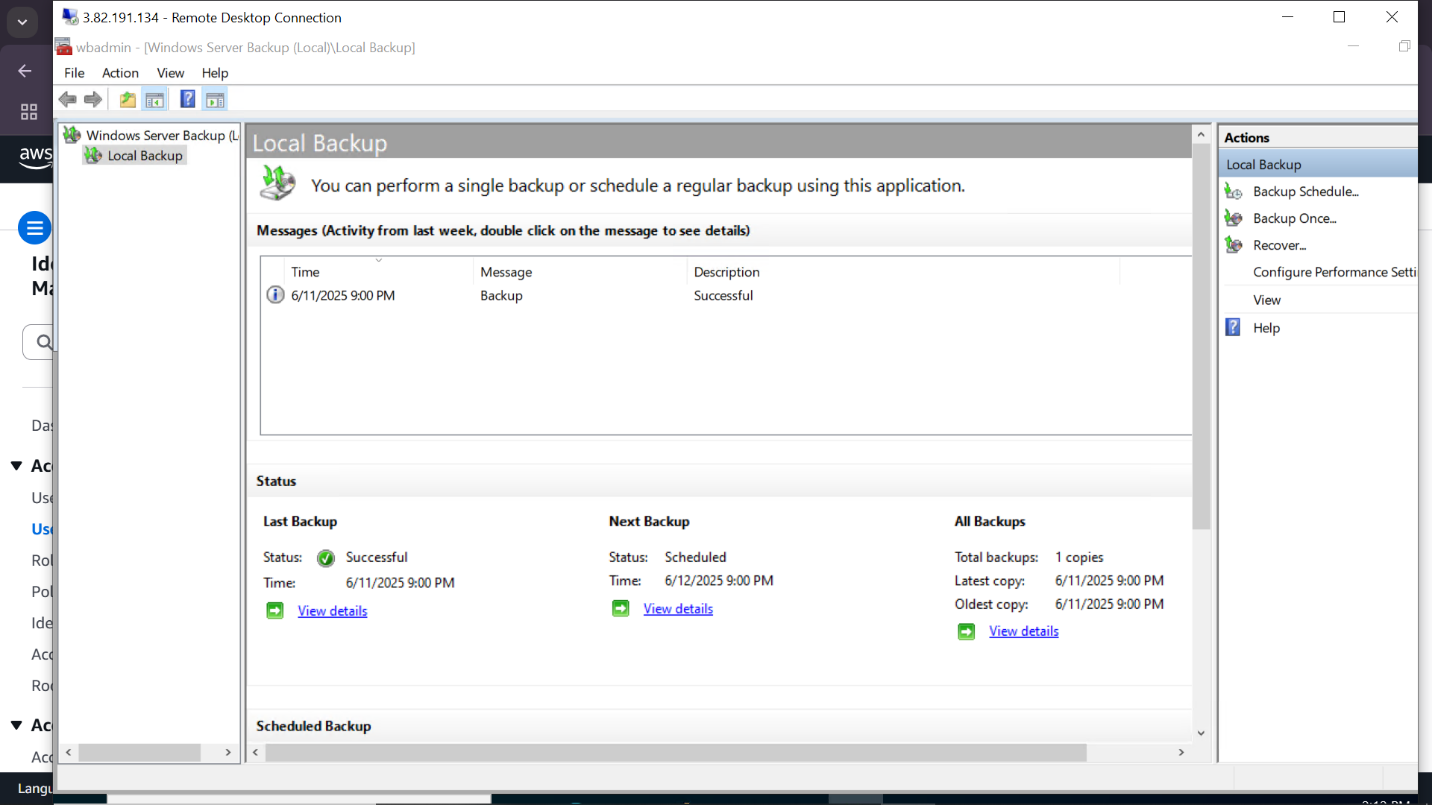
\* Install Windows Server Backup:

```powershell

Install-WindowsFeature Windows-Server-Backup

```

\* Schedule daily backups to D:\ or separate volume



Here is the UML diagram for the project carried out:

