Lab Report

**Lab 02: Dynamic Routing and Access Control List**

**Subject:** Quản trị mạng và hệ thống

**Class:** NT132.N21.1

**Group Members (Group 02):**

|  |  |  |
| --- | --- | --- |
|  | **Students’s names** | **Student ID** |
| 1 | Nguyễn Trần Bảo Quốc | 21520421 |
| 2 | Nguyễn Trọng Tấn Phong | 21522460 |
| 3 | Nguyễn Thành Đăng | 21520683 |
| 4 | Trịnh Tấn Đạt | 21520714 |

|  |
| --- |
| **Self-evaluated Score** |
| **9** |

**Evaluation:**

|  |  |
| --- | --- |
| Total time spent | 5 days |
| Lab Task | • Task 1: Đăng  • Task 2: Phong  • Task 3: Quốc  • Task 4: Đạt  • Report Writing: Đăng |
| Issues *(if any)*  + Difficulty  + Recommendations |  |

Table of Contents

[**A.** **Lab Task** 4](#_Toc135681182)

[1. Active Directory and domain model 4](#_Toc135681183)

[2 Additional Domain Controller 18](#_Toc135681196)

[3 The Active Directory Policies 22](#_Toc135681207)

[4. Read Only Domain Controller 27](#_Toc135681212)

[**B.** **References** 28](#_Toc135681213)

# Lab Task

## Active Directory and domain model

### Set the Primary DNS Suffix to group2.local.

**Step 1**: Open Control panel.

**Step 2**: Choose System and Security.

**Step 3**: Choose System.

**Step 4**: Advance System settings.

**Step 5**: Choose Computer Name.

**Step 6**: Choose Change button.

**Step 6**: Choose Domain and setname.

**Step 7**: Choose More button.

**Step 8**: Set name and choose OK button.

**Step 9**: Choose OK button.

A screenshot of a computer

Description automatically generated

### Install the Active Directory Domain Service (AD DS).

**Step 1**: Server Manager -> Manager -> Add roles and features -> Next

**Step 2**: Choose Role-based or feature-based installation -> Next

**Step 3**: Choose Domain you want to install

**Step 4**: Check Active Directory Domain Services -> Next

**Step 5**: Choose features you want to install

**Step 6**: Install

A screenshot of a computer

Description automatically generated

### Promote this server to a domain controller. You need to create a new forest that its "root domain name" is groupX.local and set the “BIOS domain name" to UIT during promoting.

**Step 1**: Choose Warning icon in the top left corner of the screen.

**Step 2**: Check root domain “group2.local” on “Add a new forest” radio.

**Step 3**: Set password.

**Step 4**: Set Bios domain name “UIT”.

**Step 5**: Next -> Next -> Install.

A screenshot of a computer

Description automatically generated

A computer screen shot of a computer

Description automatically generated with low confidence

### Log in to Domain Controler with UIT\Administrator account.

A screenshot of a computer

Description automatically generated

### Create a new account for your group’s members. The username is student’s ID and the password is 123 on Active Directory. You may create and manage users though the "Active Directory User and Computer" tool.

Set policy password:

**Step 1**: Server Manager -> Tool -> Group Policy Management.

**Step 2:** Choose “Group Policy” in node Domain (tree view).

**Step 3:** Right click on “Default Domain Policy” -> Edit.

**Step 4:** Policies -> Windows settings

**Step 5**: Choose node “Account Policy” in node “Security”.

**Step 6**: Customize Password Policy you want.

**Step 7**: Input command “gpupdate /force” in cmd to update policies.

Log in Domain Controler:

**Step 1**: Server Manager -> Tool -> Active Directory Users and Computers

**Step 2**: Click right mouse on folder “User” in my domain to choose “New” -> “User”.

**Step 3**: In “New Object – User” dialog box, input user’s first name, last name and user’s login name (Student’s ID).

**Step 4**: Input password and confirm (123).

**Step 5**: Choose “Next”, then choose “Finish”.

A screenshot of a computer

Description automatically generated

### Join file server to groupX.local domain

**Step 1**: Open Control panel.

**Step 2**: Choose System and Security.

**Step 3**: Choose System.

**Step 4**: Advance System settings.

**Step 5**: Choose Computer Name.

**Step 6**: Choose “Change settings” button.

**Step 7**: Check “Domain” and join domain you want (group2.local).

**Step 8**: Choose “OK” button.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

### Create new folders.

A computer screen shot of a computer

Description automatically generated with low confidence

### All users (account on Active Directory) can access the folder Data. But only Administrator can write on it.

**Step 1**: Open folder need to edit.

**Step 2**: Choose assign permissions for folders you want.

**Step 3**: Right click on it.

**Step 4**: Choose “Sharing” tab.

**Step 5**: Choose “Advanced Sharing” -> Check “Share this folder”.

**Step 6**: Permissions -> Remove “Everyone” -> Add -> Advanced.

**Step 7**: Find Users need to edit.

**Step 8**: OK -> OK -> check “Read” -> OK -> OK.

**Step 9**: Choose “Security” tab.

**Step 10**: Edit permissions (GROUP02 just read) -> OK.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

### Grant the privileges to users on corresponding folders so that your group’s member can write to their folders (student 1, student 2,…).

A computer screen shot of a computer screen

Description automatically generated with low confidence

A screenshot of a computer

Description automatically generated

### Make this host is the member of groupX.local domain.

**Step 1**: Open Control panel.

**Step 2**: Choose System and Security.

**Step 3**: Choose System.

**Step 4**: Advance System settings.

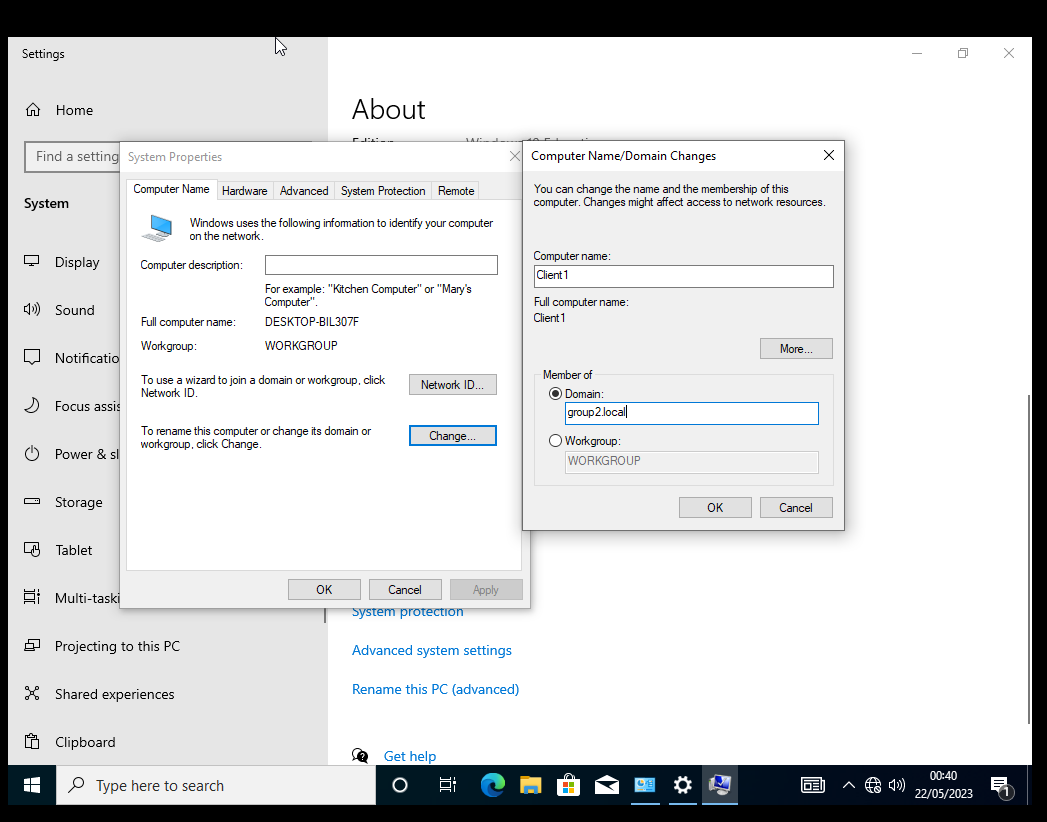
**Step 5**: Choose Computer Name.

**Step 6**: Choose Change button.

**Step 7**: Choose Domain and set name.

**Step 8**: Set Computer name and choose OK button.

**Step 9**: Choose OK button.



### Log in to Windows with account UIT\ (this account is managed on Active Directory). Then access the folder Data on File Server, and test read/write capability.

**Step 1**: Log in account in “Other Account”.

**Step 2**: Input user and password

**Step 3**: Win + R

**Step 4**: Input [\\192.168.1.10](file:///\\192.168.1.10) (IP of File Server)

A screenshot of a computer

Description automatically generated

A computer screen shot of a computer screen

Description automatically generated with low confidence

A picture containing text, screenshot, software, display

Description automatically generated

### Find out the purpose and the difference between Workgroup and Domain.

Workgroup and Domain are two concepts used in computer networks to manage resources and users.

A workgroup is a group of computers that are connected to each other through a LAN (Local Area Network) and share resources such as printers, folders, and files. Workgroup has no main server and computers in Workgroup can be managed independently.

Domain is a model for managing resources and users on a computer network. A domain consists of one or more main servers (domain controllers) to manage resources and users across the entire network. The computers in the Domain are managed by policies set by the Domain Administrator. Domain provides higher security features than Workgroup.

|  |  |
| --- | --- |
| Workgroup | Domain |
| All computers are equivalent and no computer has control over the other | A network administrator uses one or more computers as a server and provides all access and security rights to all other computers on the network. |
| In a workgroup, each computer maintains its own database | Domain is a form of computer network in which computers, printers, and user accounts are registered in a central database. |
| Each computer has its own authentication rules for each user account | Each computer has its own authentication rules for each user account |
| Each computer has set up user accounts. If the user has an account on that computer, only the user can access the computer | Each computer has set up user accounts. If the user has an account on that computer, only the user can access the computer |
| The workgroup is not tied to any security permission or requires any password | Domain users must provide secure login information whenever they access the domain network |
| Machine settings need to be changed manually for each computer in the workgroup | In a domain, changes made in one computer will automatically make the same changes to all other computers on the network. |
| All computers must be on the same local network | In one domain, the computer may be on another local area network |
| In a workgroup, there may be only 20 computers connected | In a domain, thousands of computers can be connected |

## Additional Domain Controller

### Deploy and promote this server to Primary Domain Controller

A screenshot of a computer

Description automatically generated

### Join this server to groupX.local domain

A screenshot of a computer

Description automatically generated

### Deploy and promote this server to an additional domain controller.

**Step 1**: Log out account on DC2.

**Step 2**: Log in Administrator Account on DC1.

**Step 3**: Similar part 1.3.

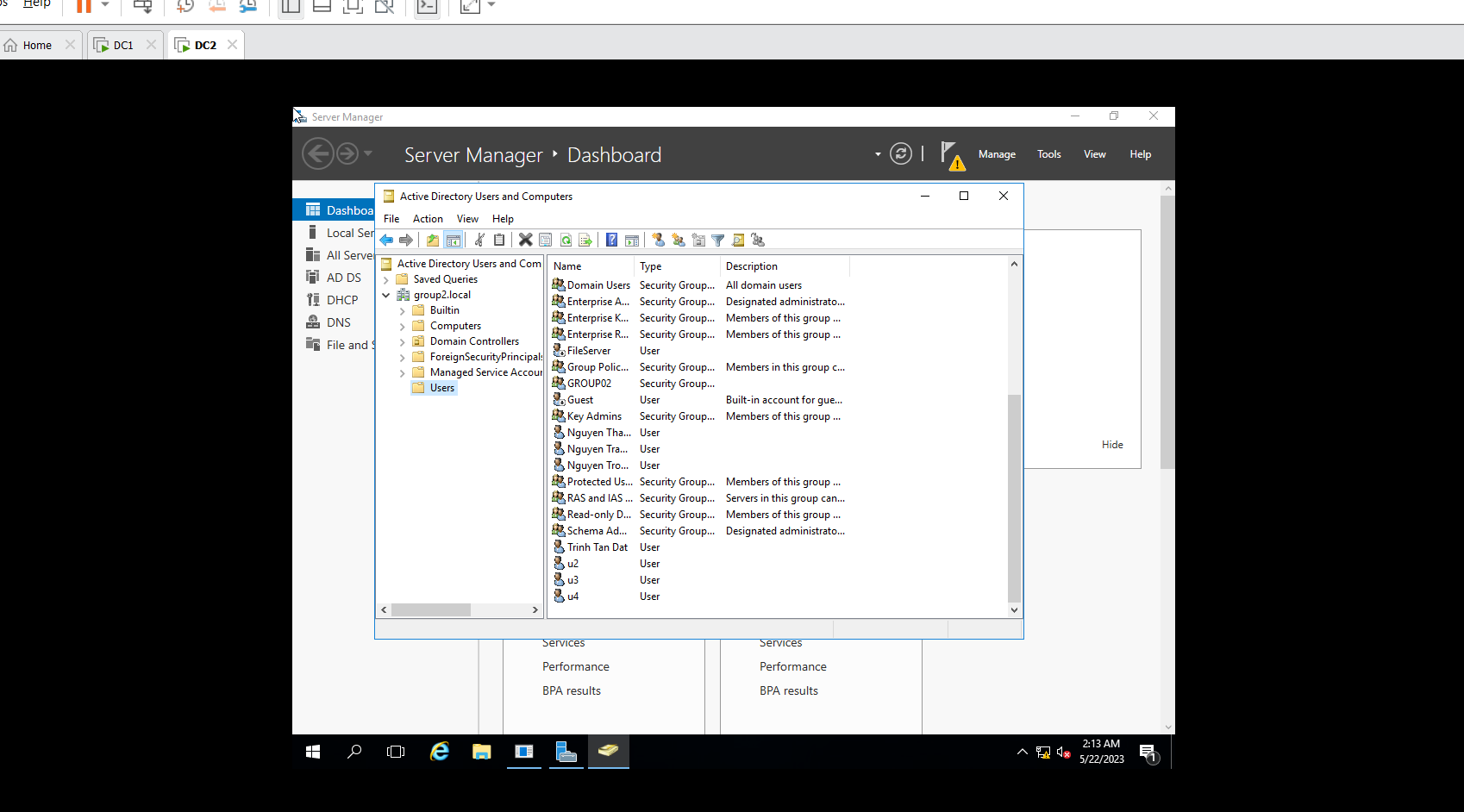
A computer screen shot of a computer

Description automatically generated with low confidence

### On Primary Domain Controller, create new accounts u2/123, u3/123, and u4/123. Then observing on the Additional Domain Controller and verify whether these users are synchronized automatically or not.

Same step as part 1.5.

Additional Controller Domains sync when creating users from Primary Controller Domain



### Can we log in with the account UIT\u2 on Client?

We can log in with the account UIT\u2 on Client.

A screenshot of a computer

Description automatically generated

### Turn off the Primary Domain Controller, then log in with account UIT\u3 on Client. What happened?

When the primary controller is disabled, users cannot log in because the additional domain cannot replace the primary controller in the event that the PCD is not failing.

A screenshot of a login screen

Description automatically generated with low confidence

### Turn off the Additional Domain Controller, then log in with account UIT\u4 on Client. What’s happened?

When turning off the additional domain while the main domain is still active, the user can still log in normally.

The additional controller domain helps balance the load with the main control domain and can replace the main control domain when it fails.

A picture containing text, screenshot, software, computer icon

Description automatically generated

### Turn on the Primary Domain Controller, then log in with account UIT\u5 on Client. What’s happened?

When Primary Domain Controller is enabled, the client can still access it if it has been connected to the domain before. However, if the Primary Domain Controller is turned off or disconnected, the client will not be able to access the domain.

### Turn on the Additional Domain Controller, then log in with account UIT\u5 on Client. What’s happened?

When Additional Domain Controller is enabled, the client can still access it as usual1. However, enabling an additional Domain Controller will help with load balancing of services and reduce the risk of critical services crashing.

### From what you observe, let's briefly summarize the ADC model. Can the controller's workload be shared with all controllers on the domain (typically called load balancing) to avoid overloading?

The ADC (Additional Domain Controller) model is a model in which multiple controllers on the domain share the workload to avoid overloading. An ADC is a server configured to replicate data from the main server (PDC) and keep the data synchronized between the servers. ADCs can be used to load balance servers on a domain.

## The Active Directory Policies

### 3.1 Automatically set the picture specified by the domain's administrator as the desktop wallpaper when the user logs in any computer on domain

**Step 1**: Server Manager -> Tool -> Group Policy Management.

**Step 2**: Right click on domain need to set background, then choose “Create a GP0 in this dom ain, and Link it here…”

**Step 3**: Edit the file you just created.

**Step 4**: User Configuration -> Administrative Temp -> Desktop -> Desktop

**Step 5**: Choose Desktop Wallpaper.

**Step 6**: Check “Enable” and paste the shared photo link for all users.

**Step 7**: Choose “OK” button.

**Step 8**: Enter the command “gpupdate /force” in cmd.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

### Prevent clients from using external storage devices (such as USB, CD, DVD,…)

**Step 1**: Server Manager -> Tool -> Group Policy Management.

**Step 2**: Right click on domain to choose “Create a GP0 in this domain, and Link it here…”

**Step 3**: Edit the file you just created.

**Step 4**: Policies -> Administrative Templates -> System -> Removable Storage Access.

**Step 5**: Open “All Removable Storage classes: Deny all access”.

**Step 6**: Check “Enable” -> “OK” button.

**Step 7**: Enter the command “gpupdate /force” in cmd.

A screenshot of a computer

Description automatically generated

### Prevent users on the domain using Task Manager or CMD.

Task Manager:

**Step 1**: Server Manager -> Tool -> Group Policy Management.

**Step 2**: Right click on domain to choose “Create a GP0 in this domain, and Link it here…”

**Step 3**: Edit the file you just created.

**Step 4**: Policies -> Administrative Templates -> System -> Ctrl + Alt + Del Options

**Step 5**: Open “All Removable Storage classes: Deny all access”.

**Step 6**: Check “Enable” -> “OK” button

A screenshot of a computer

Description automatically generated

CMD:

**Step 1**: Server Manager -> Tool -> Group Policy Management.

**Step 2**: Right click on domain to choose “Create a GP0 in this domain, and Link it here…”

**Step 3**: Edit the file you just created.

**Step 4**: Policies -> Administrative Templates -> System -> Removable Storage Access.

**Step 5**: Open “All Removable Storage classes: Deny all access”.

**Step 6**: Check “Enable” -> “OK” button

A screenshot of a computer

Description automatically generated

**End**: Enter the command “gpupdate /force” in cmd.

### Automatically distribute a program to client computers or users.

**Step 1:** Create a folder containing the program that needs to be automatically distributed to users (type: Windows Installer).

**Step 2**: Server Manager -> Tool -> Active Directory Users and Computers

**Step 3**: Right mouse on domain to choose “New” -> “Organizational Unit”

**Step 4**: Set file name.

**Step 5**: Server Manager -> Tool -> Group Policy Management.

**Step 6** Domain (group2.local) then Right click on the file you just created.

**Step 7**: Right click on domain to choose “Create a GP0 in this domain, and Link it here…”

**Step 8**: Edit the file you just created.

**Step 9**: User Configuration -> Policies -> Software settings.

**Step 10**: Right click on “Software installation” -> New -> Package.

**Step 11**: Choose file setup -> Open -> Assigned -> OK.

**Step 12**: Right click on the file you just created and select properties -> Deployment.

**Step 13**: Check “Install this application at logon” in “Deployment options” area.

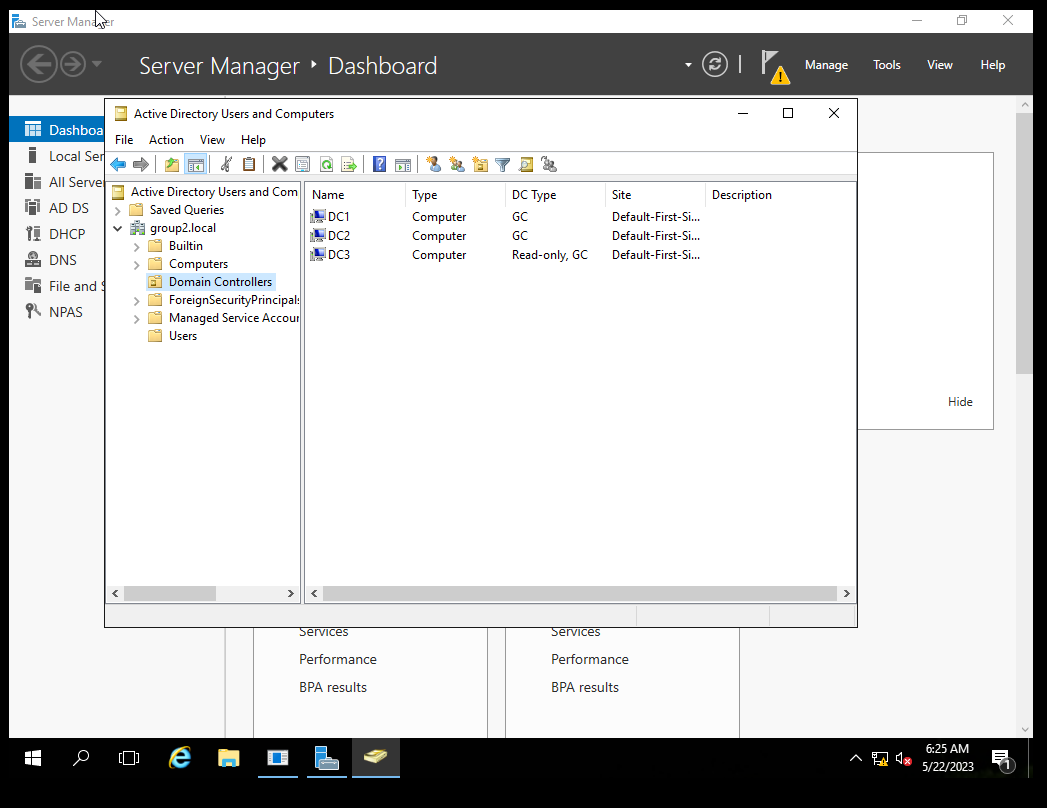
**Step 14**: Choose “Basic” in “Install this application: user interface options” area -> OK

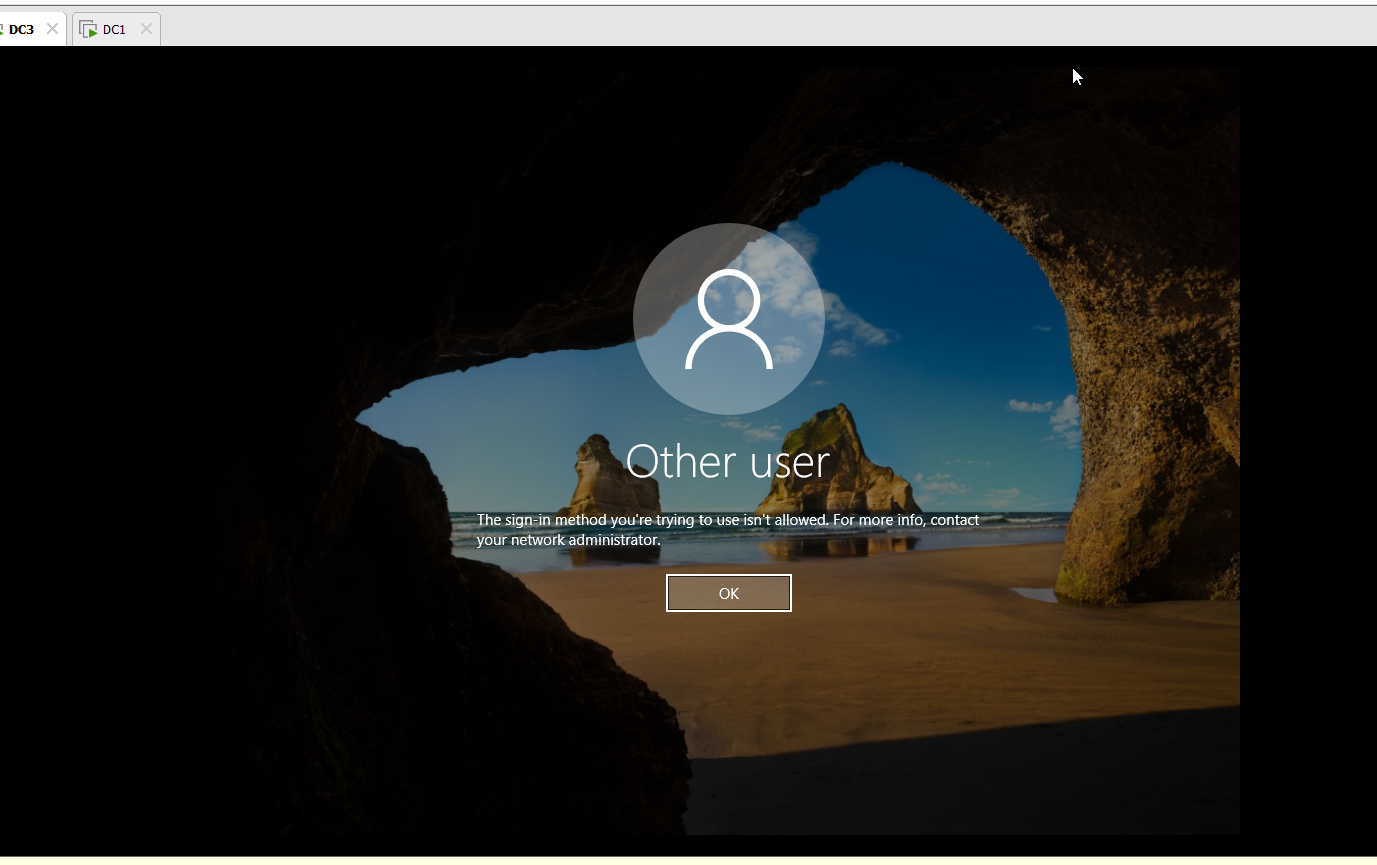
**Step 15**: Enter the command “gpupdate /force” in cmd.

## Read Only Domain Controller

|  |  |  |
| --- | --- | --- |
| Device | IP (DC3) | DNS |
| DC3 | 192.168.1.7 | 192.168.1.5 |
| Client2 | 192.168.1.21 | 192.168.1.5 |

When a user logs in to the RODC, that user only has access to the items that are allowed to read. Users in RODC do not have permission to write and edit files.





A picture containing text, screenshot, software, computer icon

Description automatically generated

# References

<https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview>

<https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/deploy/ad-ds-deployment>