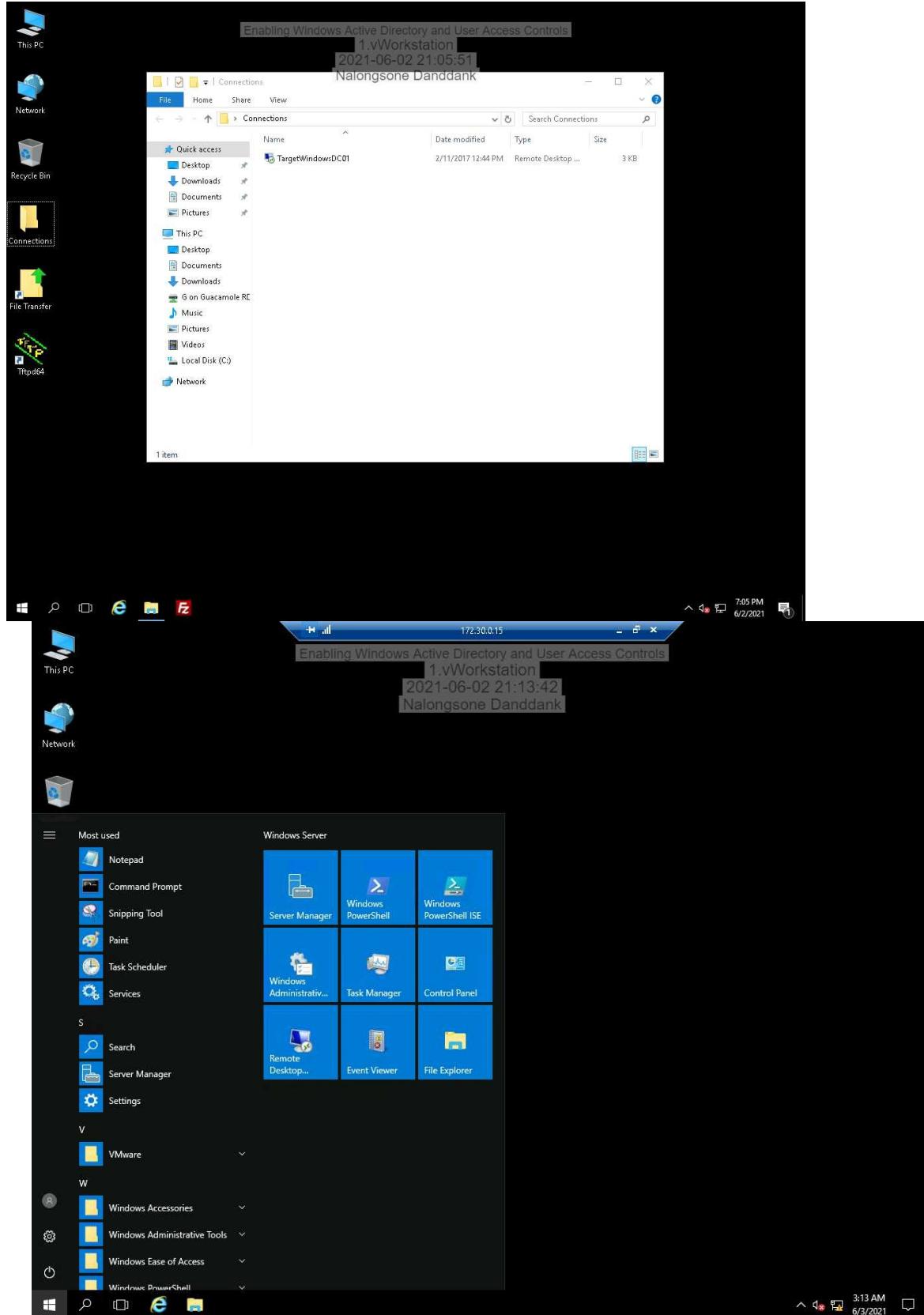
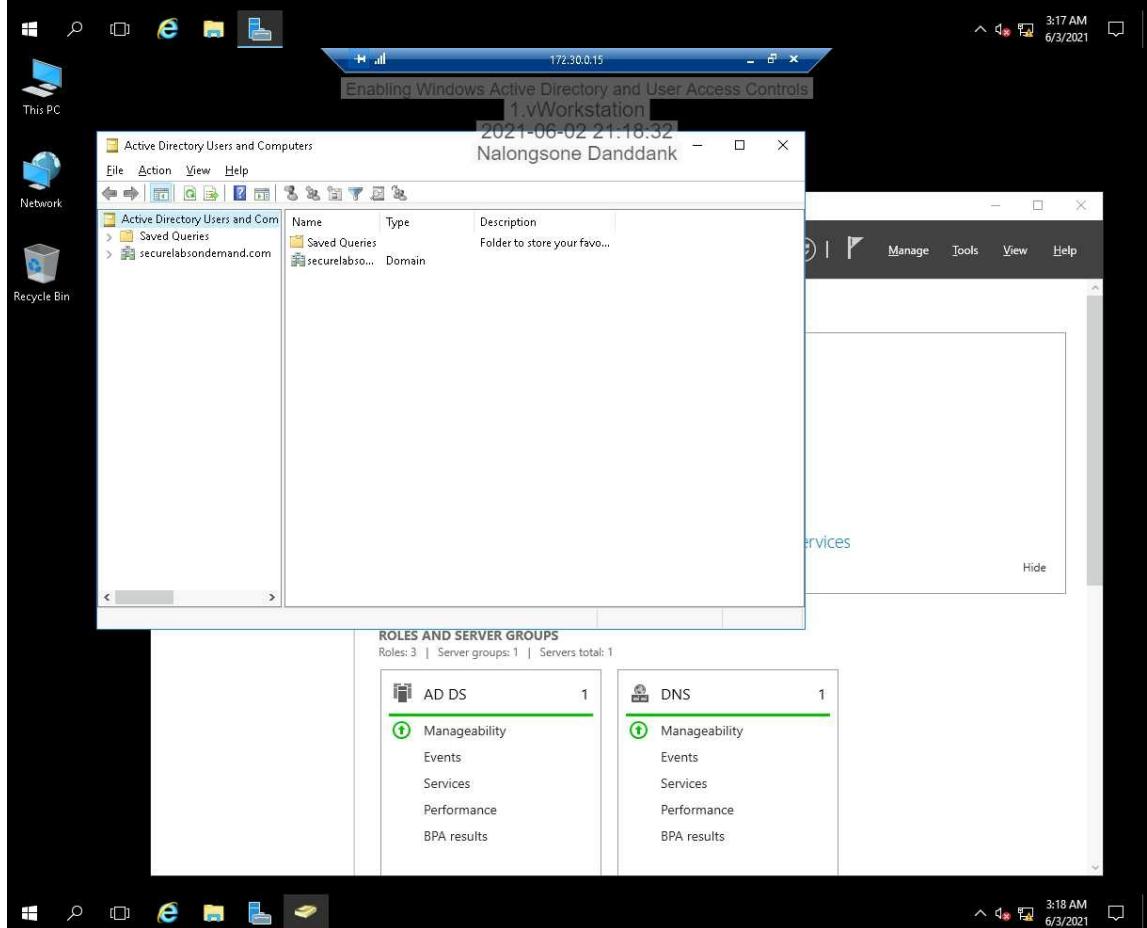
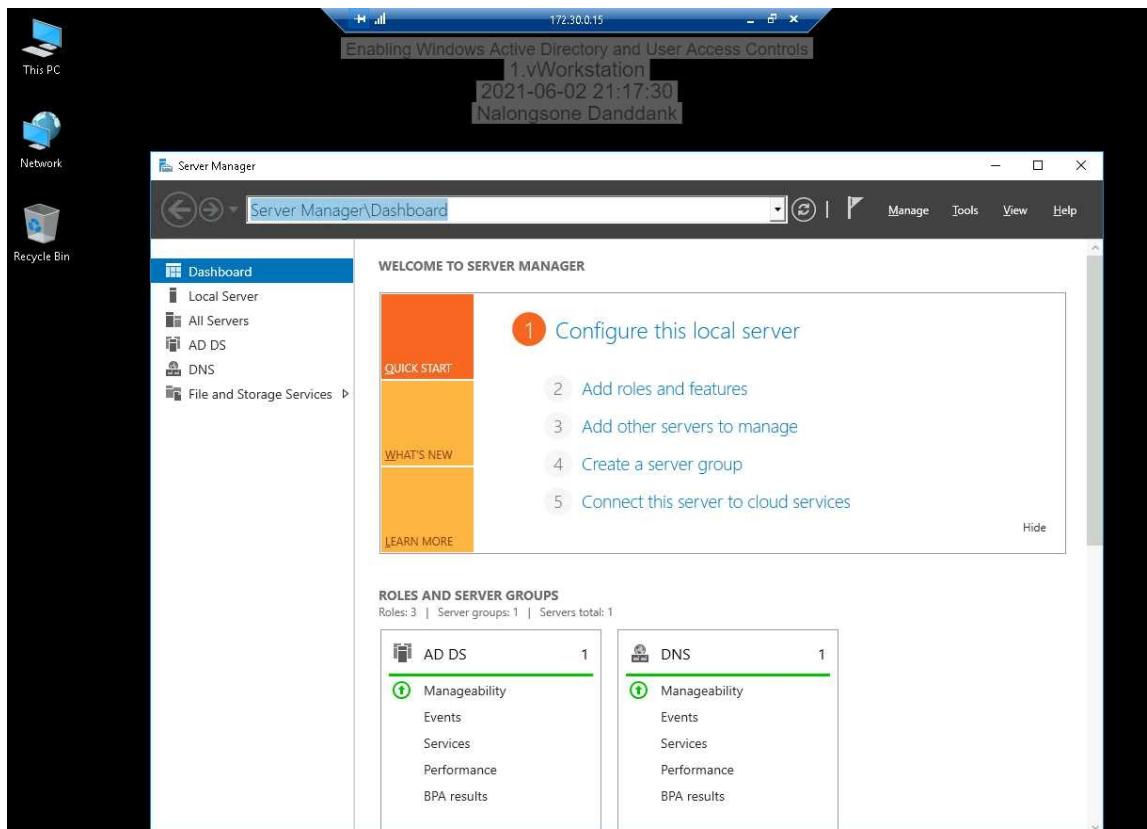
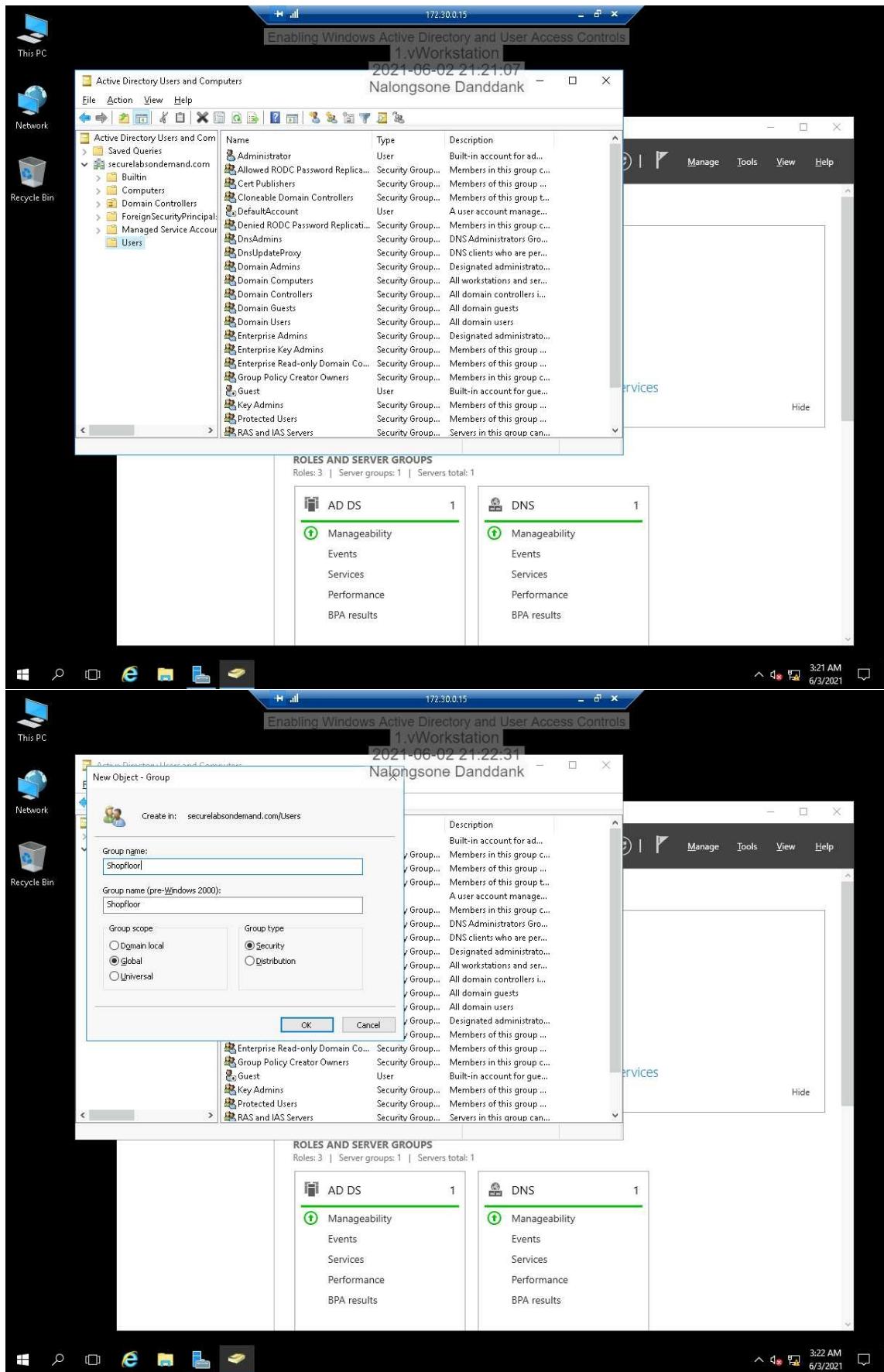


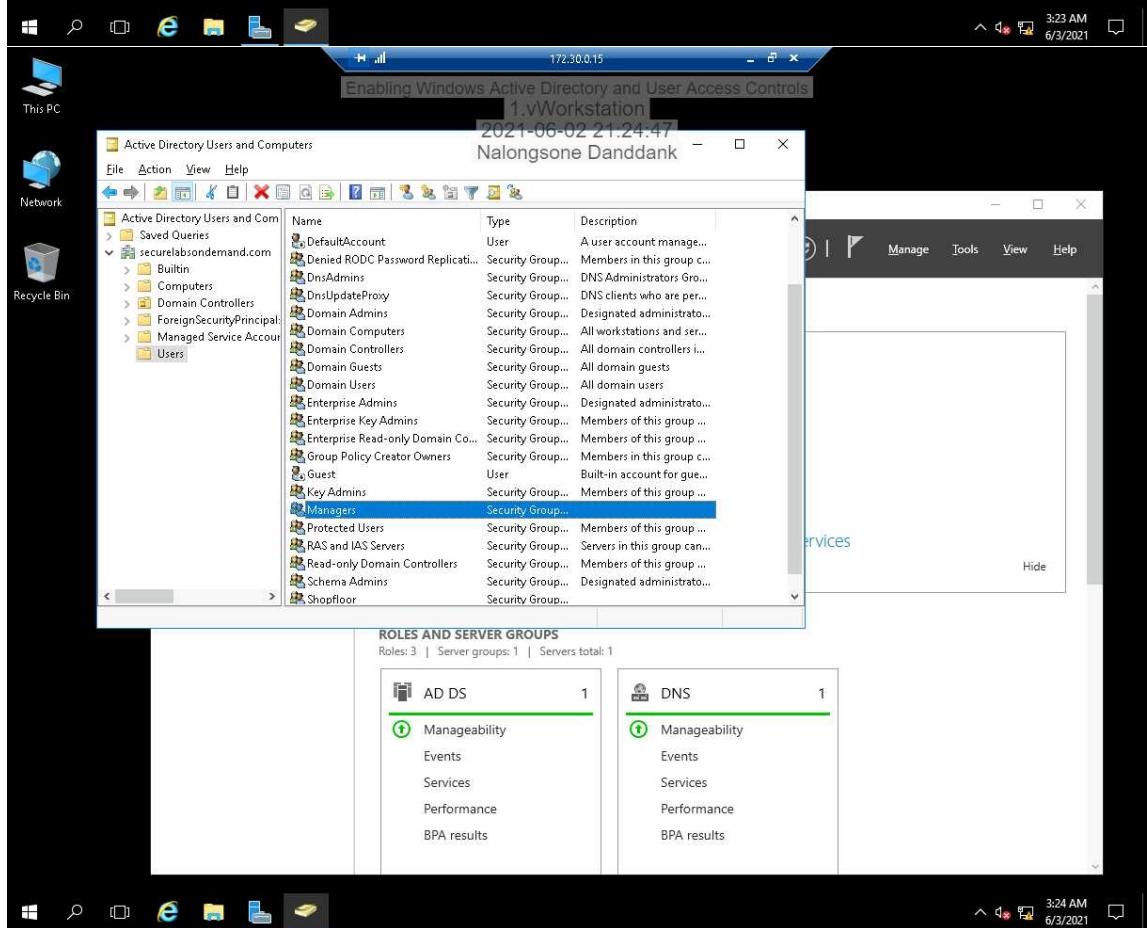
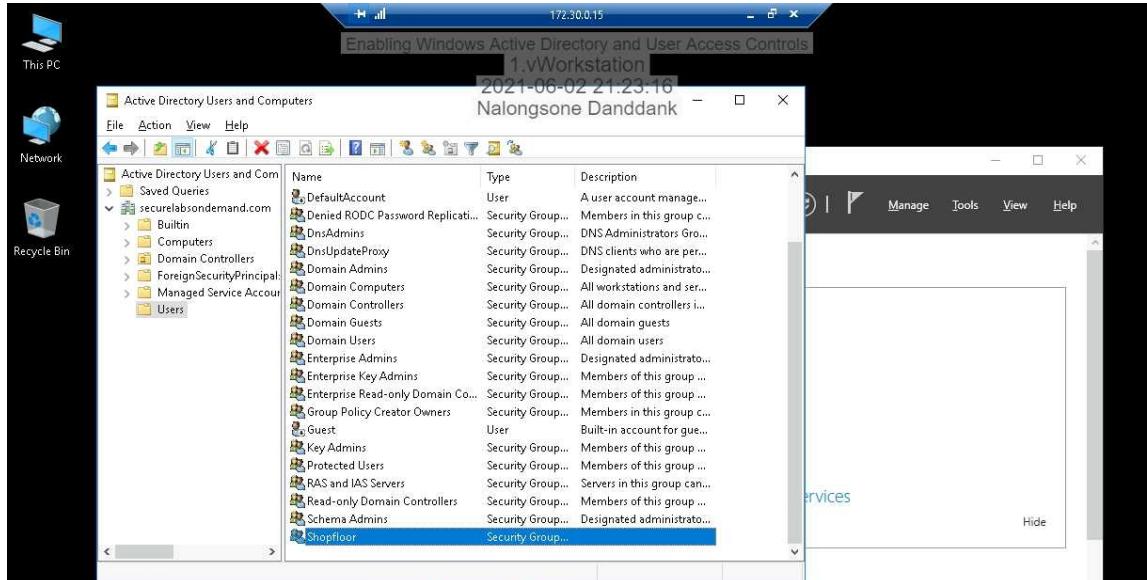
# Enabling Windows Active Directory and User Access Controls

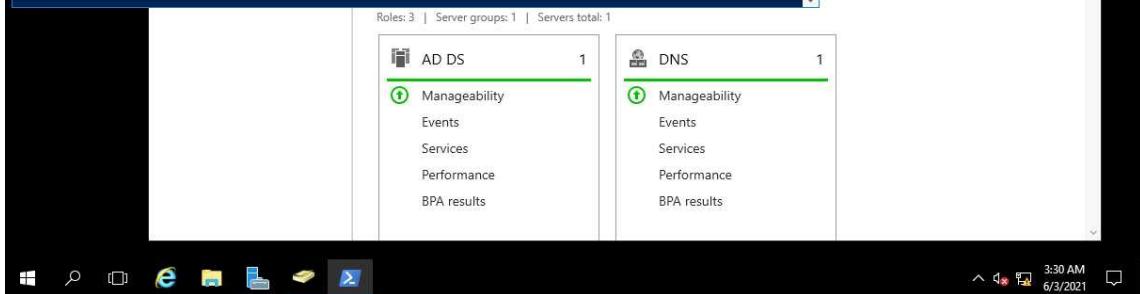
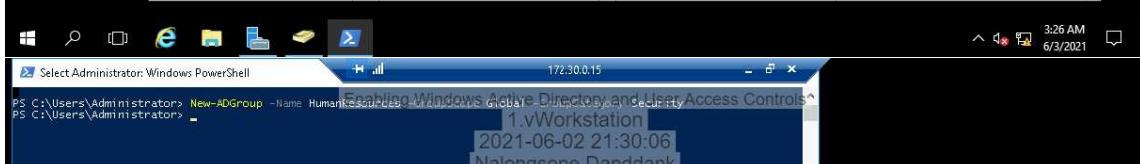
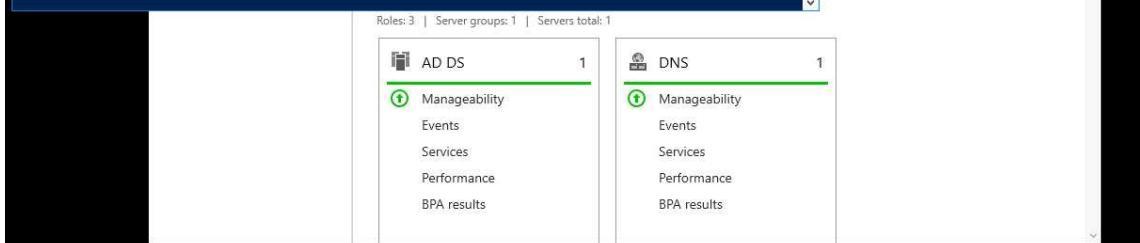
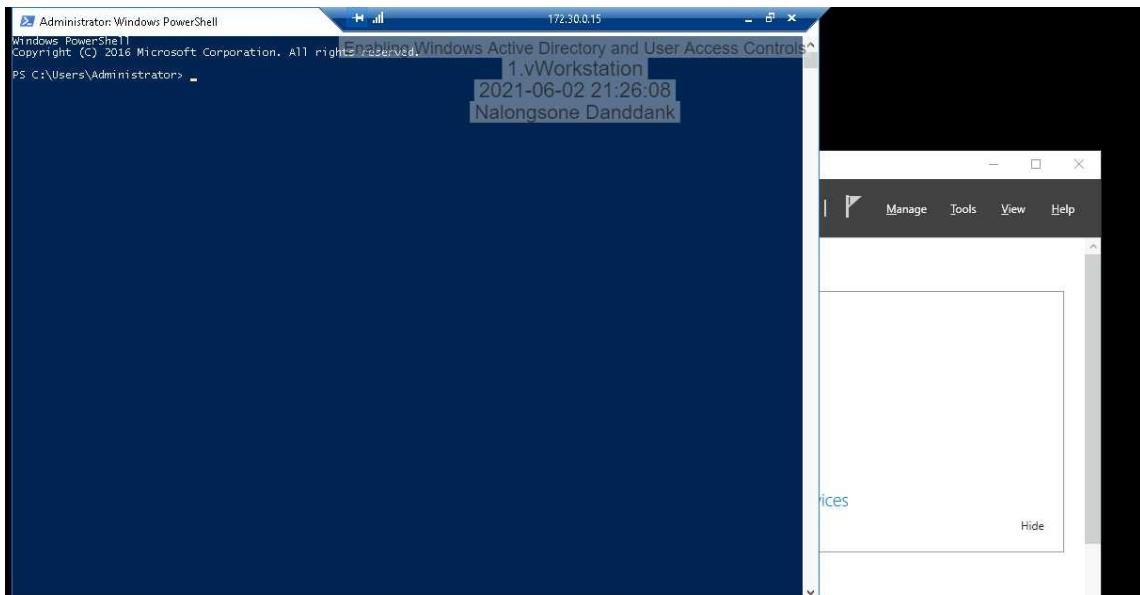
## Part 1: Enabling Windows Active Directory and User Access Controls

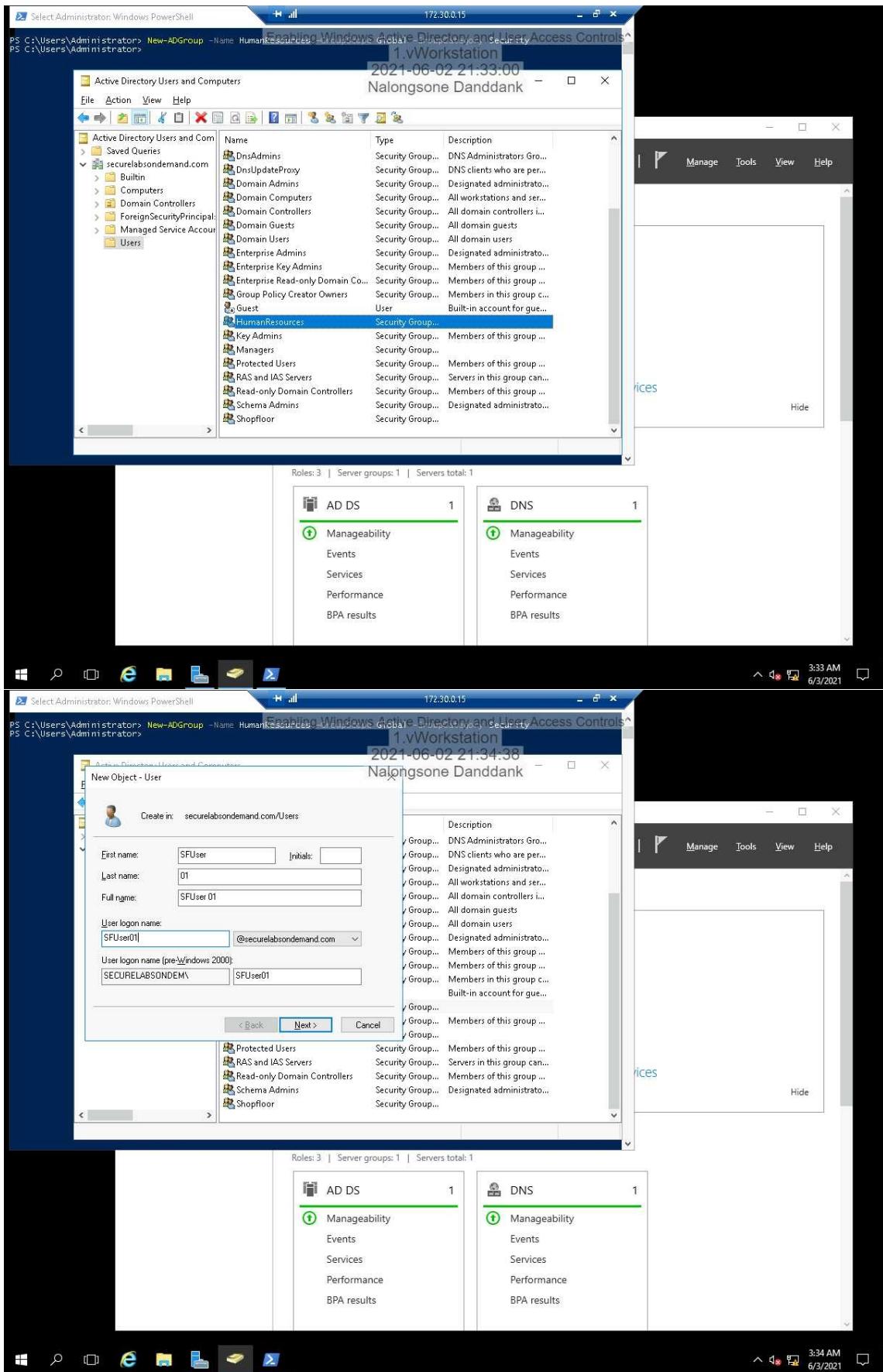












Select Administrator: Windows PowerShell      172.30.0.15

```
PS C:\Users\Administrator> New-ADGroup -Name HumanResources -GroupScope Global -Description "Human Resources department" -Path "OU=Human Resources,DC=securelabsondemand,DC=com"
```

Enabling Windows Active Directory and User Access Controls  
1.vWorkstation  
2021-06-02 21:36:43  
Naljöngsone Danddank

New Object - User

Create in: securelabsondemand.com/Users

Password:  Confirm password:

User must change password at next logon  
 User cannot change password  
 Password never expires  
 Account is disabled

< Back    Next >    Cancel

Description

- / Group... DNS Administrators Gro...
- / Group... DNS clients who are per...
- / Group... Designated administrato...
- / Group... All workstations and ser...
- / Group... All domain controllers ...
- / Group... All domain guests
- / Group... All domain users
- / Group... Designated administrato...
- / Group... Members of this group ...
- / Group... Members of this group ...
- / Group... Members in this group c...
- Built-in account for gue...
- / Group... Members of this group ...
- / Group... Members of this group ...

Protected Users    Security Group...  
RAS and IAS Servers    Security Group...  
Read-only Domain Controllers    Security Group...  
Schema Admins    Security Group...  
Shopfloor    Security Group...

Roles: 3 | Server groups: 1 | Servers total: 1

AD DS 1  
Manageability  
Events  
Services  
Performance  
BPA results

DNS 1  
Manageability  
Events  
Services  
Performance  
BPA results

3:36 AM  
6/3/2021

Select Administrator: Windows PowerShell      172.30.0.15

```
PS C:\Users\Administrator> New-ADGroup -Name HumanResources -GroupScope Global -Description "Human Resources department" -Path "OU=Human Resources,DC=securelabsondemand,DC=com"
```

Enabling Windows Active Directory and User Access Controls  
1.vWorkstation  
2021-06-02 21:37:23  
Naljöngsone Danddank

New Object - User

Create in: securelabsondemand.com/Users

When you click Finish, the following object will be created:

Full name: SFUser01  
User logon name: SFUser01@securelabsondemand.com

< Back    Finish >    Cancel

Description

- / Group... DNS Administrators Gro...
- / Group... DNS clients who are per...
- / Group... Designated administrato...
- / Group... All workstations and ser...
- / Group... All domain controllers ...
- / Group... All domain guests
- / Group... All domain users
- / Group... Designated administrato...
- / Group... Members of this group ...
- / Group... Members of this group ...
- / Group... Members in this group c...
- Built-in account for gue...
- / Group... Members of this group ...
- / Group... Members of this group ...

Protected Users    Security Group...  
RAS and IAS Servers    Security Group...  
Read-only Domain Controllers    Security Group...  
Schema Admins    Security Group...  
Shopfloor    Security Group...

Roles: 3 | Server groups: 1 | Servers total: 1

AD DS 1  
Manageability  
Events  
Services  
Performance  
BPA results

DNS 1  
Manageability  
Events  
Services  
Performance  
BPA results

3:37 AM  
6/3/2021

PS C:\Users\Administrator> New-ADGroup -Name HumanResources -Description "Human Resources department" -GroupScope Global

PS C:\Users\Administrator>

Active Directory Users and Computers

Select Groups

Select this object type:  
Groups or Built-in security principals  
From this location:  
securelabsondemand.com  
Enter the object names to select (examples):  
Shopfloor  
Advanced... OK Cancel

Description

Group... DNS Administrators Gro...  
group... DNS clients who are per...  
group... Designated administrato...  
group... All workstations and ser...  
group... All domain controllers ...  
group... All domain guests  
group... All domain users  
group... Designated administrato...  
group... Members of this group ...  
Enterprise Read-only Domain Co... Security Group... Members of this group ...  
Group Policy Creator Owners Security Group... Members in this group c...  
Guest User Built-in account for gue...  
HumanResources Security Group... Members of this group ...  
Key Admins Security Group... Members of this group ...  
Managers Security Group...  
Protected Users Security Group... Members of this group ...  
RAS and IAS Servers Security Group... Servers in this group can...  
Read-only Domain Controllers Security Group... Members of this group ...  
Schema Admins Security Group... Designated administrato...  
SFUser 01 User  
Shopfloor Security Group...

Roles: 3 | Server groups: 1 | Servers total: 1

AD DS 1 Manageability Events Services Performance BPA results

DNS 1 Manageability Events Services Performance BPA results

3:40 AM 6/3/2021

PS C:\Users\Administrator> New-ADGroup -Name HumanResources -Description "Human Resources department" -GroupScope Global

PS C:\Users\Administrator>

Active Directory Users and Computers

Name Type Description

DnsAdmins Security Group... DNS Administrators Gro...  
DnsUpdateProxy Security Group... DNS clients who are per...  
Domain Admins Security Group... Designated administrato...  
Domain Computers Security Group... All workstations and ser...  
Domain Controllers Security Group... All domain controllers ...  
Domain Guests Security Group... All domain guests  
Domain Users Security Group... All domain users  
Enterprise Admins Security Group... Designated administrato...  
Enterprise Key Admins Security Group... Members of this group ...  
Enterprise Read-only Domain Co... Security Group... Members of this group ...  
Group Policy Cre... Guest  
HumanResources Security Group... Members of this group ...  
Key Admins Security Group...  
Managers Security Group...  
Protected Users Security Group... Members of this group ...  
RAS and IAS Serv... Security Group... Servers in this group can...  
Read-only Domai... Security Group... All domain controllers ...  
Schema Admins Security Group... Designated administrato...  
SFUser 01 User  
Shopfloor Security Group...

The Add to Group operation was successfully completed.

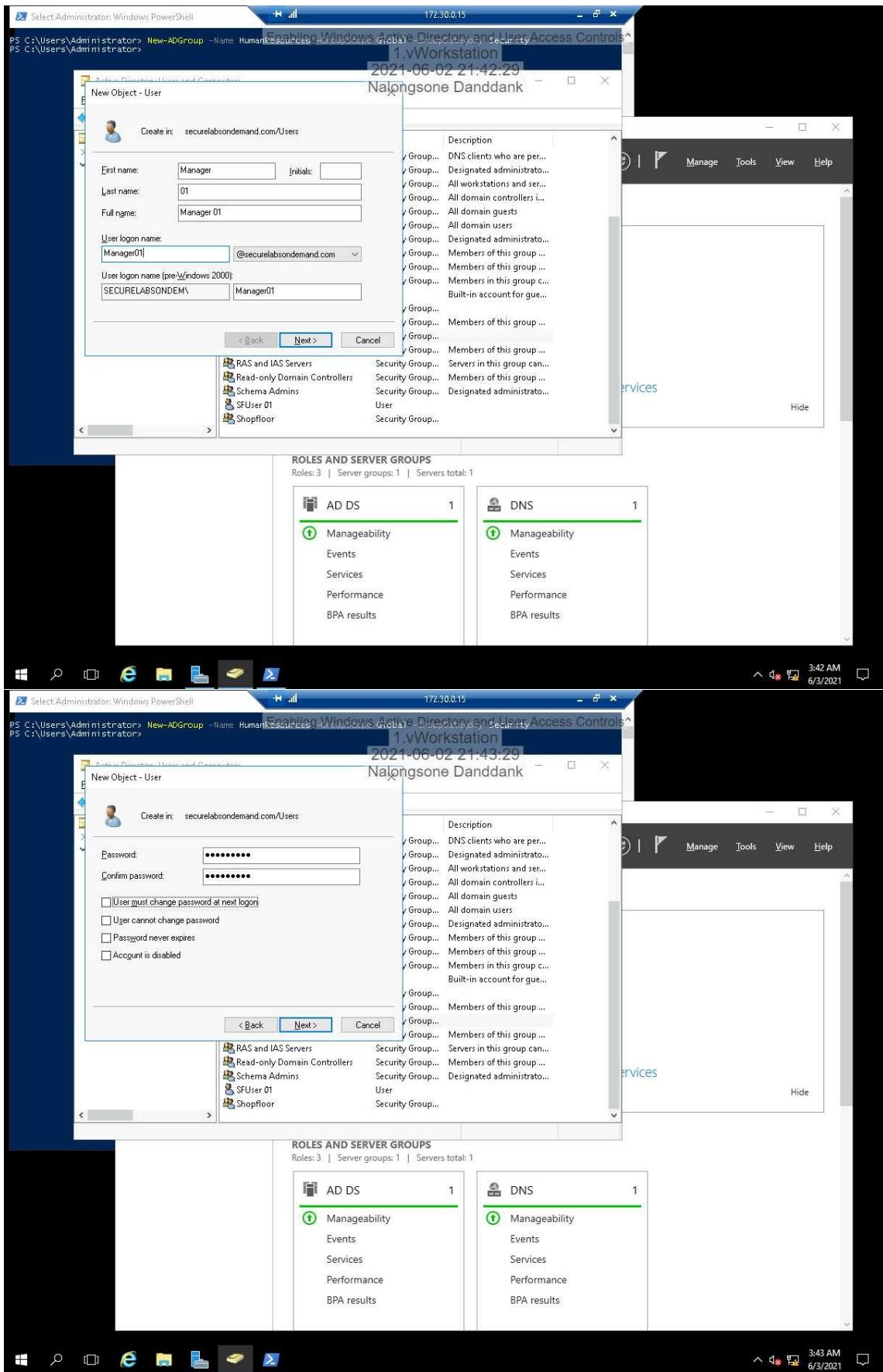
OK

Active Directory Domain Services

AD DS 1 Manageability Events Services Performance BPA results

DNS 1 Manageability Events Services Performance BPA results

3:40 AM 6/3/2021



PS C:\Users\Administrator> New-ADGroup -Name HumanResources -Description "Human Resources department" -GroupScope Global

PS C:\Users\Administrator>

Active Directory Users and Computers

File Action View Help

Name Type Description

- DnsUpdateProxy Security Group... DNS clients who are per...
- Domain Admins Security Group... Designated administrato...
- Domain Computers Security Group... All workstations and ser...
- Domain Controllers Security Group... All domain controllers i...
- Domain Guests Security Group... All domain guests
- Domain Users Security Group... All domain users
- Enterprise Admins Security Group... Designated administrato...
- Enterprise Key Admins Security Group... Members of this group ...
- Enterprise Read-only Domain Co... Security Group... Members of this group ...
- Group Policy Creator Owners Security Group... Members in this group c...
- Guest User Built-in account for gue...
- HumanResources Security Group... Human Resources department
- Key Admins Security Group... Members of this group ...
- Manager 01 User Manager 01
- Managers Security Group... Members of this group ...
- Protected Users Security Group... Servers in this group can...
- RAS and IAS Servers Security Group... Members of this group ...
- Read-only Domain Controllers Security Group... Members of this group ...
- Schema Admins Security Group... Designated administrato...
- SFUser 01 User SFUser 01
- Shopfloor Security Group...

ROLES AND SERVER GROUPS

Roles: 3 | Server groups: 1 | Servers total: 1

Role	Count
AD DS	1
DNS	1

Manageability Events Services Performance BPA results

Manageability Events Services Performance BPA results

Select Groups

Select this object type: Groups or Built-in security principals Object Types...

From this location: securelabsondemand.com Locations...

Enter the object names to select [examples]: Managers Check Names

Advanced... OK Cancel

Description

- Group... DNS clients who are per...
- Group... Designated administrato...
- Group... All workstations and ser...
- Group... All domain controllers i...
- Group... All domain guests
- Group... All domain users
- Group... Designated administrato...
- Group... Members of this group ...
- Group... Members of this group ...

ROLES AND SERVER GROUPS

Roles: 3 | Server groups: 1 | Servers total: 1

Role	Count
AD DS	1
DNS	1

Manageability Events Services Performance BPA results

Manageability Events Services Performance BPA results

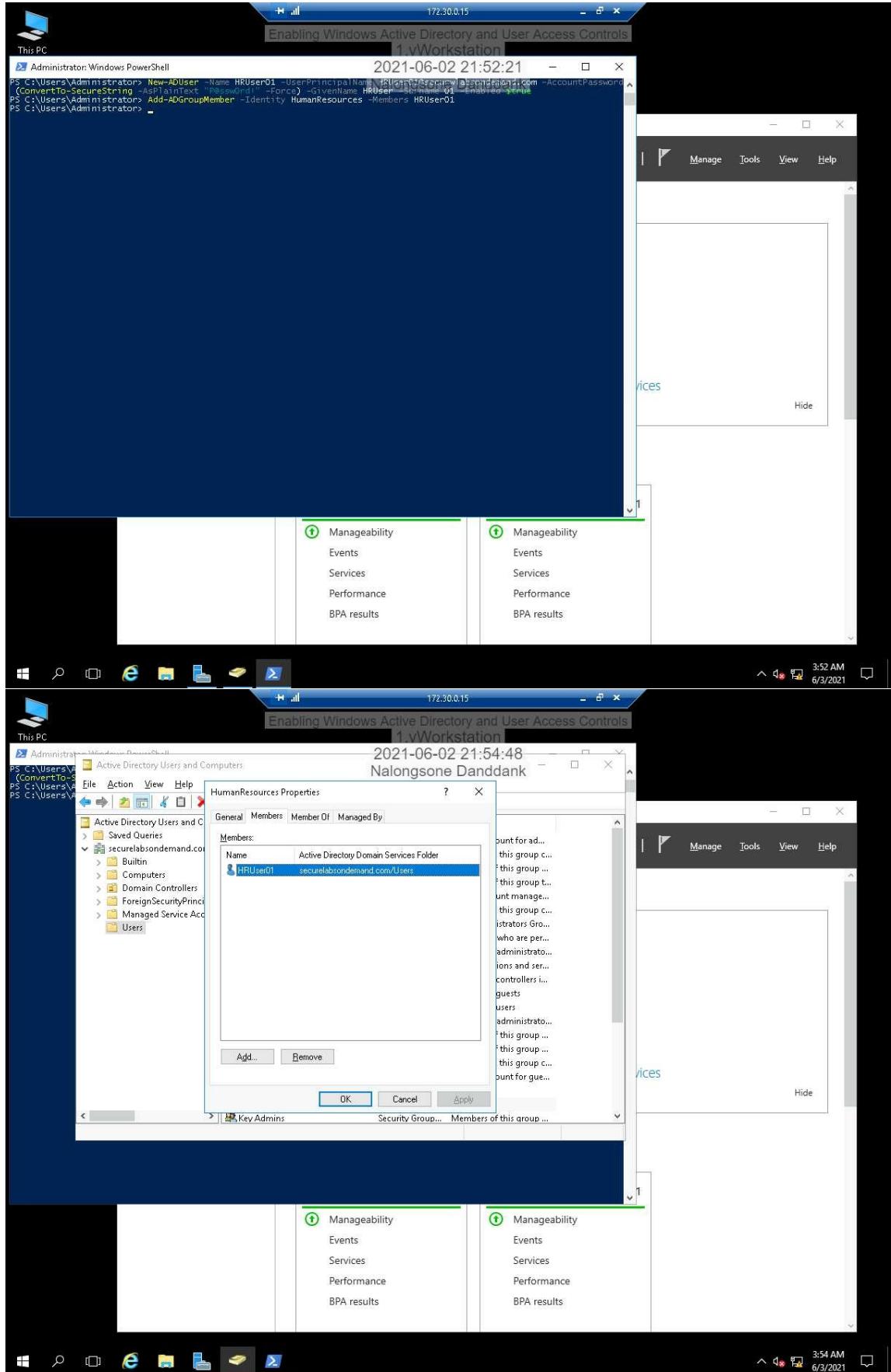
The screenshot displays a Windows desktop environment with two open windows and a taskbar at the bottom.

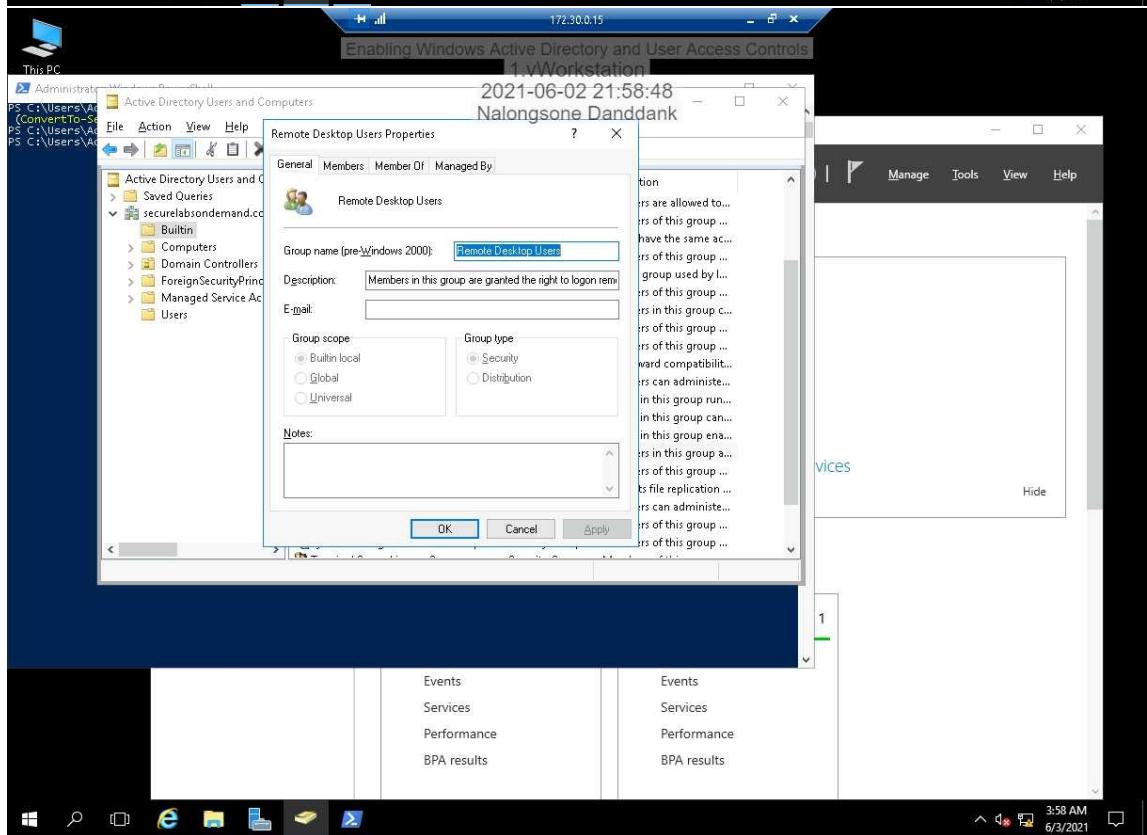
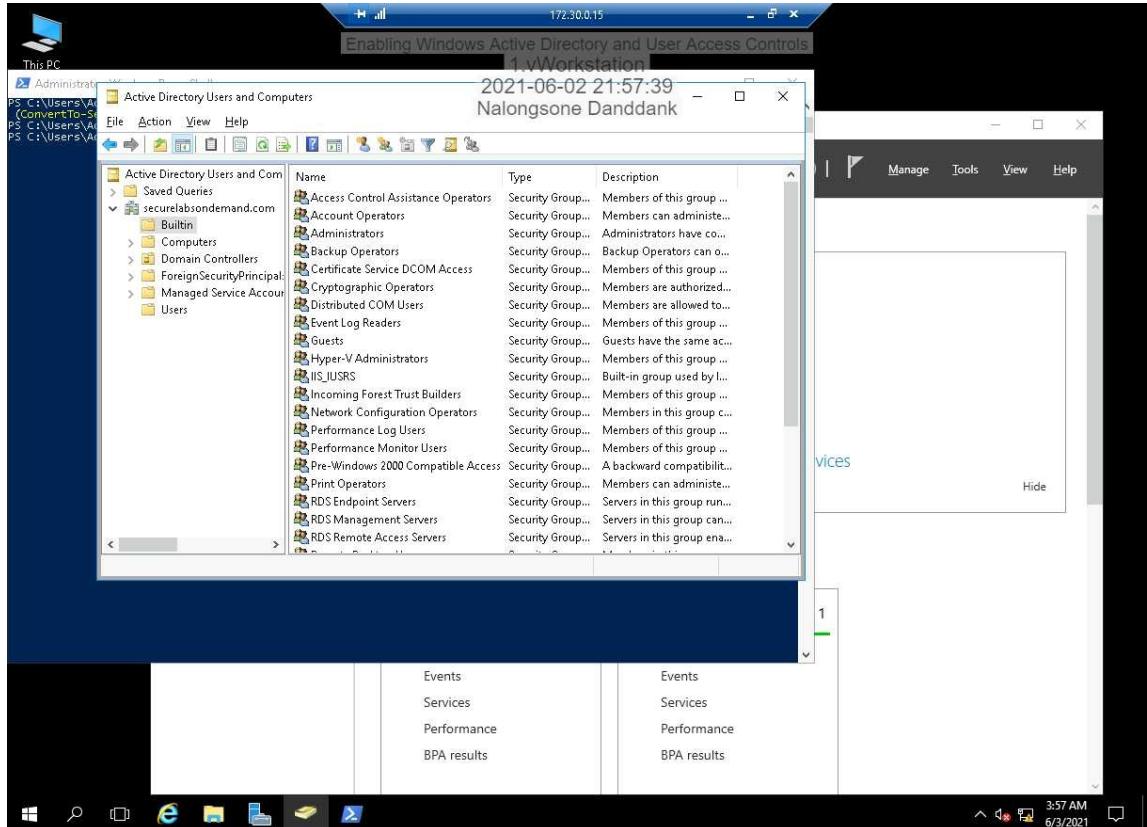
**Top Window:** An "Active Directory Users and Computers" snap-in window titled "Active Directory Domain Services". It shows a list of security groups under the "Users" container. A modal dialog box is displayed, stating "The Add to Group operation was successfully completed." with an "OK" button.

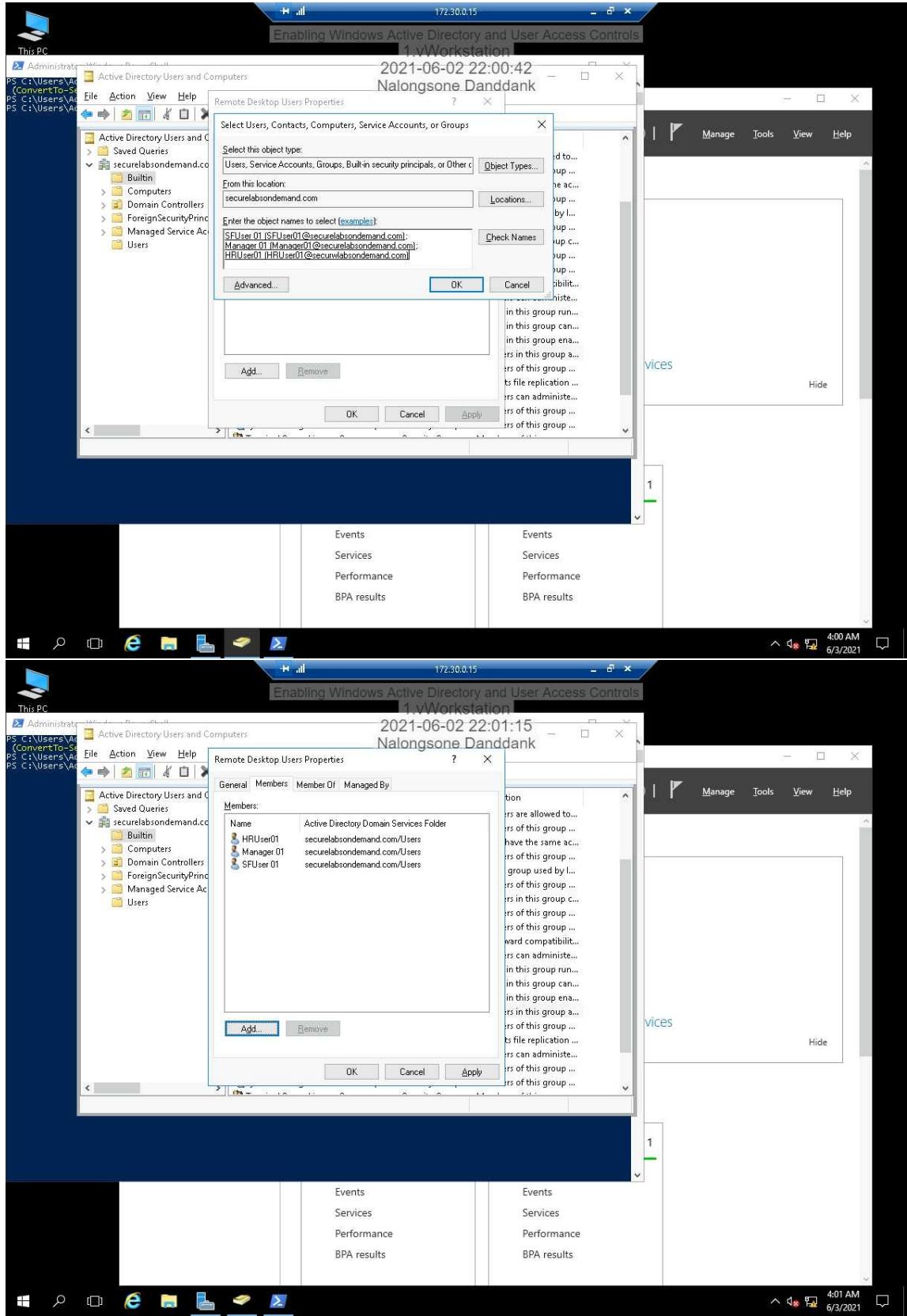
**Bottom Window:** An "Administrator: Windows PowerShell" window titled "Enabling Windows Active Directory and User Access Controls". The command run is:

```
PS C:\Users\Administrator> New-ADGroup -Name HumanResources -UserPrincipalName HumanResources@securlabsondemand.com -Accountpassword (ConvertTo-SecureString -AsPlainText "P@ssw0rd!" -Force) -GivenName HRUser -Surname O1 -Enabled $true
```

**Taskbar:** Shows the Start button, Task View, File Explorer, Edge browser, File Explorer, File Explorer, and Task View icons.







This PC

Enabling Windows Active Directory and User Access Controls  
1.vWorkstation 2021-06-02 22:03:48

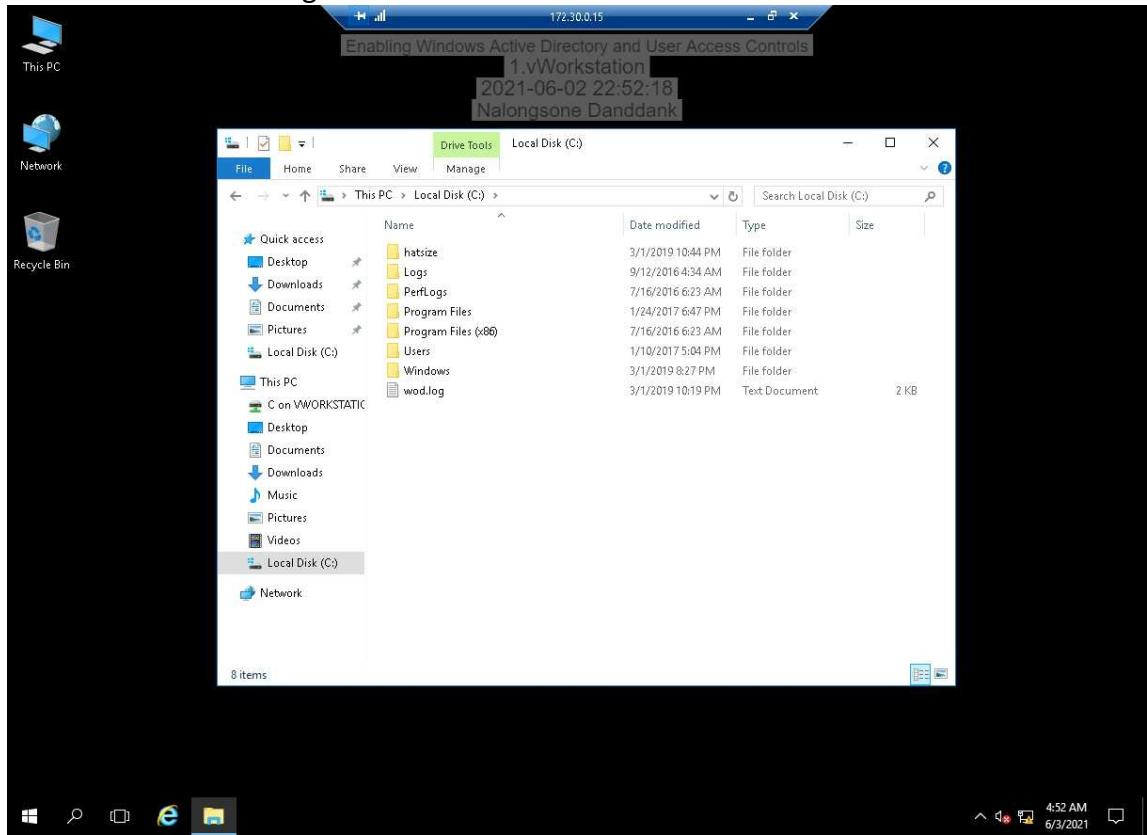
```
Administrator: Windows PowerShell
PS C:\Users\Administrator> New-ADUser -Name HRUser01 -UserPrincipalName HRUser01@domain.com -AccountPassword (ConvertTo-SecureString -String "P@ssw0rd" -Force) -GivenName HRUser01 -Surname HRUser01
PS C:\Users\Administrator> Add-ADGroupMember -Identity HumanResources -Members HRUser01
PS C:\Users\Administrator> gpupdate /force
Updating policy...
Computer Policy update has completed successfully.
User Policy update has completed successfully.

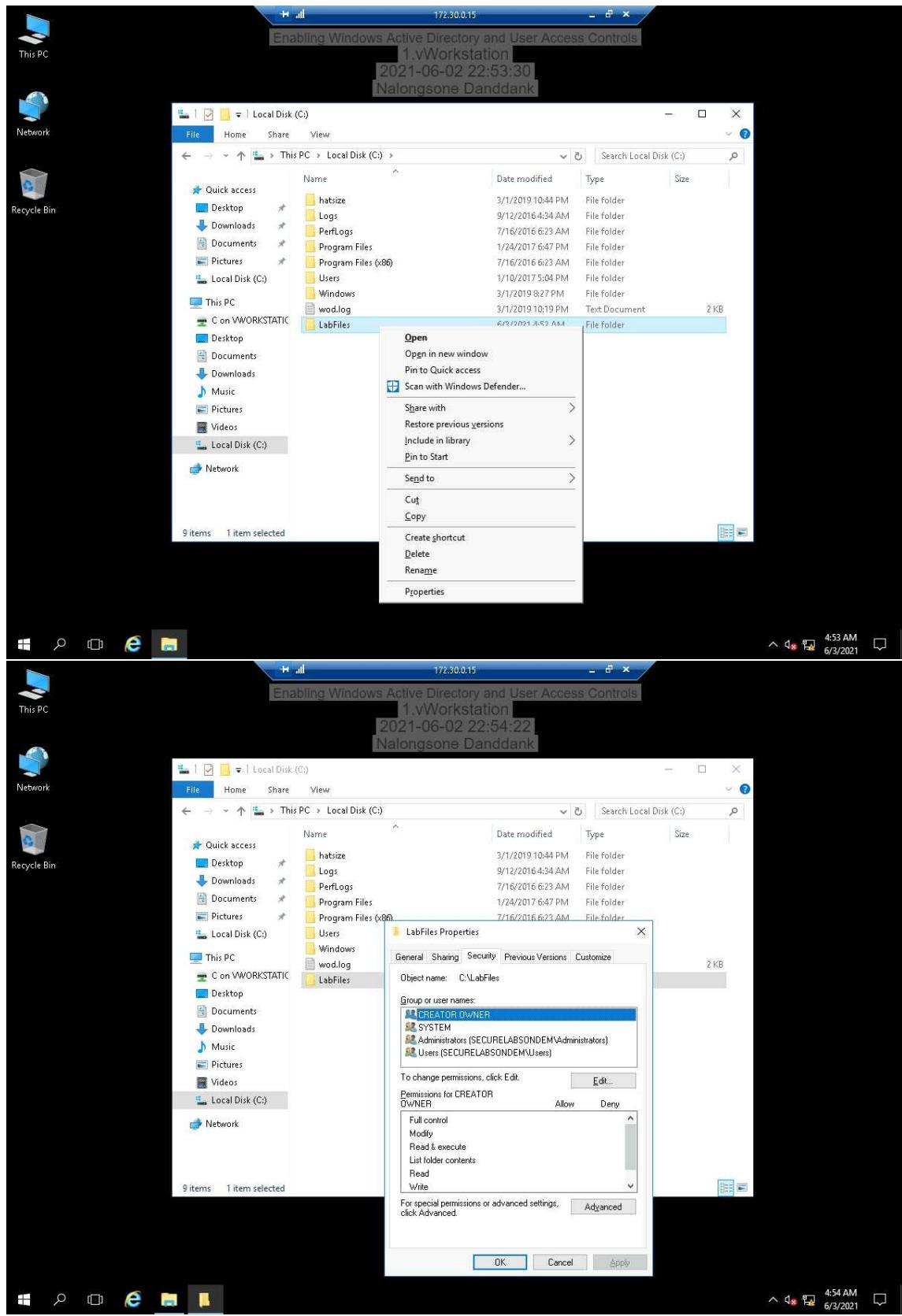
PS C:\Users\Administrator>
```

Windows Taskbar icons: Start, Search, Task View, Edge, File Explorer, Taskbar settings.

System tray: 4:03 AM, 6/3/2021

## Part 2: Resource Management





172.30.0.15 1.vWorkstation 2021-06-02 22:55:48 Nalongsone Danddank

This PC Network Recycle Bin

Local Disk (C): Advanced Security Settings for LabFiles

Name: C:\LabFiles  
Owner: Administrators (SECURELABSONDEM\Administrators) Change

Permissions Auditing Effective Access

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Type	Principal	Access	Inherited from	Applies to
Allow	SYSTEM	Full control	C:\	This folder, subfolders and files
Allow	Administrators (SECURELABSONDEM\Administrators)	Full control	C:\	This folder, subfolders and files
Allow	Users (SECURELABSONDEM\...)	Read & execute	C:\	This folder, subfolders and files
Allow	Users (SECURELABSONDEM\...)	Special	C:\	This folder and subfolders
Allow	CREATOR OWNER	Full control	C:\	Subfolders and files only

Add Remove View  
Disable inheritance  
 Replace all child object permission entries with inheritable permission entries from this object

OK Cancel Apply

9 items 1 item selected

Read Write  
For special permissions or advanced settings, click Advanced.

OK Cancel Apply

Block Inheritance

What would you like to do with the current inherited permissions?

You are about to block inheritance to this object, which means that permissions inherited from a parent object will no longer be applied to this object.

Convert inherited permissions into explicit permissions on this object.  
Remove all inherited permissions from this object.

Cancel

OK Cancel Apply

9 items 1 item selected

Read Write  
For special permissions or advanced settings, click Advanced.

OK Cancel Apply

4:55 AM 6/3/2021

172.30.0.15 1.vWorkstation 2021-06-02 22:57:21 Nalongsone Danddank

This PC Network Recycle Bin

Local Disk (C): Advanced Security Settings for LabFiles

Name: C:\LabFiles  
Owner: Administrators (SECURELABSONDEM\Administrators)

Permissions

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Type	Prin	Access	Inherited from	Applies to
Allow	SY	Full control	C:\	This folder, subfolders and files
Allow	Ad	Full control	C:\	This folder, subfolders and files
Allow	Us	Read & execute	C:\	This folder, subfolders and files
Allow	Us	Special	C:\	This folder and subfolders
Allow	CR	Full control	C:\	Subfolders and files only

Add Remove View  
Disable inheritance  
 Replace all child object permission entries with inheritable permission entries from this object

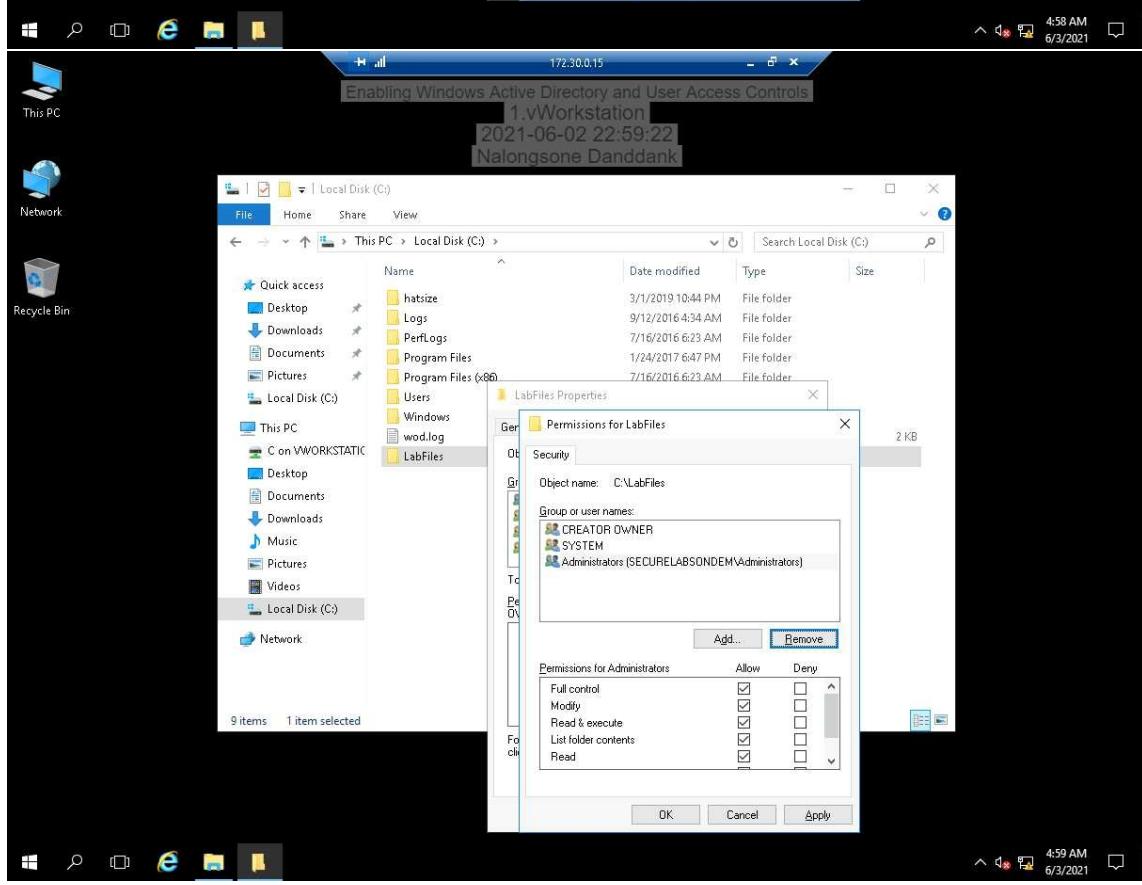
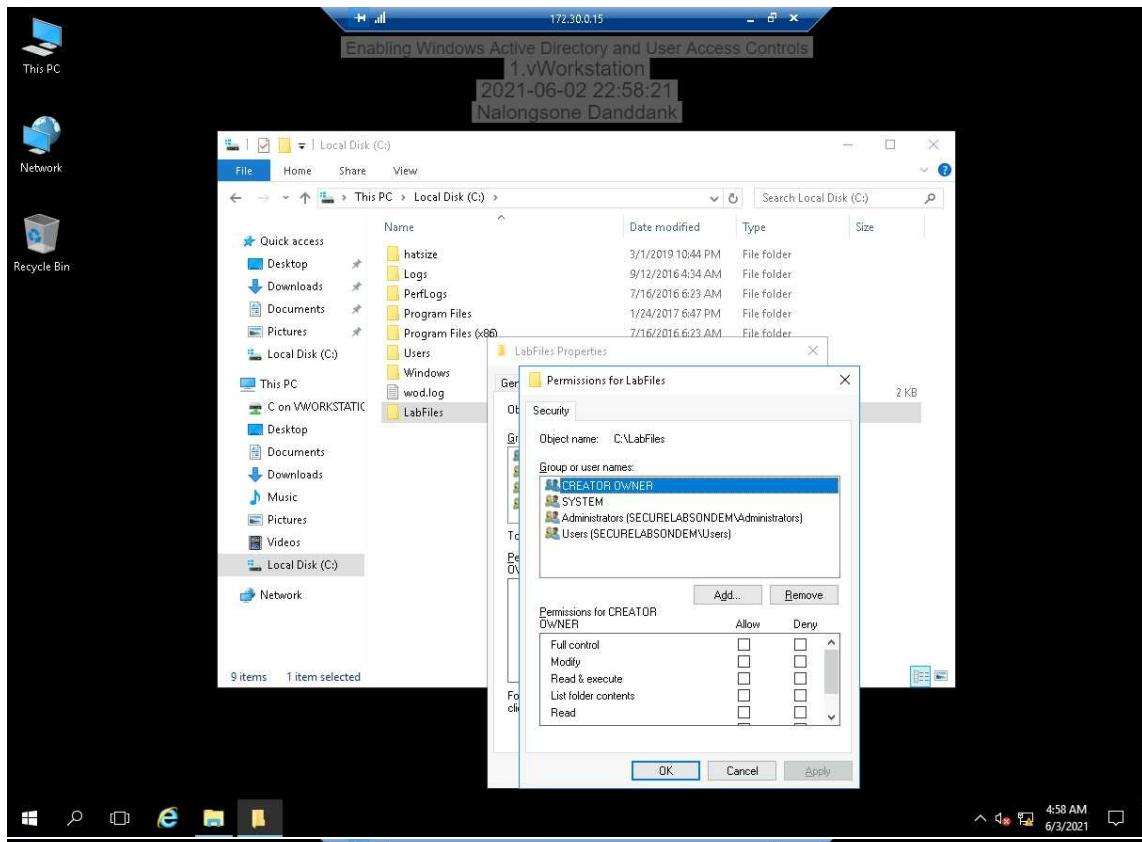
OK Cancel Apply

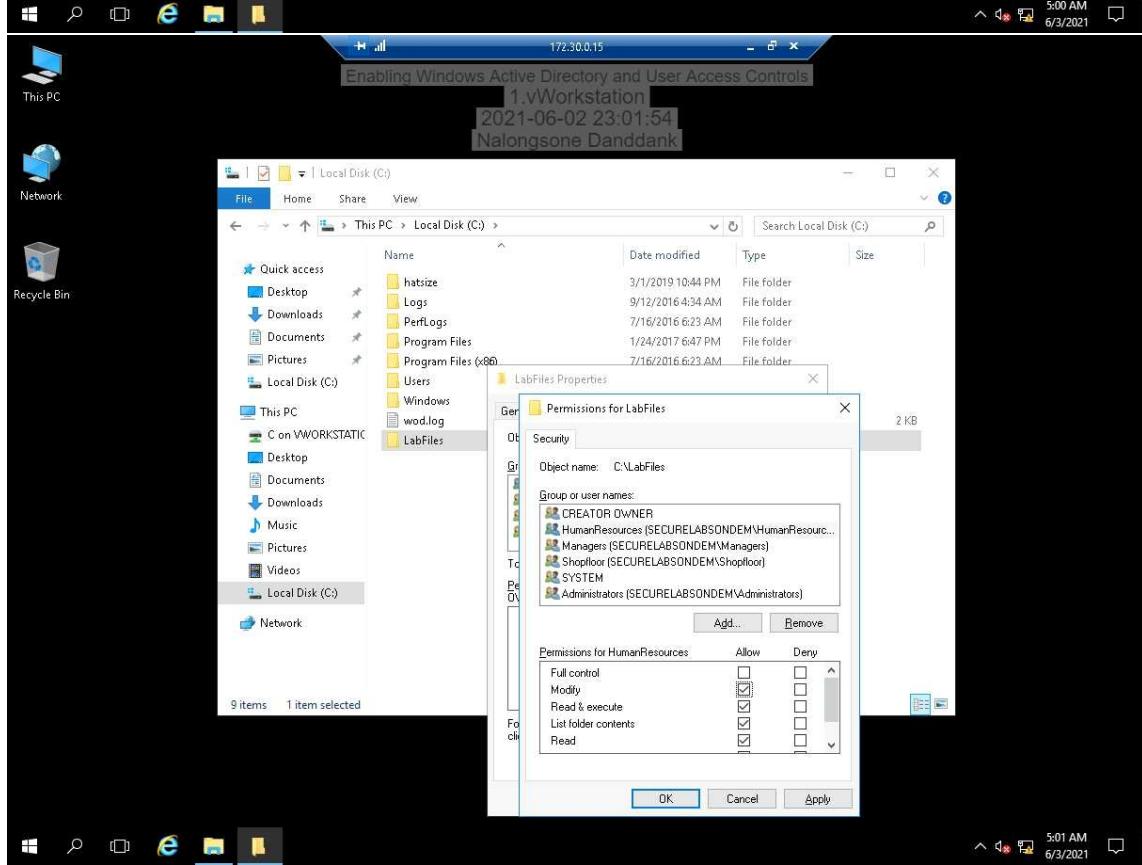
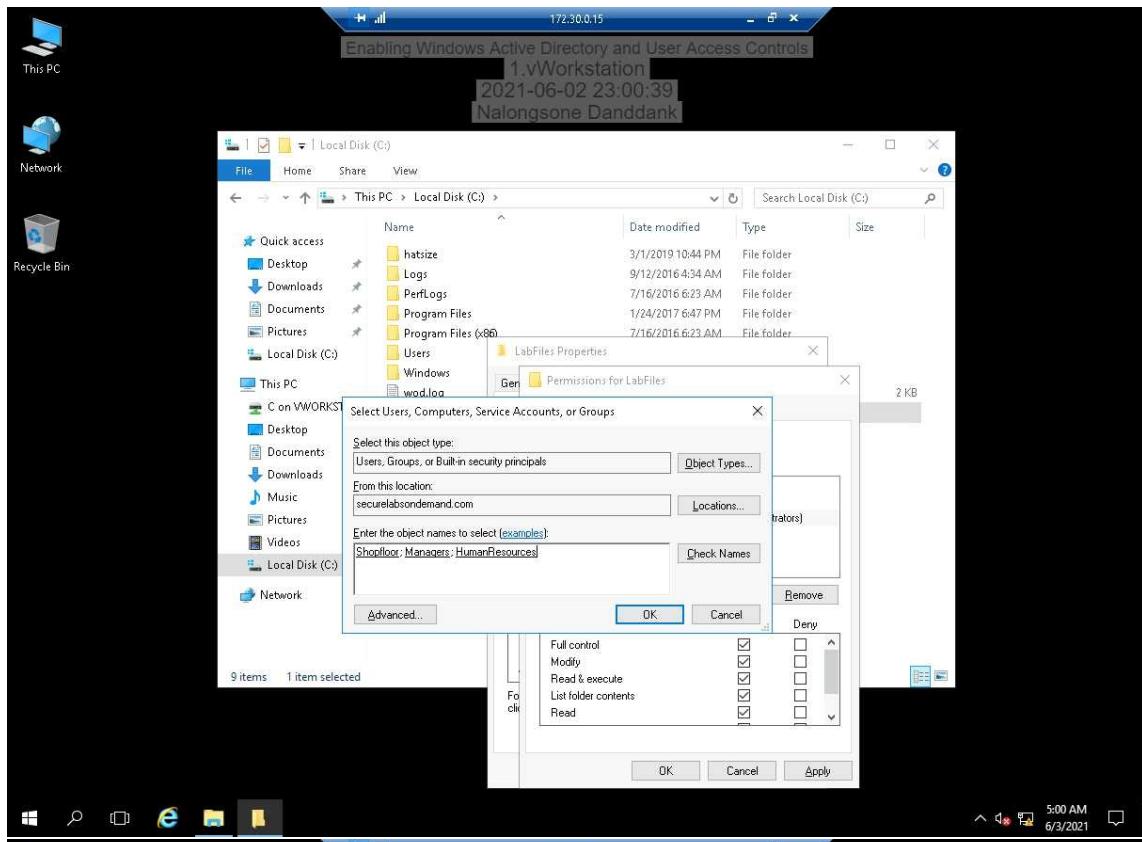
9 items 1 item selected

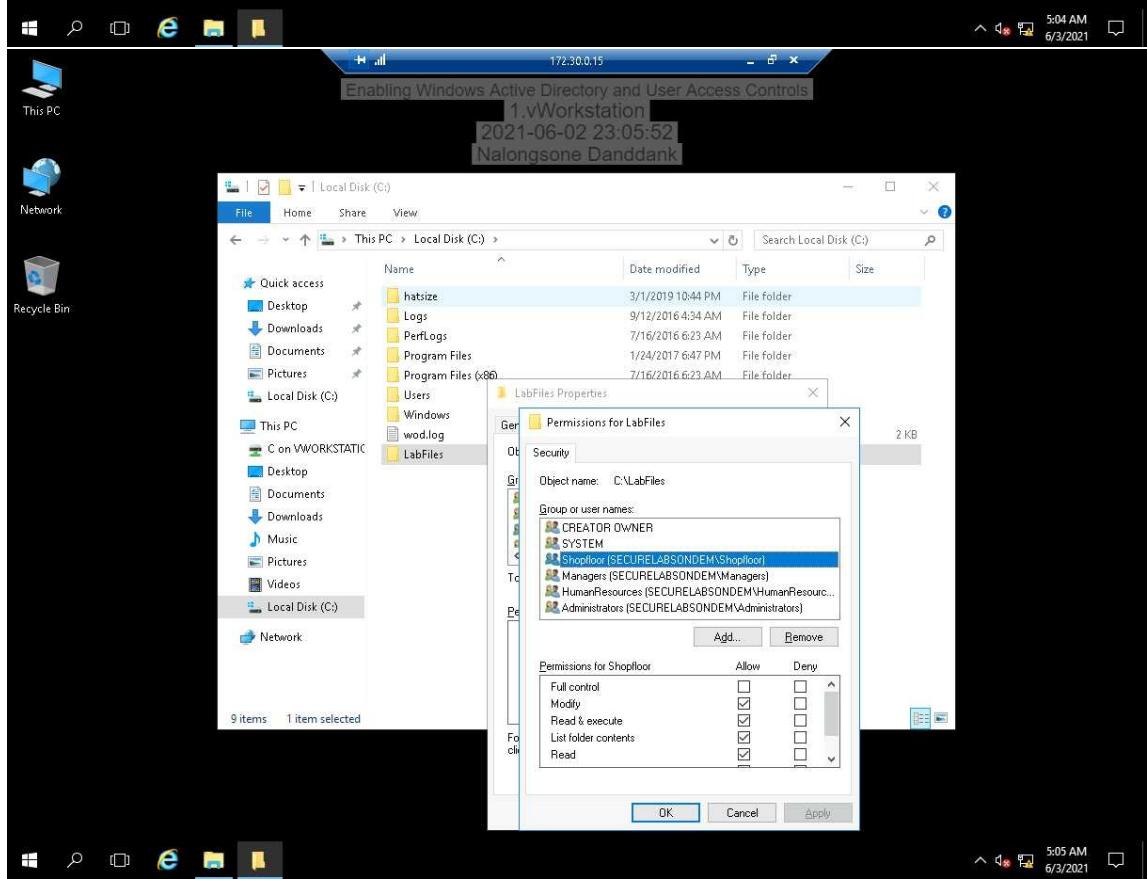
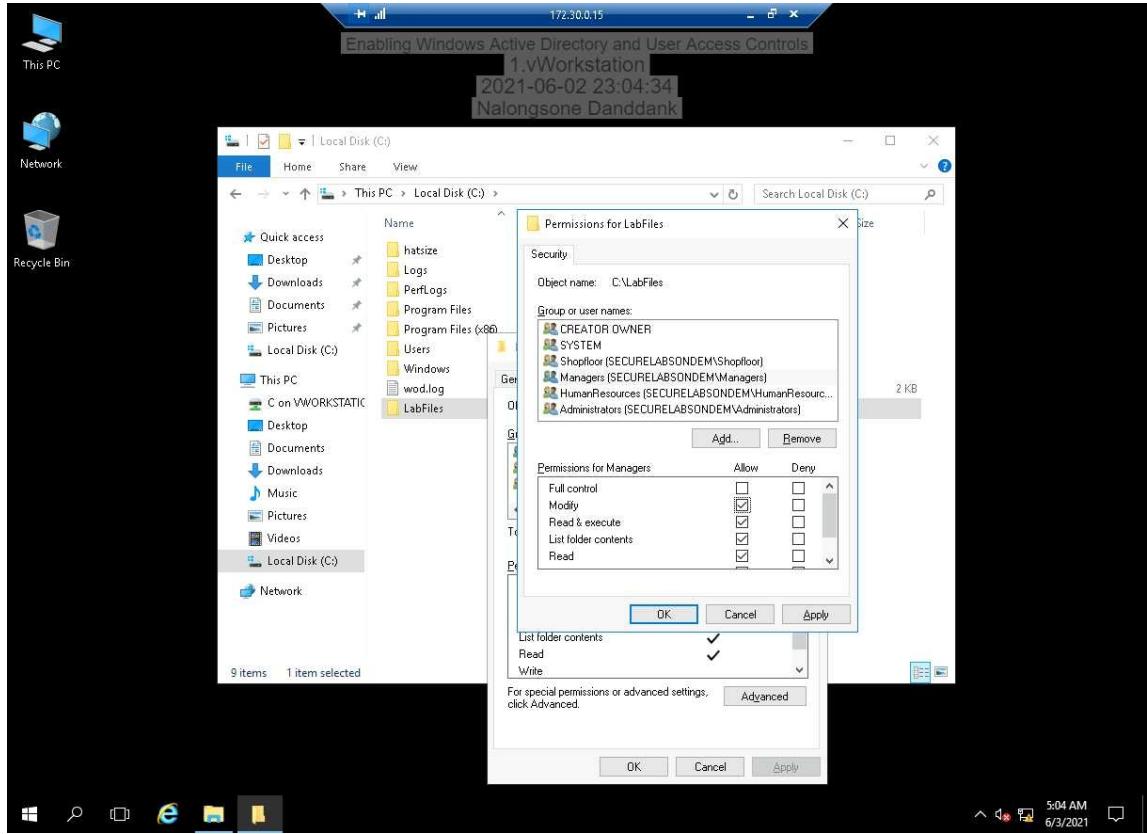
Read Write  
For special permissions or advanced settings, click Advanced.

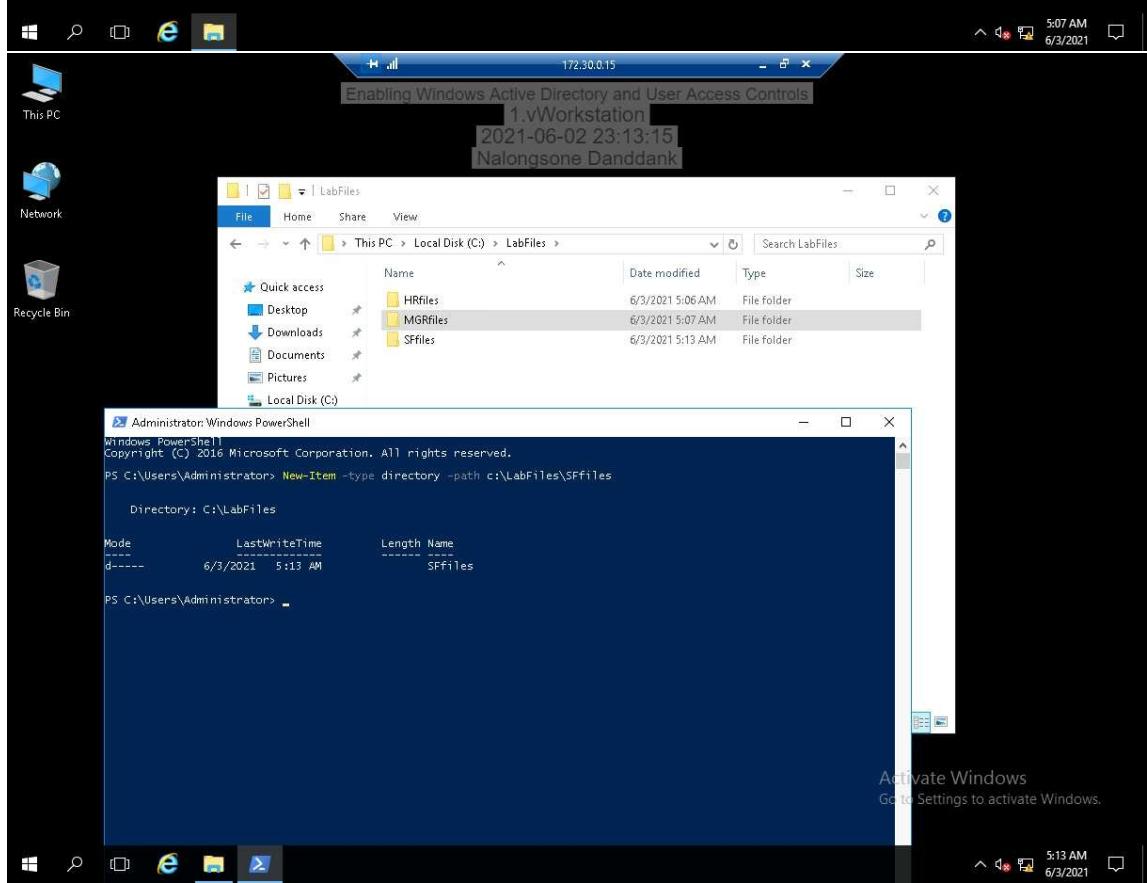
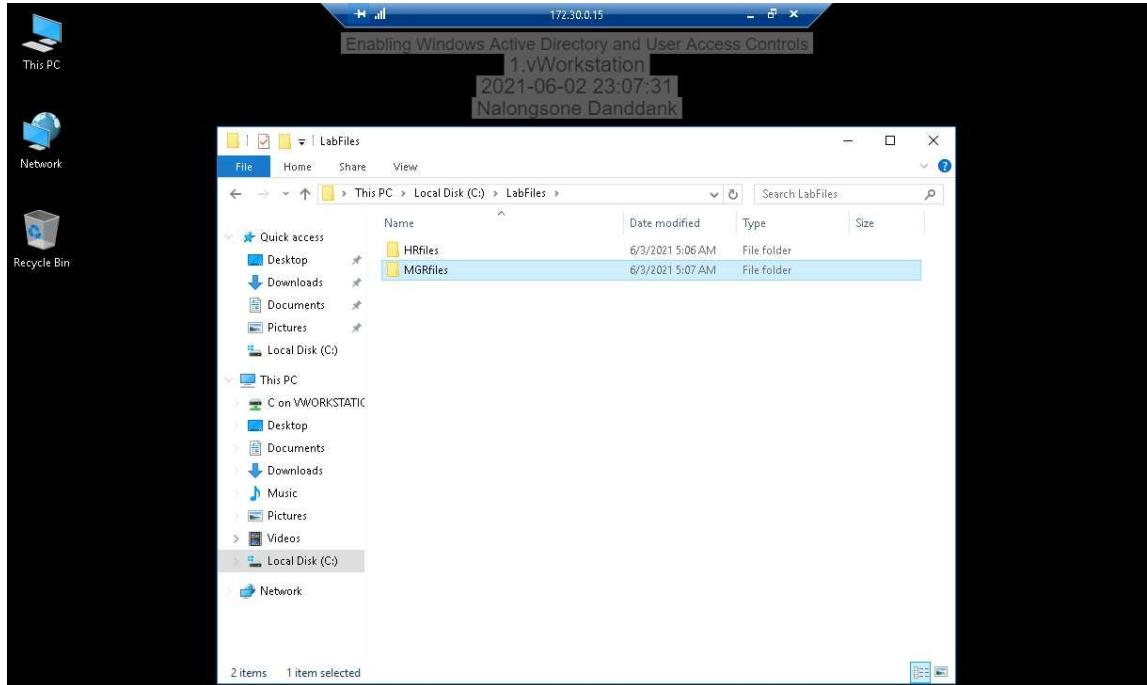
OK Cancel Apply

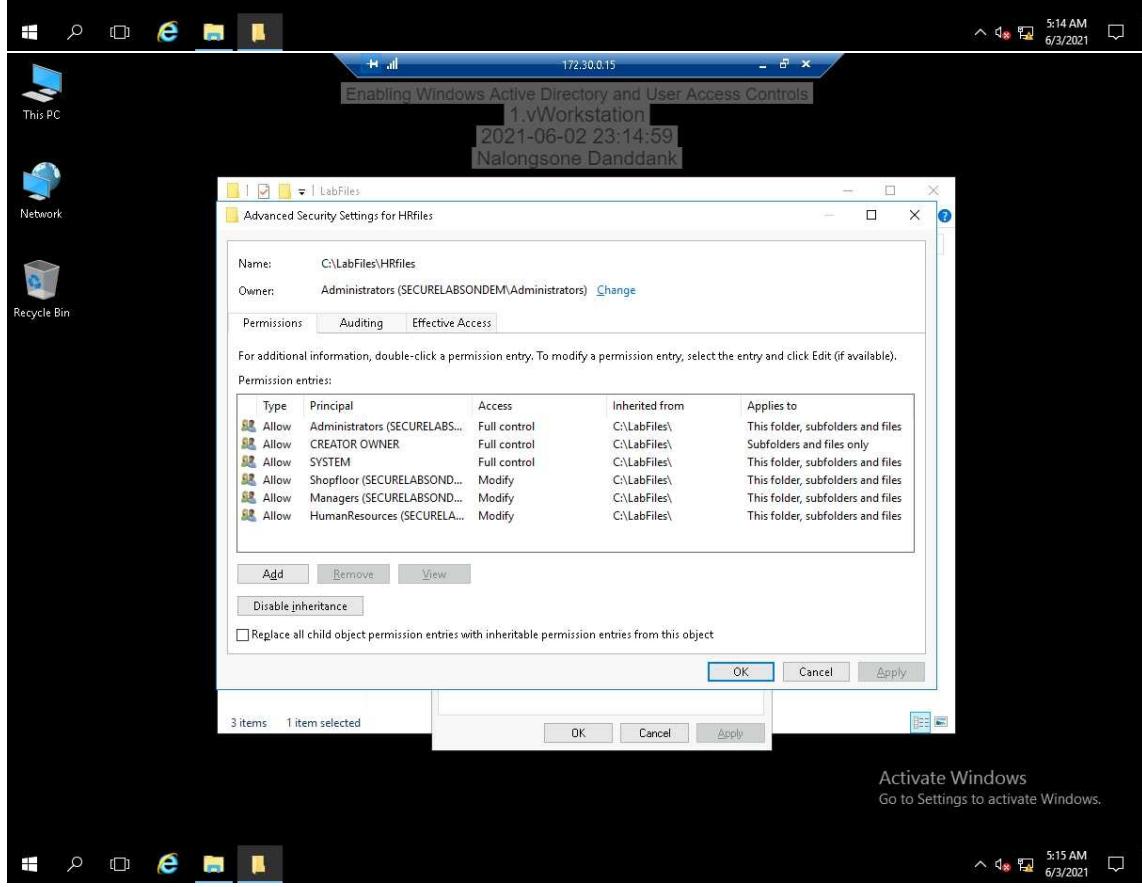
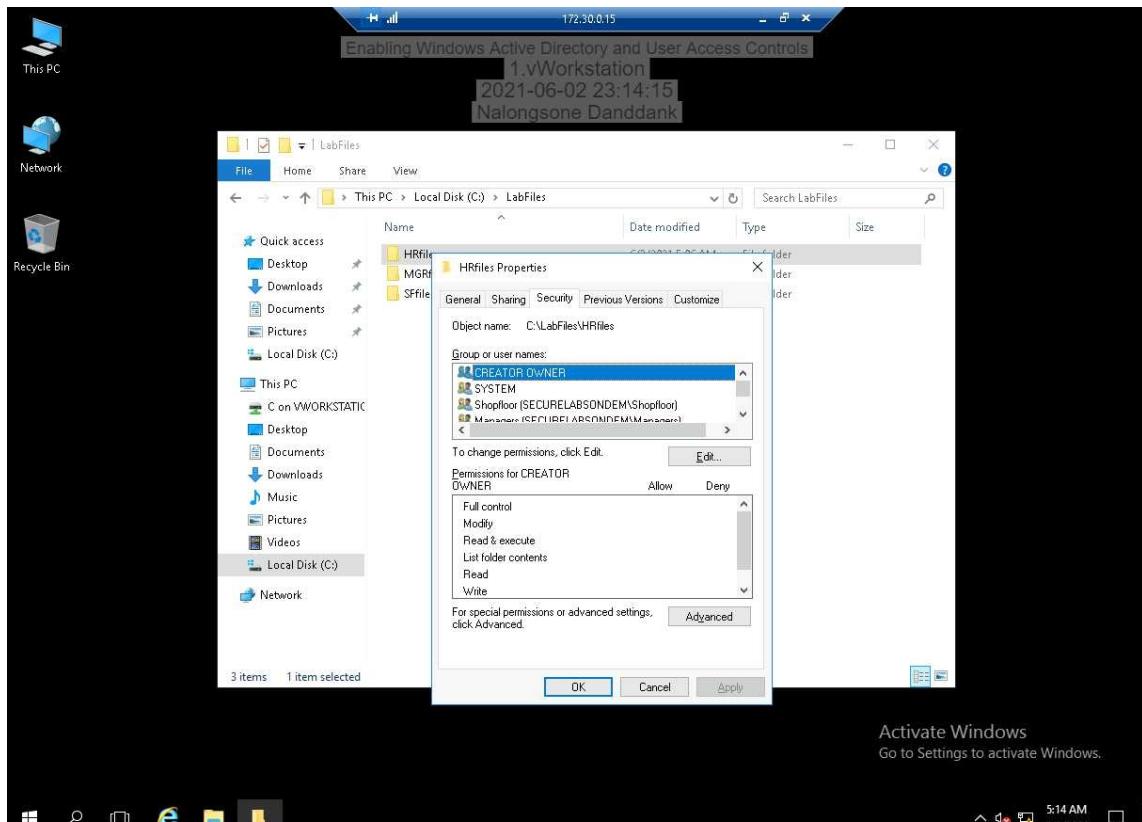
4:57 AM 6/3/2021

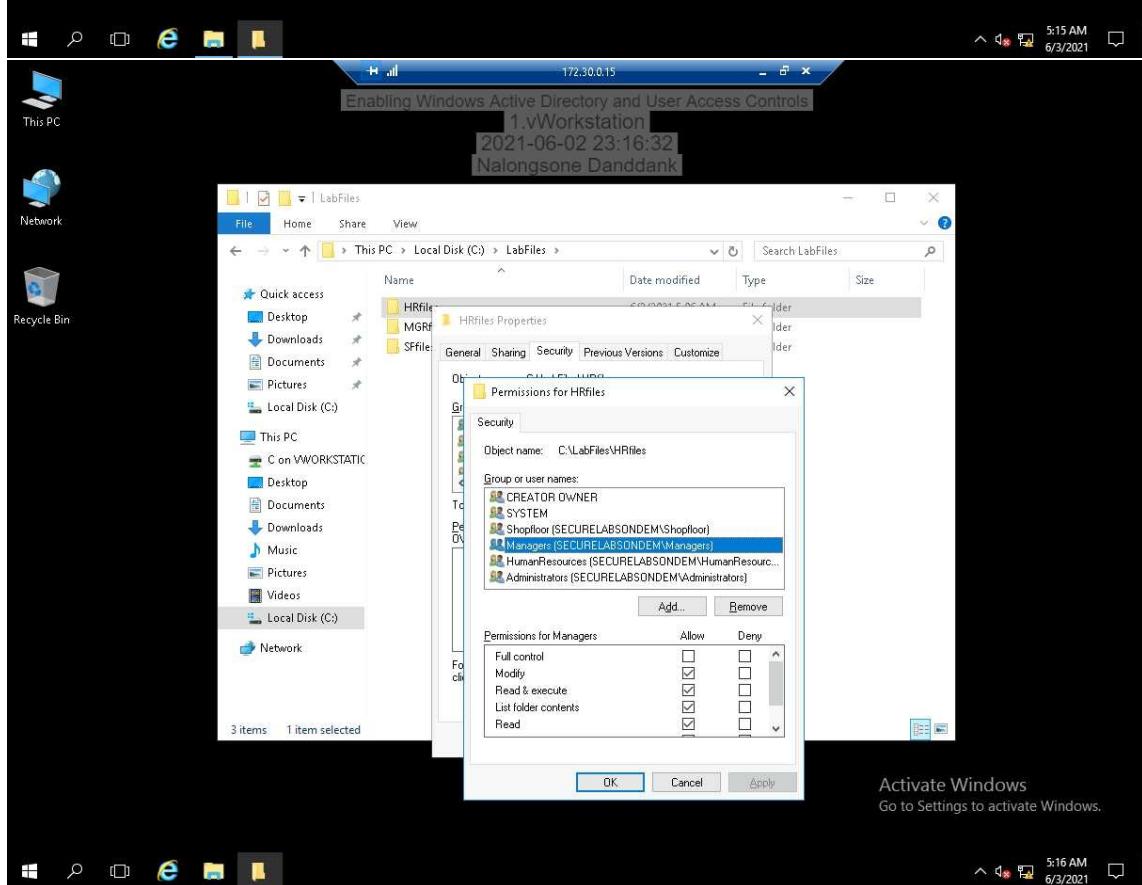
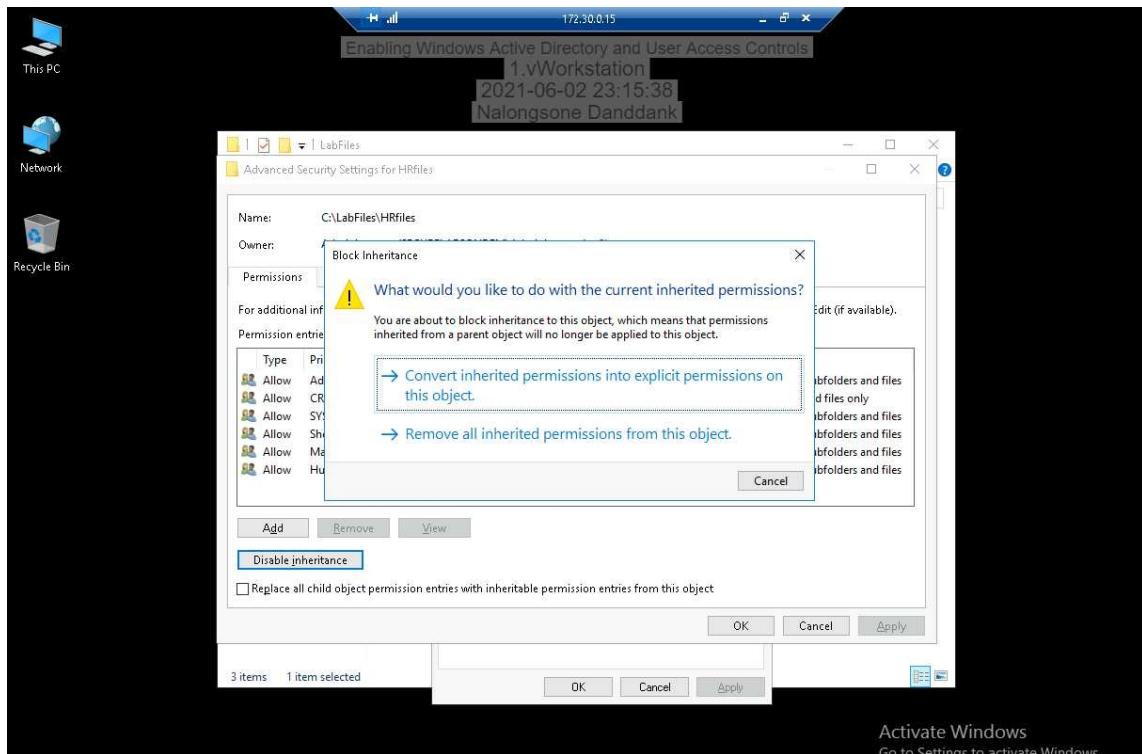


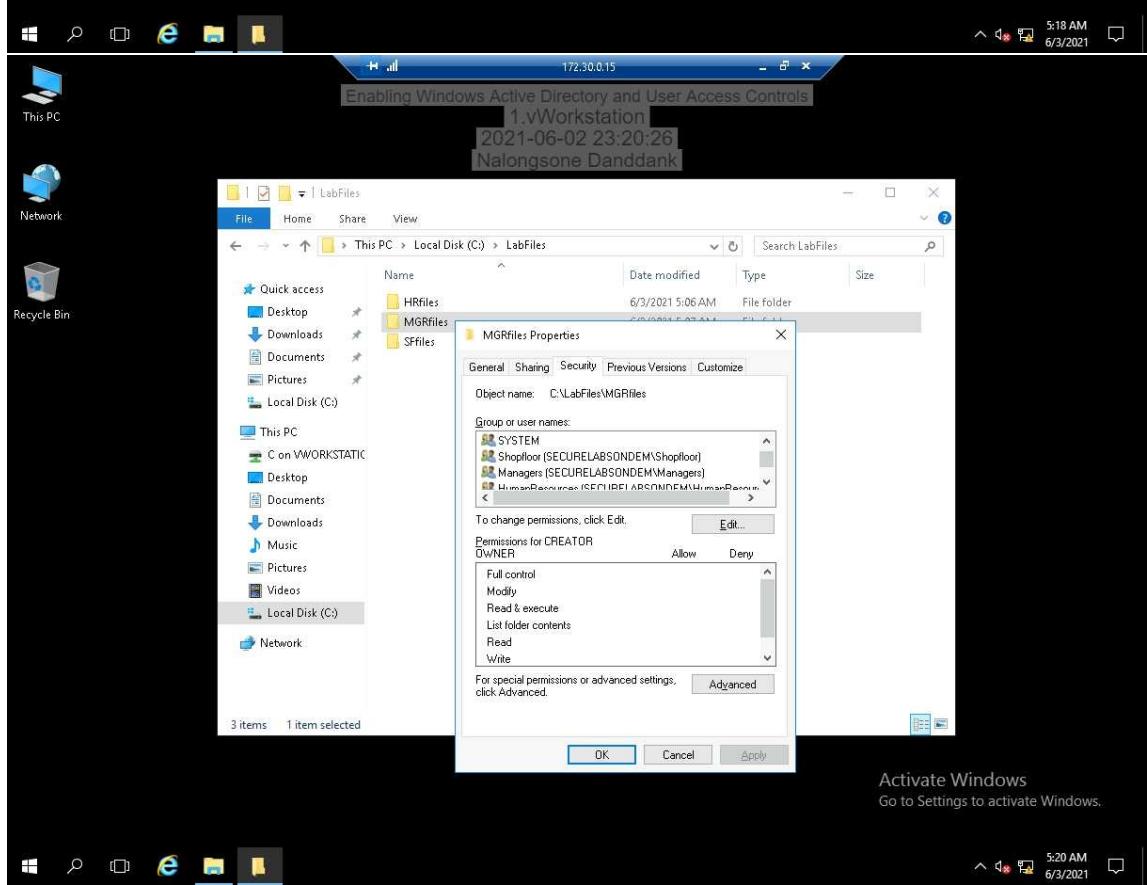
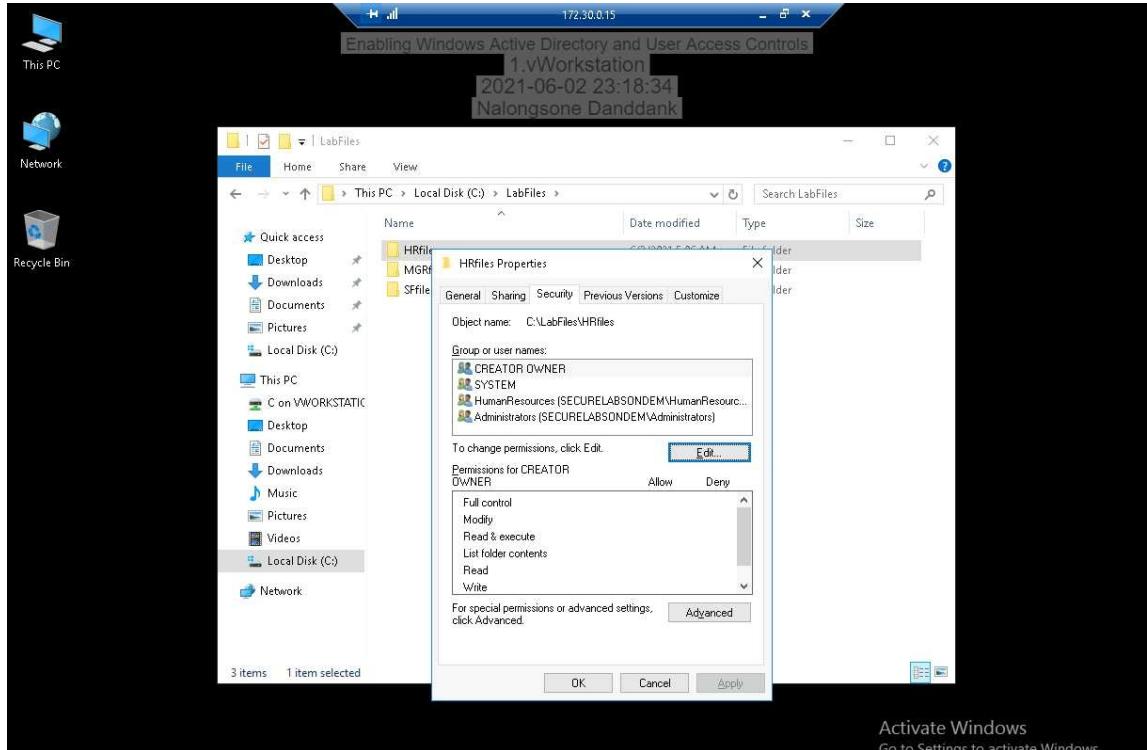


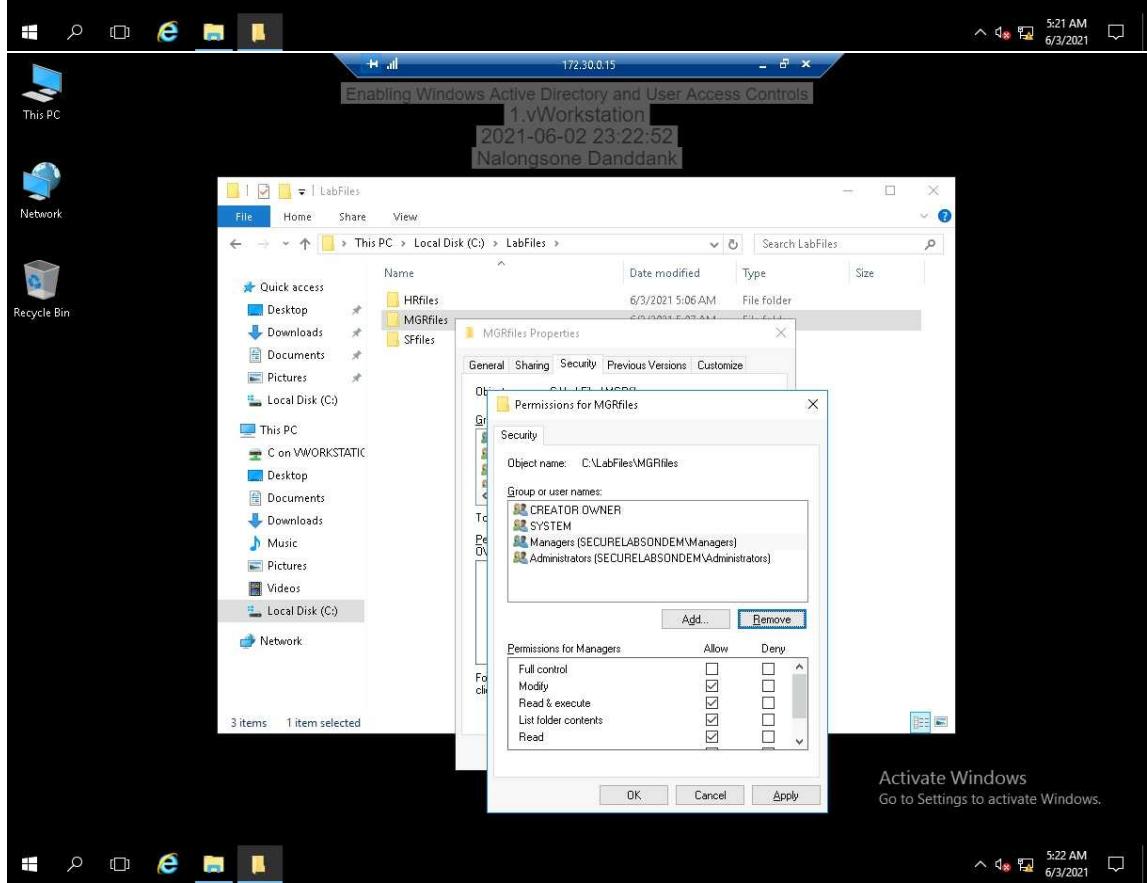
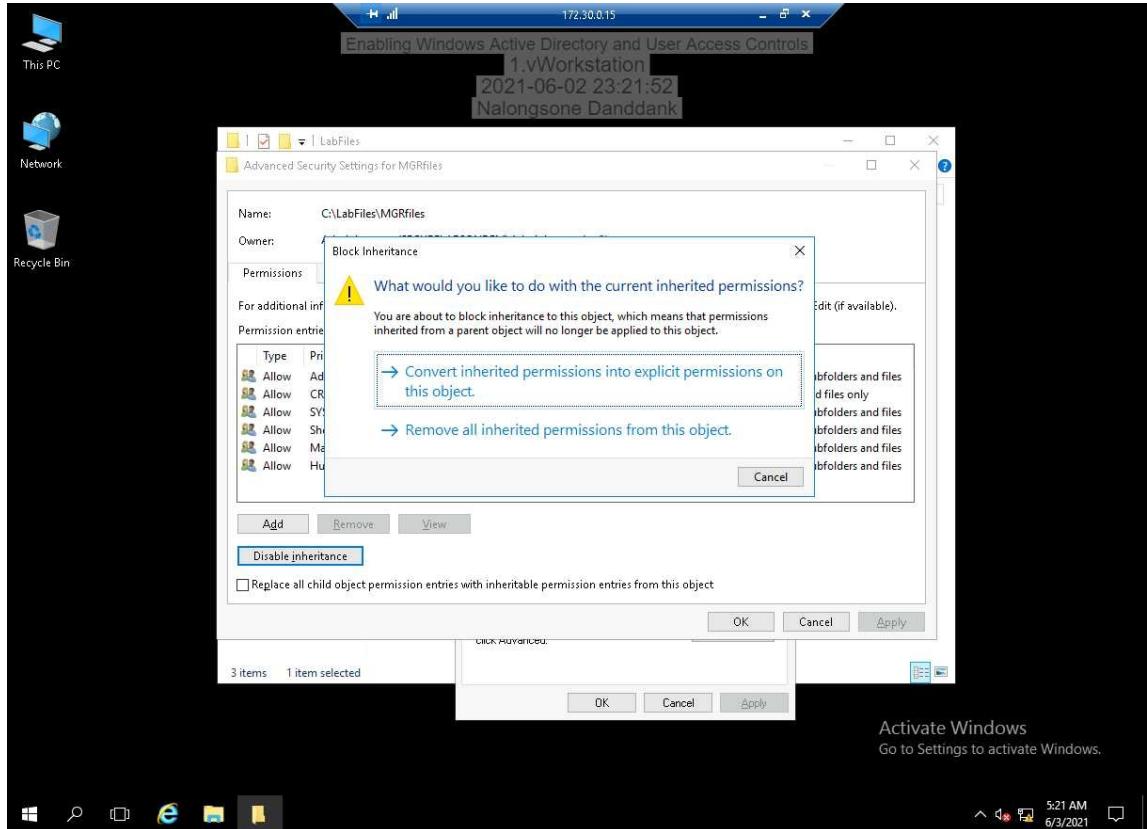










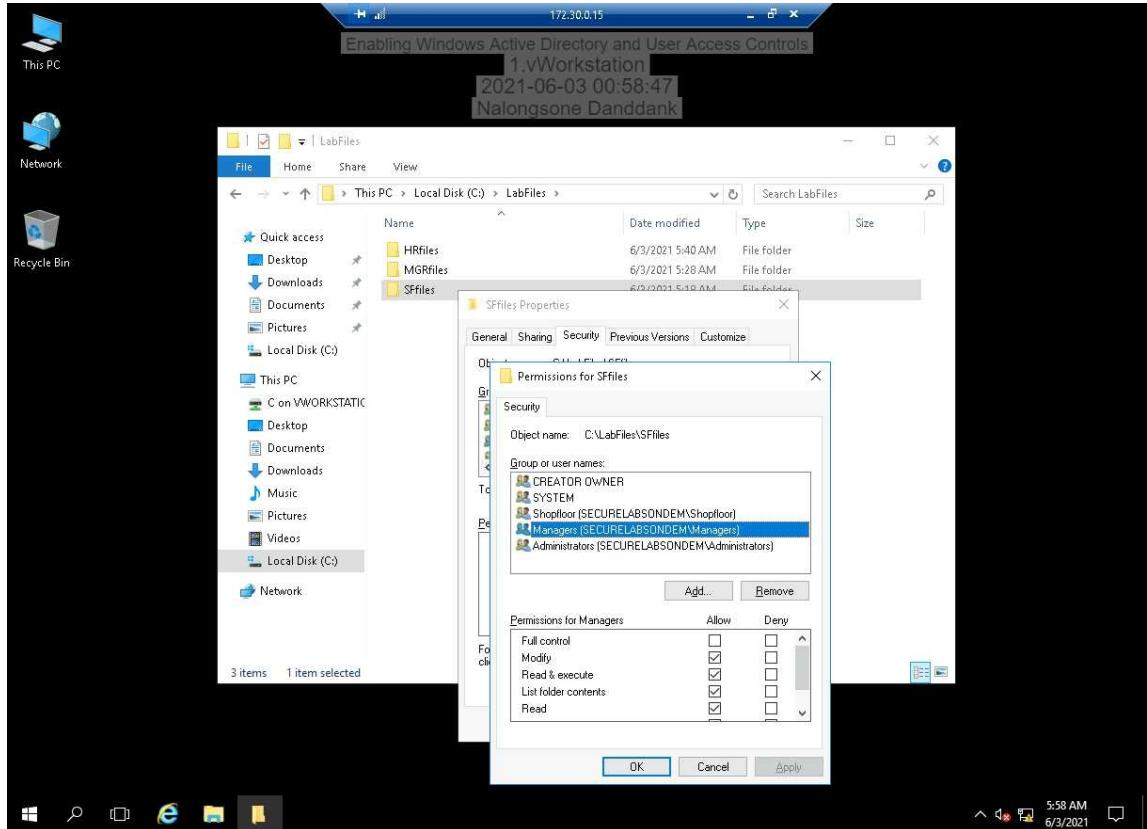


The screenshot shows a Windows desktop environment with a black theme. A File Explorer window is open, displaying the contents of the 'LabFiles' folder on the 'Local Disk (C:)'. The 'SFfiles' folder is selected. A context menu is open over the 'SFfiles' folder, with the 'Properties' option highlighted. The 'Properties' dialog box is displayed, showing the 'Security' tab. The 'Object name' is listed as 'C:\LabFiles\SFfiles'. Under 'Permissions for CREATOR OWNER', it shows 'Allow' for 'Full control', 'Modify', 'Read & execute', 'List folder contents', 'Read', and 'Write'. Below this, there is a link to 'Advanced' settings. At the bottom of the dialog are 'OK', 'Cancel', and 'Apply' buttons.

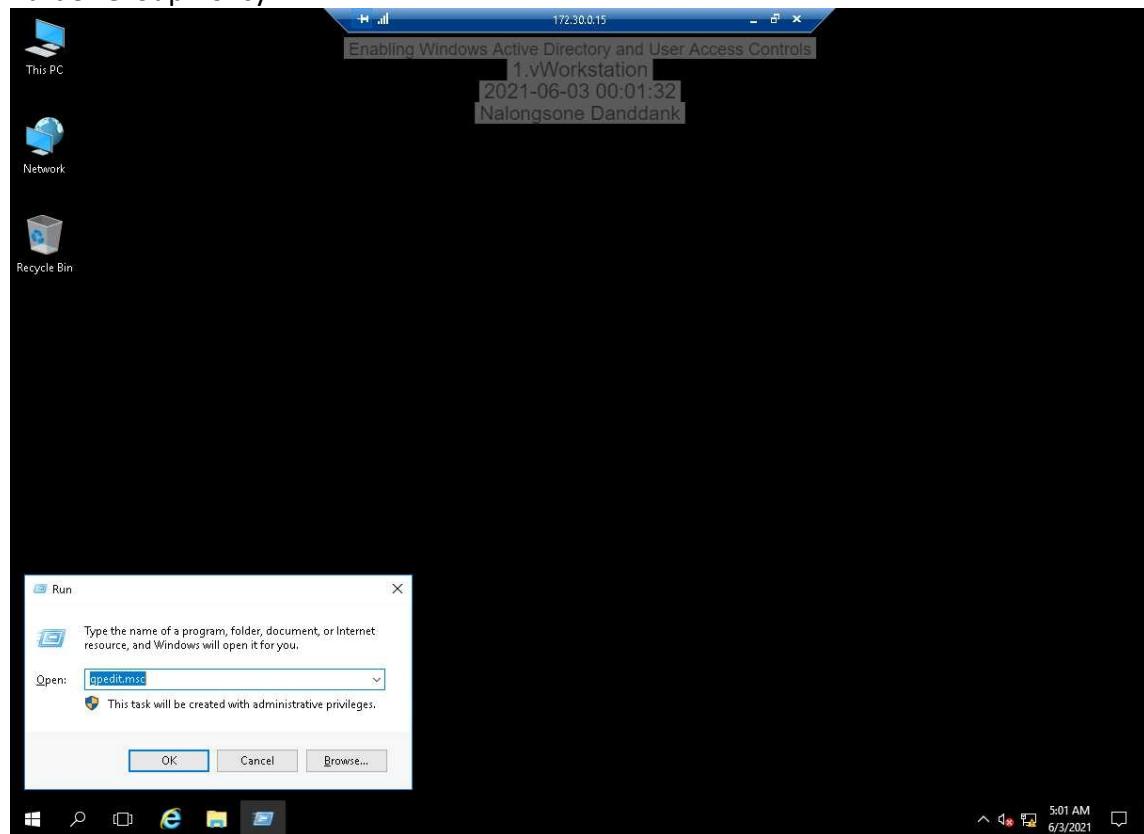
Activate Windows  
Go to Settings to activate Windows.

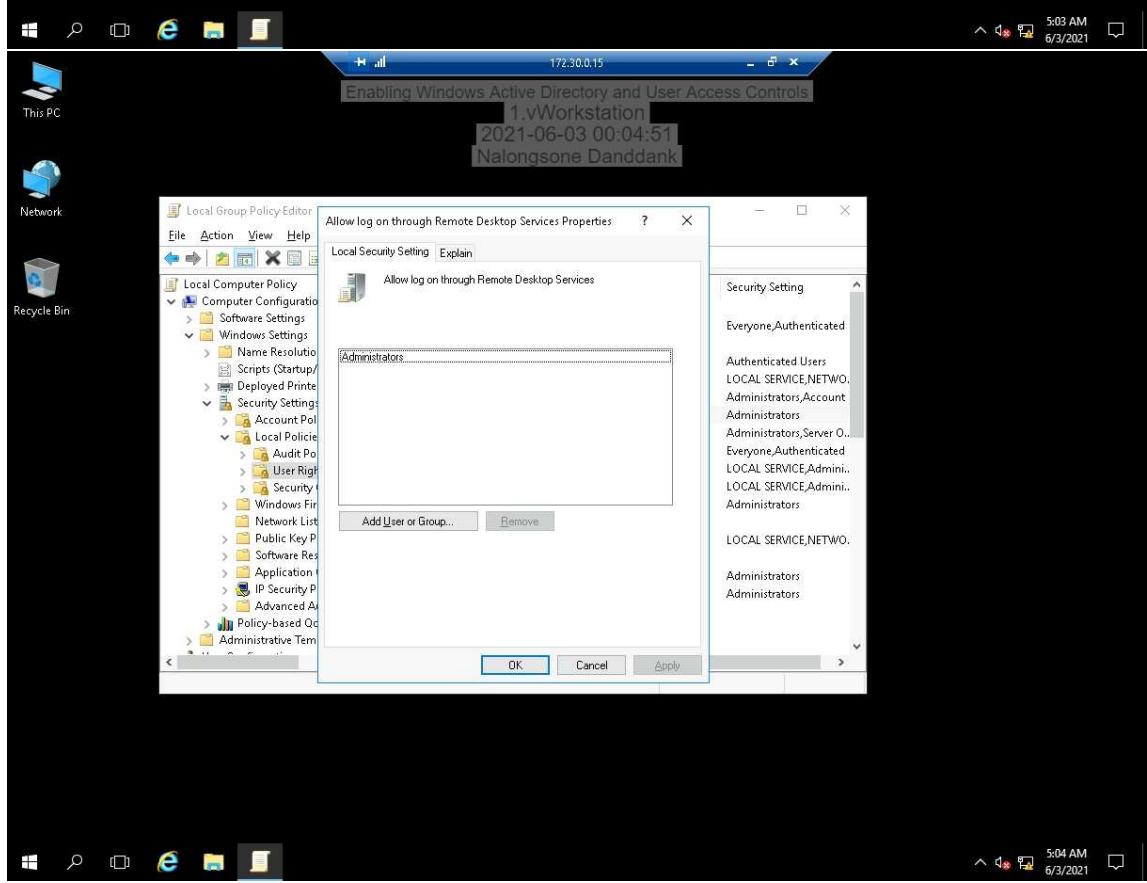
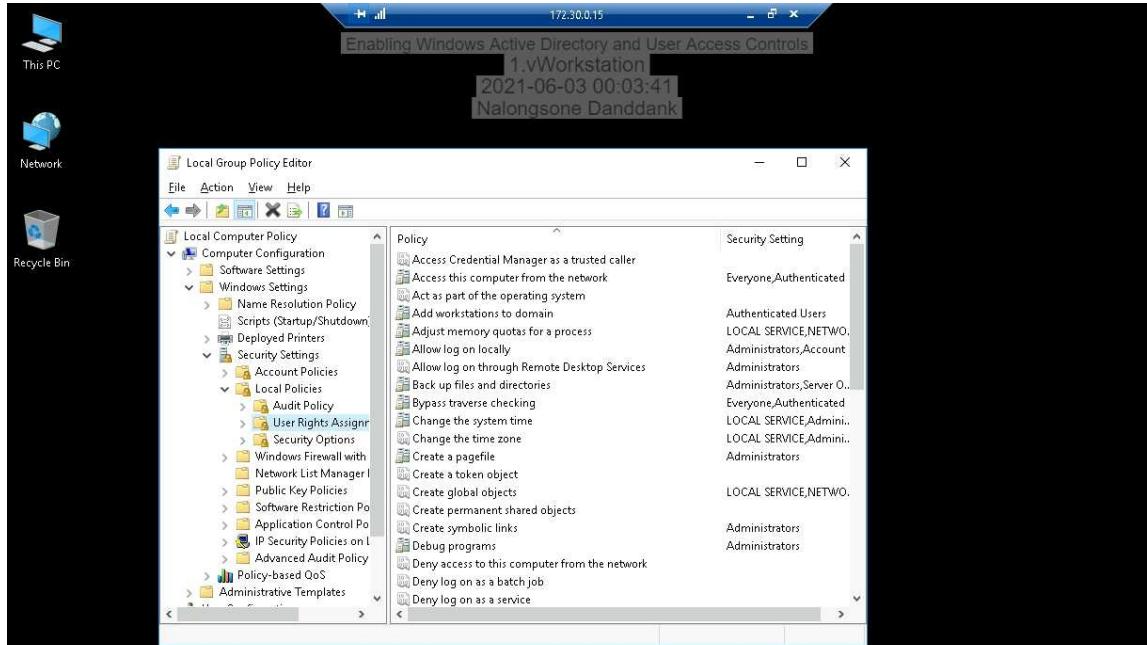
The screenshot shows the 'Advanced Security Settings' dialog for the 'SFfiles' folder. The 'Permissions' tab is selected. A warning message box titled 'Block Inheritance' is overlaid on the dialog. The message asks what to do with current inherited permissions, providing two options: 'Convert inherited permissions into explicit permissions on this object.' and 'Remove all inherited permissions from this object.' Both options have arrows pointing to them. The 'OK' button is visible at the bottom of the dialog.

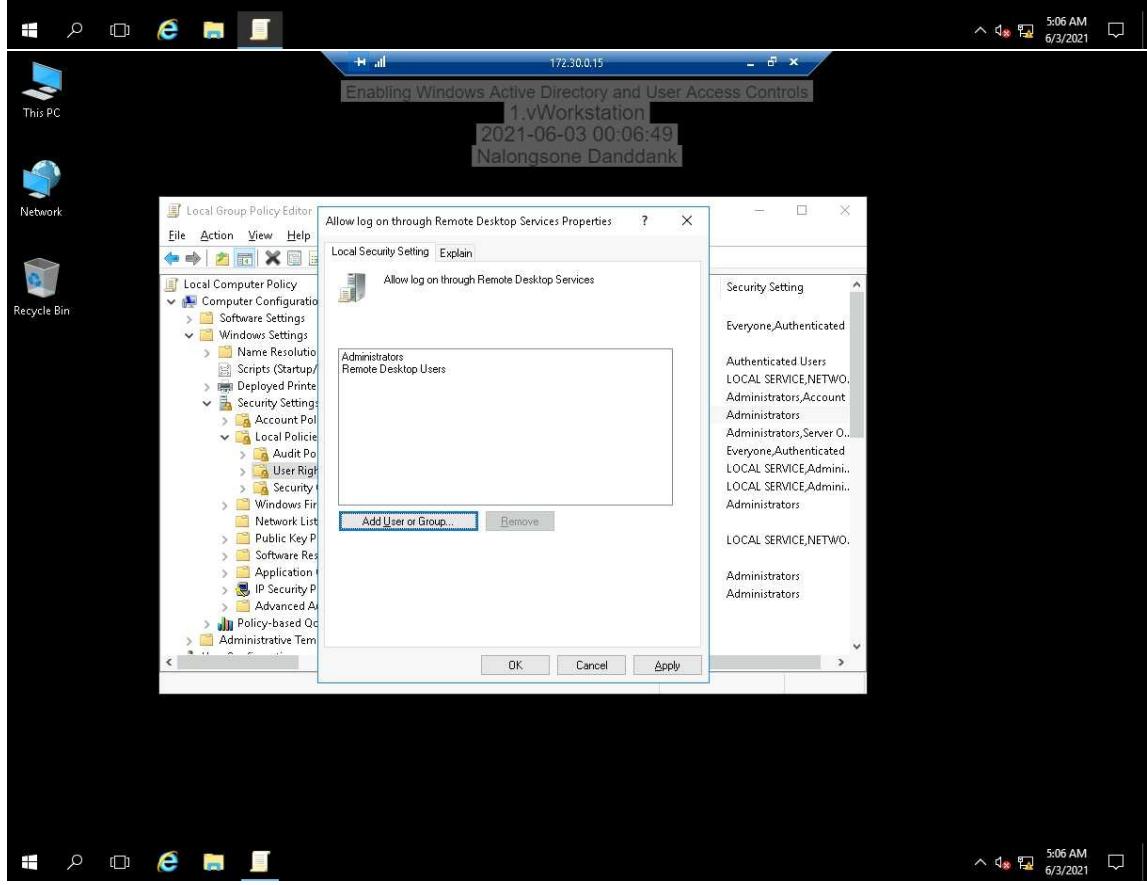
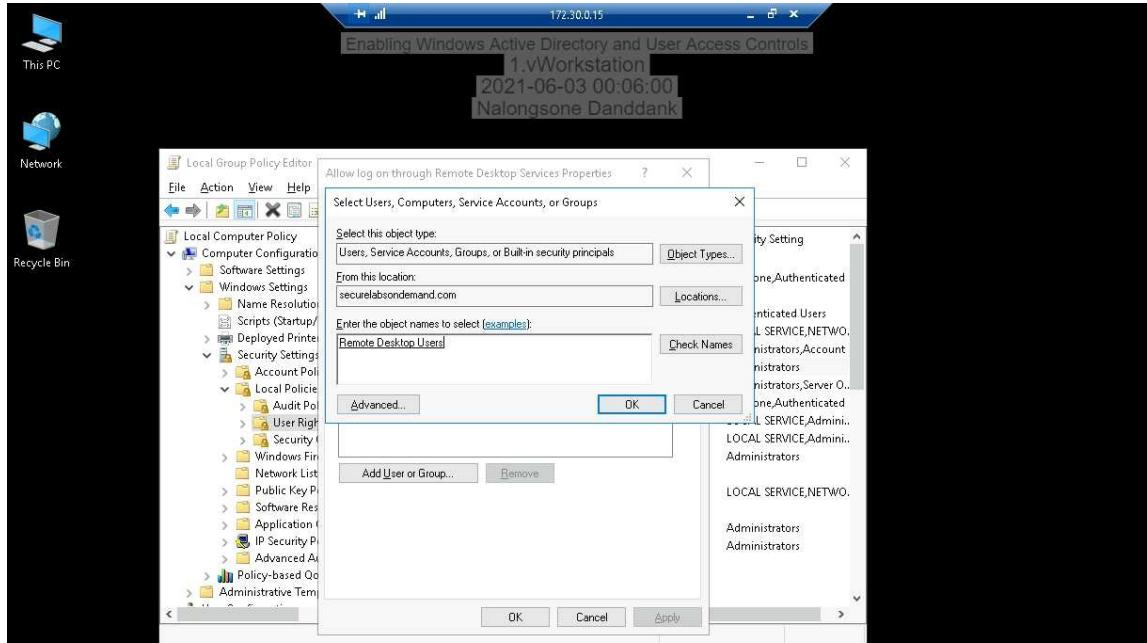
Activate Windows  
Go to Settings to activate Windows.



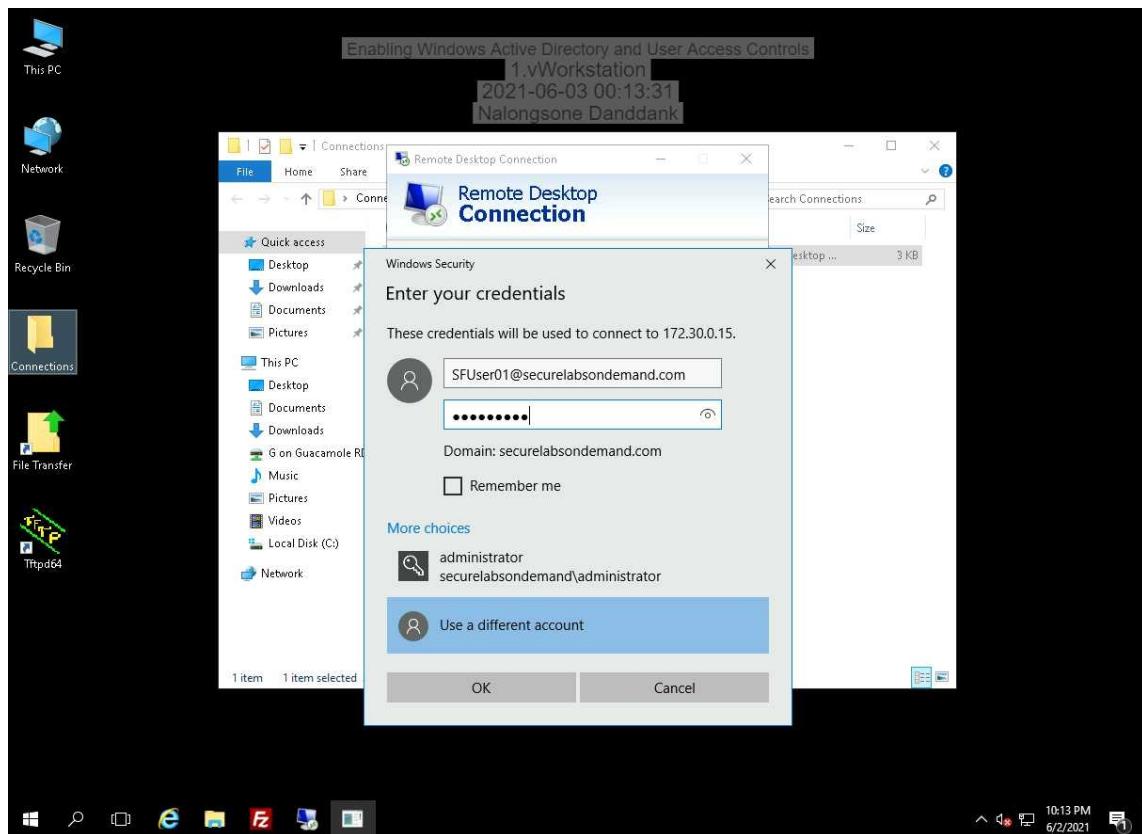
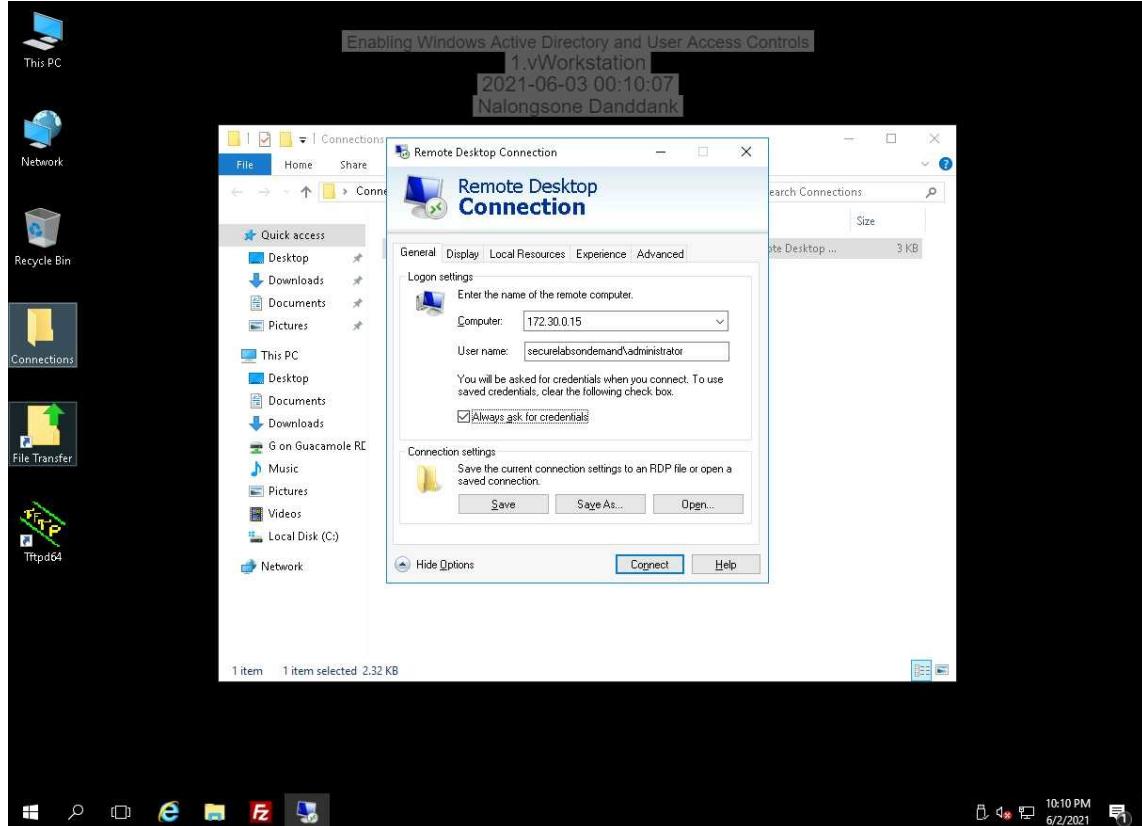
### Part 3: Group Policy

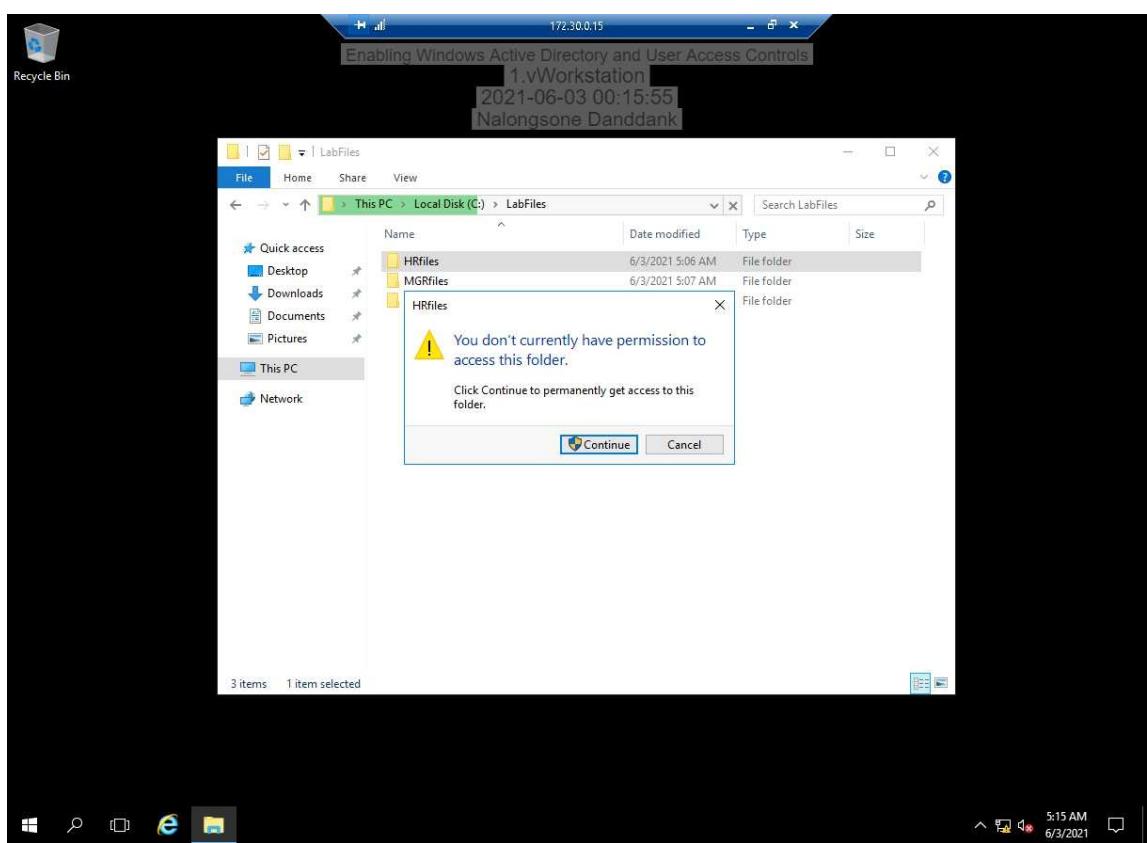
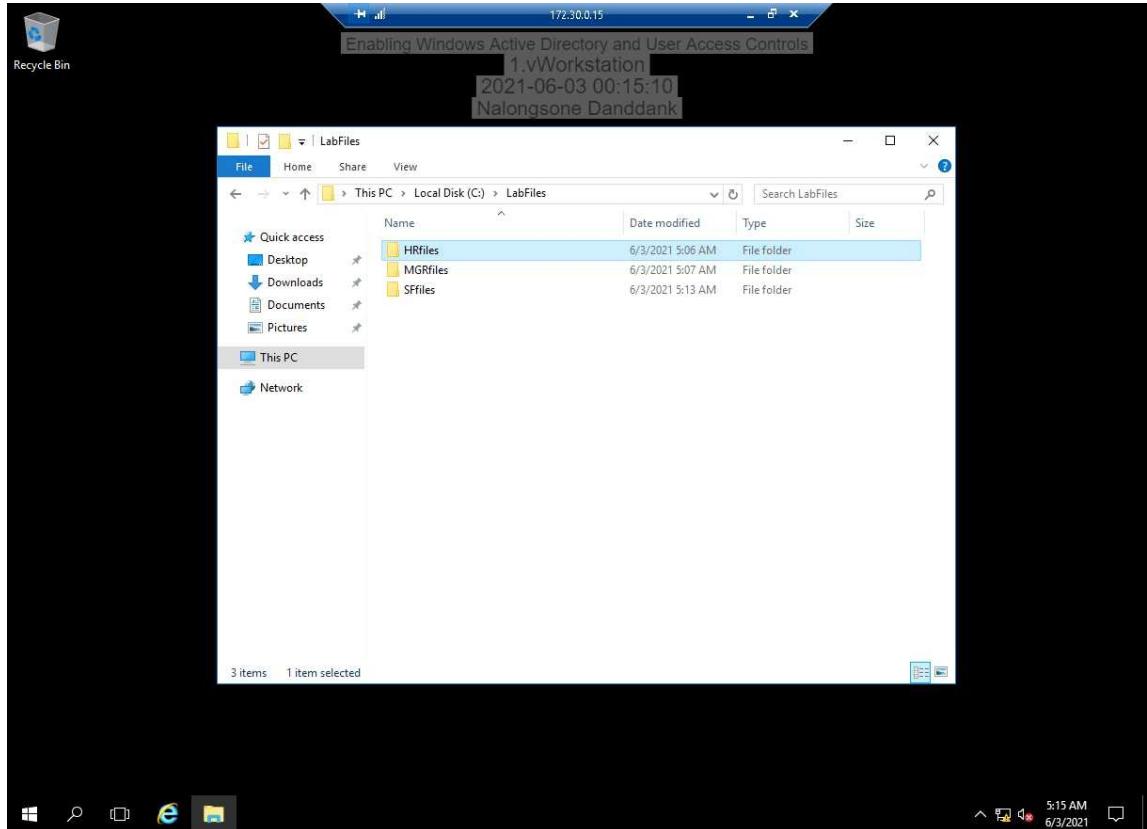


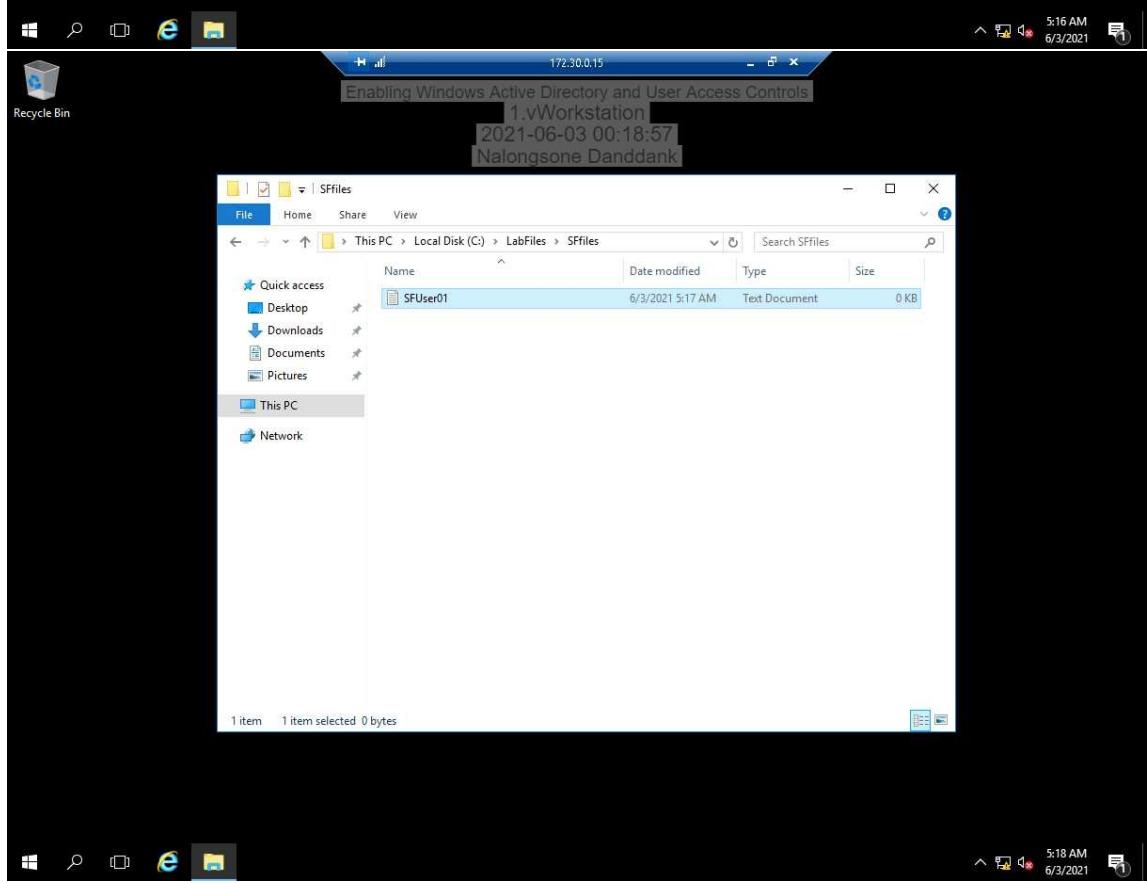
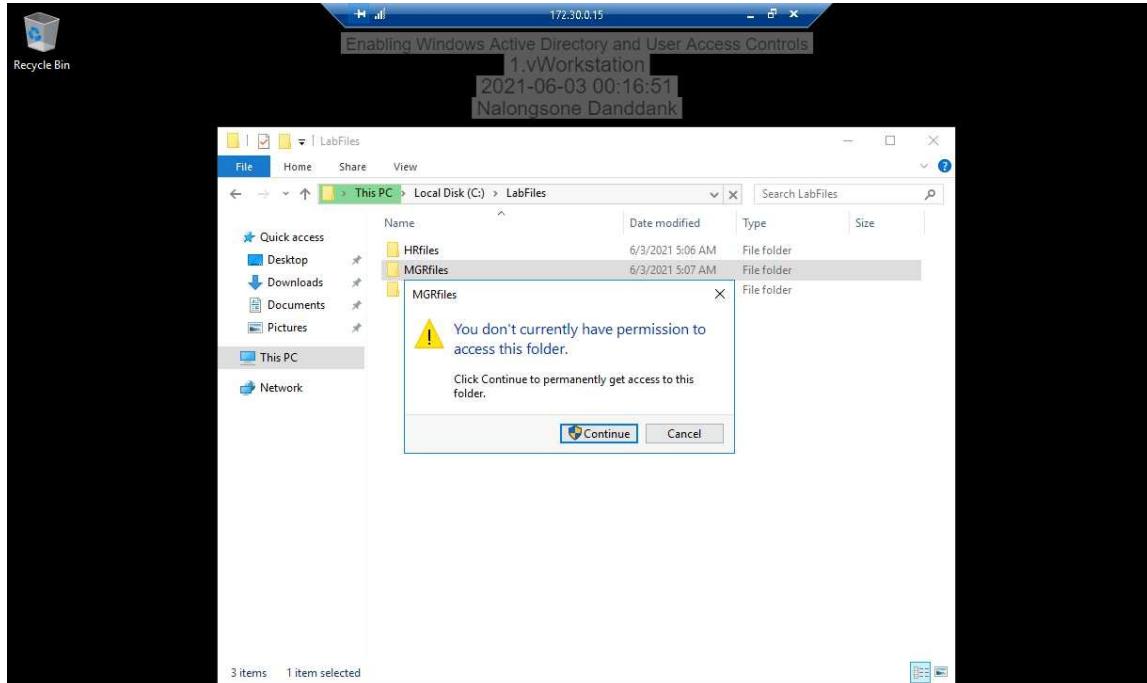


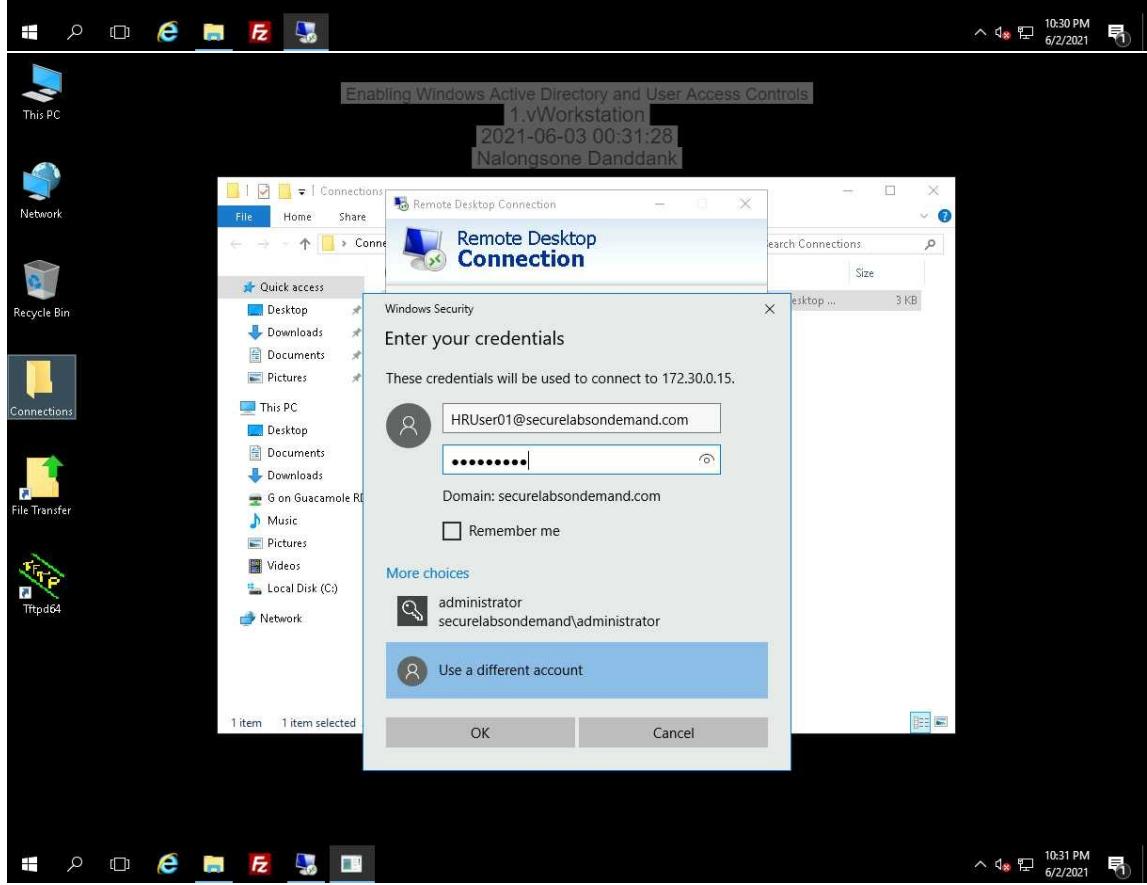
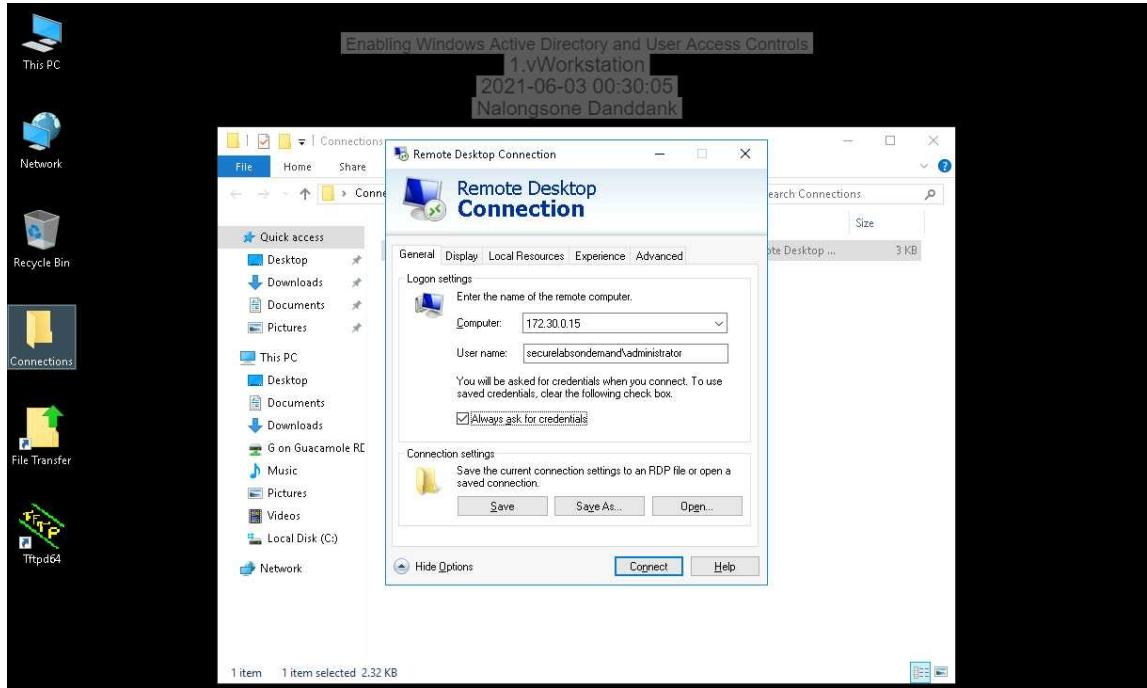


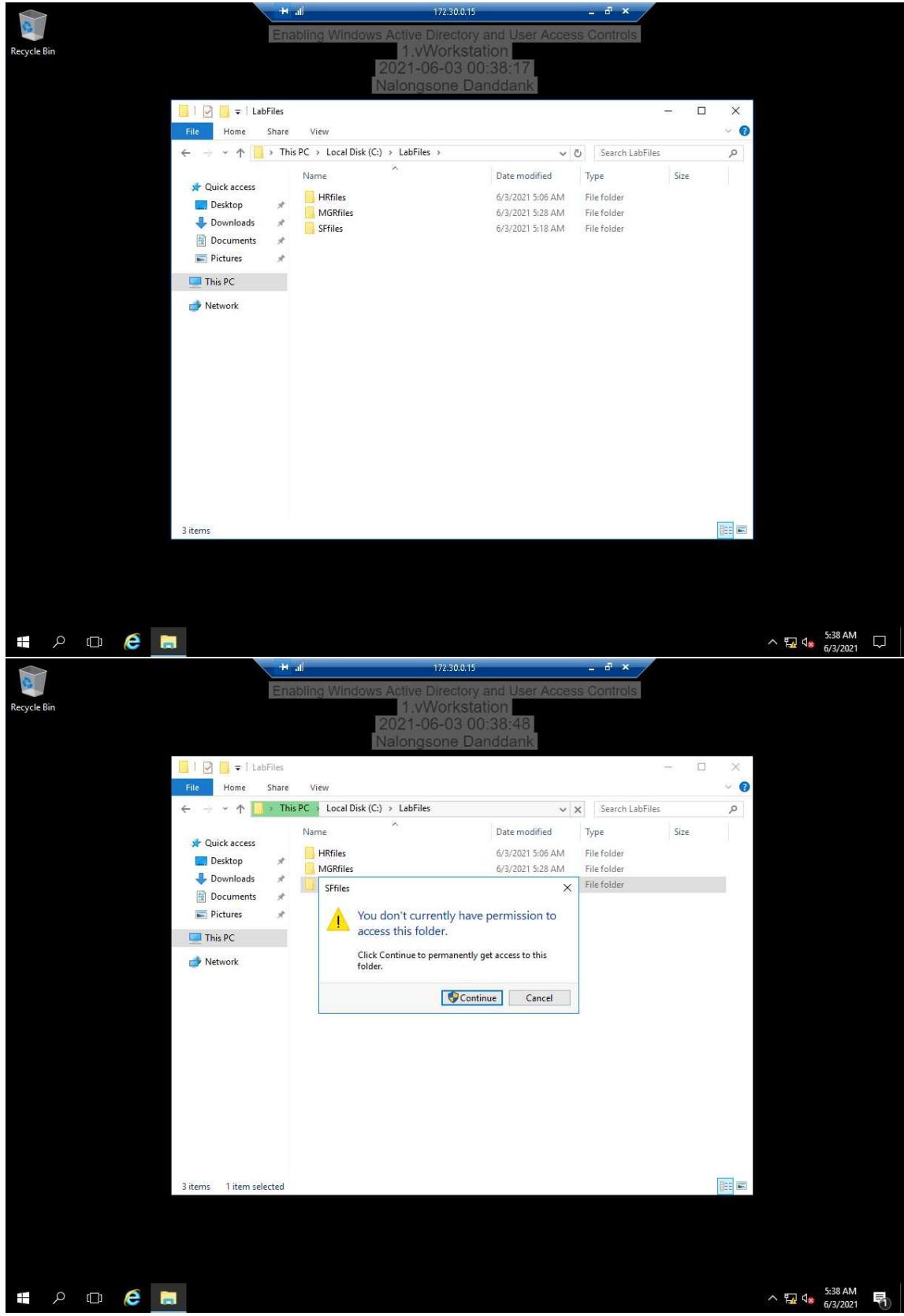
## Part 4: Practical Application

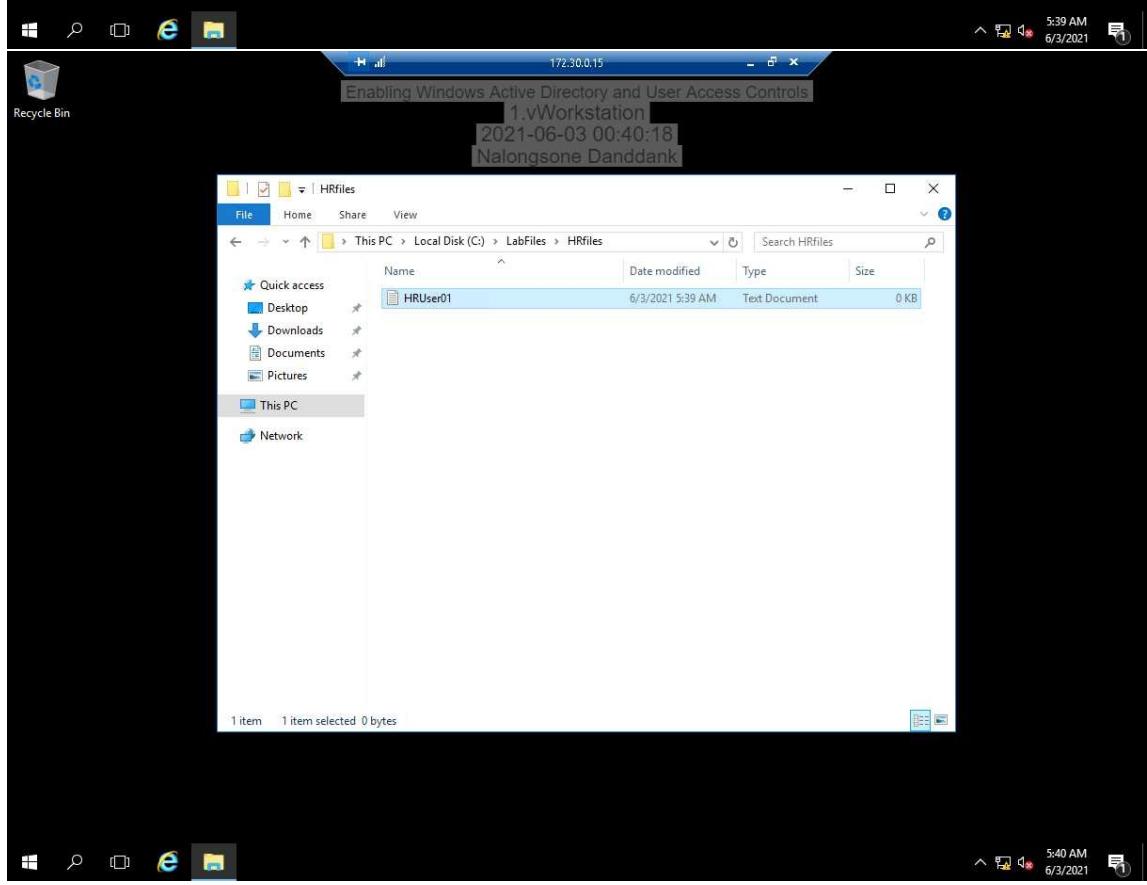
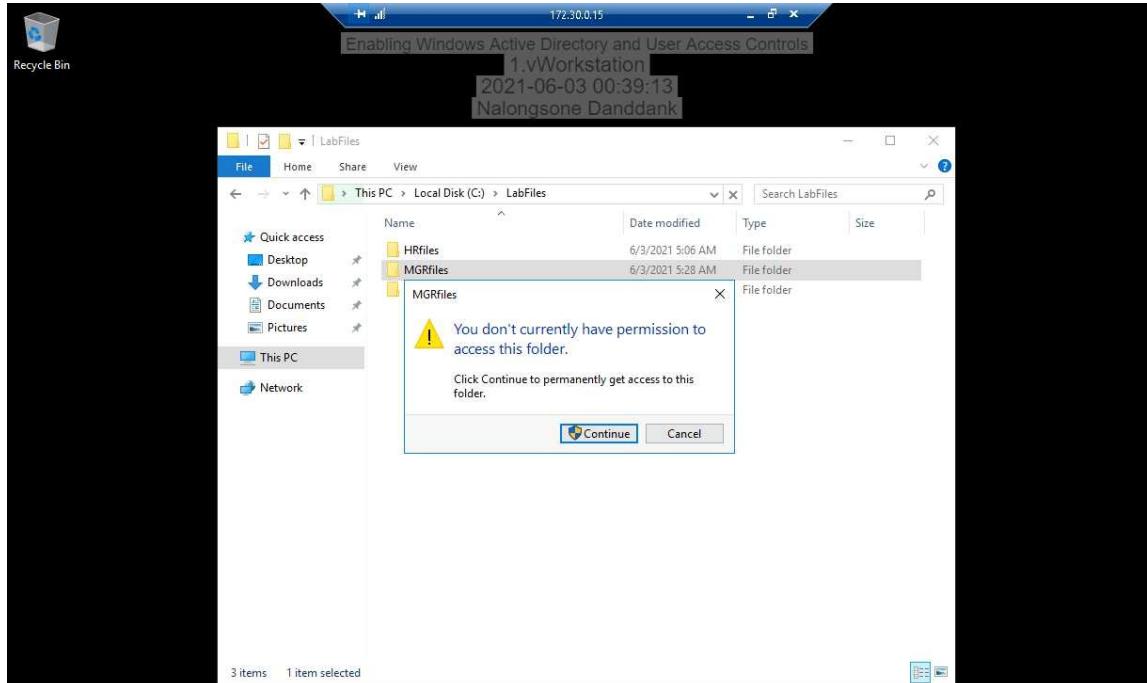


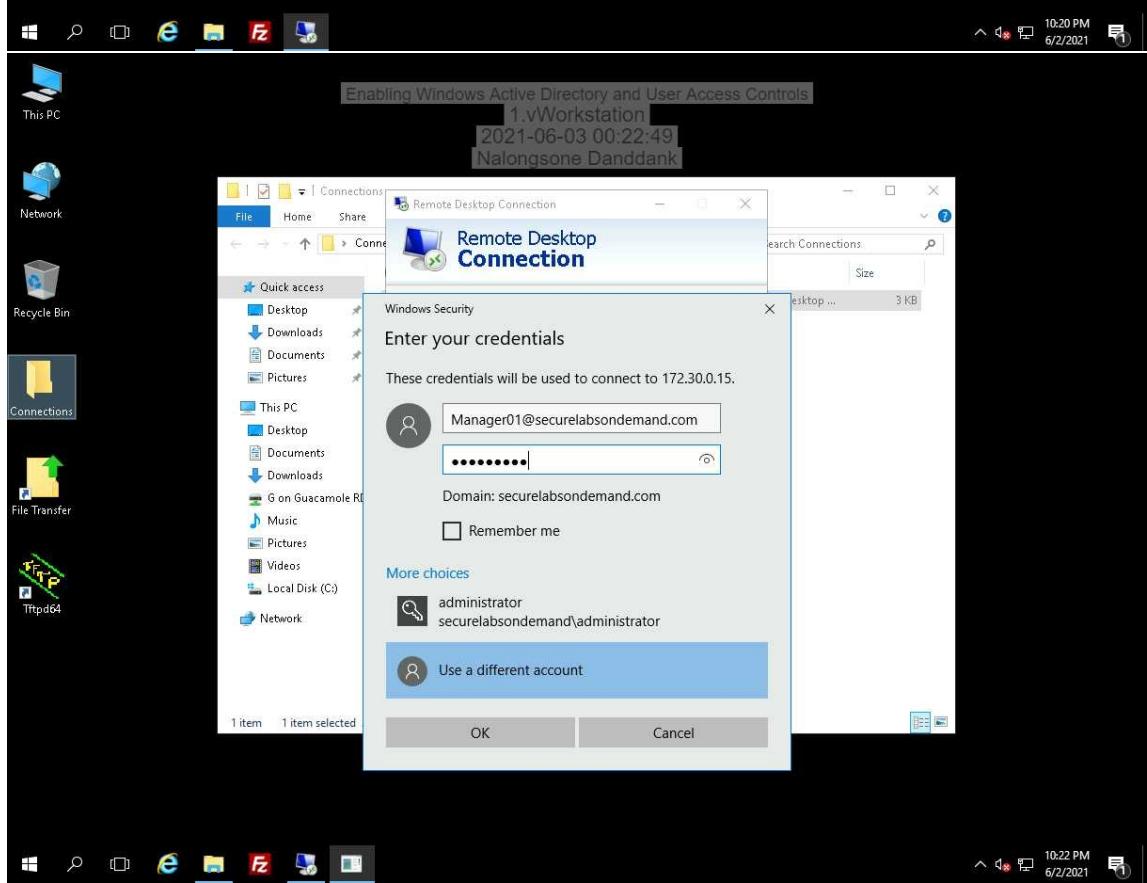
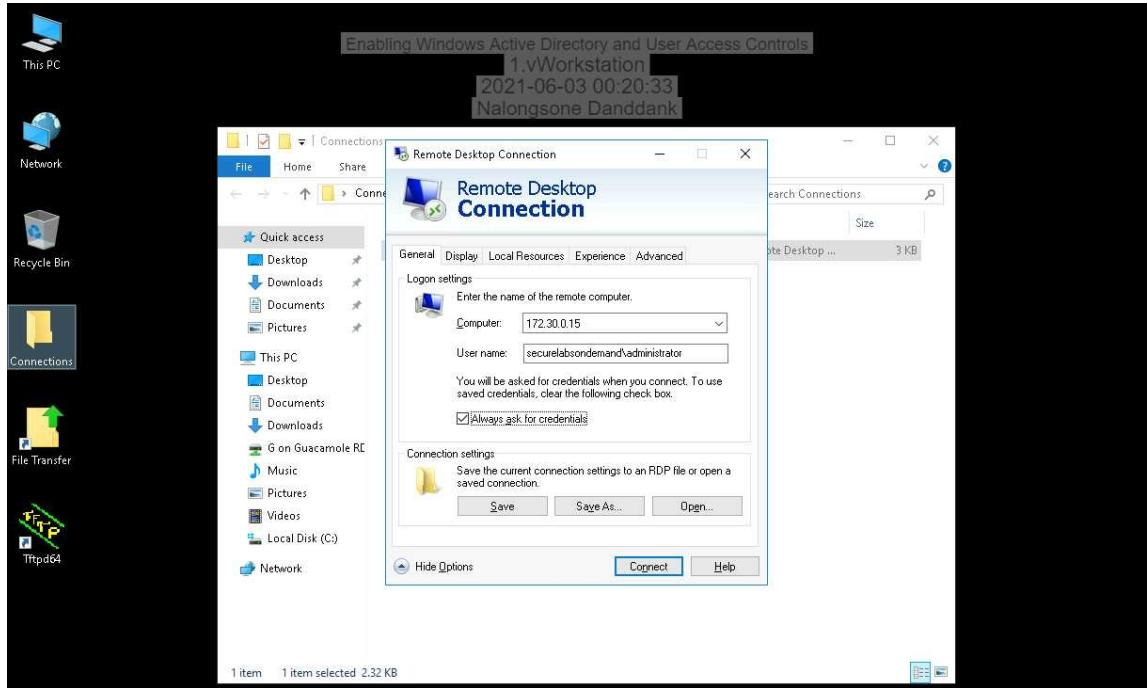


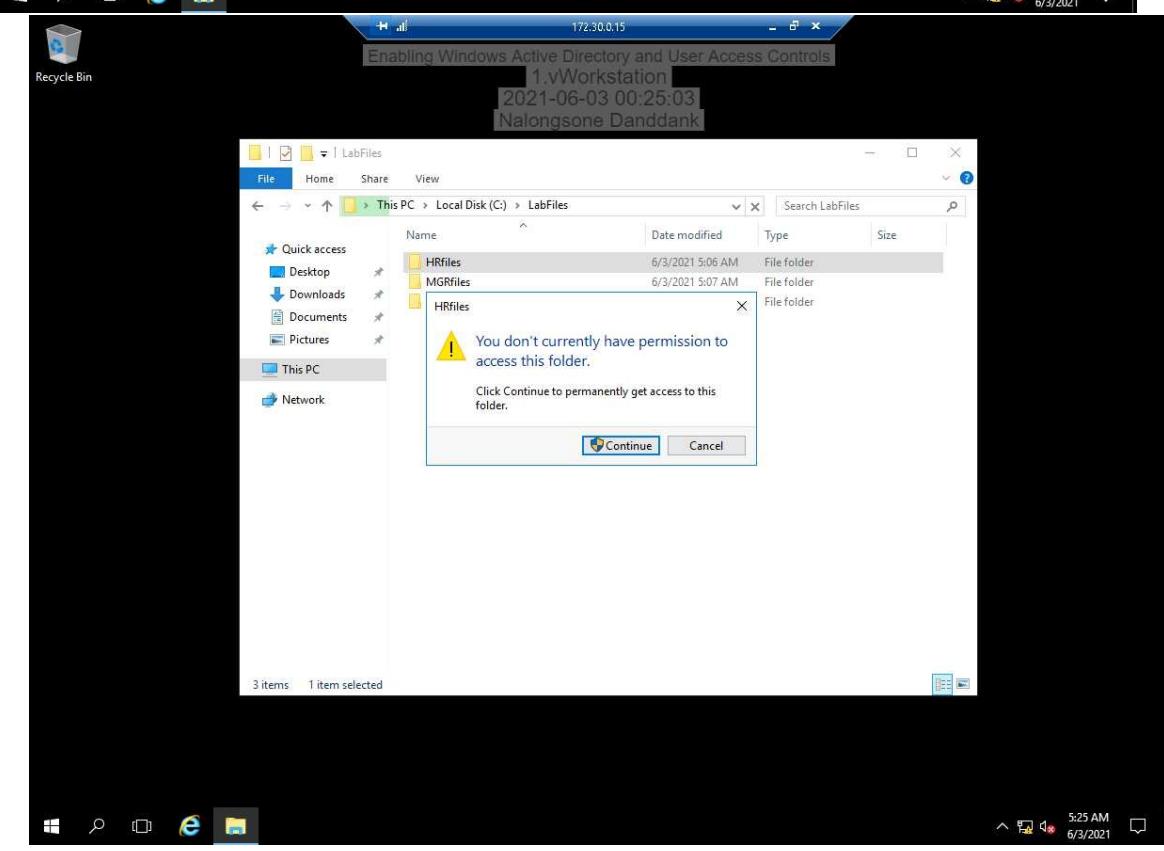
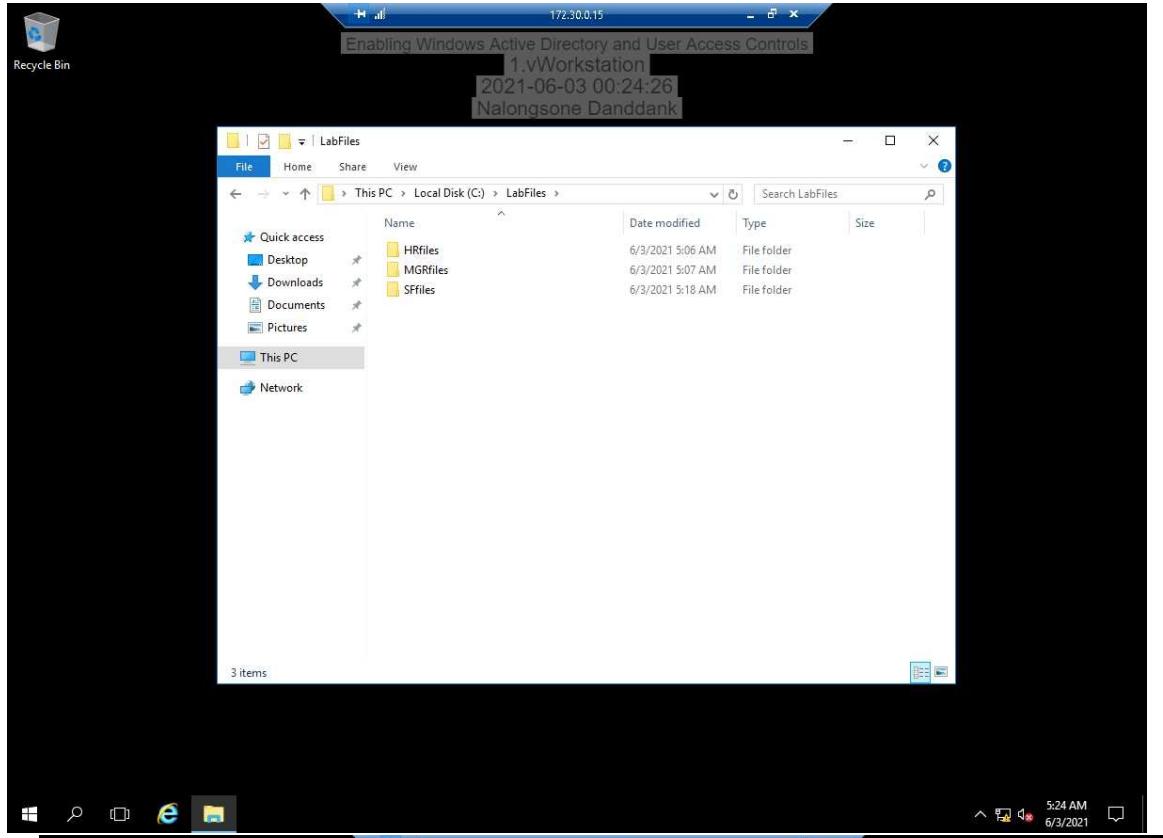


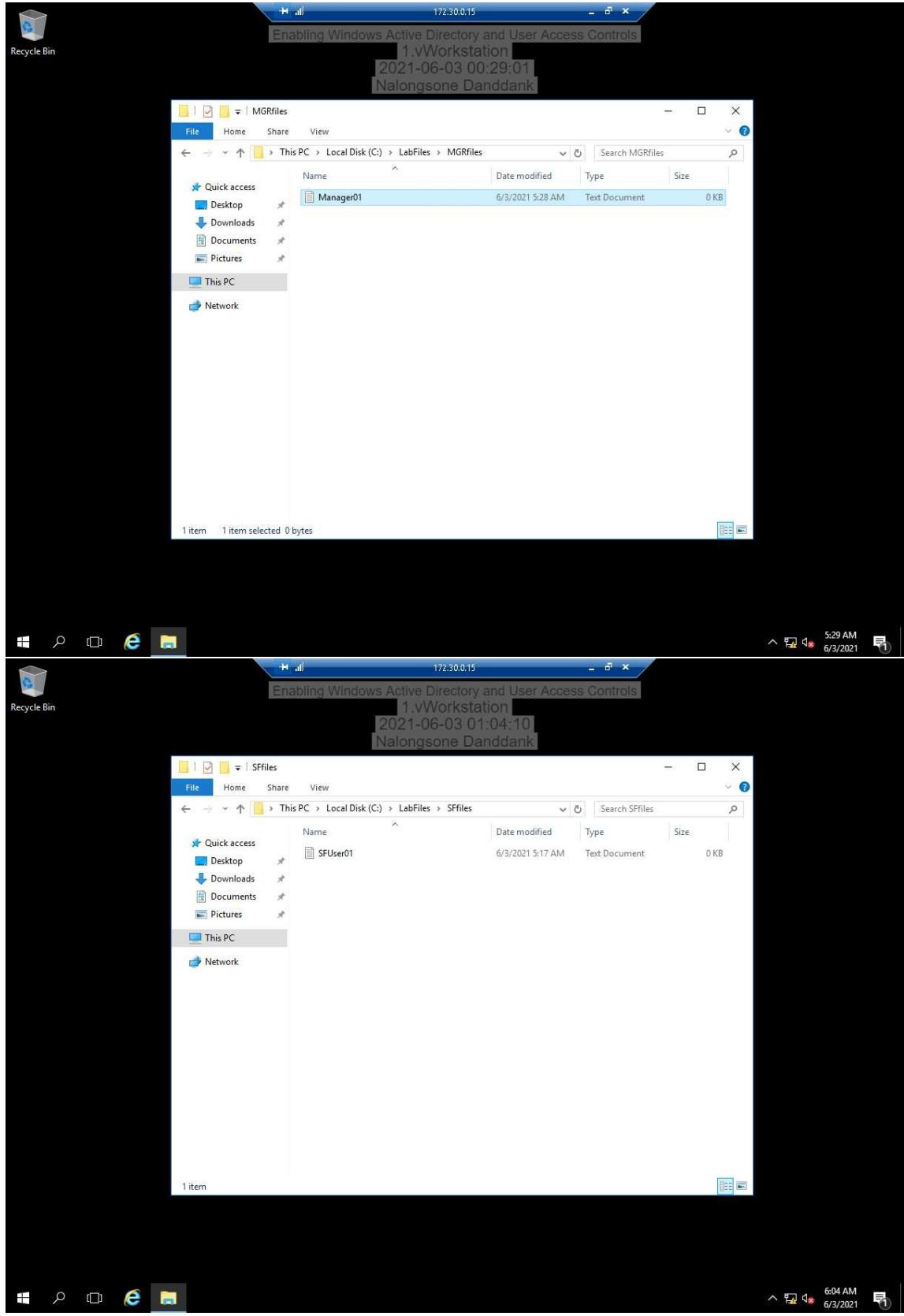












End.