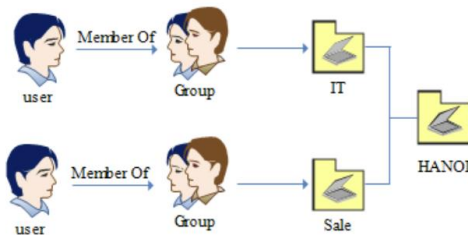


CHƯƠNG 5. QUẢN TRỊ GROUP POLICY

5.1. TRIỂN KHAI CHÍNH SÁCH GPO CƠ BẢN

5.1.1. Chuẩn bị

- Chuẩn bị 1 máy Server SRV19-DC-01 đã nâng cấp lên Domain quản lý miền qtm.com
- Tạo các OU tương ứng.



- Triển khai các chính sách trên phòng ban IT.
- Kiểm tra các chính sách khi áp dụng cho phòng ban IT bằng cách đăng nhập tài khoản thuộc phòng ban IT trên máy Client01.
- Sơ đồ địa chỉ IP như sau:

Thông số	SRV19-DC-01	Client01
IP address	192.168.1.2	192.168.1.100
Gateway	192.168.1.1	255.255.255.0
Subnet mask	255.255.255.0	192.168.1.1
DNS Server	192.168.1.2	192.168.1.2

5.1.2. Yêu cầu

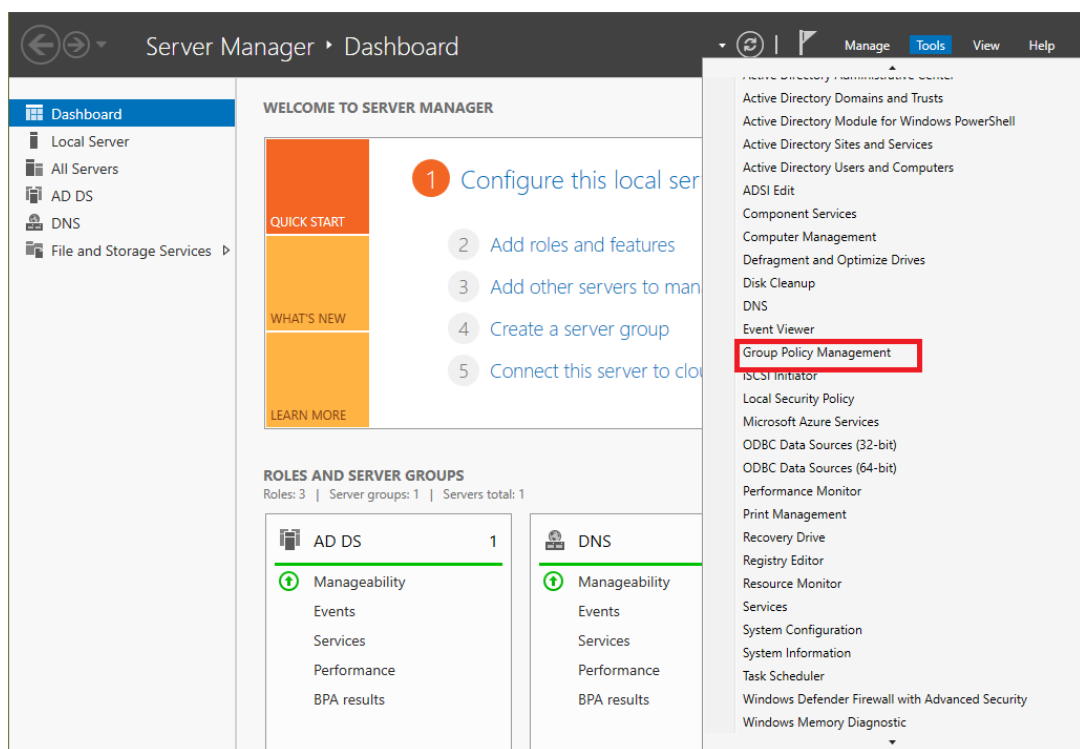
- Triển khai chính sách áp dụng trên Domain:
 - Chính sách password: số lượng password lưu trữ tối đa là 20, thời gian sử dụng tối đa là 30 ngày, sau 3 ngày thì mới có thể đổi password mới, chiều dài tối thiểu 9 ký tự, password có độ phức tạp và có mã hóa.
 - Chính sách đăng nhập sai 3 lần sẽ bị khóa trong 30 phút, thời gian để đặt lại bộ đếm khóa tài khoản là 5 phút.
 - Chính sách map ổ đĩa trên server.
- Triển khai chính sách áp dụng trên OU IT:
 - Đặt màn hình nền Desktop tất cả các máy tính

- Khóa Registry
- Khóa Task Manager
- Cấm DOS Command
- Xóa icon Computer trên Desktop
- Chặn đổi Theme
- Chặn Properties IP
- Khóa Taskbar
- Chặn truy cập Paint
- Ẩn item trong Control Panel

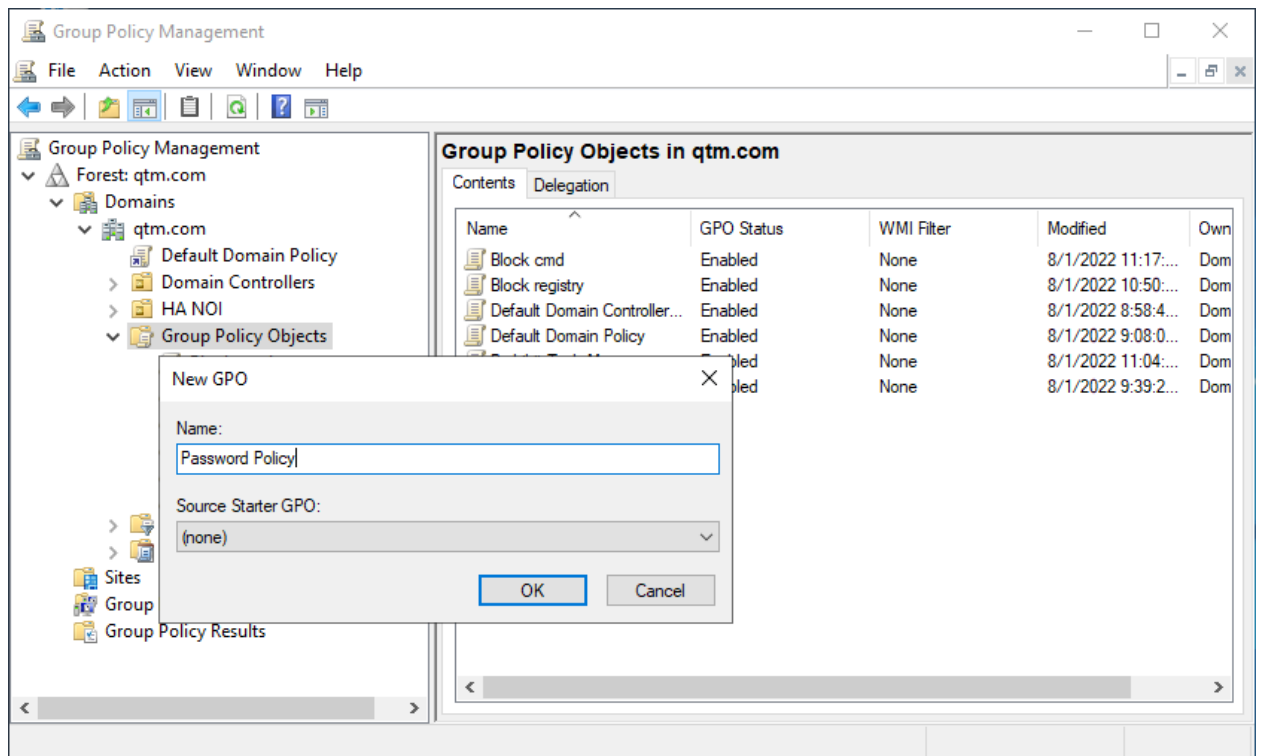
5.1.3. Triển khai chính sách áp dụng trên Domain

5.1.3.1. Chính sách password theo yêu cầu

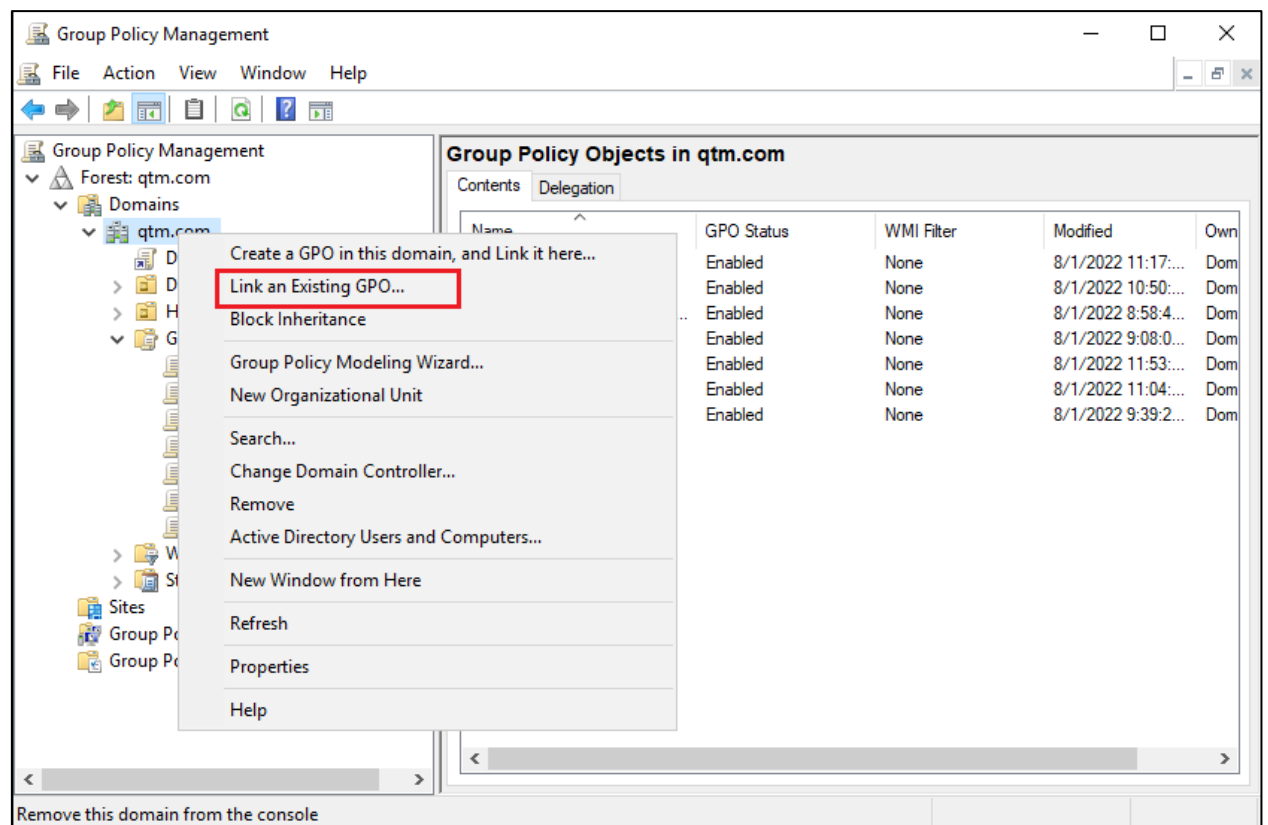
Bước 1. Cấu hình GPO trên máy **SRV19-DC-01**. Tạo các chính sách password trên domain. Vào **Server Manager / Tools / Group Policy Management**.



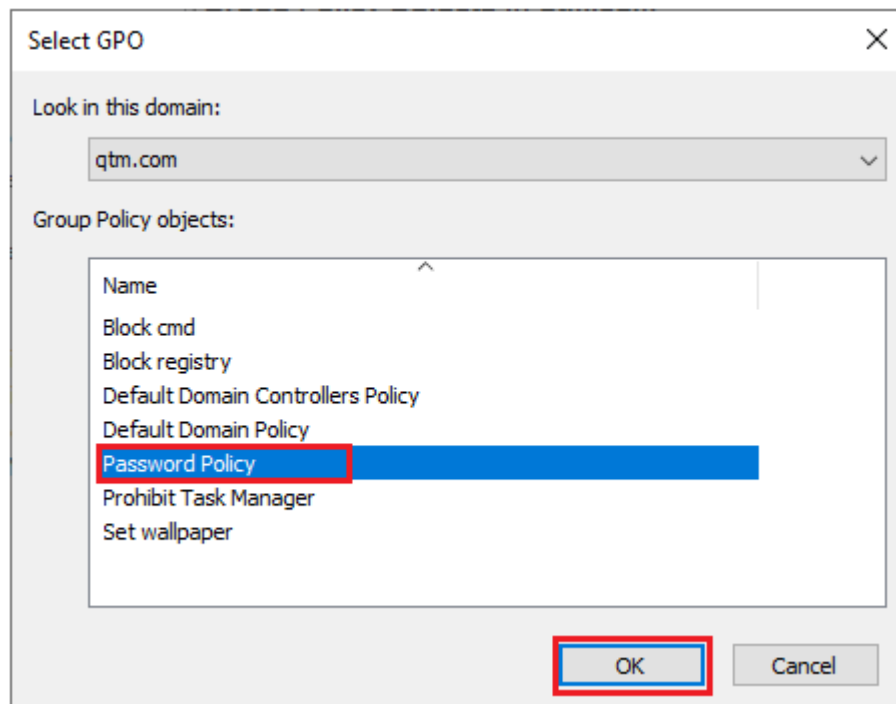
Bước 2. Tại cửa sổ **Group Policy Management**, click chuột phải vào **Group Policy Object**, chọn **New**. Tại cửa sổ **New GPO**, nhập vào tên **Name** là **Password Policy**.



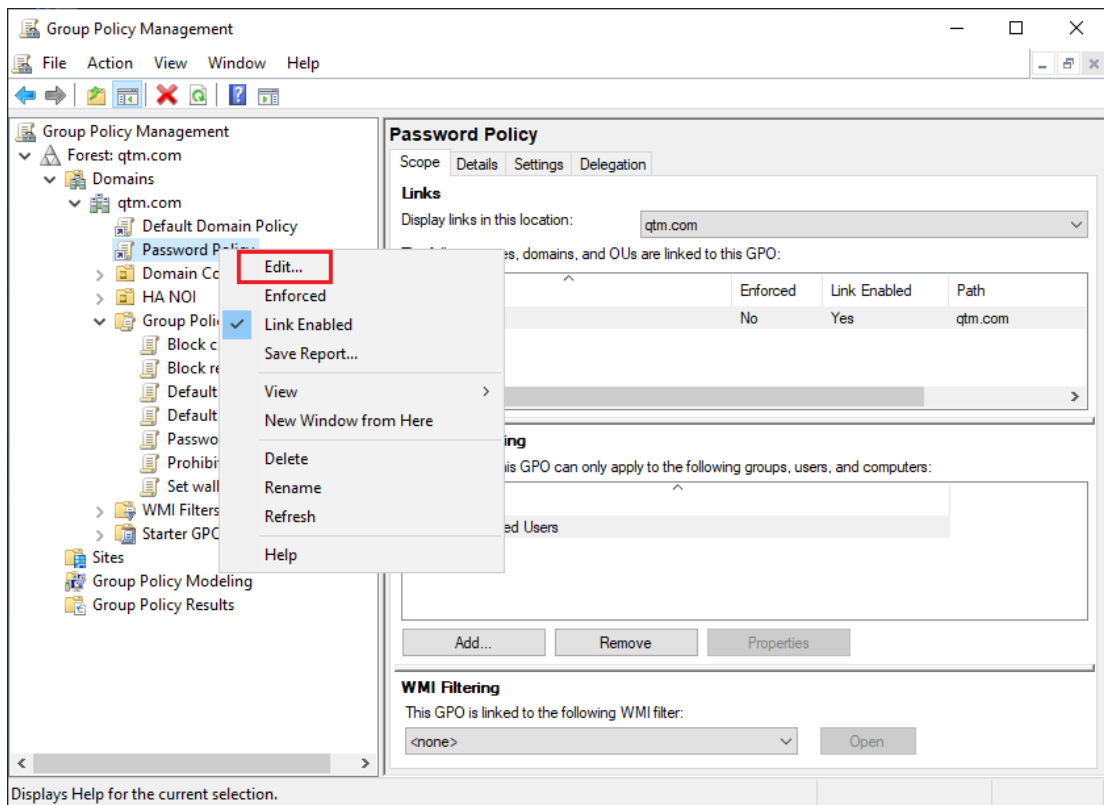
Bước 3. Tại cửa sổ **Group Policy Management**, click chuột phải vào **qtm.com**, chọn **Link an Existing GPO**.



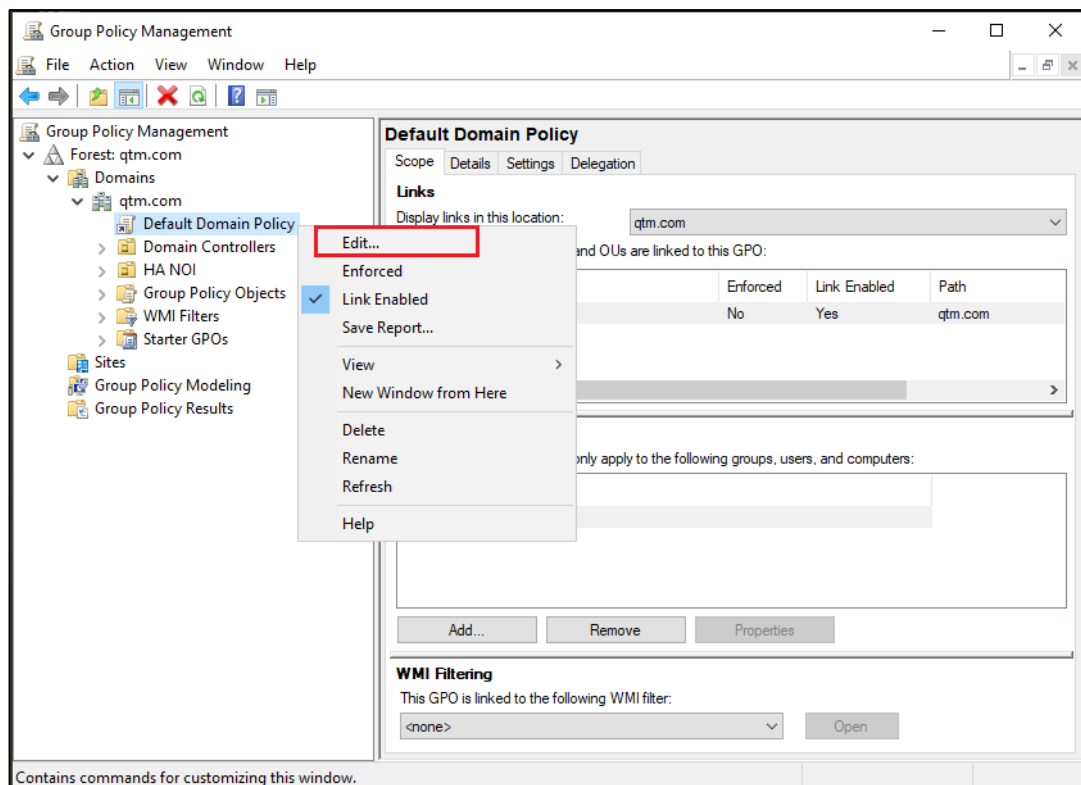
Bước 4. Tại cửa sổ **Select GPO**, chọn chính sách **Password Policy**, sau đó chọn **OK**.



Bước 5. Tại cửa sổ **Group Policy Management**, chọn chính sách **Password Policy** và chọn **Edit**.



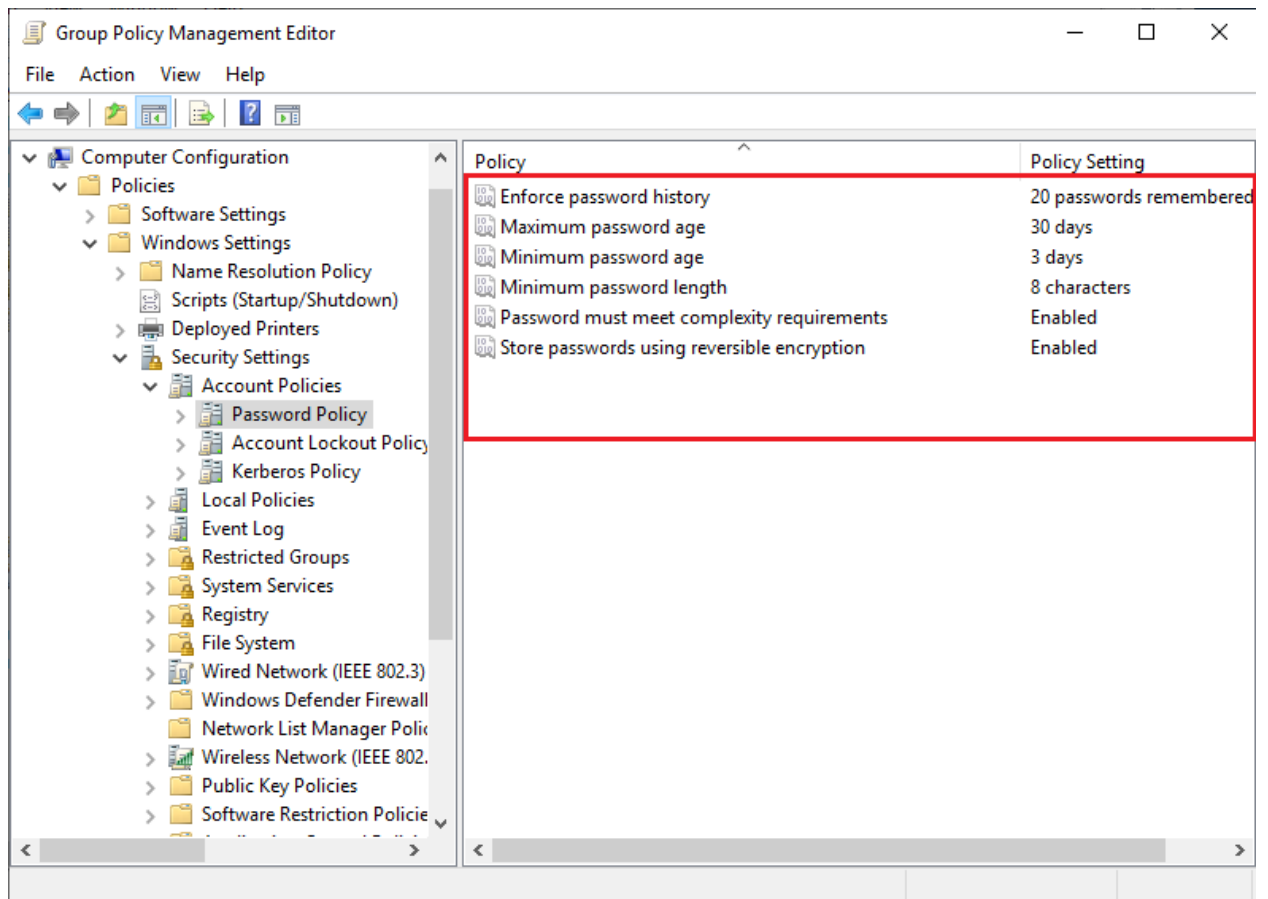
Lưu ý: Tạo chính sách áp dụng trên Domain có thể thực hiện tại chính sách “**Default Domain Policy**” (như hình bên dưới) hoặc có thể tạo chính sách mới tại mục **Group Policy Objects** và thực hiện **link** tới domain (thực hiện như bước 2, 3, 4).



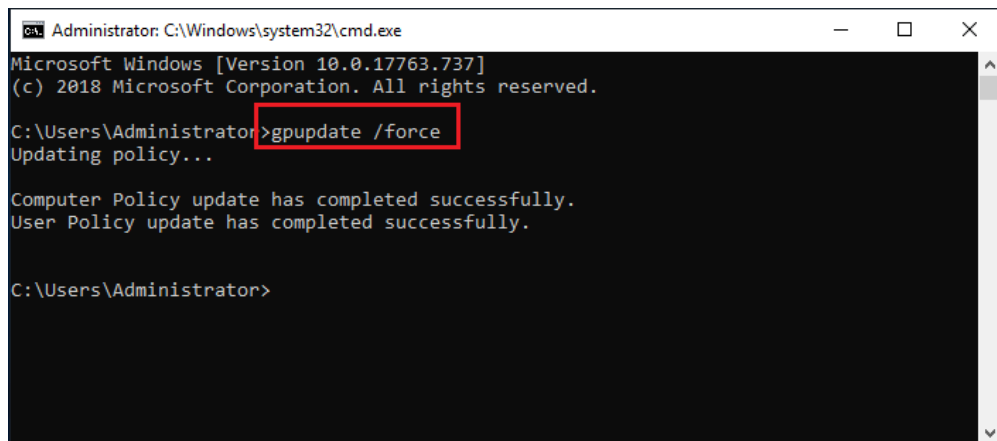
Bước 5. Tại cửa sổ **Group Policy Managerment Editor**, chọn vào mục **Computer Configuration / Policies / Windows Settings\ Security Settings\ Account Policies\ Password Policy**. Thay đổi các chính sách mật khẩu ở bảng bên phải:

- *Enforce password history*: Số lượng password của User mà hệ thống sẽ ghi nhớ (tối đa là 24).
- *Maximum password age*: Thời gian sử dụng tối đa của mật khẩu, sau thời gian này hệ thống yêu cầu đổi mật khẩu mới.
- *Minimum password age*: Tuổi thọ tối thiểu của mật khẩu, nếu để là 1 days thì sau 1 ngày User mới có quyền đổi mật khẩu.
- *Minimum password length*: Quy định chiều dài ký tự tối thiểu của mật khẩu.
- *Password must meet complexity requirements*: Yêu cầu mật khẩu phức tạp nếu Enable tính năng này lên. Độ khó mật khẩu yêu cầu chứa các ký tự từ ba trong bốn danh mục sau:
 - Chữ viết hoa (A đến Z)
 - Chữ viết thường (a đến z)
 - Chữ số cơ bản (0 đến 9)
 - Các ký tự đặc biệt (ví dụ: !, \$, #, %).
- *Store passwords using reversible encryption*: Mặc định Windows Server lưu mật khẩu User dưới dạng mã hóa trong file SAM (Security Account Manager). Windows sử dụng hai dạng mã hóa mật khẩu là:
 - Reversible đây là mã hóa hai chiều, có thể dịch ngược lại mật khẩu. Nếu chọn enable thì hệ thống sẽ sử dụng dạng mã hóa này, làm giảm độ an toàn khi bị đánh cắp thông tin trong file SAM.
 - Irreversible dạng mã hóa một chiều, mật khẩu không thể dịch lại được.

Thực hiện mở từng chính sách password và thực hiện theo yêu cầu, kết quả như sau:



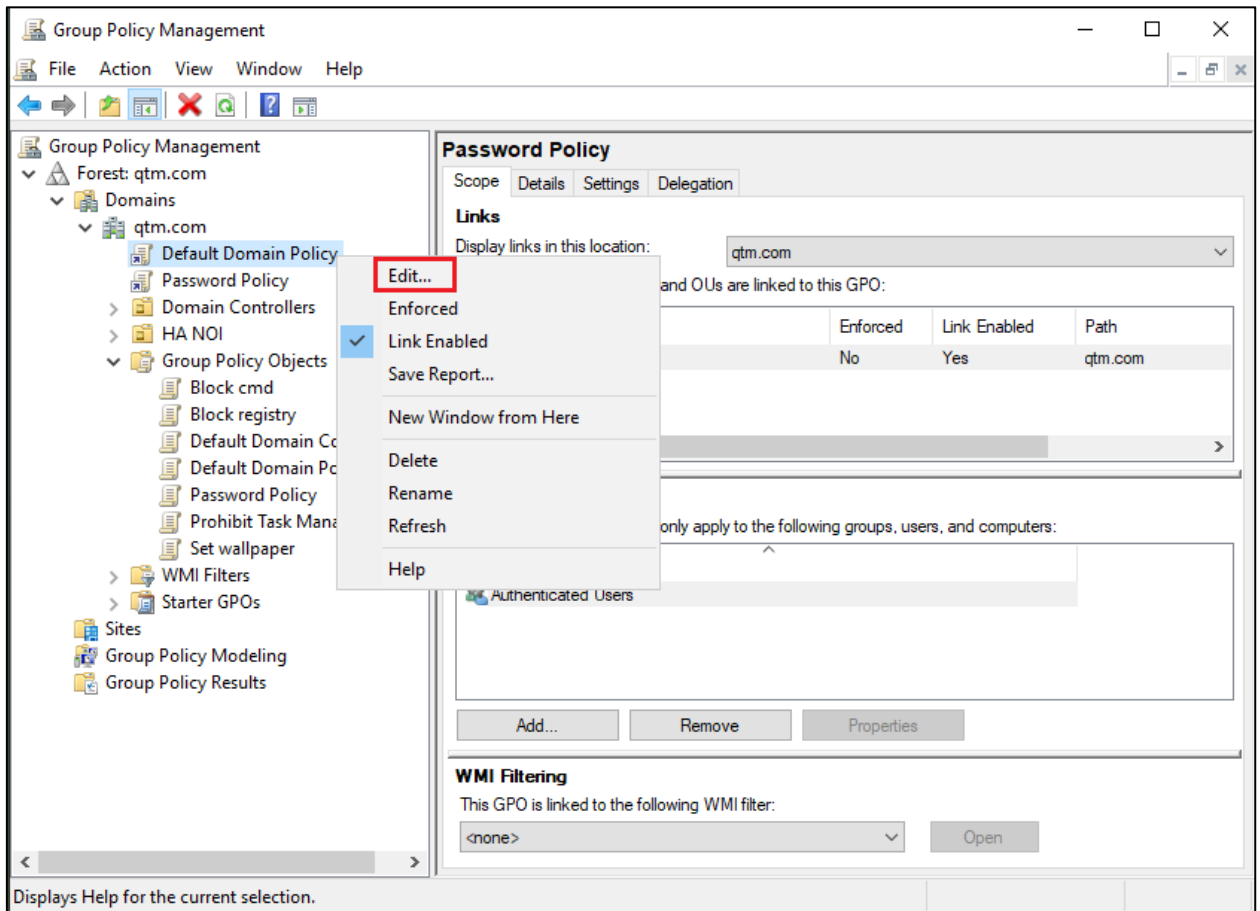
Bước 6. Cập nhật GPO, vào Cmd / gõ lệnh *gpupdate /force*



Bước 7. Thực hiện tạo user mới và đặt password để kiểm tra chính sách.

5.1.3.2. Chính sách đăng nhập theo yêu cầu

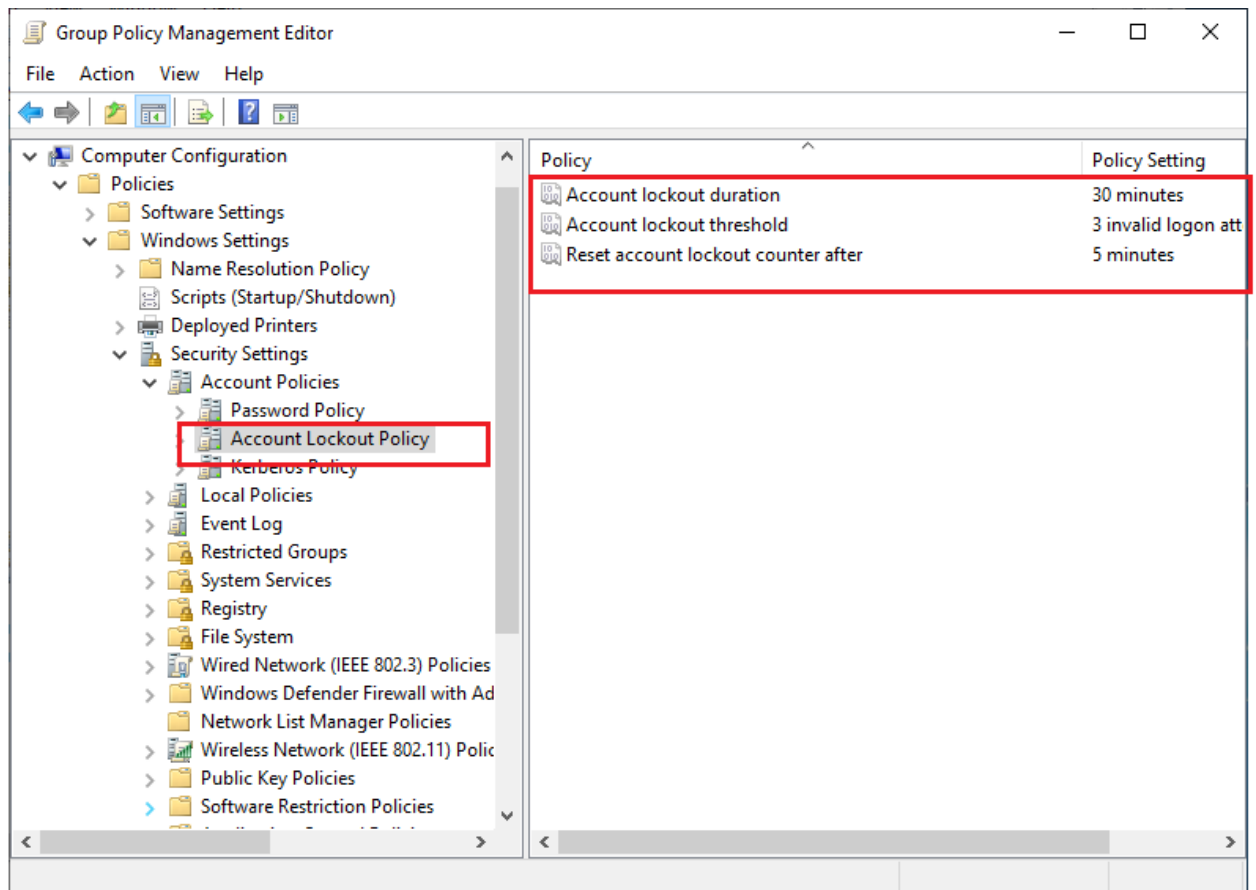
Bước 1. Tại cửa sổ **Group Policy Management**, click chuột phải vào **Domain Default Policy**, chọn **Edit**.



Bước 2. Tại cửa sổ **Group Policy Managerment Editor**, chọn vào mục **Computer Configuration / Policies / Windows Settings\ Security Settings\ Account Policies\ Account Lockout Policy**. Thay đổi các chính sách mật khẩu ở bảng bên phải:

- Account lockout duration: chỉ định thời gian tính bằng phút mà tài khoản có thể bị khóa. Ví dụ: nếu tài khoản bị khóa trong 10 phút, người dùng có thể thử lại sau thời gian đó. Mặc định là không có khóa. Khi xác định chính sách, thời gian mặc định là 30 phút. Cài đặt có thể từ 0 đến 99,999. Khi được đặt thành 0, tài khoản sẽ vẫn bị khóa cho đến khi quản trị viên mở khóa theo cách thủ công.
- Account lockout threshold: chỉ định số lần đăng nhập không thành công mà người dùng được phép trước khi tài khoản bị khóa (ví dụ: 3). Sau khi đạt đến ngưỡng, tài khoản sẽ bị khóa. Nếu giá trị này được đặt thành 0, tài khoản sẽ không bị khóa. Cài đặt này có thể từ 0 đến 999.
- Reset account lockout counter after: có thể chọn đặt lại bộ đếm khóa tài khoản sau một vài phút. Tại thời điểm đó, số đếm sẽ bắt đầu lại từ 1.

Thực hiện mở từng chính sách Account Lockout Policy và thực hiện theo yêu cầu, kết quả như sau:



Bước 3. Cập nhật GPO, vào Cmd / gõ lệnh *gpupdate /force*

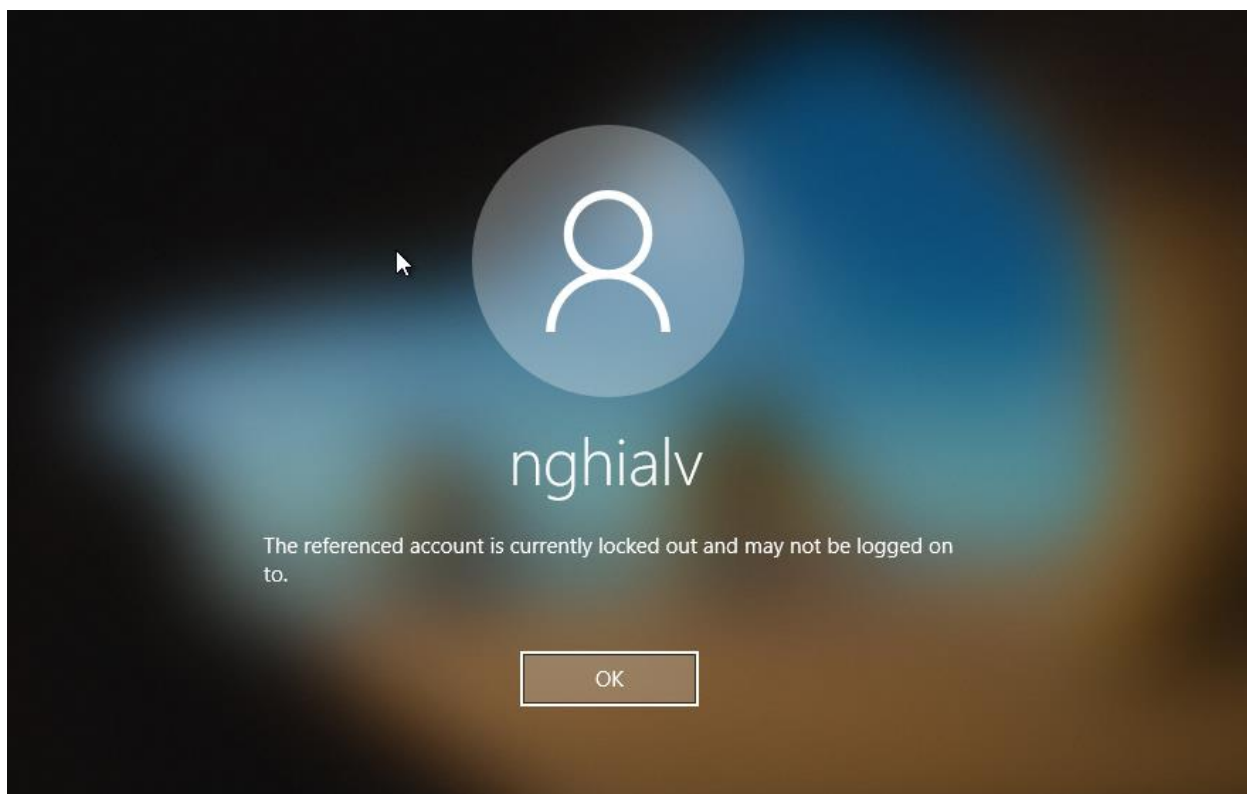
```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.

C:\Users\Administrator>
```

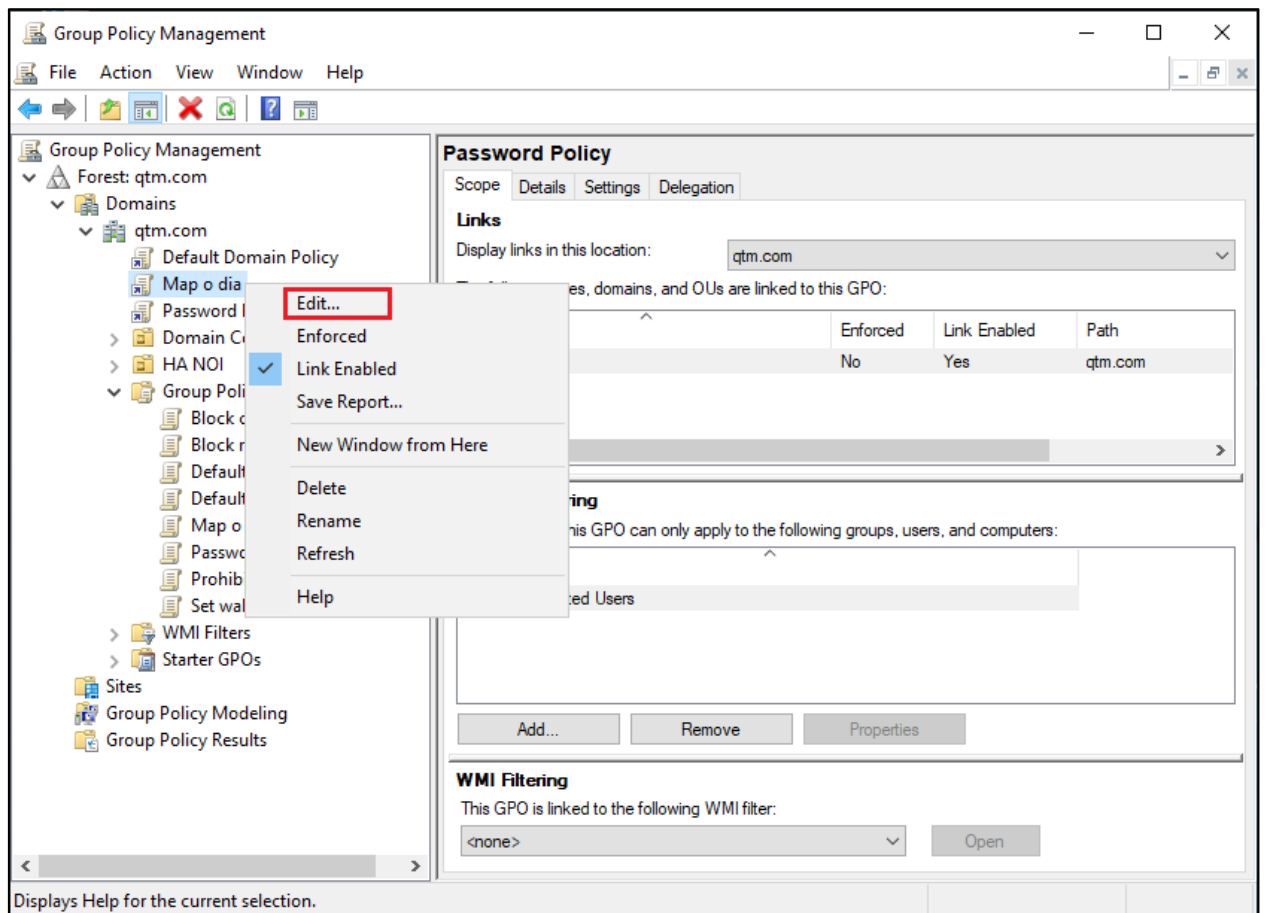
Bước 4. Thực hiện tạo đăng nhập sai 3 lần bằng tài khoản **nghialv** trên máy **Client01**. Kết quả.



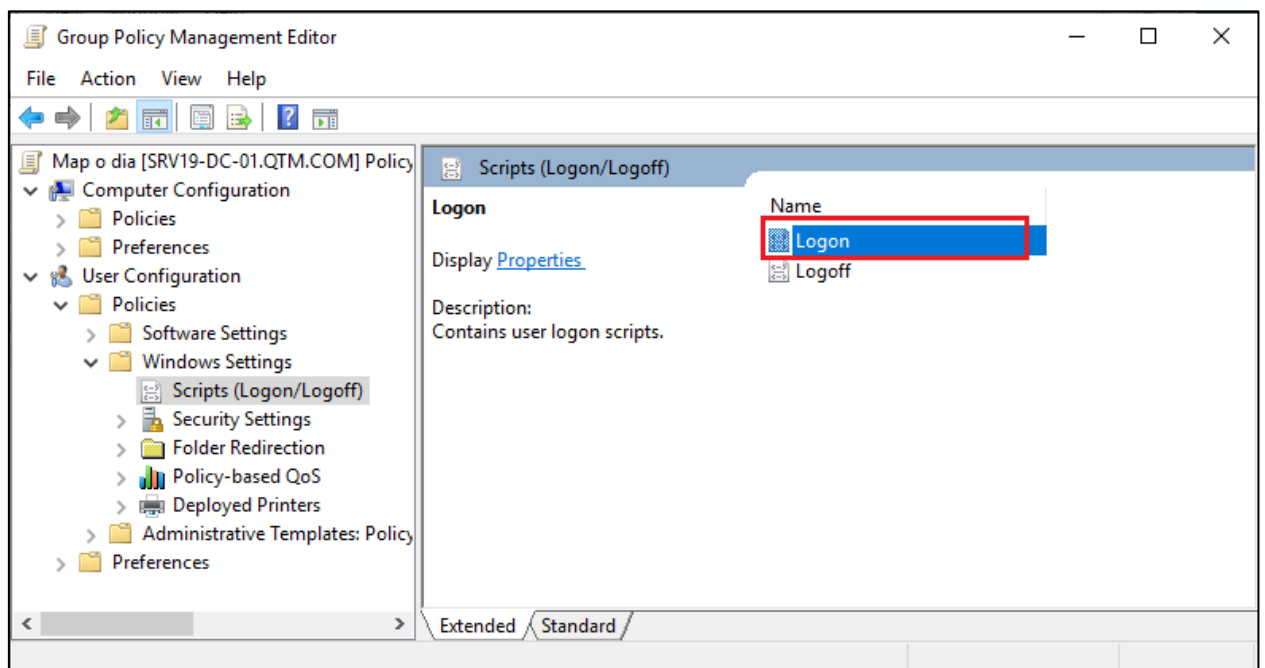
5.1.3.3. Chính sách map ổ đĩa trên Server xuống các máy Client

Bước 1. Tại cửa sổ **Group Policy Management**:

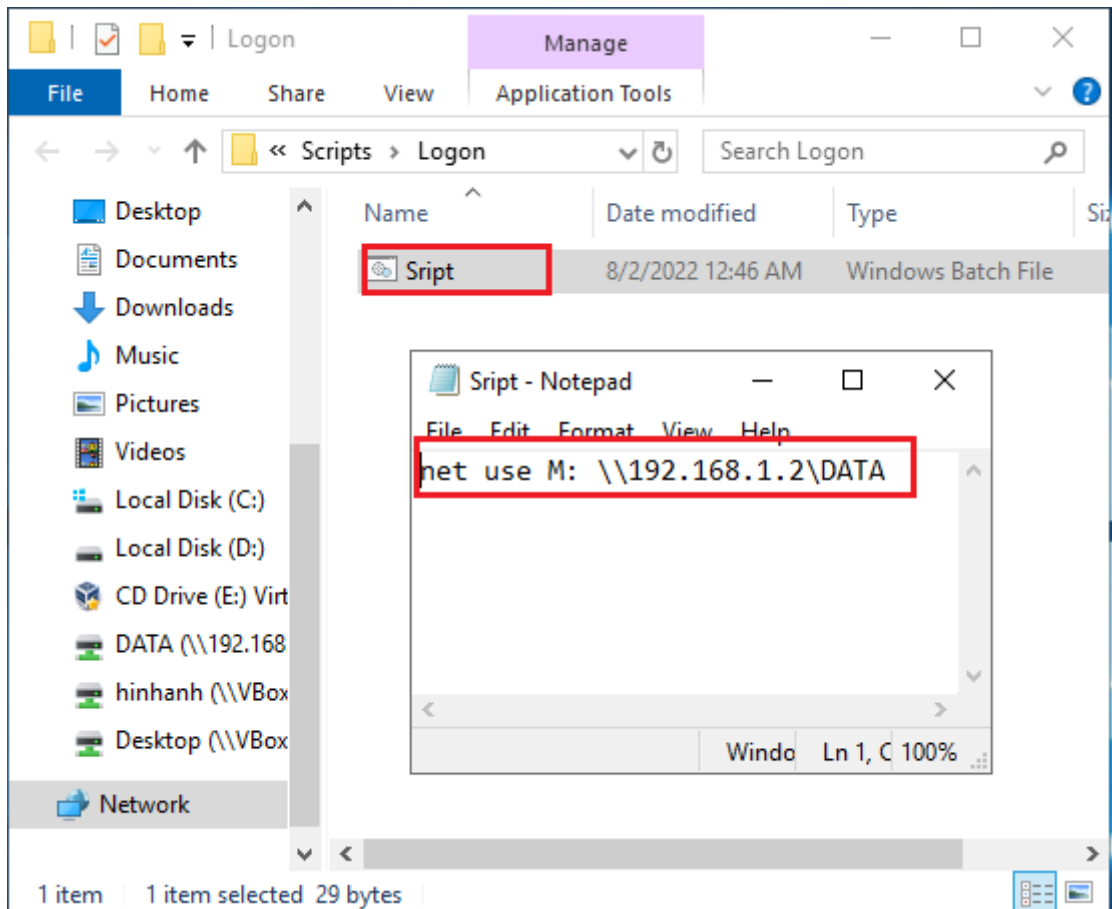
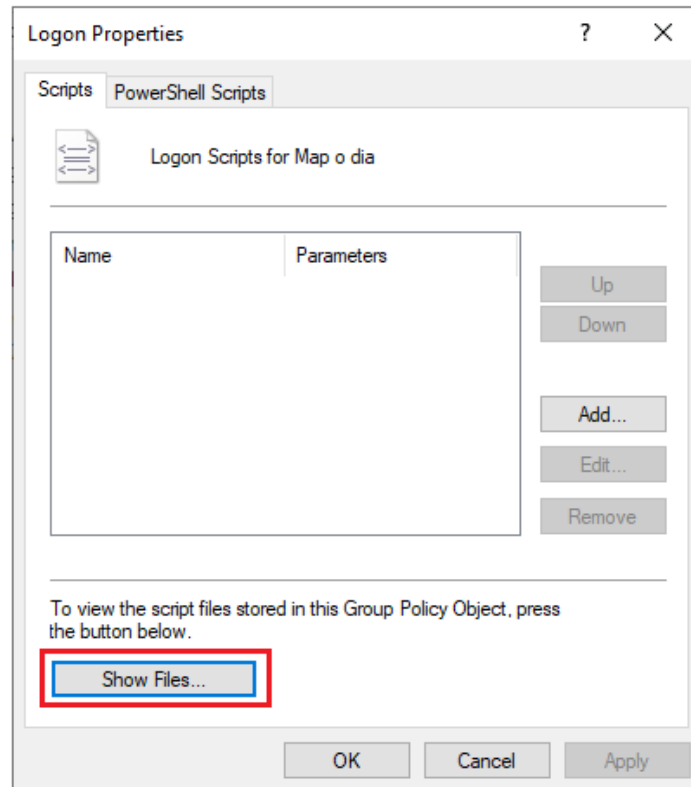
- Click chuột phải vào **Group Policy Object**, chọn **New**.
- Tại cửa sổ **New GPO**, nhập vào tên **Name** là **Map o dia**.
- Tại cửa sổ **Group Policy Management**, click chuột phải vào **qtm.com**, chọn **Link an Existing GPO**.
- Tại cửa sổ **Select GPO**, chọn chính sách **Map o dia**, sau đó chọn **OK**.
- Tại cửa sổ **Group Policy Managerment**, chọn chính sách **Pasword Policy** và chọn **Edit**.



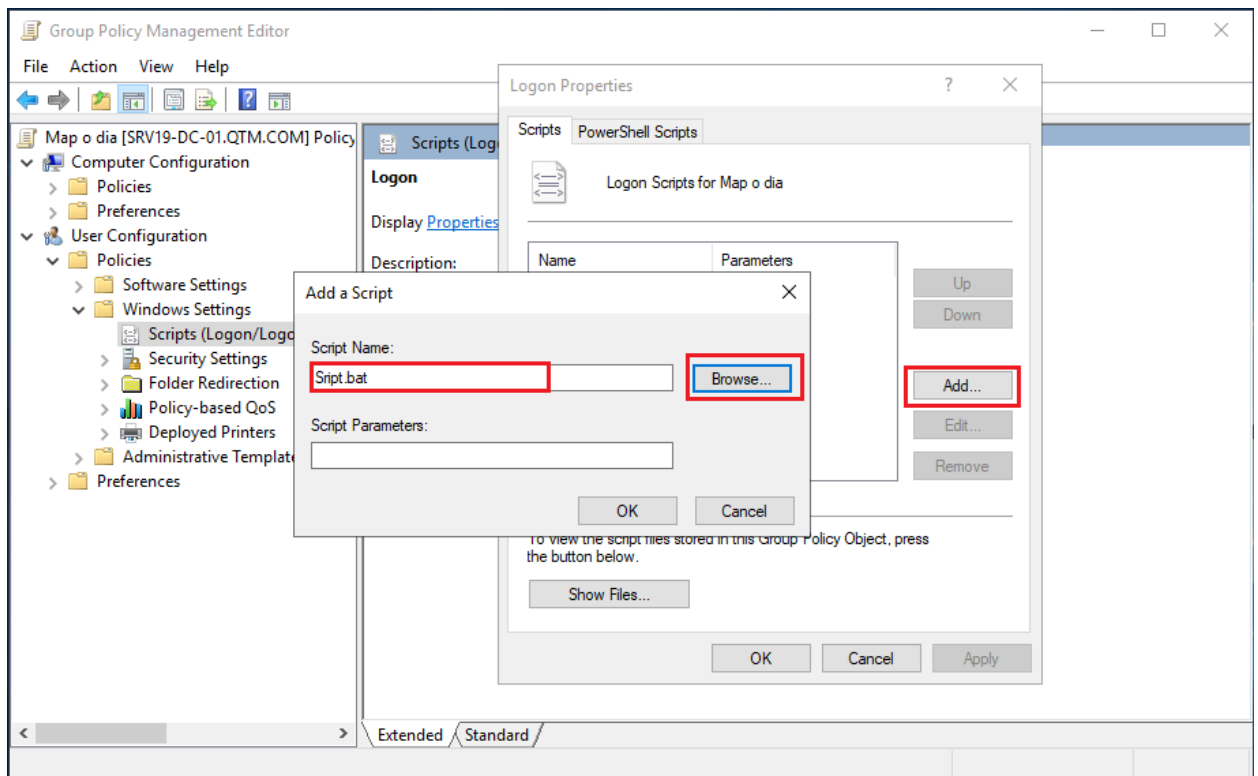
Bước 2. Tại cửa sổ **Group Policy Management Editor**, chọn vào mục **User Configuration / Policies / Windows Settings\ Scripts (Logon/Logoff)**, chọn **Logon**.



Bước 3. Tại cửa sổ **Logon Properties**, chọn **Show Files** để truy cập tới folder **Logon** tạo file **Scrip.bat** với nội dung như sau: `net use M: \\192.168.1.2\Data` (với Data là thư mục được chia sẻ bởi Server).



Bước 4. Tại cửa sổ **Logon Properties**, chọn **Add**, chọn **Browse** tới file **Script.bat**, chọn **OK**, chọn **OK**.



Bước 5. Cập nhật GPO, vào **Cmd** / gõ lệnh **gpupdate /force**

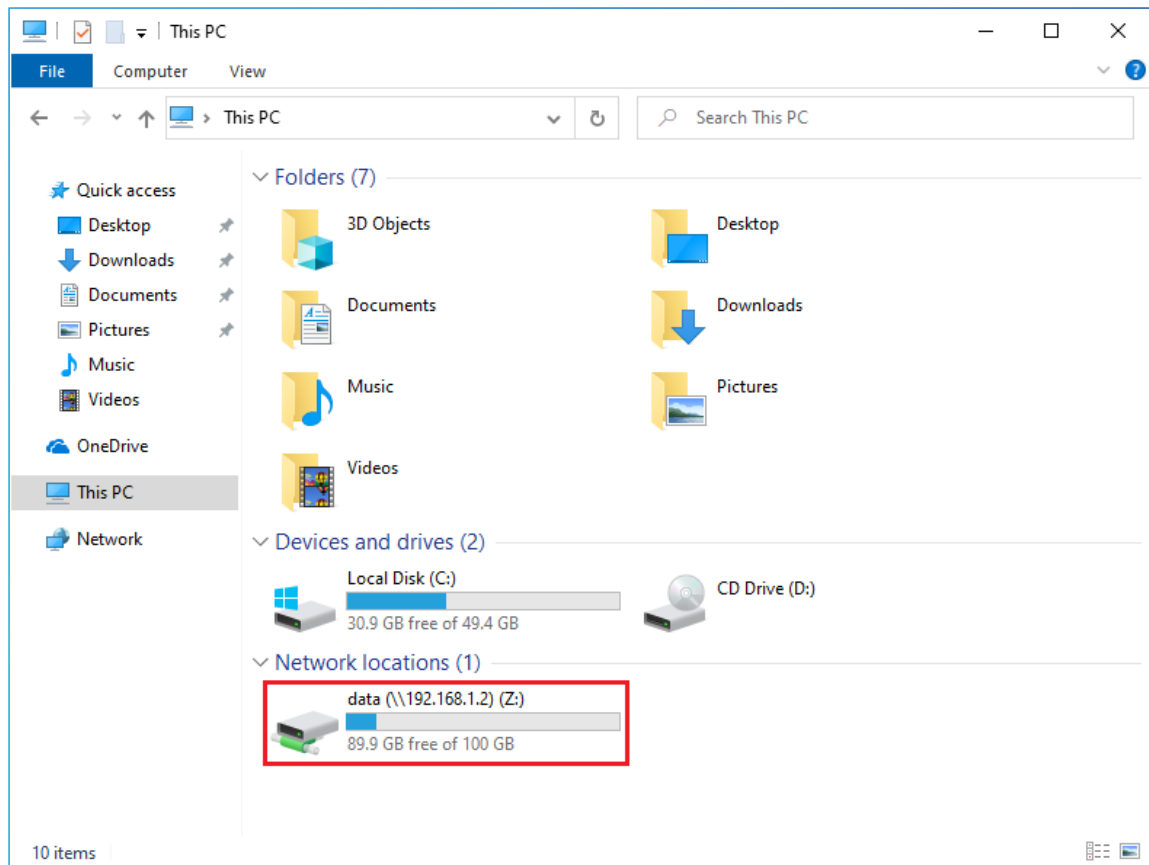
```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.

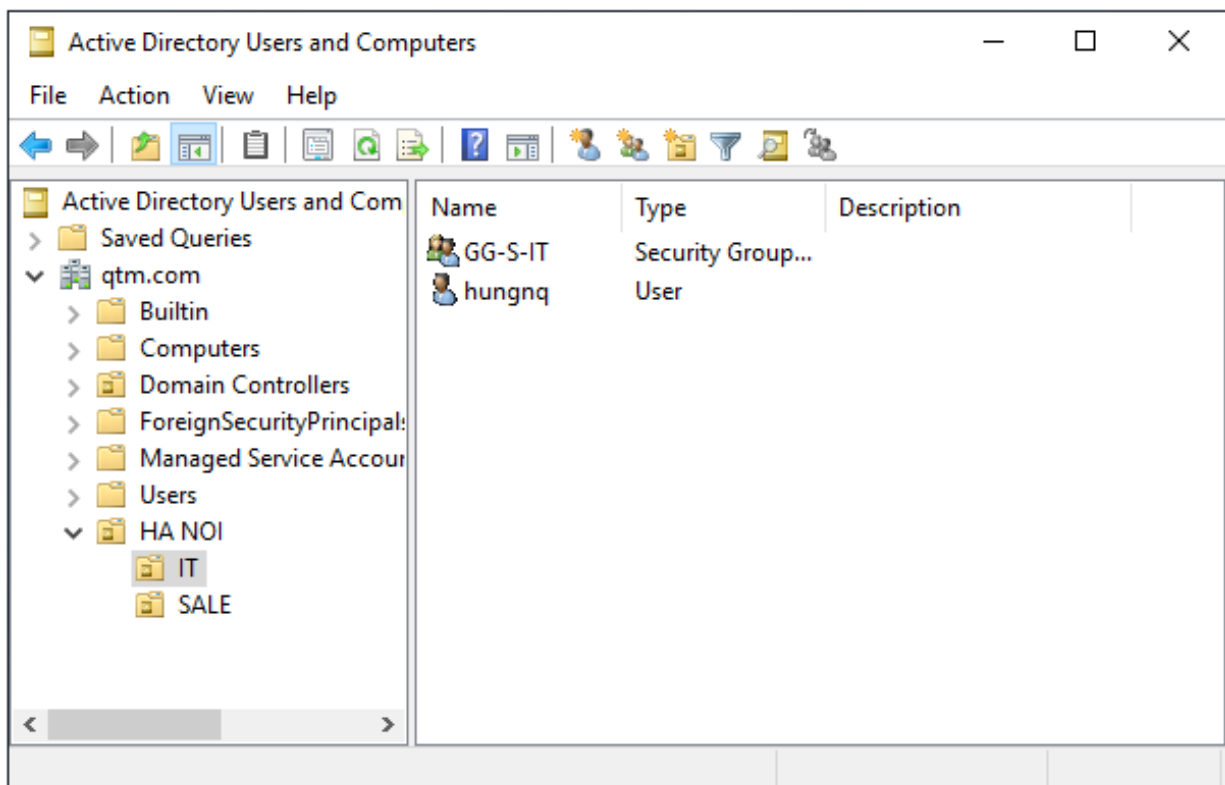
C:\Users\Administrator>
```

Bước 6. Thực hiện đăng nhập trên máy Client để kiểm tra.



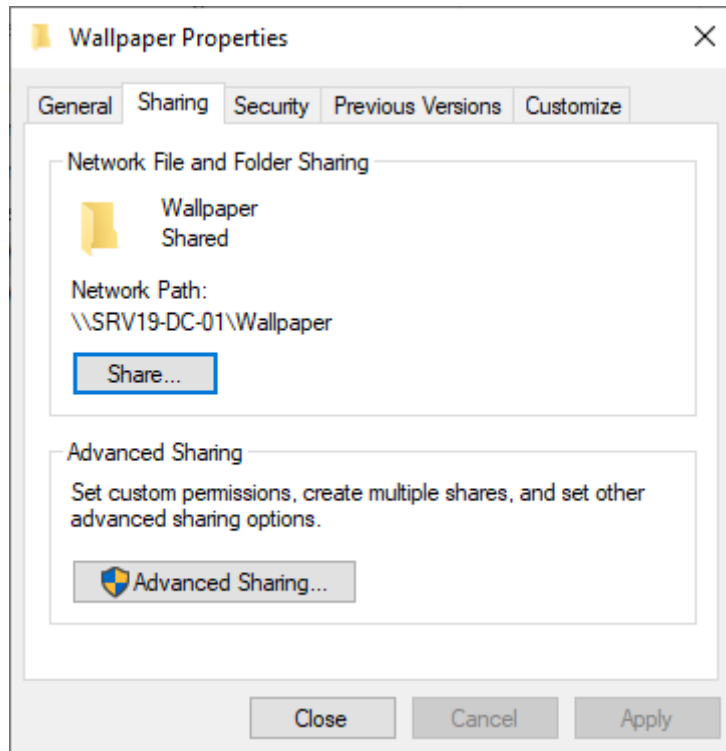
5.1.4. Triển khai chính sách áp dụng trên OU IT

Thực hiện trên máy SRV19-DC-01, tạo OU, group, user như yêu cầu, add user vào group.

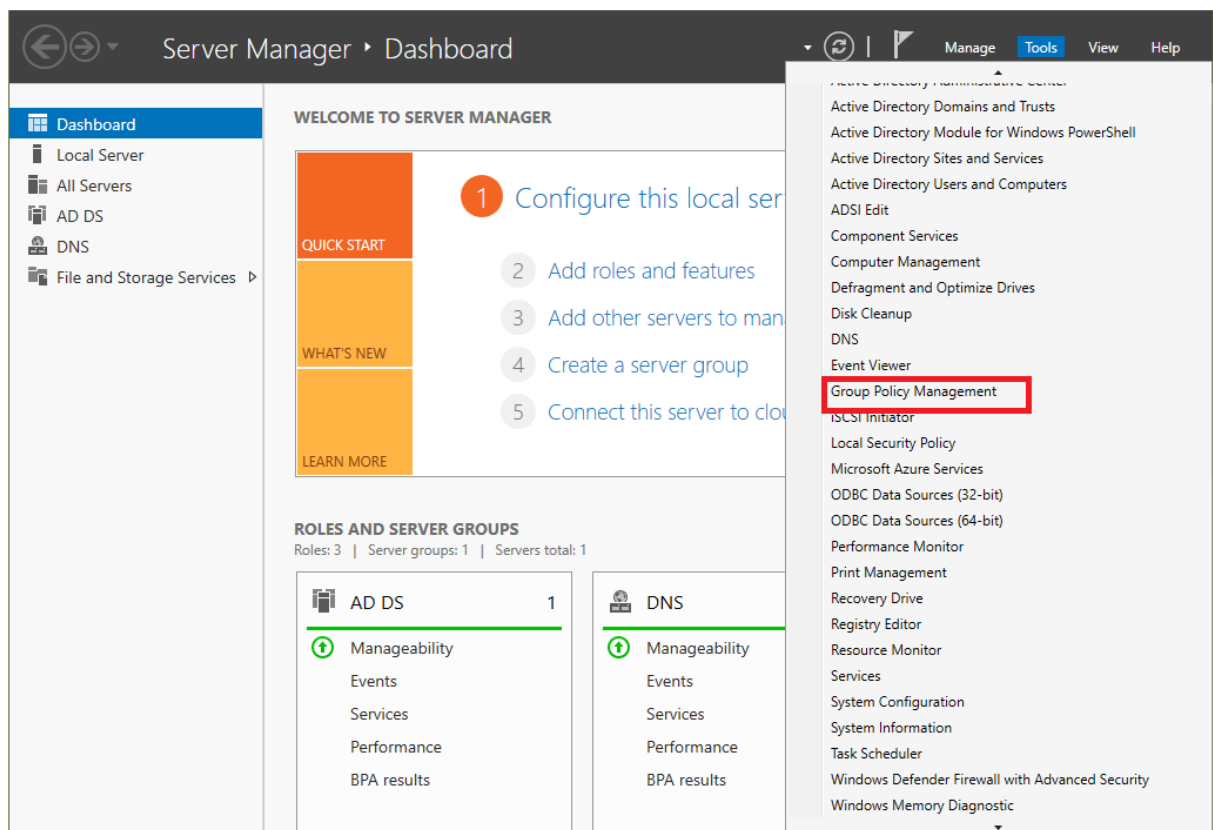


5.1.4.1. Chính sách “Đặt màn hình nền Desktop tất cả các máy tính”

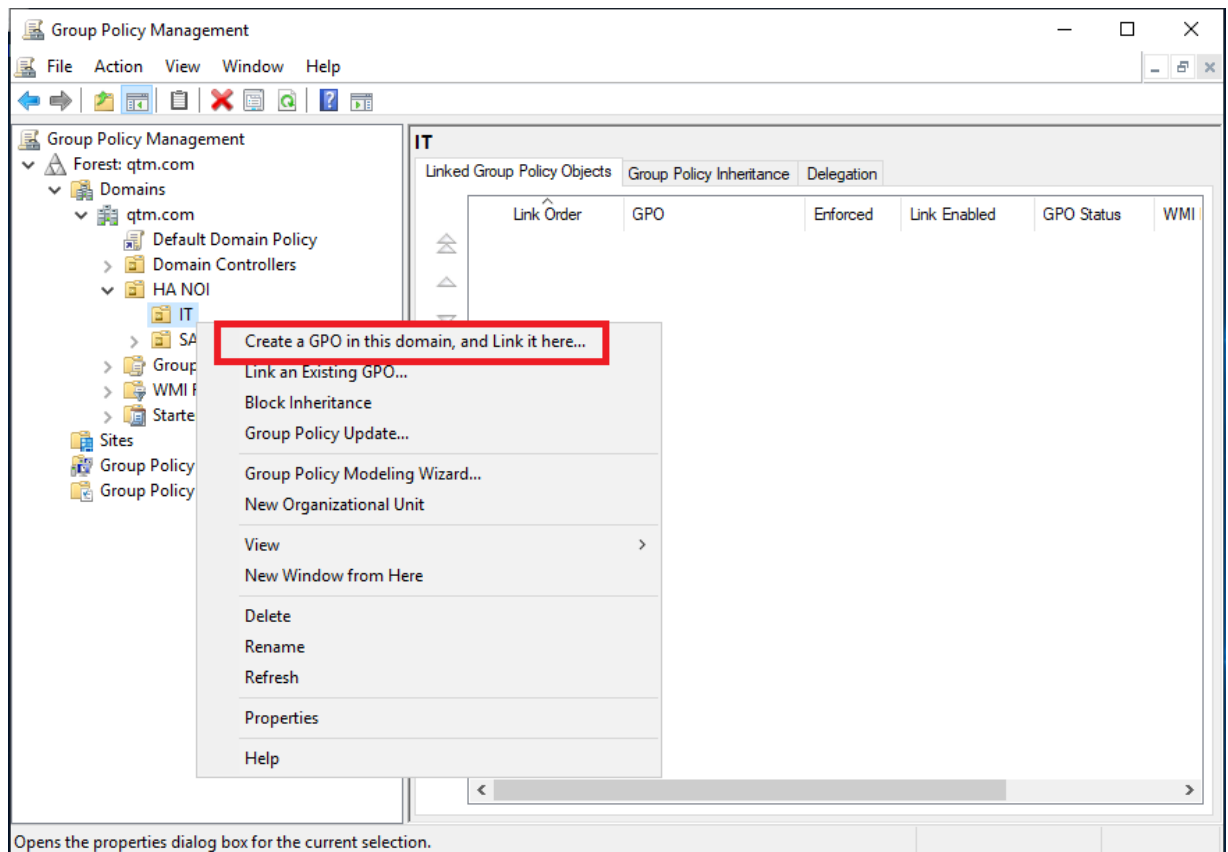
Bước 1. Tạo thư mục wallpaper trong ổ C (thư mục chứa background màn hình nền), tiến hành chia sẻ thư mục.



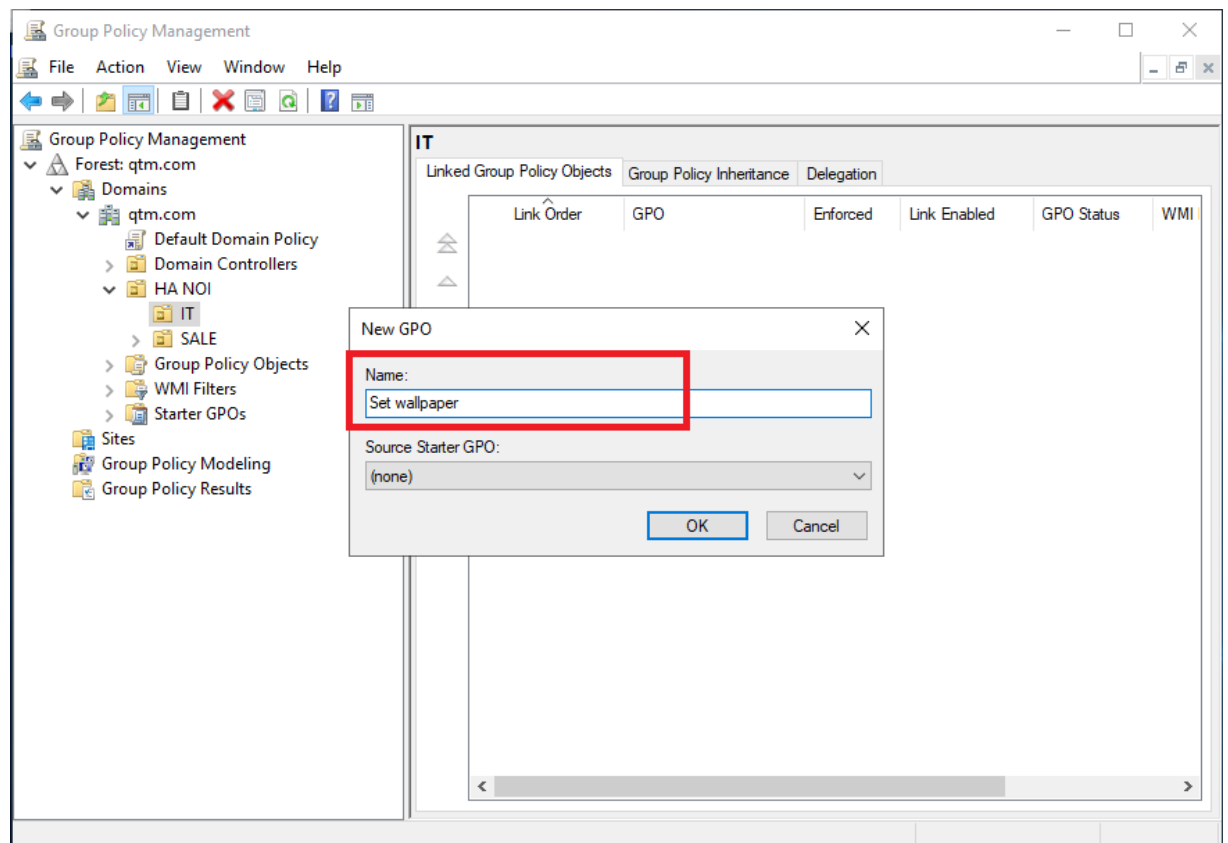
Bước 2. Cấu hình GPO trên máy **SRV19-DC-01**. Tạo các chính sách trên phòng ban **IT**. Vào **Server Manager / Tools / Group Policy Management**.



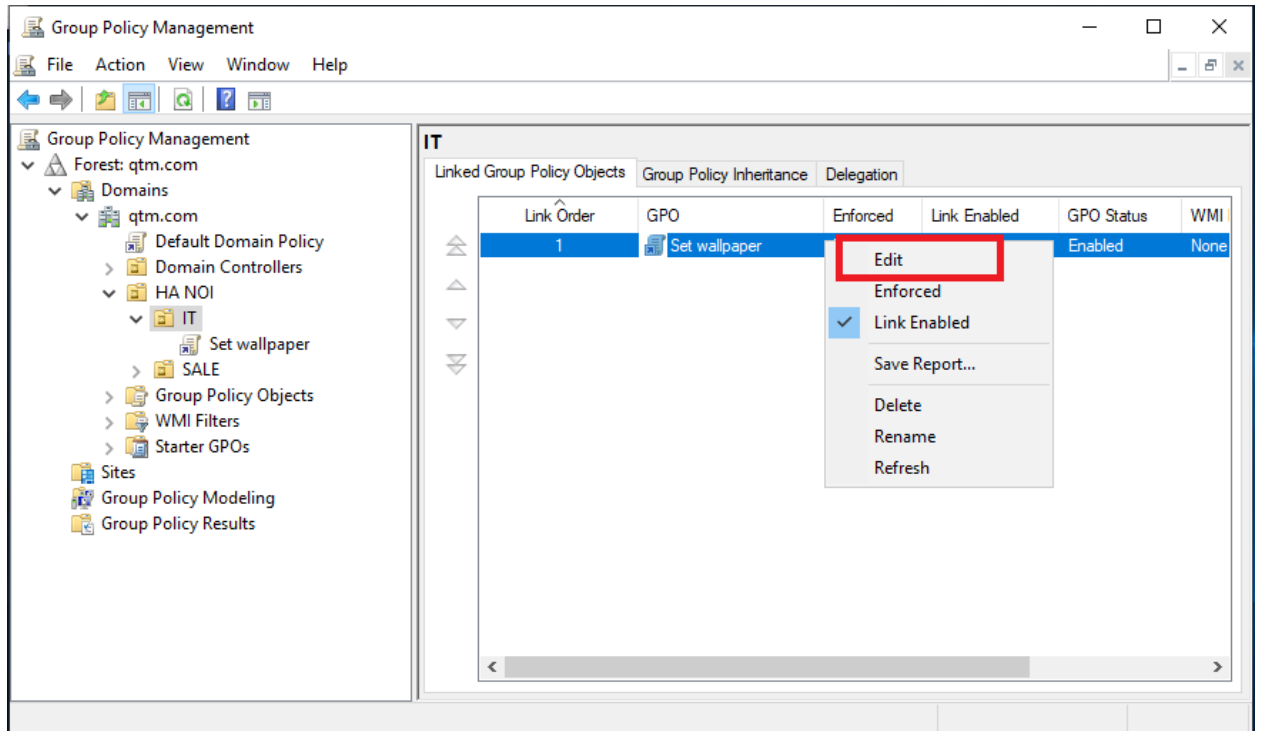
Bước 3. Tại cửa sổ **Group Policy Management**, click chuột phải vào **OU IT**, chọn **Create a GPO in this domain, and Link it here...**



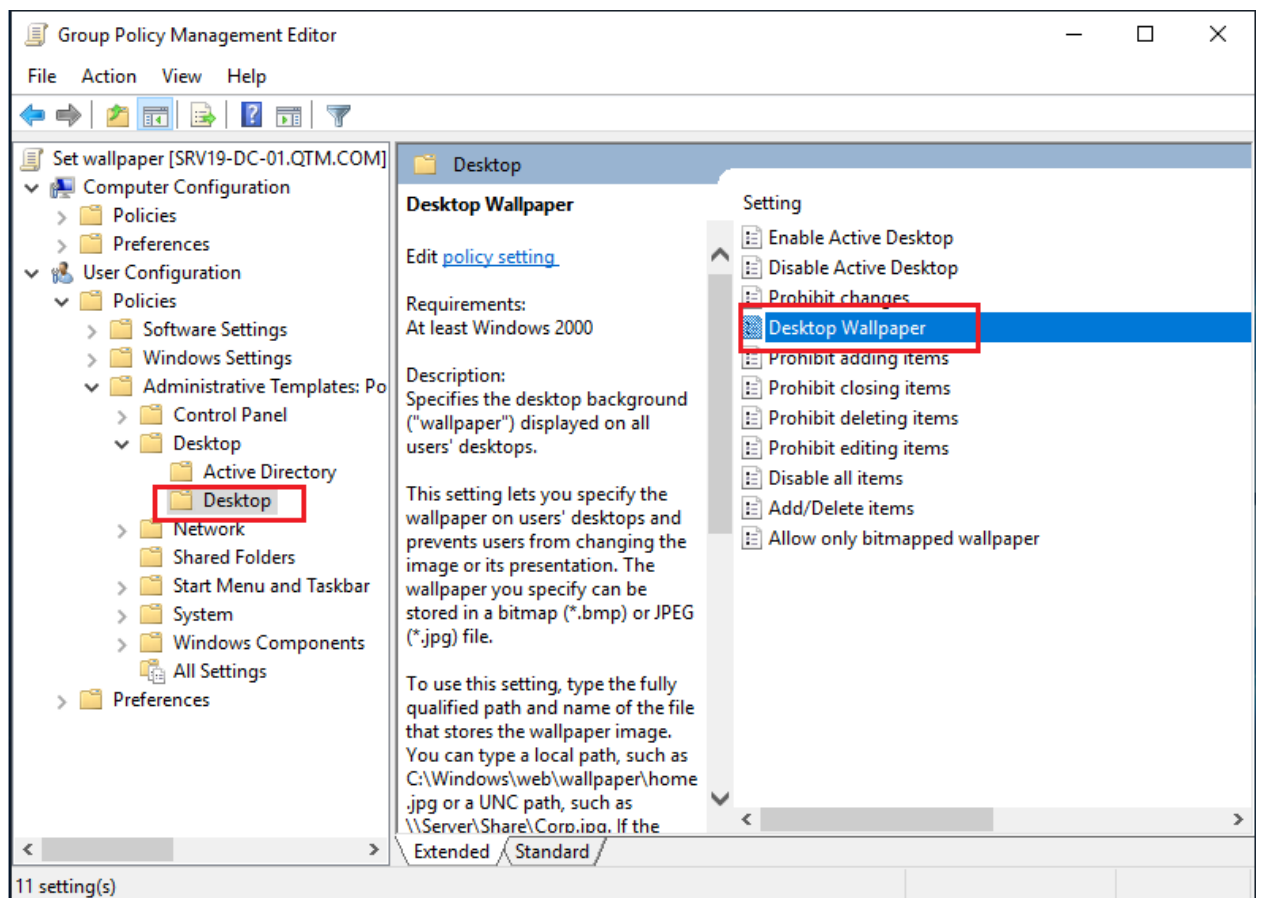
Bước 4. Tại cửa sổ **New GPO**, nhập vào mục Name: *Set wallpaper*, sau đó chọn **OK**.



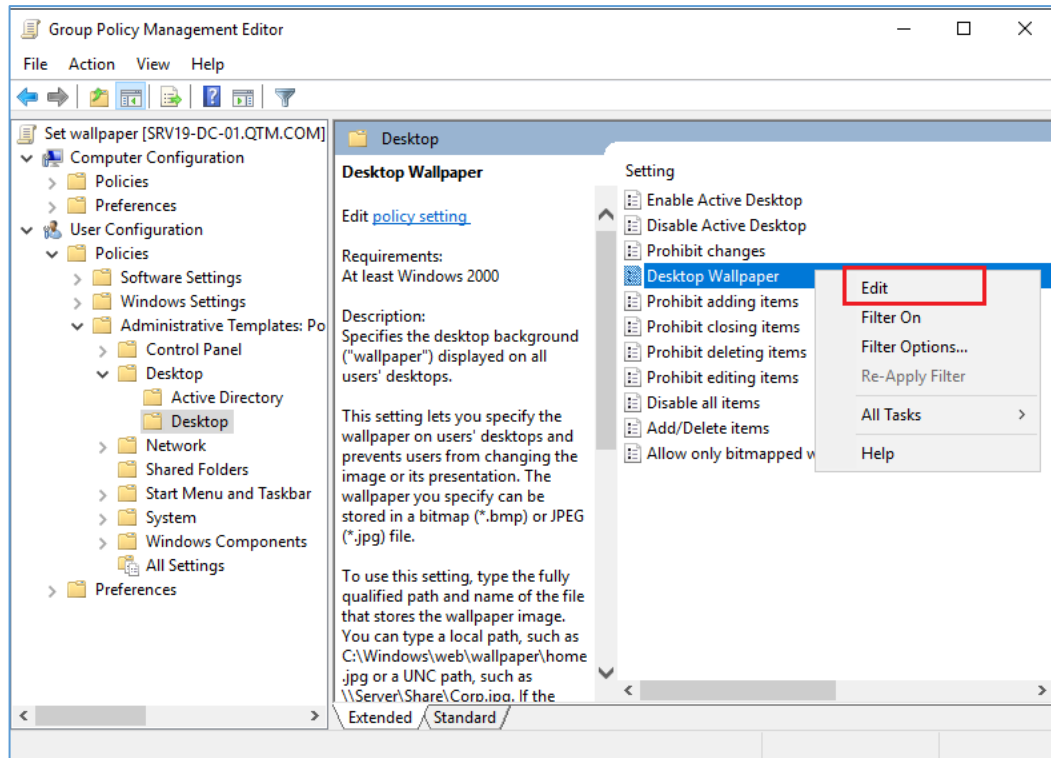
Bước 5. Click chuột phải tại chính sách **Set wallpaper** vừa tạo, chọn **Edit**.



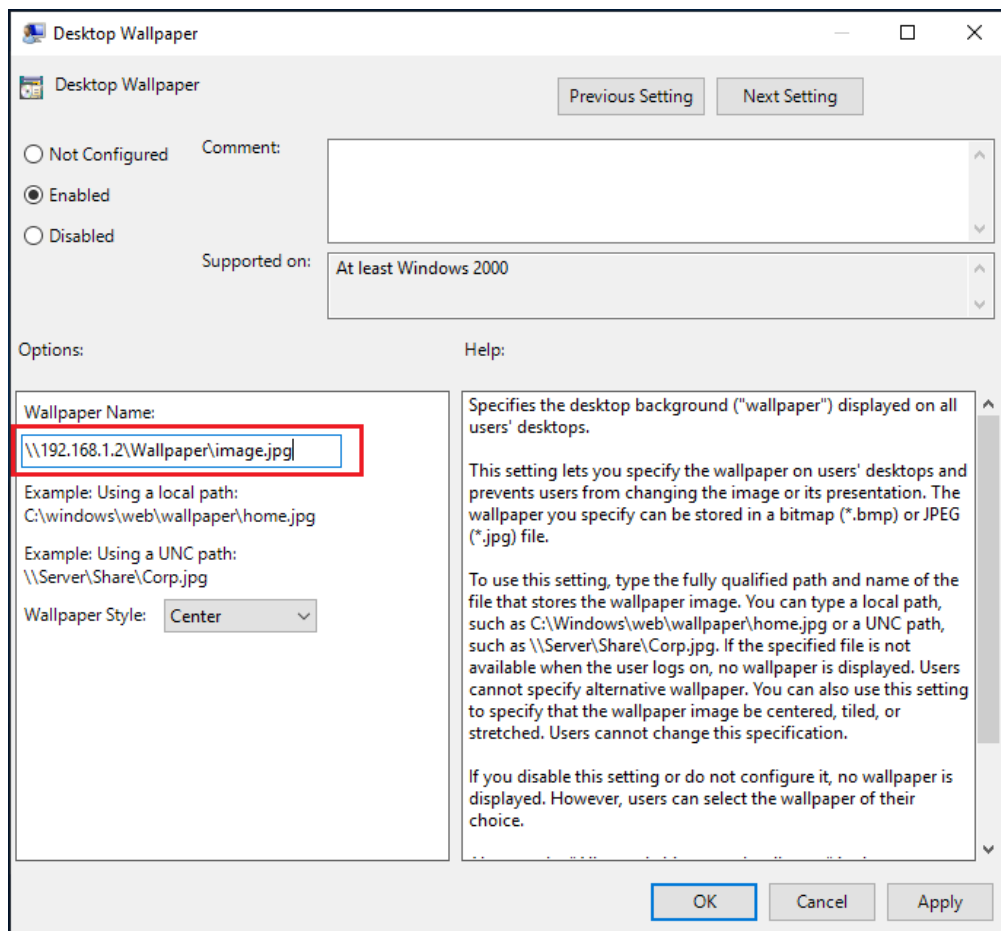
Bước 6. Tại cửa sổ **Group Policy Management Editor**, click chọn **User Configuration** / **Policies** / **Administrative Template...** / **Desktop** / **Desktop**. Chọn vào **Desktop Wallpaper**.



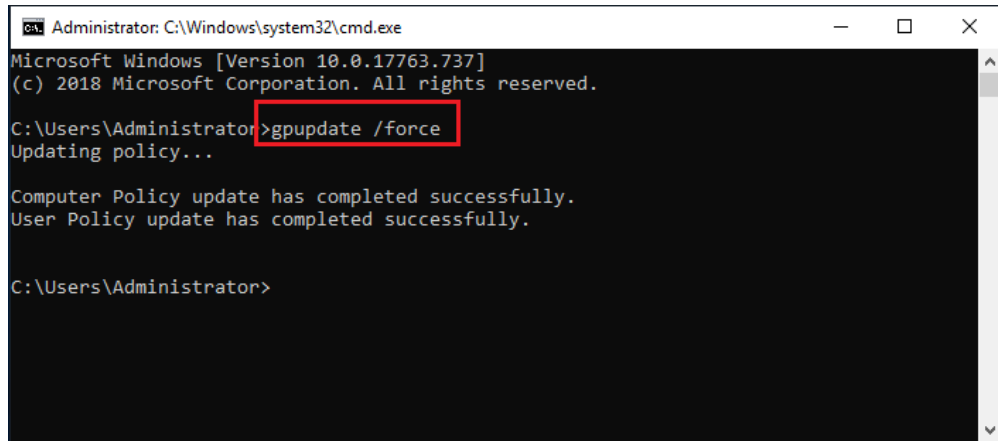
Bước 7. Click vào **Desktop Wallpaper**, chọn **Edit**.



Bước 8. Tại cửa sổ **Desktop Wallpaper**, click vào **Enable**. Tại **Wallpaper Name**: đưa vào đường dẫn folder wallpaper vừa share ở trên là: [\\192.168.1.2\wallpaper\image.jpg](http://192.168.1.2/wallpaper/image.jpg)



Bước 9. Cập nhật GPO, vào Cmd / gõ lệnh *gpupdate /force*



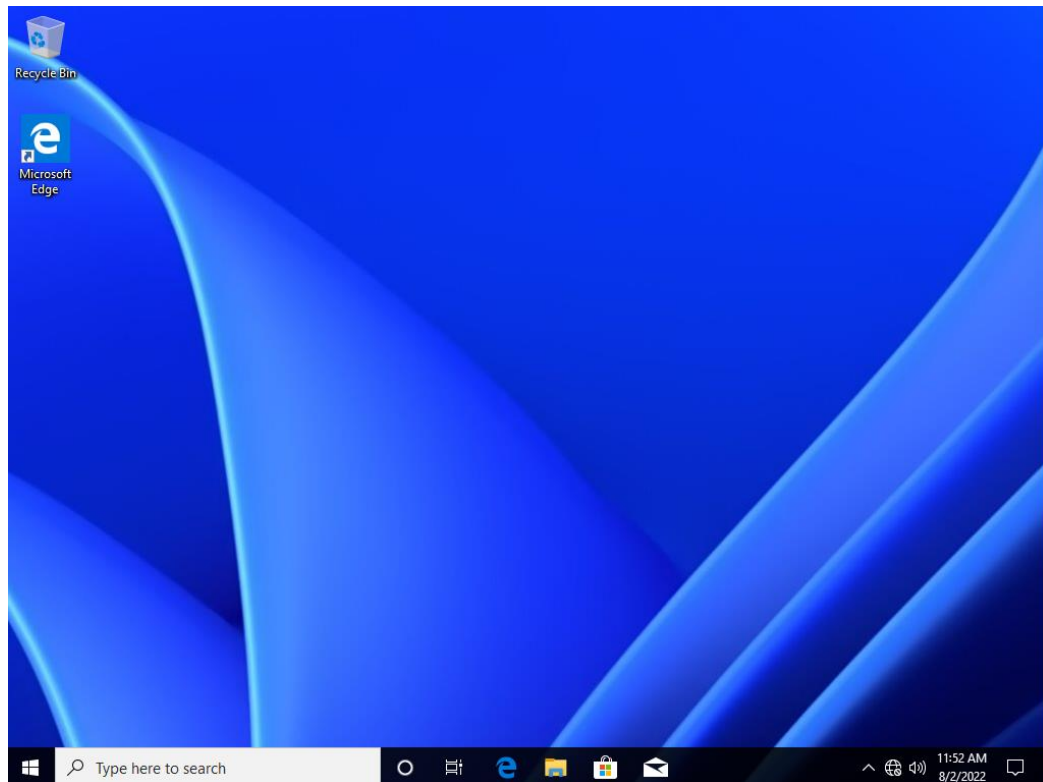
```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.

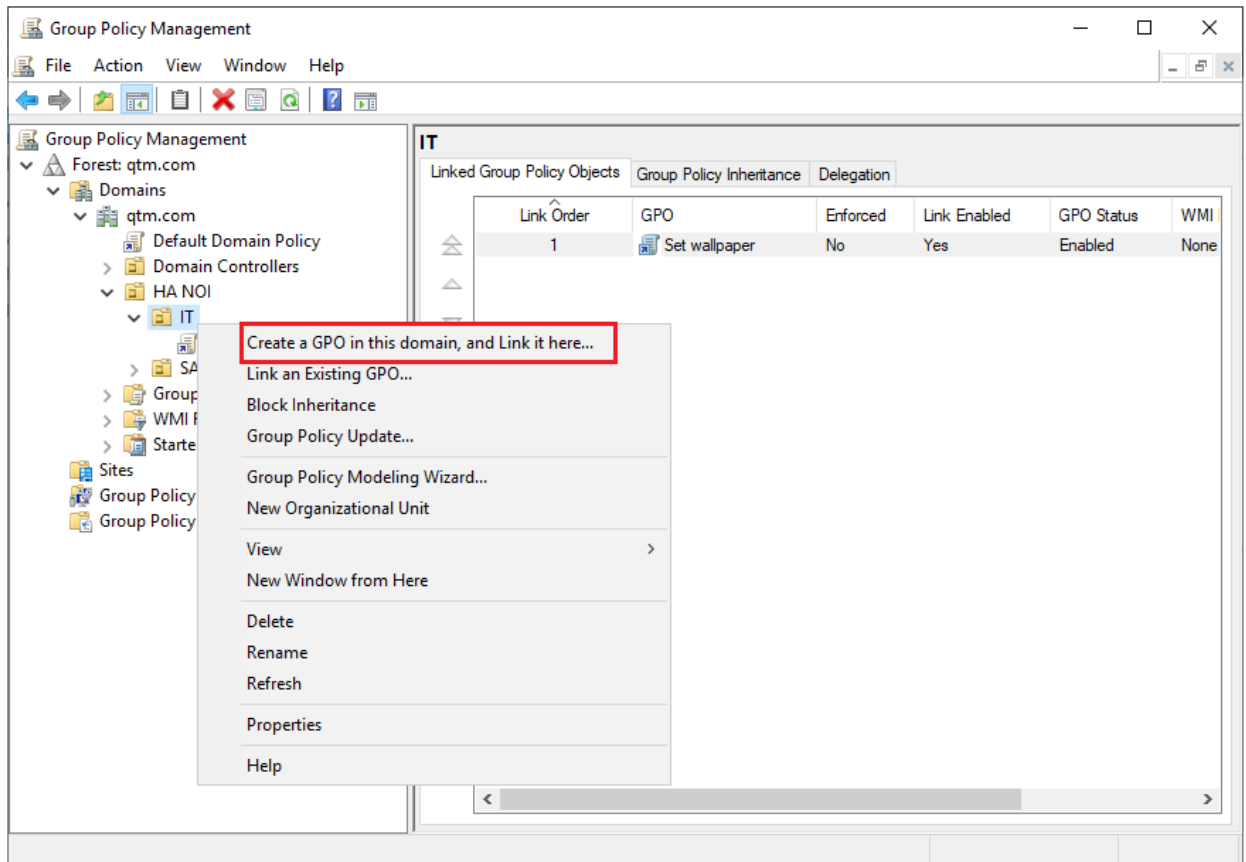
C:\Users\Administrator>
```

Bước 10. Chuyển sang máy **Client01**, đăng nhập bằng tài khoản *hungnq* trong phòng ban IT kiểm tra thấy màn hình máy client đã cập nhật hình nền thành công.

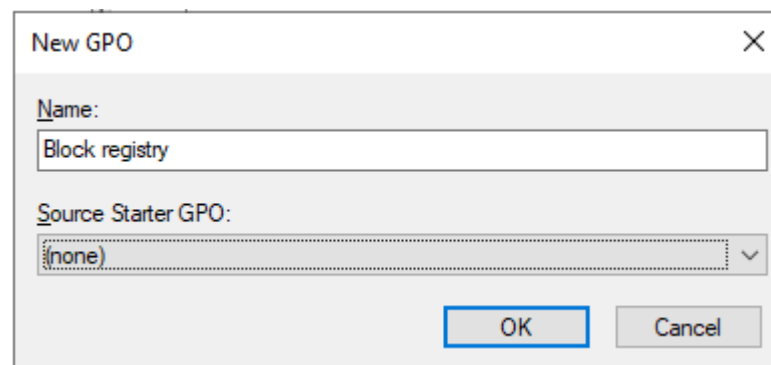


5.1.4.2. Chính sách “Khóa Registry”

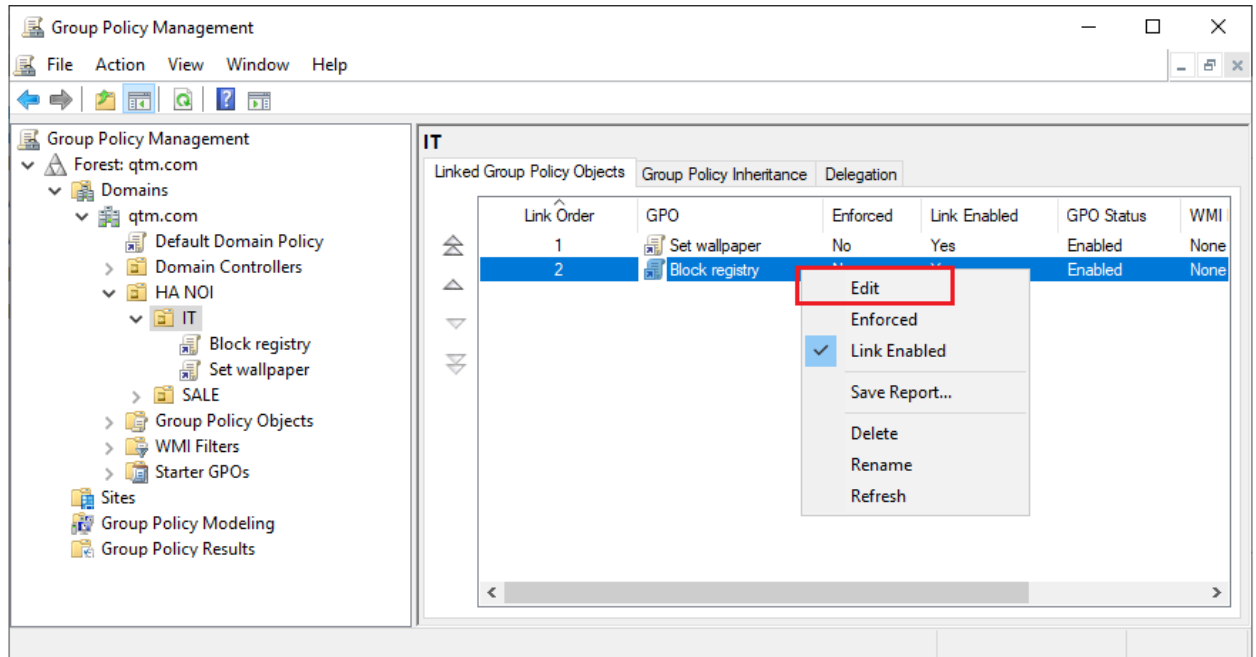
Bước 1. Trên máy **SRV19-DC-01**, tạo chính sách **Block Registry**. Click chuột phải tại OU **IT**, chọn **Create a GPO in this domain, and link it here...**



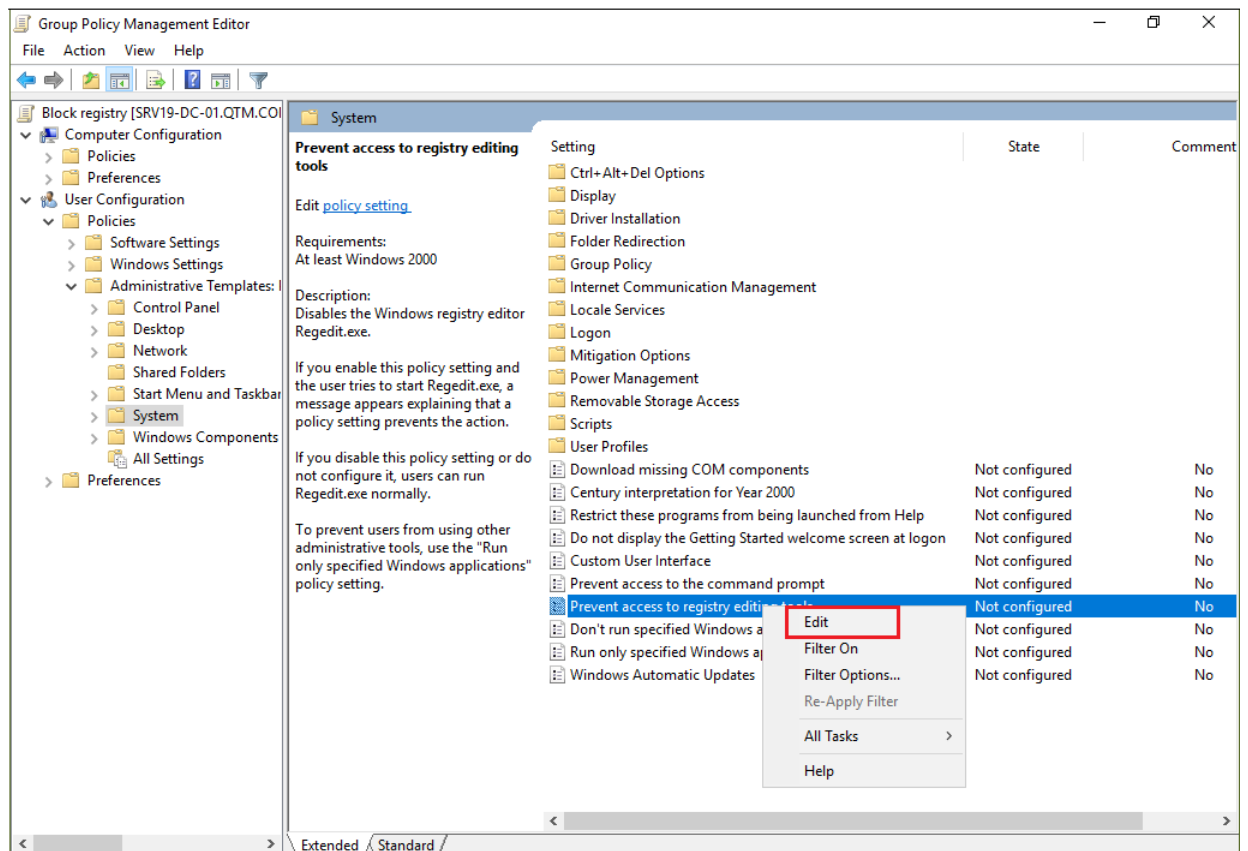
Bước 2. Tại cửa sổ **New GPO**, nhập vào tên **Name** là **Block registry**.



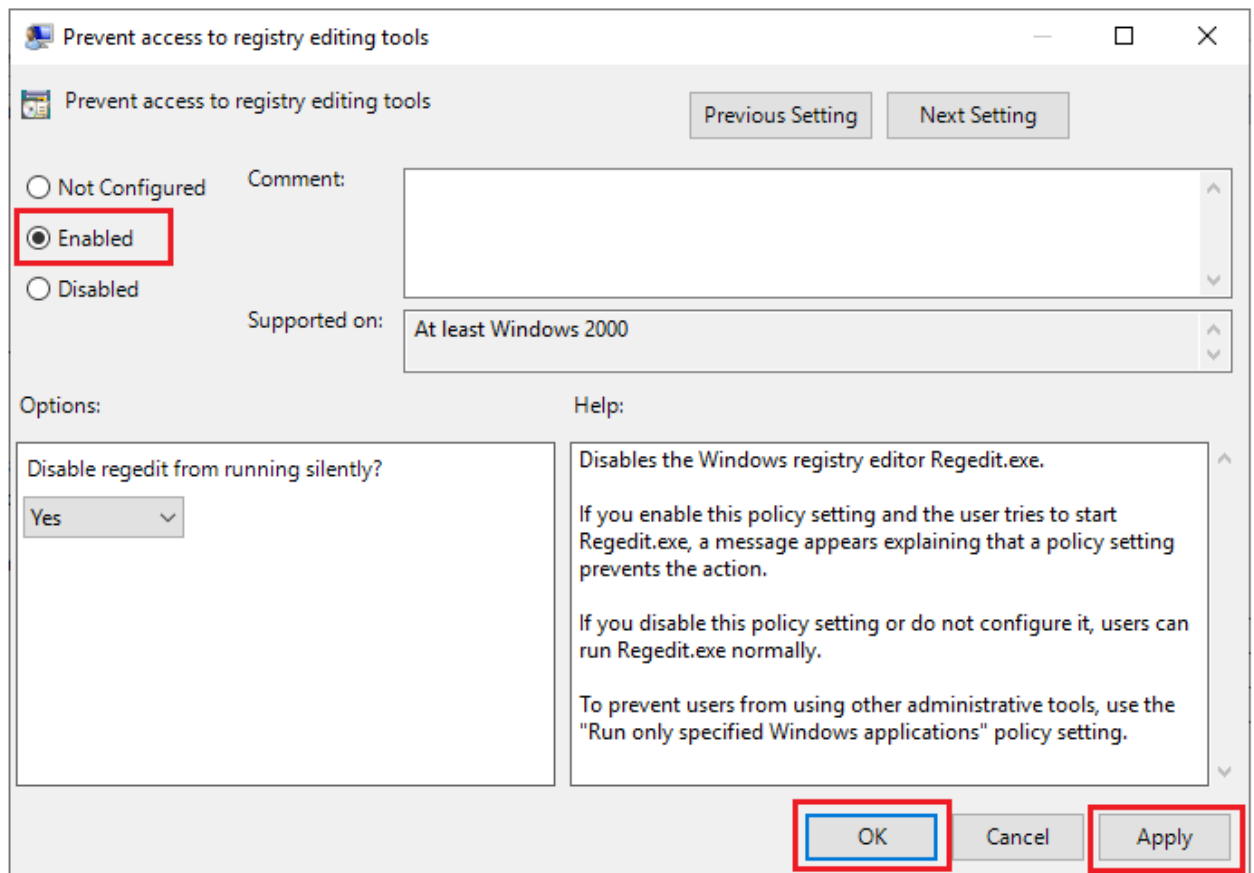
Bước 3. Click chuột phải vào chính sách **Block Registry** vừa tạo, chọn **Edit**.



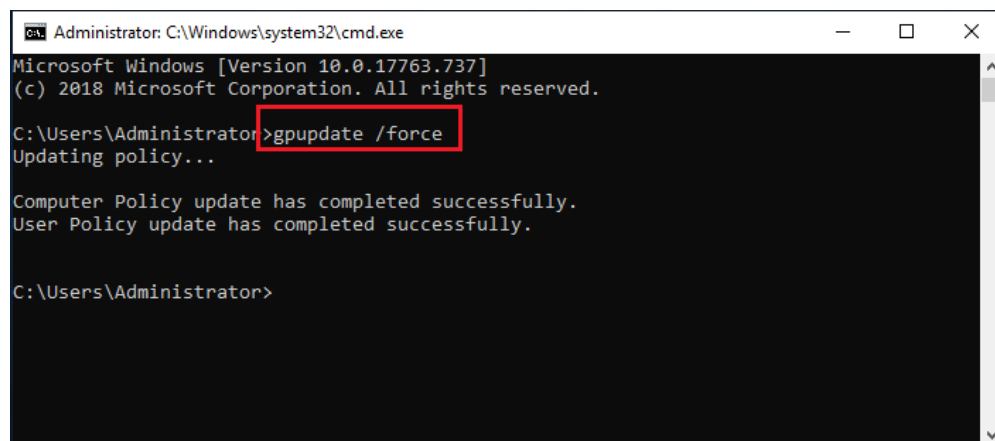
Bước 4. Tại cửa sổ **Group Policy Management Editor**, chọn vào mục **User Configuration / Policies / Administrative Templates... / System**, chọn vào chính sách **Prevent access to registry editing tools**, tại đây click chuột phải chọn **Edit**.



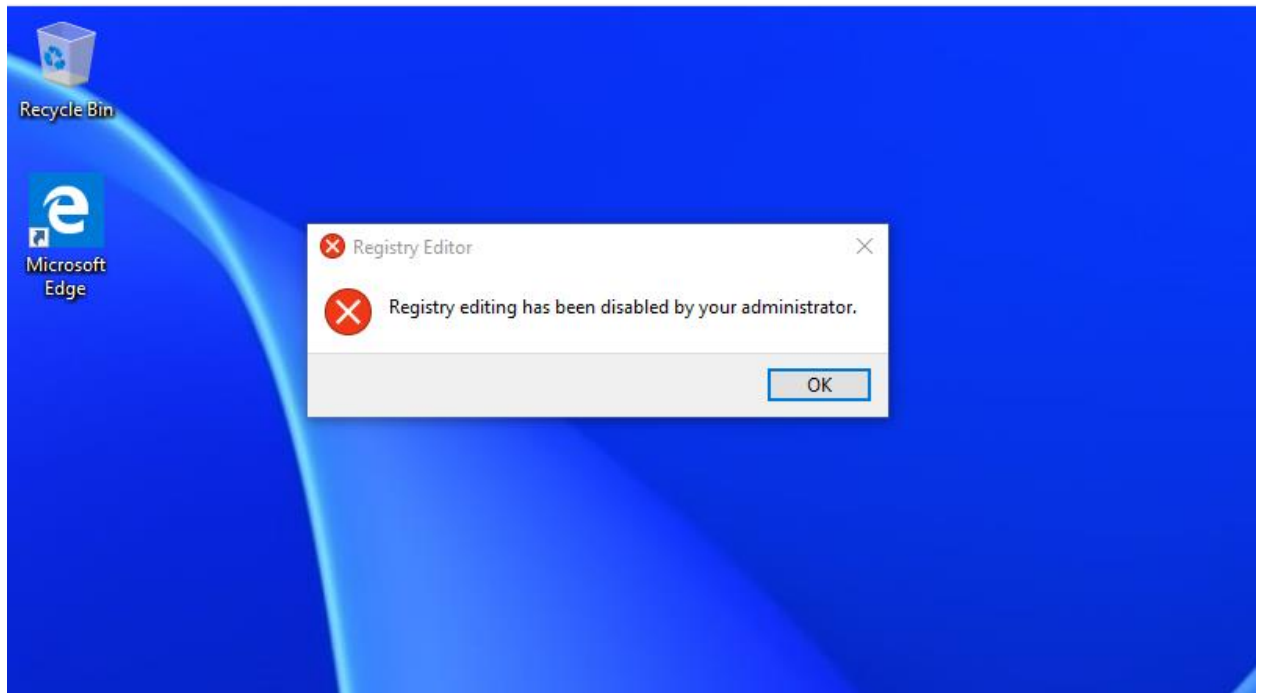
Bước 5. Tại cửa sổ **Prevent access to registry editing tools**, click chọn vào **Enable**, chọn **Apply**, chọn **OK**.



Bước 6. Cập nhật chính sách bằng lệnh *gpupdate /force* trong cmd.



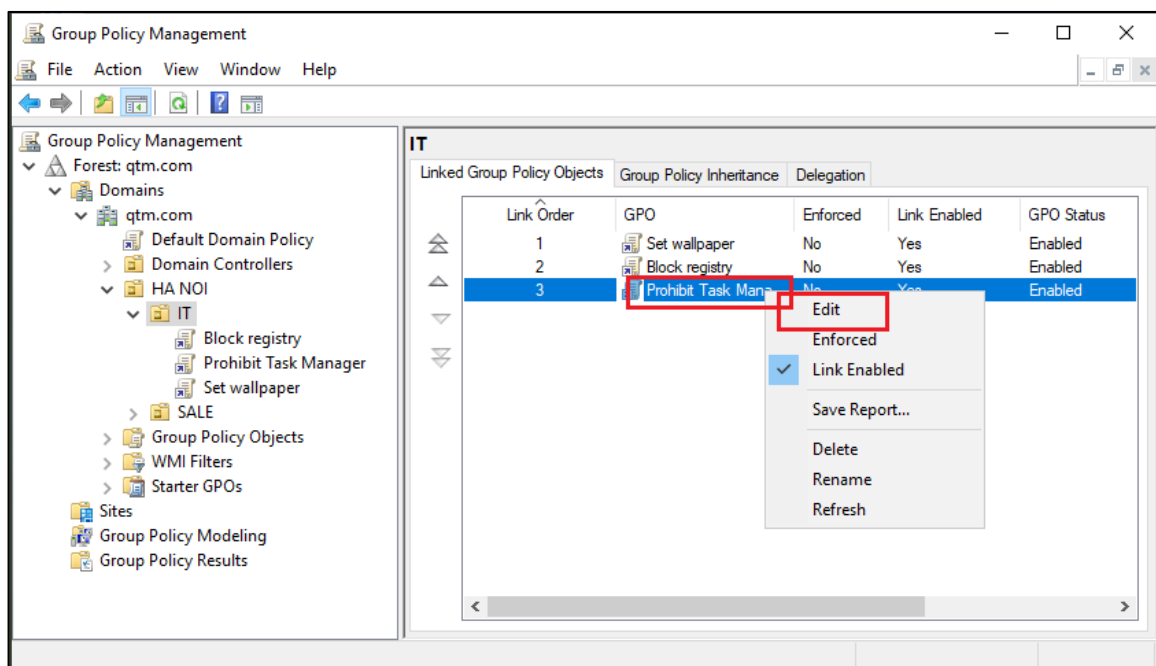
Bước 7. Chuyển sang máy **Client01** đăng nhập bằng tài khoản **hungnq** trong phòng ban **IT** kiểm tra thấy **Registry Editor** đã bị khóa.



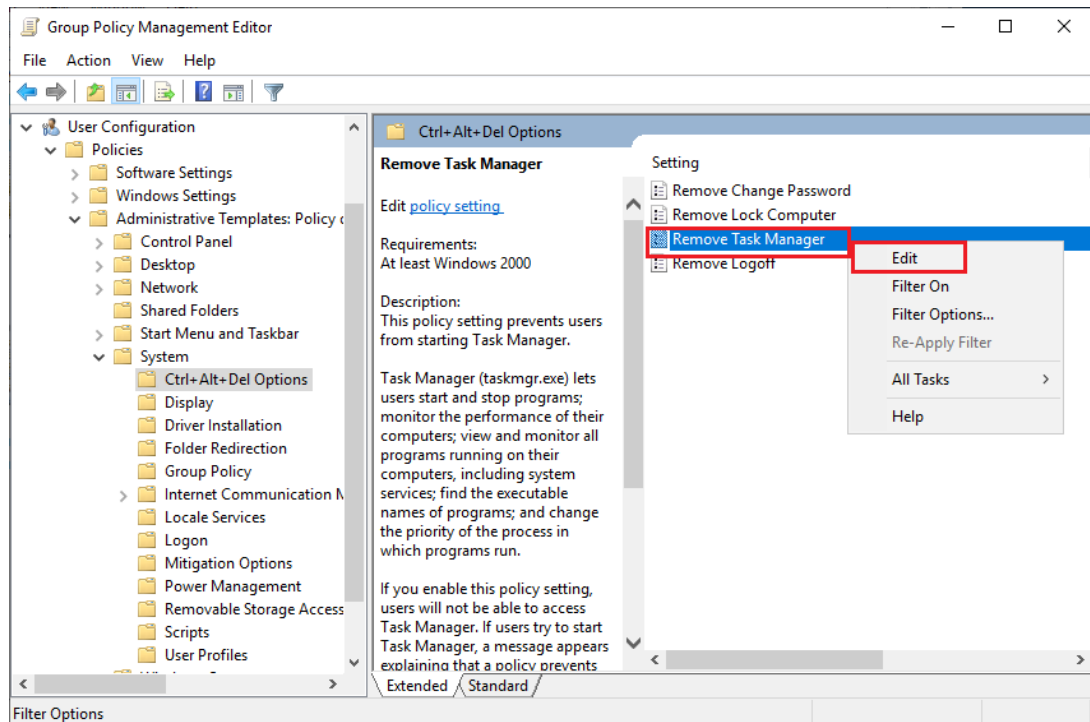
5.1.4.3. Chính sách “Khóa Task Manager”

Bước 1. Trên máy SRV19-DC-01, tạo thêm chính sách chặn **Task Manager**.

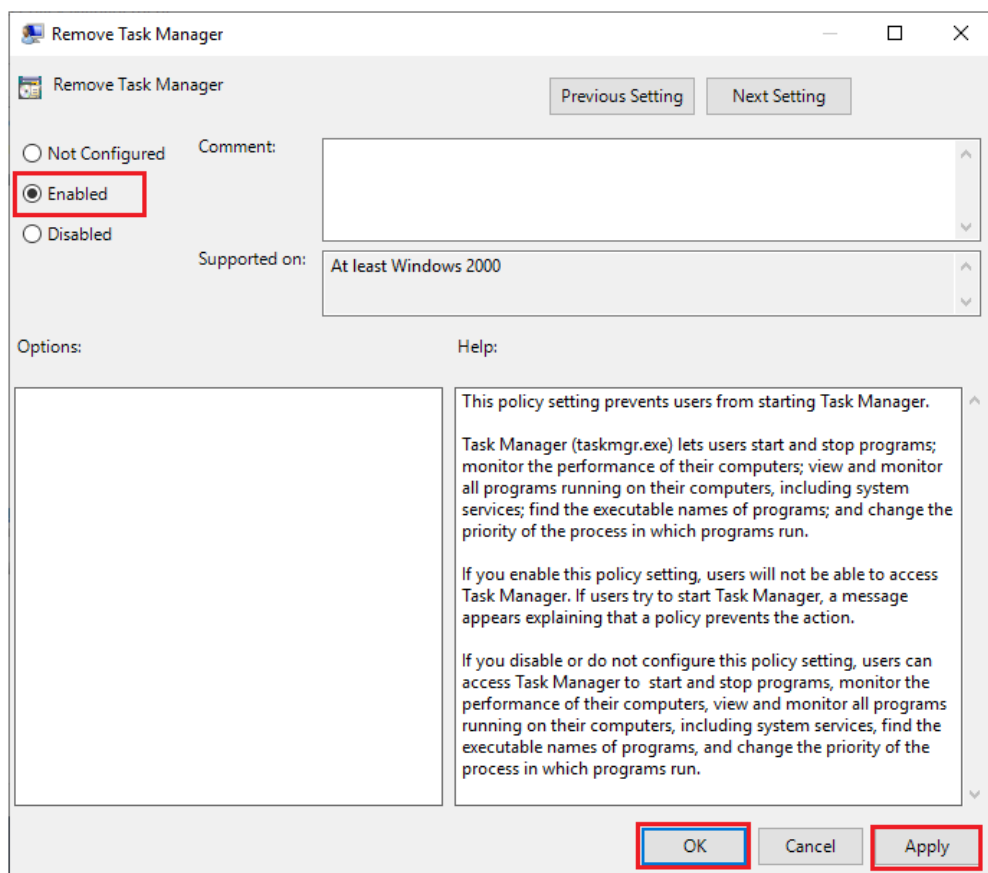
- Click chuột phải tại OU **IT**, chọn **Create a GPO in this domain...**
- Tại cửa sổ **New GPO**, nhập vào tên chính sách **Name** là **Prohibit Task Manager**.
- Click chuột phải vào chính sách vừa tạo, chọn **Edit**.



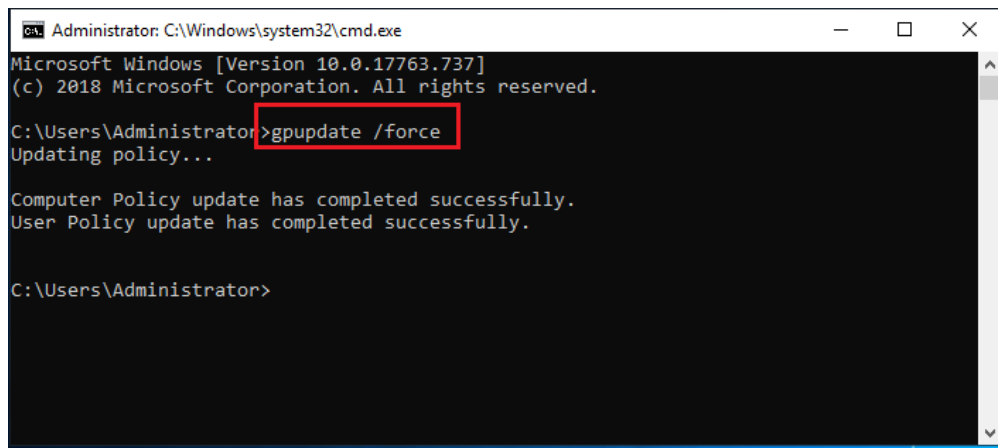
Bước 2. Tại cửa sổ **Group Policy Management Editor**, chọn vào **User Configuration / Policies / Administrative Template... / System / Ctrl+Alt+Del Options**. Chọn vào chính sách **Remove Task Manager**, tại đây click chuột phải chọn **Edit**.



Bước 3. Tại cửa sổ **Remove Task Manager**, click vào **Enabled**, chọn **Apply**, chọn **OK**.



Bước 4. Cập nhật chính sách bằng lệnh **gpupdate /force** trong **cmd**.



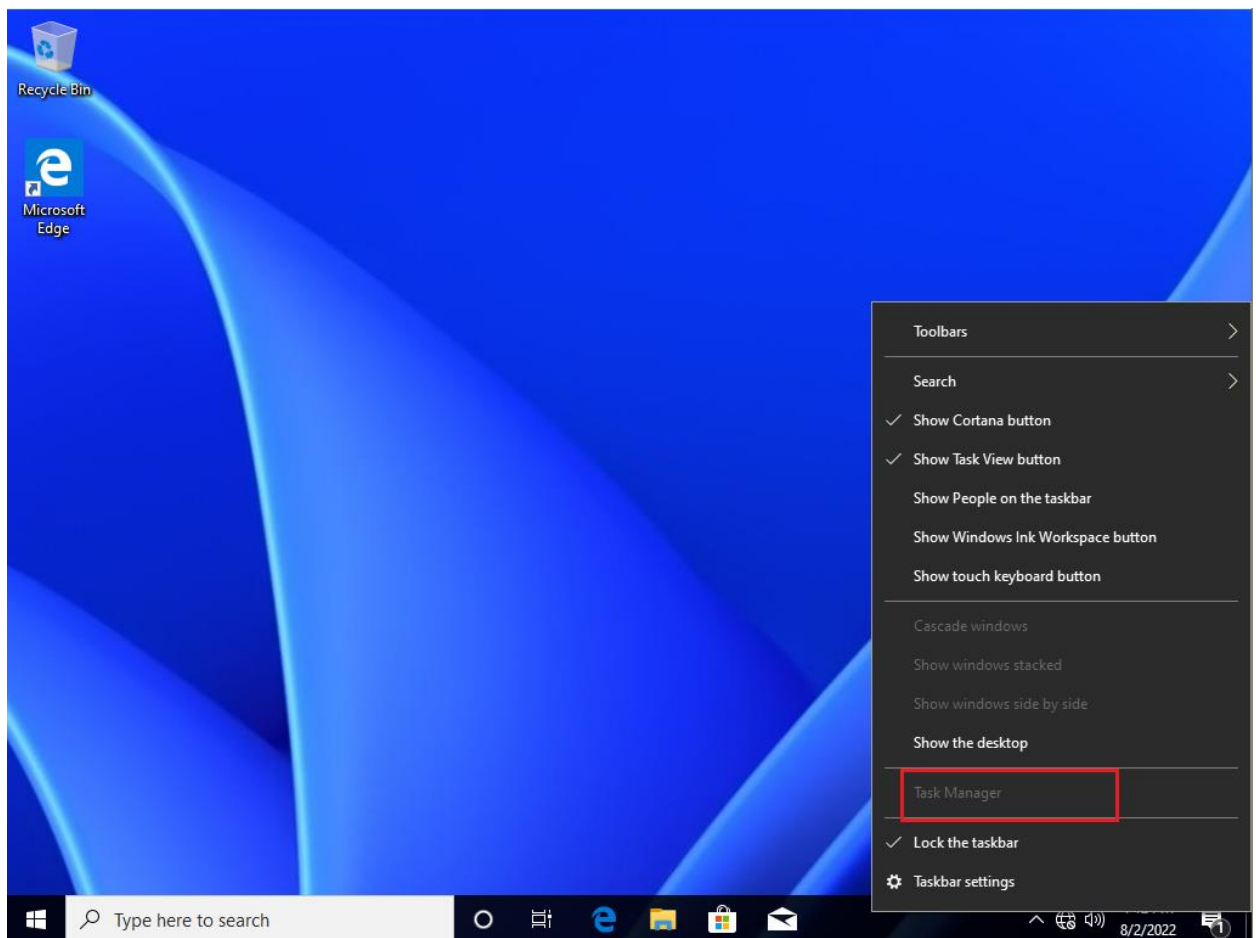
```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.

C:\Users\Administrator>
```

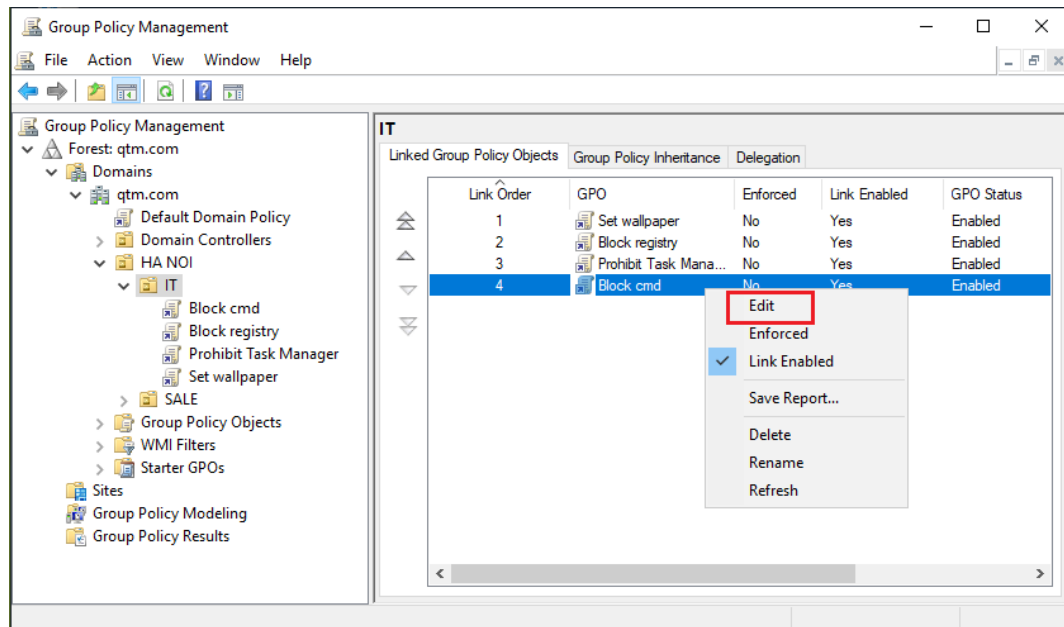
Bước 5. Chuyển sang máy **Client01** đăng nhập bằng tài khoản **hungnq** trong phòng ban IT kiểm tra thấy **Task Manager** đã bị khóa.



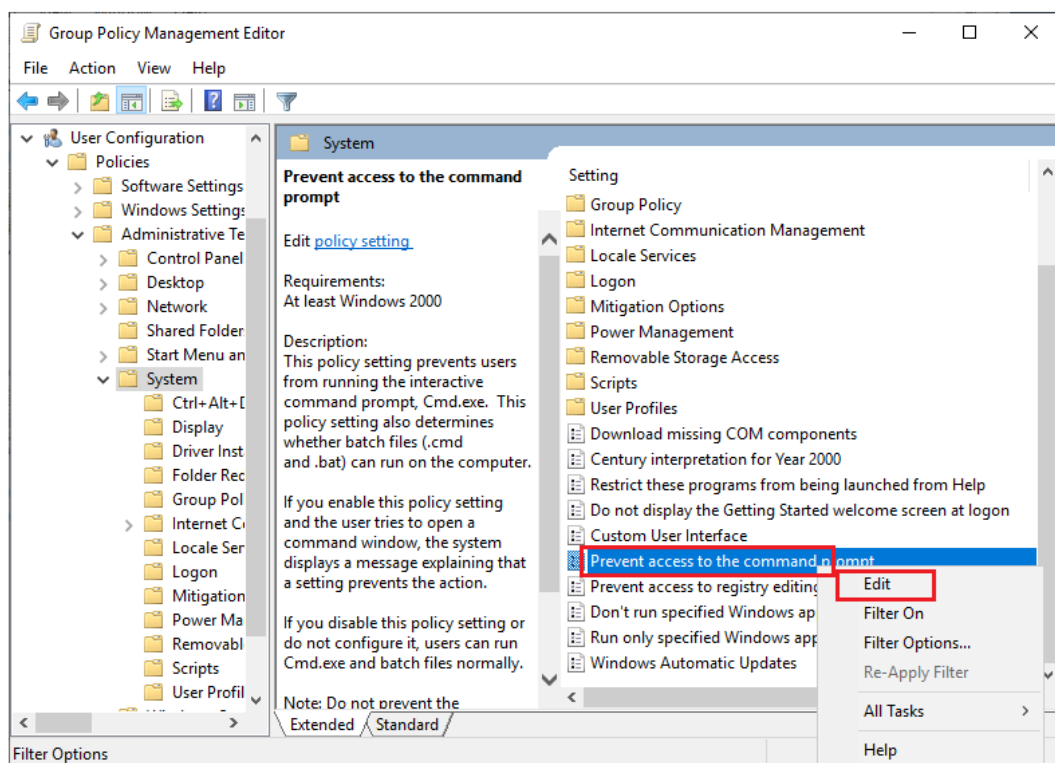
5.1.4.4. Chính sách “Cấm DOS Command”

Bước 1. Trên máy SRV19-DC-01, tạo thêm chính sách chặn **Block cmd**.

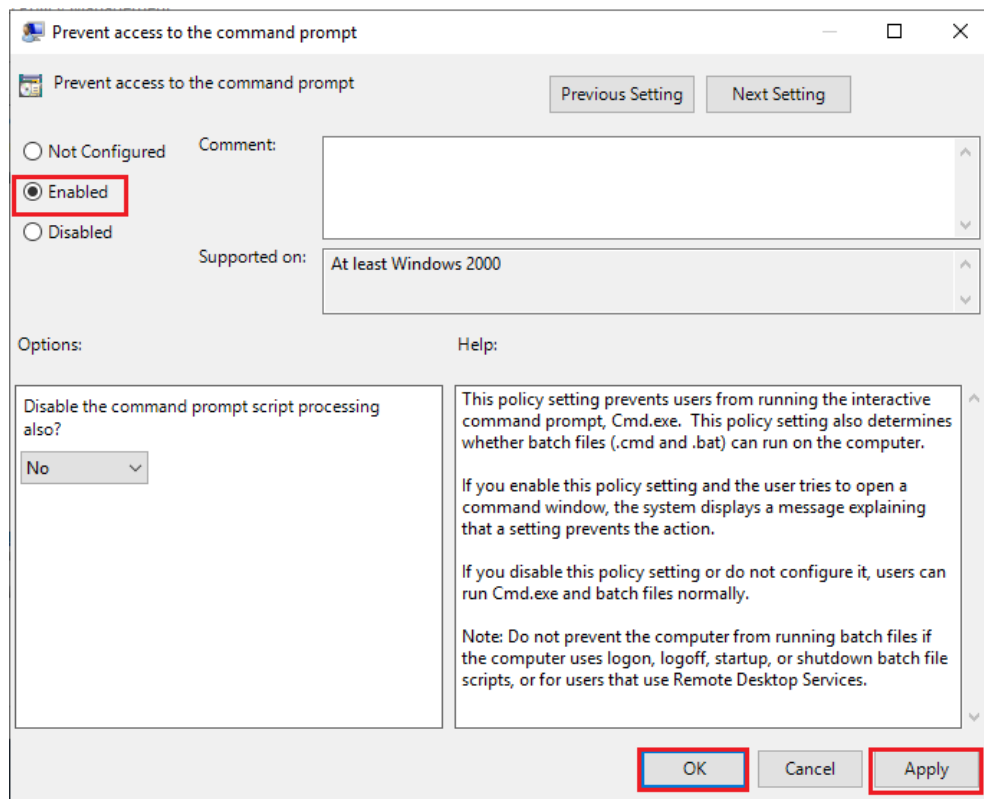
- Click chuột phải tại OU **IT**, chọn **Create a GPO in this domain...**
- Tại cửa sổ **New GPO**, nhập vào tên chính sách **Name** là **Block cmd**.
- Click chuột phải vào chính sách vừa tạo, chọn **Edit**.



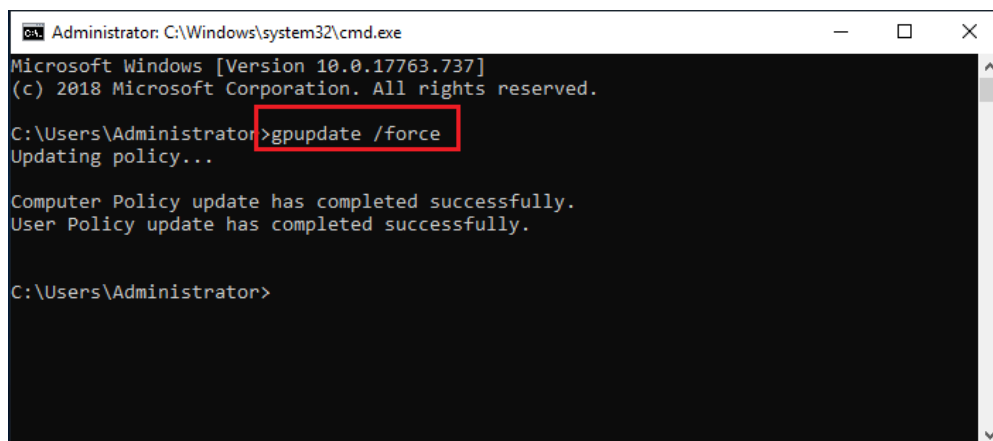
Bước 2. Group Policy Management Editor, chọn vào **User Configuration / Policies / Administrative Template... / System**, chọn vào chính sách **Prevent access to the command prompt**. Tại chính sách này, click chuột phải chọn **Edit**.



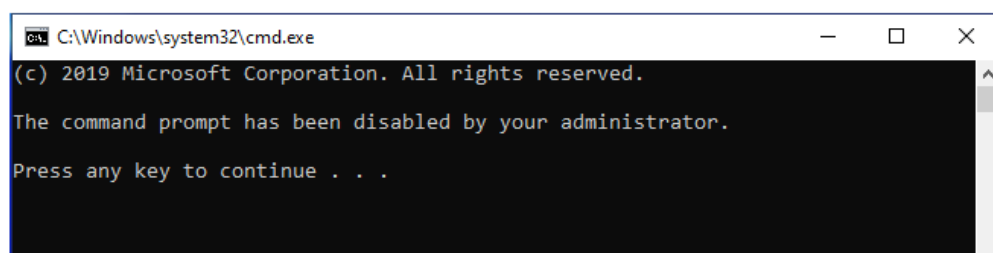
Bước 3. Tại cửa sổ **Prevent access to the command prompt**, click vào **Enable**, chọn **Apply**, chọn **OK**.



Bước 4. Cập nhật chính sách bằng lệnh *gpupdate /force* trong **cmd**.



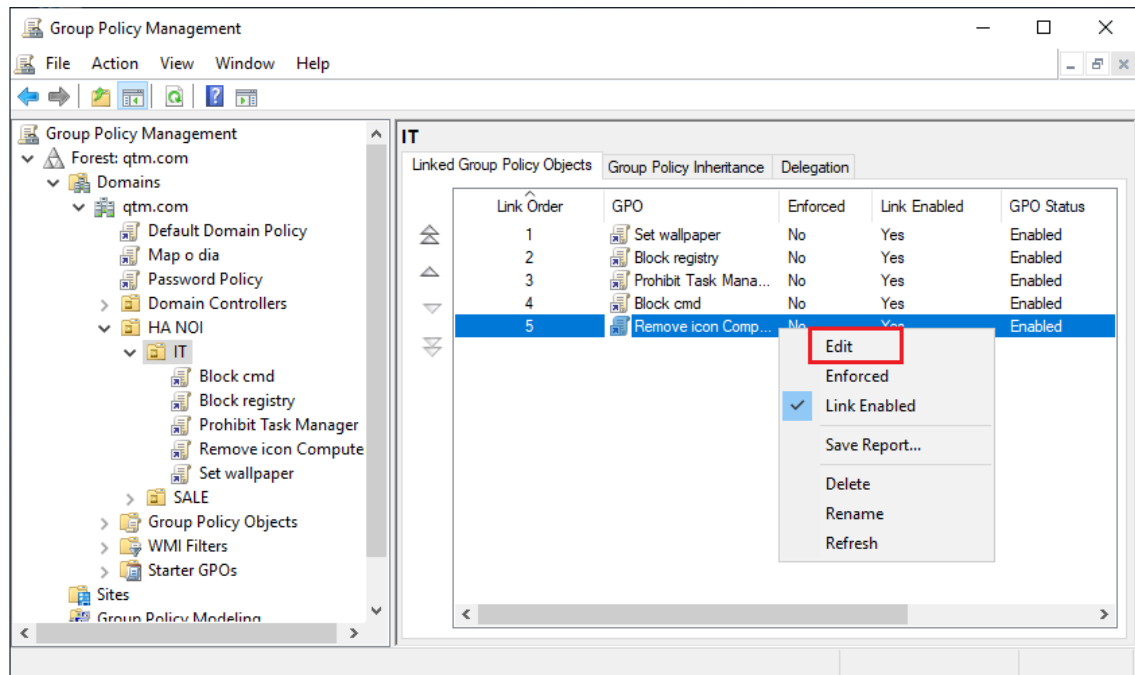
Bước 5. Chuyển sang máy **Client01** đăng nhập bằng tài khoản **hungnq** trong phòng ban **IT** kiểm tra thấy **cmd** đã bị khóa.



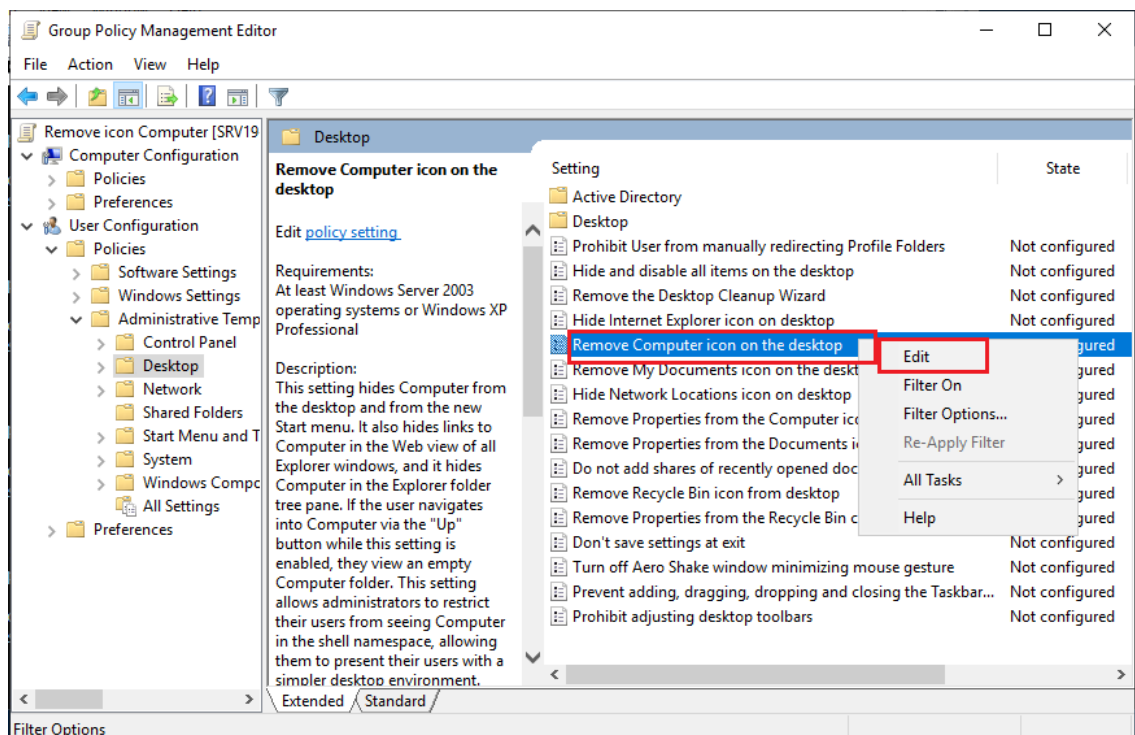
5.1.4.5. Chính sách “Xóa icon Copumter trên Desktop”

Bước 1. Trên máy SRV19-DC-01, tạo thêm chính sách chặn **Remove icon Computer**.

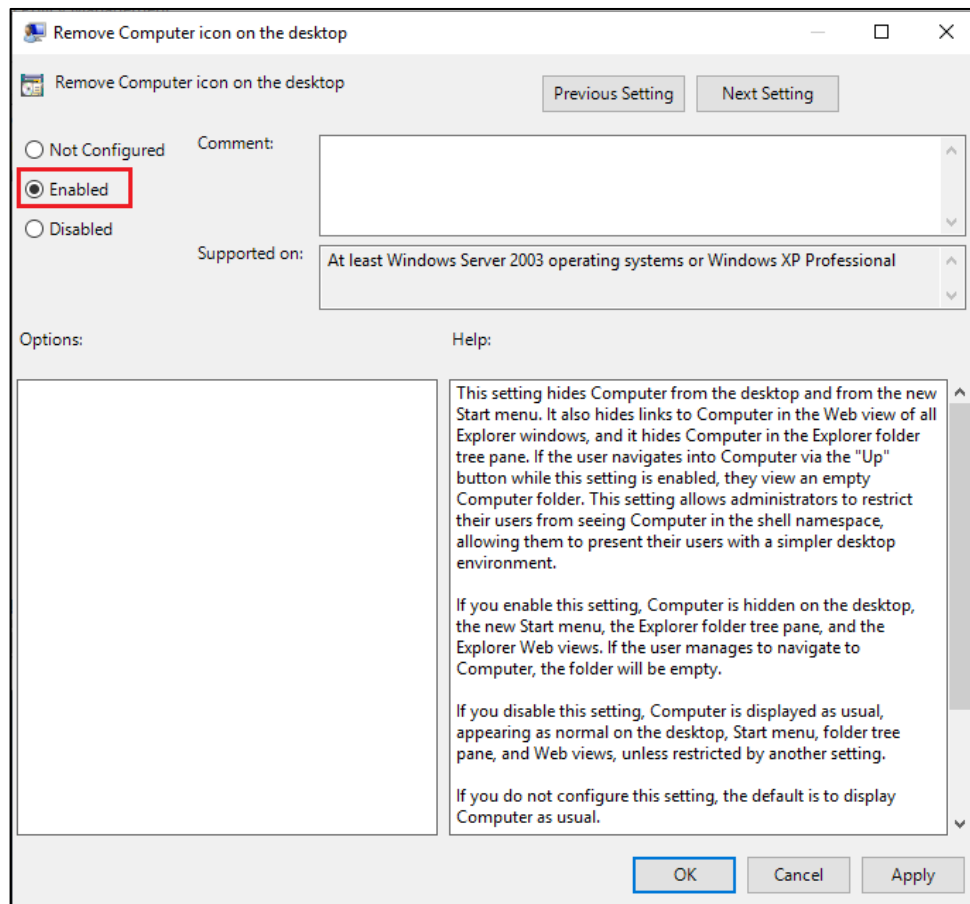
- Click chuột phải tại OU **IT**, chọn **Create a GPO in this domain...**
- Tại cửa sổ **New GPO**, nhập vào tên chính sách **Name** là **Remove icon Computer**.
- Click chuột phải vào chính sách vừa tạo, chọn **Edit**.



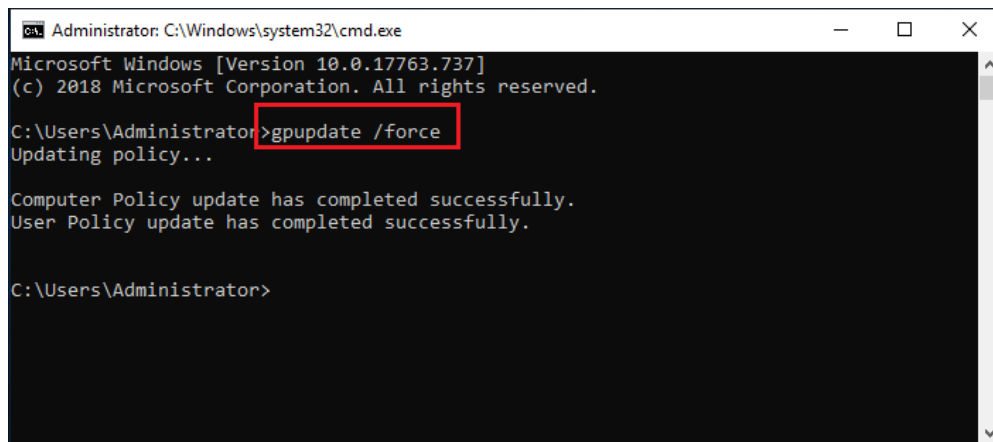
Bước 2. Group Policy Management Editor, chọn vào **User configuration/ Policies/ Administrative Templates.../ Desktop**, chọn vào chính sách **Remove Computer icon on the desktop**. Tại chính sách này, click chuột phải chọn **Edit**.



Bước 3. Tại cửa sổ **Remove Computer icon on the desktop**, click vào **Enabled**, chọn **Apply**, chọn **OK**.

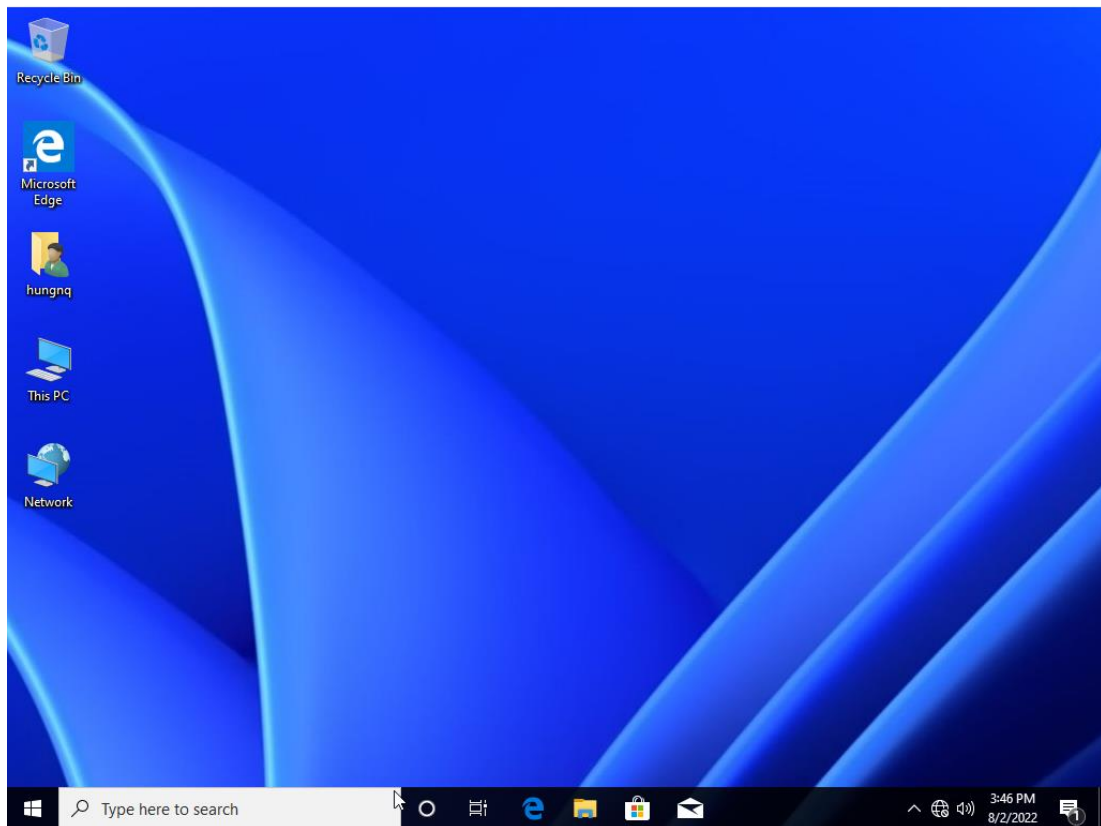


Bước 4. Cập nhật chính sách bằng lệnh **gpupdate /force** trong **cmd**.

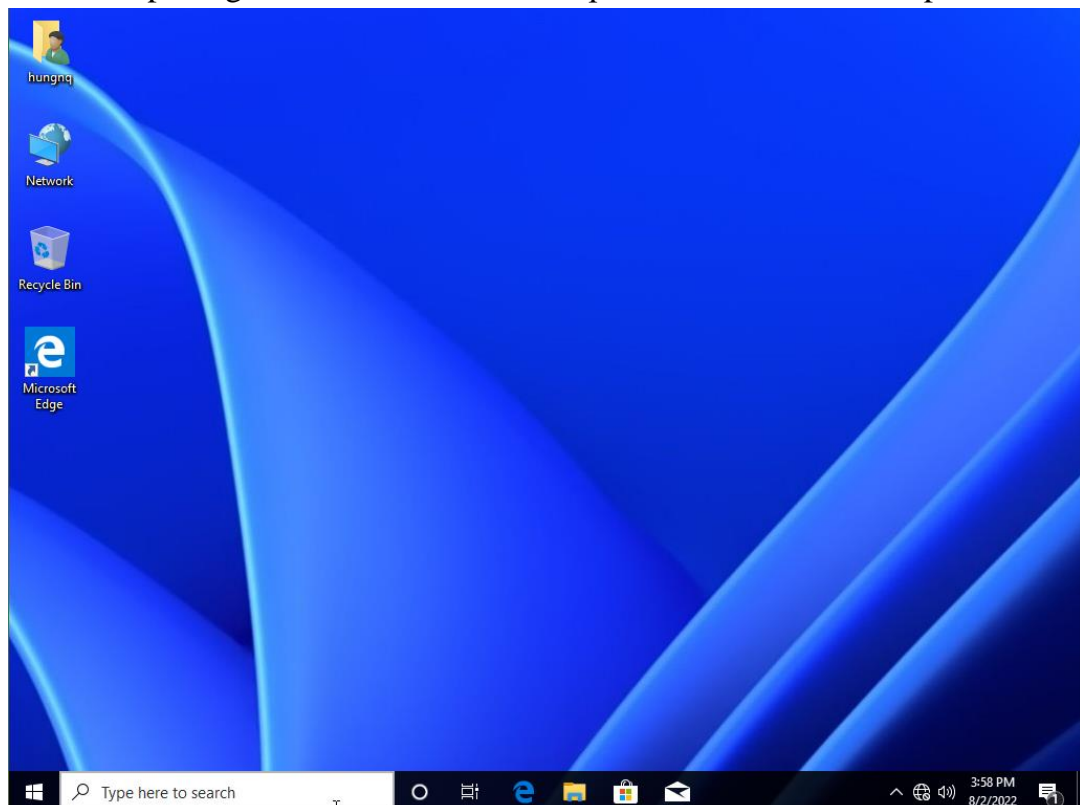


Bước 5. Chuyển sang máy **Client01** đăng nhập bằng tài khoản **hungnq** trong phòng ban **IT** kiểm tra thấy icon **Computer** trên desktop đã mất.

- Trước khi áp dụng chính sách.



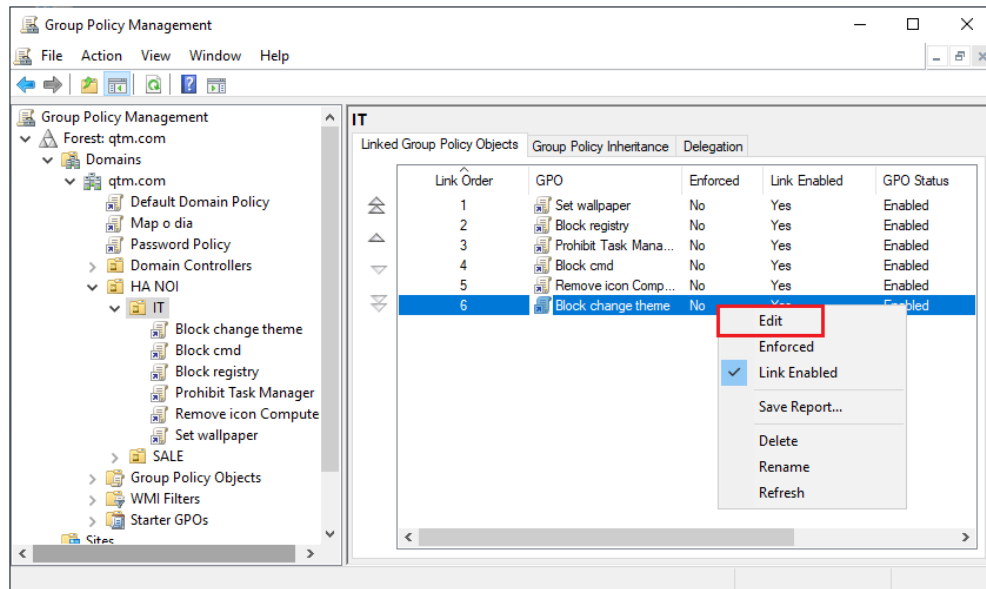
- Sau khi áp dụng chính sách thì icon Computer đã mất trên desktop.



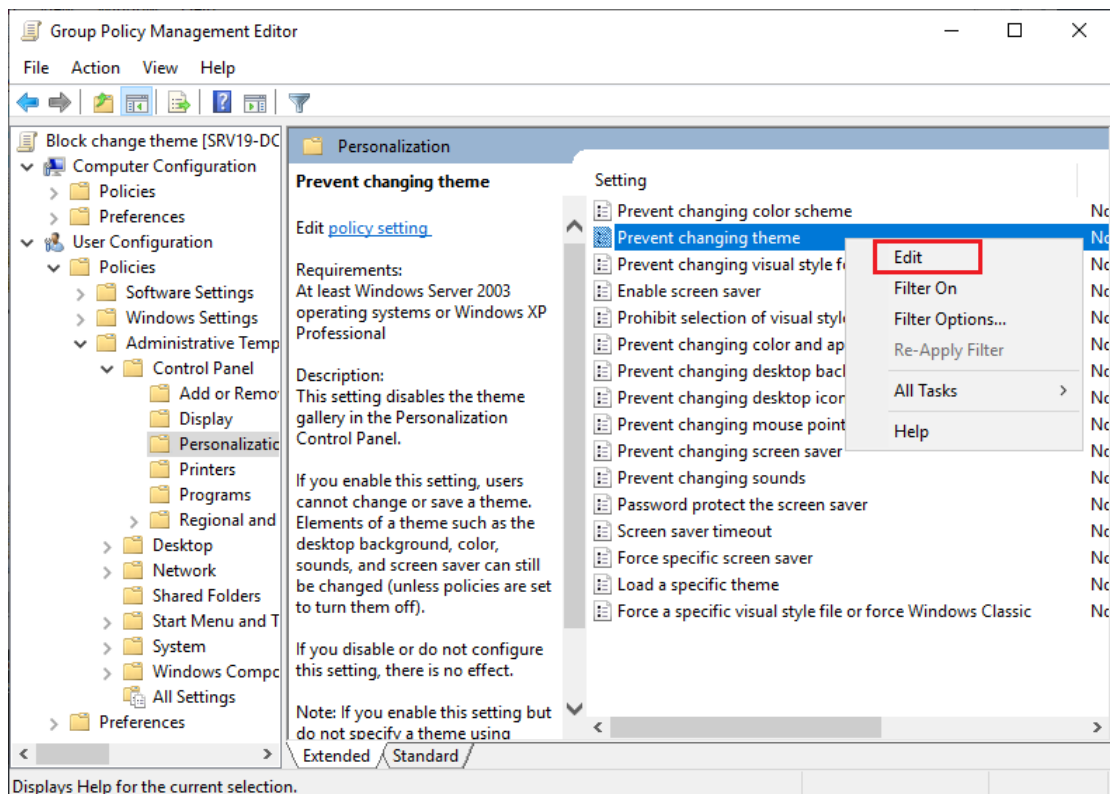
5.1.4.6. Chính sách “Chặn đổi Theme”

Bước 1. Trên máy SRV19-DC-01, tạo thêm chính sách chặn **Block change theme**.

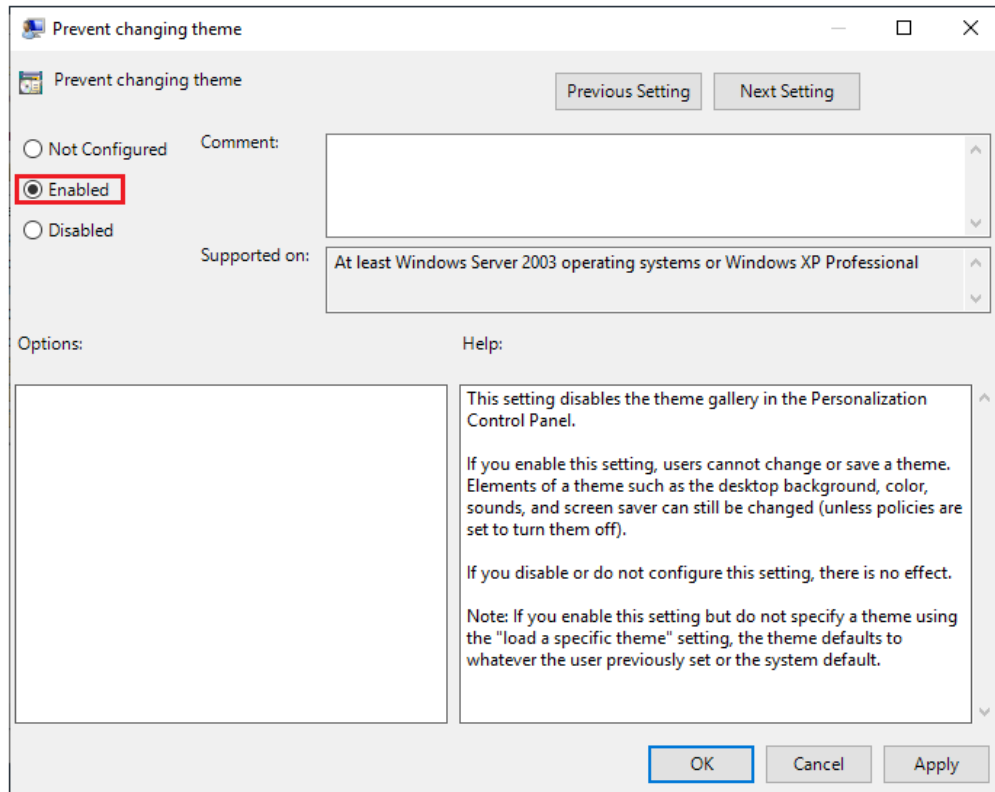
- Click chuột phải tại OU **IT**, chọn **Create a GPO in this domain...**
- Tại cửa sổ **New GPO**, nhập vào tên chính sách **Name** là **Block change theme**.
- Click chuột phải vào chính sách vừa tạo, chọn **Edit**.



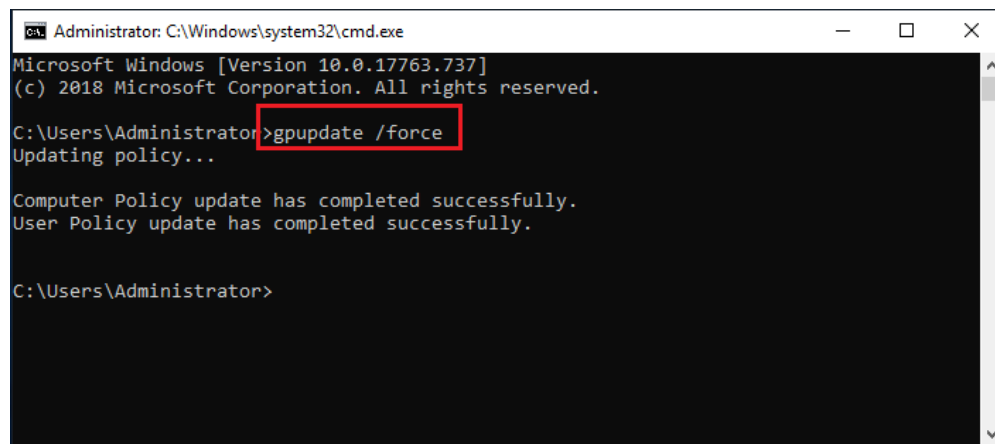
Bước 2. Group Policy Management Editor, chọn vào **User Configuration / Policies / Administrative Templates... / Control Panel/ Personalization**, chọn vào chính sách **Prevent changing theme**. Tại chính sách này, click chuột phải chọn **Edit**.



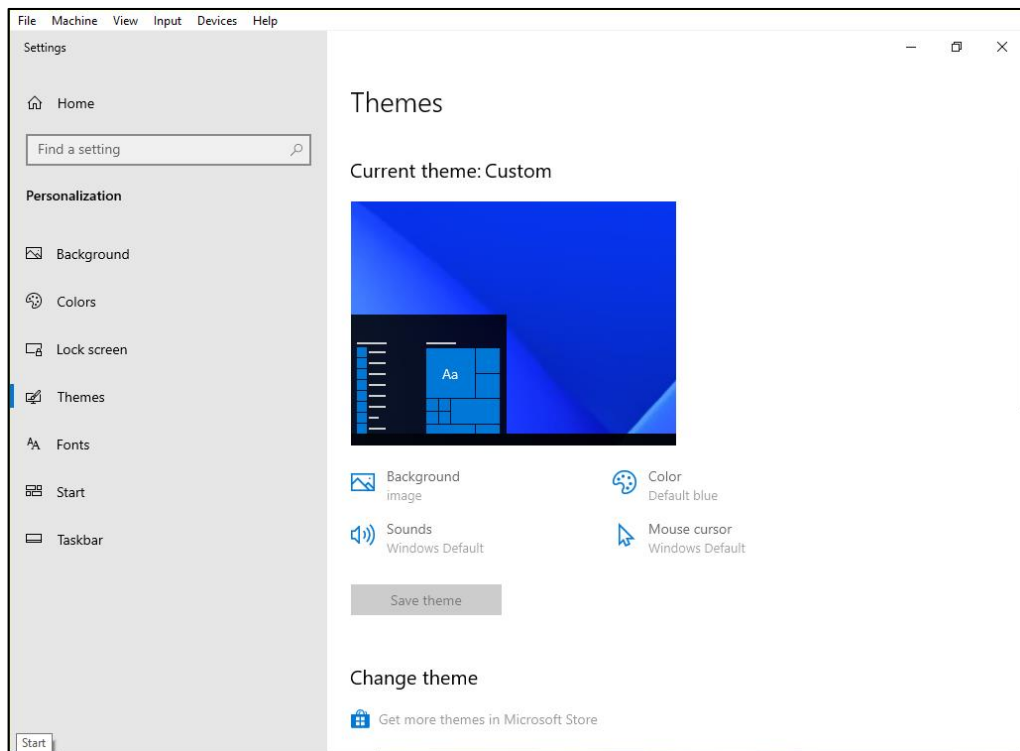
Bước 3. Tại cửa sổ **Prevent changing theme**, click vào **Enable**, chọn **Apply**, chọn **OK**.



Bước 4. Cập nhật chính sách bằng lệnh *gpupdate /force* trong **cmd**.



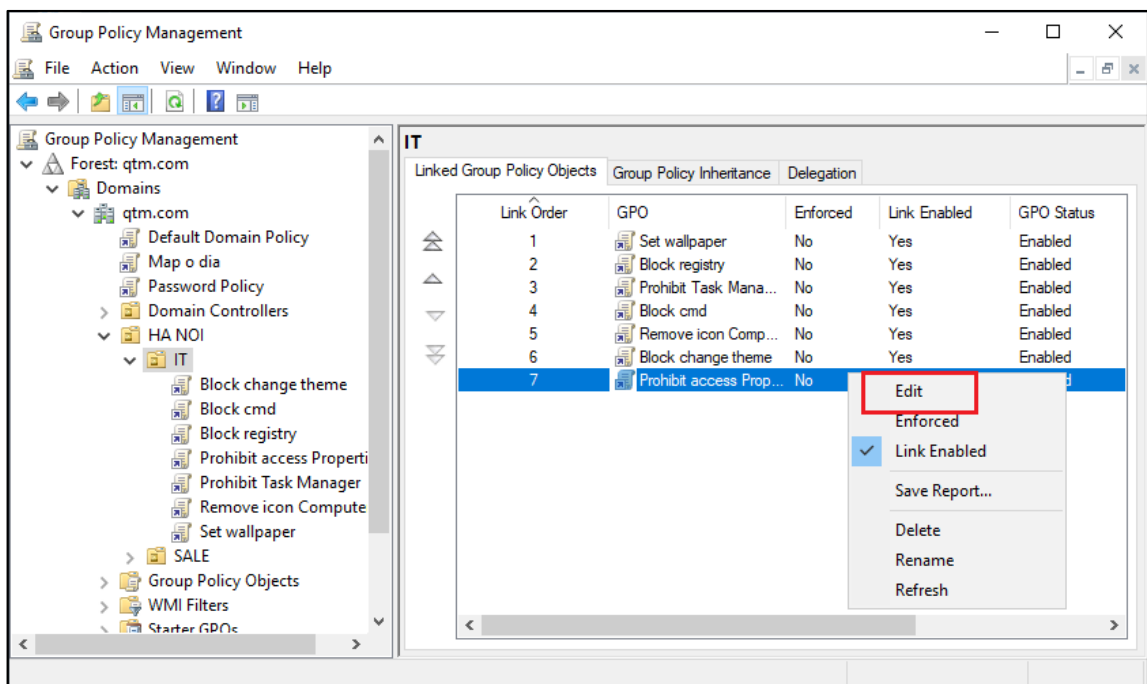
Bước 5. Chuyển sang máy **Client01** đăng nhập bằng tài khoản **hungnq** trong phòng ban **IT** kiểm tra thấy mục Theme đã ẩn.



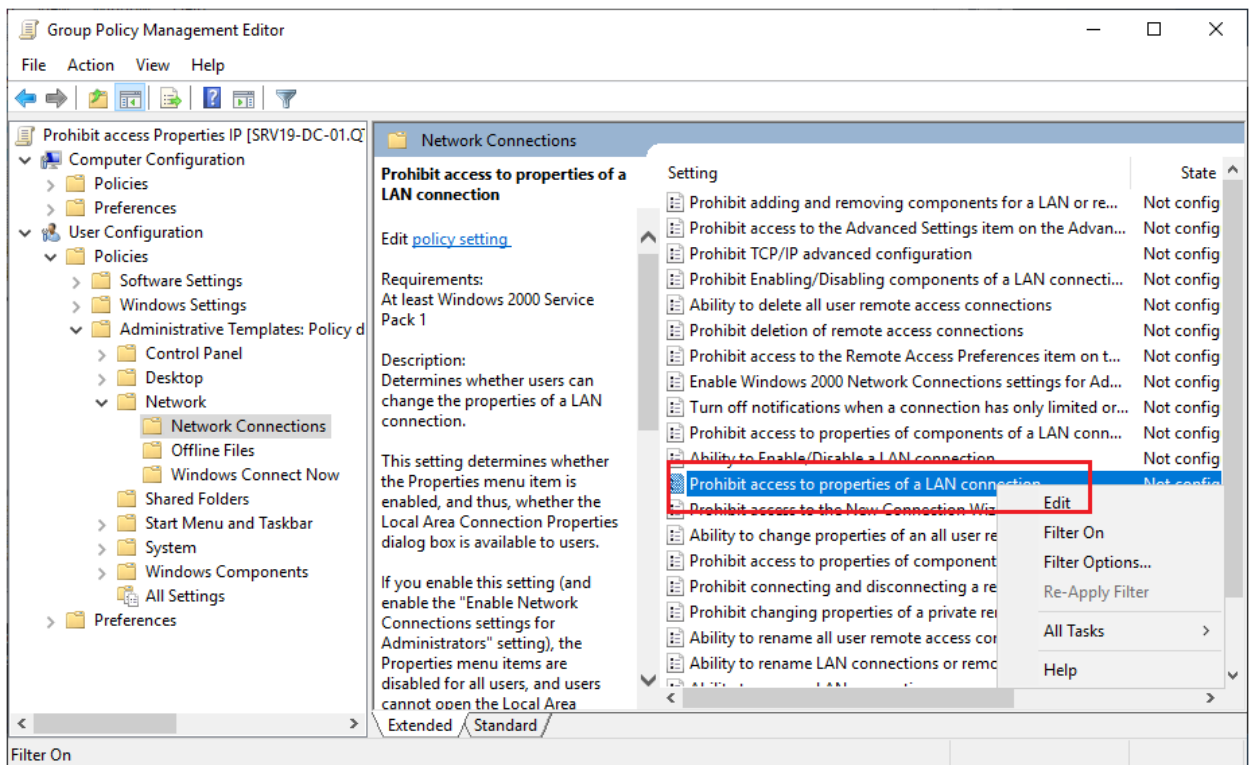
5.1.4.7. Chính sách “Chặn Properties IP”

Bước 1. Trên máy SRV19-DC-01, tạo thêm chính sách chặn **Prohibit access Properties IP**.

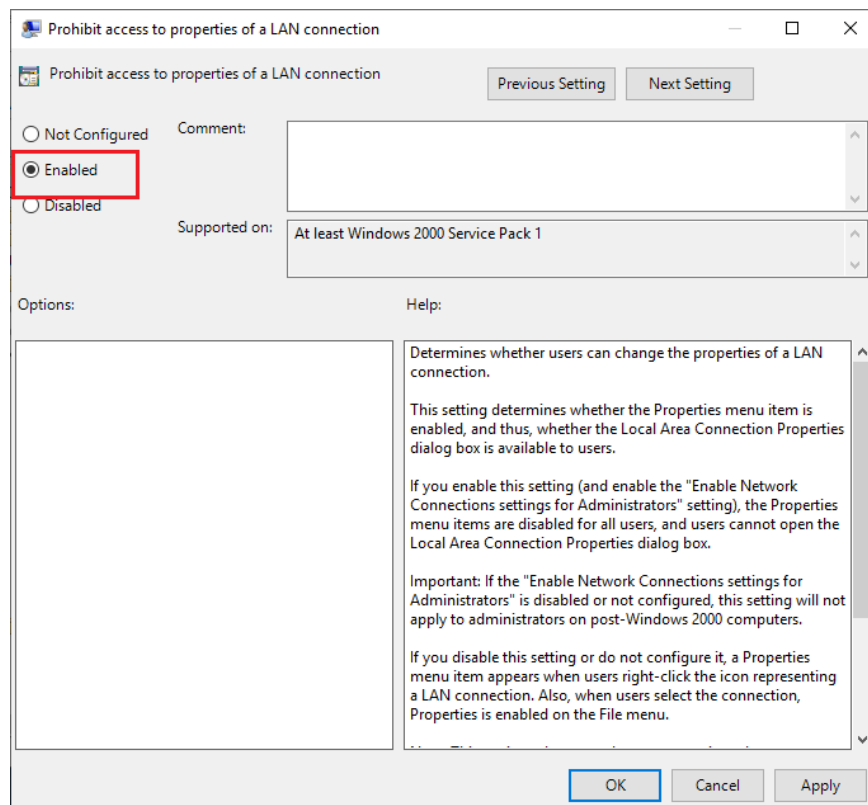
- Click chuột phải tại OU **IT**, chọn **Create a GPO in this domain...**
- Tại cửa sổ **New GPO**, nhập vào tên chính sách **Name** là **Prohibit access Properties IP**.
- Click chuột phải vào chính sách vừa tạo, chọn **Edit**.



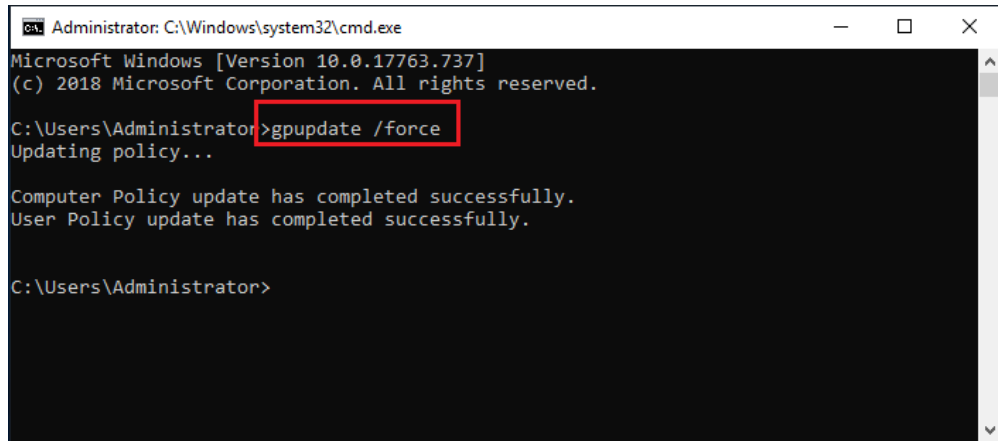
Bước 2. Group Policy Management Editor, chọn vào **User Configuration / Policies / Administrative Template... / Network/ network Connections**, chọn vào chính sách **Prohibit access to properties of a LAN connection**. Tại chính sách này, click chuột phải chọn **Edit**.



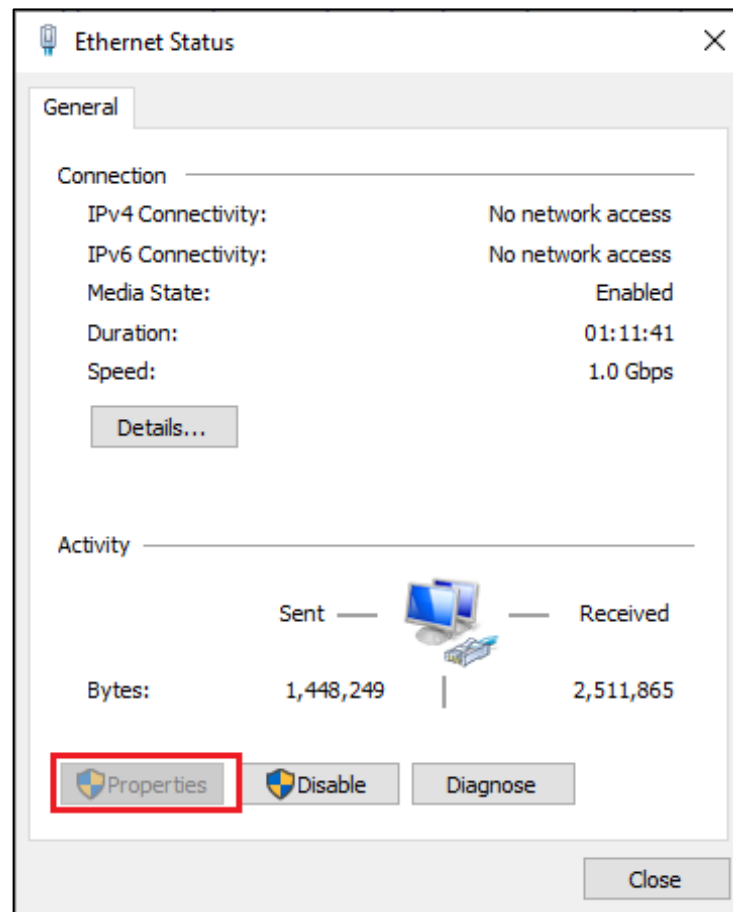
Bước 3. Tại cửa sổ **Prohibit access to properties of a LAN connection**, click vào **Enabled**, chọn **Apply**, chọn **OK**.



Bước 4. Cập nhật chính sách bằng lệnh *gpupdate /force* trong *cmd*.



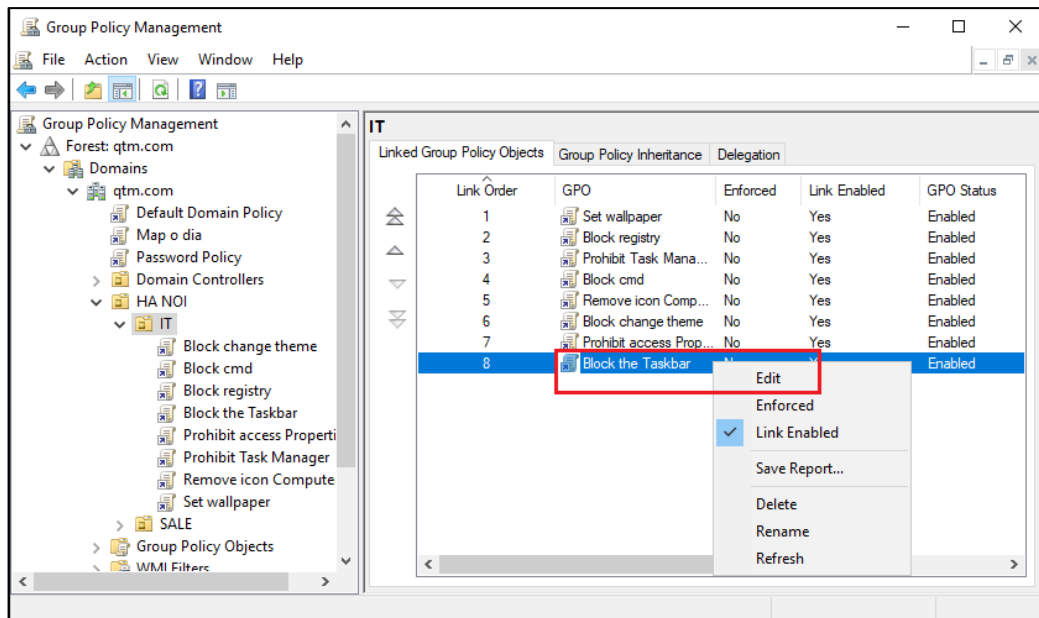
Bước 5. Chuyển sang máy **Client01** đăng nhập bằng tài khoản *hungnq* trong phòng ban IT kiểm tra thấy không thể truy cập vào Properties của card mạng.



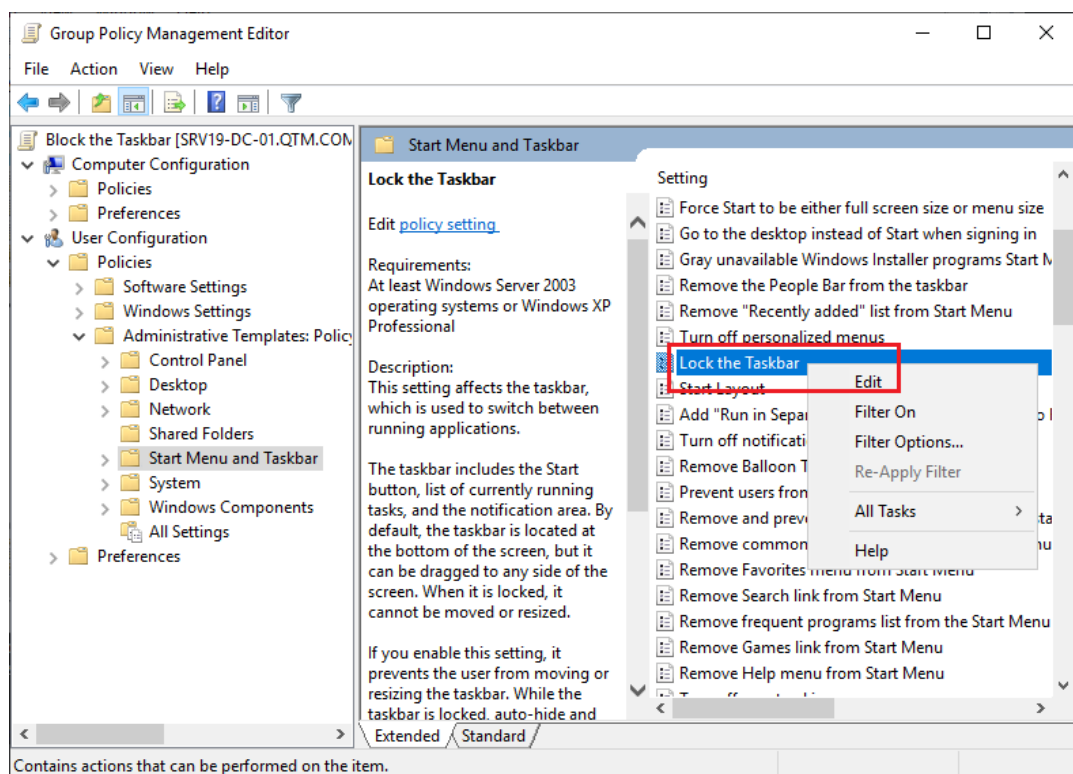
5.1.4.8. Chính sách “Khóa Taskbar”

Bước 1. Trên máy SRV19-DC-01, tạo thêm chính sách chặn **Lock the Taskbar**.

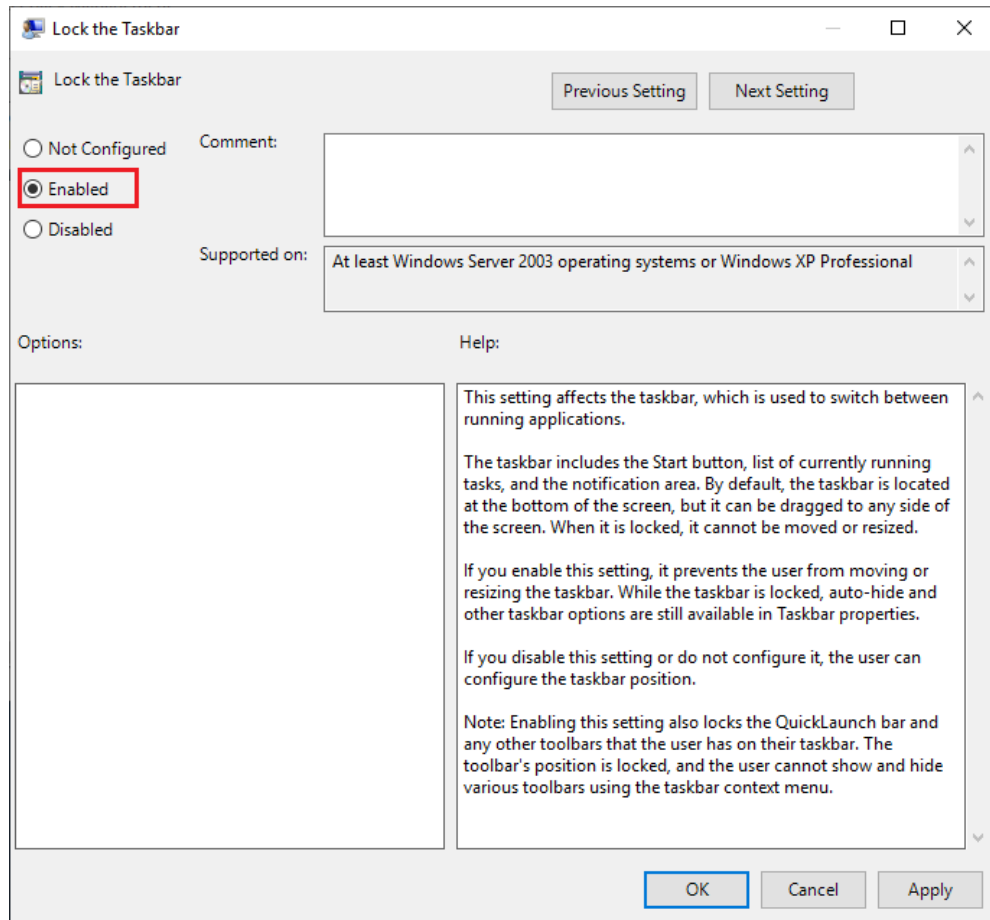
- Click chuột phải tại OU **IT**, chọn **Create a GPO in this domain...**
- Tại cửa sổ **New GPO**, nhập vào tên chính sách **Name** là **Lock the Taskbar**.
- Click chuột phải vào chính sách vừa tạo, chọn **Edit**.



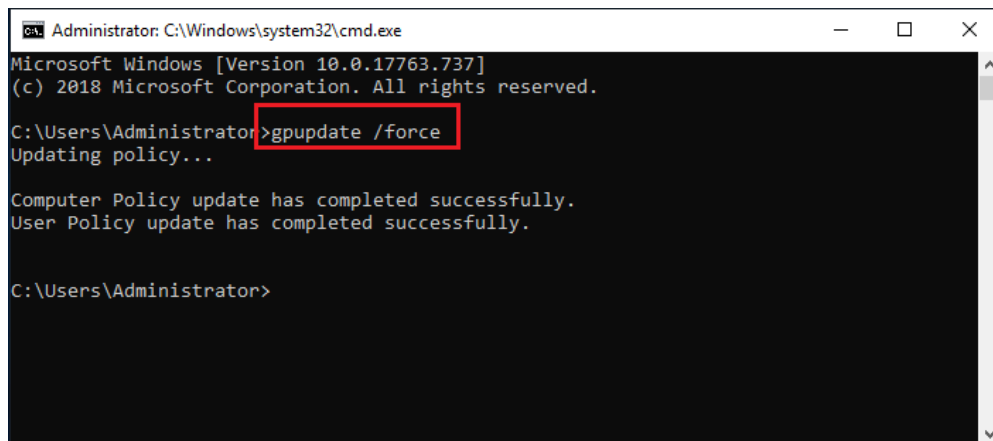
Bước 2. Group Policy Management Editor, chọn vào **User Configuration / Policies / Administrative Template... /Start Menu and Taskbar**, chọn vào chính sách **Lock the Taskbar**. Tại chính sách này, click chuột phải chọn **Edit**.



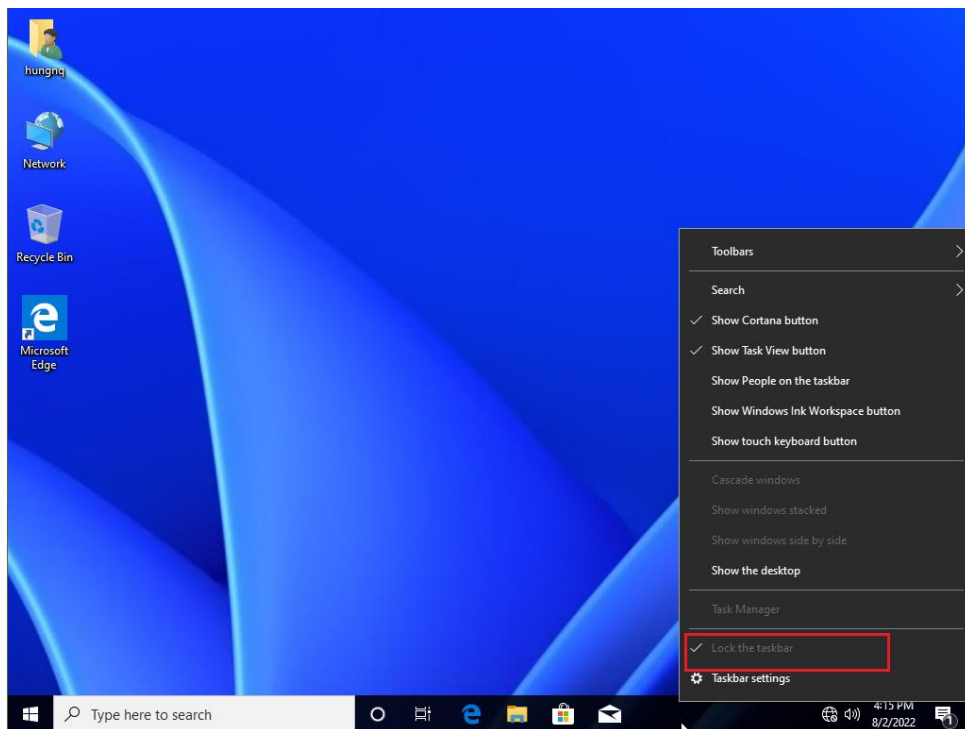
Bước 3. Tại cửa sổ **Lock the Taskbar**, click vào **Enable**, chọn **Apply**, chọn **OK**.



Bước 4. Cập nhật chính sách bằng lệnh *gpupdate /force* trong **cmd**.



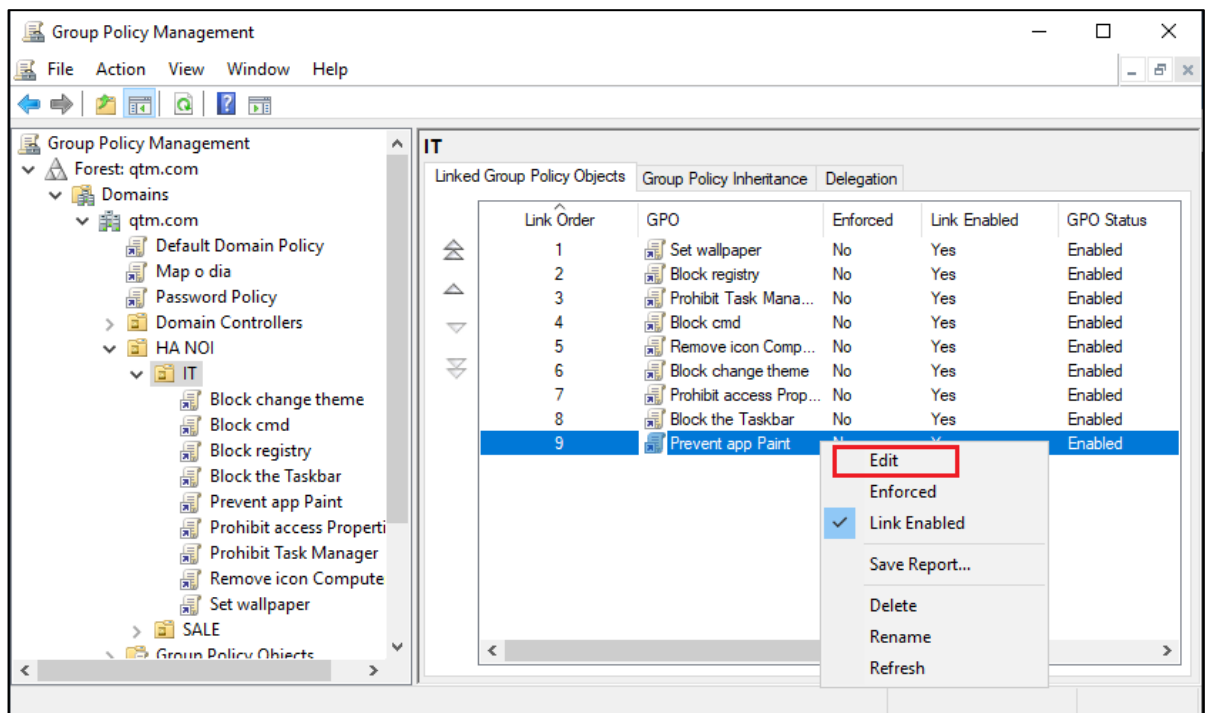
Bước 5. Chuyển sang máy **Client01** đăng nhập bằng tài khoản **hungnq** trong phòng ban **IT** kiểm tra kết quả.



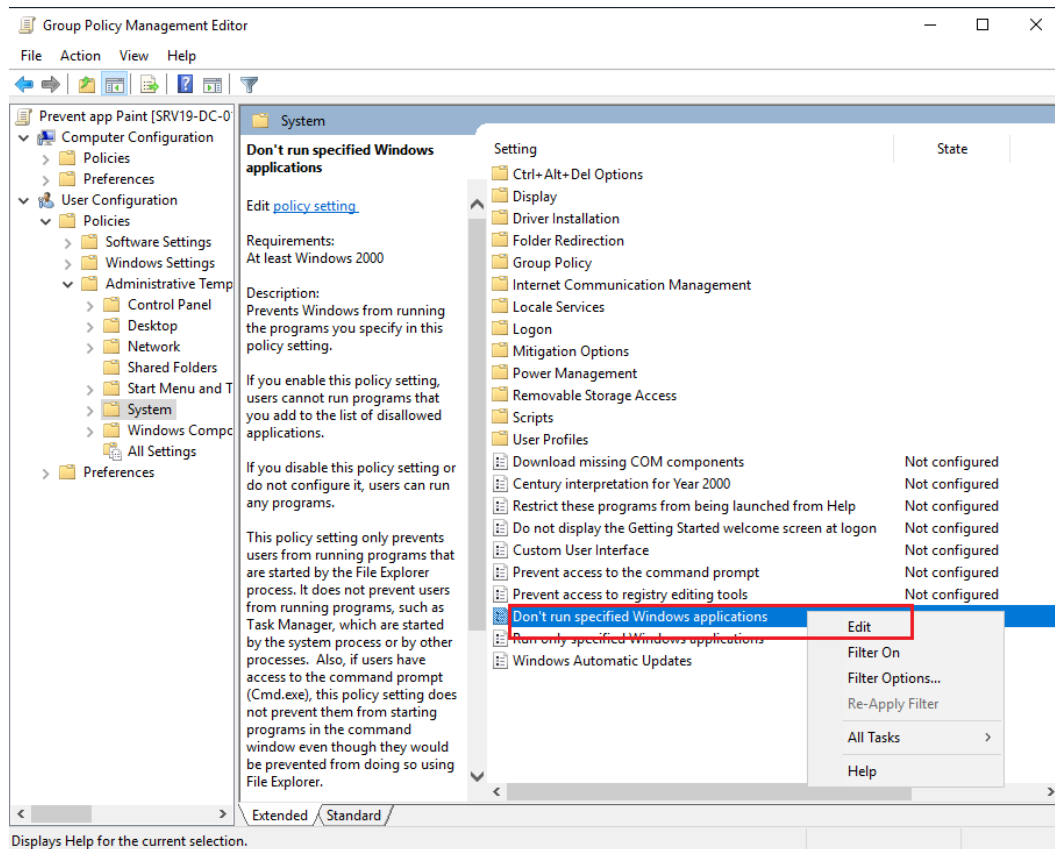
5.1.4.9. Chính sách “Chặn truy cập Paint”

Bước 1. Trên máy SRV19-DC-01, tạo thêm chính sách chặn **Prevent app paint**.

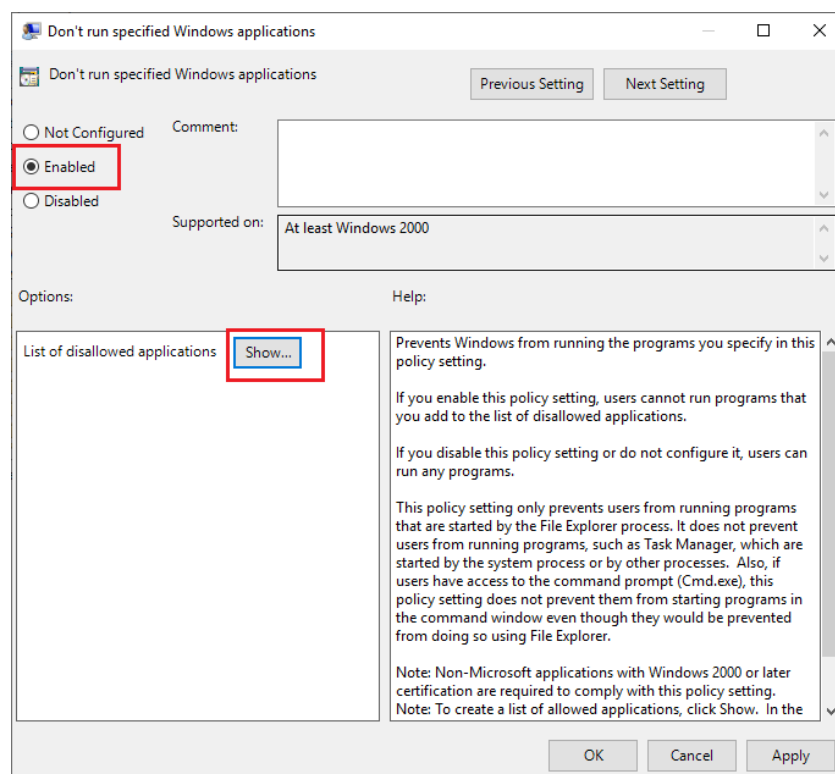
- Click chuột phải tại OU **IT**, chọn **Create a GPO in this domain...**
- Tại cửa sổ **New GPO**, nhập vào tên chính sách **Name** là **Prevent app paint**.
- Click chuột phải vào chính sách vừa tạo, chọn **Edit**.



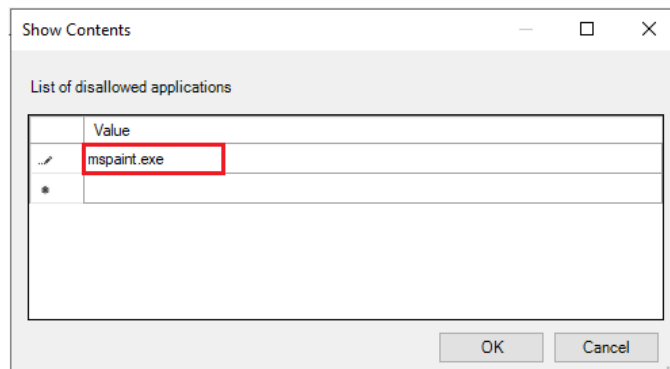
Bước 2. Group Policy Management Editor, chọn vào **User Configuration / Policies / Administrative Template... / System**, chọn vào chính sách **Don't run specified Windows applications**. Tại chính sách này, click chuột phải chọn **Edit**.



Bước 3. Tại cửa sổ **Don't run specified Windows applications**, click vào **Enable**, chọn **Show**.

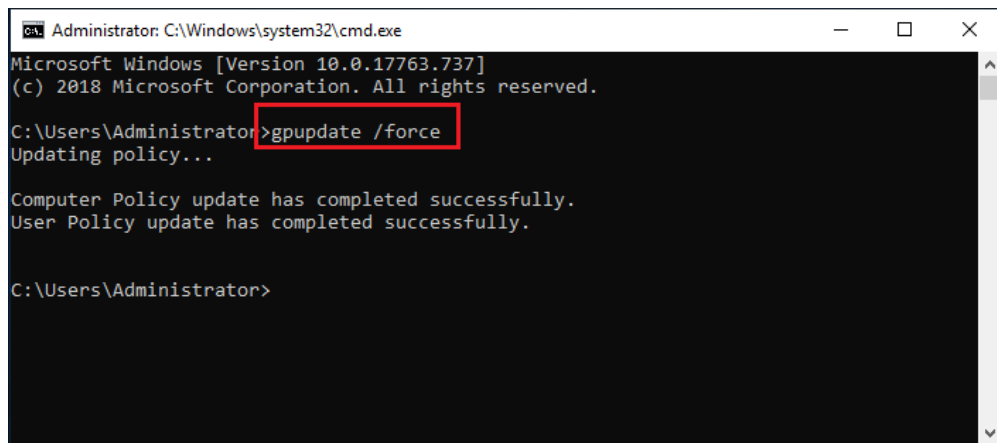


Bước 4. Tại hộp thoại **Show Contents**, gõ vào **mspaint.exe**, chọn **OK**. Tại cửa sổ **Don't run specified Windows applications** chọn **Apply**, chọn **OK**.

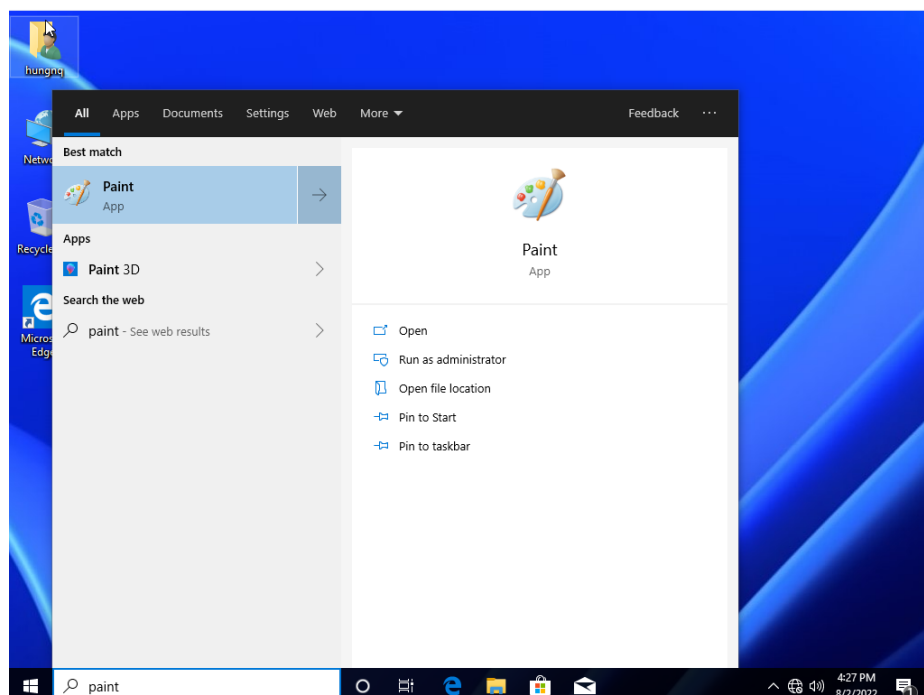


Lưu ý: nếu muốn chặn sử dụng ứng dụng khác thì thêm vào tên, mỗi ứng dụng trên 1 dòng.

Bước 5. Cập nhật chính sách bằng lệnh **gpupdate /force** trong **cmd**.



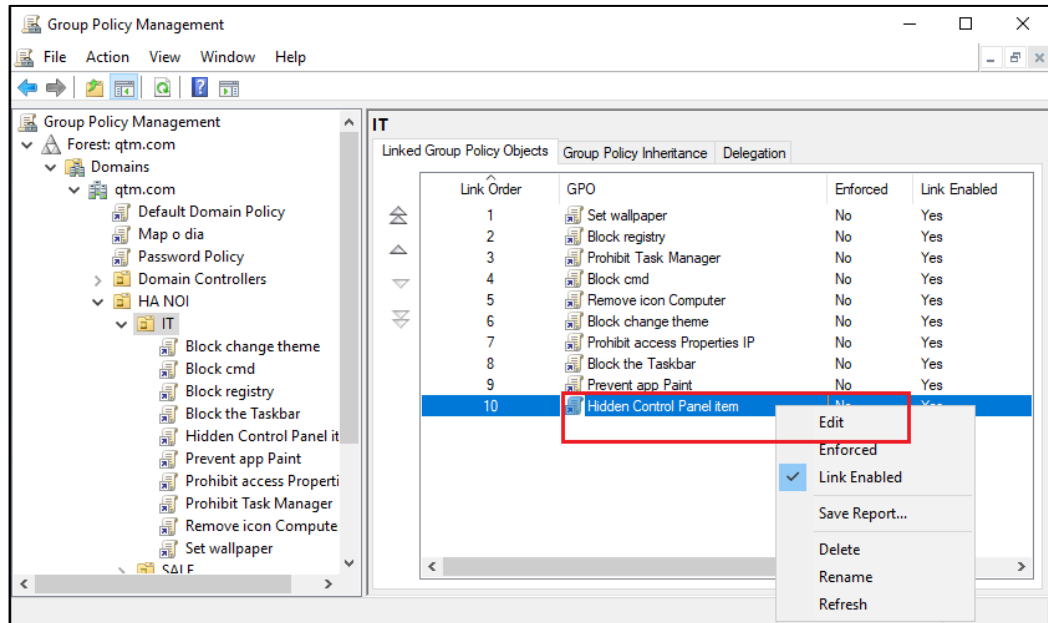
Bước 6. Chuyển sang máy **Client01** đăng nhập bằng tài khoản **hungnq** trong phòng ban **IT** kiểm tra thấy nhưng không thể mở Paint.



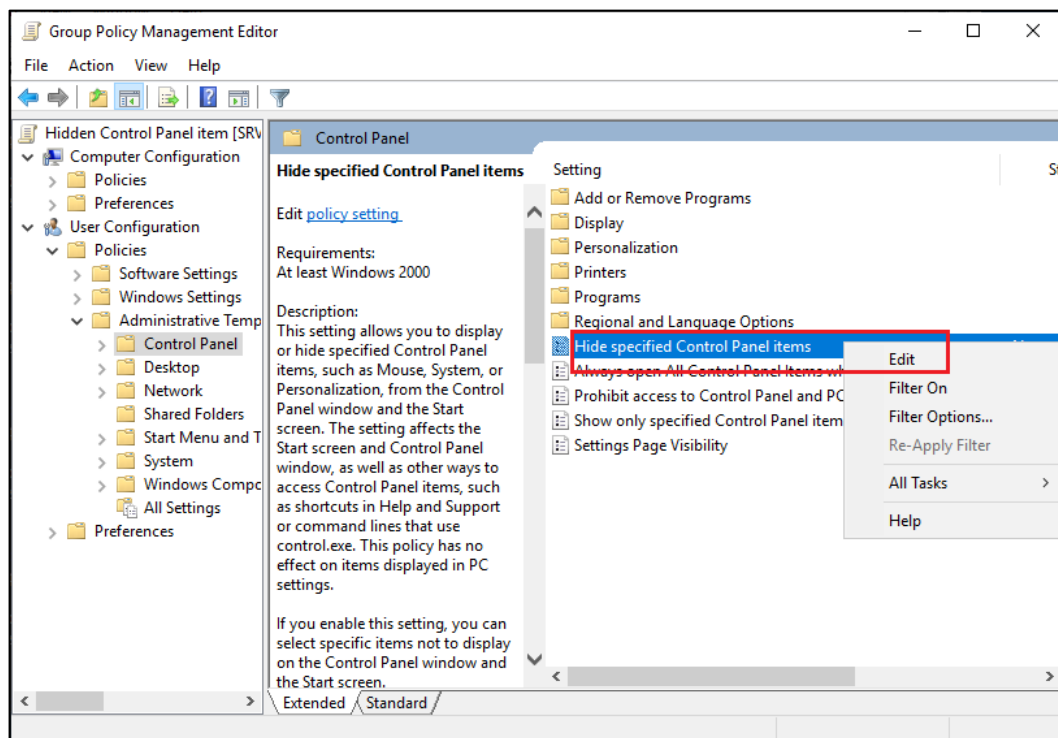
5.1.4.10. Chính sách “Ẩn item trong Control Panel”

Bước 1. Trên máy SRV19-DC-01, tạo thêm chính sách chặn **Hidden Control Panel item**.

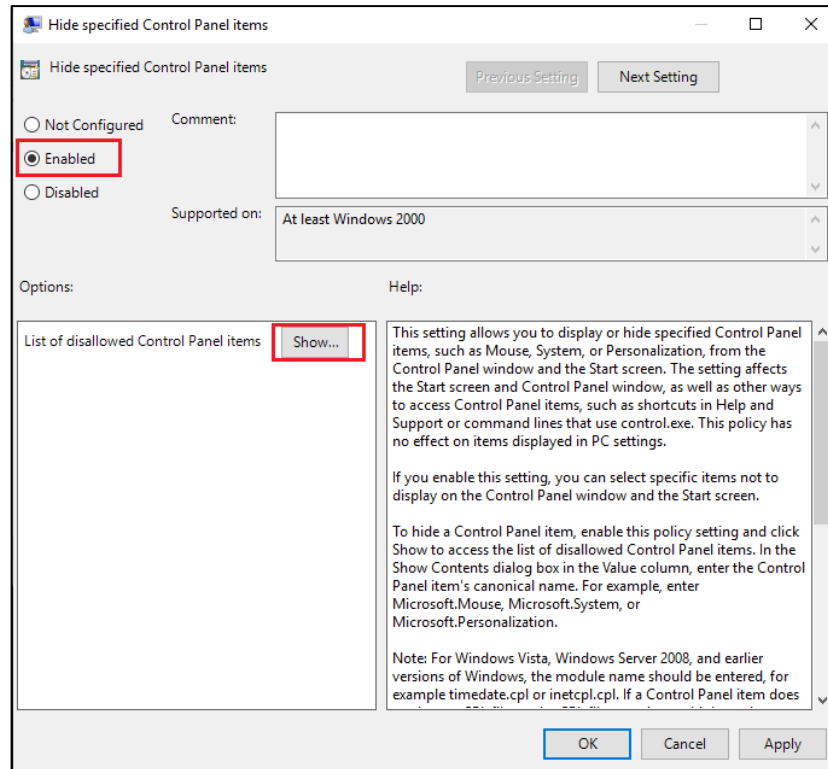
- Click chuột phải tại OU **IT**, chọn **Create a GPO in this domain...**
- Tại cửa sổ **New GPO**, nhập vào tên chính sách **Name** là **Hidden Control Panel item**.
- Click chuột phải vào chính sách vừa tạo, chọn **Edit**.



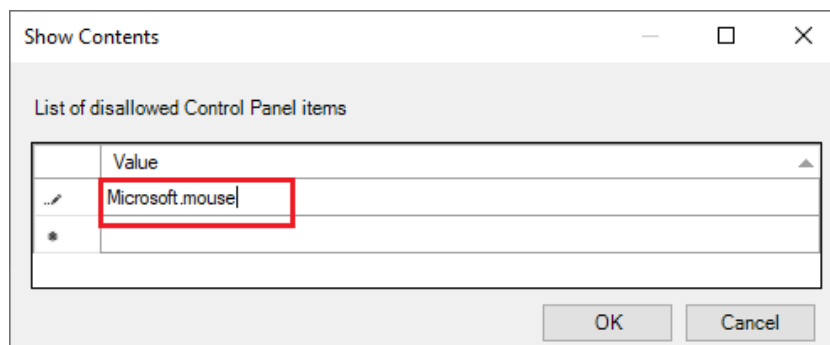
Bước 2. Group Policy Management Editor, chọn vào **User Configuration / Policies / Administrative Template... / Control Panel**, chọn vào chính sách **Hide specified Control Panel items**. Tại chính sách này, click chuột phải chọn **Edit**.



Bước 3. Tại cửa sổ **Hide specified Control Panel items**, click vào **Enable**, chọn **Show**.

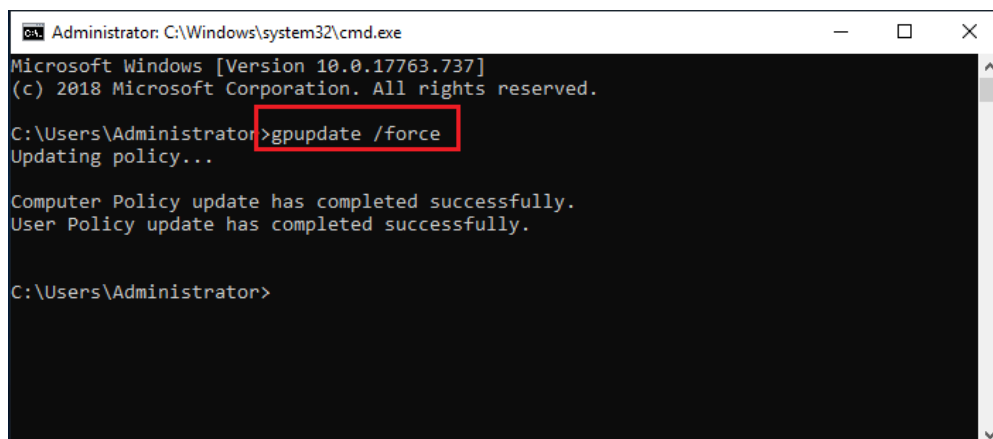


Bước 4. Tại hộp thoại **Show Contents**, gõ vào **Microsoft.mouse** > **OK**. Tại cửa sổ **Hide specified Control Panel items** chọn **Apply**, chọn **OK**.

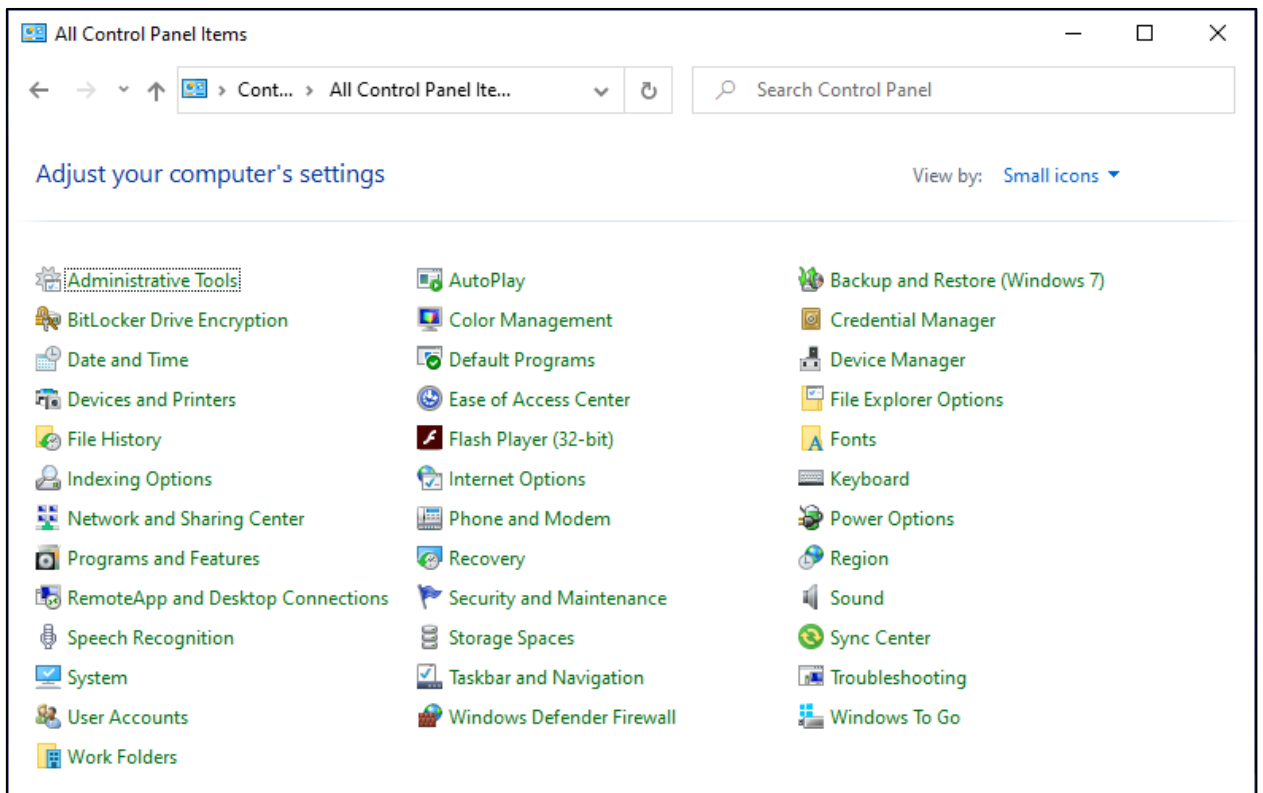


Lưu ý: nếu muốn chặn sử dụng item khác thì thêm vào tên, mỗi item trên 1 dòng.

Bước 5. Cập nhật chính sách bằng lệnh **gpupdate /force** trong **cmd**.



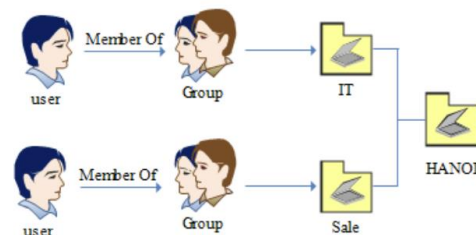
Bước 5. Chuyển sang máy **Client01** đăng nhập bằng tài khoản **hungnq** trong phòng ban **IT** kiểm tra không thấy icon **mouse** trong **Control Panel**



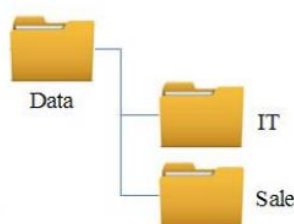
5.2. GIÁM SÁT TẬP TIN VÀ BẮT XOÁ FILE

5.2.1. Chuẩn bị

- 01 máy Server SRV19-DC-01 đã nâng cấp lên Domain quản lý miền qtm.com. Cài đặt cấu hình DNS và tạo các OU tương ứng.



- 01 máy Server SRV19-10 join miền qtm.com và dùng để tạo thư mục và phân quyền truy cập.



- 01 máy Client1 join miền qtm.com dùng để kiểm tra xóa file.

- Sơ đồ địa chỉ IP như sau:

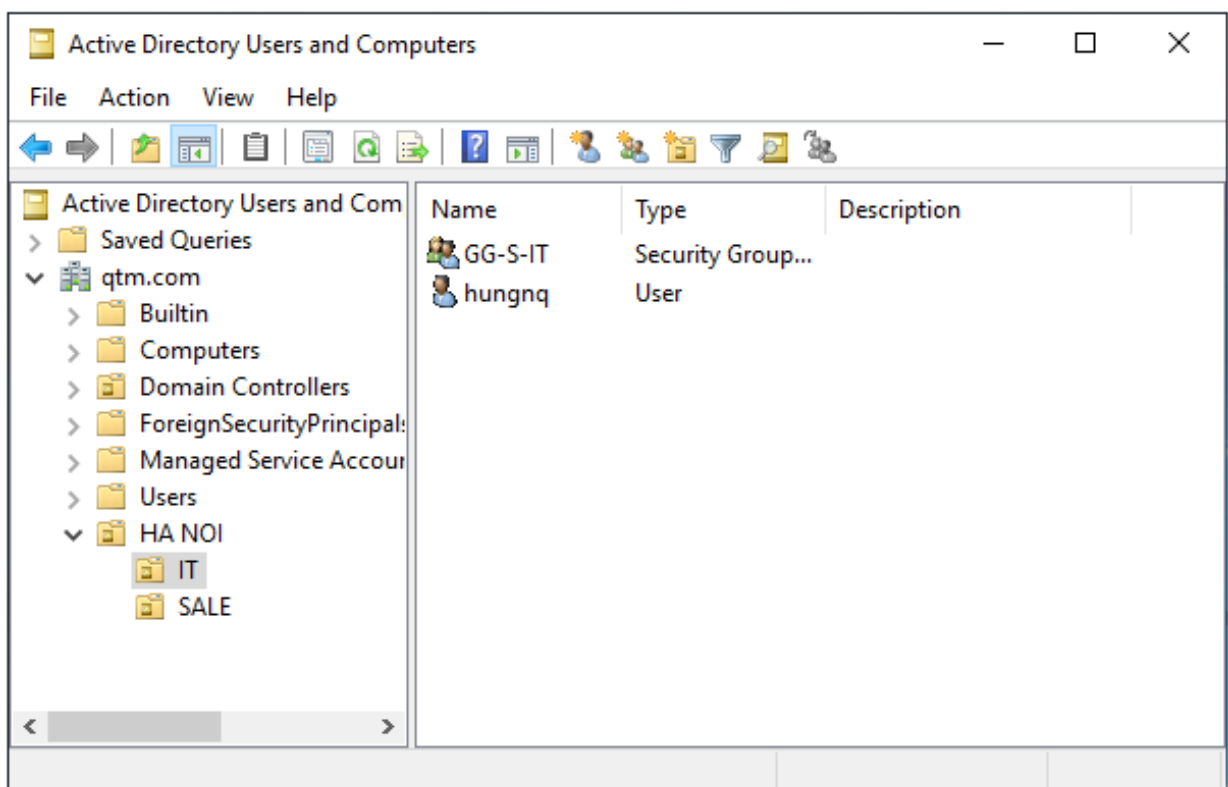
Thông số	SRV19-DC-01	SRV19-10	Client01
IP address	192.168.1.2	192.168.1.10	192.168.1.100
Gateway	192.168.1.1	192.168.1.1	255.255.255.0
Subnet mask	255.255.255.0	255.255.255.0	192.168.1.1
DNS Server	192.168.1.2	192.168.1.2	192.168.1.2

5.2.2. Yêu cầu

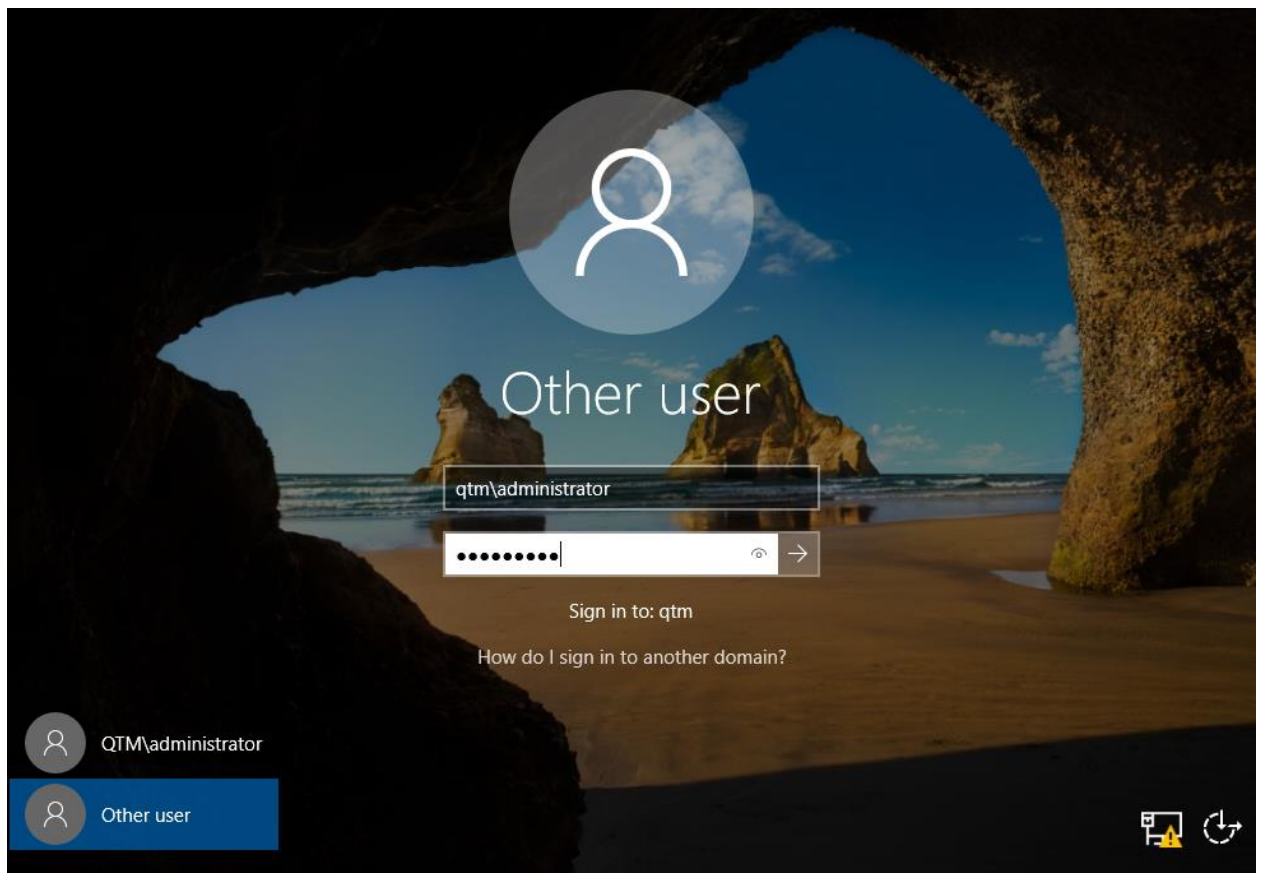
- Tạo OU, tài khoản người dùng và tài khoản nhóm theo miền qtm.com
- Tạo lần lượt các thư mục IT, SALE trên máy **SRV19-10**.
- Cấu hình giám sát tệp tin và bắt xóa File.
- Kiểm tra sau khi xóa file.

5.2.3. Thực hiện

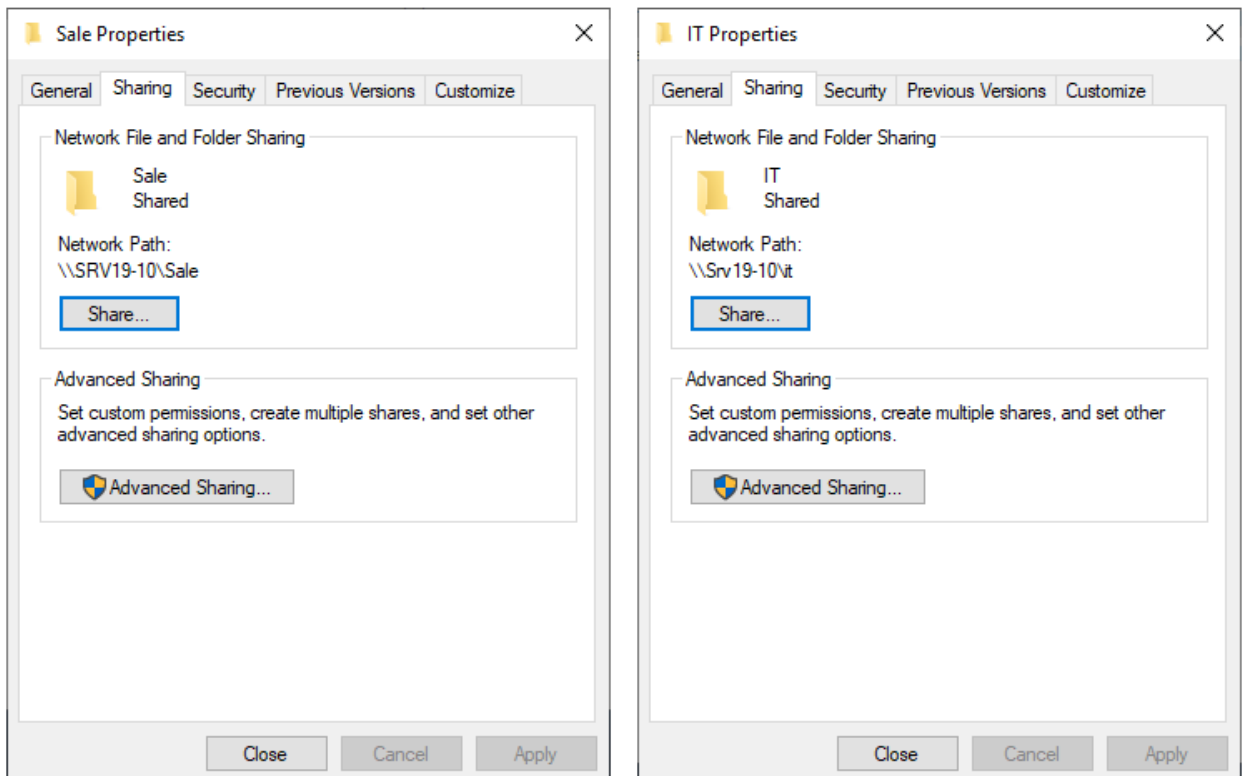
Bước 1. Thực hiện trên máy **SRV19-DC-01**, tạo OU, group, user như yêu cầu, add user vào group và kiểm tra phân giải địa chỉ IP.



Bước 2. Chuyển sang máy **SRV19-10**, tiến hành Join vào domain, đăng nhập bằng tài khoản Administrator của miền.

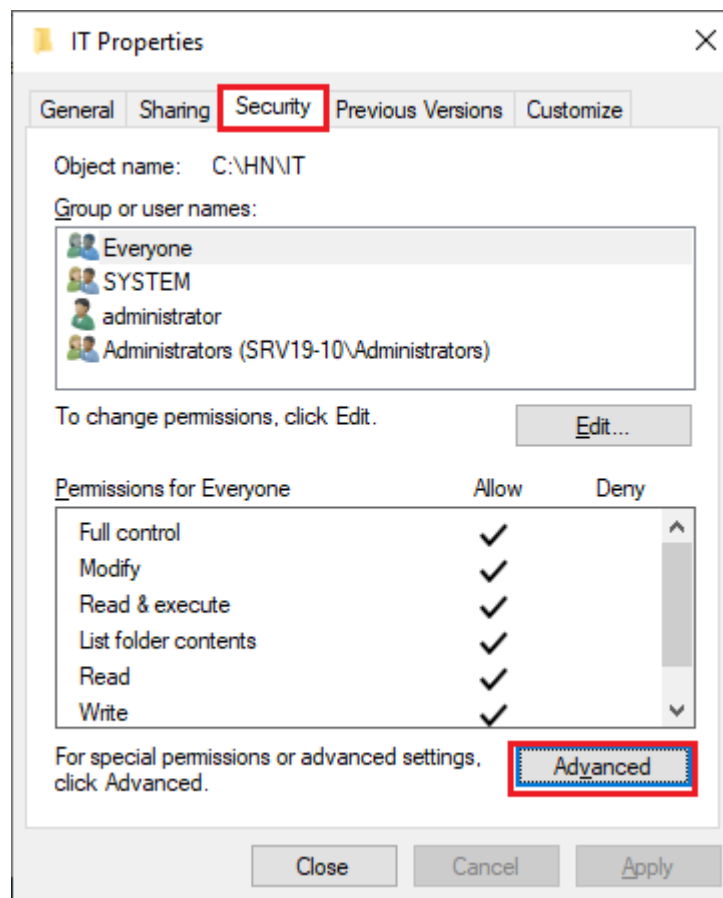


Bước 3. Vào ổ C của máy **SRV19-10**. Tạo thư mục HN, trong thư mục HN, tạo 2 thư mục IT và Sale. Tiến hành chia sẻ, phân quyền 2 thư mục IT và Sale.

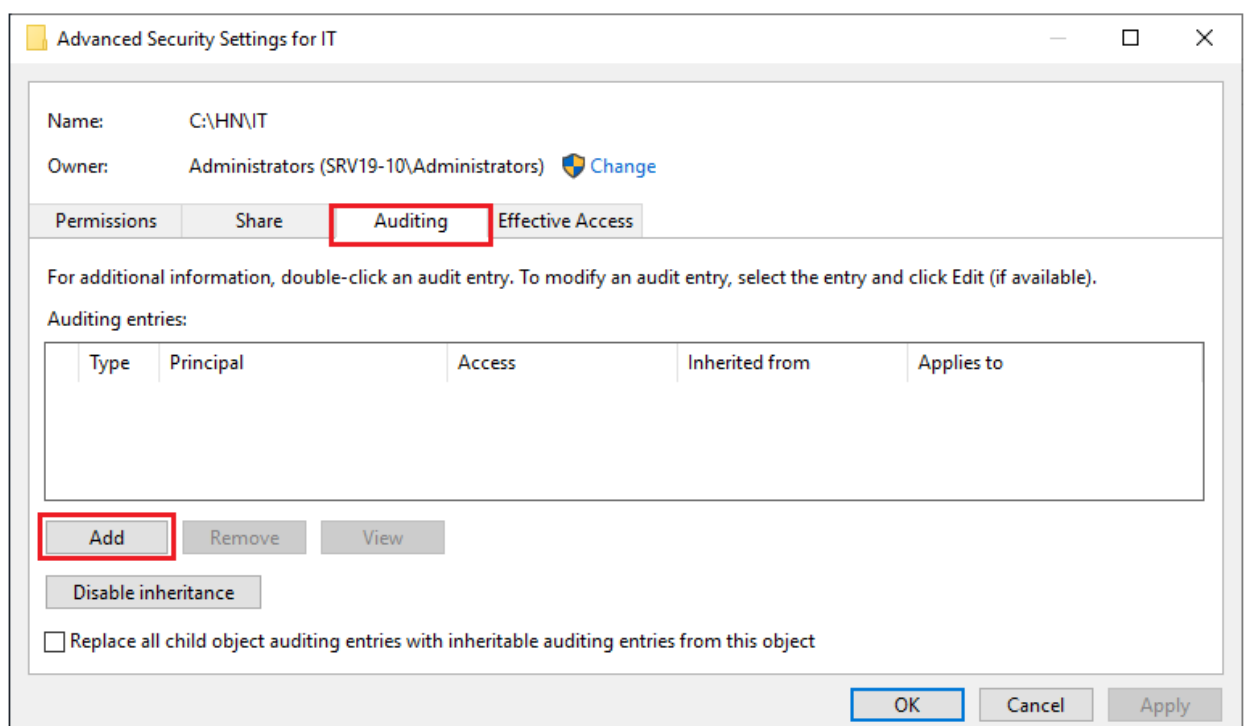


Bước 4. Cấu hình ghi lại hoạt động của thư mục:

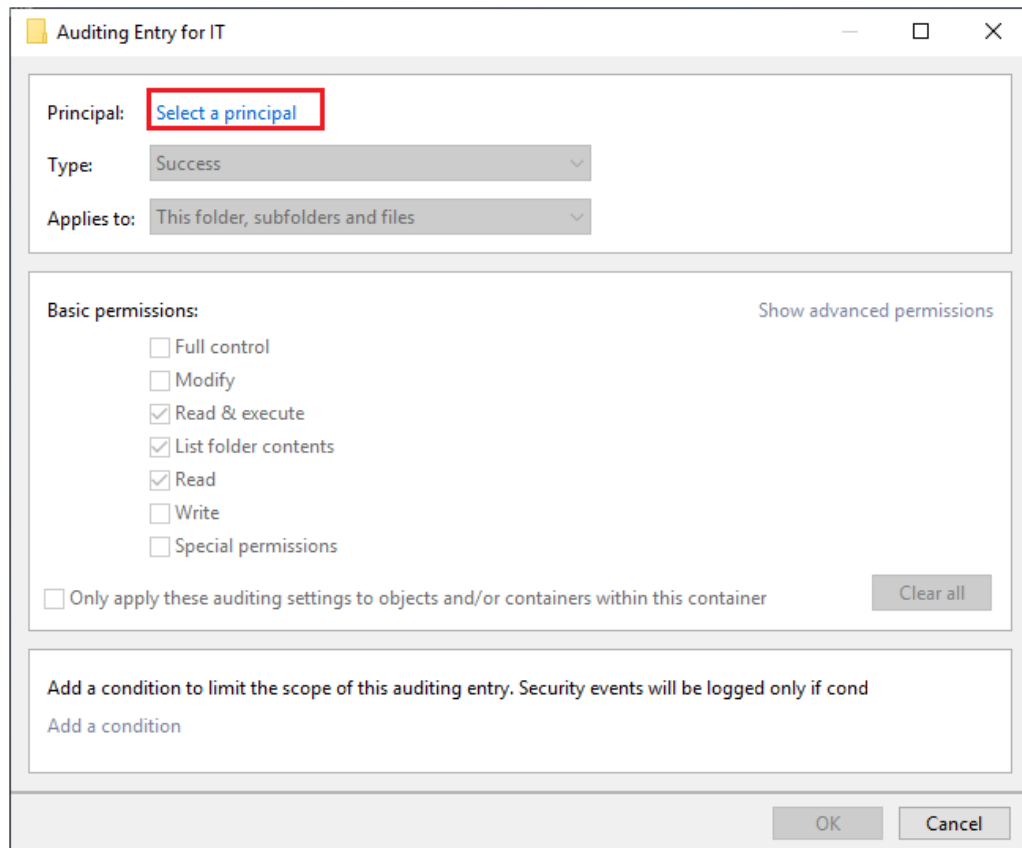
- Trong cửa sổ **IT Properties**, chuyển sang tab **Security**, chọn **Advanced**.



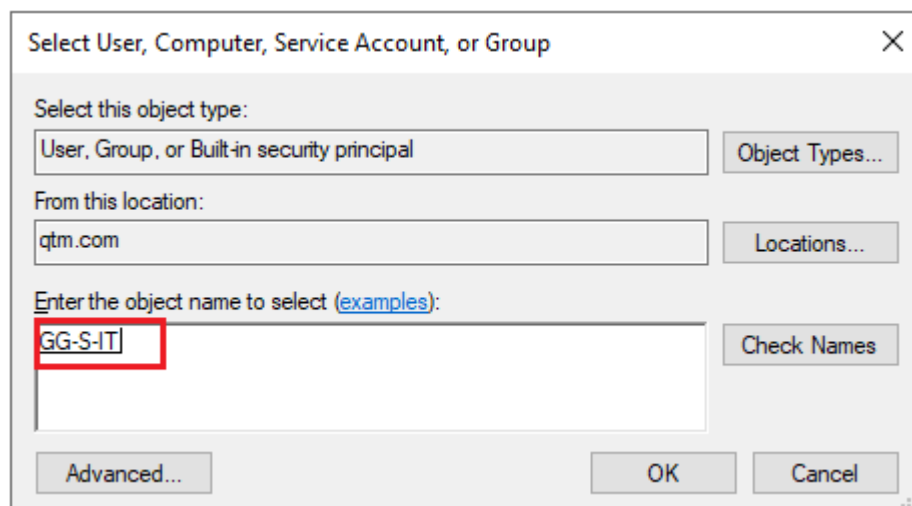
- Trong cửa sổ **Advanced Security Settings for IT**, chuyển sang tab **Auditing**, tại đây click vào **Add**.



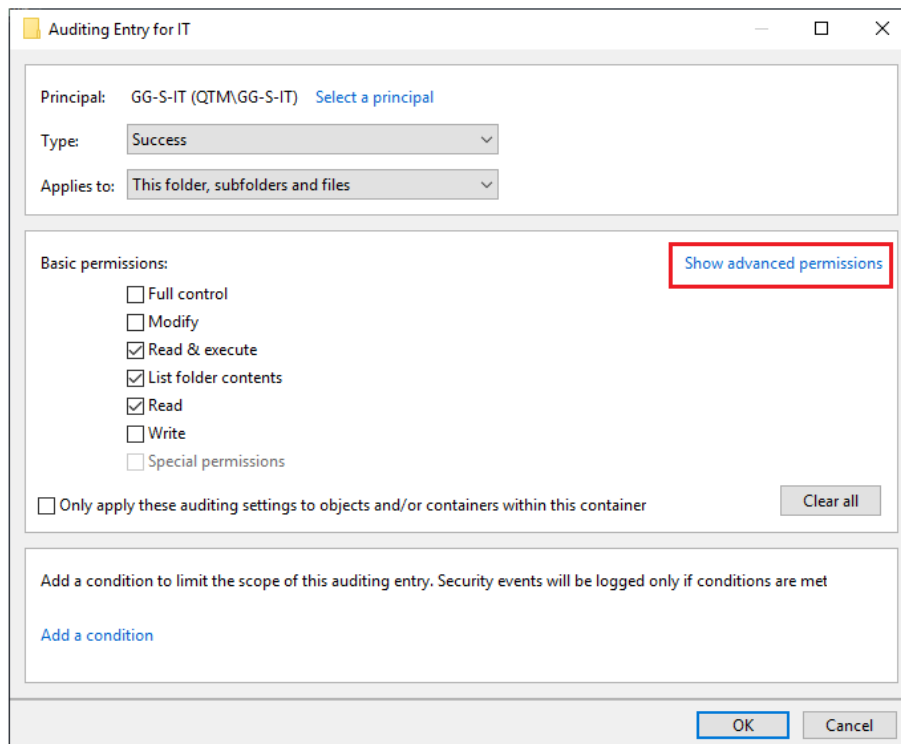
Bước 5. Tại cửa sổ **Auditing Entry for IT**, click vào dòng chữ màu xanh **Select a principal**.



Bước 6. Tại cửa sổ **Select User, Computer ...** thêm vào group **GG_S_IT**.



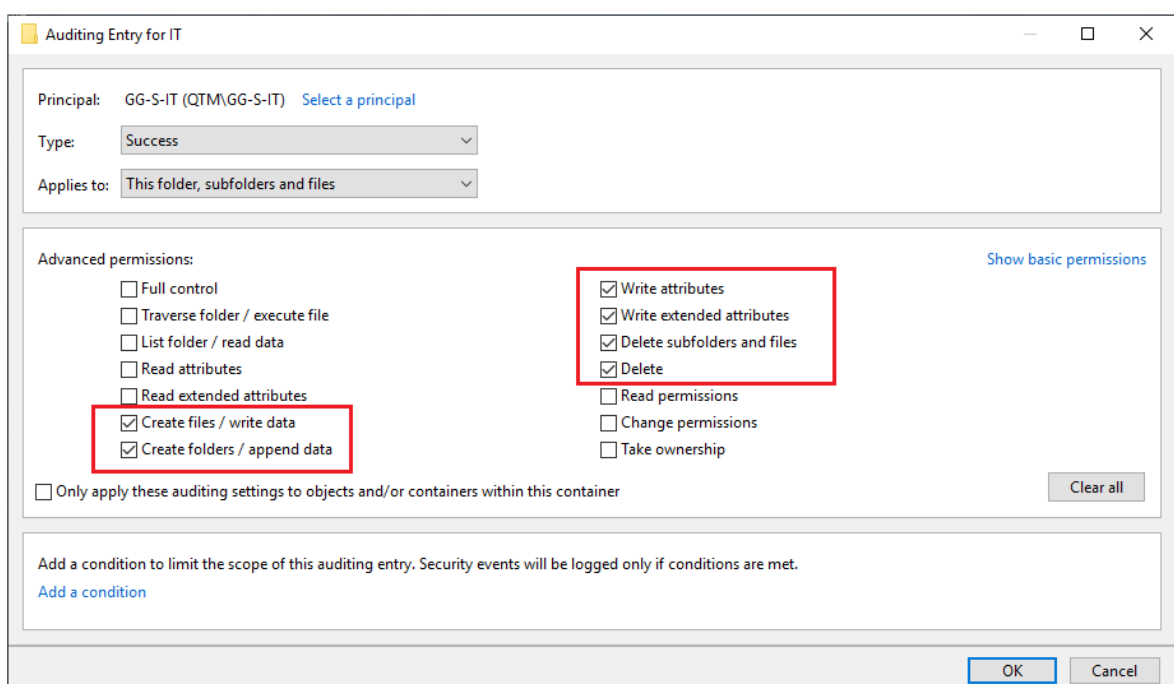
Bước 7. Tại cửa sổ **Auditing Entry for IT**, chọn vào dòng chữ xanh **Show advanced permissions**.



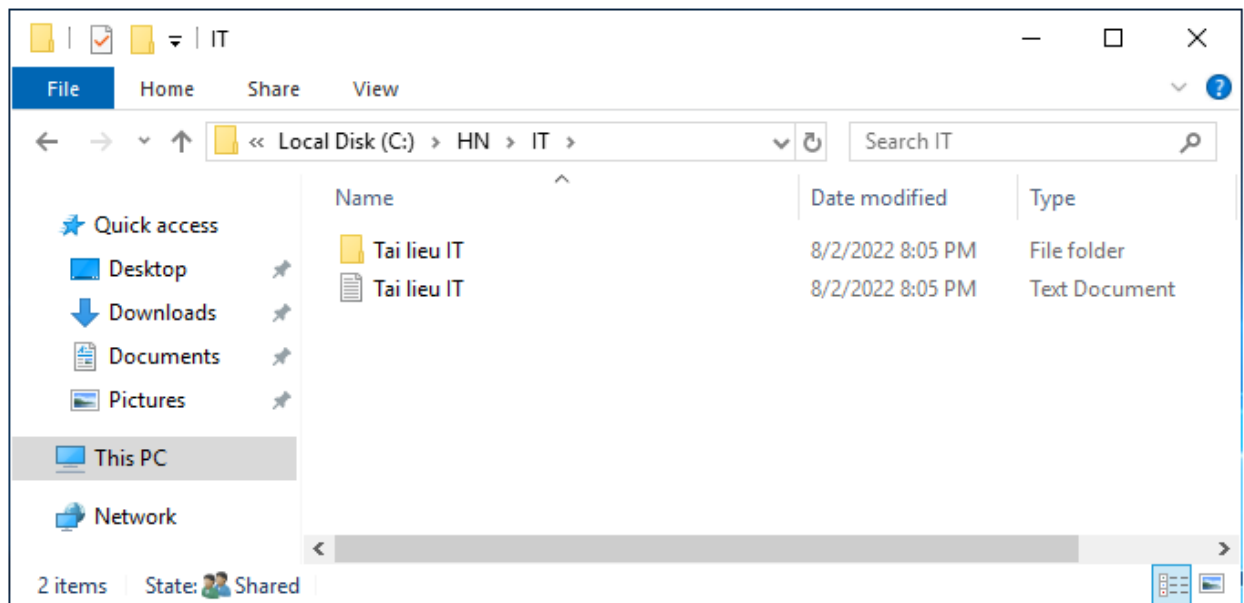
Bước 8. Tại cửa sổ **Advanced permissions**, bỏ chọn các quyền đã được tích dấu, chọn vào các quyền sau:

- Create file / write data
- Create folders / append data
- Write attributes
- Write extended attributes
- Delete subfolder
- Delete

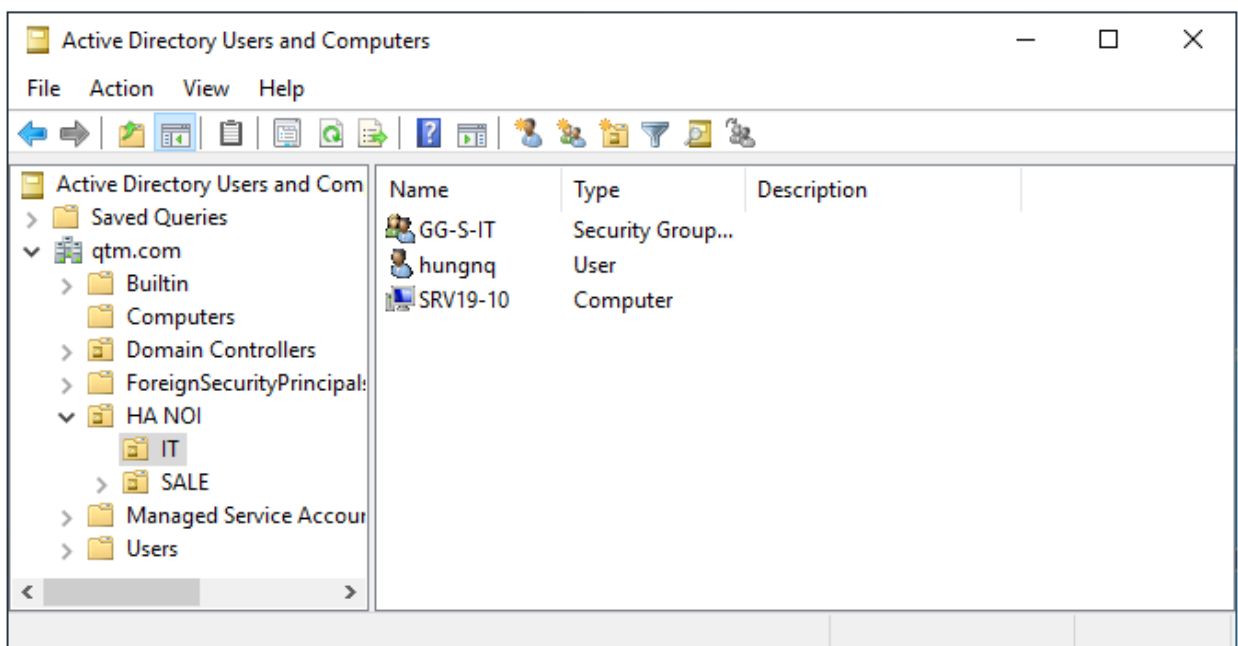
Sau đó, chọn **OK**.



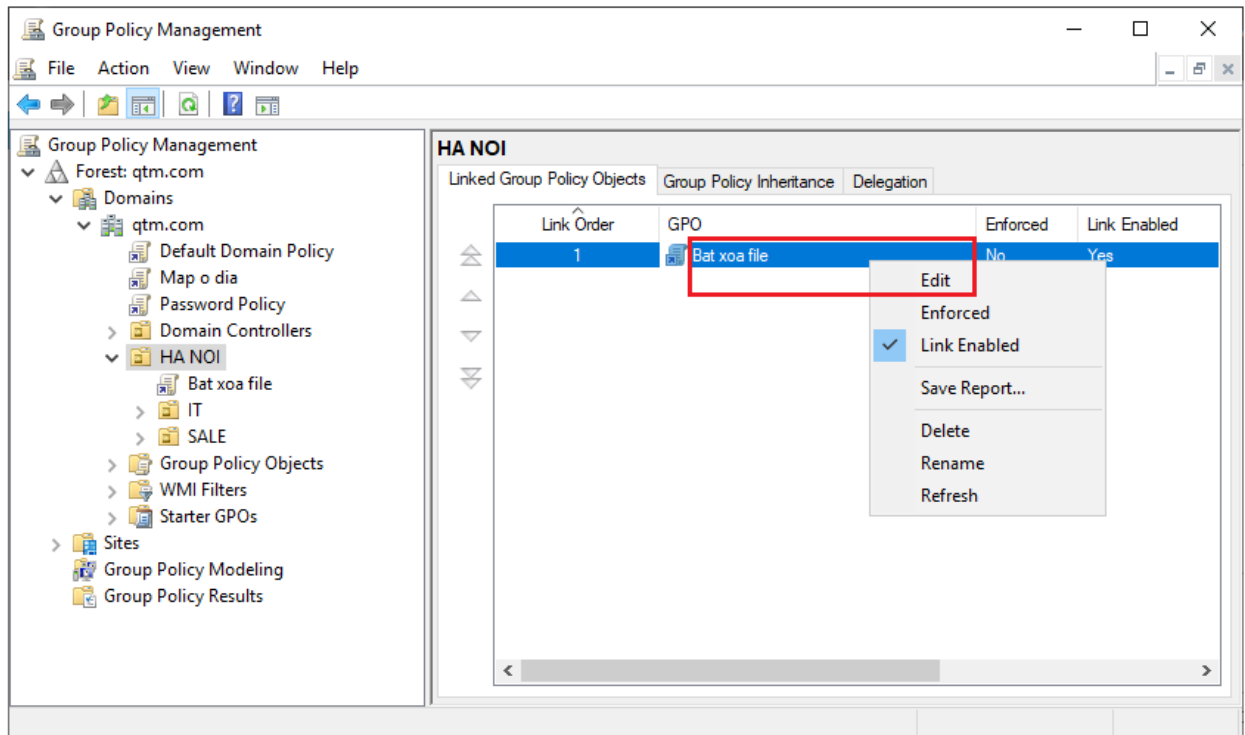
Bước 9. Trong thư mục **IT**, tạo các thư mục và các file con để kiểm tra.



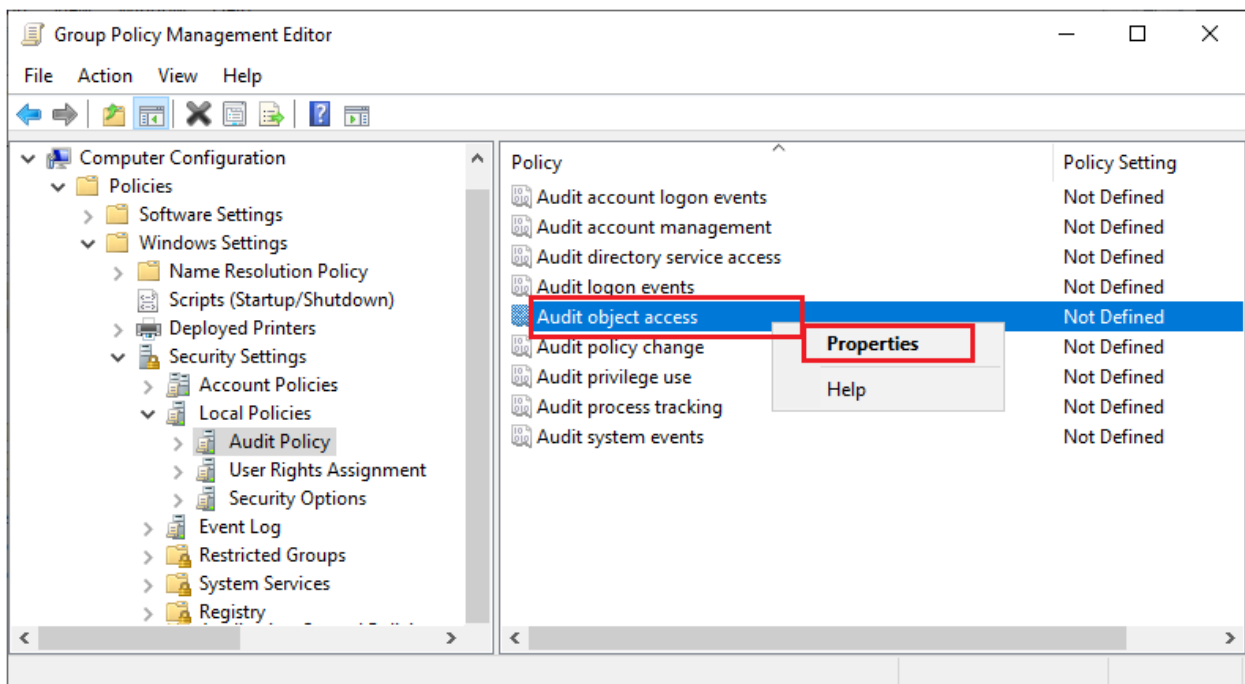
Bước 10. Chuyển sang máy **SRV19-DC-01** triển khai chính sách ghi lại hoạt động của thư mục. Vào dịch vụ **Active Directory User and Computer**, di chuyển máy **SRV19-10** vào OU **IT**.



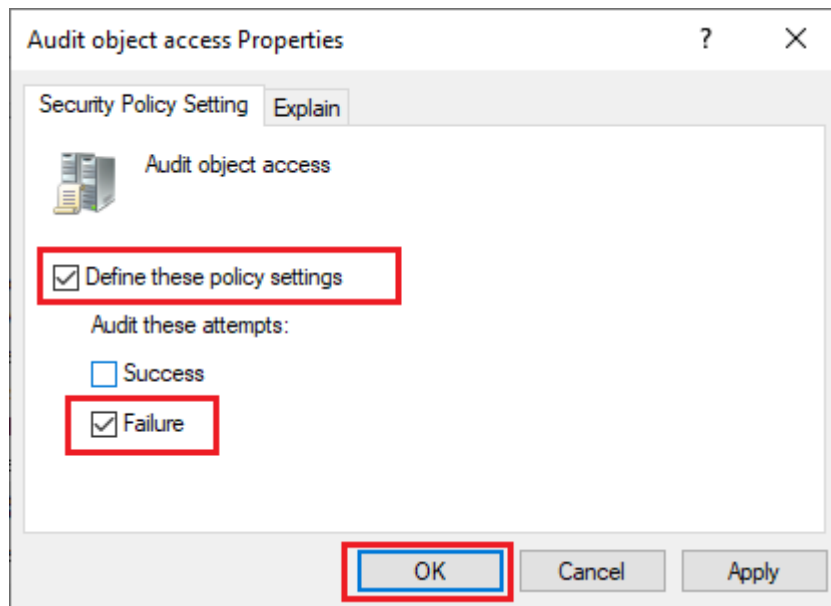
Bước 11. Triển khai chính sách xóa File trong các phòng ban: Vào **Group Policy Management**. Tại OU HANOI, tạo 1 chính sách tên “*bắt xóa file*”. Click chuột phải tại chính sách vừa tạo, chọn **Edit**.



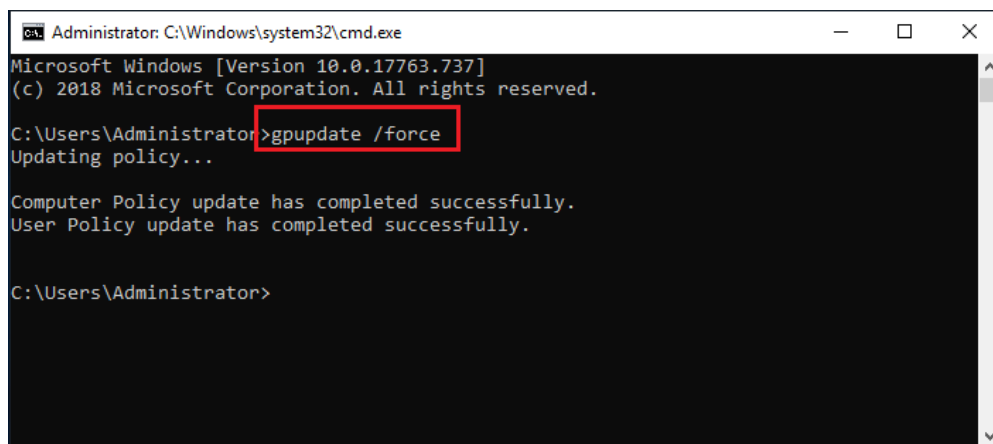
Bước 12. Trong cửa sổ **Group policy Management Editor**, click vào **Computer Configuration / Policies / Windows Settings / Security Settings / Local Policies / Audit Policy**. Chọn chính sách **Audit object access**. Click chuột phải tại chính sách này, chọn **Properties**.



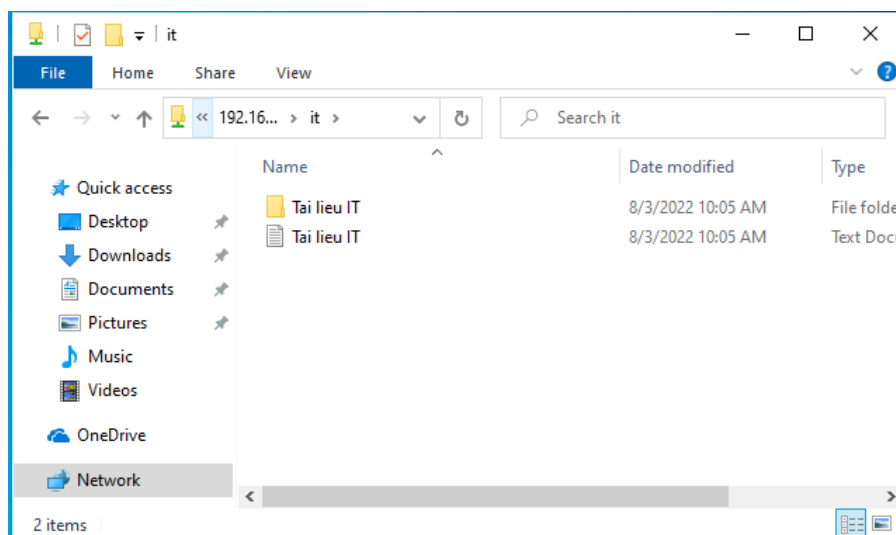
Bước 13. Tại cửa sổ **Audit object access Properties**, click chọn vào **Define these policy settings** và 2 tùy chọn **Success**, **Failure**. Sau đó, chọn **Apply**, chọn **OK**.

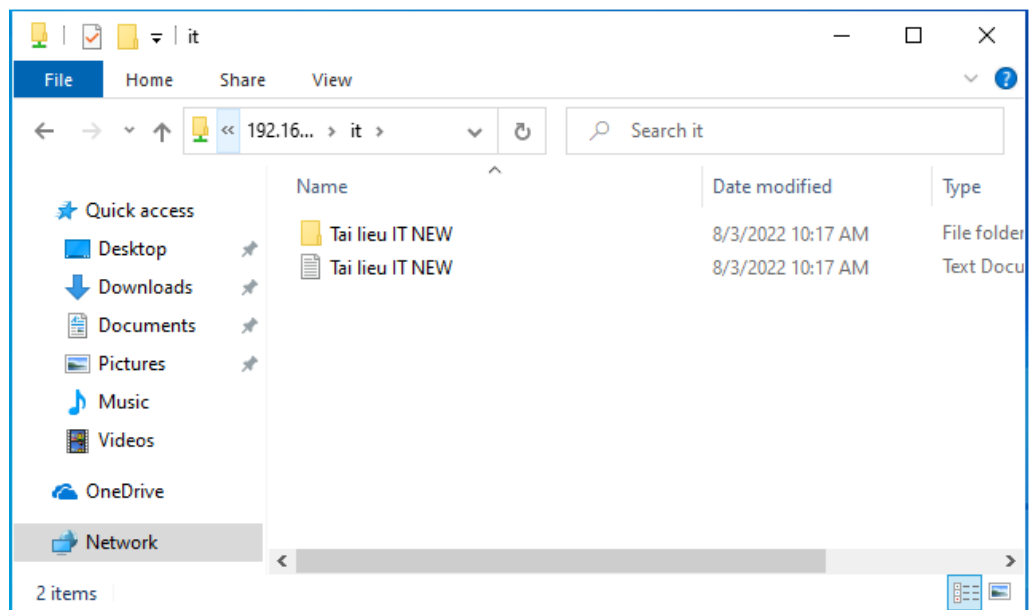


Bước 14. Sử dụng lệnh **gpupdate /force** trong **cmd** để áp dụng chính sách.



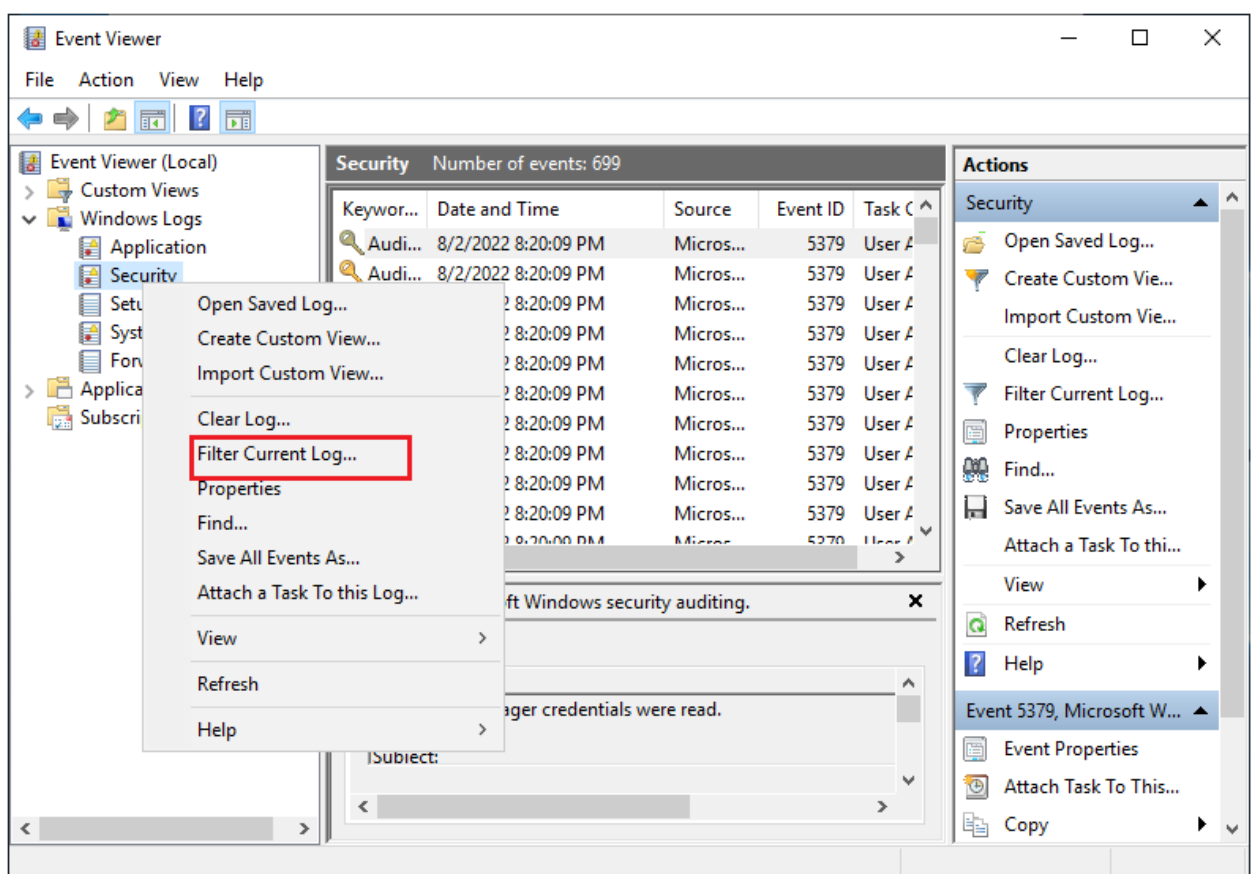
Bước 15. Chuyển sang máy **Client01** đăng nhập bằng tài khoản **hungnq** trong phòng ban **IT**, truy cập vào thư mục **IT**, xóa file cũ, tạo file mới.





Bước 16. Chuyển sang máy **SRV19-10** kiểm tra xóa file.

- Vào **Event Viewer**.
- Trong cửa sổ **Event Viewer**, click chọn **Windows Log / Security**.
- Click chuột phải tại **Security** / chọn **Filter Current Log**.



Bước 17. Tại cửa sổ **Filter Current Log**, nhập vào ID 5145, tiến hành kiểm tra.

Filter Current Log

Filter XML

Logged: Any time

Event level: ☐ Critical ☐ Warning ☐ Verbose
☐ Error ☐ Information

☒ By log Event logs: Security

☐ By source Event sources:

Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

5145

Task category:

Keywords:

User: <All Users>

Computer(s): <All Computers>

Clear

OK Cancel