

BÁO CÁO THỰC HÀNH

Môn học: Hệ thống tìm kiếm, phát hiện và ngăn ngừa xâm nhập

Tên chủ đề: Triển khai Sophos Endpoint Security

GVHD: Trương Thị Hoàng Hảo

Nhóm: 07

1. THÔNG TIN CHUNG:

Lớp: NT204.P21.ANTT.2

STT	Họ và tên	MSSV	Email
1	Nguyễn Khánh Linh	22520769	22520769@gm.uit.edu.vn
2	Nguyễn Phúc Nhi	22521041	22521041@gm.uit.edu.vn
3	Phạm Thị Cẩm Tiên	22521473	22521473@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:¹

STT	Nội dung	Trang
1	Yêu cầu 1.1	2 – 3
2	Yêu cầu 1.2	3 – 4
3	Yêu cầu 2.1	4 – 16
4	Yêu cầu 2.2	16 – 22
5	Yêu cầu 2.3	22 – 30
6	Yêu cầu 2.4	30 – 40

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

¹ Ghi nội dung công việc, các kịch bản trong bài Thực hành

BÁO CÁO CHI TIẾT

1. Yêu cầu 1.1: Tìm hiểu về Sophos Endpoint Security

- **Sophos Endpoint Security** là một giải pháp bảo mật được thiết kế để bảo vệ các thiết bị (hay endpoint) kết nối với hệ thống và cơ sở hạ tầng của bạn. Giải pháp này bao gồm diệt virus, bảo vệ dữ liệu người dùng, ngăn chặn hacker tấn công và các biện pháp bảo mật nâng cao khác.

a) 1.1a. Trình bày những tính năng chính của Sophos Endpoint Security.

- Sophos Endpoint Security tích hợp nhiều công nghệ bảo mật hiện đại, gồm:
 - Real-time Threat Prevention: Ngăn chặn mã độc, ransomware và các mối đe dọa ngay khi phát hiện.
 - AI-powered Malware Detection: Phát hiện mối đe dọa bằng trí tuệ nhân tạo, kể cả các biến thể chưa được biết đến.
 - Exploit Prevention: Ngăn chặn việc khai thác lỗ hổng phần mềm dù chưa được vá.
 - Ransomware Protection: Phát hiện và ngăn chặn hành vi mã hóa dữ liệu trái phép.
 - Web Filtering: Kiểm soát truy cập Internet, ngăn người dùng truy cập vào trang web độc hại.
 - Application Control: Quản lý quyền chạy ứng dụng trên thiết bị đầu cuối.
 - Device Control: Kiểm soát thiết bị ngoại vi như USB, ổ cứng gắn ngoài.
 - Data Loss Prevention: Bảo vệ dữ liệu quan trọng, ngăn chặn rò rỉ dữ liệu nhạy cảm.
 - Managed Threat Response: Dịch vụ chuyên gia giám sát 24/7, phản hồi và xử lý sự cố.
 - Centralized Management: Quản lý tất cả thiết bị và chính sách bảo mật từ một bảng điều khiển trung tâm trên nền web.

b) 1.1b. Sophos Endpoint Security có những mô-đun nào? Trình bày tính năng chính và ứng dụng của những mô-đun đó.

- Intercept X:
 - Tính năng chính:
 - Ngăn chặn tấn công khai thác
 - Chống ransomware
 - Sử dụng trí tuệ nhân tạo để phát hiện malware chưa biết
 - Phân tích tấn công
 - Ứng dụng: Bảo vệ mạnh mẽ chống lại các tấn công hiện đại như như ransomware, fileless malware và tấn công zero-day.
- Endpoint Detection and Response
 - Tính năng chính:
 - Truy vết, phân tích hành vi mối đe dọa
 - Cung cấp khả năng điều tra và phản ứng khi phát hiện sự cố

- Kết hợp dữ liệu từ endpoint, email, server, firewall
 - Ứng dụng: Dành cho đội ngũ SOC hoặc chuyên viên bảo mật để phân tích sự cố, truy nguyên nguồn gốc tấn công, giảm thời gian phát hiện và xử lý.
- Device Encryption:
 - Tính năng chính:
 - Mã hóa toàn bộ ổ đĩa
 - Quản ký khóa mã hóa từ Sophos Central
 - Tích hợp với BitLocker hoặc FileVault
 - Ứng dụng: Bảo vệ dữ liệu trong trường hợp thiết bị bị mất hoặc đánh cắp.
- Web control:
 - Tính năng chính:
 - Chặn các website độc hại, không phù hợp
 - Cho phép cấu hình chính sách duyệt web theo nhóm người dùng.
 - Ứng dụng: Ngăn người dùng truy cập nội dung độc hại hoặc gây phân tâm trong môi trường làm việc.
- Application Control:
 - Tính năng chính:
 - Cho phép/quản lý danh sách ứng dụng được phép chạy
 - Hạn chế phần mềm không mong muốn hoặc không được phép
 - Ứng dụng: Tăng cường kiểm soát môi trường CNTT, giảm rủi ro phần mềm không được kiểm duyệt.
- Peripheral Control:
 - Tính năng chính:
 - Kiểm soát kết nối của các thiết bị USB, ổ đĩa ngoài, Bluetooth,..
 - Thiết lập quyền truy cập thiết bị theo nhóm hoặc người dùng.
 - Ứng dụng: Ngăn chặn rò rỉ dữ liệu qua thiết bị ngoại vi.
- Data Loss Prevention:
 - Tính năng chính:
 - Giám sát và ngăn chặn rò rỉ dữ liệu nhạy cảm (theo từ khóa, mẫu dữ liệu)
 - Tích hợp với cách kênh truyền dữ liệu như email, upload, USB.
 - Ứng dụng: Bảo vệ dữ liệu quan trọng như thông tin cá nhân, tài chính, hồ sơ y tế.

2. Yêu cầu 1.2: Tìm hiểu về Sophos Central Admin

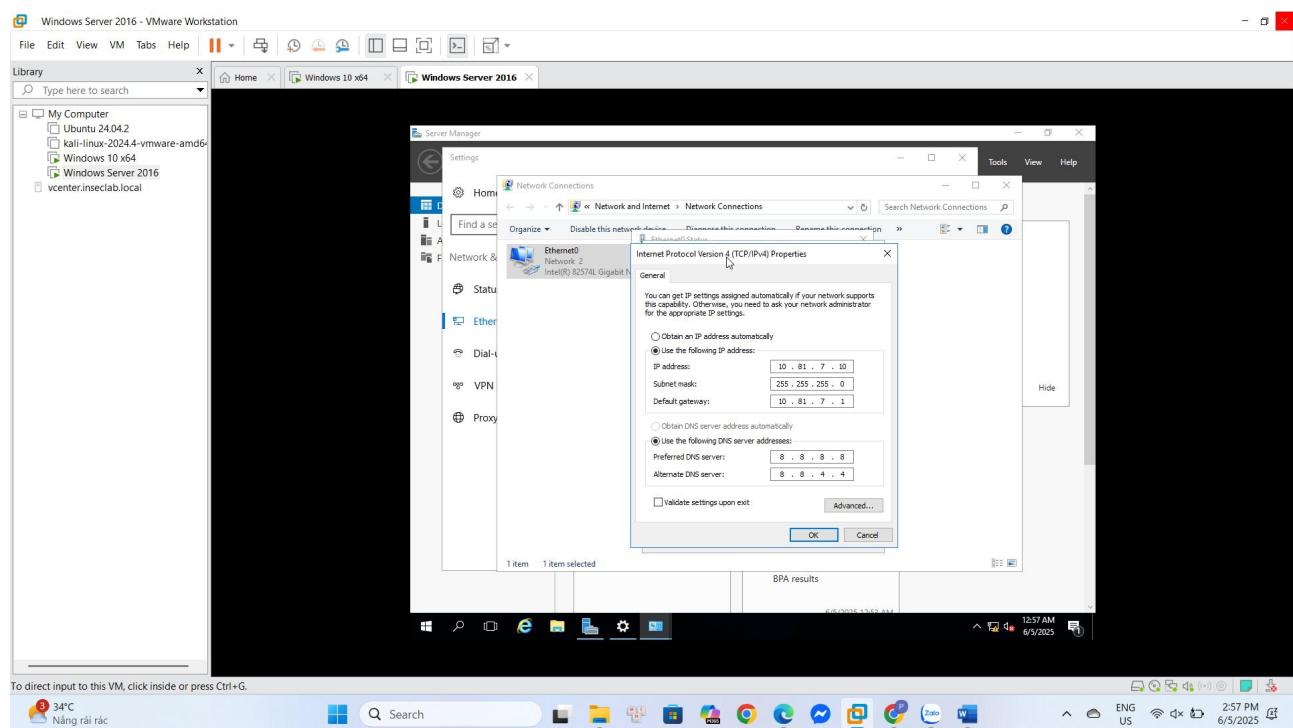
Những tính năng chính của Sophos Central Admin:

- Quản lý thiết bị đầu cuối (Endpoint Protection): Bảo vệ máy tính trước virus, phần mềm độc hại và phân tích hành vi mối đe dọa, tự động cách ly thiết bị bị nhiễm.
- Bảo mật web và kiểm soát truy cập: Cho phép lọc nội dung web theo nhóm người dùng hoặc thiết bị hoặc ngăn chặn truy cập vào các trang web độc hại, ghi nhật ký hoạt động web để giám sát.

- Bảo mật email (Email Security): Chống spam, phishing, mã độc đính kèm, tính năng Advanced Threat Protection (ATP) và sandboxing phát hiện mối đe dọa nâng cao.
- Quản lý thiết bị di động (Mobile Device Management - MDM): Quản lý điện thoại Android và iOS, cấu hình chính sách bảo mật từ xa, mã hóa, khóa và xóa thiết bị bị mất.
- Quản lý người dùng & nhóm: Tích hợp với Active Directory hoặc Azure AD để đồng bộ người dùng, phân quyền quản trị theo vai trò, theo dõi hoạt động người dùng và cảnh báo.
- Tự động hóa và phản ứng sự cố (Threat Response): Tự động cô lập máy tính bị nhiễm khỏi mạng để ngăn lây lan, điều tra nguyên nhân gốc rễ (root cause analysis), phối hợp với các giải pháp khác thông qua Sophos XDR và Data Lake.
- Giao diện quản lý và báo cáo: Bảng điều khiển trực quan, cập nhật theo thời gian thực, báo cáo đầy đủ về trạng thái bảo mật, mối đe dọa, cảnh báo, gửi báo cáo định kỳ qua email.
- Tích hợp và đồng bộ với các sản phẩm Sophos khác: Tích hợp chặt chẽ với Sophos Firewall, Wireless, Server Protection,... chia sẻ thông tin đe dọa giữa các thiết bị để phản ứng nhanh chóng (Synchronized Security).

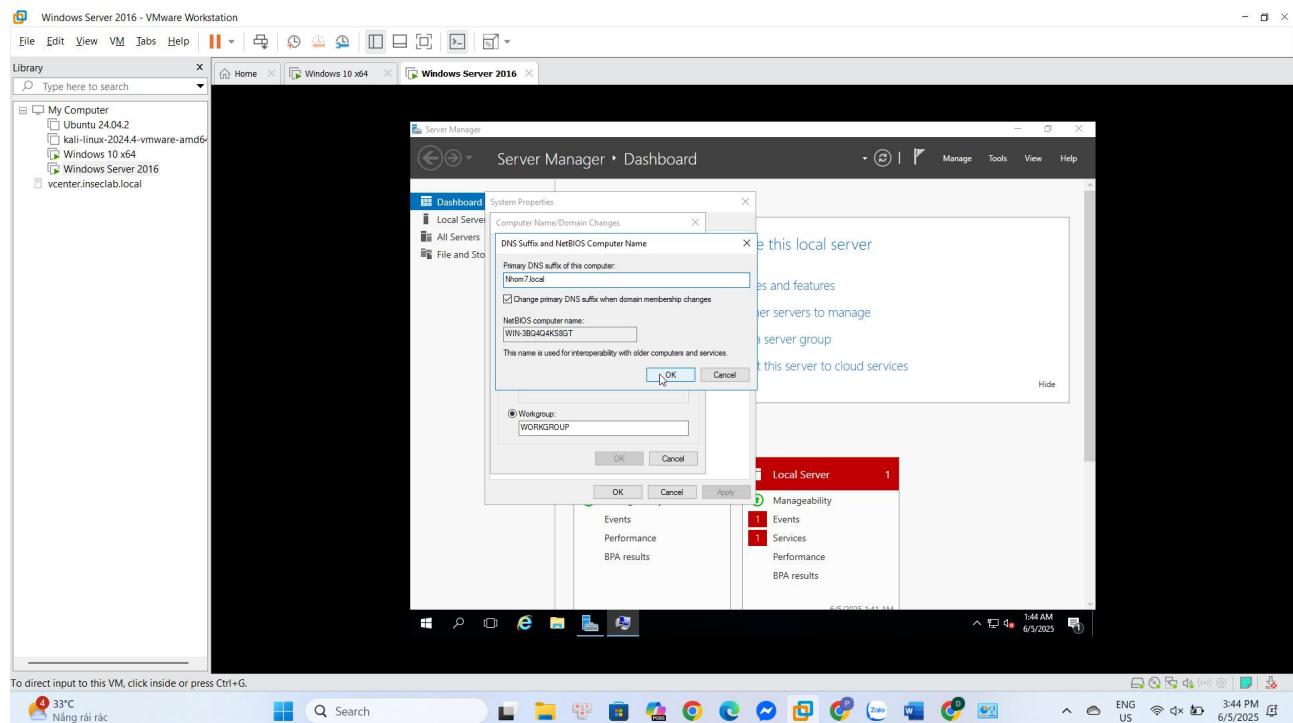
3. Yêu cầu 2.1: Cài đặt AD và kết nối host với domain

Cấu hình địa chỉ IP cho máy AD.



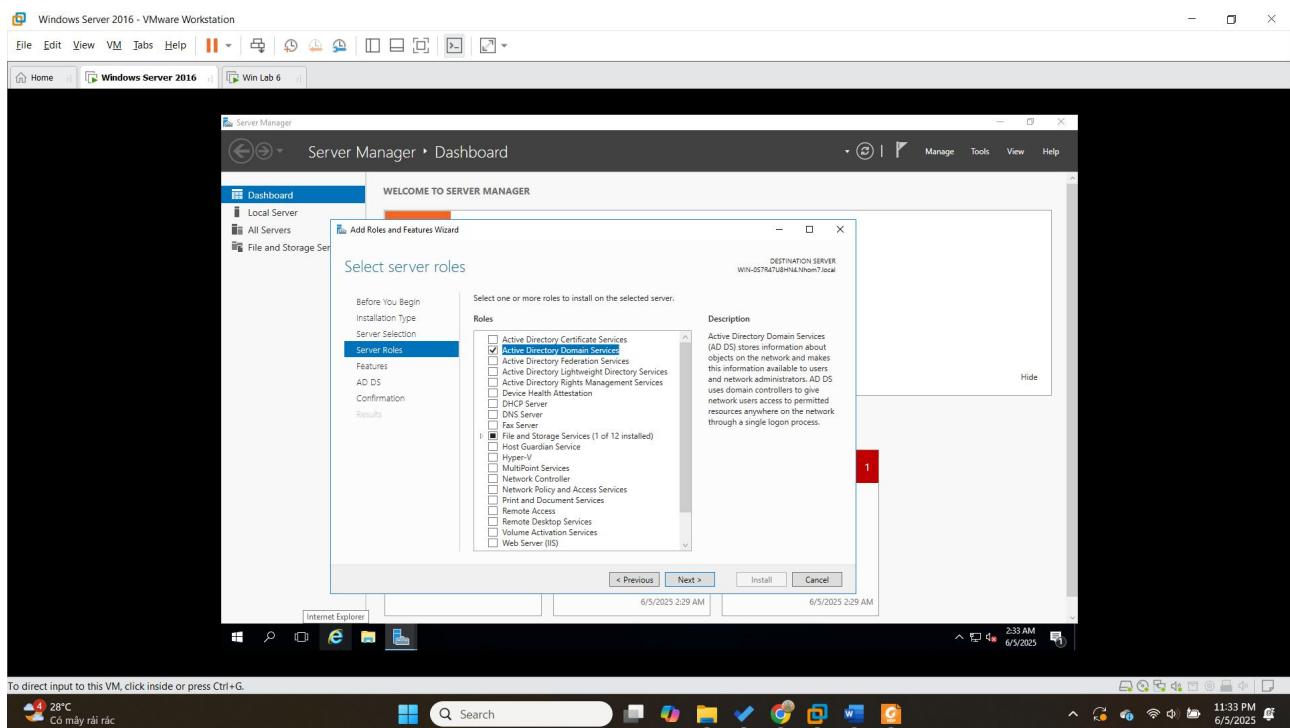
2.1a Cài đặt AD trên máy AD với domain là: nhom7.local.

Đầu tiên, ta thay đổi primary DNS suffix của máy server. Mở Windows + R gõ sysdm.cpl.

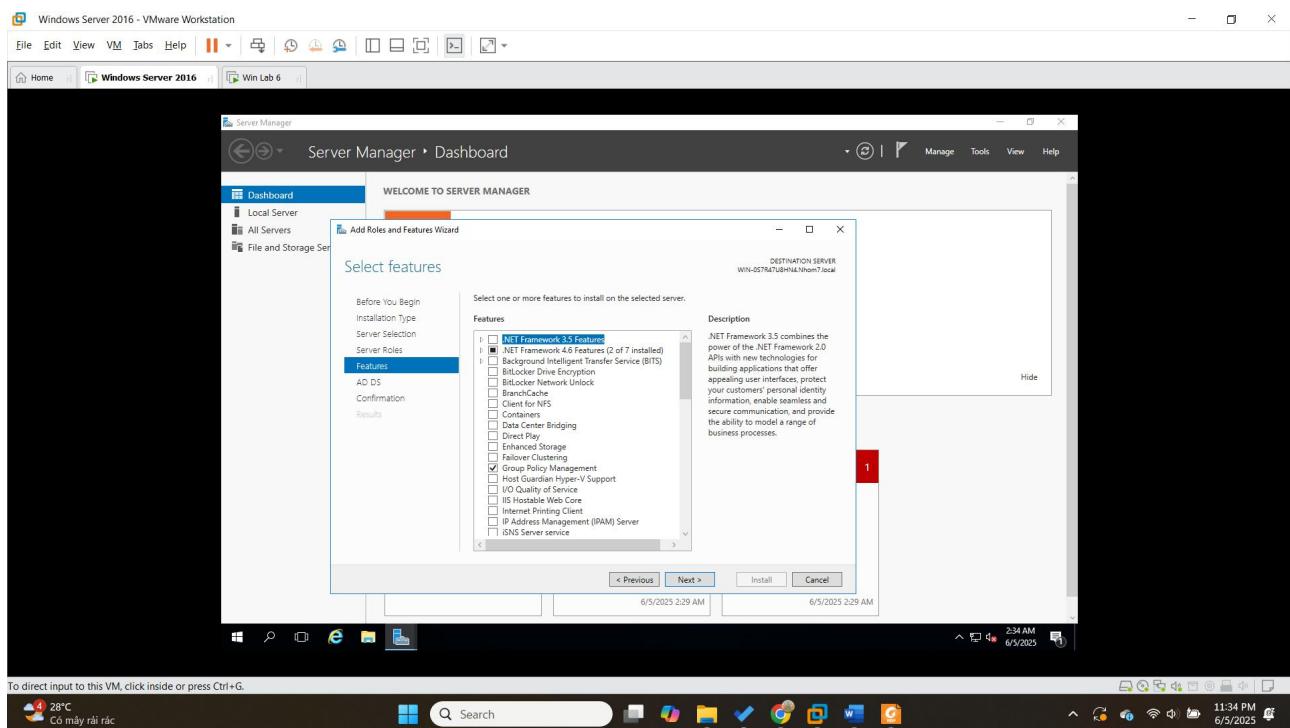


Sau đó, tiến hành thêm roles cho server để có thể nâng cấp nó thành AD:

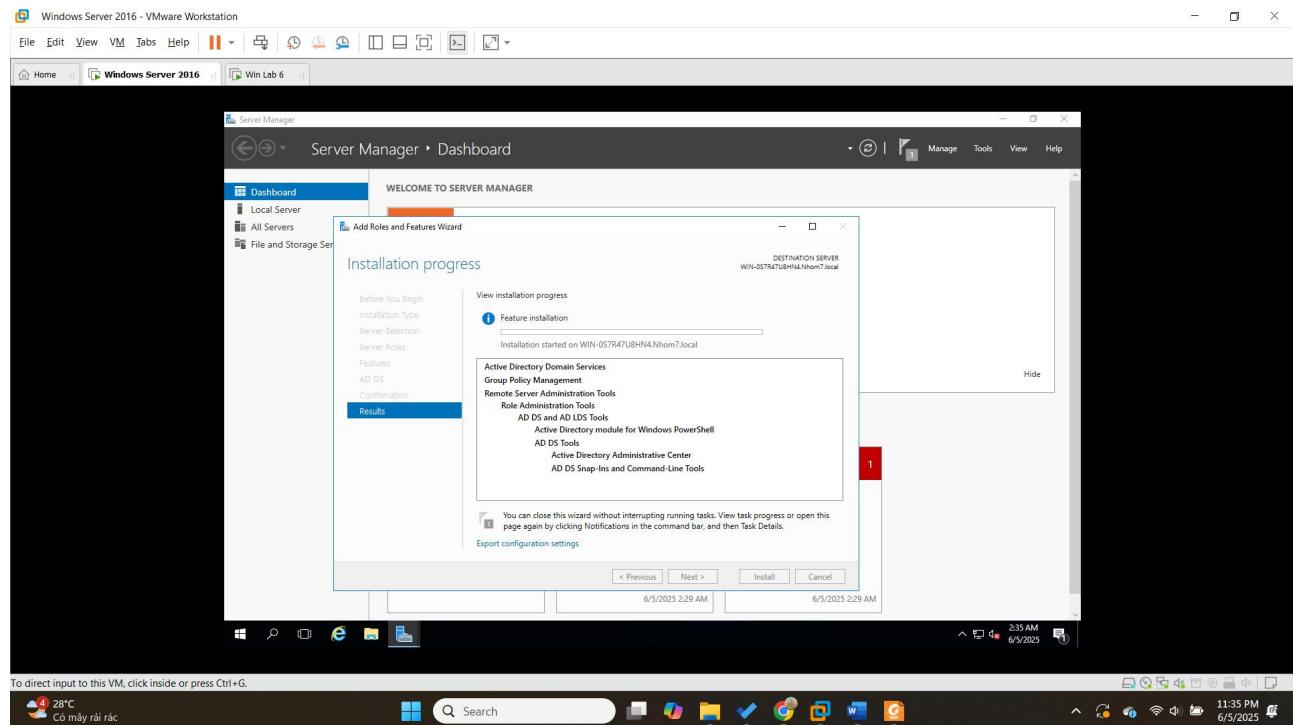
- Vào Server Manager > Manage > Add Roles and Features.
- Chọn Next tại các bước Before You Begin, Installation Type, Server Selection.
- Tại bước Server Roles, chọn Active Directory Domain Services.



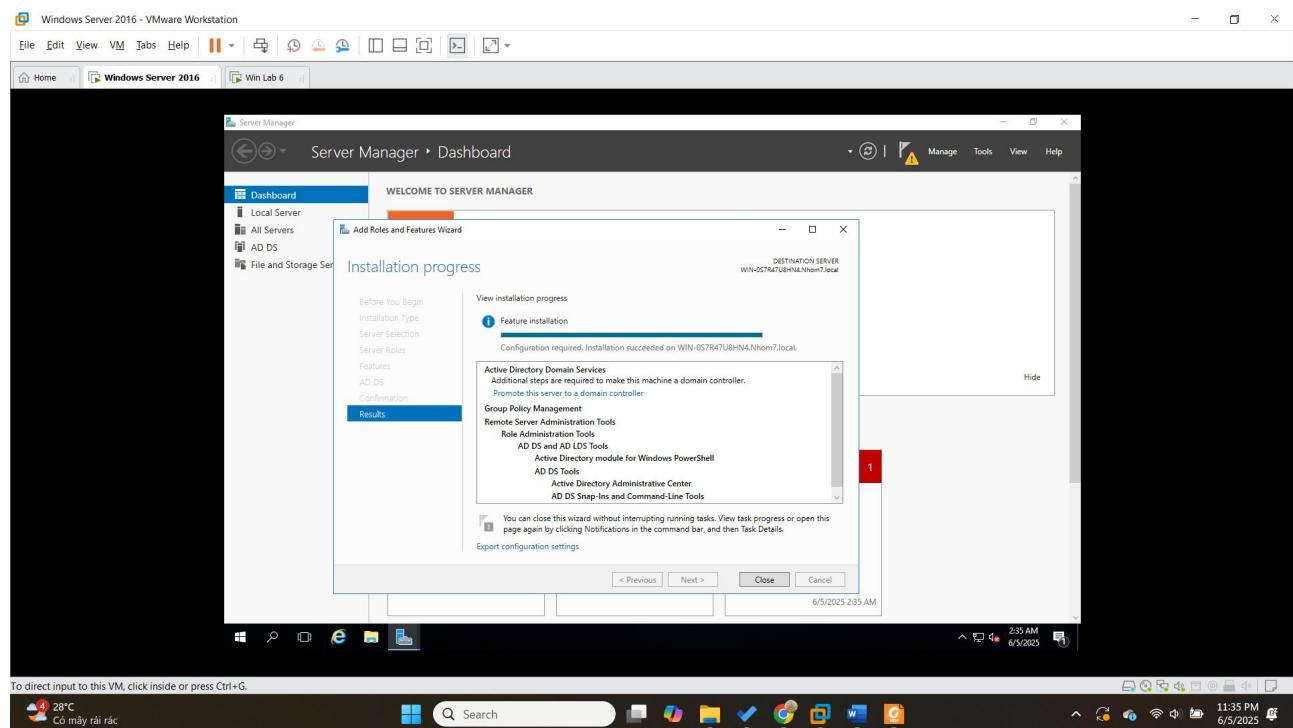
- Ở bước Features, chọn Group Policy Management.



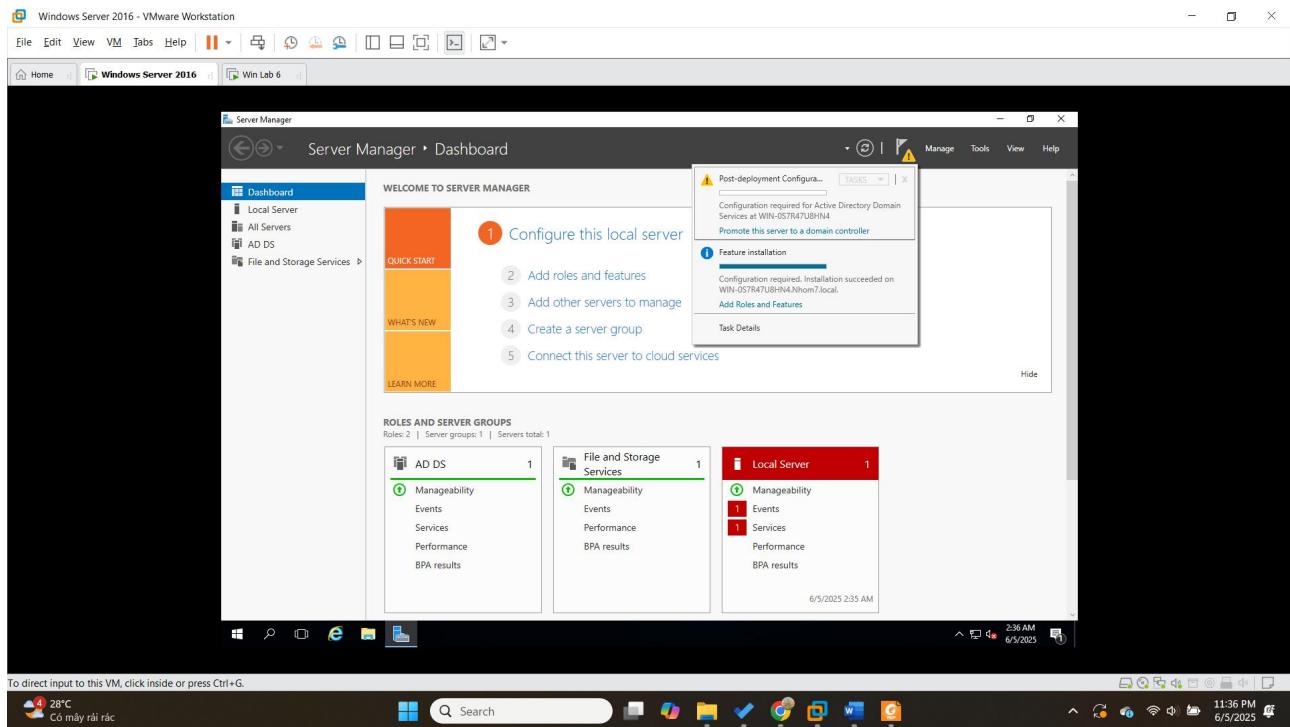
- Ở bước AD DS, chọn Next.
- Ở bước Confirmation, xác nhận lại thông tin và chọn Install.



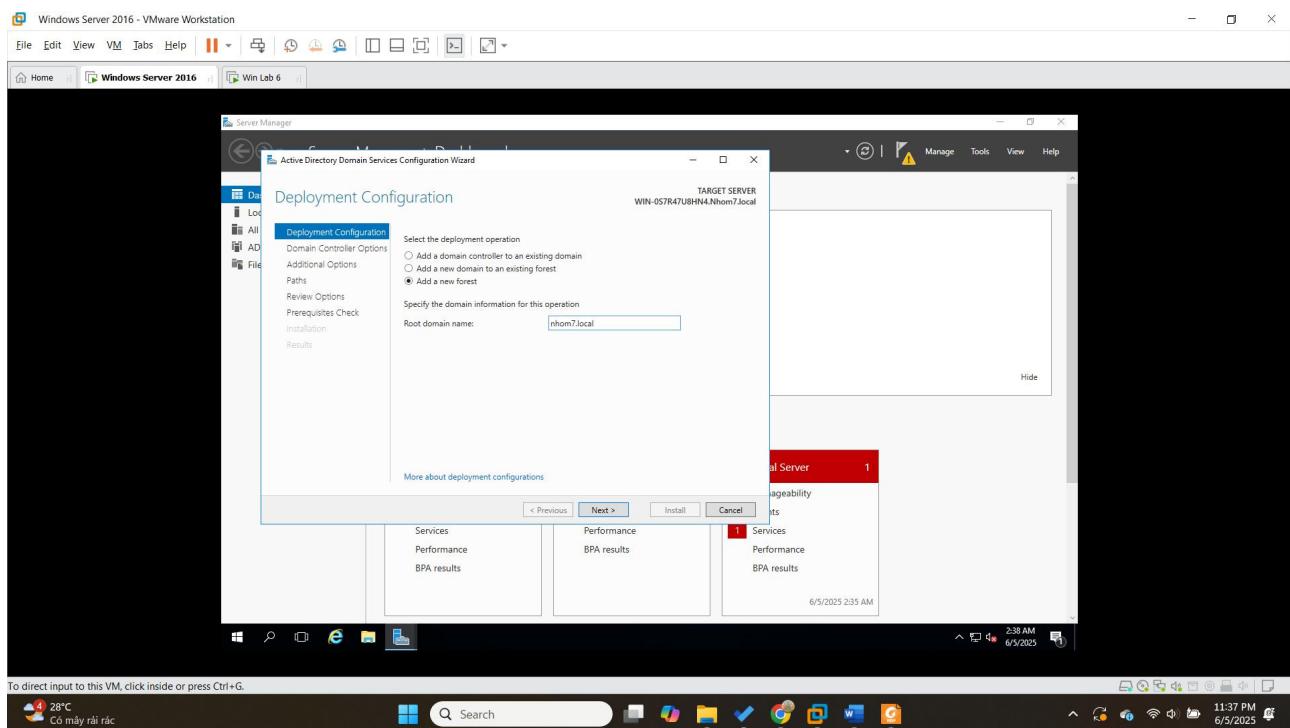
- Chờ quá trình cài đặt hoàn thành và chọn Close để kết thúc.



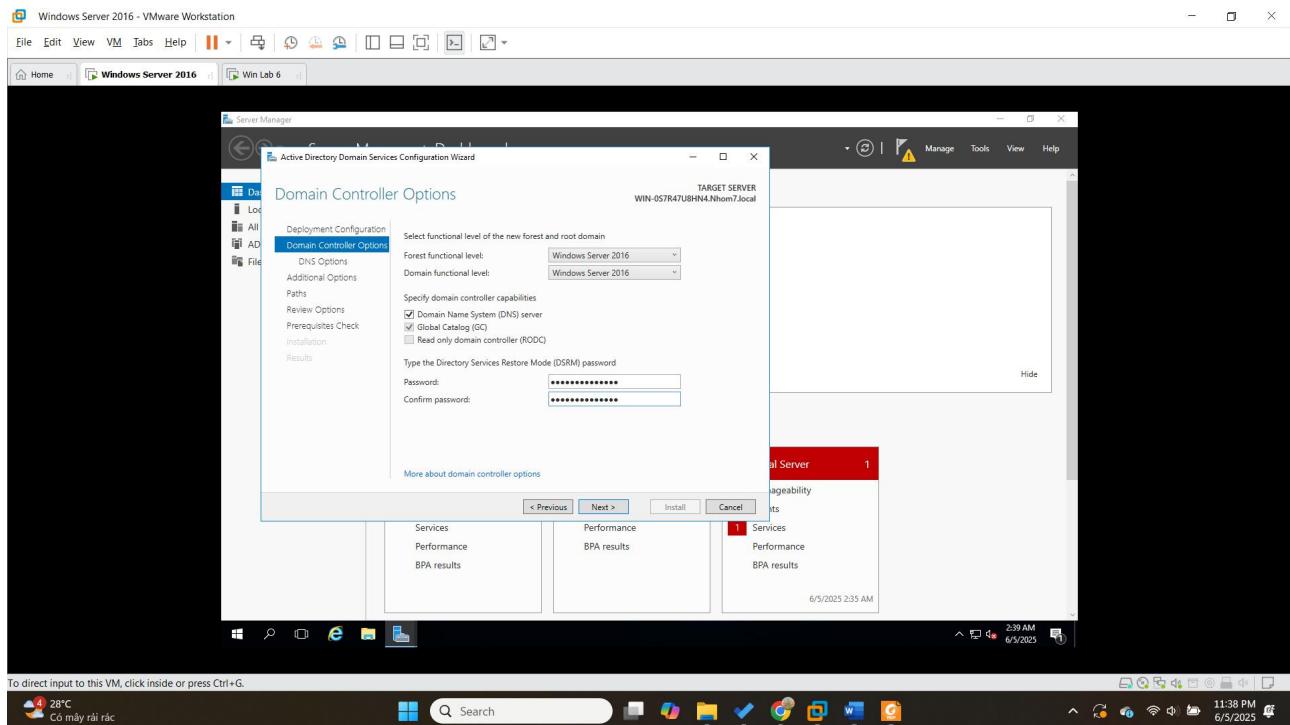
- Vào Server Manager sẽ thấy biểu tượng cảnh báo, nhấp vào và chọn Promote this server to a domain controller.



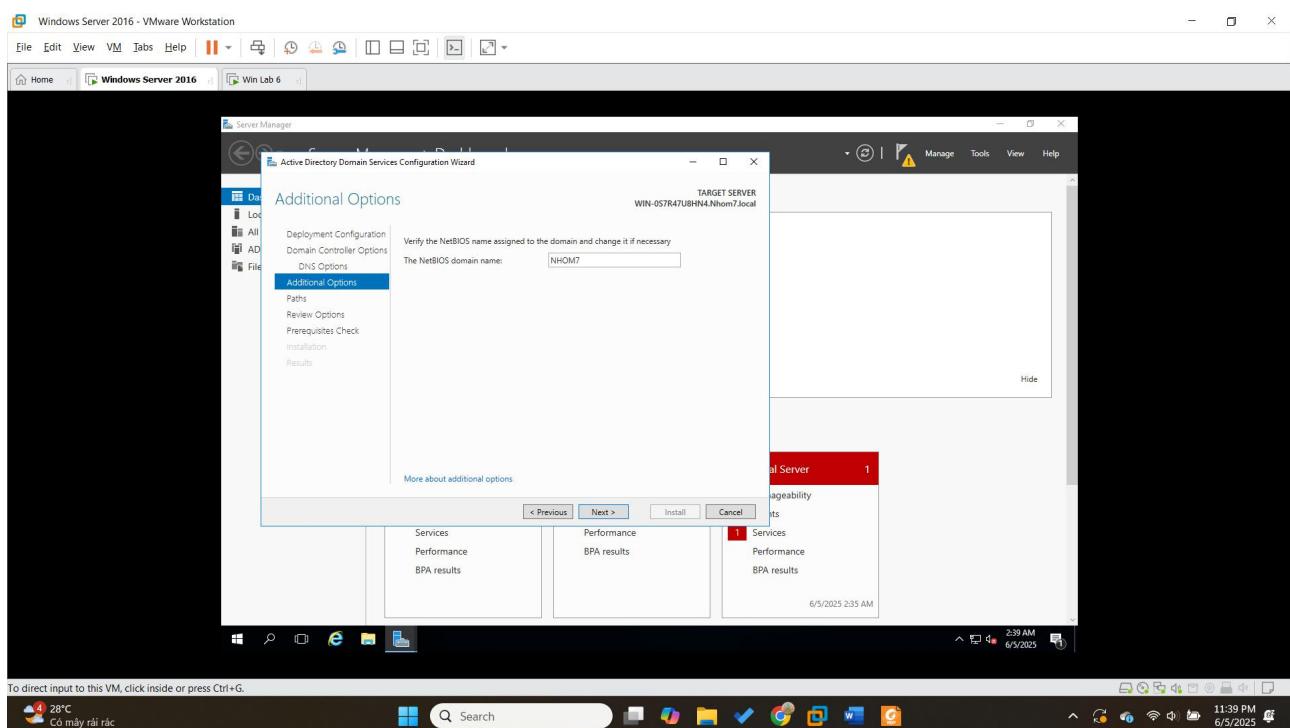
- Đặt tên root domain là tên domain của nhóm.



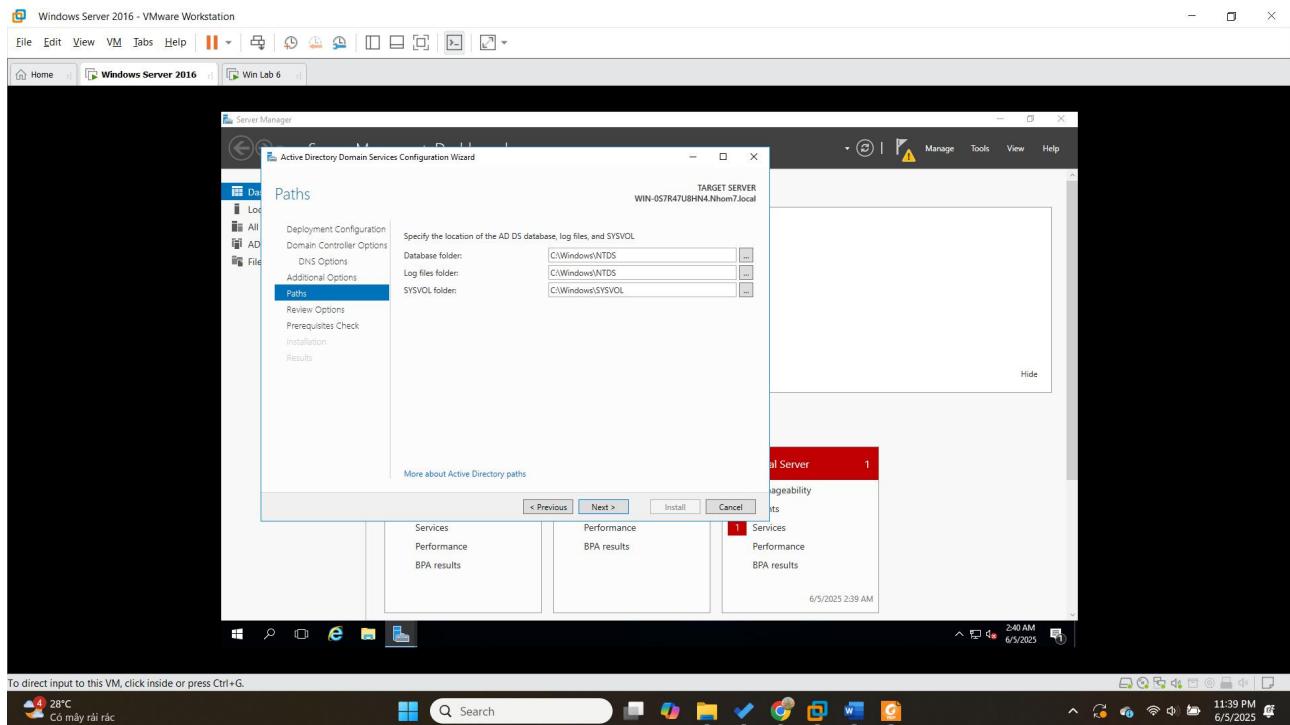
- Thiết lập DSRM password và các thiết lập khác.



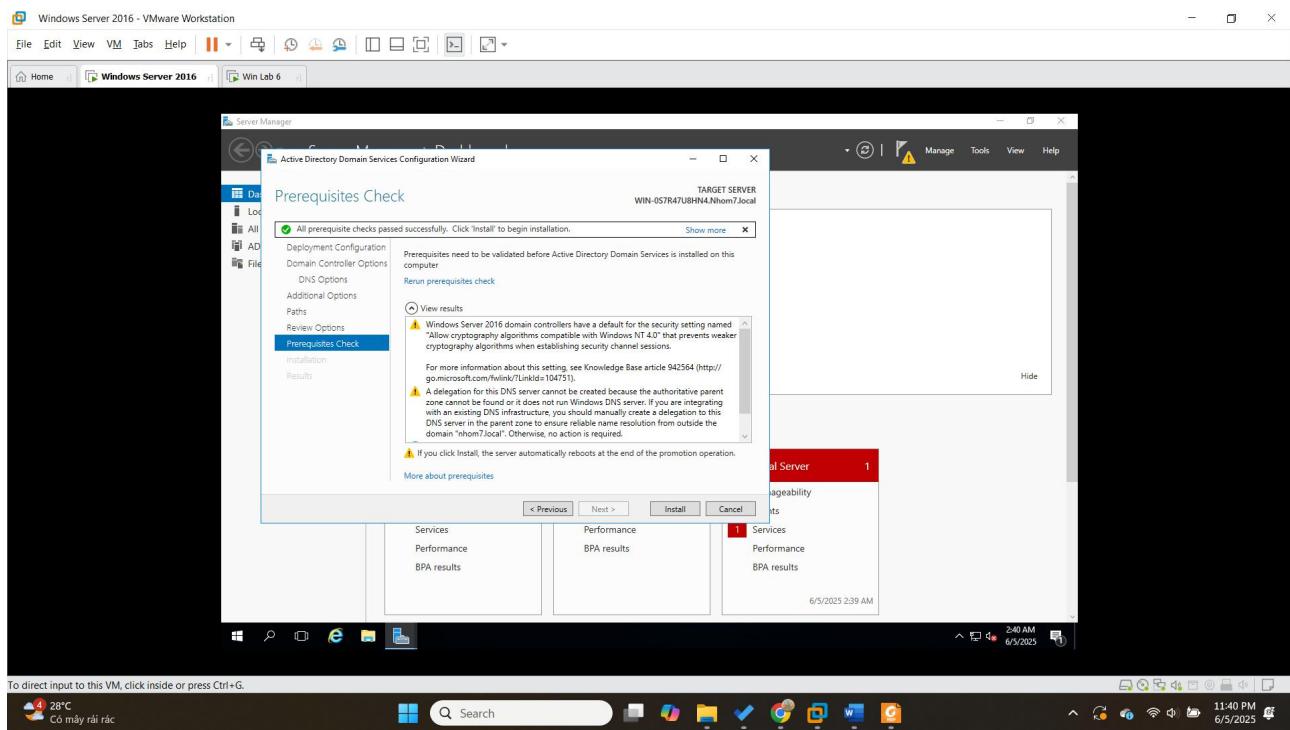
- Thiết lập NetBIOS domain name.

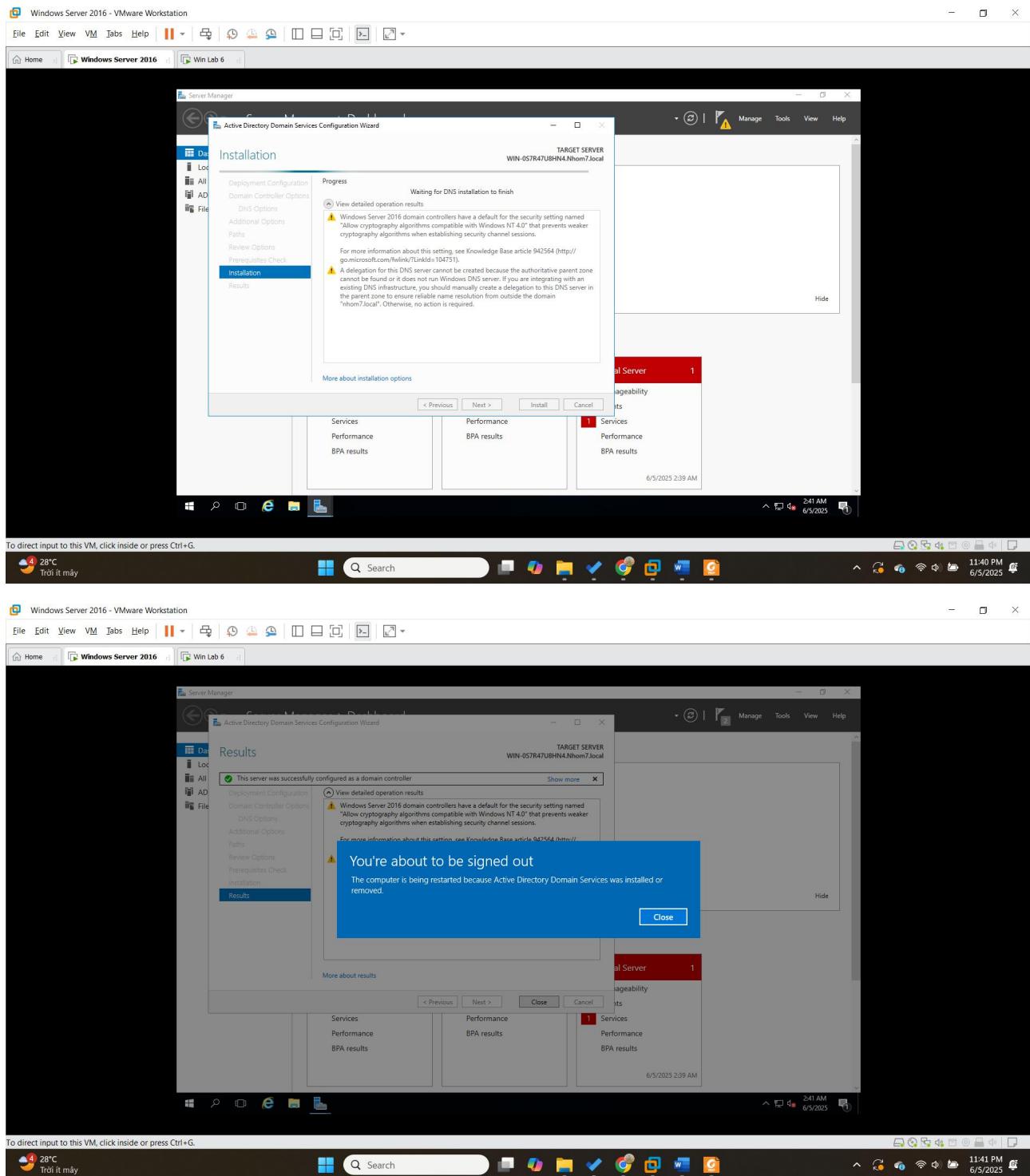


- Giữ nguyên các tùy chỉnh mặc định ở mục Paths.



- Thực hiện bước Prerequisites Check hoàn thành, sau đó chọn Install và chờ quá trình nâng cấp hoàn tất.

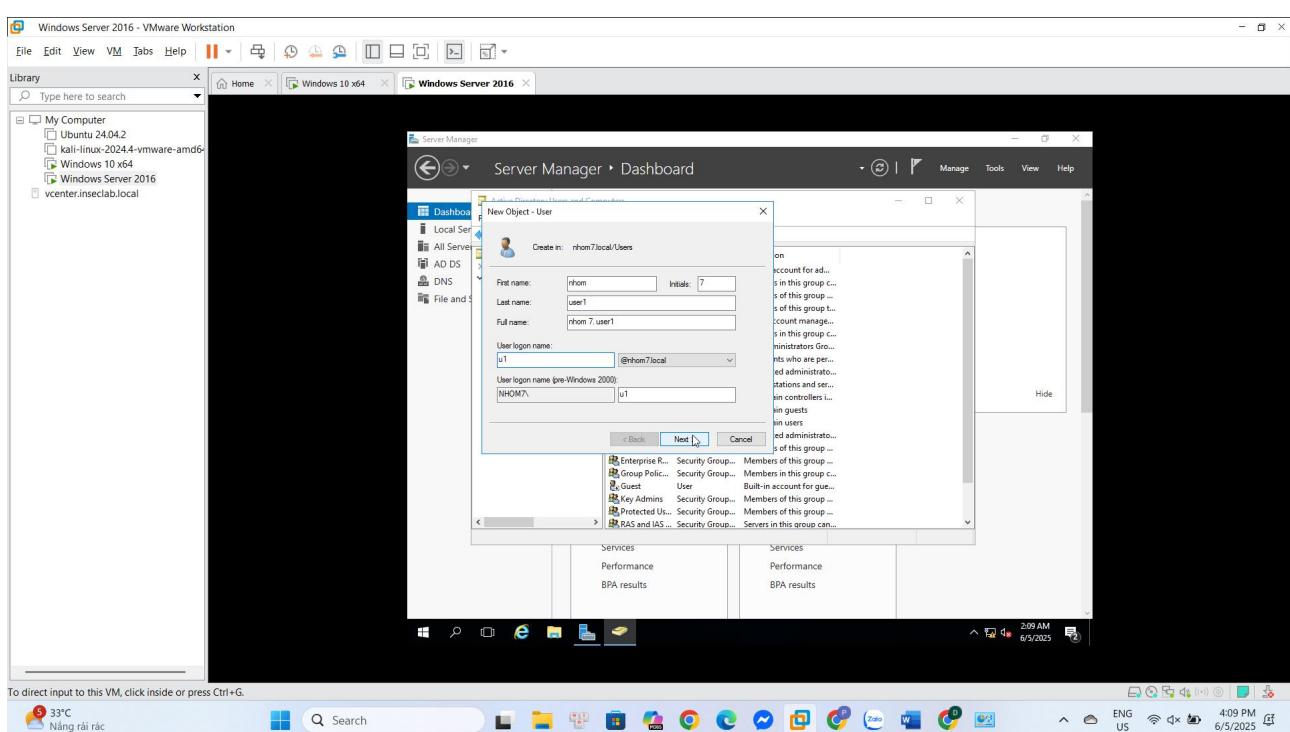
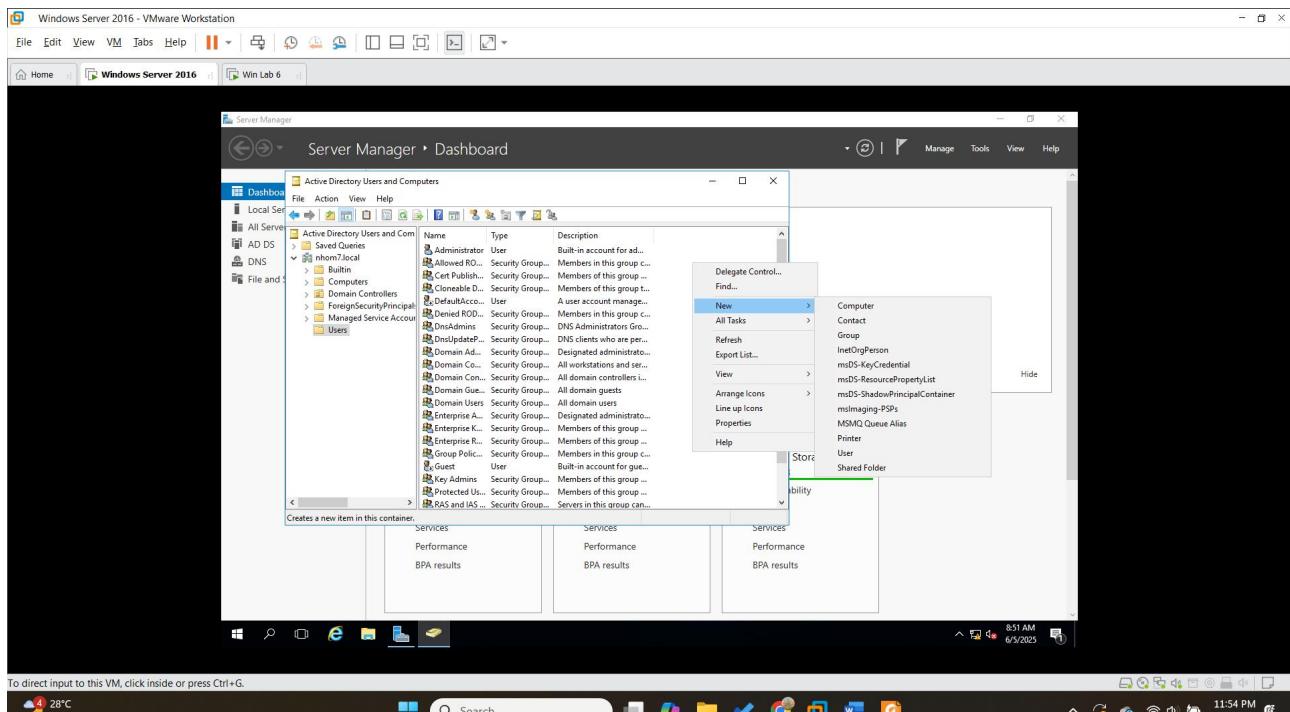




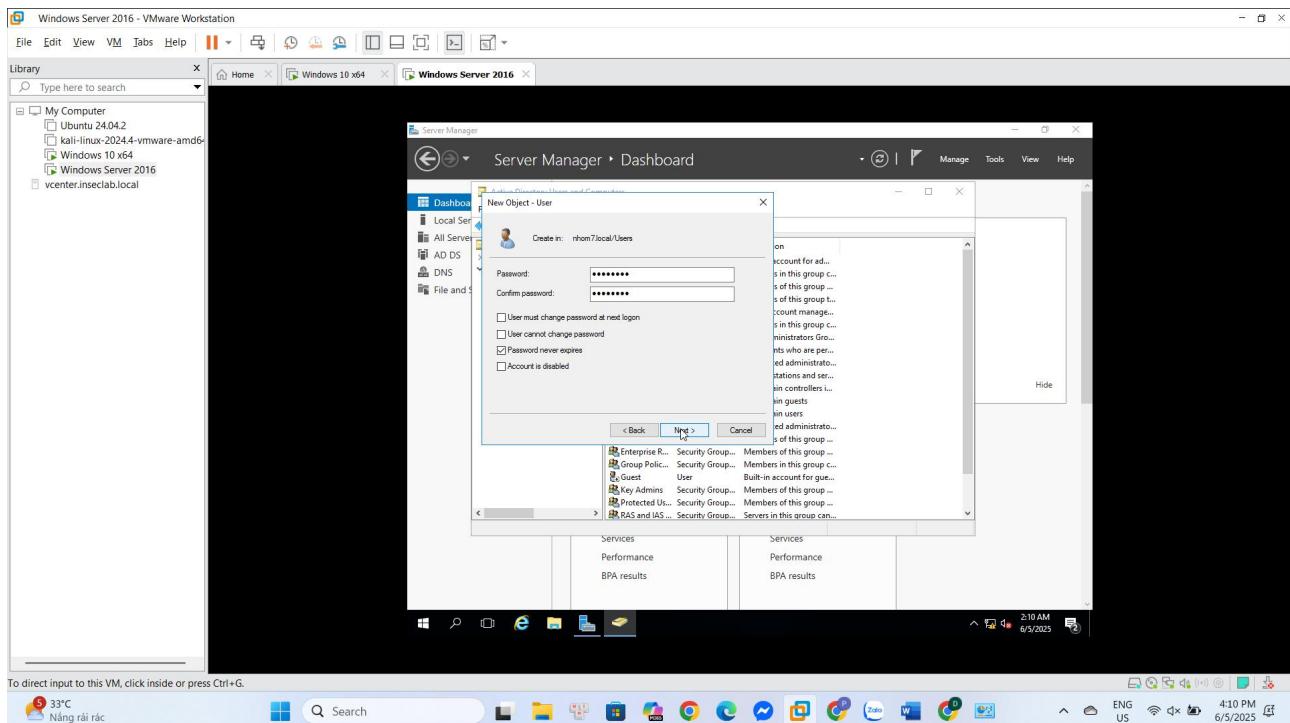
2.1b Tham gia máy Windows 10 vào domain đã tạo với user là u1.

Đầu tiên, ta tiến hành tạo user 1 như hình:

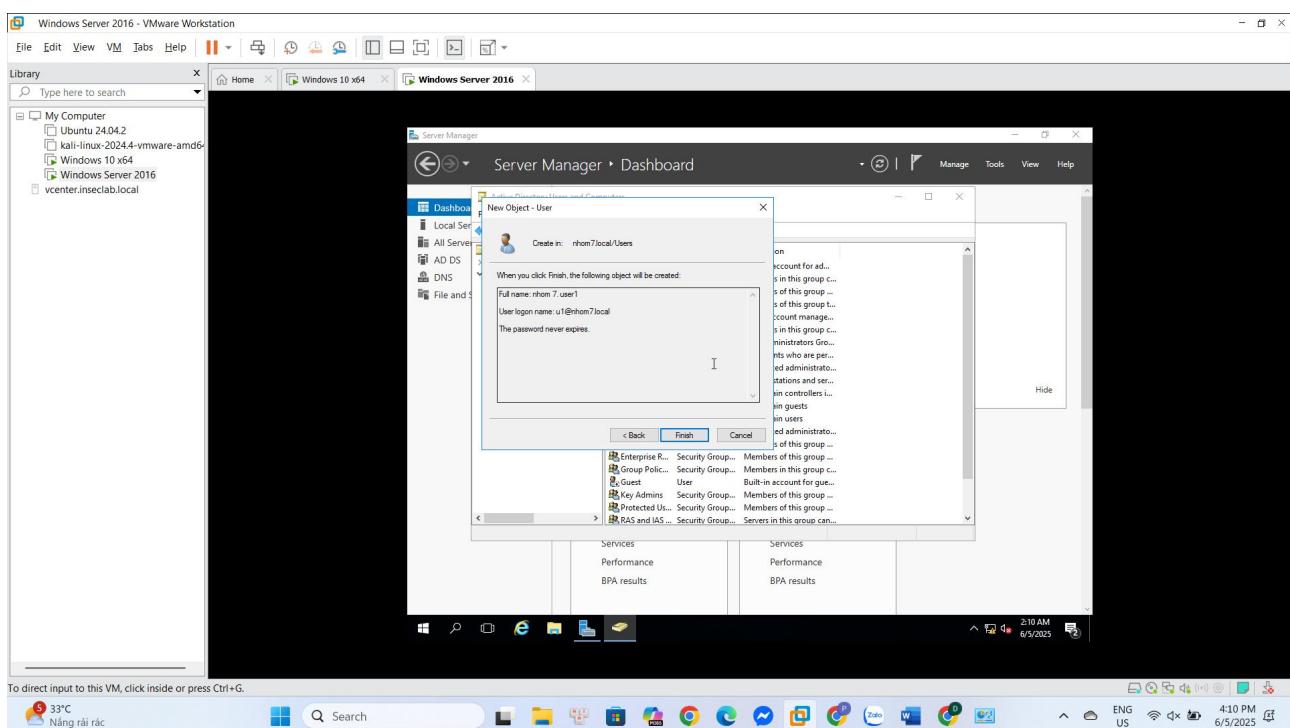
- Server Manager -> Tools -> Active Directory Users and Computers.
- Trong nhom7.local > Users, nhấp chuột phải trong khung hiển thị các user, chọn New > User và nhập thông tin user muốn tạo.



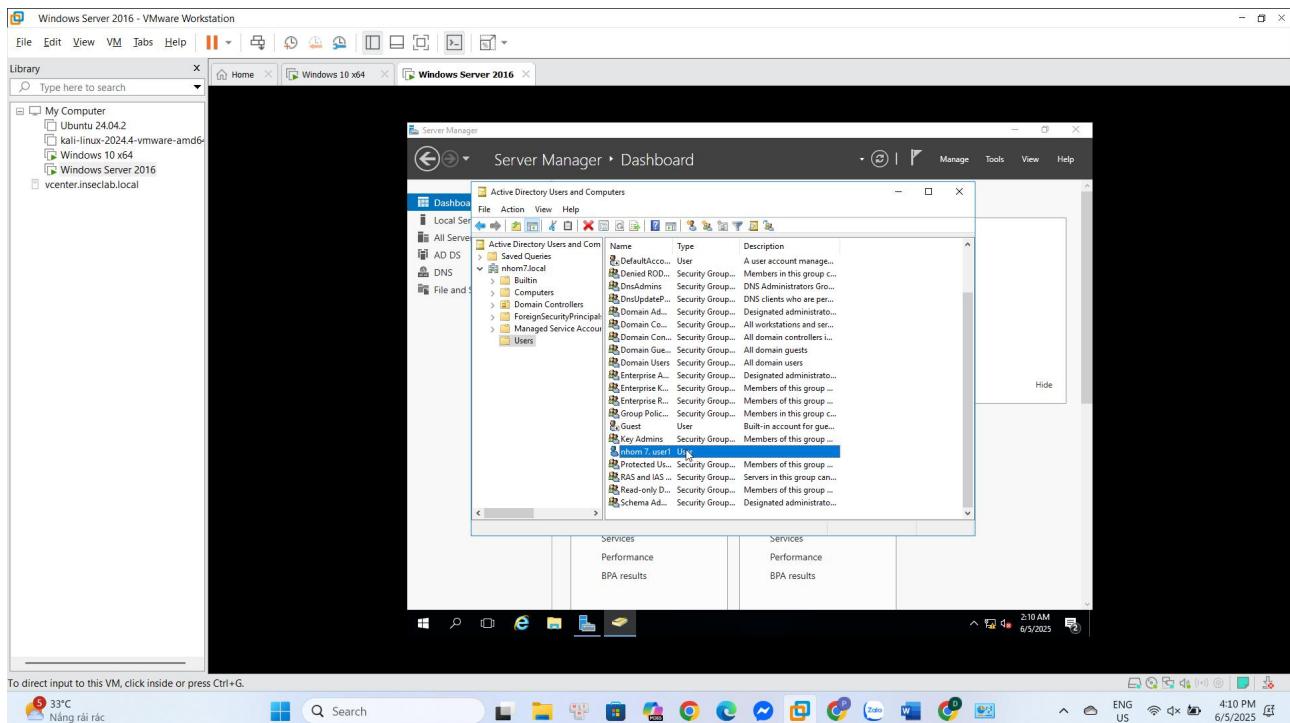
- Nhập mật khẩu và chọn các lựa chọn phù hợp.



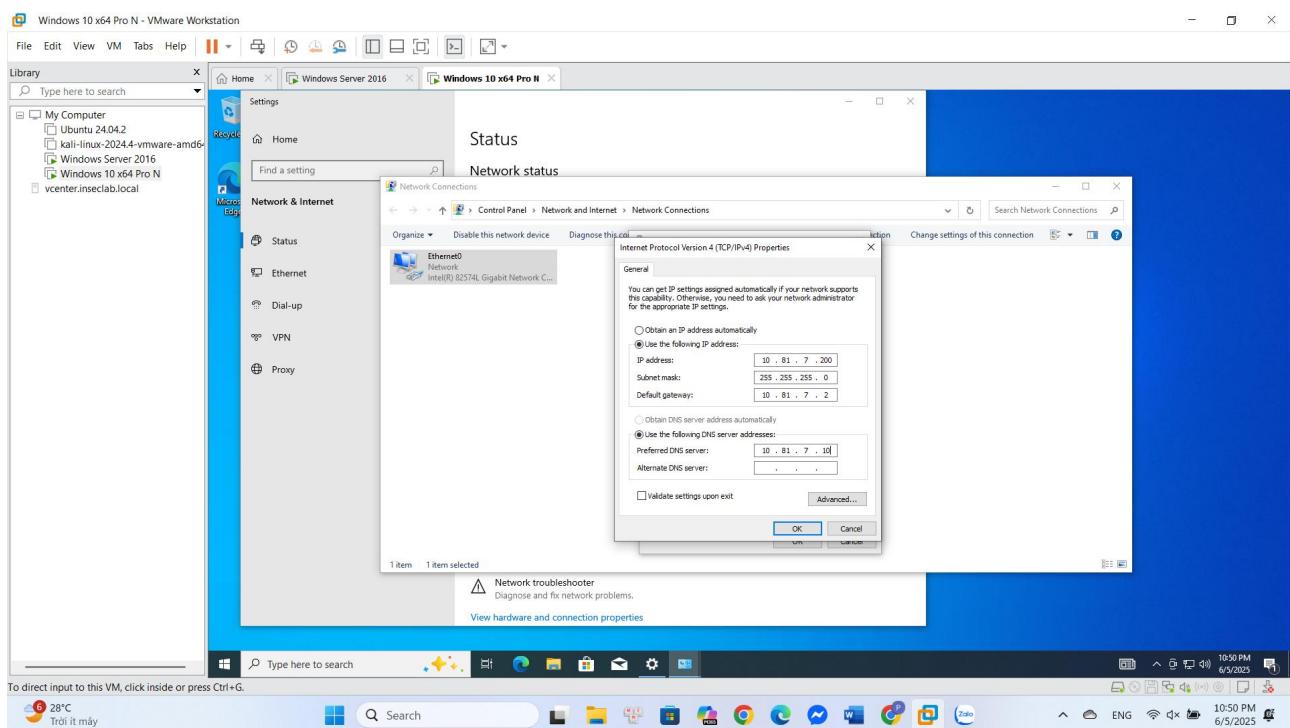
- Nhấn Finish để hoàn thành.



- Ta thấy user 1 đã được tạo.



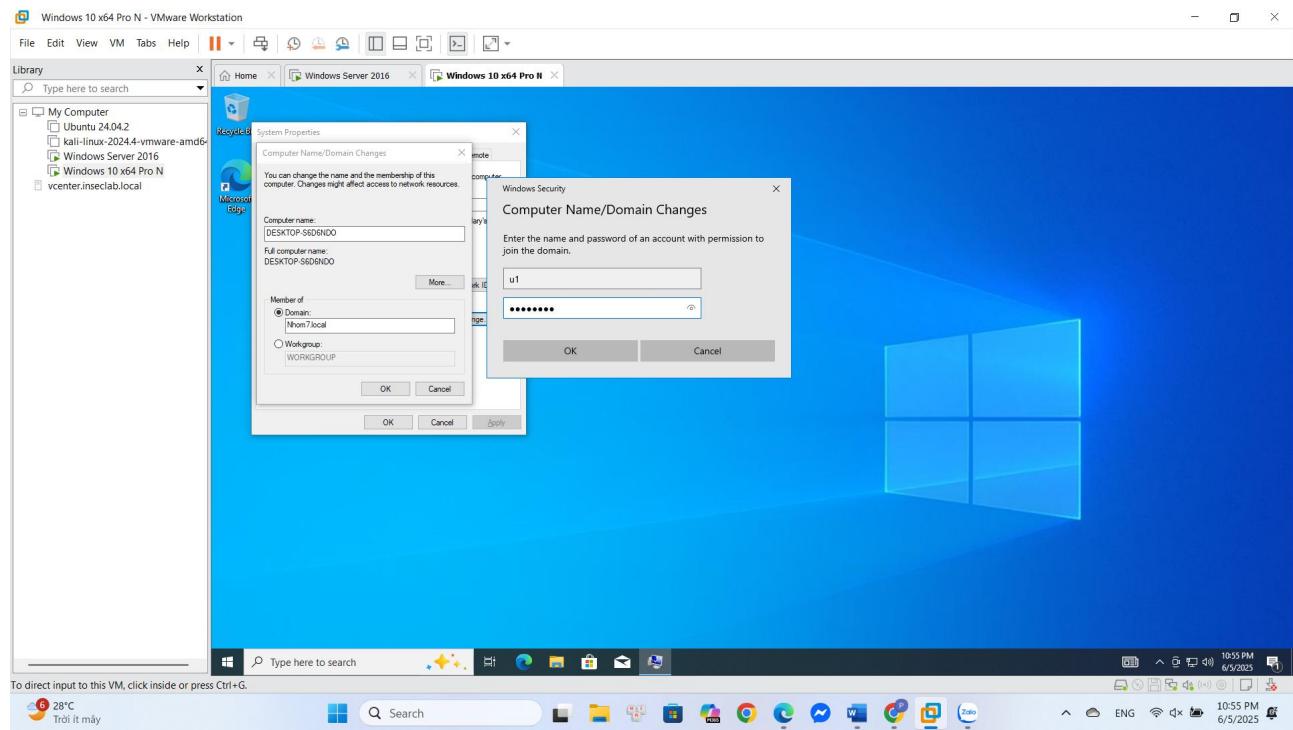
Cấu hình địa chỉ IP cho máy Windows 10 và thêm máy Windows 10 vào domain đã tạo.



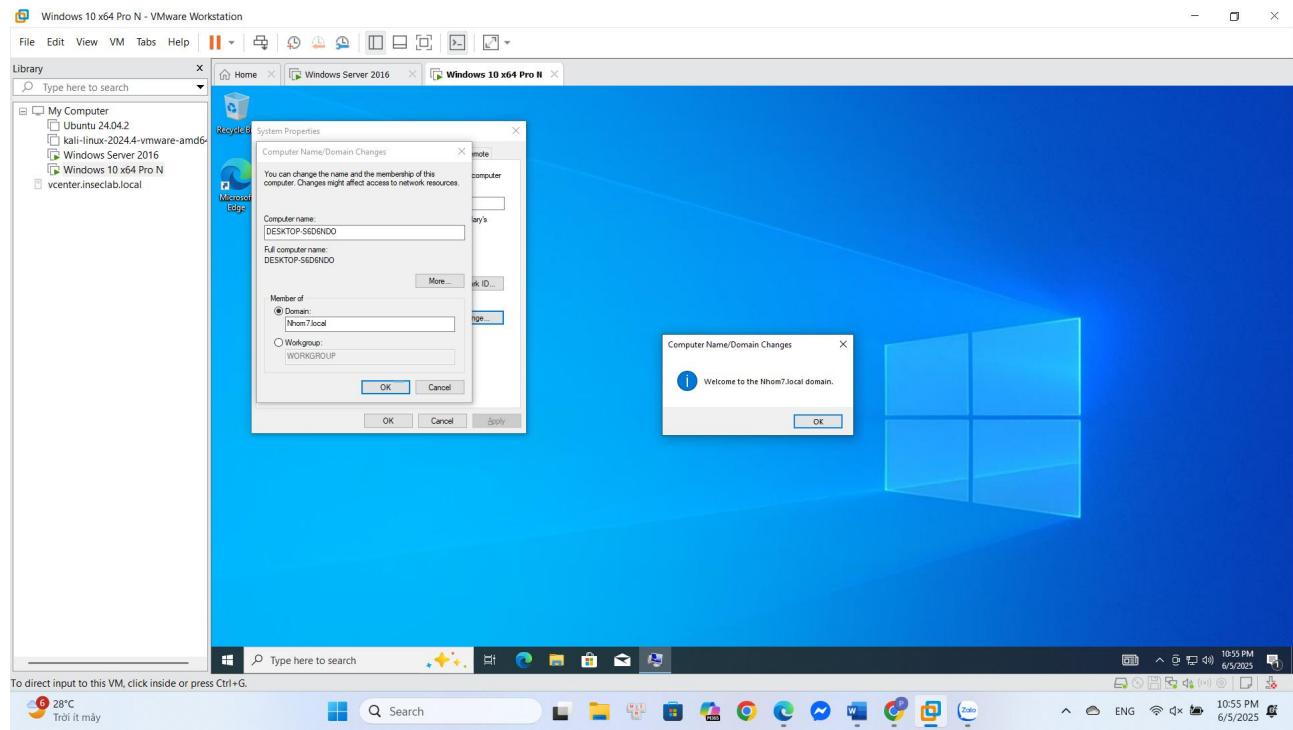
Sau đó, đăng nhập tài khoản user vừa tạo trên máy Windows 10 để tham gia vào domain nhom7.local :

- Vào mục System trong Control Panel, chọn Change settings. Trong cửa sổ System Properties, tab Computer Name, chọn Change.
- Sau đó tại trường Member of, chọn Domain và nhập tên domain muốn tham gia.

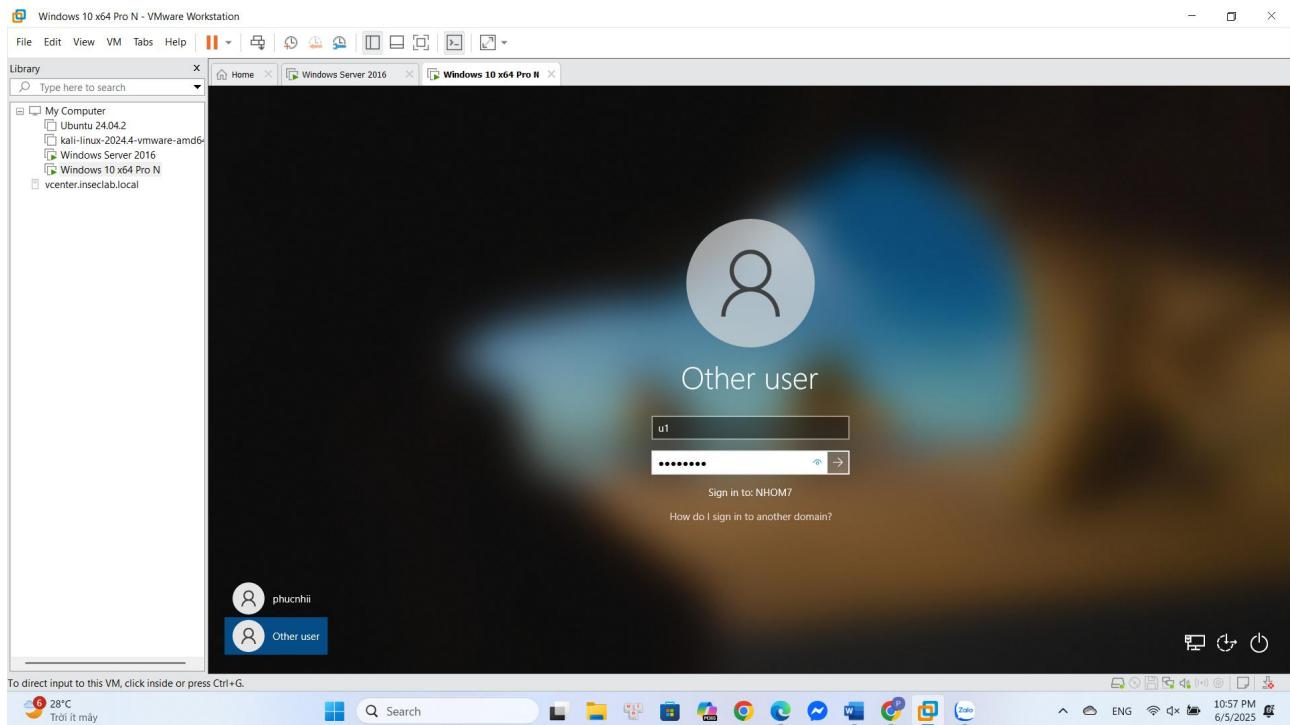
- Sau đó đăng nhập với tài khoản user 1 đã tạo bên máy AD.



- Thông báo xác thực thành công xuất hiện.



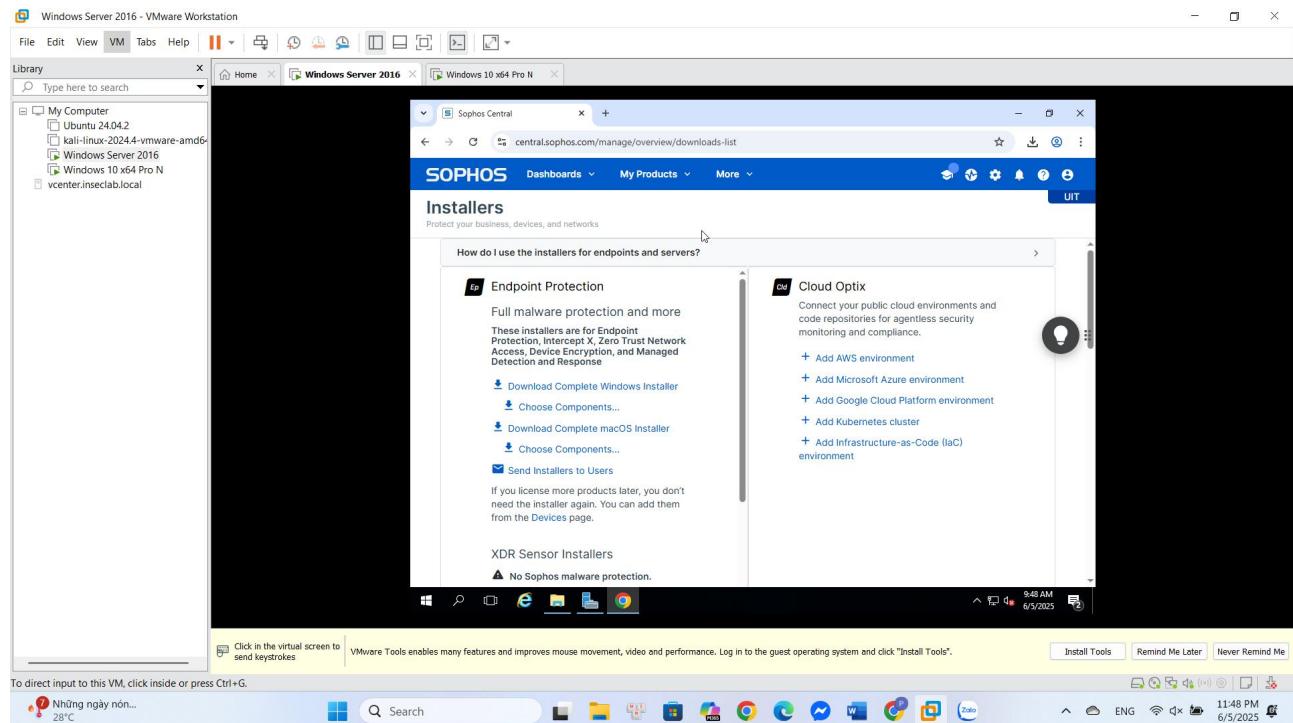
Sau khi thành công, tiến hành restart máy ta được giao diện như hình dưới.



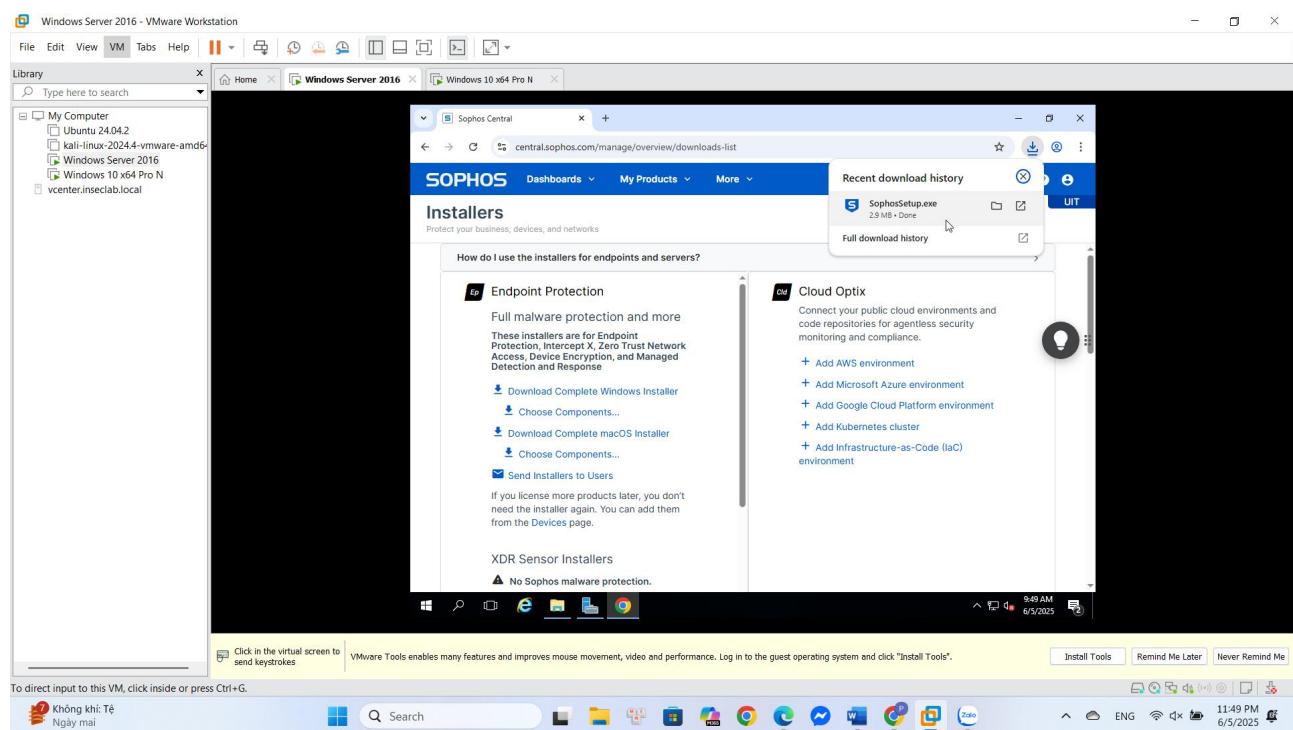
4. Yêu cầu 2.2: Triển khai Sophos Endpoint

- Thực hiện đăng ký tại: Free Trial Sophos Endpoint powered by Intercept X

- Sau khi đăng ký, các bạn đăng nhập vào Sophos Central Admin trên máy AD

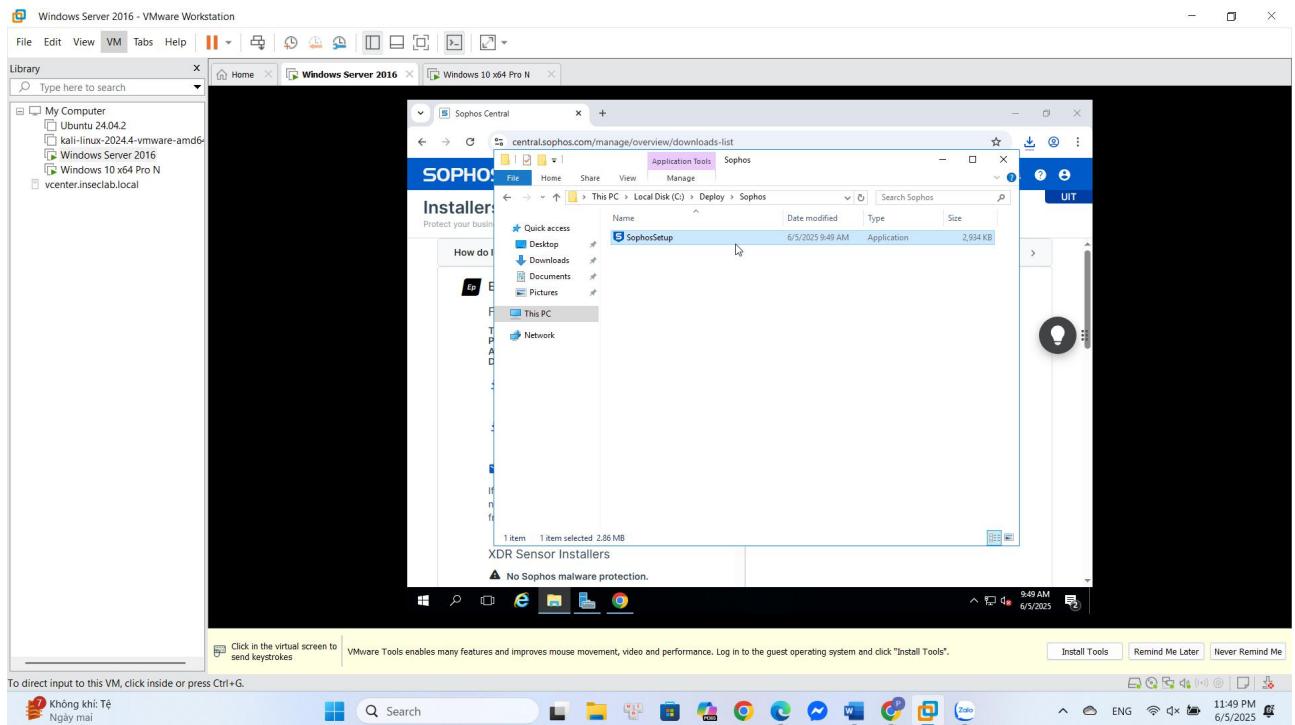


Chọn “Download Complete Windows Installer” để tải về file SophosSetup.exe.

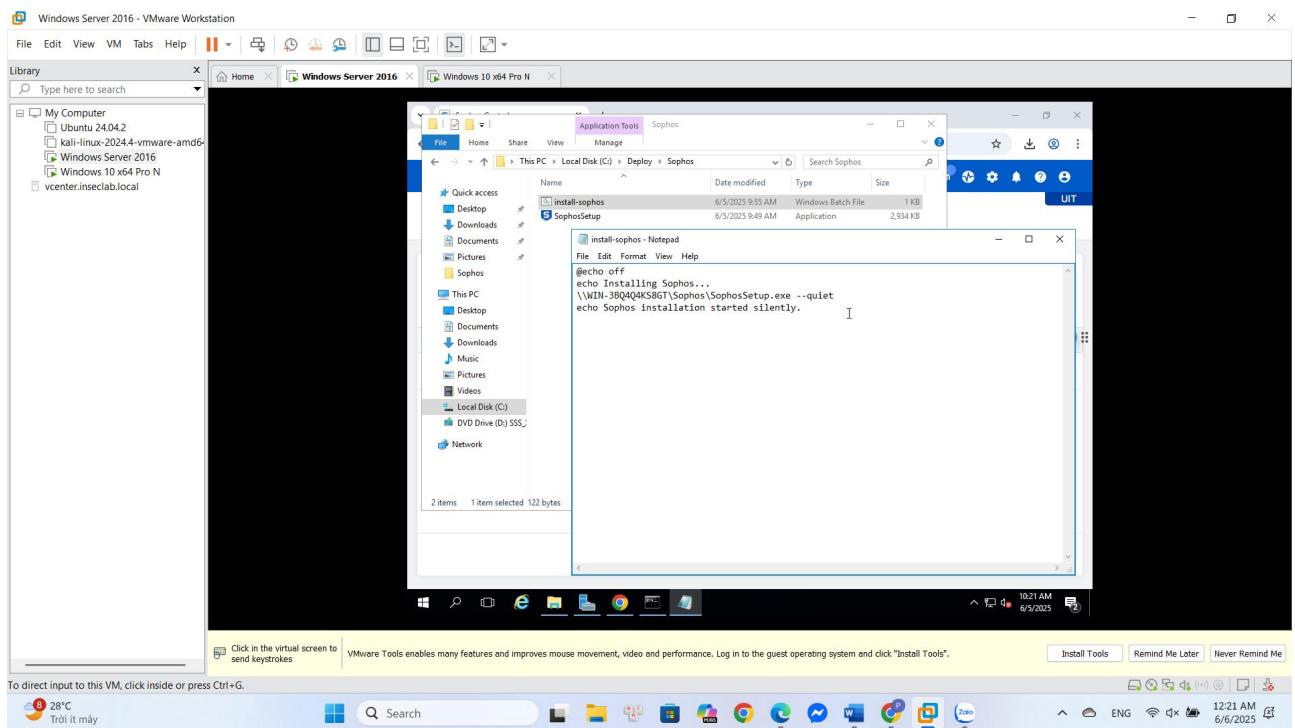


2.2a. Trên máy AD, thực hiện:

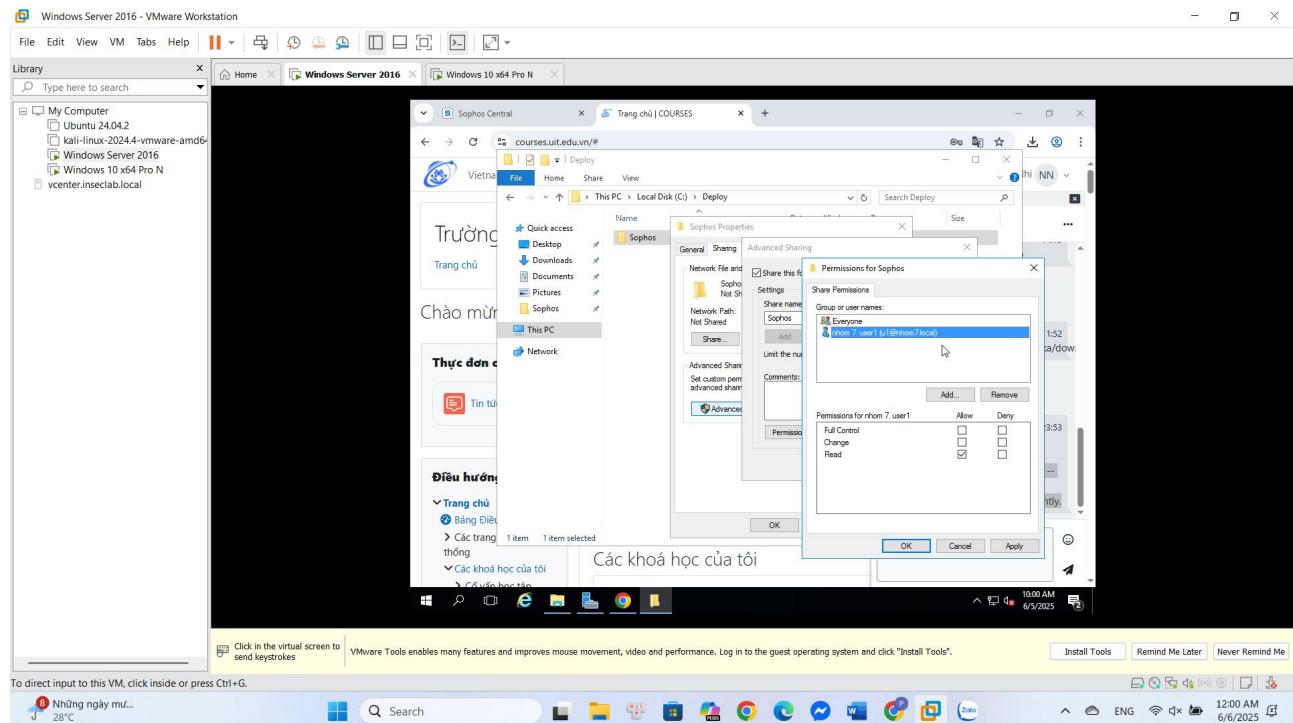
Tạo thư mục C:\Deploy\Sophos và chuyển file SophosSetup.exe vào thư mục này.



Tạo batch script với tên là “install-sophos.bat” để cài đặt Sophos trên máy Windows ở chế độ không giao diện (-quiet).

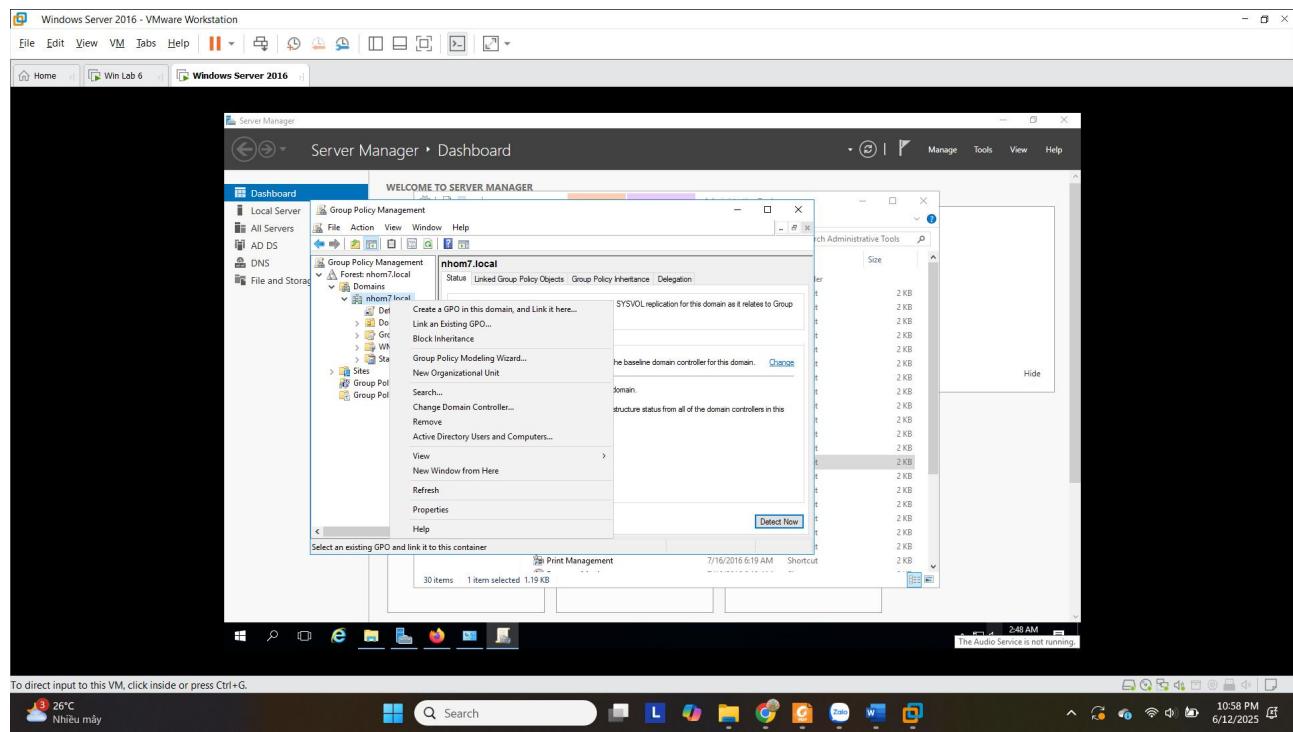


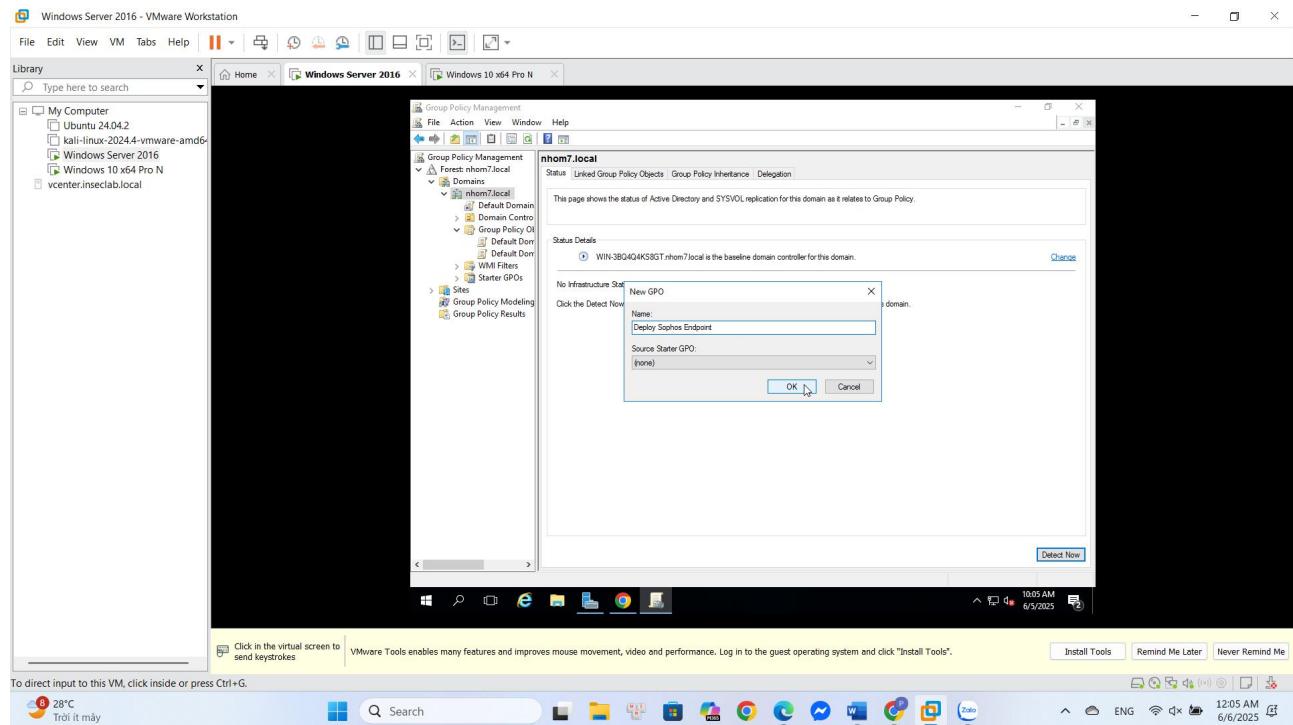
Chia sẻ thư mục vừa tạo với user đã tạo ở trên và máy Windows 10: chuột phải → Properties → tại tab Sharing → Advanced Sharing... → Permissions → Add... → tại mục Enter the object names to select nhập «u1» → OK



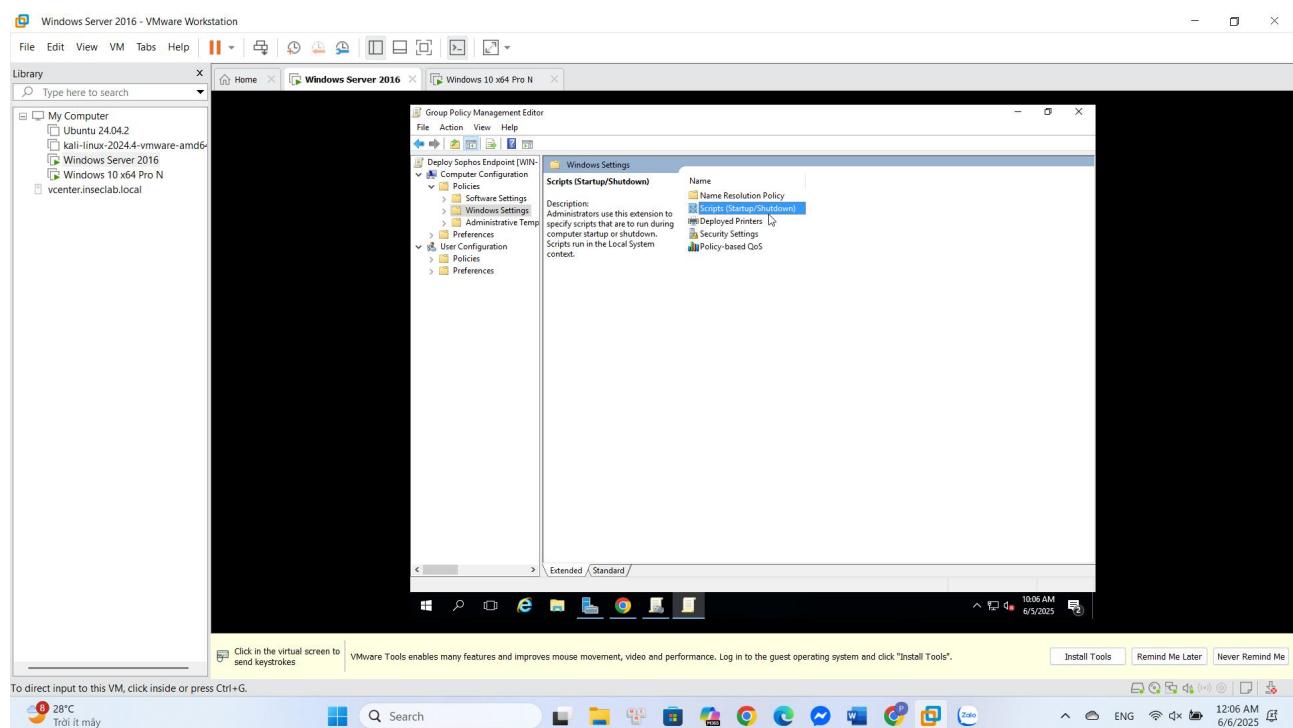
2.2b. Tạo Group Policy Object (GPO) với startup script

Trên máy AD, mở Start Menu → Windows Administrative Tools → Group Policy Management và tiến hành tạo một GPO mới có tên là “Deploy Sophos Endpoint”.

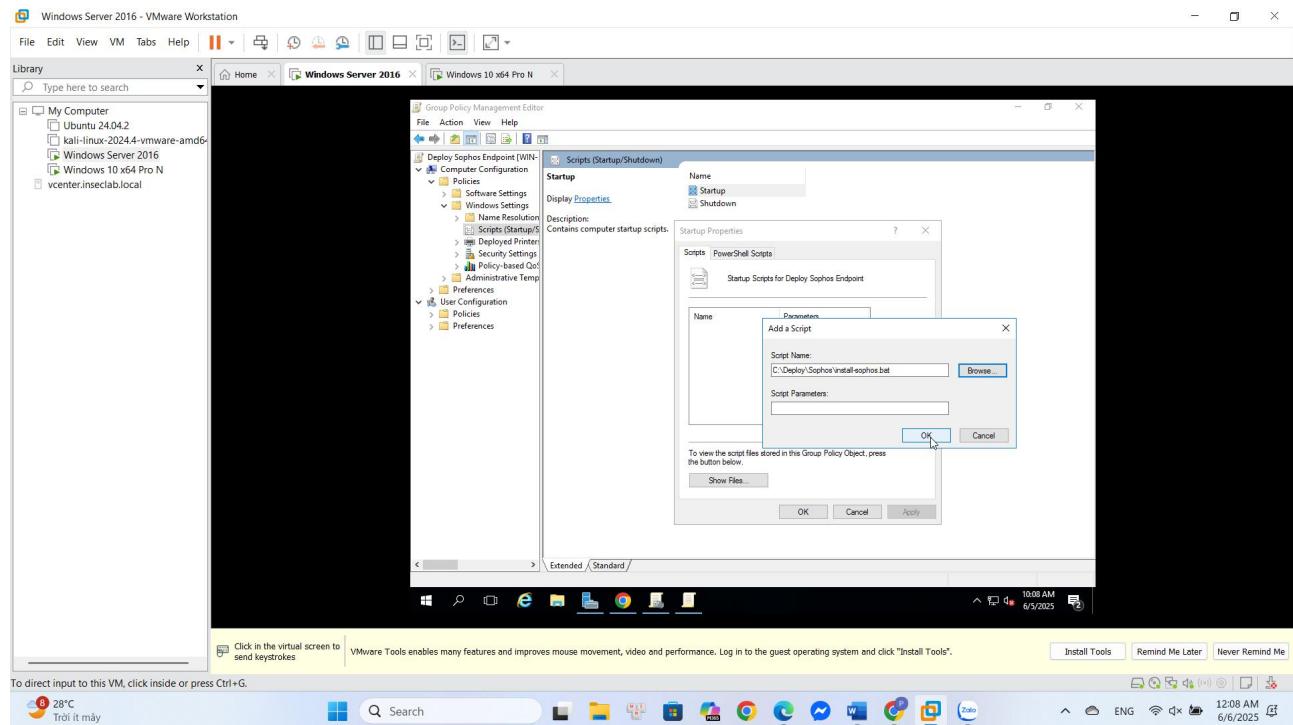




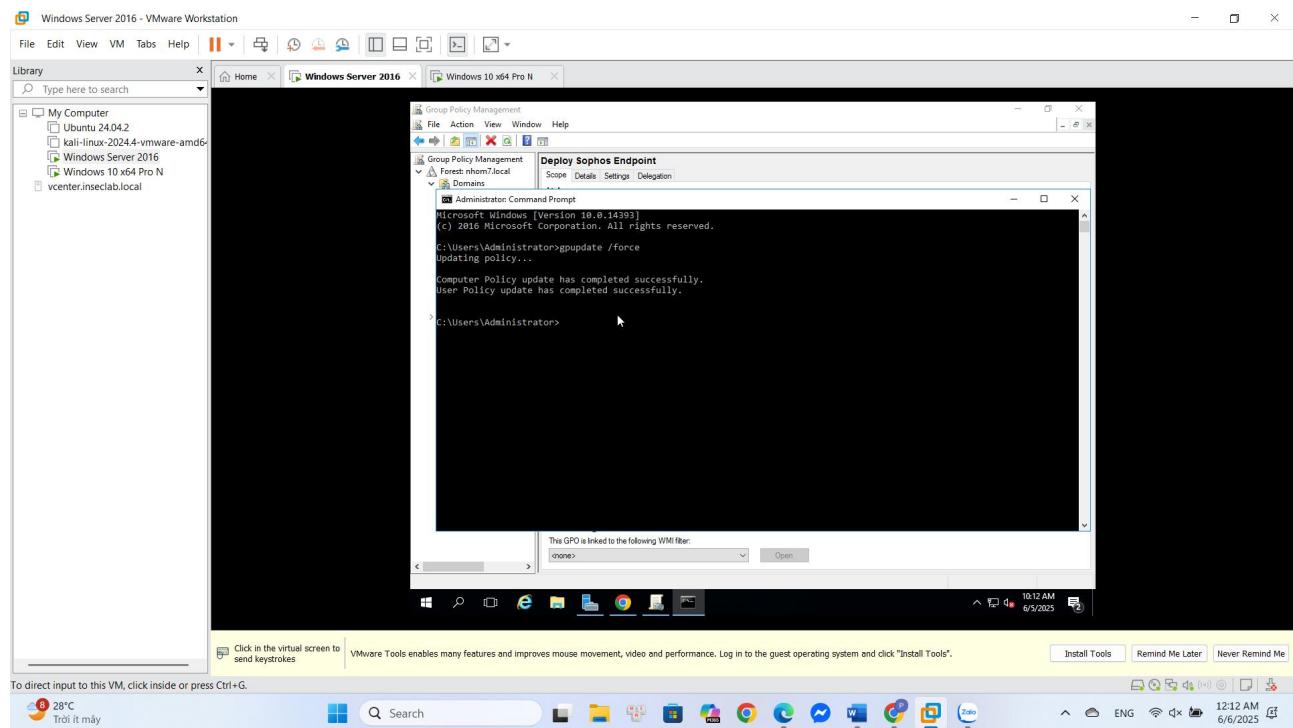
Nhấp chuột phải vào GPO vừa tạo, chọn Edit để vào GPO Editor thêm Script.



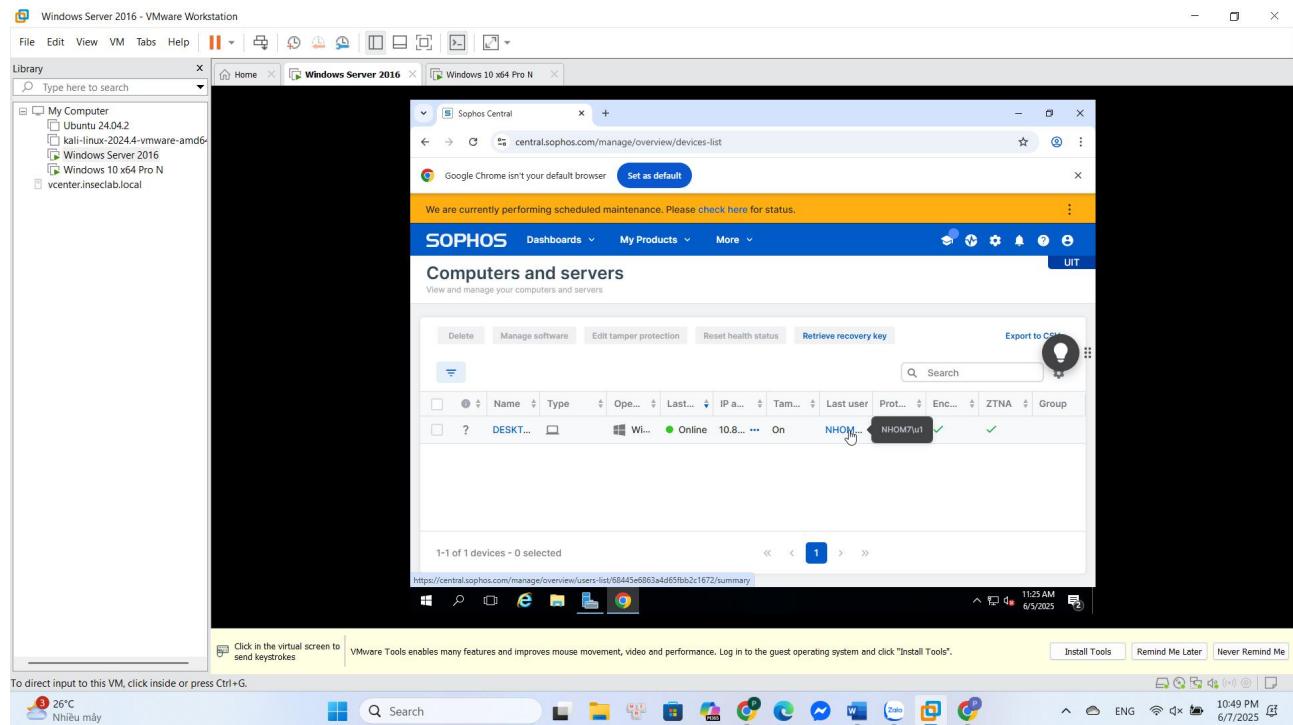
Trong mục Startup, nhấn Add -> Browse để thêm batch script “install-sophos.bat” cho GPO. Cuối cùng, xác nhận bằng Apply -> OK.



Sau khi đã cấu hình xong, chạy lệnh gpupdate /force và tiến hành khởi động lại máy Windows 10.



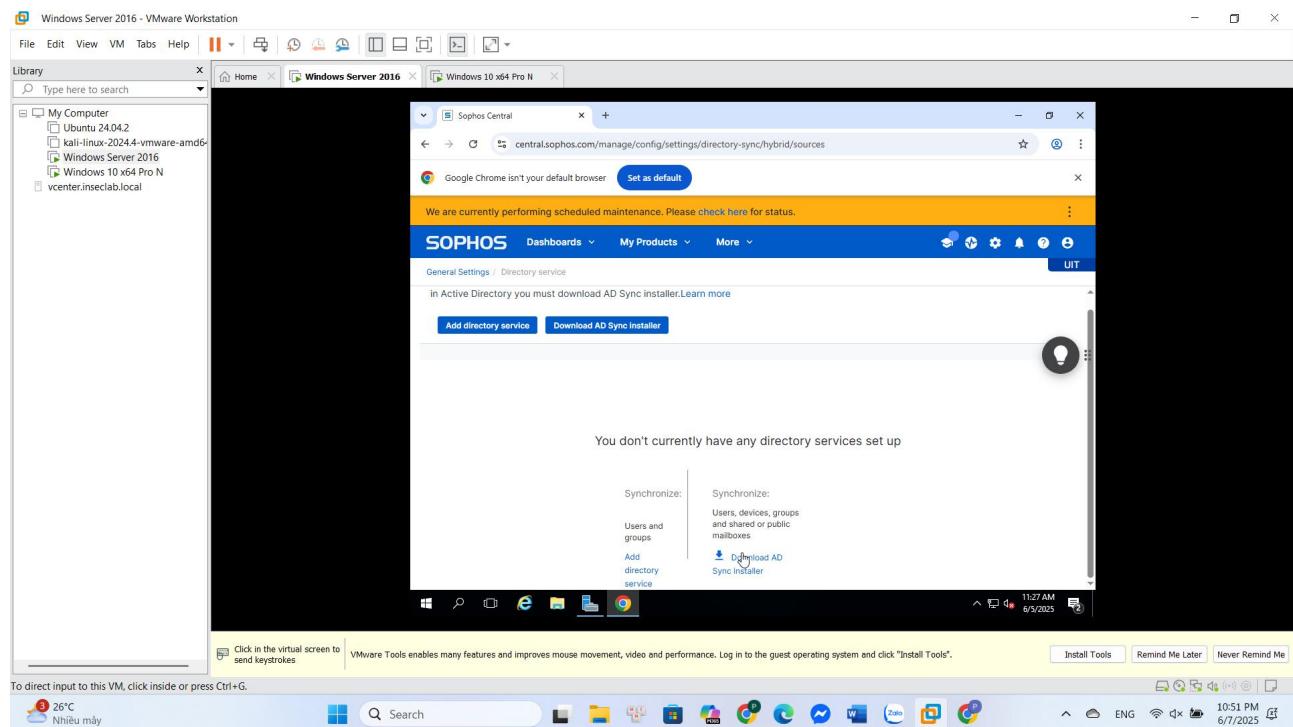
Kiểm tra trên Sophos Central Admin -> Devices để xác nhận rằng Sophos Endpoint đã được triển khai thành công trên máy Windows 10.



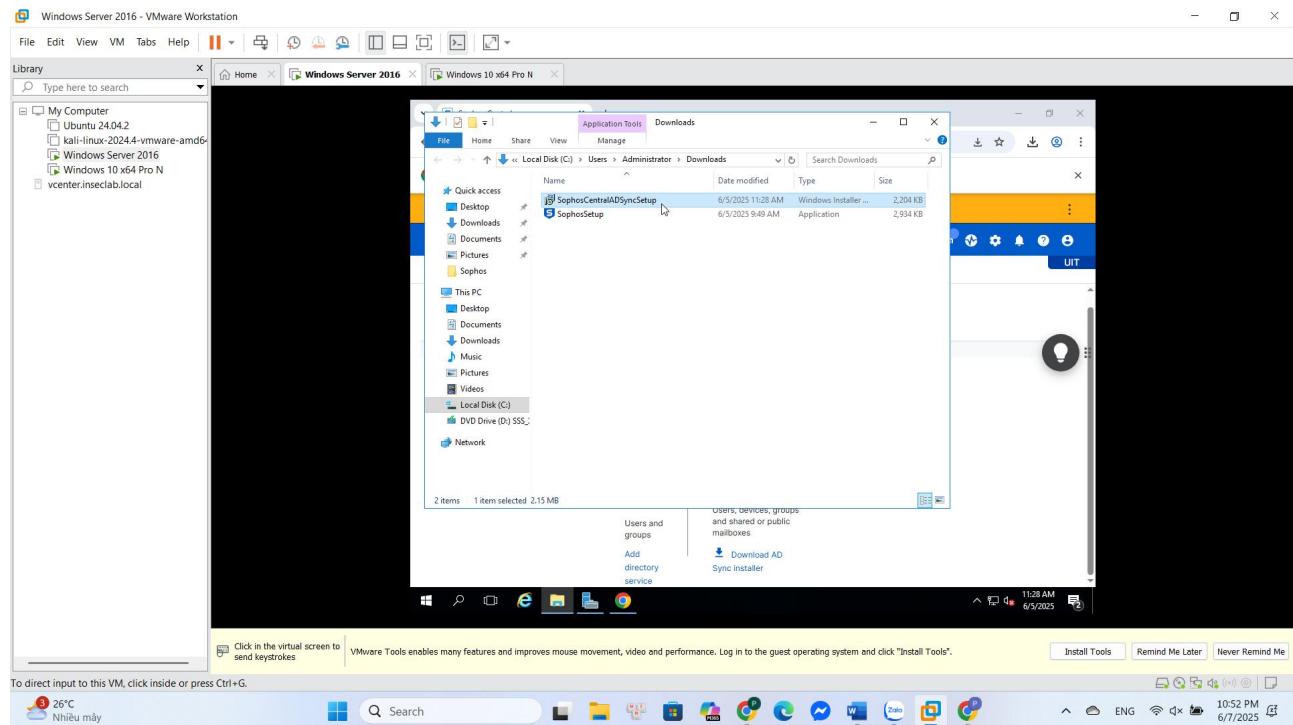
5. Yêu cầu 2.3: Đồng bộ hóa AD với Sophos Central Admin

2.3a. Tải và cài đặt Sophos Central AD Sync Tool trên máy AD

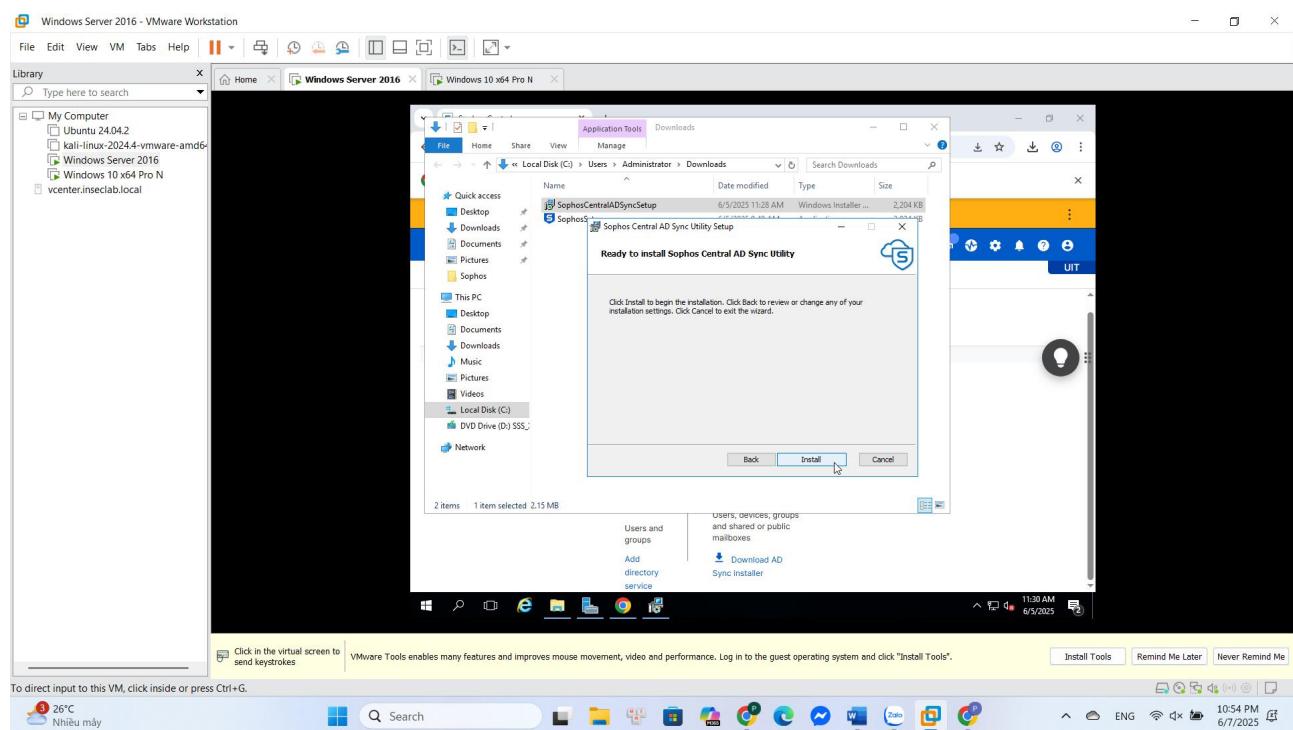
Trong Sophos Central, chọn People -> Set Up Directory Service.



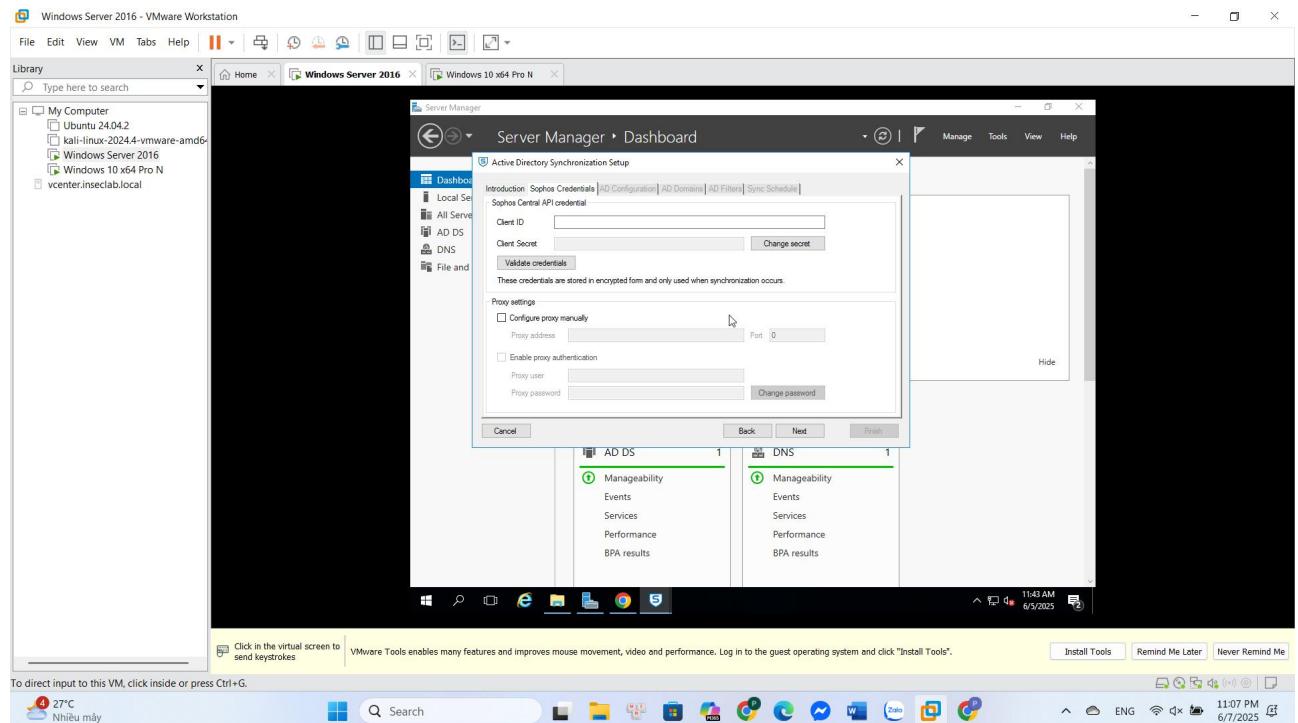
Ta tiến hành tải về “AD Sync installer”.



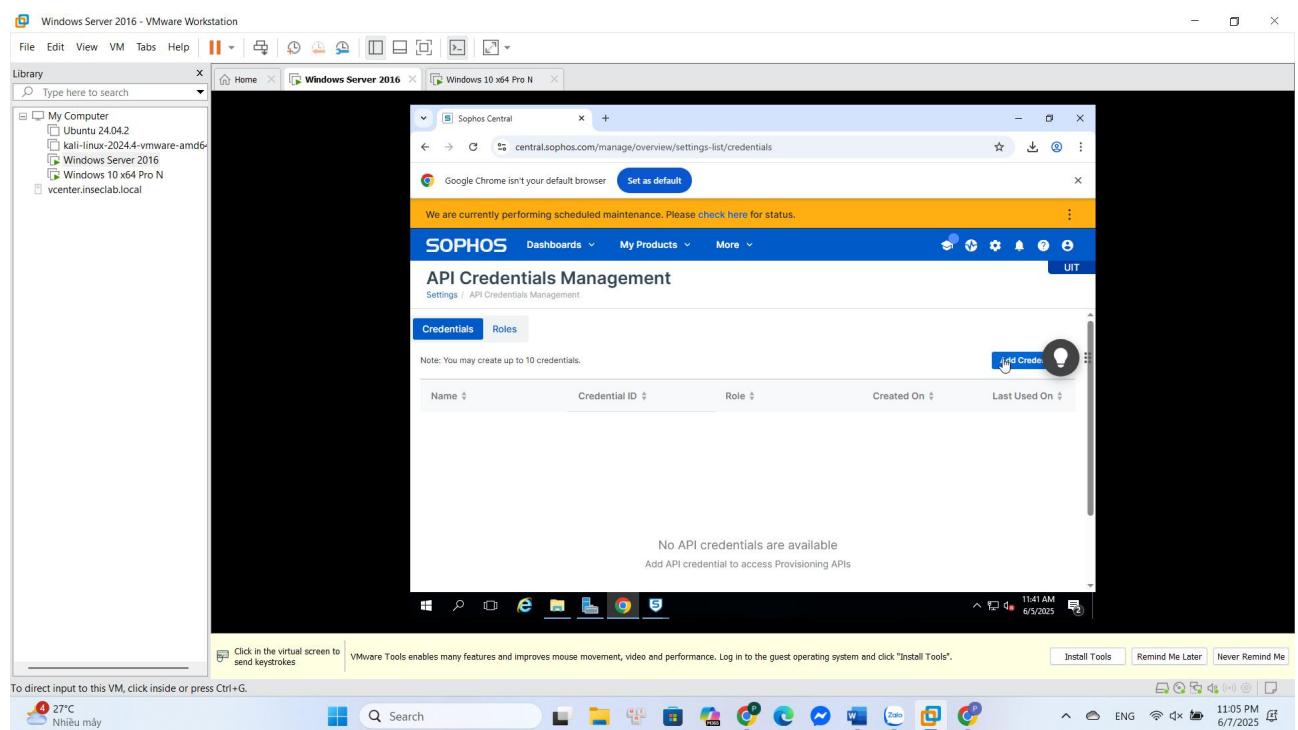
Cài đặt Sophos AD Sync Tool trên máy AD.



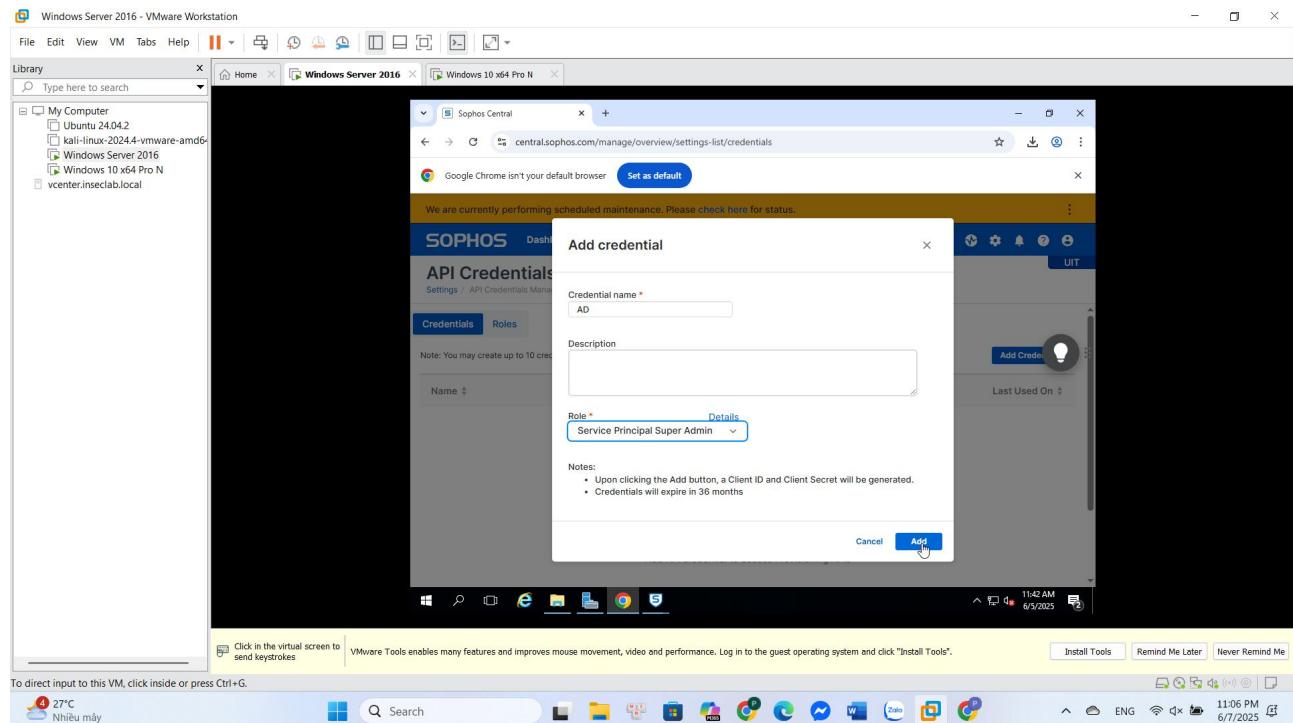
Lưu ý: Để bắt đầu cài đặt AD Sync Tool, ta cần tạo Sophos Credentials API.



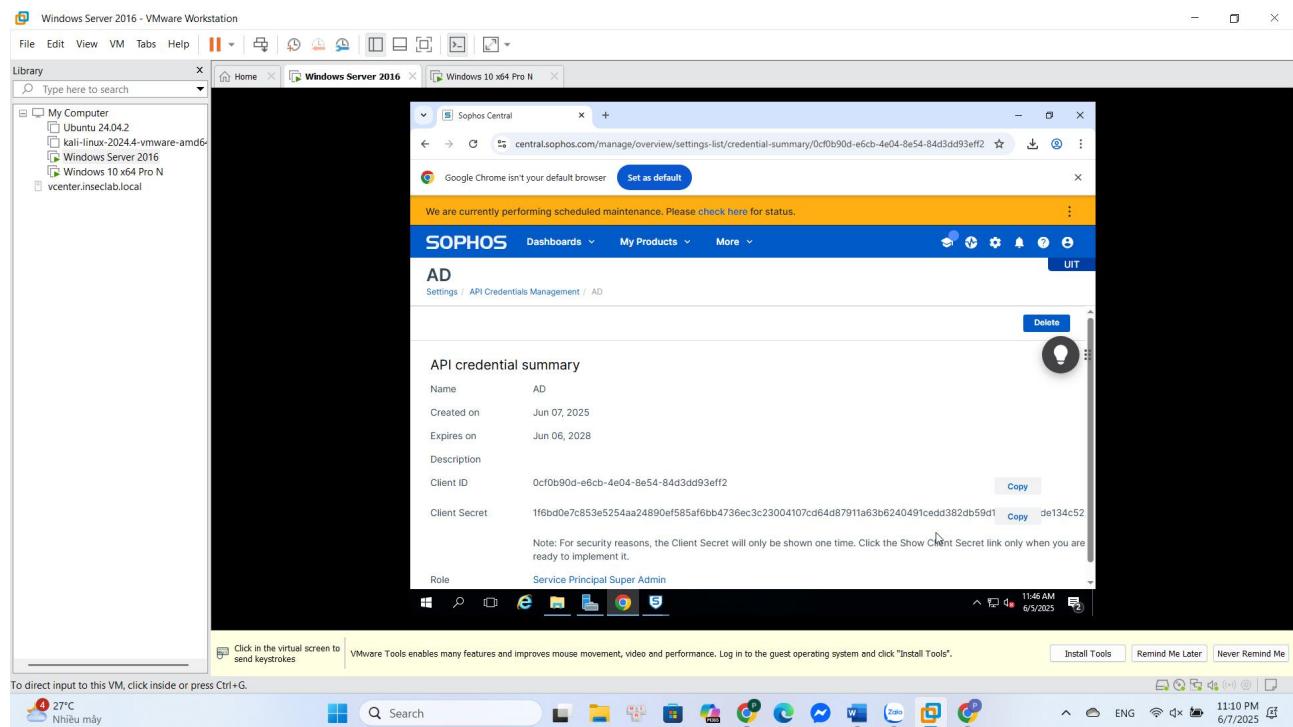
Truy cập Settings → chọn API Credentials Management.



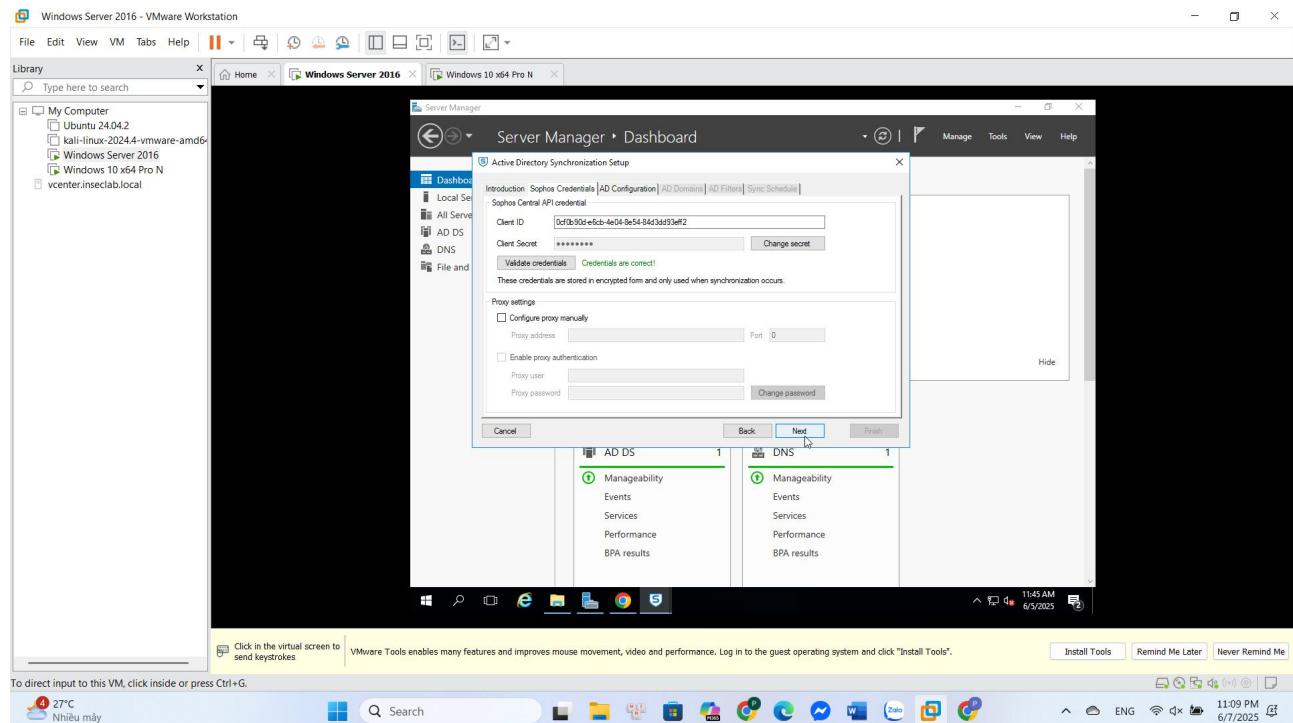
Nhấn Add Credential, đặt tên và chọn quyền.



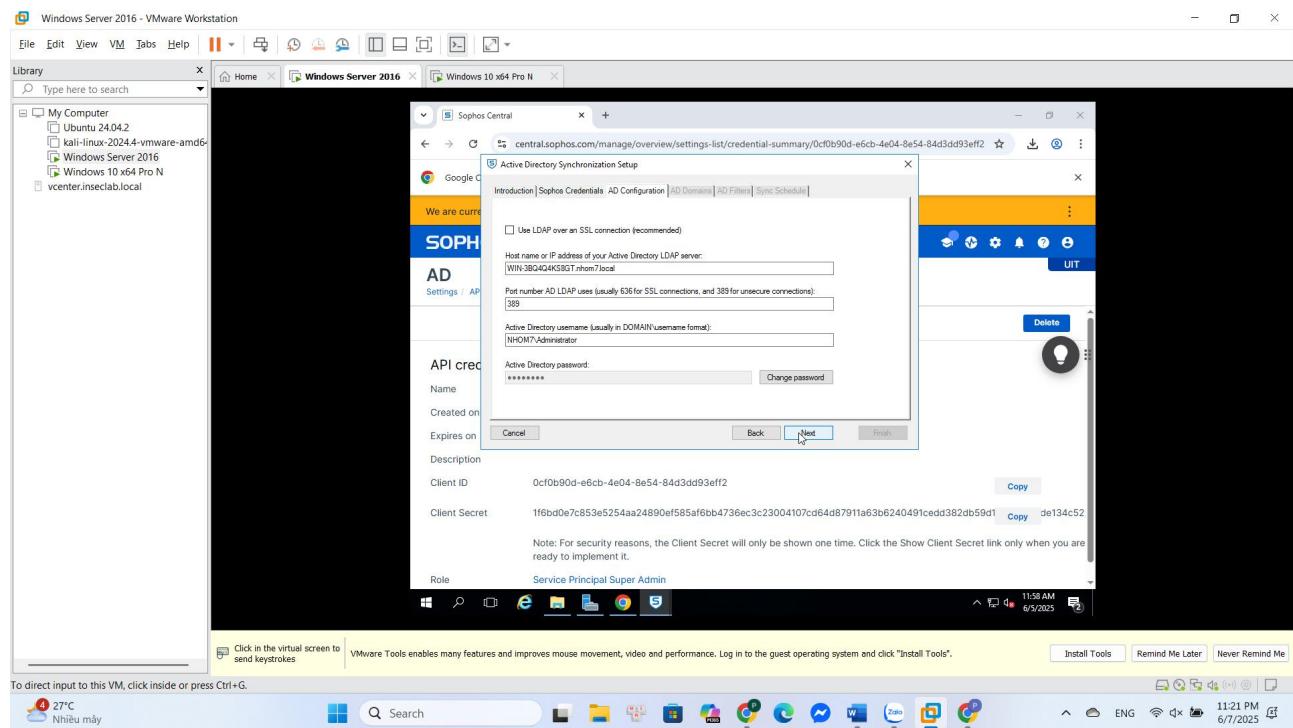
Sau khi tạo, sao chép Client ID và Client Secret.



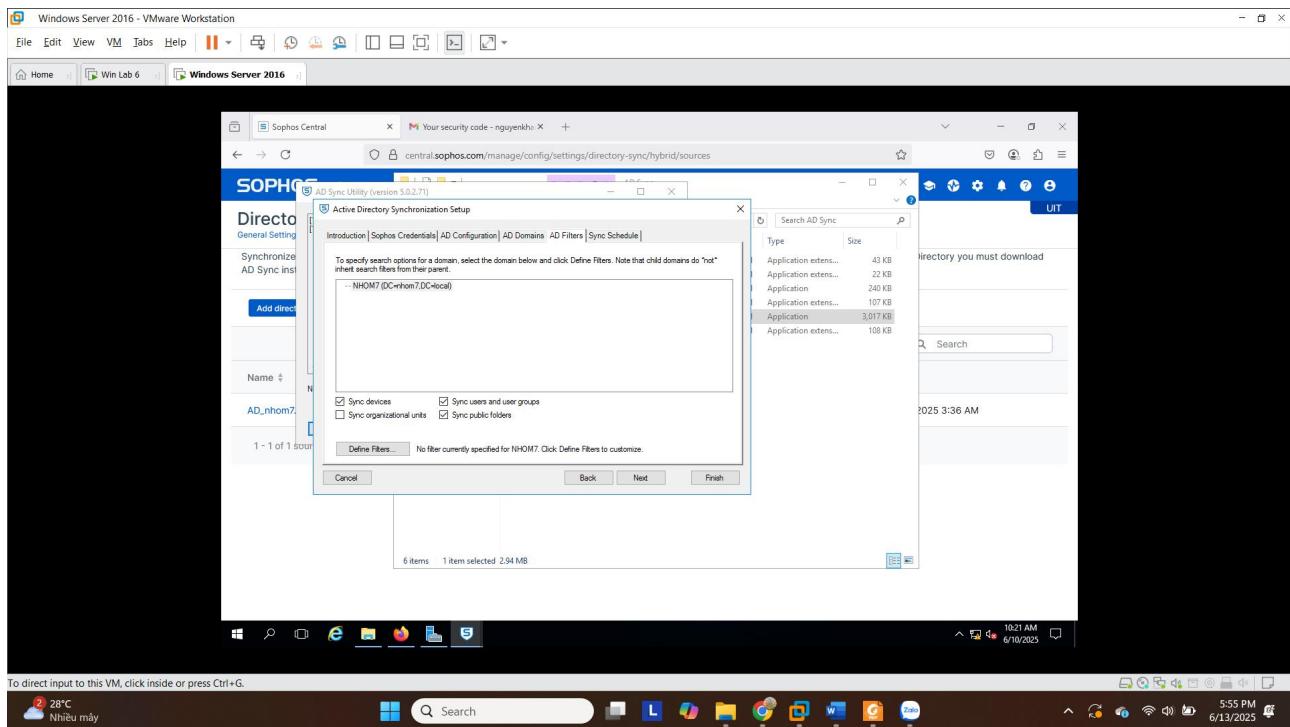
Dán các thông tin này vào cửa sổ cài đặt AD Sync Tool và nhấn Next.



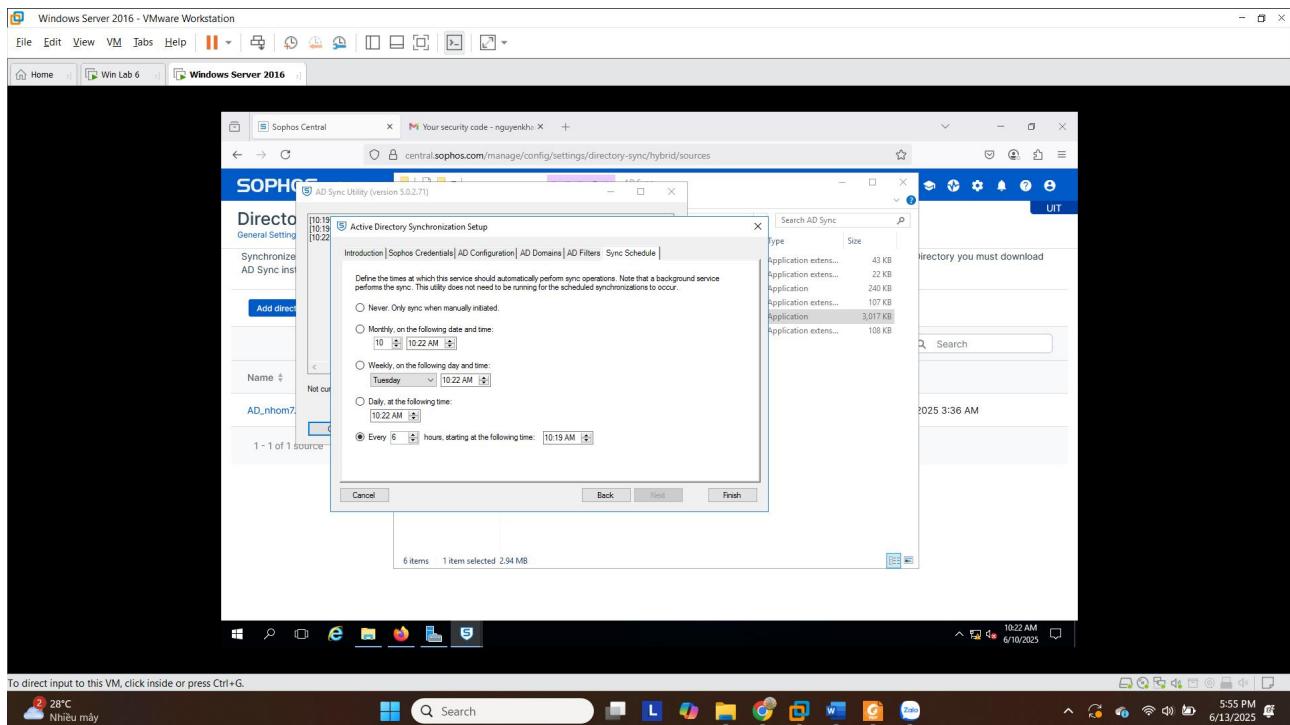
Tiếp theo ta điền các thông tin như Active Directory username và Active Directory password và nhấn Next.



- Chọn Next tới tab AD Filters, tick chọn thêm tùy chọn “Sync Devices”

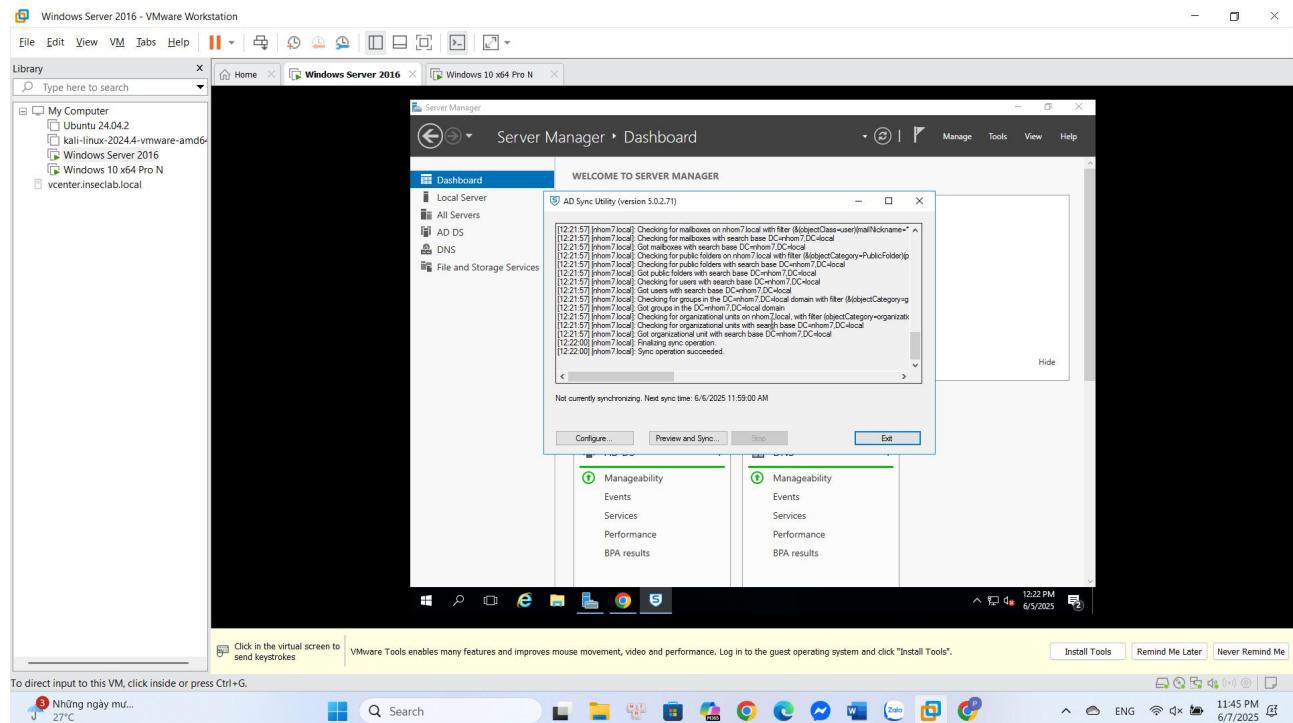


- Tại tab Sync Schedule, chọn lịch để đồng bộ là mỗi 6 giờ.

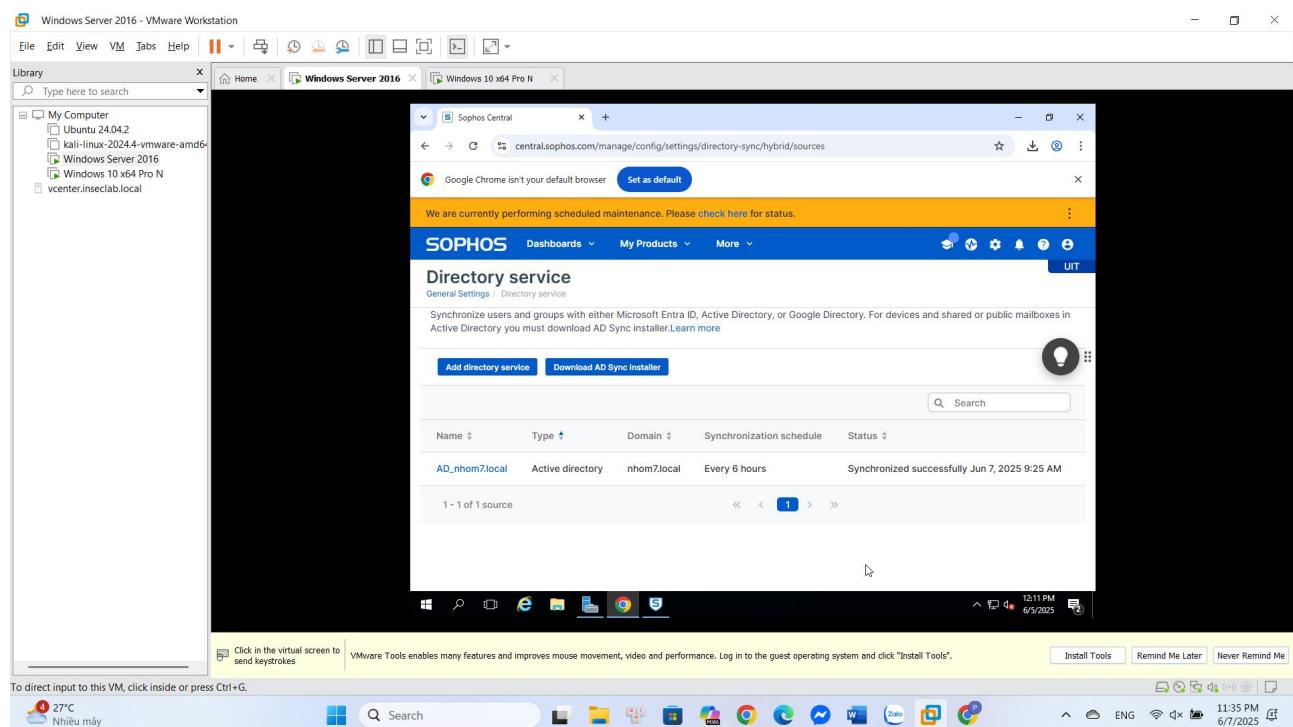


2.3b. Thực hiện đồng bộ hóa AD với Sophos Central

- Chọn Preview and Sync... để tiến hành đồng bộ.



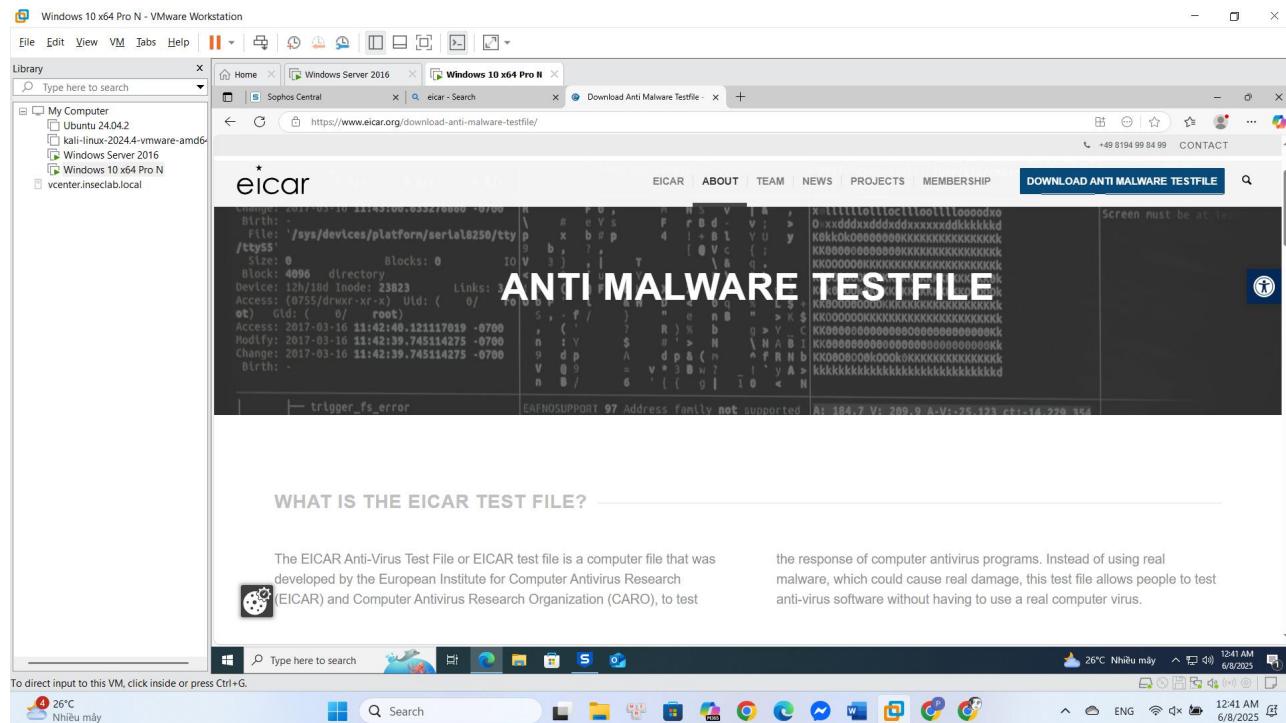
Sau khi đồng bộ hóa hoàn tất, các bạn vào lại mục “Set Up Directory Service” để kiểm tra kết quả đồng bộ:



6. Yêu cầu 2.4: Kiểm tra tính năng của Sophos Endpoint Protection

c) 2.4a. Copy hoặc download một số virus về máy và kiểm tra kết quả.

Truy cập trang: <https://www.eicar.org/download-anti-malware-testfile/> để download một số file virus về máy.

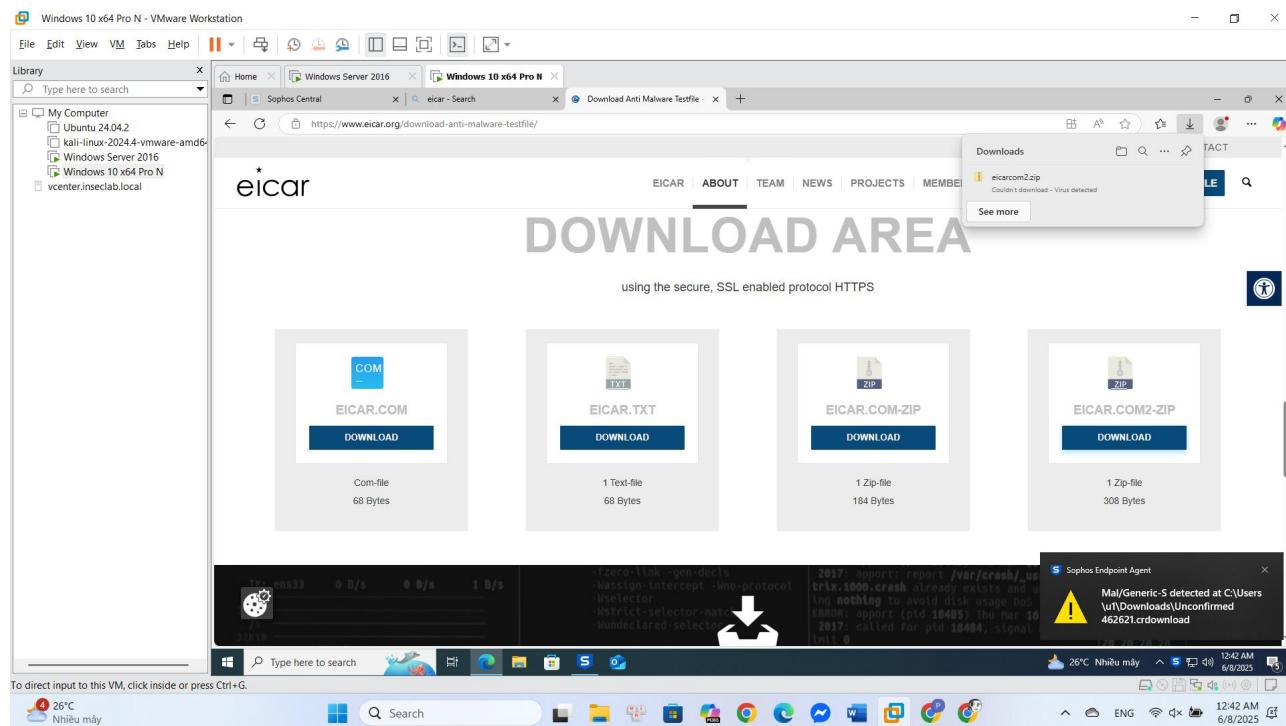


WHAT IS THE EICAR TEST FILE?

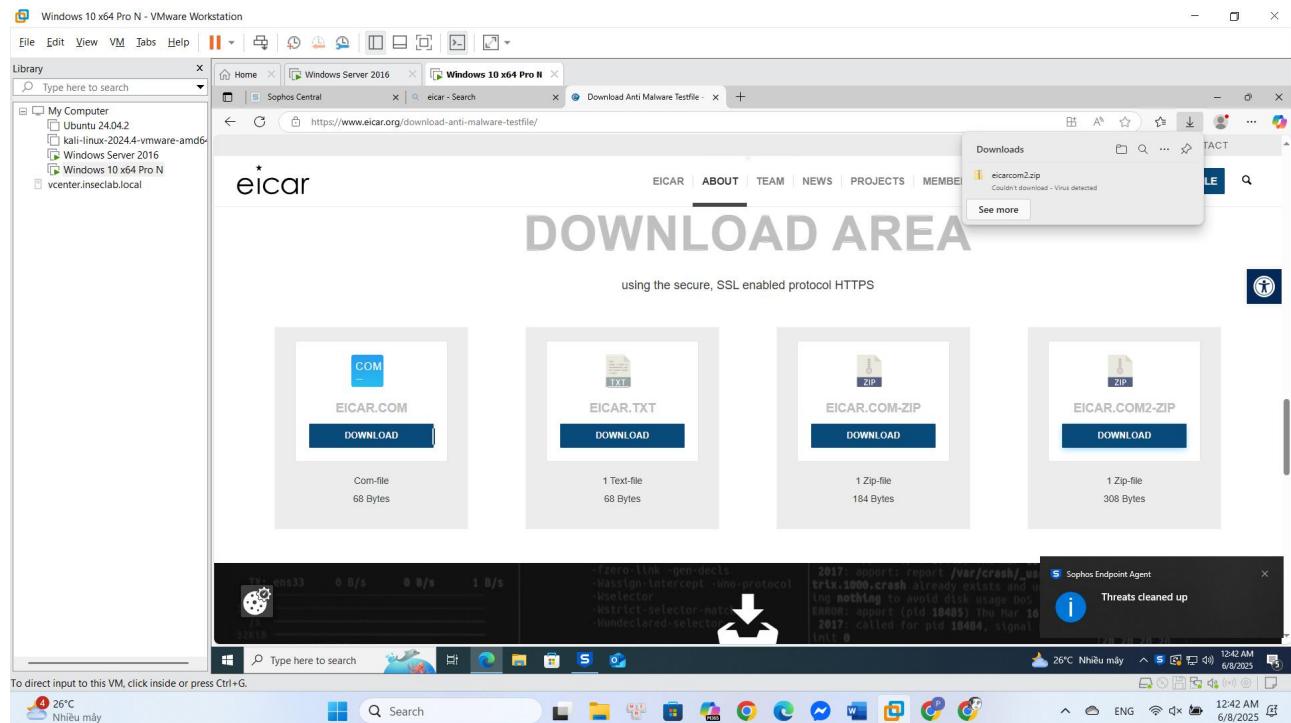
The EICAR Anti-Virus Test File or EICAR test file is a computer file that was developed by the European Institute for Computer Antivirus Research (EICAR) and Computer Antivirus Research Organization (CARO), to test

the response of computer antivirus programs. Instead of using real malware, which could cause real damage, this test file allows people to test anti-virus software without having to use a real computer virus.

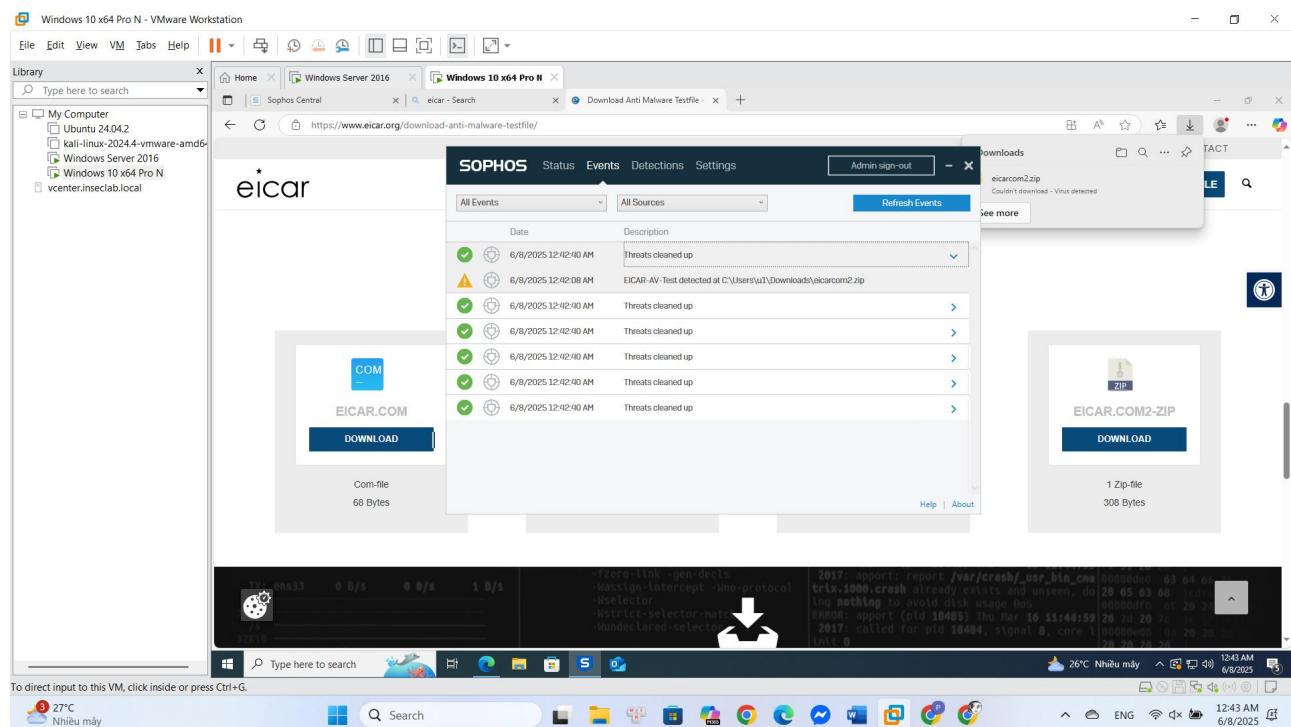
Tải các tệp test như: eicar.com, eicar_com.zip, eicarcom2.zip... và ta thấy cảnh báo từ Sophos.



Quan sát thấy Sophos ngăn không cho tải về và cảnh báo ngay lập tức.



Vào Sophos Endpoint Agent → Events để xem các sự kiện được ghi nhận.



Ta cũng có thể vào Threat Analysis Center -> Detections trên Sophos Central Admin để xem.

Detailed Detection Record:

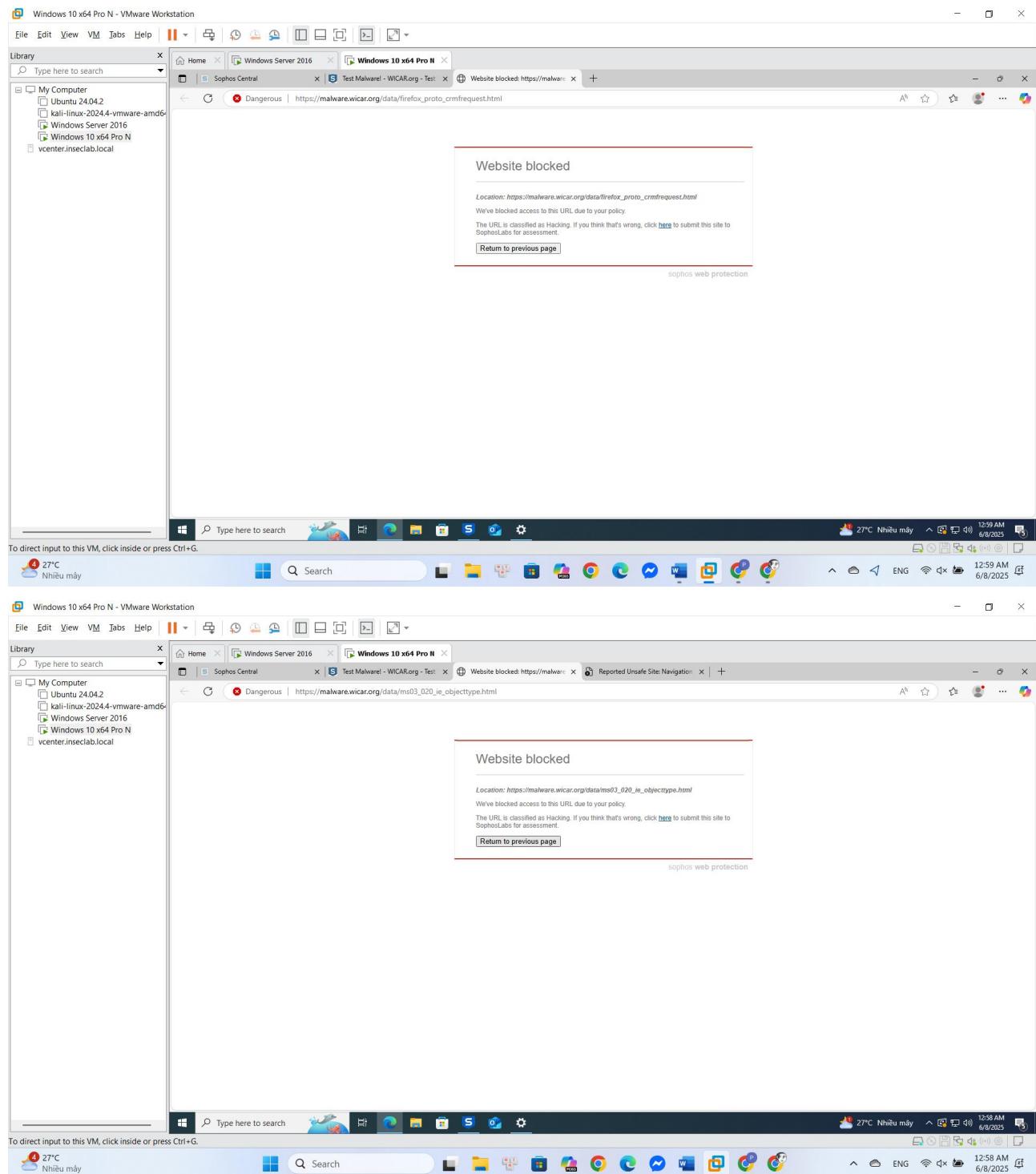
Severity	Type	Rule	Time
Medium	Threat	WIN-PROT-REP-MALWARE-MAL-GENERIC-S	Jun 8, 2025, 12:42:57 AM
Medium	Threat	WIN-PROT-VDL-MALWARE-CXWEB-GENERIC-X	Jun 8, 2025, 12:42:57 AM
Medium	Threat	WIN-PROT-VDL-MALWARE-EICAR-AV-TEST	Jun 8, 2025, 12:42:57 AM
Medium	Threat	WIN-PROT-VDL-MALWARE-EICAR-AV-TEST	Jun 8, 2025, 12:42:57 AM
Medium	Threat	WIN-PROT-REP-MALWARE-MAL-GENERIC-S	Jun 8, 2025, 12:42:57 AM
Medium	Threat	WIN-PROT-VDL-MALWARE-EICAR-AV-TEST	Jun 8, 2025, 12:42:57 AM

d) **2.4b. Sử dụng trang Test Malware! - WICAR.org - Test Your Anti-Malware Solution! để kiểm tra Sophos có phát hiện những khai thác (exploit) hay không. Kiểm tra kết quả.**

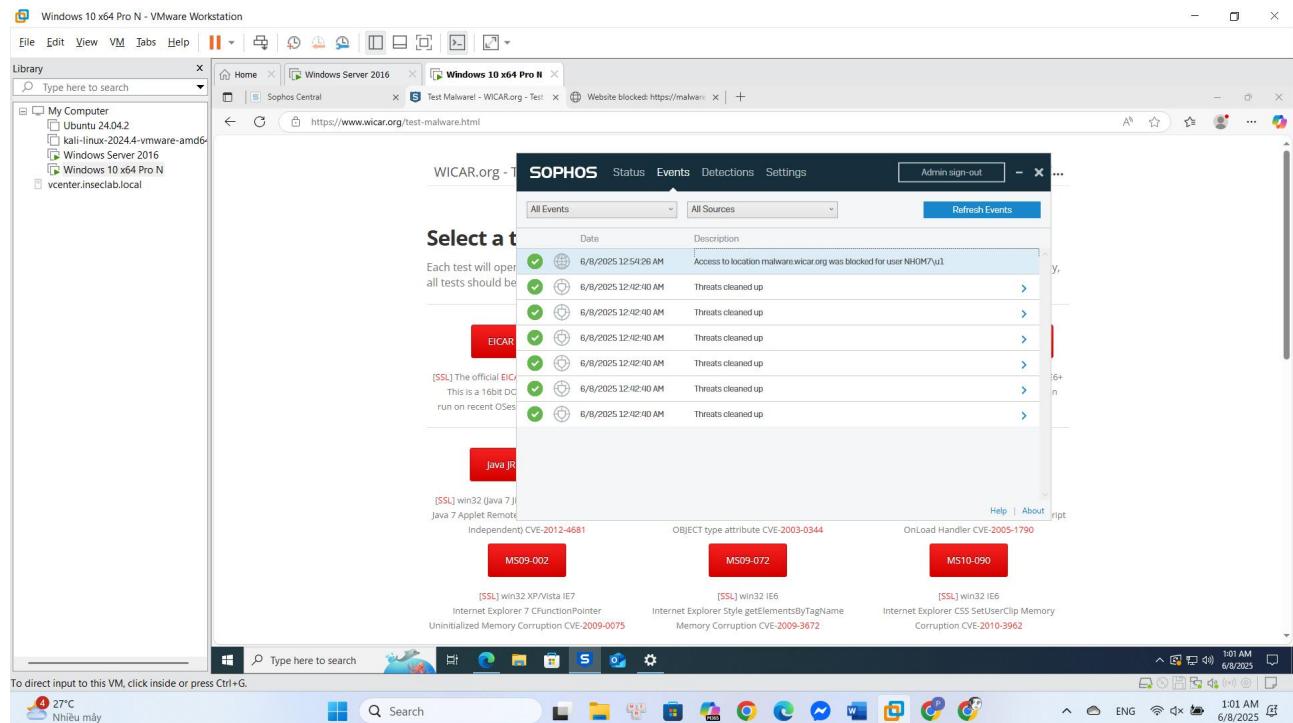
Truy cập vào trang web <https://www.wicar.org/test-malware.html> và lần lượt click vào một số liên kết test như: Drive-by download, JavaScript malware, PDF exploit, HTML5 browser exploit,...

Payload Type	Description	Link
EICAR TEST-VIRUS	[SSL] The official EICAR.COM anti-virus test file. This is a 16bit DOS COM file and cannot run on recent OSes, but should be detected.	[SSL] EICAR TEST-VIRUS
MS14-064 XP and below	[SSL] All Windows NT/95/98/2000/XP IE+ Internet Explorer Windows OLE Automation Array (pre XP) CVE-2014-6332	[SSL] MS14-064 XP and below
MS14-064 2003 to Windows 10	[SSL] All Windows 2003/Vista/2008/7/10 IE6+ Internet Explorer Windows OLE Automation Array (post XP) CVE-2014-6332	[SSL] MS14-064 2003 to Windows 10
Java JRE 1.7 Applet	[SSL] win32 (Java 7 JRE/OK) Chrome Firefox IE Java 7 Applet Remote Code Execution (Browser Independent) CVE-2012-4681	[SSL] Java JRE 1.7 Applet
MS03-020	[SSL] win32 NT/XP/2003 (E6) MS03-020 Internet Explorer's handling of the OBJECT type attribute CVE-2003-0344	[SSL] MS03-020
MS05-054	[SSL] win32 XP IE6 MS05-054 Microsoft Internet Explorer JavaScript OnLoad Handler CVE-2005-1790	[SSL] MS05-054
MS09-002	[SSL] win32 XP/Vista IE7 Internet Explorer 7 CFunctionPointer Uninitialized Memory Corruption CVE-2009-0075	[SSL] MS09-002
MS09-072	[SSL] win32 IE6 Internet Explorer Style getElementsByTagNameByName Memory Corruption CVE-2009-3672	[SSL] MS09-072
MS10-090	[SSL] win32 IE6 Internet Explorer CSS SetUserClip Memory Corruption CVE-2010-3962	[SSL] MS10-090
Firefox 5.0 - 15.0.1 exposedProps	[SSL] win32 XP/Vista IE7 Internet Explorer 7 CFunctionPointer Uninitialized Memory Corruption CVE-2009-0075	[SSL] Firefox 5.0 - 15.0.1 exposedProps
Embedded VLC AMV	[SSL] win32 IE6 Internet Explorer CSS SetUserClip Memory Corruption CVE-2010-3962	[SSL] Embedded VLC AMV
Adobe Flash Hacking Team leak	[SSL] win32 IE6 Internet Explorer CSS SetUserClip Memory Corruption CVE-2010-3962	[SSL] Adobe Flash Hacking Team leak

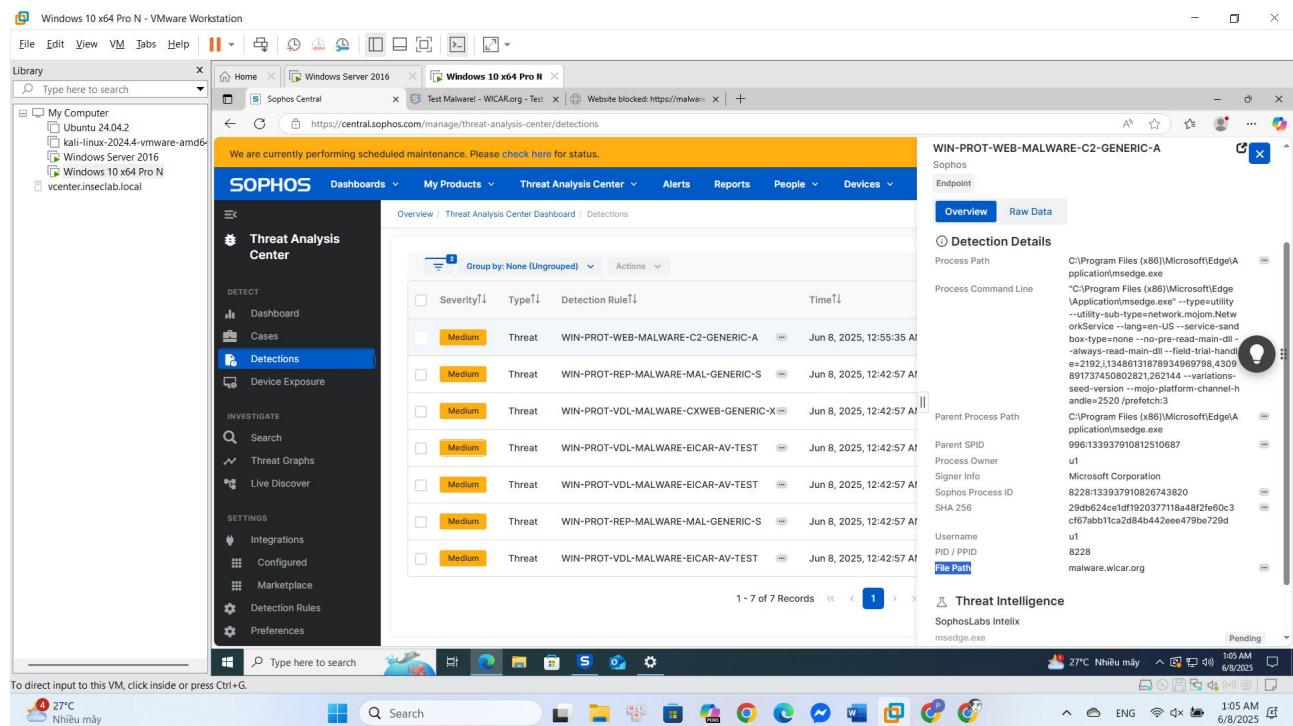
Quan sát kết quả ta thấy Sophos có ngăn chặn kết nối, hiển thị cảnh báo và ghi log lại hành vi truy cập độc hại.



Vào Sophos Endpoint Agent → Events để xem các logs đã được ghi nhận.



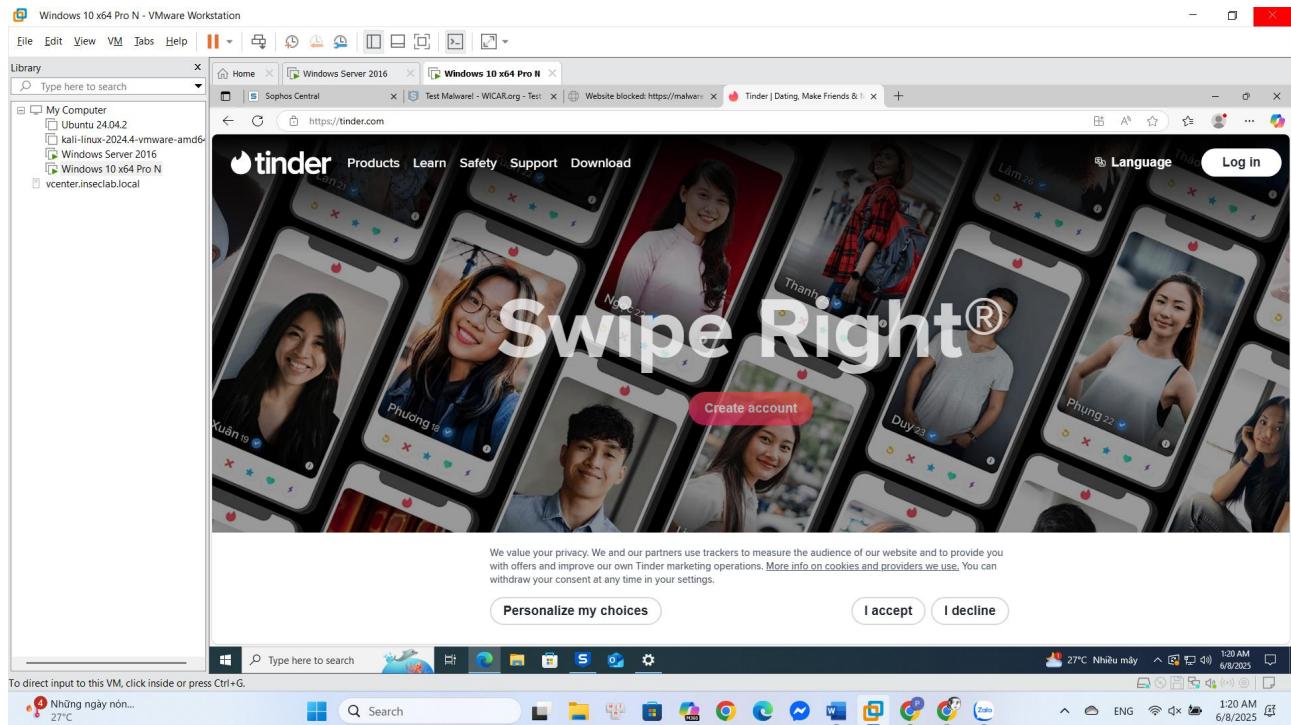
Ta cũng có thể vào Threat Analysis Center -> Detections trên Sophos Central Admin để xem.



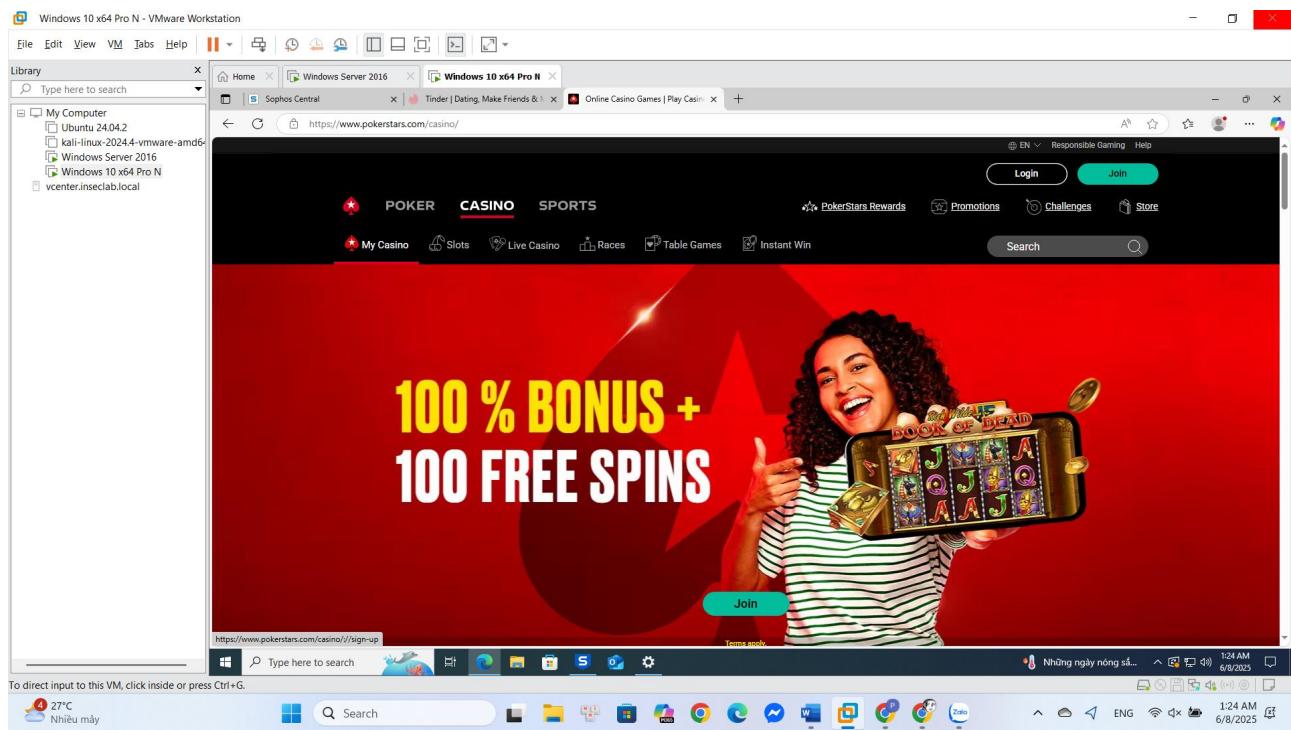
e) 2.4c. Sinh viên tạo kịch bản để kiểm tra tính năng của chính sách Web Control.

Trước khi chỉnh sửa Policy, ta thử truy cập vào các trang được cho phép và không được cho phép như:

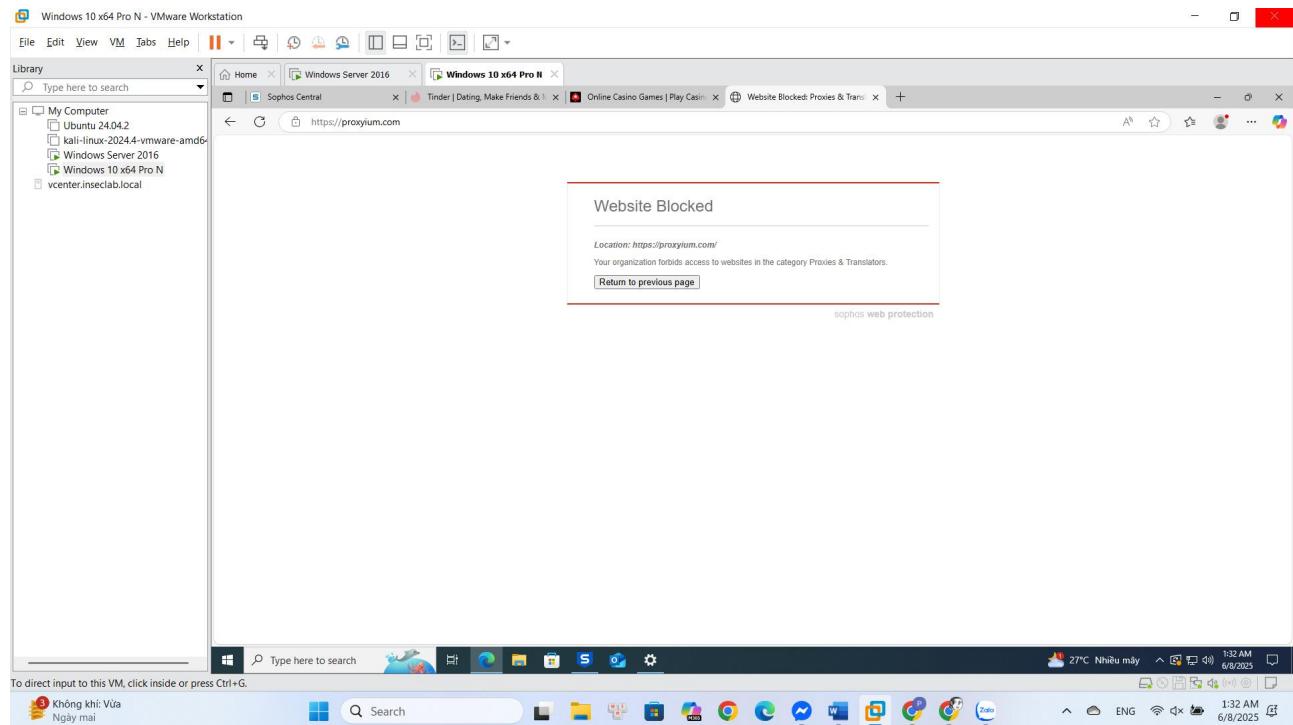
- Tinder (thuộc danh mục Personals & Dating/được cho phép):



- Pokerstars (thuộc danh mục Gambling/được cho phép):



- Proxyium (thuộc danh mục Proxy & Translator/không được cho phép):



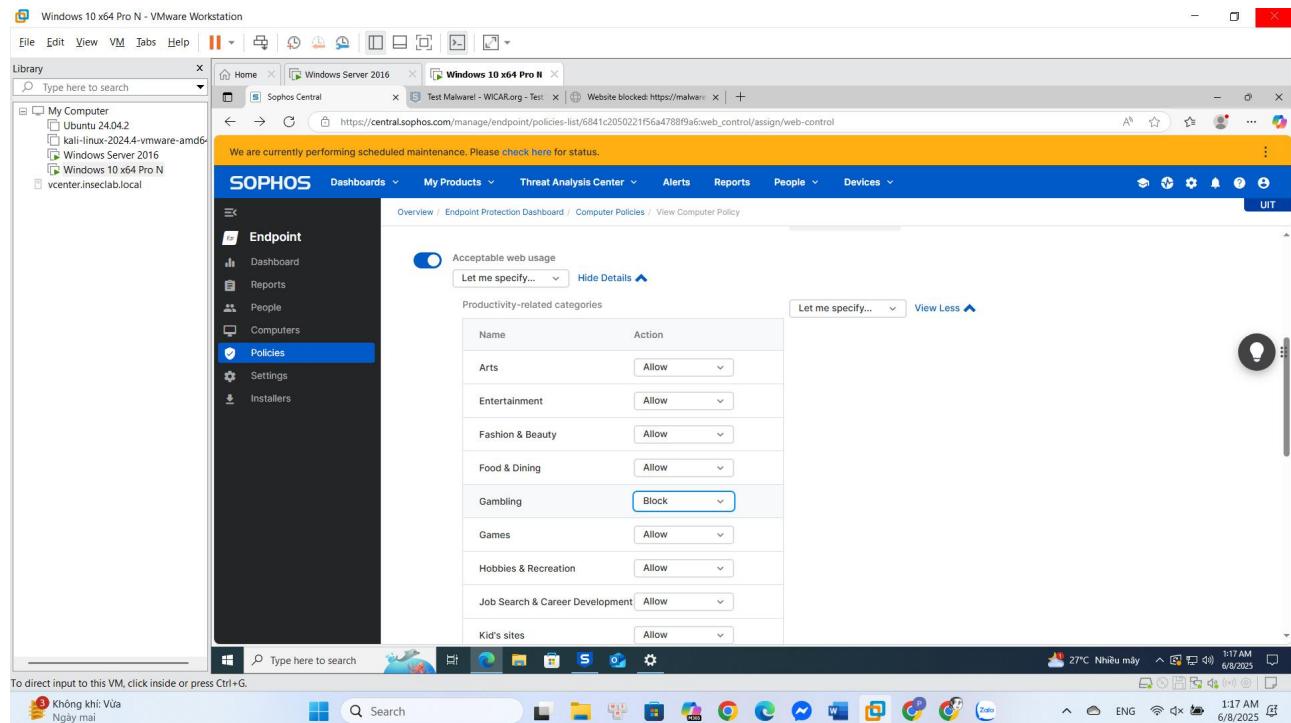
Truy cập Sophos Central Admin → Endpoint Protection → Policies.

Name	Status	Type (single / group)	Last modified
Base Policy - Threat Protection	Active		Jun 5, 2025

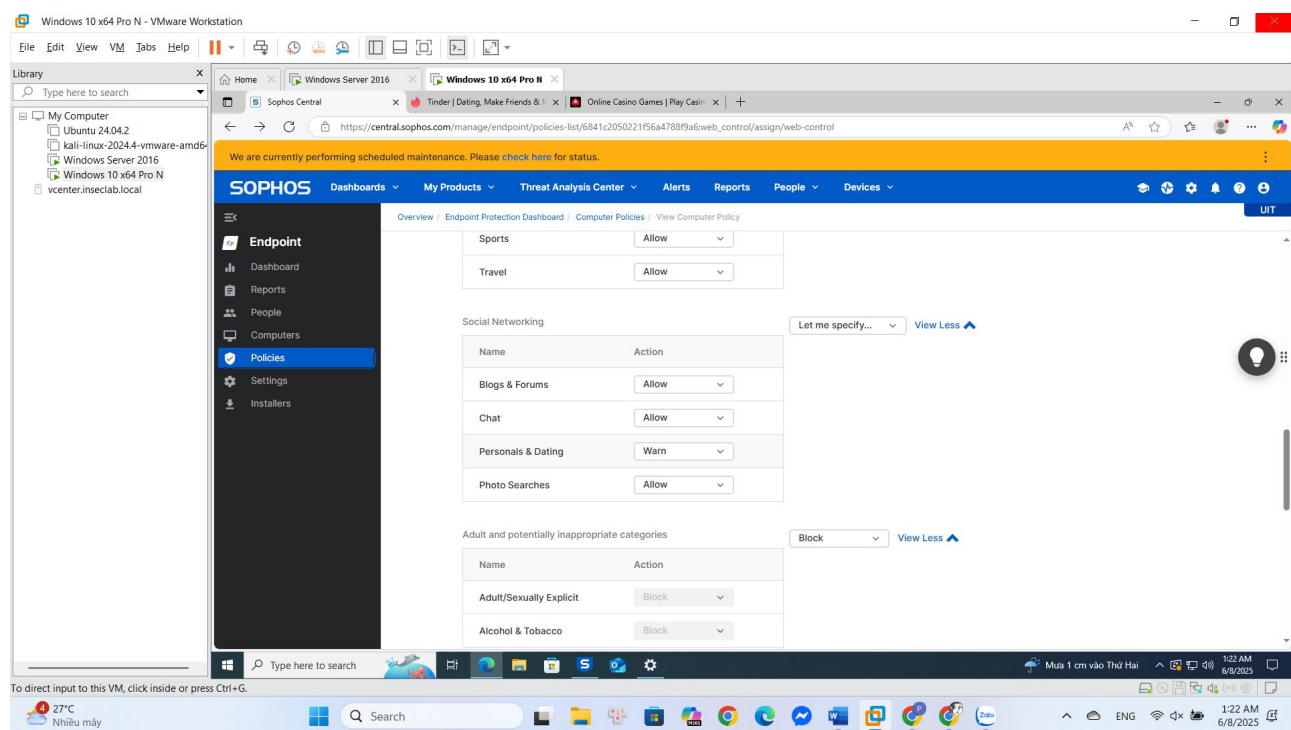
Name	Status	Type (single / group)	Last modified
Base Policy - Peripheral Control	Active		Jun 5, 2025

Name	Status	Type (single / group)	Last modified
Base Policy - Application Control	Active		Jun 5, 2025

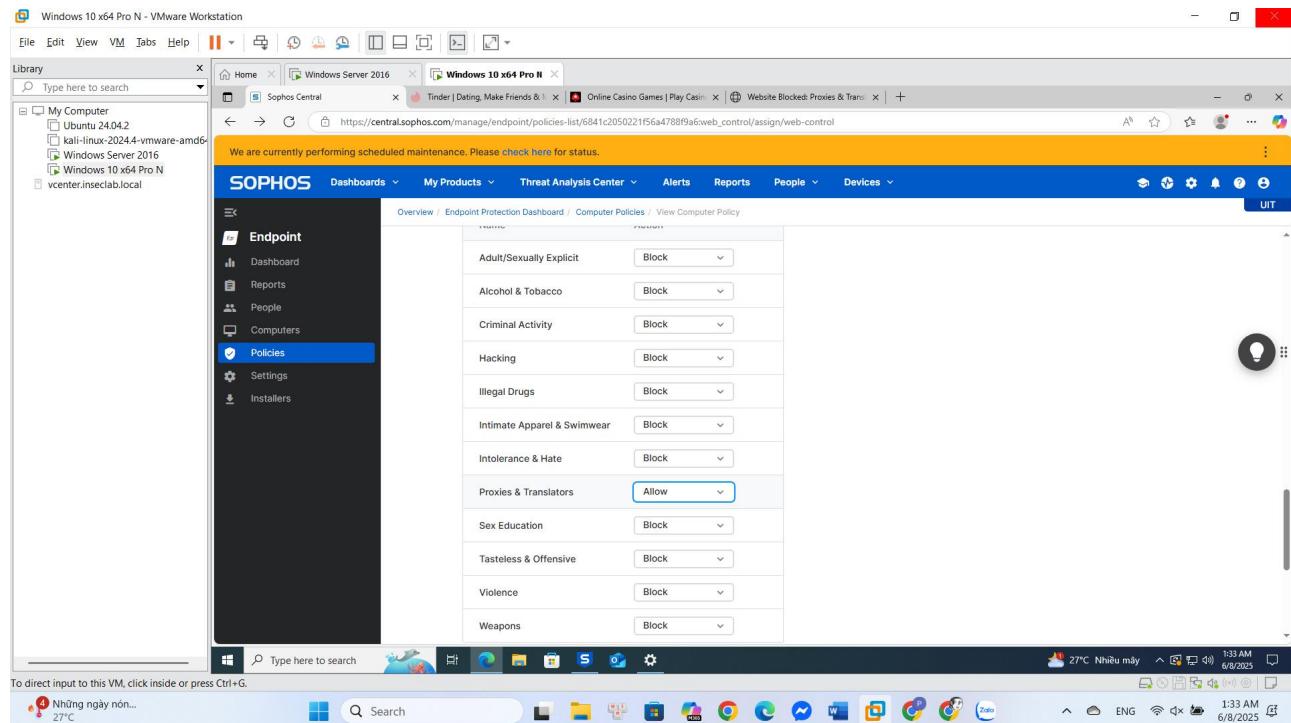
Chỉnh sửa policy Web Control bằng cách bật tính năng Web Control và chọn chặn danh mục Gambling (Cờ bạc/Pokerstars).



Chọn cảnh báo cho danh mục Personals & Dating (Kết bạn và hẹn hò/Tinder).



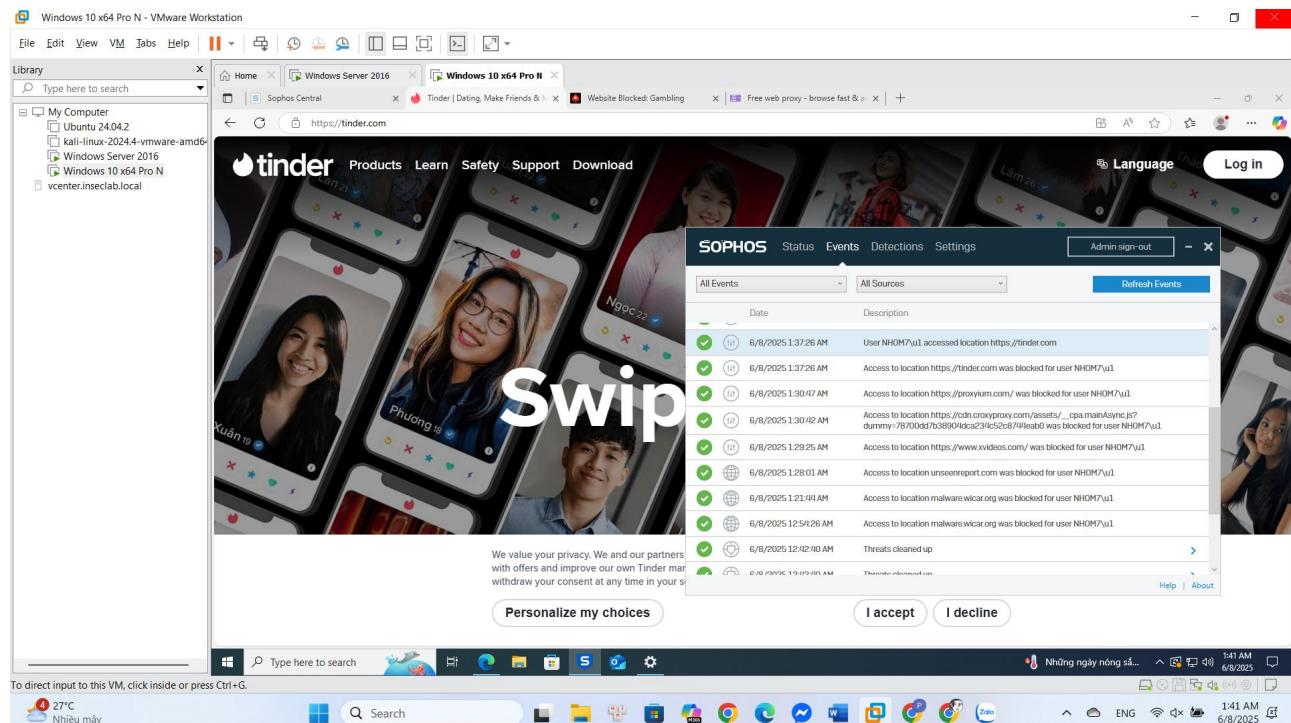
Cho phép danh mục Proxy & Translator (Proxyium).



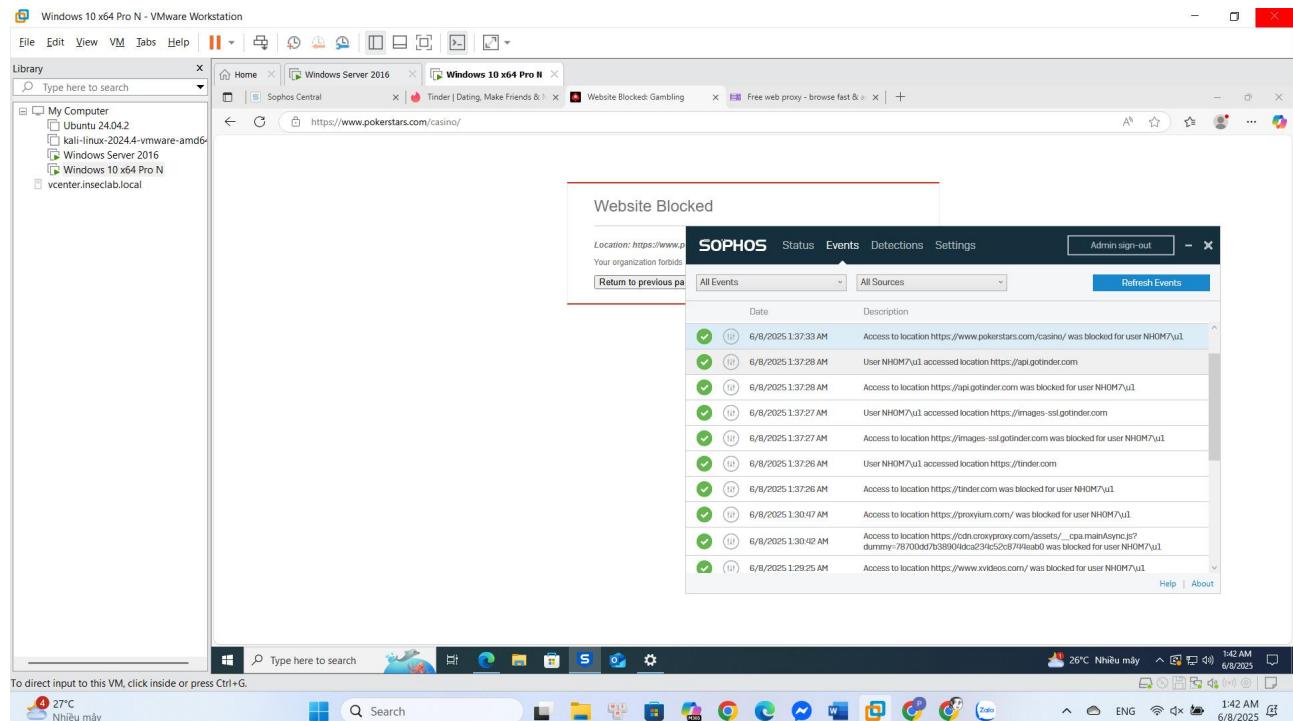
Trên máy Windows 10, dùng trình duyệt truy cập các website thuộc danh mục bị chặn.

Quan sát kết quả ta thấy:

- Tinder không bị chặn nhưng có cảnh báo từ Sophos.



- Pokerstars bị chấn và có cảnh báo từ Sophos.



- Proxyium không bị chặn và không bị cảnh báo từ Sophos.

