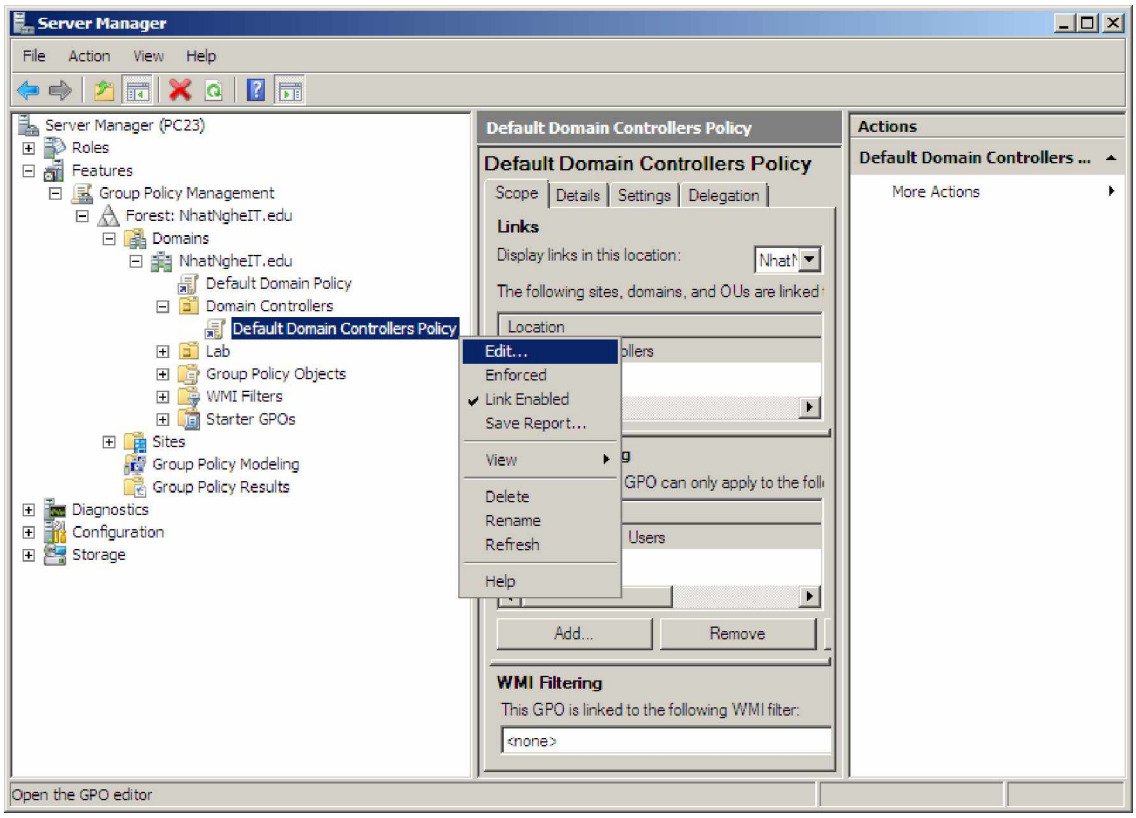
9. Thiết lập GPO giám sát hoạt động truy cập tài nguyên

MỤC TIÊU: Giám sát việc truy cập thành công, trái phép và xóa tài nguyên

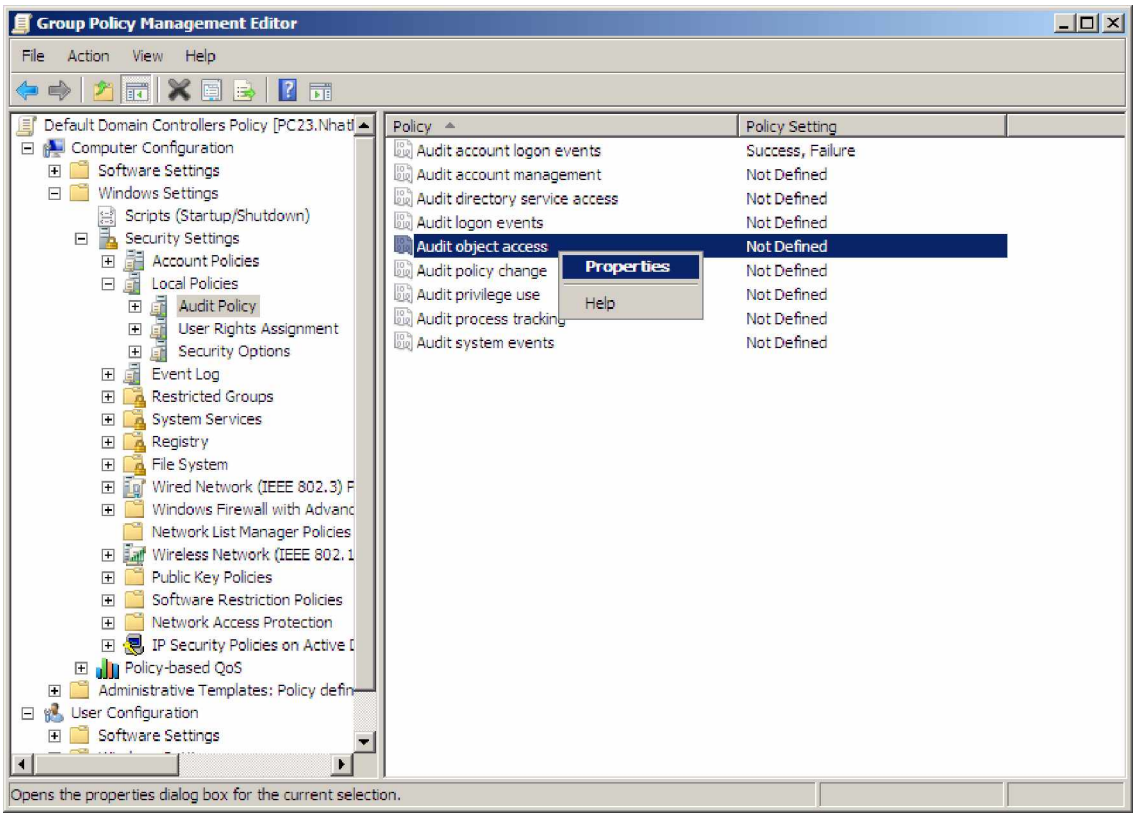
THỰC HIỆN: trên Server

B1. Điều chỉnh GPO Default Domain Controllers Policy

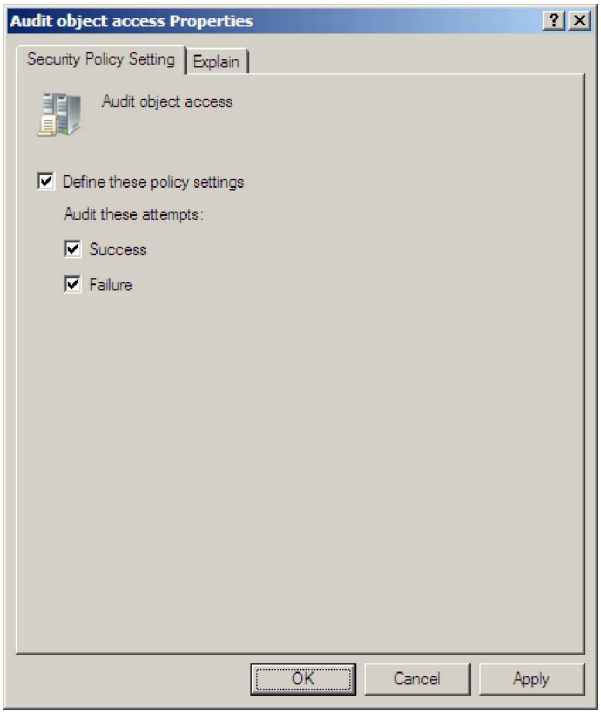
Cửa sổ Server Manager: theo đường dẫn > Click phải Default Domain Controllers Policy > Edit



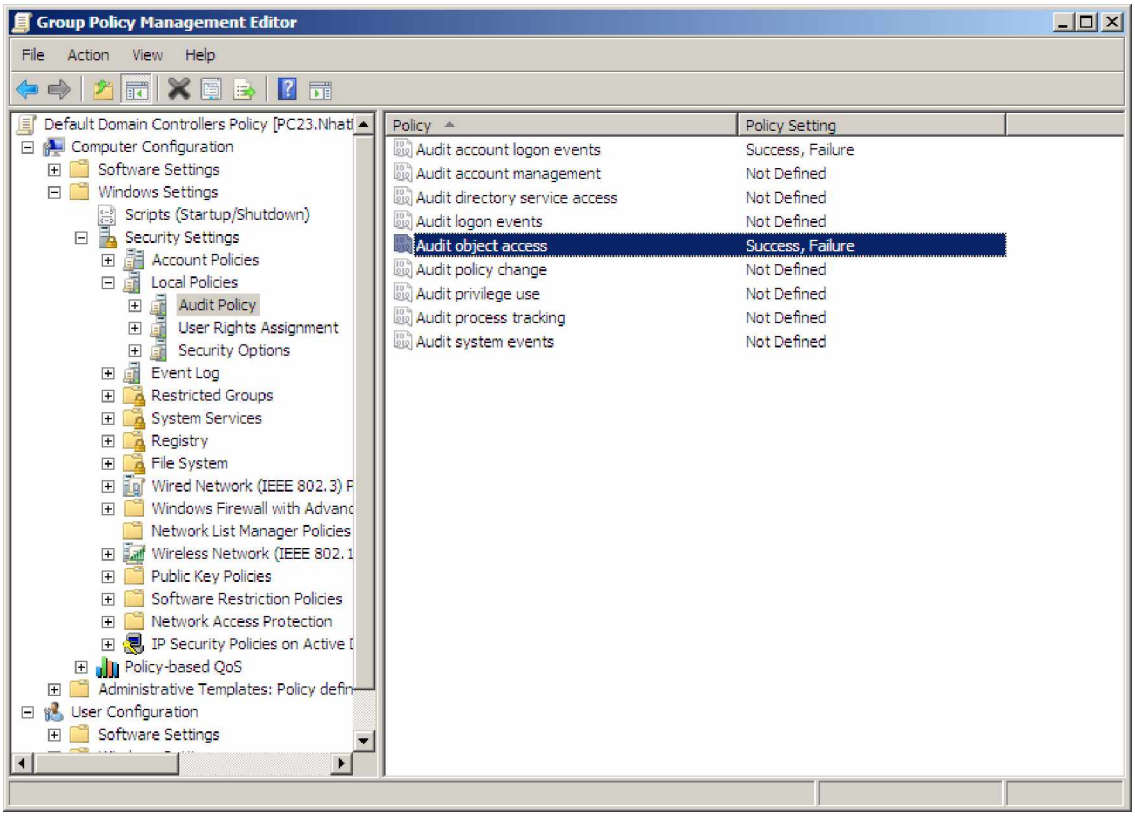
Cửa sổ Group Policy Management Editor: theo đường dẫn > Chọn Audit Policy > Click phải Audit object access > Properties



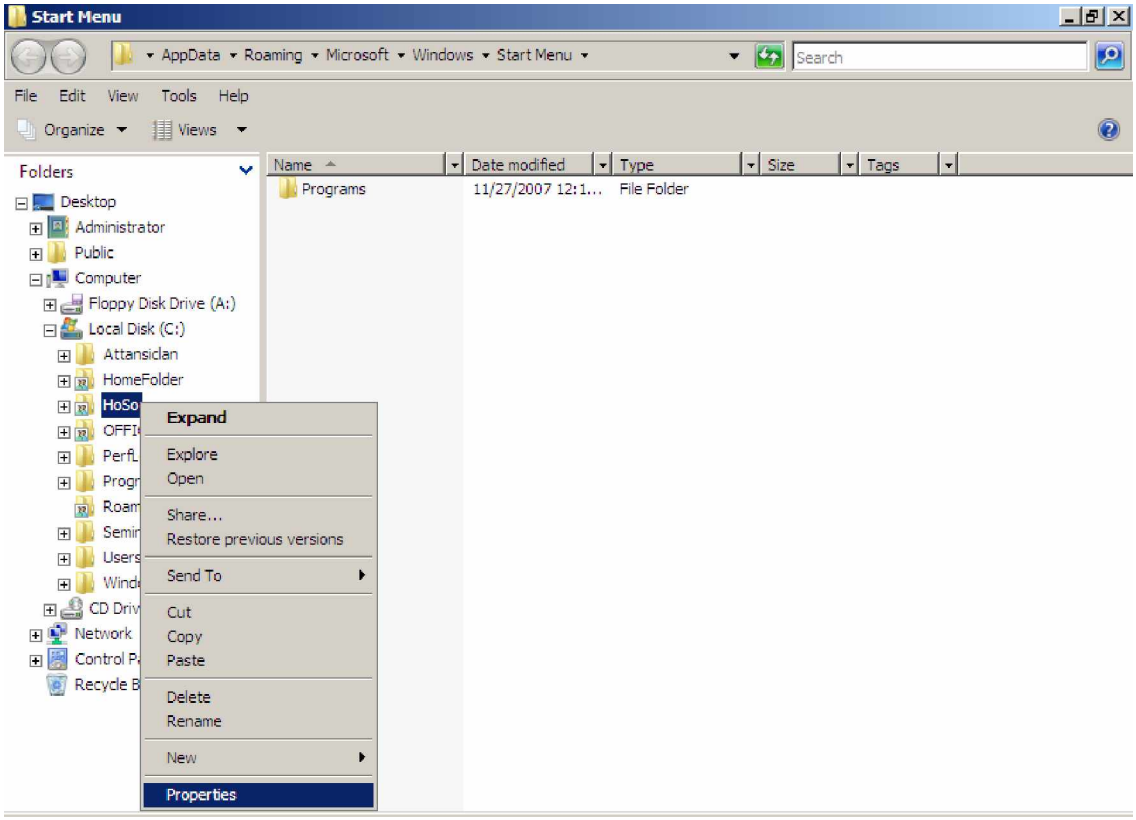
Hộp thoại Audit object access > Chọn Success và Failure > OK



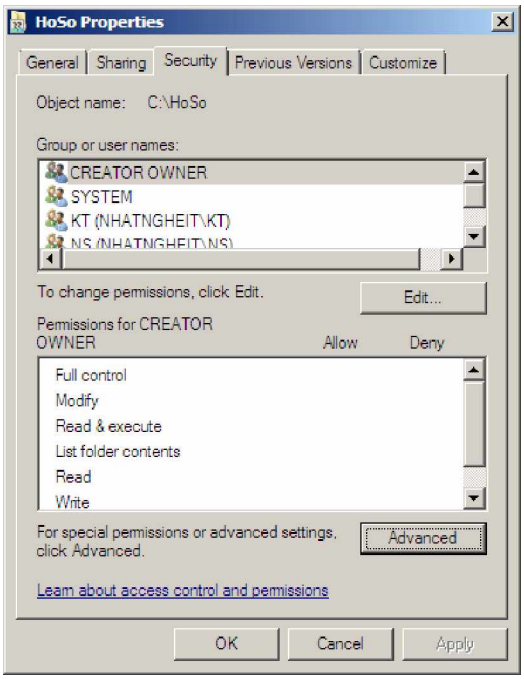
Kết quả


Group Policy Management Editor
File Action View Help
Default Domain Controllers Policy [PC23.Nhatl
Computer Configuration
Software Settings
Windows Settings
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) P
Windows Firewall with Advanc
Network List Manager Policies
Wireless Network (IEEE 802.1
Public Key Policies
Software Restriction Policies
Network Access Protection
IP Security Policies on Active D
Policy-based QoS
Administrative Templates: Policy defin
User Configuration
Software Settings
Policy
Policy Setting
Audit account logon events
Success, Failure
Audit account management
Not Defined
Audit directory service access
Not Defined
Audit logon events
Not Defined
Audit object access
Success, Failure
Audit policy change
Not Defined
Audit privilege use
Not Defined
Audit process tracking
Not Defined
Audit system events
Not Defined

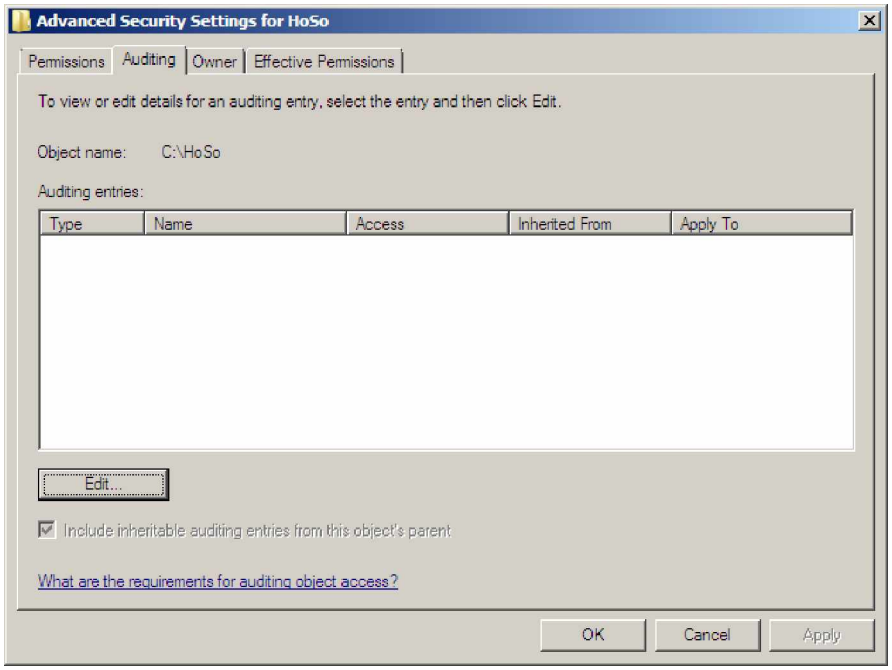
B2. Khai báo đối tượng và hành động cần giám sát trên tài nguyên
Cửa sổ Windows Explorer: Click phải thư mục HoSo > Properties



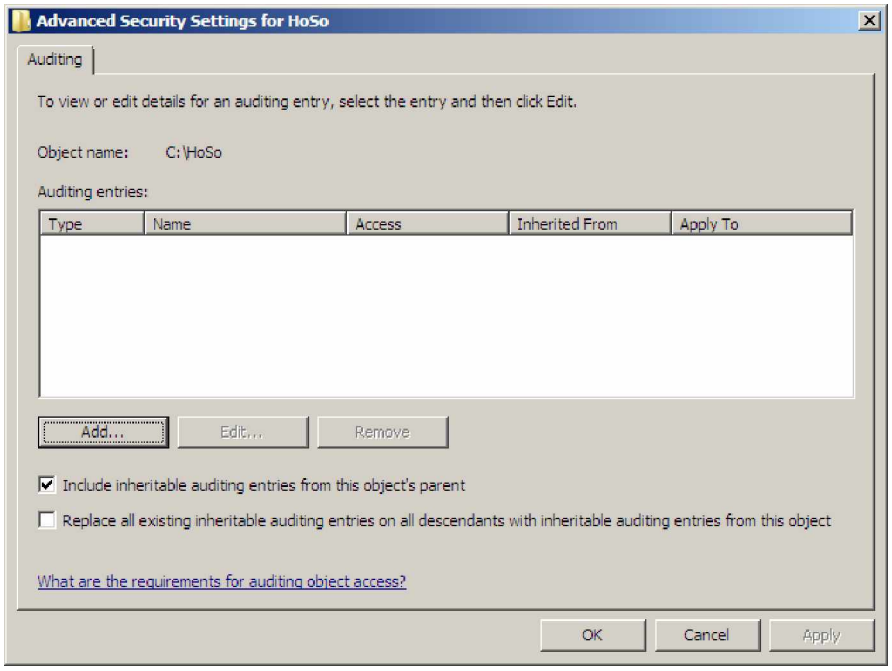
Hộp thoại HoSo properties > Tab Security > Advanced



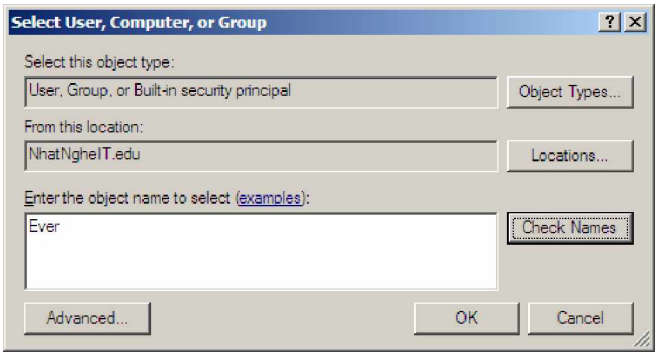
Hộp thoại Advanced Security > Tab Auditing > Edit

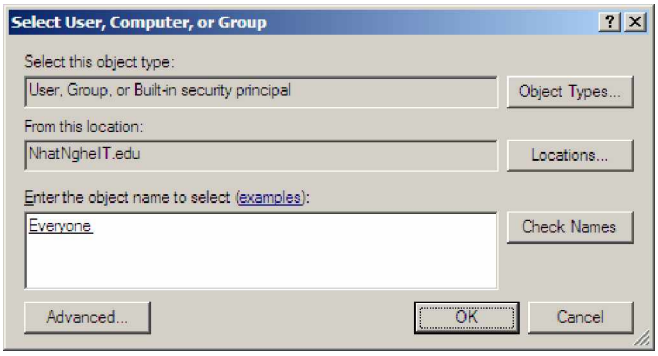


Hộp thoại Advanced Security > Add



Hộp thoại Select user > Nhập ***Ever*** > Check Names > OK



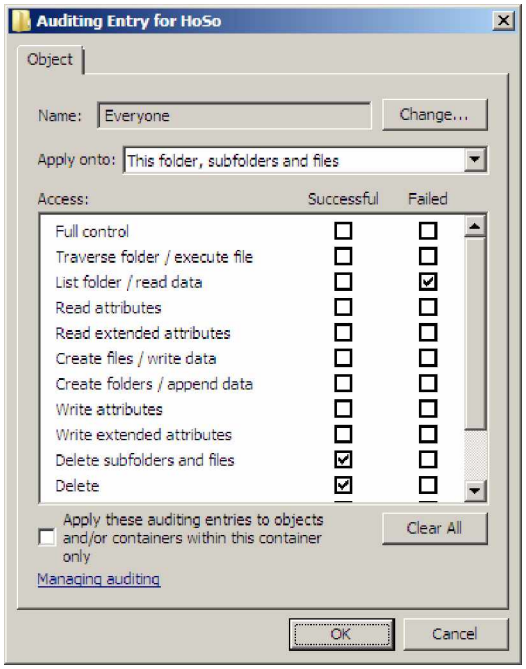


Hộp thoại Auditing Entry > Đánh dấu check

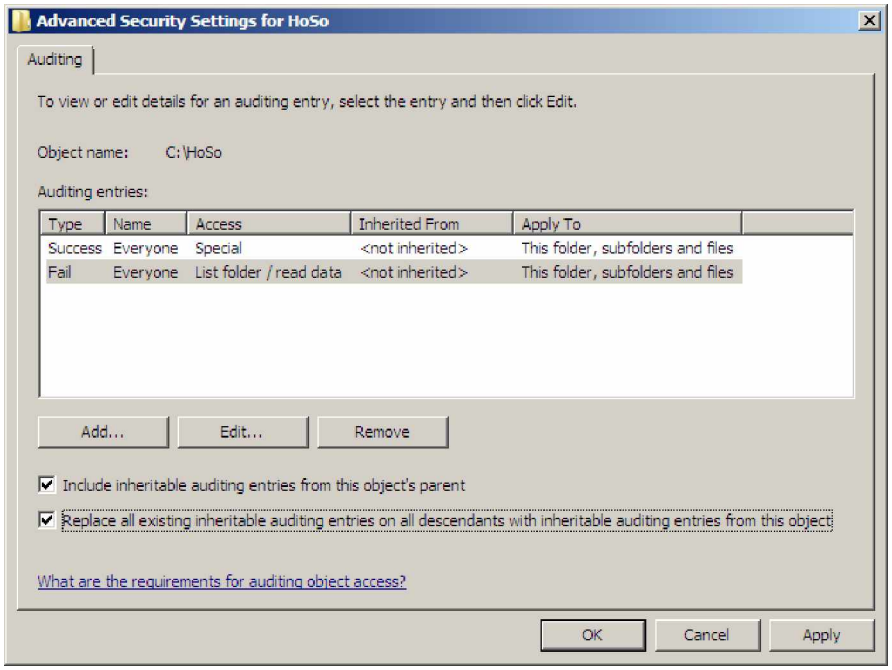
Delete subfolders and files và Delete: Successful

List Folder / Read data: Failed

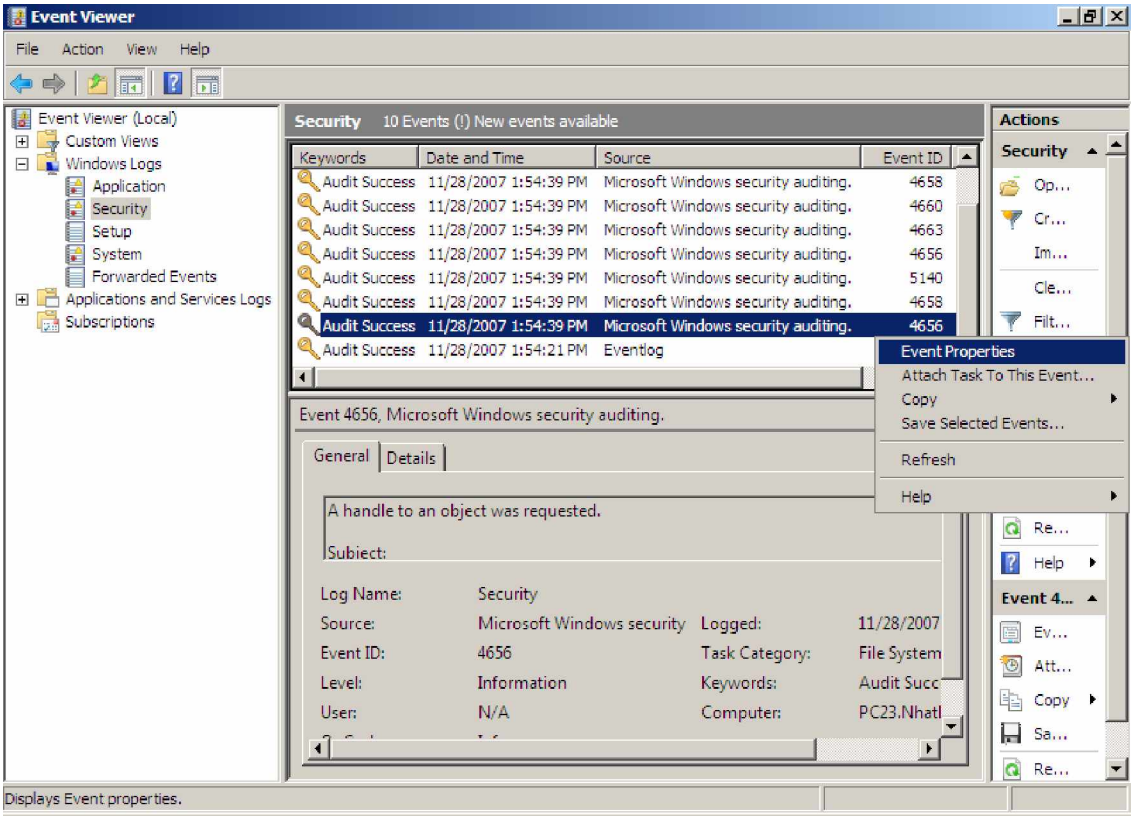
OK



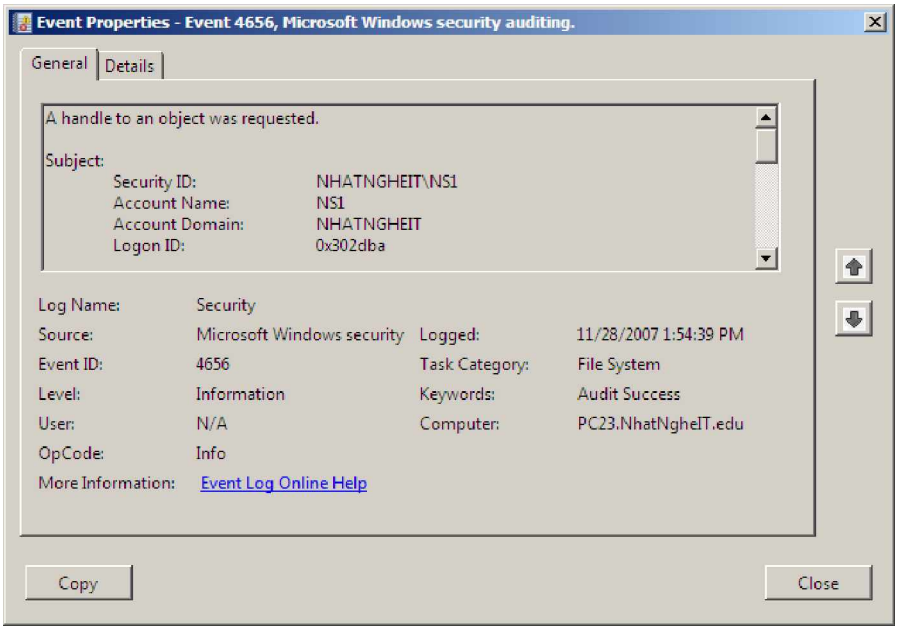
Hộp thoại Advanced Security > Check Replace all exiting… > OK > OK > OK

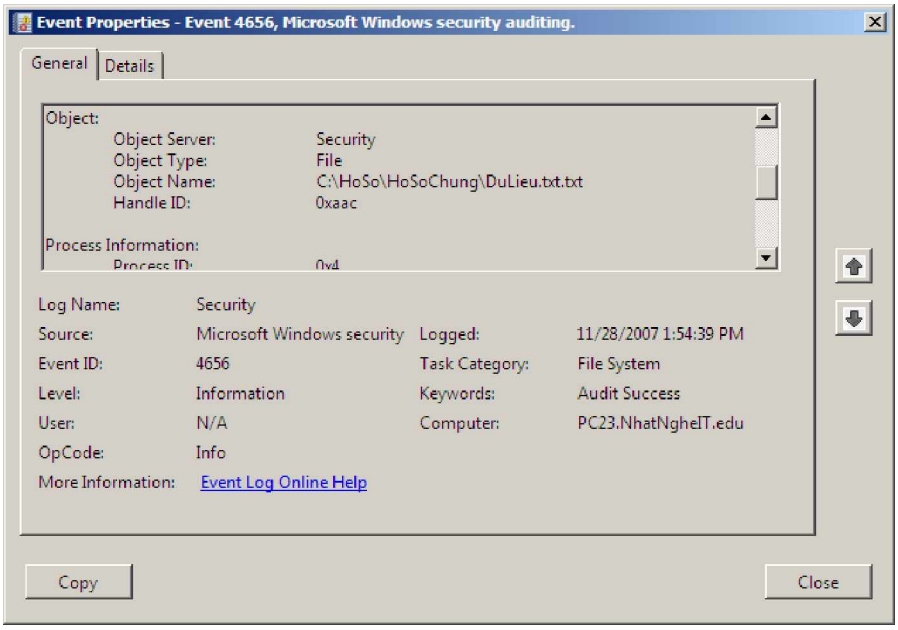


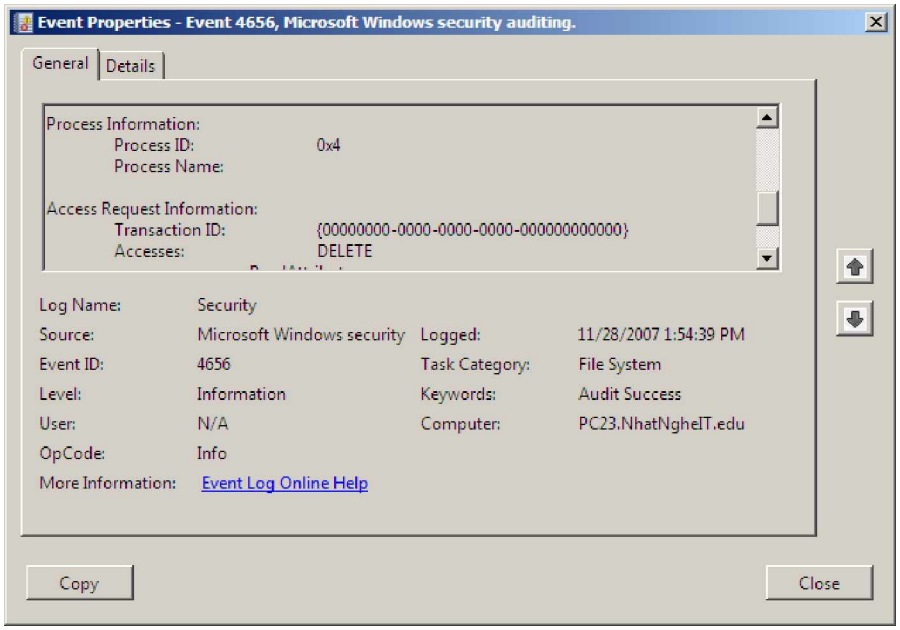
B3. Thử nghiệm xóa dữ liệu:
Hộp thoại Event Viewer: theo đường dẫn > Security > Click phải lên dòng có Event ID là 4656 > Event Properties



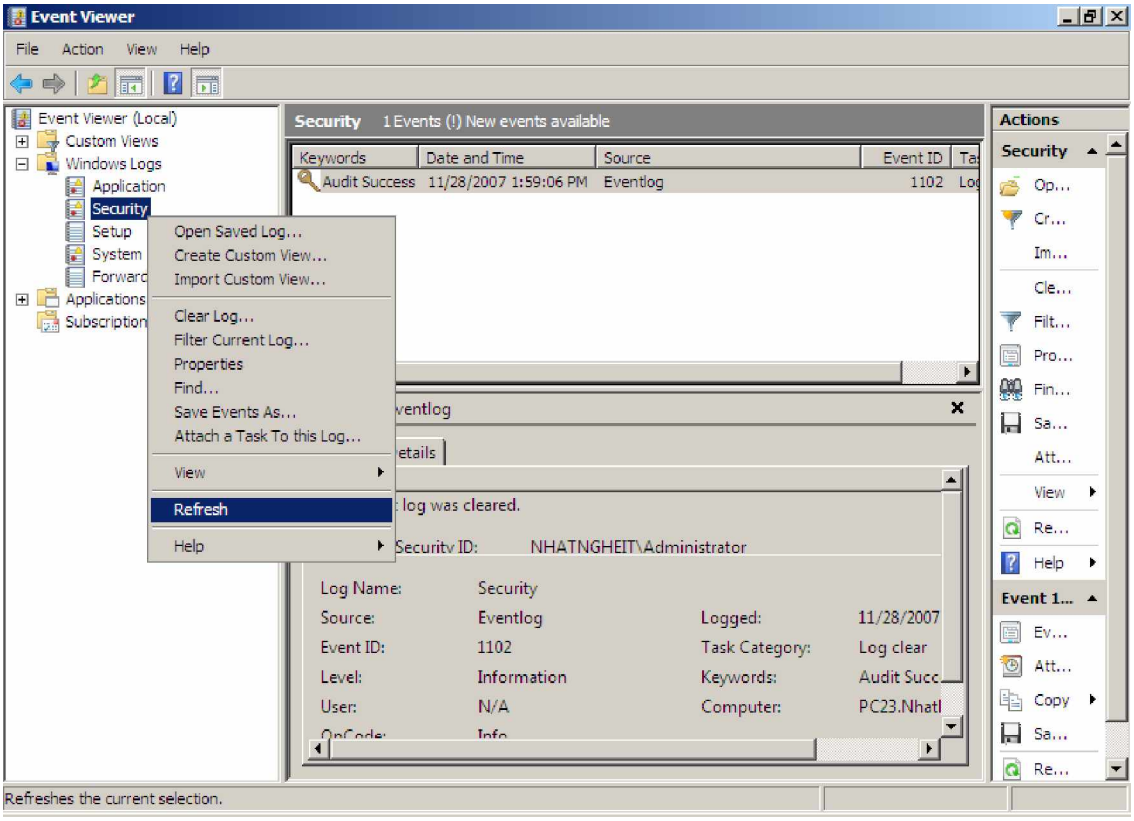
Quan sát kết quả thấy NS1 đã Delete file Dulieu.txt



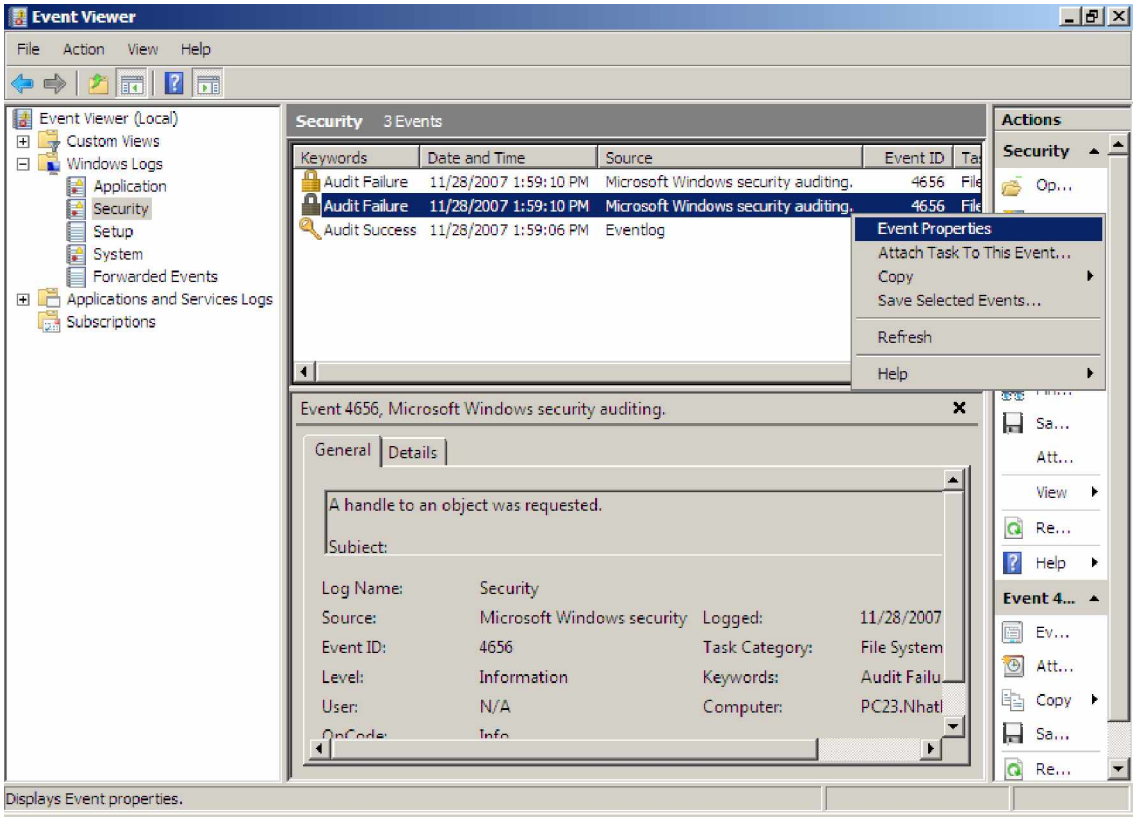




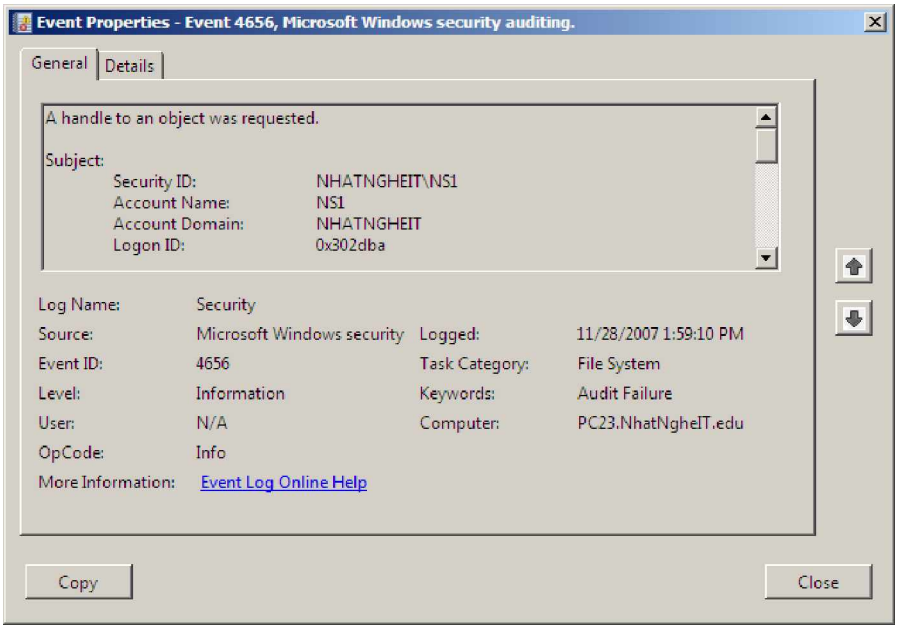
Hộp thoại Event Viewer: theo đường dẫn > Security > Click phải Refesh

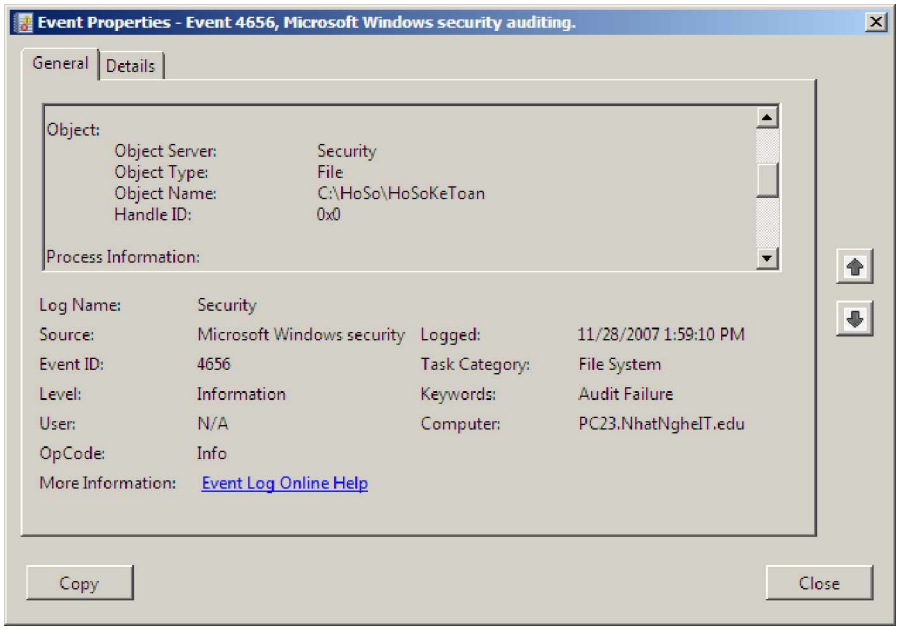


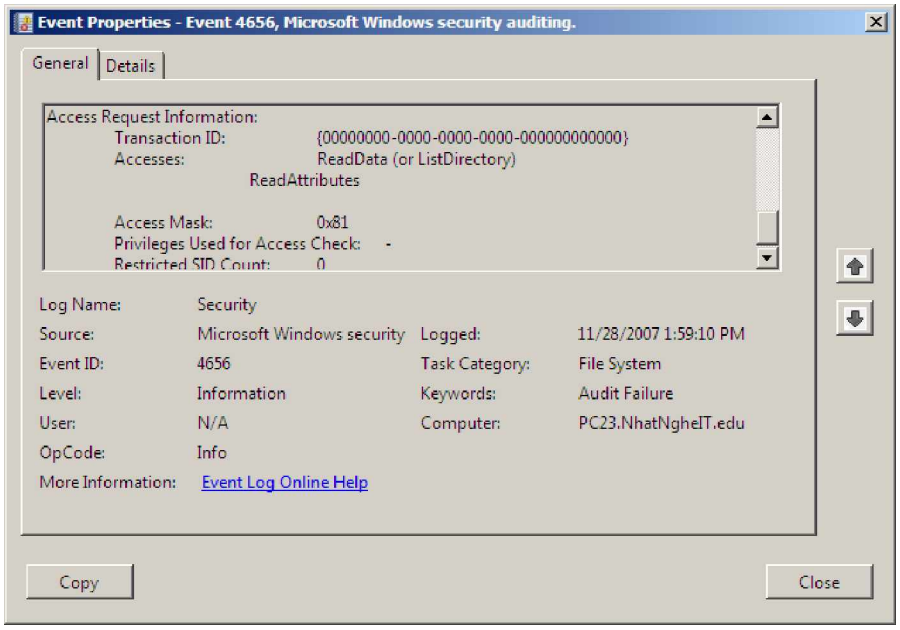
Hộp thoại Event Viewer: theo đường dẫn > Security > Click phải lên dòng có Event ID là 4656 > Event Properties



Quan sát kết quả thấy NS1 truy cập không được folder HoSoKeToan




Event Properties - Event 4656, Microsoft Windows security auditing.
General
Details
Object:
Object Server: Security
Object Type: File
Object Name: C:\HoSo\HoSoKeToan
Handle ID: 0x0
Process Information:
Log Name: Security
Source: Microsoft Windows security
Logged: 11/28/2007 1:59:10 PM
Event ID: 4656
Task Category: File System
Level: Information
Keywords: Audit Failure
User: N/A
Computer: PC23.NhatNgheIT.edu
OpCode: Info
More Information: Event Log Online Help
Copy
Close


Event Properties - Event 4656, Microsoft Windows security auditing.
General
Details
Access Request Information:
Transaction ID: {00000000-0000-0000-0000-000000000000}
Accesses: ReadData (or ListDirectory)
ReadAttributes
Access Mask: 0x81
Privileges Used for Access Check: -
Restricted SID Count: 0
Log Name: Security
Source: Microsoft Windows security
Logged: 11/28/2007 1:59:10 PM
Event ID: 4656
Task Category: File System
Level: Information
Keywords: Audit Failure
User: N/A
Computer: PC23.NhatNgheIT.edu
OpCode: Info
More Information: Event Log Online Help
Copy
Close