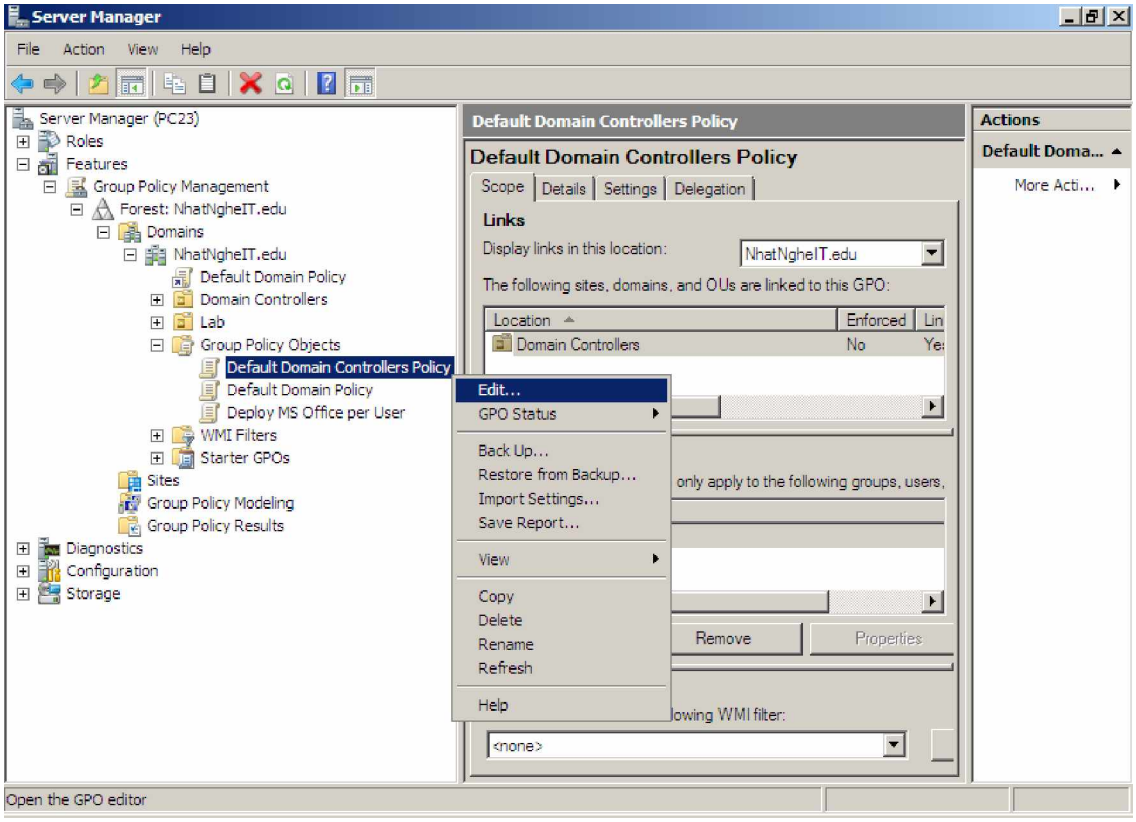
8. Thiết lập GPO giám sát hoạt động đăng nhập

MỤC TIÊU: Giám sát sự kiện đăng nhập của User

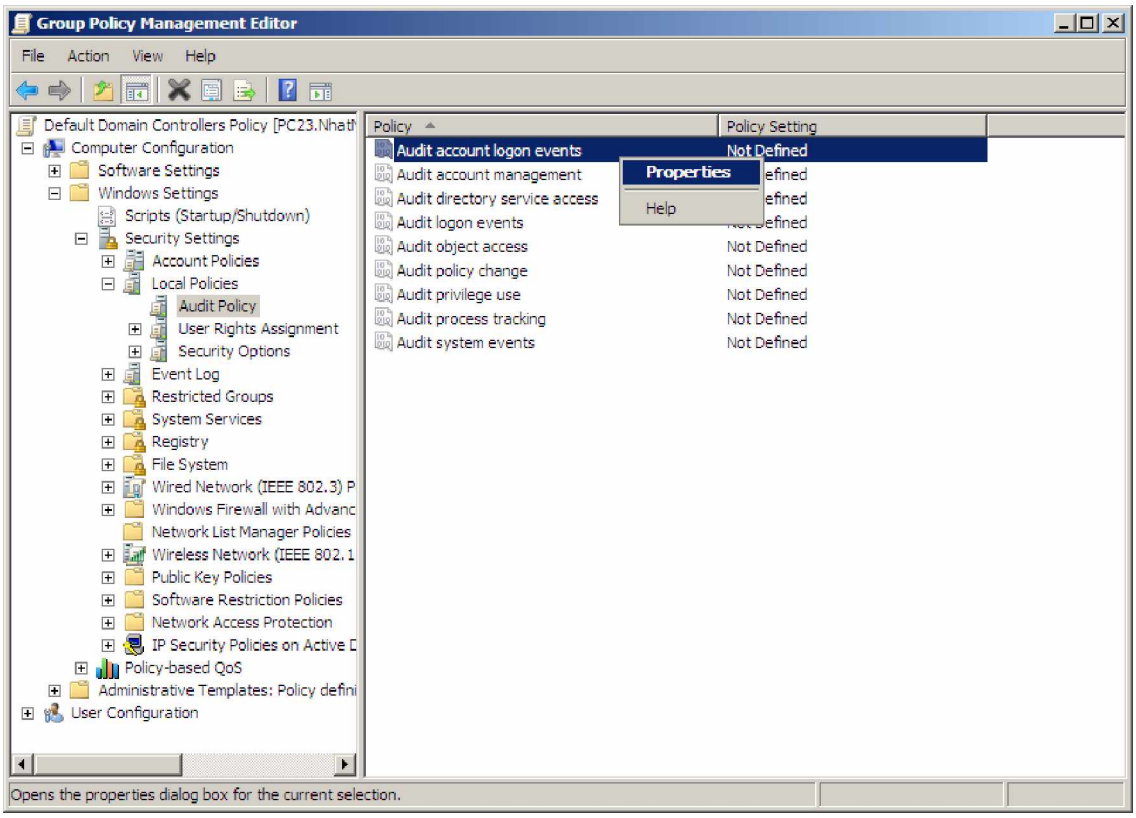
THỰC HIỆN: trên server

B1. Điều chỉnh GPO Default Domain Controller Policy

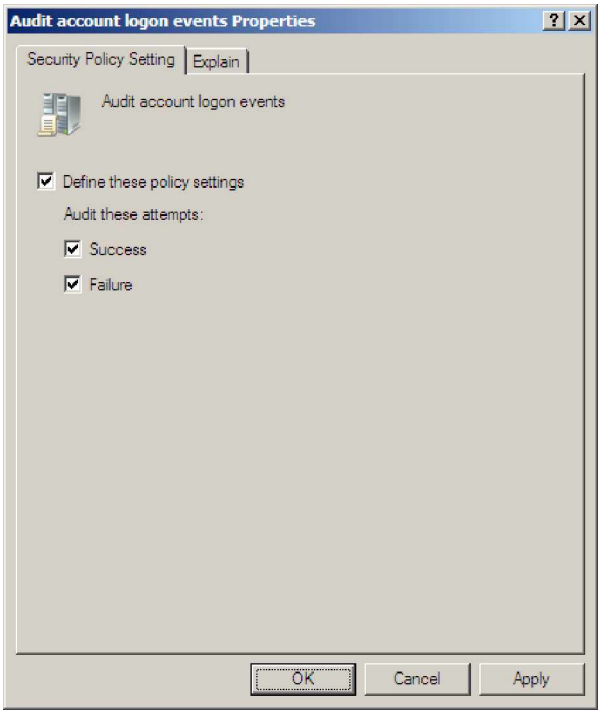
Cửa sổ Server Manager: theo đường dẫn > Click phải Default Domain Controllers Policy > Edit



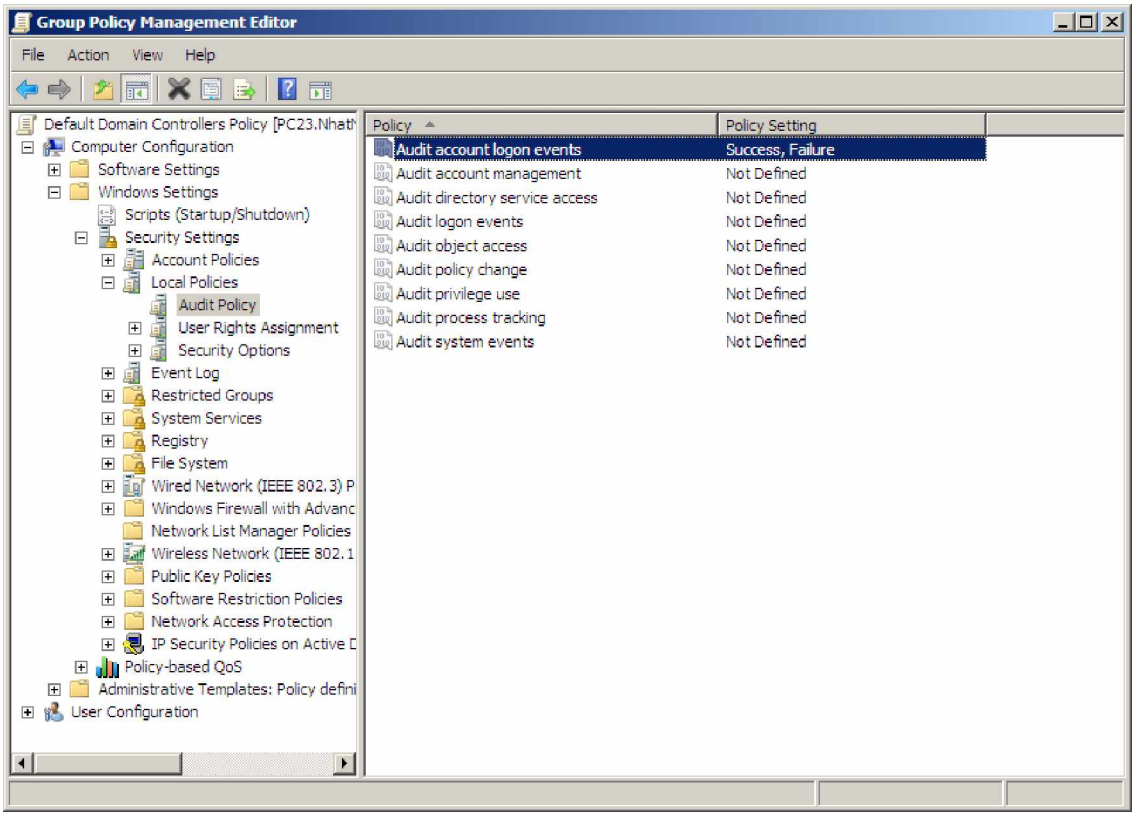
Cửa sổ Group Policy Management Editor: theo đường dẫn > Chọn Audit Policy > Click phải Account Logon Events > Properties



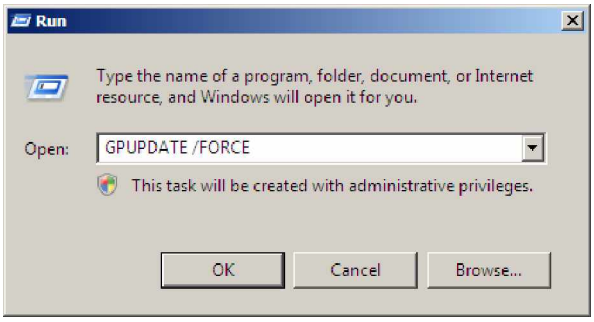
Hộp thoại Audit object access > Chọn Success và Failure > OK



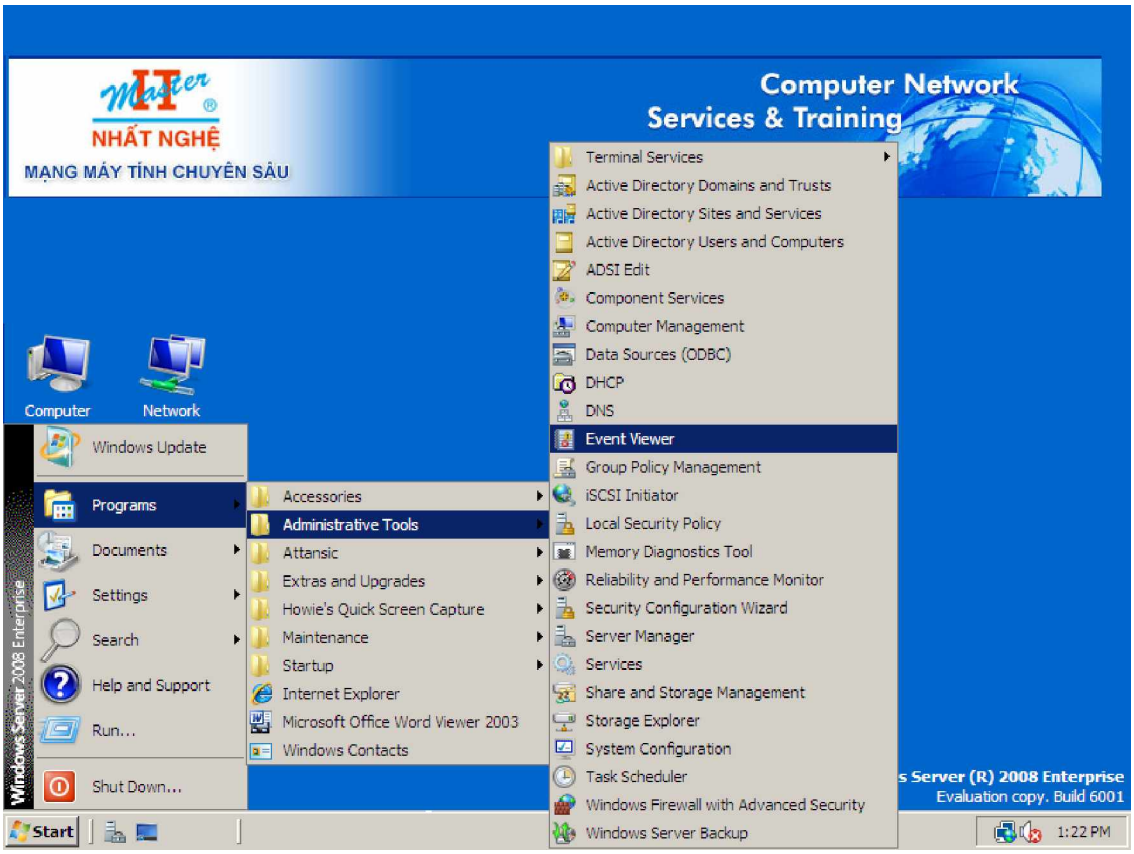
Kết quả



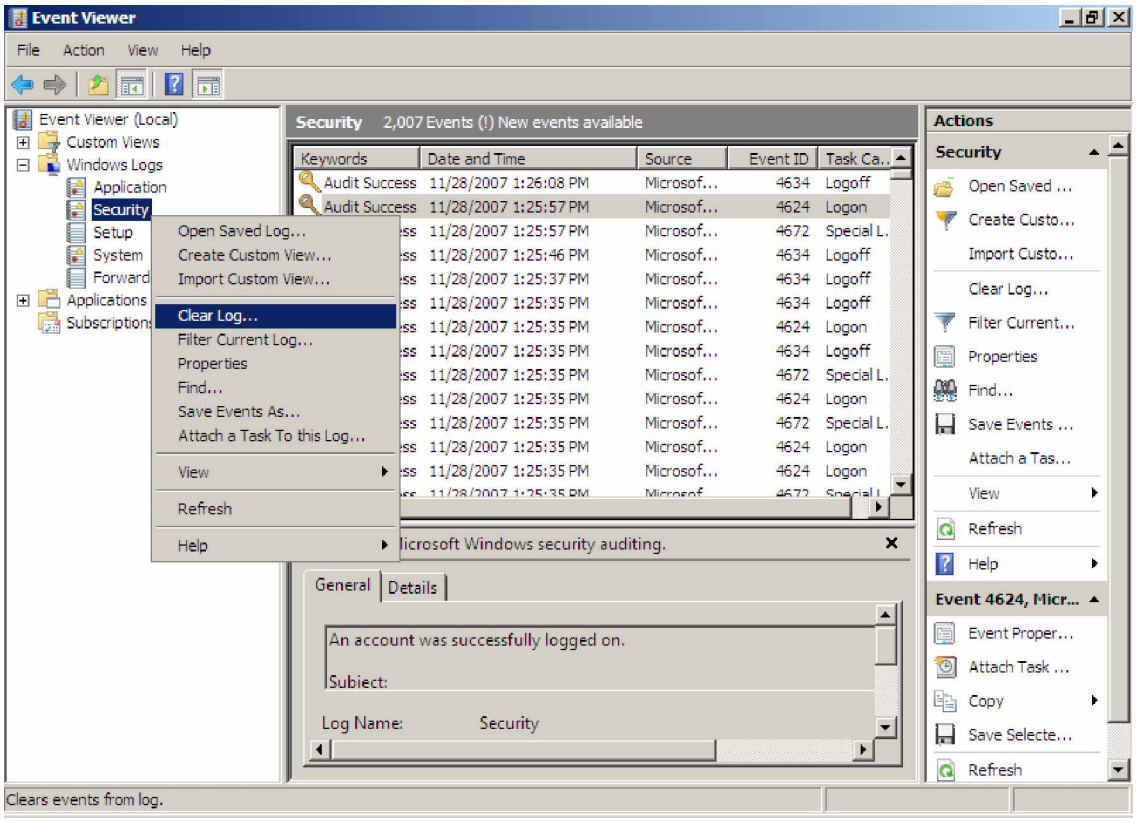
Start > Run > Nhập ***GPUPDATE /FORCE*** > OK



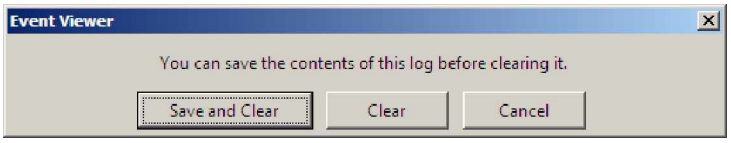
B2. Lưu log file và xóa sự kiện hiển thị
Start > Programs > Administrative Tools >Event Viewer



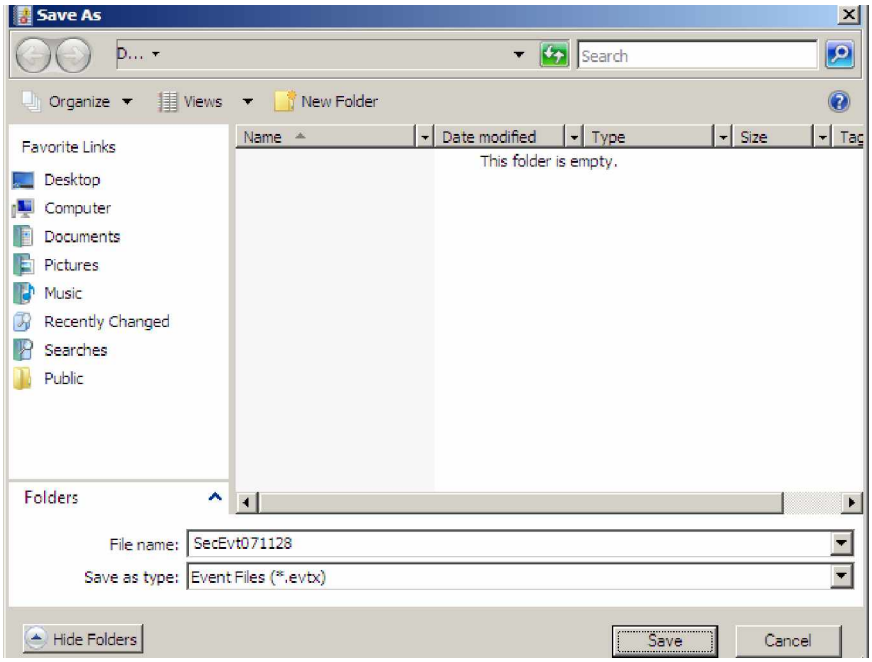
Hộp thoại Event Viewer: theo đường dẫn > Click phải Security > Clear log



Cửa sổ Event Viewer > Save and Clear

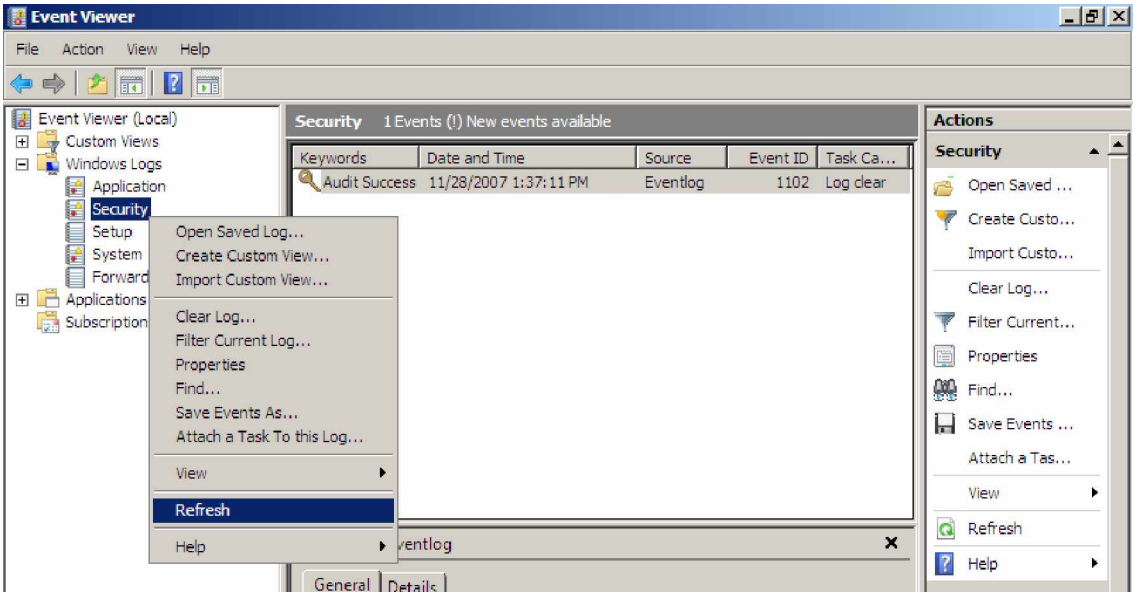


Lưu lại file SecEvt071128.evtx



Thử nghiệm trên WS: Trên màn hình Logon: UserName: ***KT1***, Password: ***BAYBA*** (cố tình nhập sai để giả lập trường hợp dò password).

Kiểm tra: Trên Server
Hộp thoại Event Viewer: theo đường dẫn > Click phải Security > Refresh



Thấy trong Log ghi nhận quá trình đăng nhập và chứng thực của user KT1: Failed