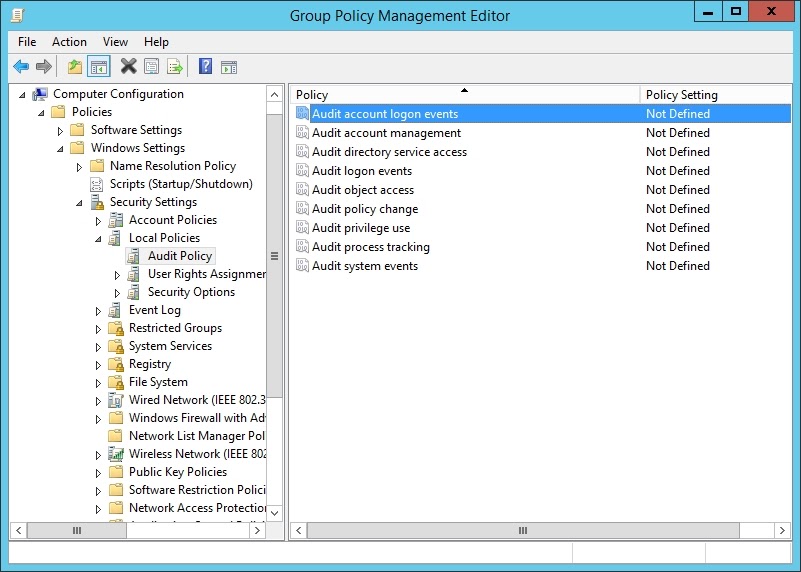
**Bài 11: MCSA 2019 – Audit – Các tiêu chí kiểm tra bảo mật cần biết trong windows**

**Việc chuẩn đoán các yếu tố ảnh hưởng đến hiệu xuất cũng như các nguy cơ về bảo mật luôn là công việc chán nhất trong công việc quản trị hệ thống. Tuy nhiên nó lại là công việc rất quan trọng mà bất cứ quản trị viên nào cũng phải biết để phục vụ tốt công việc của mình. Tham khảo bài viết: MCSA 2019 – Audit – Các tiêu chí kiểm tra bảo mật cần biết trong windows server để biết thêm nhé.**

**Một số khái niệm**

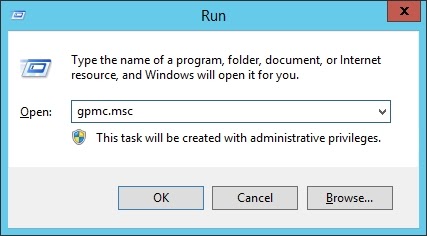
**Các policy audit**

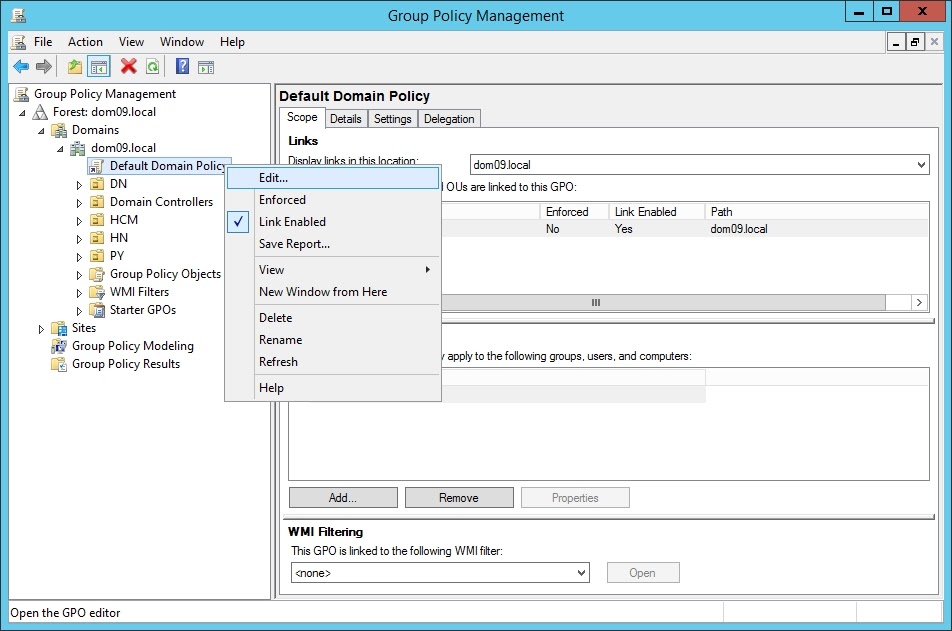
* **Account management:**tạo, xóa, sửa các đối tượng trong AD hay PC
* **Directory service access:** kiểm tra stop / start dịch vụ trong AD hay PC
* **Log events:** logon user từ xa lên máy tính AD hoặc PC
* **Object access:** kiểm soát việc tạo, sửa, xóa, các folder, file, printer
* **Policy change:** thay đổi policy
* **Privilege use**: kiểm soát việc chiếm quyền chủ sở hữu
* **Process tracking**: theo dõi thực thi các tiến trình ứng dụng
* **System events**; khởi động và shutdown hệ thống



**Mở audit policy**

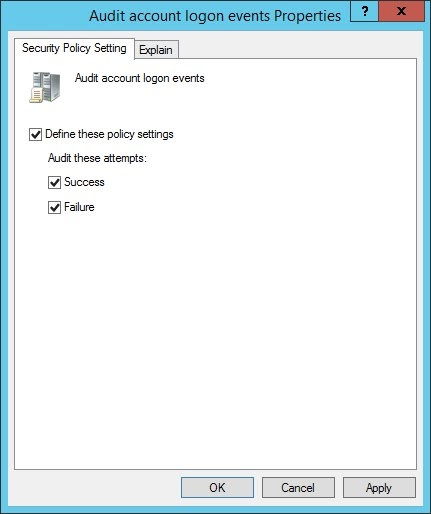
**Start run → gpmc.msc → computer configuration → policy → window setting → security setting → local policy → audit policy**

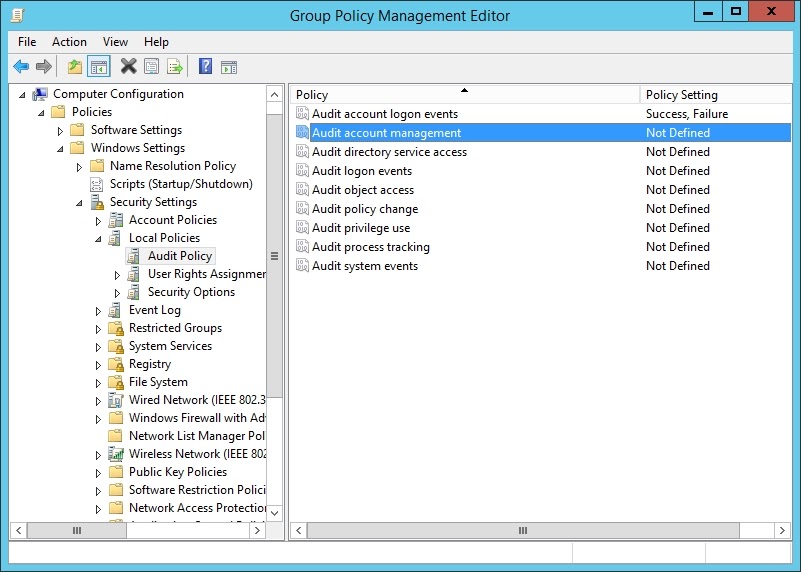


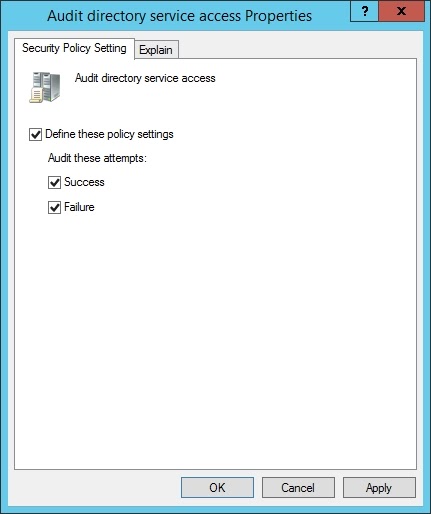


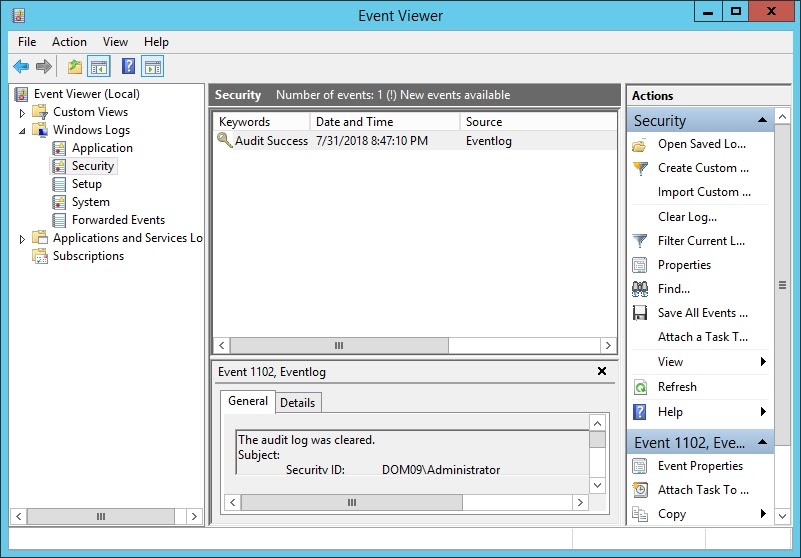
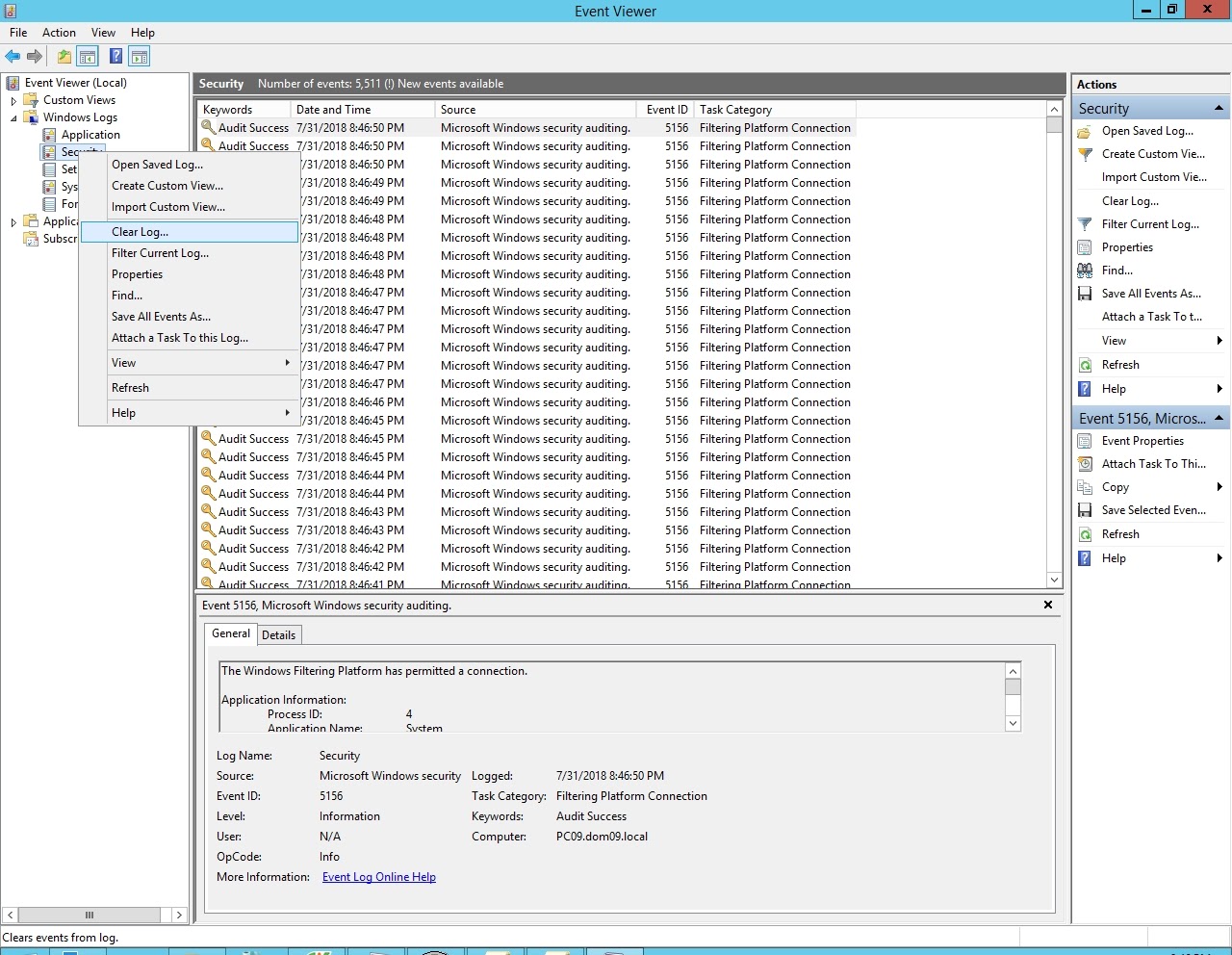
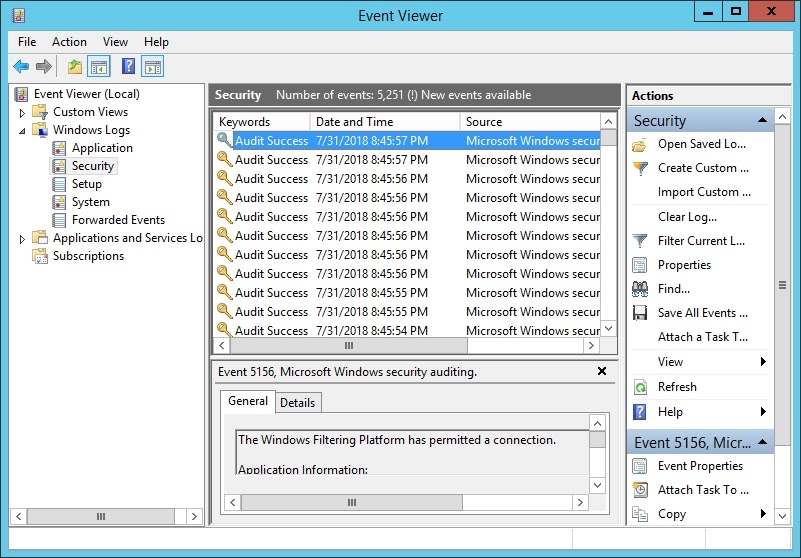
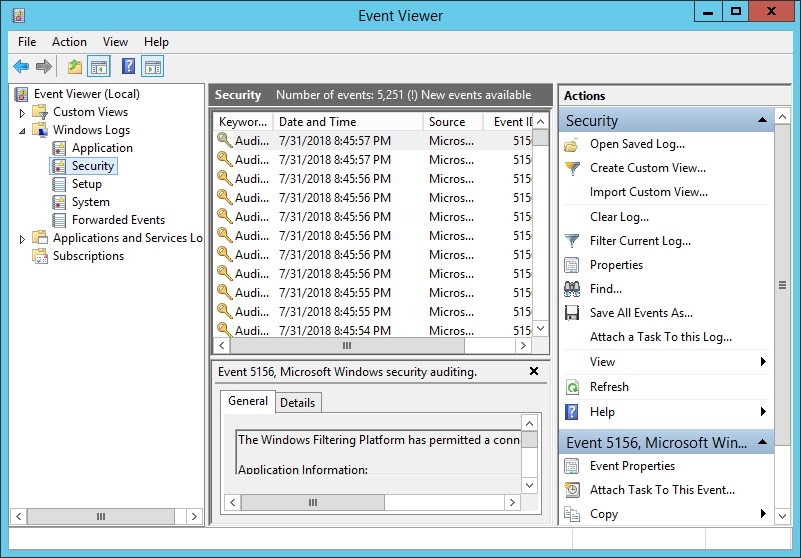
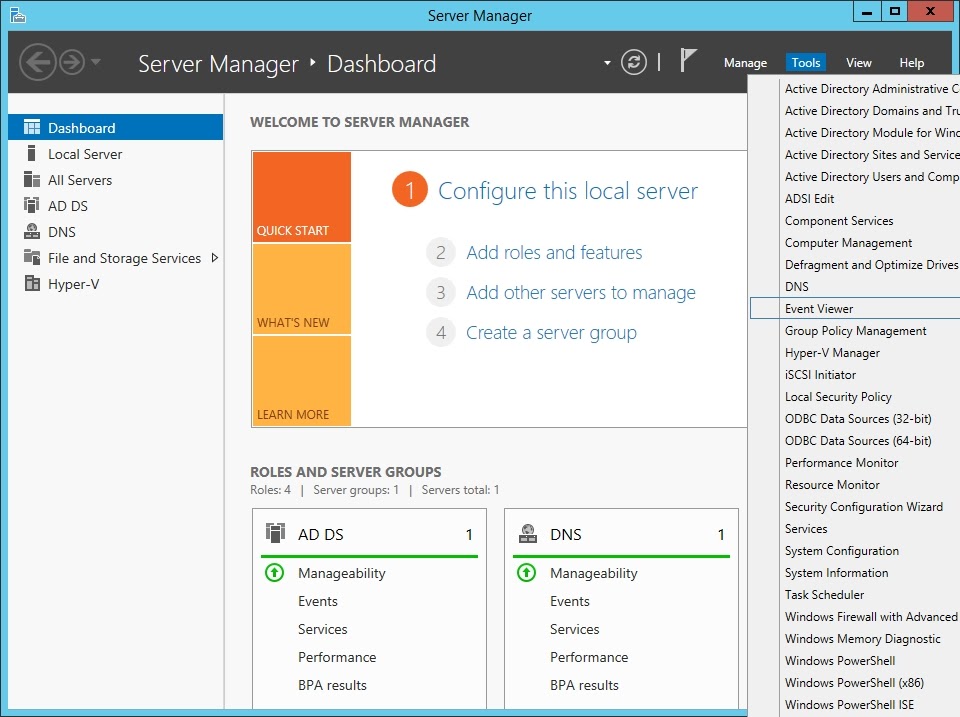
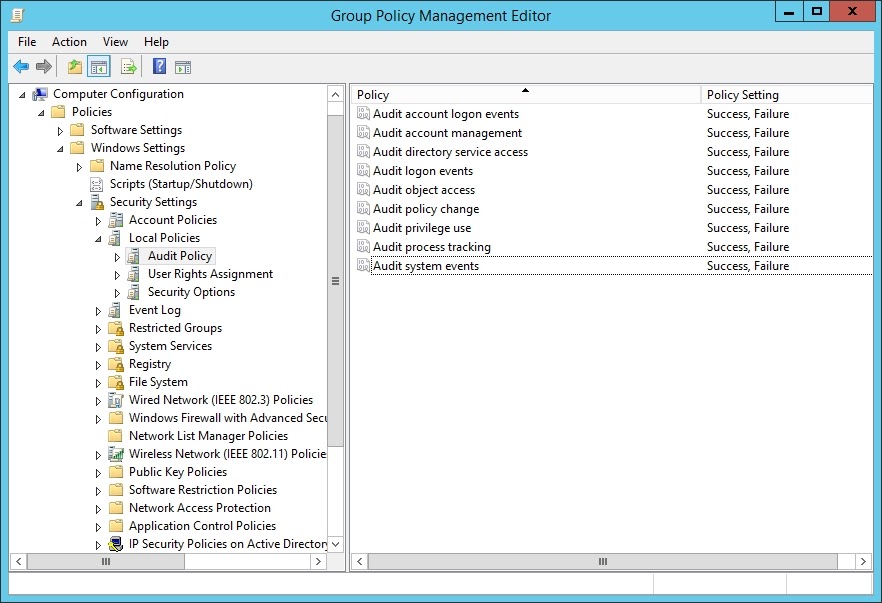
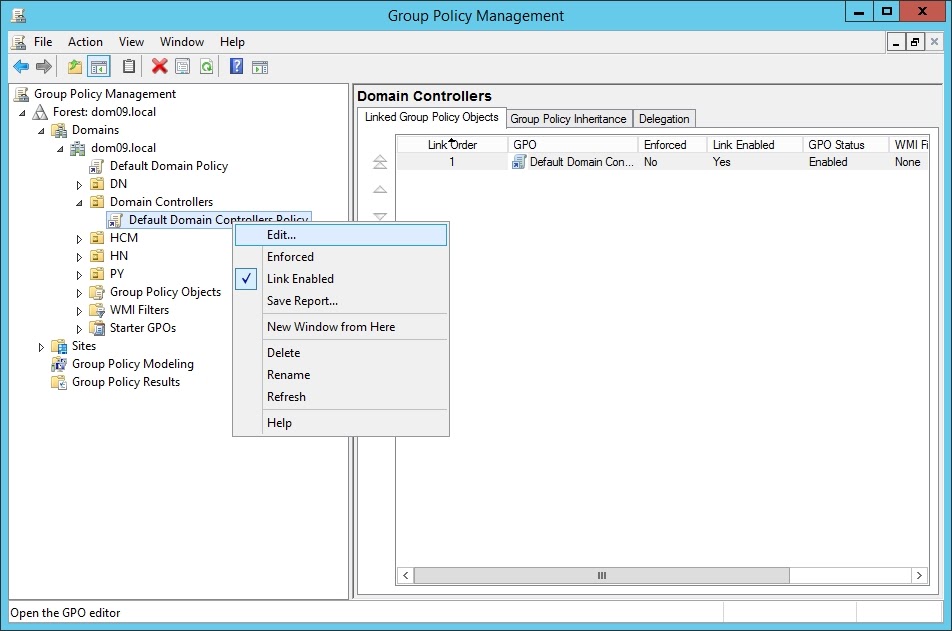
**Nơi xem sự kiện được audit**

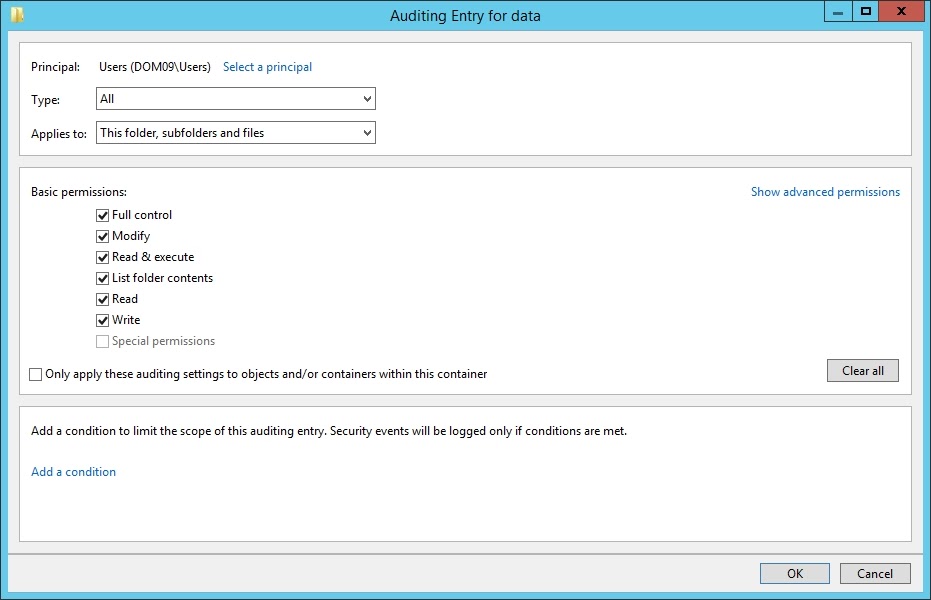
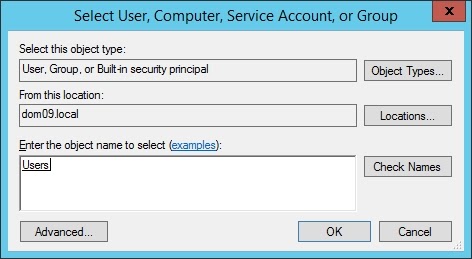
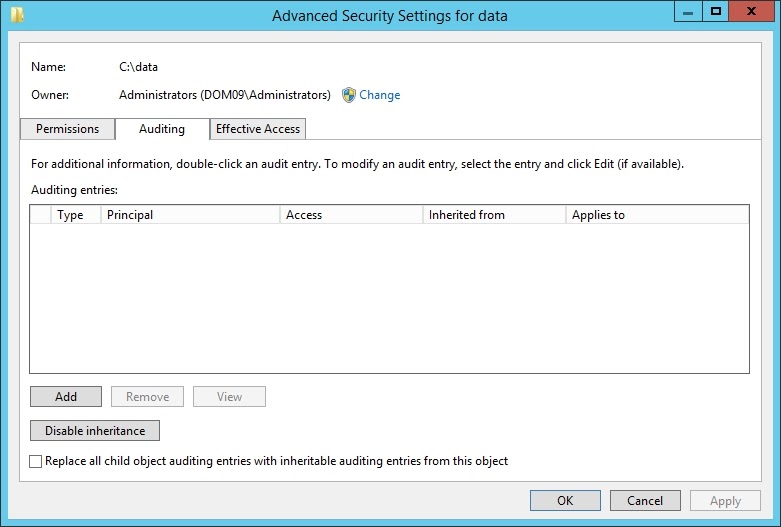
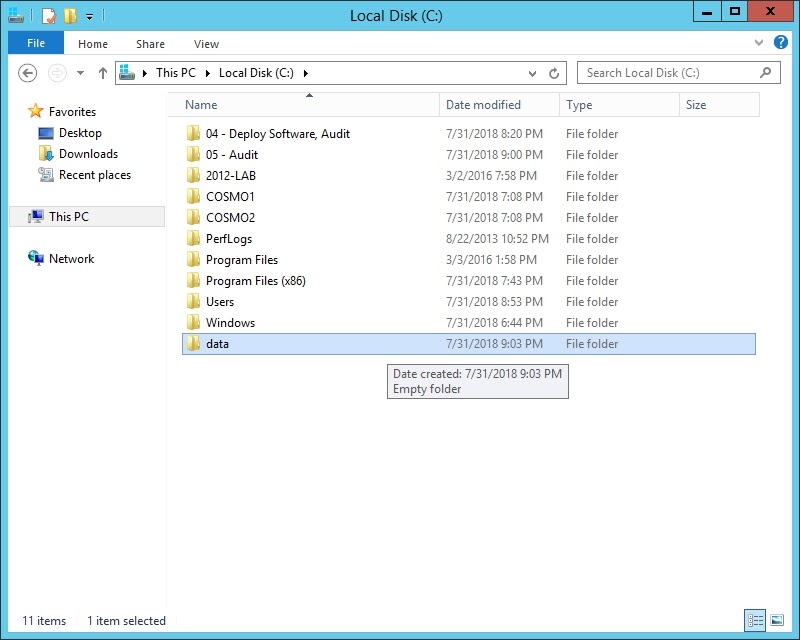
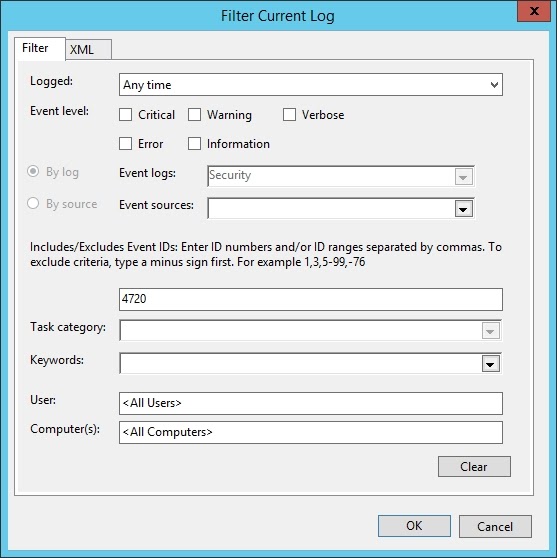
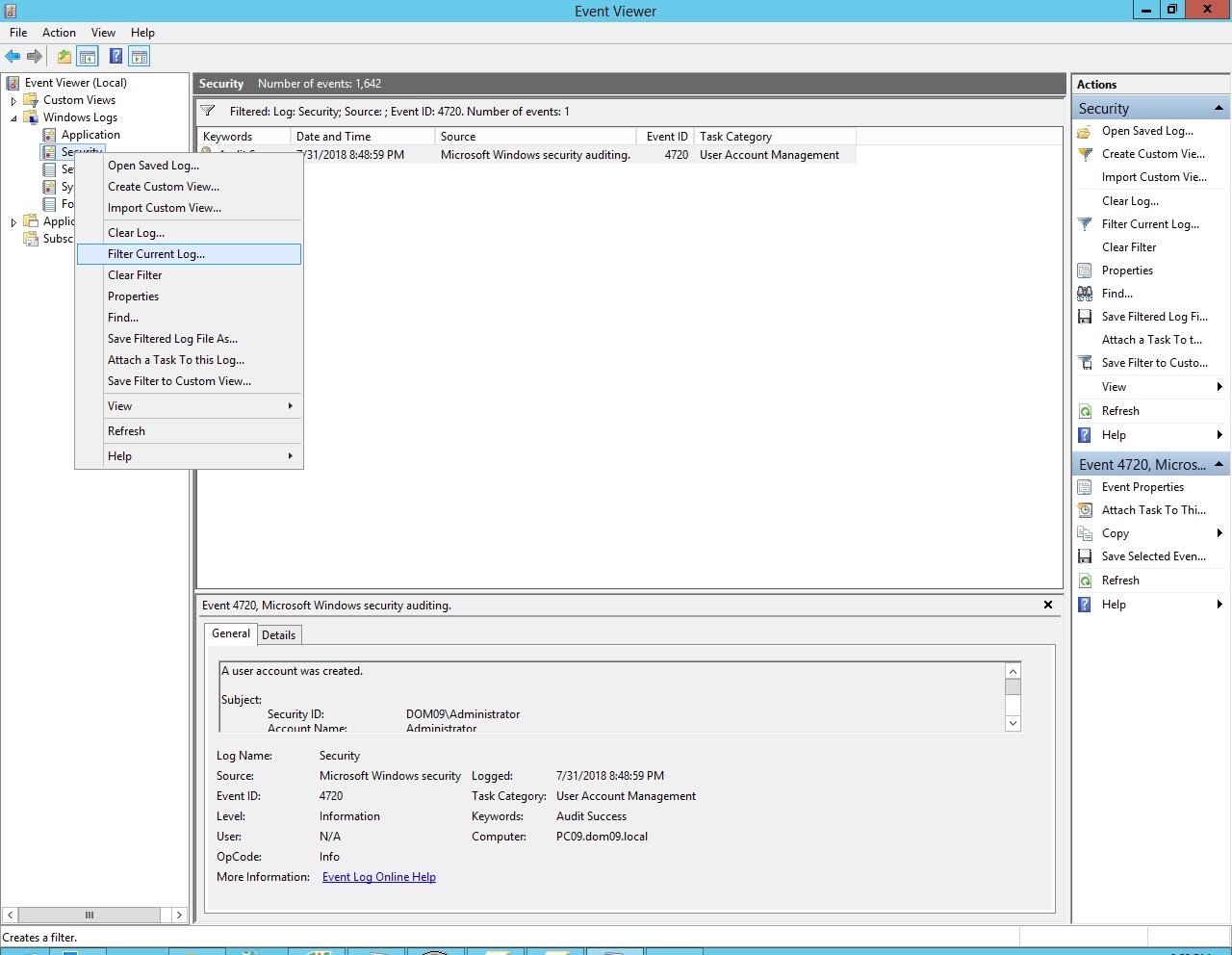
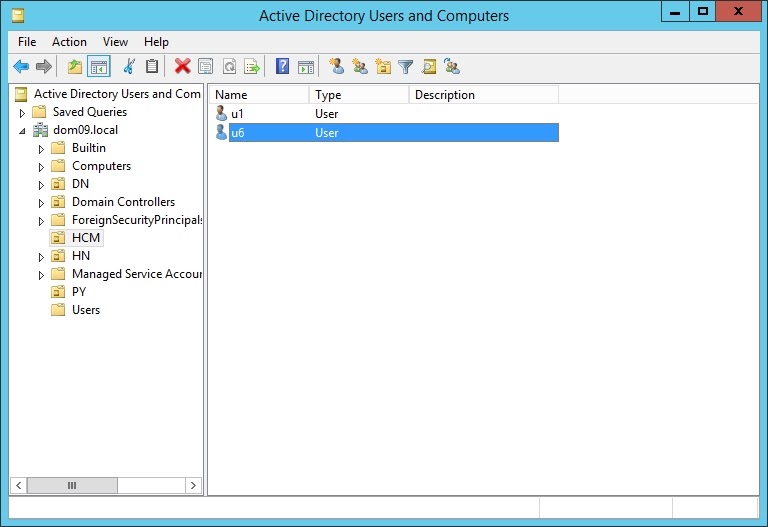
* **Server manager → tool → event viewer**
* Một số mã code sự kiện
  + **4720 → tạo user mới**
  + **4626 → login fail**
  + **4624 → logon success**
  + **1200 → service shutdown**











Dùng client test lại nhé!!!