**NTFS**

**I. LÝ THUYẾT**

1. **NTFS permission:**

NTFS permissionlà phân quyền chỉ có trên ổ đĩa định dạng bằng hệ thống tập tin (file system) NTFS. Để cấu hình NTFS permission, ta vào tab **Security** trong **Properties** của tập tin (file) hay thư mục (folder).

1. **Các loạiNTFS permission**

NTFS permission nằm trong 2 nhóm: Standard permission và Special permission

* 1. **Standard permission**:chung cho tập tin và thư mục
     + **Read**: cho thấy tên các tập tin và thư mục, độc dữ liệu trong tập tin, xem thuộc tính, xem permission, xem chủ sở hữu của các tập tin và thư mục
     + **Write**: cho phép user có thể tạo tập tin, thư mục; ghi dữ liệu vào tập tin; không có quyền xóa các tập tin và thư mục của người khác tạo ra.
     + **Modify**: cho phép user xem các tập tin, thư mục; thực thi các tập tin, tạo file, ghi dữ liệu vào tập tin, tạo các thư mục con (subfolder)
     + **Full Control**: cho phép user thay đổi permission trên tập tin và thư mục; take ownership trên tập tin và thư mục; thực thi các thao tác có trong permission khác.
     + Riêng thư mục còn thêm một permission là **List Folder Contents**: cho phép user được thấy các thư mục và tên các tập tin. Không được mở các tập tin

Trong bảng phân quyền có hai cột là **Allow** và **Deny**. Ta có 2 cách Deny

* + - Nếu để cấu chọn trong cột deny cho một user thì ta gọi là **cấm tường minh**
    - Trường hợp nếu một user không được phân quyền gì cả thì user d0ó được gọi là **cấm ngầm định**.
    - **Cấm tường minh có độ ưu tiên cao nhất**
  1. **Special permission** (Advanced permission): đây là những permission chi tiết hơn **Standard permission**

Ví dụ: trong Standard permission gồm các Special permission là:

* + - Read data
    - Read attribute
    - Read extended attributes
    - Read permission

Có 2 special permission đặc biệt là: **Change Permission** và **Take OwnerShip**. **Administrator** bao giờ cũng có permission: **Take OwnerShip**

1. **Phân quyền của một user thuộc nhiều nhóm**

Một user account có thể thuộc về nhiều nhóm (group) khác nhau. Quyền thực sự của user sẽ là tổng hợp quyền trên các nhóm đó.

**Ví dụ:**

User U1 thuộc group G1 và G2. Thư mục cần xét là DATA

G1: Allow Read; G2: Allow Write 🡺 U1: Allow Read + Allow Write

G1: Allow Read; G2: Deny Read 🡺 U1: Deny Read (vì DENY ưu tiên hơn)

Chúng ta có thể xem quyền tổng hợp (effective permission) của từng user bằng cách vào Properties của tập tin hay thư mục cần xem 🡪 tab **Security** 🡪 nút **Advanced** 🡪 tab **Effective permission** 🡪 nút **Select** và tìm user muốn biết **Effective permission** của họ.

1. **Tính kế thừa**

Tính kế thừa là một hệ thống tự động sao chép nội dung của ACL (Access Control List) từ thư mục cha xuống cho các đối tượng con.

Chúng ta có thể ngăn chặn tính kế thừa này cho các tập tin và thư mục.

1. **Kết hợp Share permission và NTFS permission**

Khi kết hợp hai loại quyền (permission) khác nhau này cần lưu ý user đang logon locally hay logon from network

* Nếu user đang **logon locally** thì user đó chỉ bị hạn chế bởi quyền NTFS
* Nếu user đang **logon from Network** thì trong 2 permission, chọn các nào hạn hẹp nhất.

Ví dụ: trên thư mục DATA, bảng phần quyền cho user U1 như sau:

|  |  |  |
| --- | --- | --- |
| **Loại permission** | **Share permission** | **NTFS permission** |
| Phân quyền trên U1 | Allow Read | Allow Full Control |

* Nếu **U1** đang **logon locally** thì **U1** được **Allow Full Control** trên thư mục DATA
* Nếu **U1** đang **logon from Network** thì **U1** chỉ được **Allow Read**

*Trên ổ đĩa NTFS, để tiện theo dõi và phân quyền được thống nhất cho* ***logon locally*** *và* ***logon from network*** *thì người ta phần quyền Share (Share permission) cho* ***Everyone – Allow Full Control****. Khi đó phần quyền chỉ còn phụ thuộc vào NTFS.*

1. **Tác dụng của việc COPY và MOVE đối với phân quyền NTFS**

* Khi COPY một thư mục hay tập tin thì bản COPY sẽ kế thừa permission của thư mục cha.
* Khi MOVE (cut/paste) có 2 trường hợp
  + **Move cùng partition**: tập tin hay thư mục bị di chuyển vẫn giữ nguyên permission của nó
  + **Move khác partition**: thực chất khi move khác partition thì hệ thống làm 2 động tác:
    - Tạo 1 bản copy của tập tin hay thư mục trên phân vùng mới
    - Xóa tập tin hay thư mục trên phân vùng cũ

Đây chỉ là dạng COPY, nên khi MOVE khác partition, nó kế thừa quyền của thư mục cha.

**II THỰC HÀNH**

**Chuẩn bị 2 máy ảo:**

* Máy Windows Server 2003 làm Domain Controller
* Máy WinXP làm Client

**Yêu cầu:**

* Bỏ giớ hạn password (Domain Security Policy 🡪 Account Policy 🡪 Password Policy)
* Vào C:\ tạo cây thư mục sau:

**DATA**

**public**

**Ketoan**

**Nhansu**

**C:\**

* Tạo OU **KETOAN** và OU **NHANSU**
* Trong OU **KETOAN** tạo group **Ketoan**. Tạo các user: **KT1**, **KT2**, **KT3**. Add có user **KT1**, **KT2**, **KT3** vào group **Ketoan**
* Trong OU **NHANSU** tạo group **Nhansu**. Tạo các user: **NS1**, **NS2**, **NS3**. Add có user **NS1**, **NS2**, **NS3** vào group **Nhansu**
* Cho group **Ketoan** và group **Nhansu** có quyền **Allow Logon Locally** (***Domain Controller Security Policy 🡪 Local Policies 🡪 User Right Assignment***)
* Cập nhật policy **Start 🡪 Run 🡪GPUPDATE /FORCE**

Phân quyền cho các group như sau:

* Trên thư mục **DATA**:
  + Group **Ketoan** và **Nhansu** có qyuền **Read**
* Trên thư mục **Public**
  + Group **Ketoan** và **Nhansu** có qyuền **Full Control**
* Trên thư mục **Ketoan**
  + Group **Ketoan** có quyền **Full Control**
  + Group **Nhansu** không có quyền
* Trên thư mục **Nhansu**
  + Group **Nhansu** có quyền **Full Control**
  + Group **Ketoan** không có quyền

Hướng dẫn cấu hình:

* **Standard permission**

1. **Phân quyền trên thư mục DATA**

|  |  |
| --- | --- |
| B1: Logon **Administrator** 🡪 vào **C:\** Click chuột phải trên thư mục **DATA** 🡪 **Properties** 🡪 vào **tab Security** 🡪 chọn **Advanced** | 🡪Bỏ dấu chọn tại mục **Allow Inheritable permission…** (như trong hình) |
|  |  |

|  |  |
| --- | --- |
| Trong hộp thoại **Security** chọn **Copy 🡪 Apply 🡪 OK** | B2: trong hộp thoại **DATA properties** chọn **Users** 🡪 chọn **Remove** 🡪 **Advanced** |
|  |  |
| Trong hộp thoại **Advanced Security Settings for DATA** 🡪 đánh dấu chọn tại ô **Replace Permission …** (như trong hình) 🡪 **OK** 🡪 trong hộp thoại **Security** chọn **Yes** | B3: Trong tab **Security** chọn **Add** 🡪 tìm và thêm 2 group **Ketoan** và **Nhansu** |
|  |  |
| Trong hộp thoại **DATA Properties** 🡪 kiểm tra **Ketoan** và **Nhansu** đang có quyền **Read** 🡪 **Apply** 🡪 **OK** |  |

1. **Phân quyền trên thư mục Public**

|  |  |
| --- | --- |
| **B1:** Vào **C:\DATA** 🡪 Click chuột phải lên thư mục **Public** 🡪 **Properties** 🡪 vào tab **Security** 🡪 Click chọn group **Ketoan** 🡪 đánh dấu chọn vào ô **Full Control** trong cột **Allow** (như trong hình) 🡪 **Apply** | **B2:** Trong hộp thoại **Public Properties** 🡪 Click chọn group **Nhansu** 🡪 đánh dấu chọn ô **Full Controll** trong cột **Allow** (như trong hình) 🡪 **Apply** 🡪 **OK** |
|  |  |

1. **Phân quyền trên thư mục Ketoan**

|  |  |
| --- | --- |
| **B1:** Vào **C:\DATA** 🡪 Click chuột phải lên thư mục **Ketoan** 🡪 **Properties** 🡪 vào tab **Security** 🡪 **Advanced** | **Trong** tab **Permission** 🡪 bỏ dấu check **Allow inheritable permission…** (như trong hình) |
|  |  |
| 🡪Trong hộp thoại **Security** chọn **Copy** 🡪 **Apply** 🡪 **OK** | Trongtab **Security** chọn group **Nhansu** 🡪 chọn **Remove** |
|  |  |
| Click vào group **Ketoan** 🡪 đánh dấu chọn vào ô **Full Controll** của cột **Allow** (như trong hình) 🡪 **Apply** 🡪 **OK** |  |

1. **Phân quyền cho thư mục nhân sự**

|  |  |
| --- | --- |
| **B1:** Vào **C:\DATA** 🡪 Click chuột phải lên thư mục **Nhansu** 🡪 **Properties** 🡪 vào tab **Security** 🡪 **Advanced** | Trongtab **Permission** 🡪 bỏ dấu check **Allow inheritable permission…** (như trong hình) |
|  |  |
| 🡪Trong hộp thoại **Security** chọn **Copy** 🡪 **Apply** 🡪 **OK** | Trongtab **Security** chọn group **Ketoan** 🡪 chọn **Remove** |
|  |  |
| Click vào group **Nhansu** 🡪 đánh dấu chọn vào ô **Full Controll** của cột **Allow** (như trong hình) 🡪 **Apply** 🡪 **OK** |  |

1. **Kết hợp Share permission và NTFS permission**

B1: trên máy Domain Controller share thư mục **C:\DATA** 🡪 cho **Everyone** quyền **Full Controll**

|  |  |
| --- | --- |
|  |  |

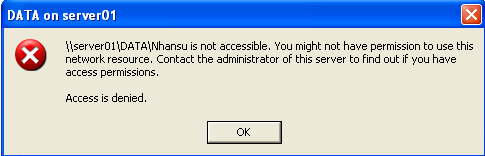
B2: Máy **Windows XP** join vào Domain

B3: Máy **Windows XP** logon với user **KT1**

B4: Trên máy **Windows XP** vào **Start** 🡪 **Run** 🡪 **\\tên máy domain (hoặc IP của máy Domain Controller)** 🡪 **OK**

|  |  |
| --- | --- |
|  |  |

* Vào thư mục **\\Server01\DATA\Public** tạo tập tin **DataKT1.txt**
* Vào thư mục **\\Server01\DATA\Ketoan** tạo tập tin **DataKT1.txt**
* Vào thư mục **\\Server01\DATA\Nhansu** tạo tập tin **DataKT1.txt** 🡪 hệ thống sẽ thong báo lỗi (như hình sau) 🡪 **OK**



B5. **KT2** và **KT3** làm tương tự như **B3** và **B4**

B6: Logon với **NS1** (trên máy XP)

* Vào thư mục **\\Server01\DATA\Public** tạo tập tin **DataNS1.txt**
* Vào thư mục **\\Server01\DATA\Nhansu** tạo tập tin **DataNS1.txt**
* Vào thư mục **\\Server01\DATA\Ketoan** tạo tập tin **DataNS1.txt** 🡪 hệ thống sẽ thông báo lỗi (như hình sau) 🡪 OK



1. **Special permission**

|  |  |
| --- | --- |
| **B1**: Máy **DC** logon với **Administrator** 🡪 vào **C:\DATA** 🡪 Click chuột phải trên thư mục **Ketoan** chọn **Properties** 🡪 Tab **Security** 🡪 **Advanced** 🡪 Click chọn group **Ketoan** 🡪 chọn **Edit** | 🡪 trong hộp thoại **Permission Entry for Ketoan** 🡪 bỏ dấu chọ tại ô **Delete Subfolders and Files** và ô **Delete** 🡪 đánh dấu chọn vào ô **Apply these permissions…** (như trong hình) 🡪 **OK** 🡪 **OK** |
|  |  |
| Trong hộp thoại **Ketoan Properties** 🡪 Click chọn group **Ketoan** 🡪 ngoài những quyền thông thường **“Ketoan”** còn có 1 quyền là **Special Permission** 🡪 **OK** |  |
| B2: Logoff **Administrato**r 🡪 Logon **KT1** 🡪 vào **C:\DATA** 🡪 vào thư mục **Ketoan** 🡪 tạo 1 tập tin tên **“DulieucuaKT1.txt”** 🡪 gõ nội dung và lưu lại. | B3: Logoff **KT1** 🡪 Logon **KT2** 🡪 vào **C:\DATA** 🡪 vào thư mục **Ketoan** 🡪 Click chuột phải trên **“DulieucuaKT1.txt”** chọn **Delete** 🡪 hệ thống sẽ báo lỗi **“Access is Denied”** |
|  |  |
| B4: Trong thư mục C:\DATA 🡪 vào thư mục **Ketoan 🡪** click chuột phải tạo 1 file tên “DulieucuaKT2.txt” 🡪 gõ nội dung và lưu lại. | B3: Logoff **KT2** 🡪 Logon **KT1** 🡪 vào **C:\DATA** 🡪 vào thư mục **Ketoan** 🡪 Click chuột phải trên **“DulieucuaKT1.txt”** chọn **Delete** 🡪 thấy **“DulieucuaKT1.txt”** bị xóa 🡪 Click chuột phải trên **“DulieucuaKT2**.txt” chọn Delete hệ thống sẽ báo lỗi **“Access is Denied”** |
|  |  |

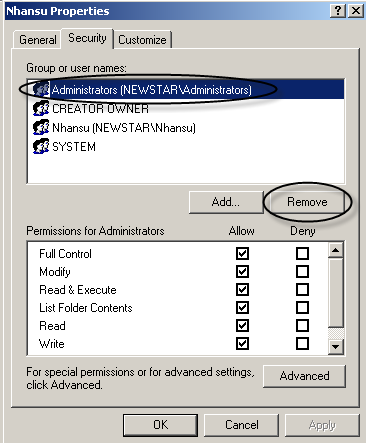
1. **Take OwnerShip**

**B1**: máy **Domain Controller** logon **Administrator**

|  |  |
| --- | --- |
| **B2**: click chuột phải trên **C:\DATA** 🡪 click chuột phải trên **Nhansu** 🡪 **Properties** 🡪 chọn tab **Security** 🡪 **Advanced** 🡪 click chọn group **Administrators** 🡪 **Edit** | B3: Kiểm tra thấy **Administrators** có quyền **Take OwnerShip** 🡪 **OK** 🡪 **OK** 🡪**OK** |
|  |  |

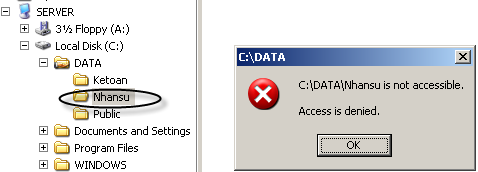
**B4**: Logoff **Administrator** 🡪 Logon **NS1**

**B5**: Vào **D:\DATA** 🡪 click chuột phải trên thư mục **Nhansu** 🡪 **Properties** 🡪 tab **Security** 🡪 Click chọn **Administrators** 🡪 Chọn **Remove** 🡪 **Apply** 🡪 **OK**

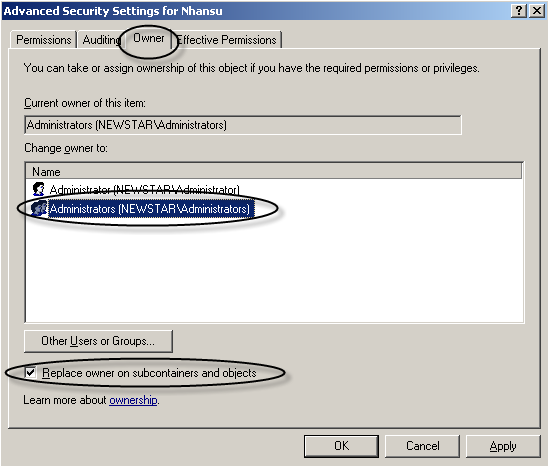


**B6**: Logoff **NS1** 🡪 Logon **Administrator**

**B7:** Vào thư mục **C:\DATA** 🡪 click vào thư mục **Nhansu** 🡪 hệ thống sẽ báo lỗi **Access is Denied**



**B8**: Click chuột phải trên thư mục **Nhansu** 🡪 **Properties** 🡪 chọn tab **Security** 🡪 chọn **Advanced** 🡪 chọn tab **Owne**r 🡪 tìm và Add group **Administrators** 🡪 **OK** 🡪 đánh dấu vào ô **Replace owner on sub container and objects 🡪 OK** 🡪 chọn **YES** ở hộp thoại hiển thị 🡪 **OK**



**B9**: Click chuột phải trên thư mục **Nhansu** 🡪 **Properties** 🡪 chọn tab **Security** 🡪 thấy group **Administrators** có quyền **Full Controll.**

