Triển khai và cài đặt cấu hình AD RMS trên windows server

Active Directory Right Management Service có vai trò bảo vệ các tài liệu nhạy cảm không bị public ra ngoài (cho phép người dùng tuỳ ý phân quyền trên tài liệu của mình)

Các tài liệu có thể là word, mail hoặc excel,...

1. Chuẩn bị

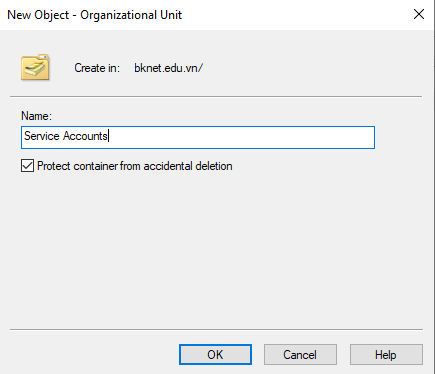
* 1 máy chủ DC
* 1 máy client có cài đặt office

1. Triển khai môi trường cho các user

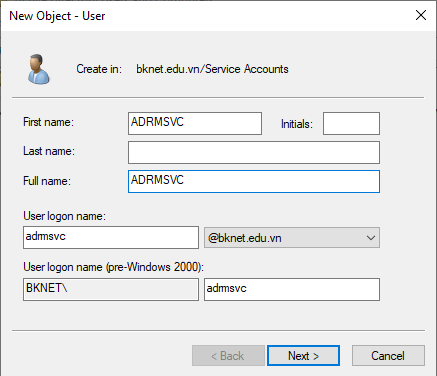
* Tiến hành tạo User trên máy DC

Tools => Active Directory User and Computer

* Tạo OU chứa các Service

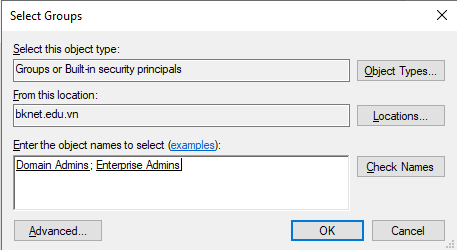


* Tạo User trong OU vừa tạo

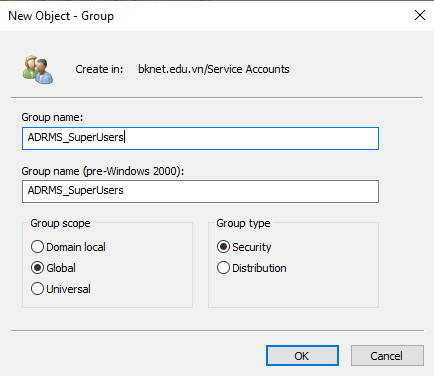


* Gán User vừa tạo vào nhóm Domain Admin hoặc Enterprise Admin

Chuột phải User => properties => member Of => Add

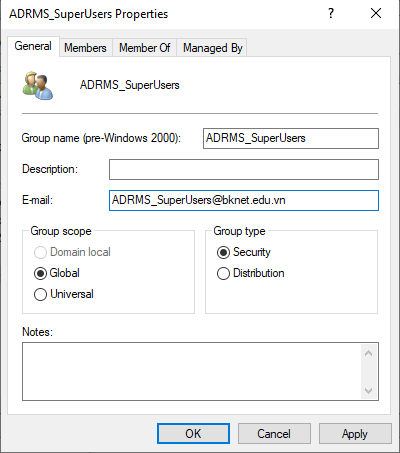


* Tạo 1 Group trong OU Service Accounts

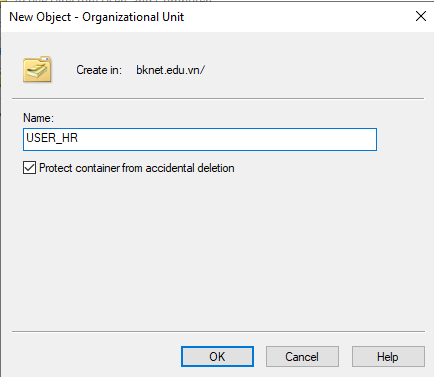


* Thêm email cho Group vừa tạo

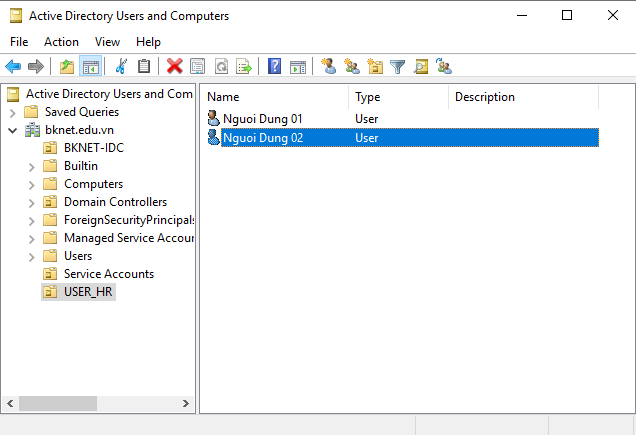
Chuột phải Group => Properties



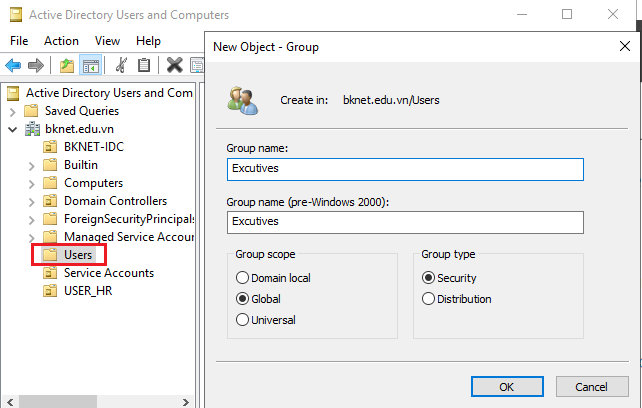
* Tạo thêm 1 OU để chứa các User



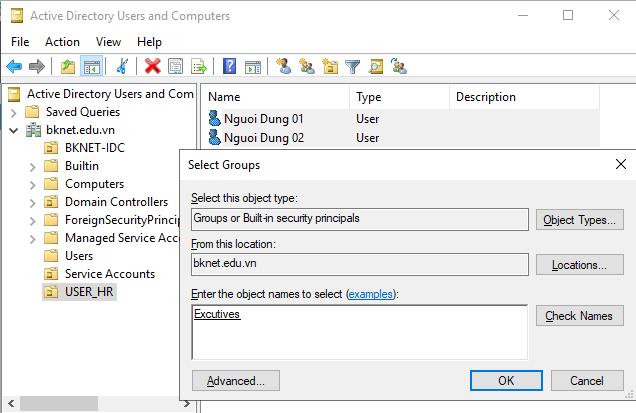
* Tạo các User trong OU đó



* Tiến hành tạo 1 group trong OU User của miền

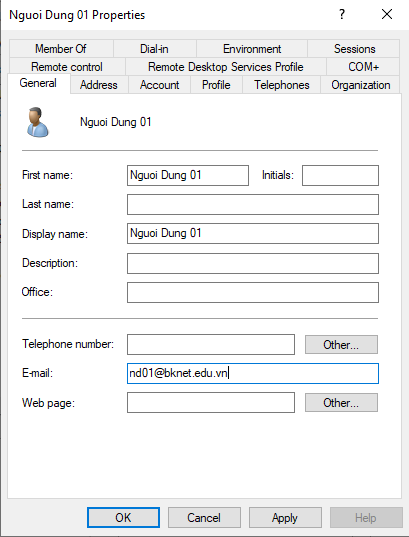


* Sau đó Add các User trong OU USER\_HR vào group vừa tạo



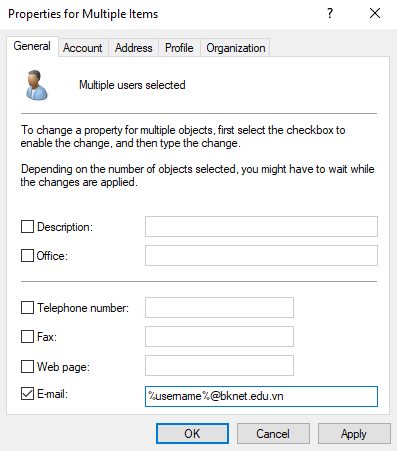
* Thêm email cho tất cả các User

Chuột phải user => properties



Trường hợp có rất nhiều user thì áp dụng cách:

Ctrl + A để lấy tất cả các user => Chuột phải => properties

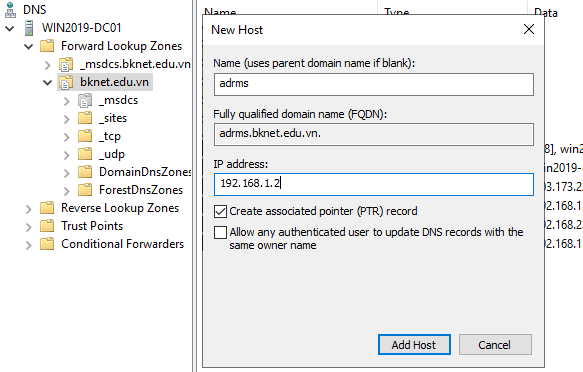


1. Cài đặt và cấu hình dịch vụ AD RMS

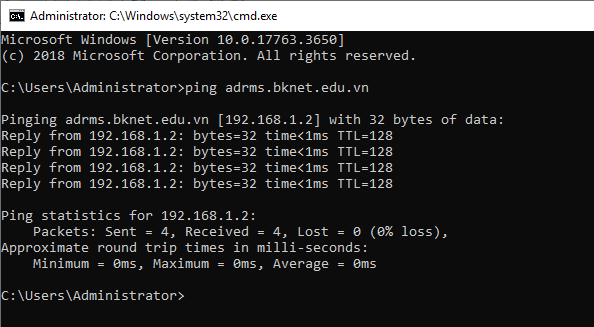
Add Roles and Features => Server Roles => Active Directory Right Management Service => Install

* Tạo 1 số bản ghi cho AD RMS

Tools => DNS => chuột phải tên miền => New Host

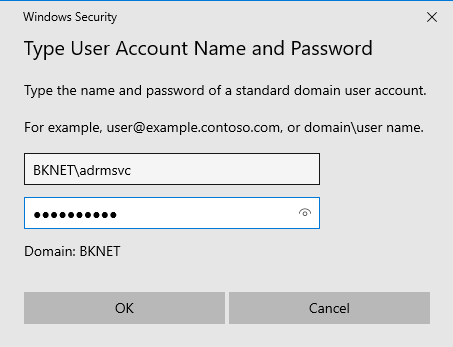


Kiểm tra phân giải tên miền

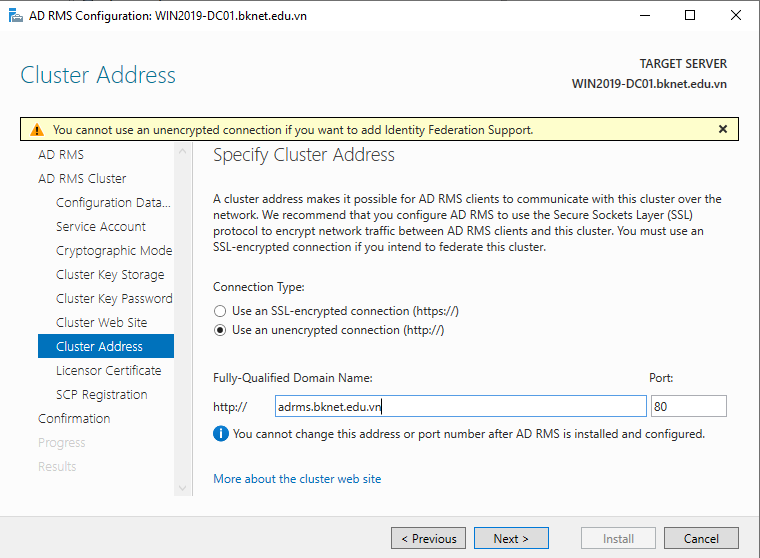


* Cài đặt phần cấu hình

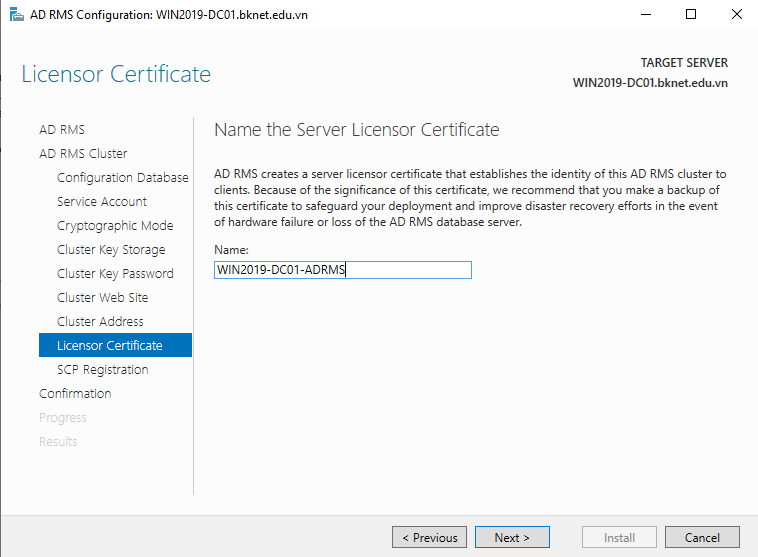
Click vào perform additional configuration => Create a new AD RMS… => used windows internal database on this server => Specify => nhập tài khoản ADRMS (ở đây là user của OU Service Accounts)



Sau đó chọn Cryptographic Mode 2… => Use AD RMS centrally… => tạo mật khẩu => Default Web Site =>



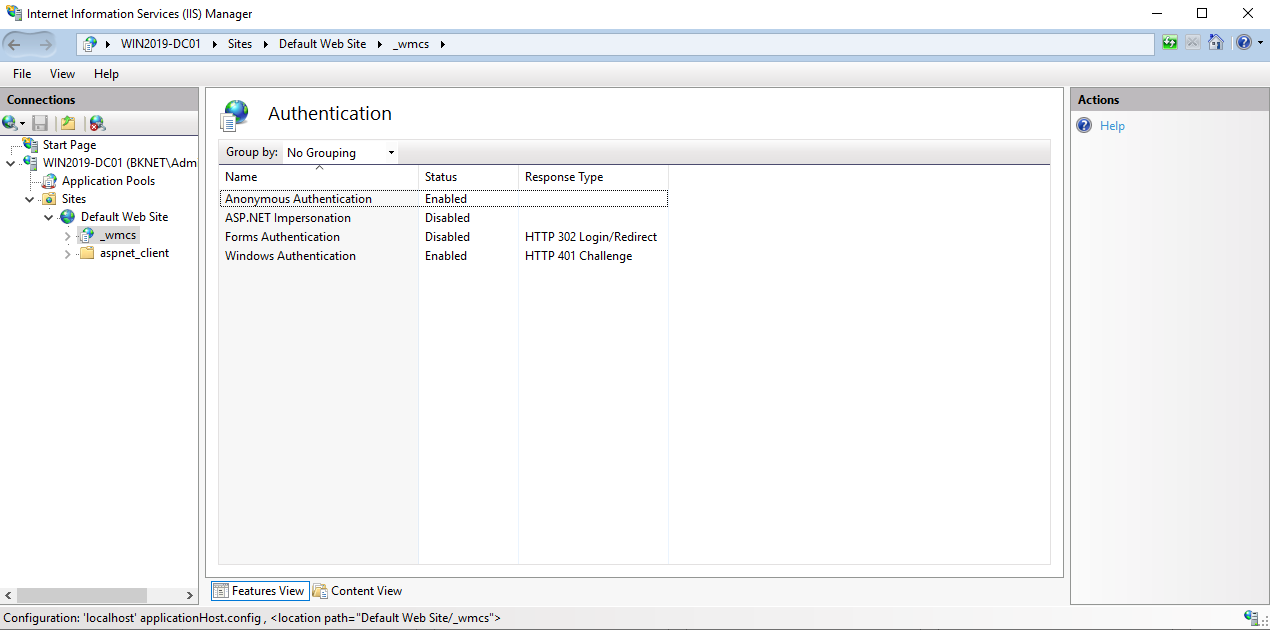
Đặt tên cho server



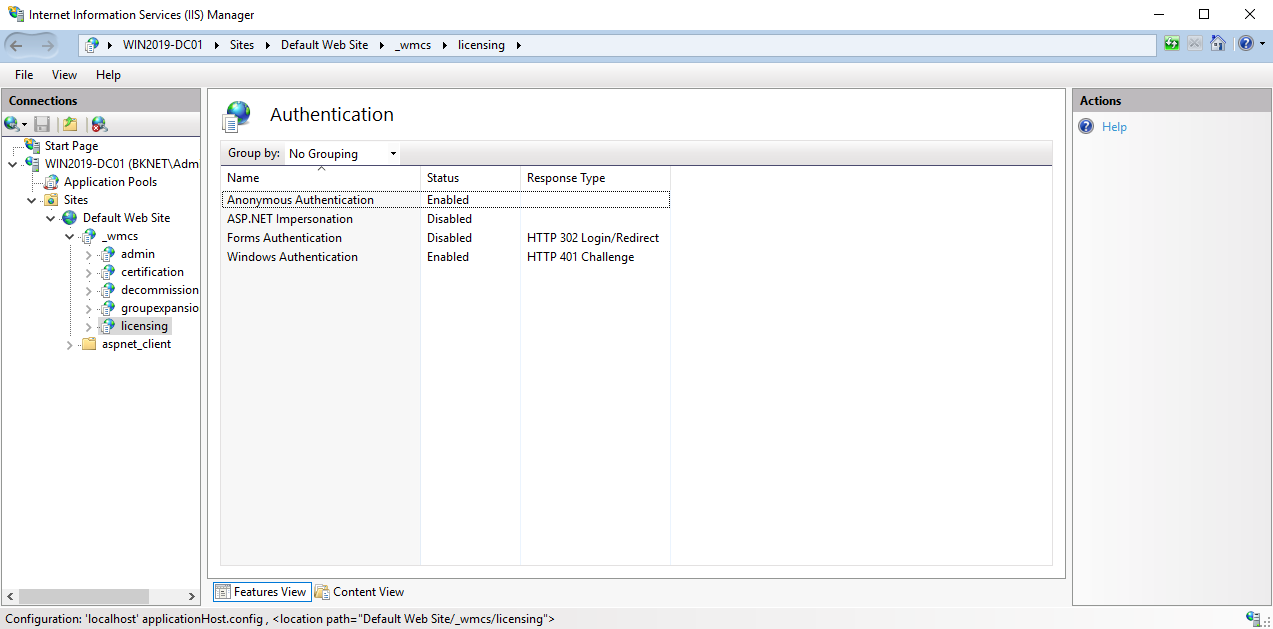
Sau đó chọn Register the SCP now => Install

* Cấu hình

Tools => IIS Manager => Máy chủ => Site => \_wmcs => nháy dub vào Authentication => Enable Anonymous Authentication

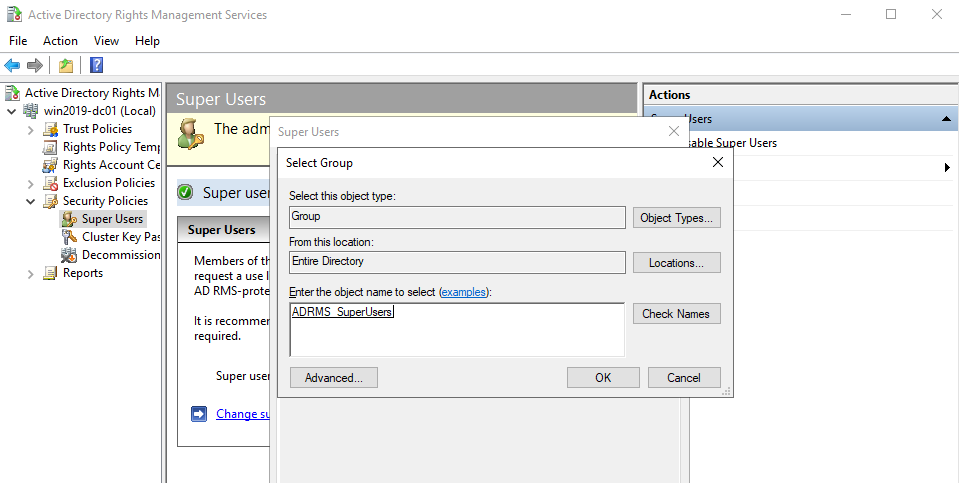


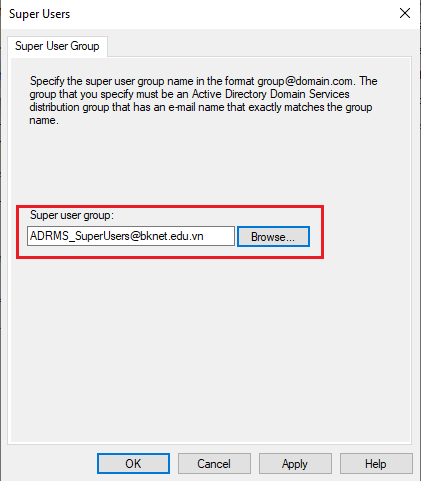
Từ \_wmcs => licensing => Authentication => Enable Anonymous Authentication



Sau đó Restart lại máy chủ

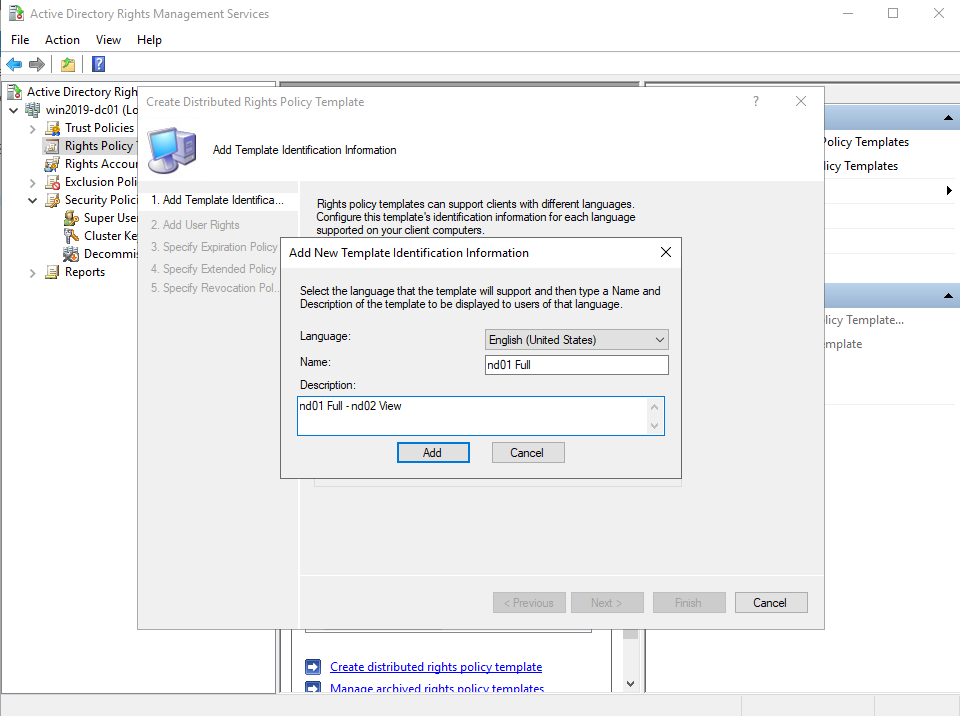
Sau khi Restart xong => Tools => AD RMS => máy chủ => Security Policies => Super Users => Click Enable Super User => Change super user group => Advanced => Tìm đến group ADRMS\_SuperUsers đã tạo trước đó



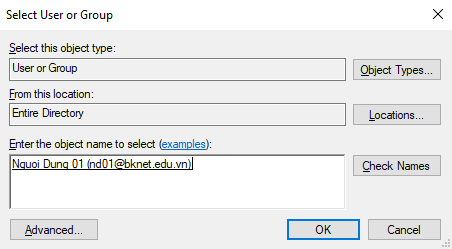


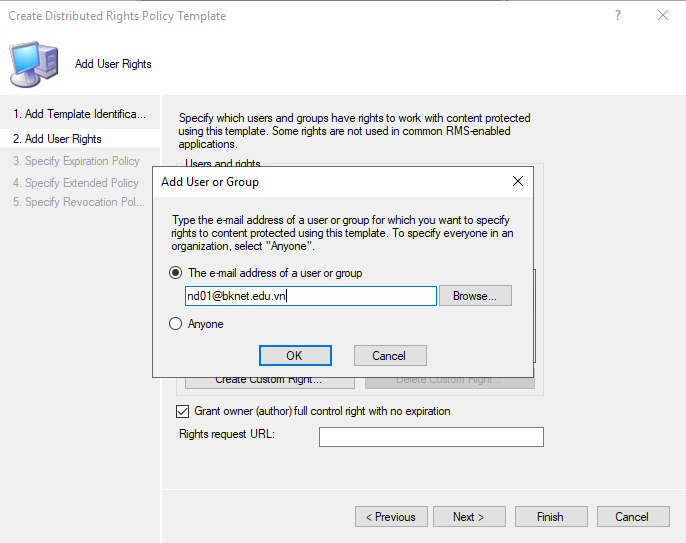
Tạo template cho các nhóm người dùng, user (VD ở đây user nd01 có quyền full, nd02 có quyền view)

Right Policy Template => Create Distributed Right Policy Templates => Add => đặt tên và mô tả

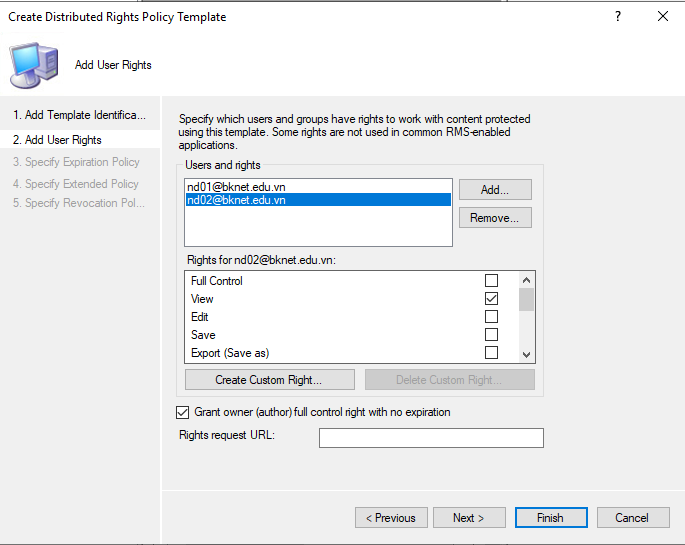


Next => Add User Rights => Add (user hoặc nhóm tuỳ vào ta lựa chọn ban đầu) =>



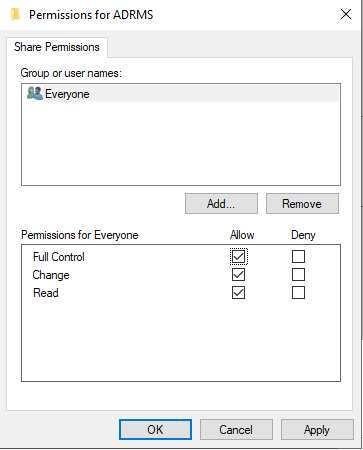


Sau đó phân quyền cho user vừa chọn (nd01 nhận full control). Tiếp tục làm tương tự với các user còn lại => Finish

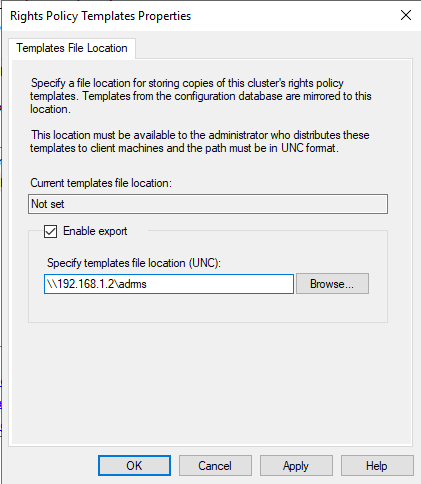


* Lưu Template vừa tạo

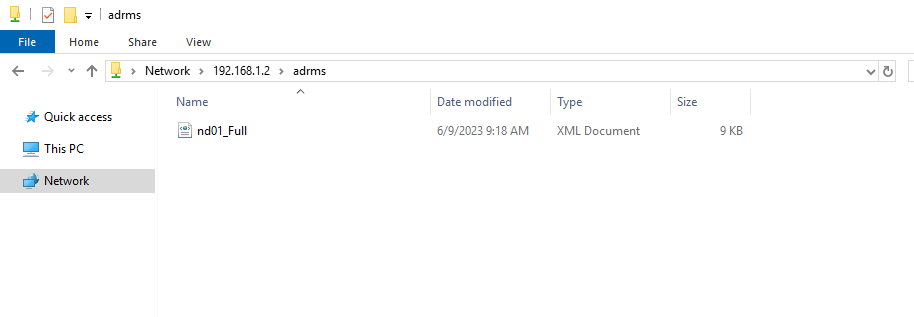
Tạo 1 folder trong ổ C => phân quyền cho folder đó



Copy đường dẫn đến folder đã tạo => chuột phải vào Right Policy Template => properties =>



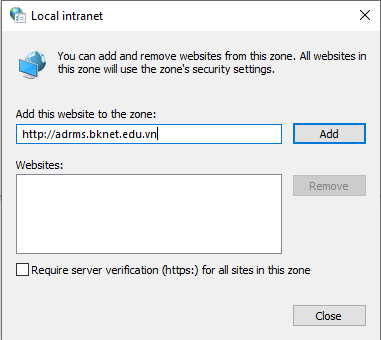
Lúc này template sẽ được lưu vào thư mục ADRMS vừa tạo



* Cấu hình trên máy Client

Tiến hành đăng nhập vào user (ở đây là nd01)

Vào control panel => Internet Options => Security => Local intranet => Site => Advance



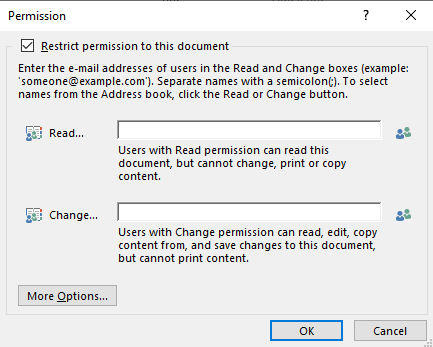
Add => OK

Tiến hành tạo 1 tài liệu bằng word

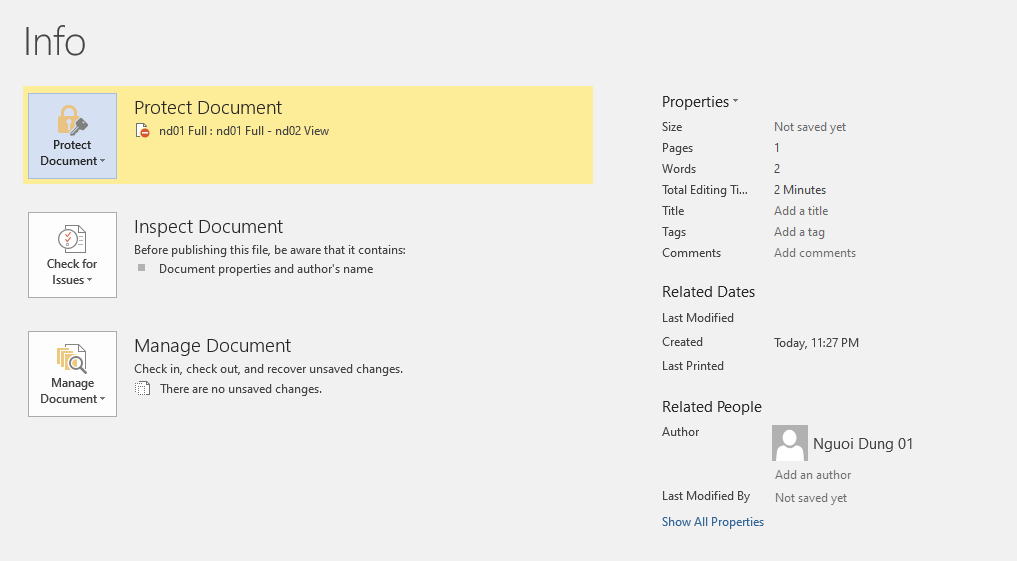
Sau khi tạo tài liệu xong => File => Protect Document => Restrict Access => Connect to AD RMS (cái này là để giới hạn quyền truy cập)

Bây giờ ta cũng có thể tự tạo 1 template mới khi chọn vào phần

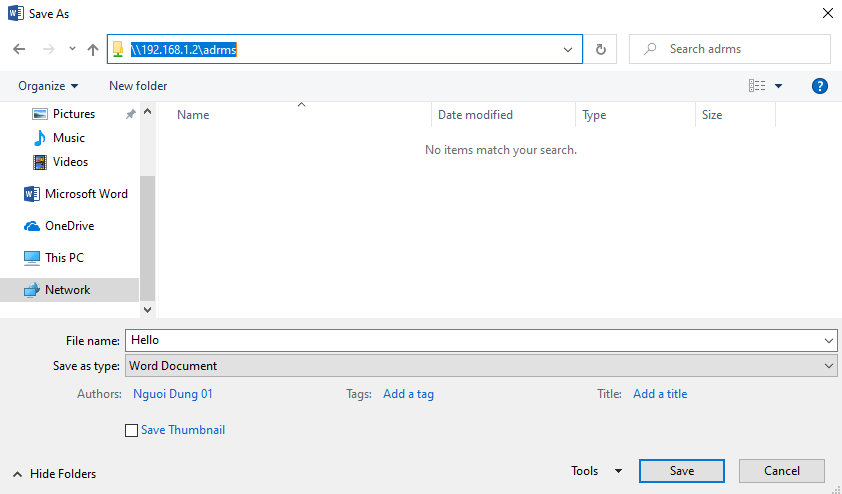
File => Protect Document => Restrict Access =>Restricted Access



Ở đây ta dùng template nd01 Full đã tạo sẵn trước đó



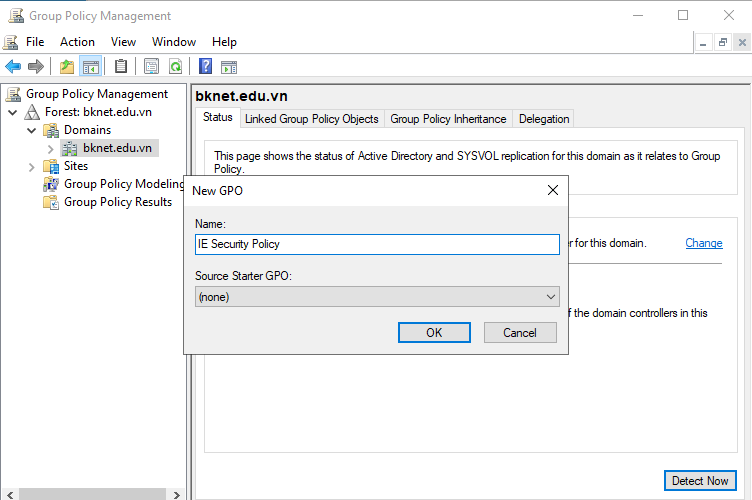
Sau đó save tài liệu đã tạo lại vào Folder ADRMS đã tạo trên máy chủ



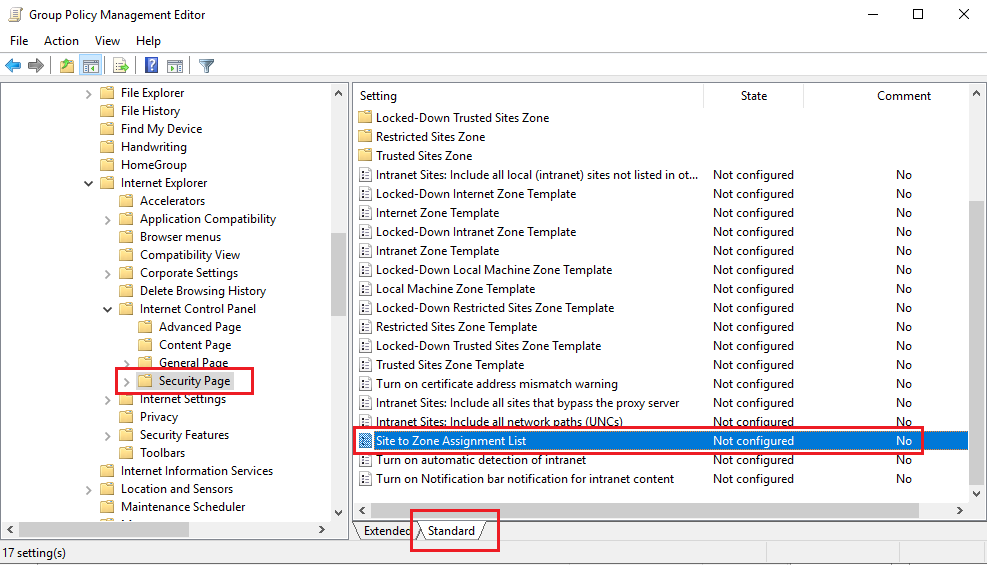
Đối với user thứ 2 ta cũng làm tương tự

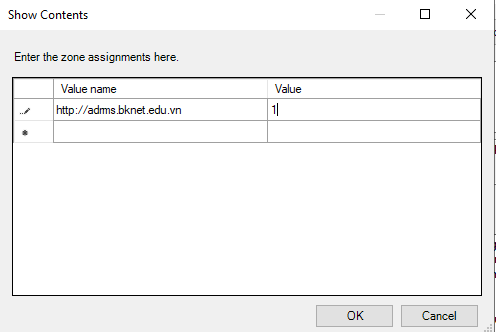
* Triển khai Group Policy cho toàn bộ các user trong hệ thống

Trên máy chủ => Tools => Group Policy Management => chuột phải vào miền => Tạo GPO mới



Chuột phải GPO vừa tạo => Edit => Computer Configuration => Policies => Administrative Template… => Windows Components => Internet Explorer => Internet Control Panel => Security Page => Enable file Site to Zone Assignment List và điền tên miền adrms vào mục Show





Sau đó chạy lệnh gpupdate /force trên cmd để update quá trình