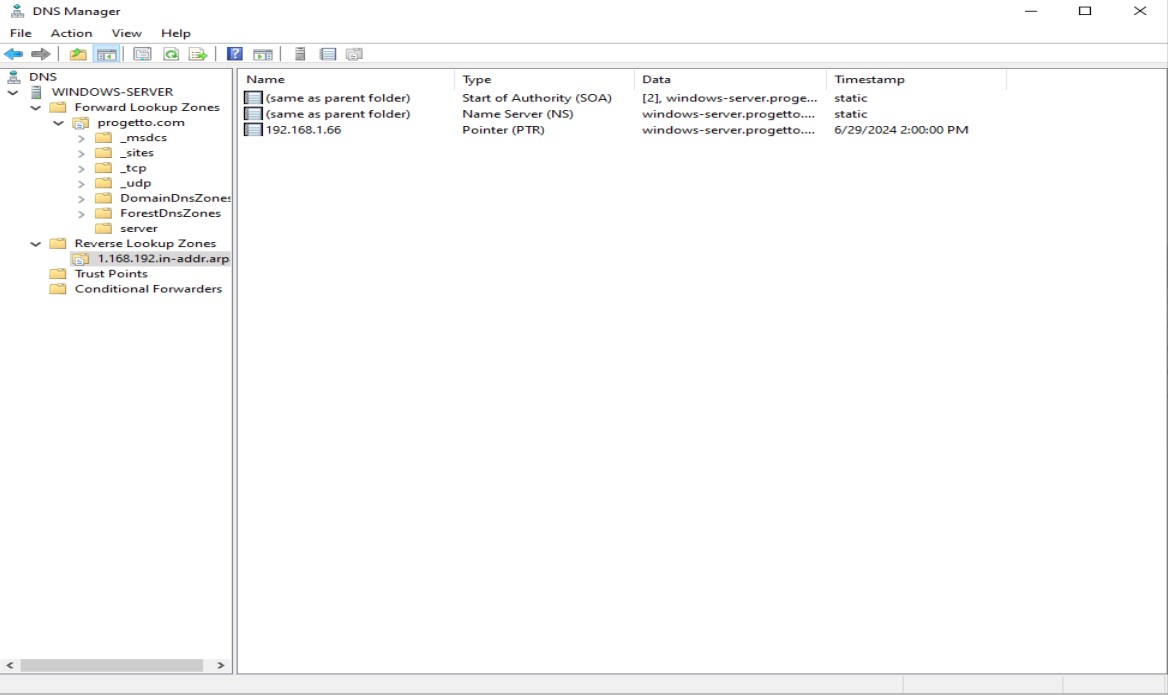
**Progetto Laboratorio di Sicurezza dei Sistemi e Privacy**

**Sviluppo di Ambiente Active Directory**

1. **Introduzione**

L'obiettivo principale di questo progetto è la creazione di un ambiente Active Directory (AD) composto, in questa istanza, da un server e un client, al fine di approfondire le tematiche di sicurezza dei sistemi informatici e la gestione della privacy dei dati all'interno di una rete aziendale simulata.  
Active Directory è un servizio directory di Microsoft che permette la gestione centralizzata di utenti, computer e risorse di rete, migliorando così la sicurezza e l'efficienza operativa.  
Attraverso l'implementazione di un dominio Active Directory, il progetto intende dimostrare come configurare e gestire le politiche di sicurezza, autenticazione e autorizzazione degli utenti, nonché la protezione delle informazioni sensibili. Verranno esplorati diversi aspetti della sicurezza, fra i quali: l'applicazione di politiche di password, la gestione dei permessi di accesso, il controllo degli accessi basato su ruoli (RBAC), la configurazione di criteri di gruppo (GPO), l’implementazione di regole Firewall e Access List ad hoc e l’instaurazione di un Server RADIUS per la gestione degli accessi remoti alla rete.

Inoltre, il progetto fornisce un'opportunità pratica per comprendere come Active Directory può contribuire a rispettare le normative sulla privacy e la protezione dei dati, garantendo che solo gli utenti autorizzati possano accedere alle informazioni sensibili e che le attività all'interno del dominio siano tracciabili e controllabili.  
Tutte le operazioni descritte di seguito sono state, in primis, svolte alternando soluzioni di “automazione” con PowerShell (cmdlets di AD) a soluzione di creazione tramite tool GUI (ADUC, GPM,...) ed in secundis definite seguendo il materiale di studio fornito, gli esempi svolti a lezione e la [Guida di Microsoft](https://learn.microsoft.com/en-us/windows-server/identity/identity-and-access) per Active Directory.

1. **Configurazione dell'Ambiente Active Directory**
   1. Creazione AD Server e Dominio:
      1. Definire, tramite l’hypervisor Virtual Box, una macchina virtuale che ricoprirà le funzioni di server. Partendo dalla immagine disco iso Windows Server 2022 Desktop Experience, assegnare le risorse di memoria e computazionali sufficienti per la gestione dei processi di AD, DNS, NPS e RADIUS e impostare la modalità bridge per la scheda di rete.
      2. Installare DNS Role:
         * Assegnare un indirizzo Ipv4 static, che diventerà l’indirizzo di riferimento per il DNS del dominio, ed impostare quest’ultimo come indirizzo DNS di riferimento per il server stesso.
         * Tramite il tool preimpostato “Server Manager”, aggiungere il ruolo DNS con annesse funzionalità.
         * Una volta installato tale ruolo, accedere alla console di gestione DNS Manager e creare una nuova zona.
         * Selezionare zona primaria, nominare il progetto, e creare nuovo file. Lasciare momentaneamente “Aggiornamento Dinamico” in “Do not Allow Dynamic Updates".
      3. Installare Active Directory Domain Service tramite PowerShell:
         * Eseguire il seguente comando in PS per installare il ruolo di Active Directory Domain Service con inclusi i tool di servizio grafici (ADUC, GPM, dxdiag,...):

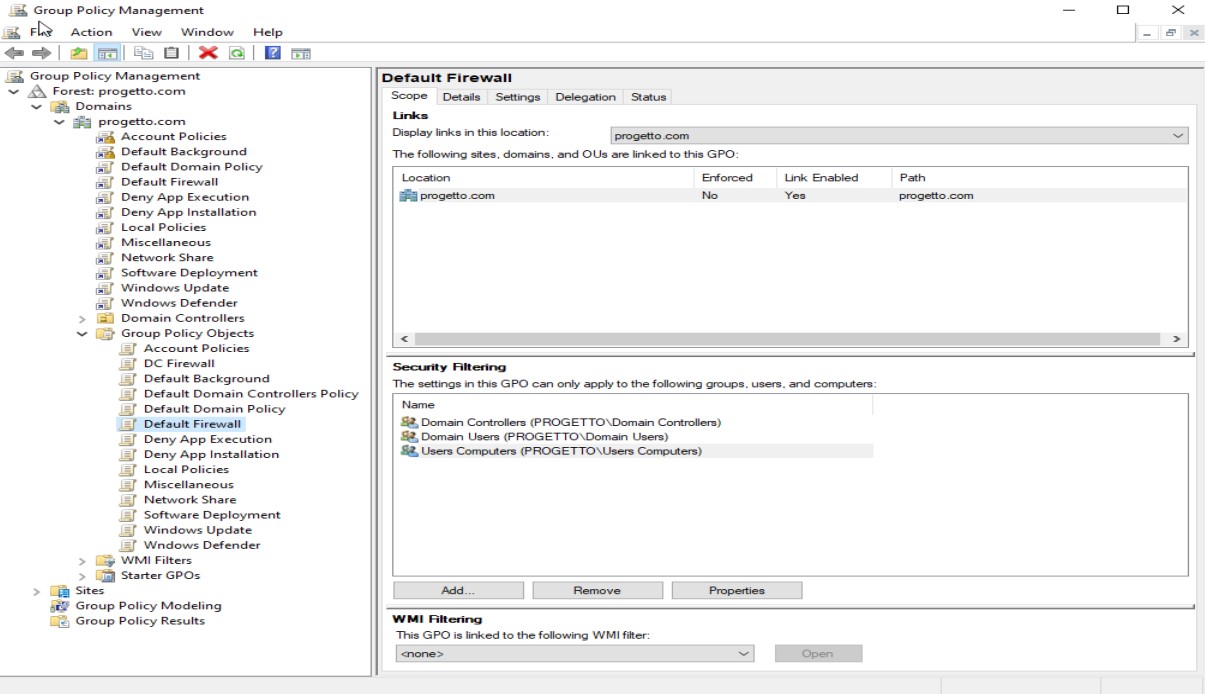
Install-WindowsFeature -name AD-Domain-Services -IncludeManagementTools

* + 1. Creare il nuovo dominio:
       - Per instaurare il nuovo dominio dobbiamo prima creare la foresta in cui i verranno localizzate le risorse tramite i seguenti comandi:
       - Tramite il seguente comando:

Install-ADDSForest -DomainName progetto.com -CreateDNSDelegation -DomainMode 6 -ForestMode 6 -DatabasePath "d:\NTDS" -SYSVOLPath "d:\SYSVOL" -LogPath "e:\Logs

Viene istanziata una nuova foresta chiamata “progetto.com”, creata una delegazione DNS nel dominio, impostati i livelli funzionali del dominio e della foresta entrambi a 6 (Windows Server 2016) e definiti percorsi per database, volume di sistema e log di sistema.  
Una volta eseguito, definire una password DSRM, a cui seguirà il riavvio del server.

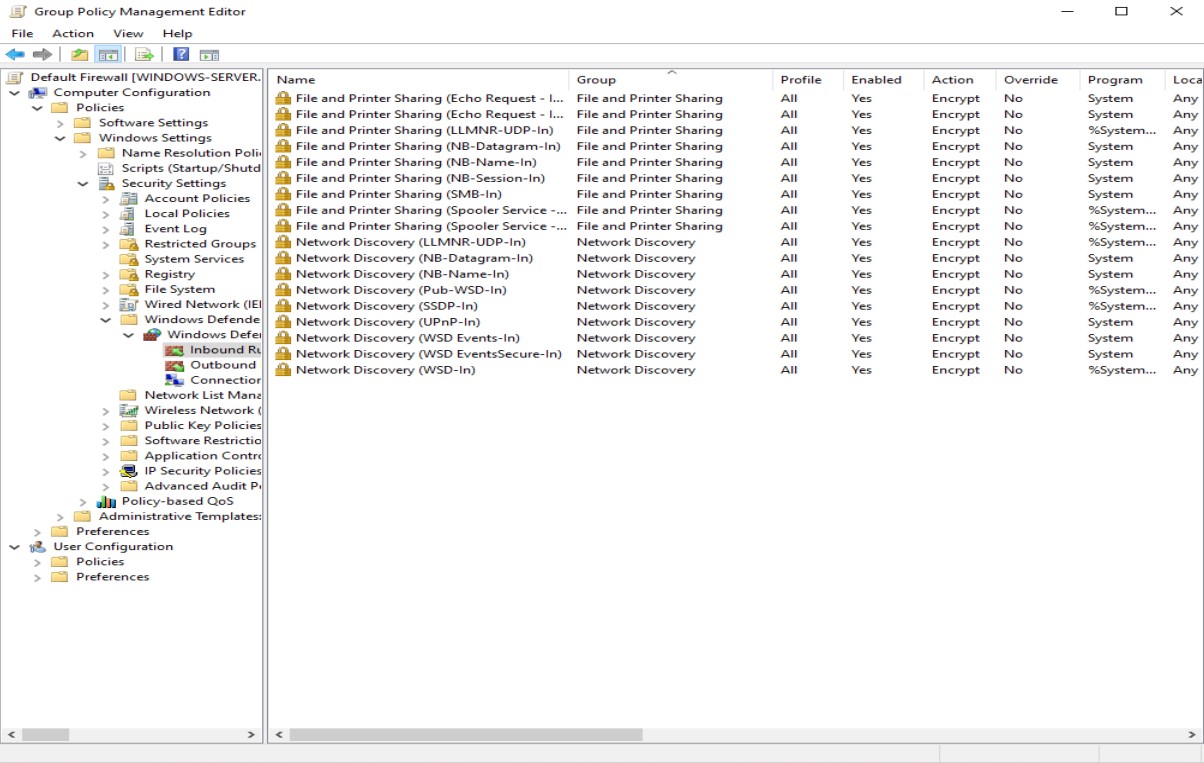
* + 1. Impostare l’aggiornamento dinamico DNS:
       - Nel tool di gestione del DNS espandere Forward Lookup Zones.
       - Accedere alle proprietà del dominio.
         1. Selezionare “Store the zone in Active Directory”
         2. Abilitare solo aggiornamenti dinamici sicuri.
  1. Creazione AD Client ed aggiunta a dominio:
     1. Definire, tramite l’hypervisor Virtual Box, una macchina virtuale che ricoprirà le funzioni di client. Partendo dalla immagine disco iso Windows 10 Pro o Enterprise, assegnare le risorse di memoria e computazionali necessarie ed impostare la modalità bridge per la scheda di rete.
     2. Impostare il server DNS di riferimento del client all’indirizzo della macchina server.
     3. Aggiungere client a dominio:
        + Accede alle impostazioni di sicurezza del sistema e selezionare “Rinomina PC (avanzate)”:
          1. Cambiare il nome del dominio a cui è legato il client.
          2. Nominare il client e confermare tramite le credenziali di admin di dominio.

1. **Sicurezza Ambiente:**
   1. Regole Firewall:   
      La scelta organizzativa per le Policy di gestione dei firewall opta per lo sfruttamento la “gerarchia” delle risorse di rete. Viene inizialmente definita ed applicata una GPO per le impostazioni Firewall di Default, chiamata “Default Firewall”, applicata a tutte le macchine ed i profili del dominio. In seguito, viene delineata una policy più specifica, esclusivamente per i Domain Controller, che non andrà a sovrascrivere bensì solo ad integrare ulteriori regole alla prima, sfruttando le proprietà di precedenza ed eredità delle Group Policy.

Le impostazioni scelte per il Default Firewall sono le seguenti:

* + 1. Startup Automatico del Firewall all’avvio: per garantire che il firewall, con le relative eventuali impostazioni di sicurezza, sia attivato di default all’avvio della macchina.
    2. Protezione di tutte le connessioni: per garantire che tutte le connessioni a livello di rete locale e non siano sottoposte alle regole di traffico specificate.
    3. Abilitati i profili di rete Domain, Private e Public: per configurare e di conseguenza garantire diverse impostazioni di sicurezza dipendentemente dal profilo di rete attivo, questo può risultare particolarmente utile qualora una macchina si connetta a reti esterne insicure o non riconosciute.
    4. A screenshot of a computer

       Description automatically generatedConfigurato blocco di default di tutte le connessioni in ingresso ed in uscita al netto di regole che esplicitamente ne consentano il traffico: misura di sicurezza di default del firewall per negar tutto il traffico non apertamente ammesso. Permette di limitare le comunicazioni e lo scambio di pacchetti solo ai canali da noi selezionati.
    5. Abilitata l’unione delle nuove impostazioni firewall con quelle esistenti: per mantenere alcune Core Networking Rules fondamentali per il normale traffico e contestualmente di specificarne di nuove per integrare a quelle di default (in caso di conflitto fra due regole, quella di default viene sovrascritta).
    6. Abilitato il logging per il traffico, con un aumento della dimensione dei file di logging fino a 32Mb: per raccogliere informazioni sulle attività di connessione, utile in particolare per troubleshooting di connessioni non valide.
    7. Attivate le notifiche per le connessioni bloccate.
    8. Definite le impostazioni di encryption e authentication per IPsec.
    9. Partendo da regole predefinite del firewall, vengono ridefinite alcune impostazioni per Network Discovery, e File/Printer Sharing: per garantire la comunicazione con DC e l’accesso alle share di rete configurate di seguito. Viene sfruttato un “preset” di queste regole a cui vengono aggiunte alcune misure di sicurezza, in particolare vengono limitate a solo specifici gruppi di utenti e vengono impostati requisiti di connessione in accordo con le precedenti impostazioni IPsec.

La Policy specifica per Domain Controller aggiunge le seguenti configurazioni:

* + 1. Regole, sia TCP che UDP, per consentire il traffico in ingresso sulla porta 53 (DNS) esclusivamente dai client: per assicurare un traffico ristretto ai gruppi utenti specifici.
    2. Aggiunta di regole che gestiscano l’accesso in Remote Desktop, in ingresso sulla porta 3389 (RDP), esclusivamente agli utenti Admin.
    3. Per permettere la connessione RDP di cui sopra sono state impostate anche le seguenti condizioni attraverso le Computer Configuration:
       - Abilitare RDP sui Domain Controller: impostare su abilitata la policy di permesso per connessione remota da parte di utenti.
       - Abilitare le connessioni da Computer con qualsiasi versione di RD.
       - Restrizione dell’accesso solo a specifici gruppi utenti (admin) o gruppi di computer (admin pc).
       - Esclusione dall’accesso a tutti gli altri utenti o computer non autorizzati.
  1. Creazione Gruppi:

Per facilitare il deployment dell’ambiente di test di Active Directory, è stato creato uno script per PS con cmdlets AD DS che, iterativamente, crea i gruppi richiesti per simulare l’ambiente aziendale, fra questi: IT, Sales, Marketing, Finance, HR e Non-Admin. Particolarmente degni di nota sono il gruppo IT, che conterrà i profili di tutti i dipendenti facenti parte del reparto IT e che ricopriranno anche il ruolo di amministratori di dominio, ed il gruppo Non-Admins, necessario come riferimento a tutti coloro i quali non godano dei permessi di ulteriori a quelli del normale utente, verrà usato soprattutto nel filtraggio delle GPO.

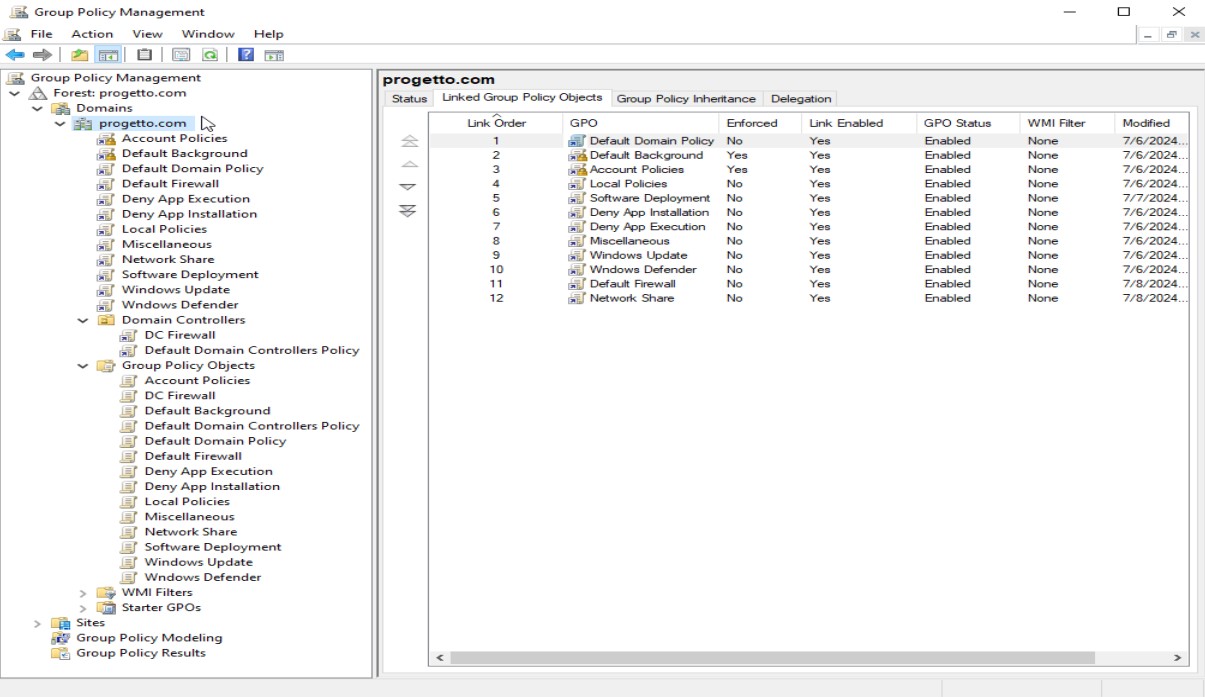
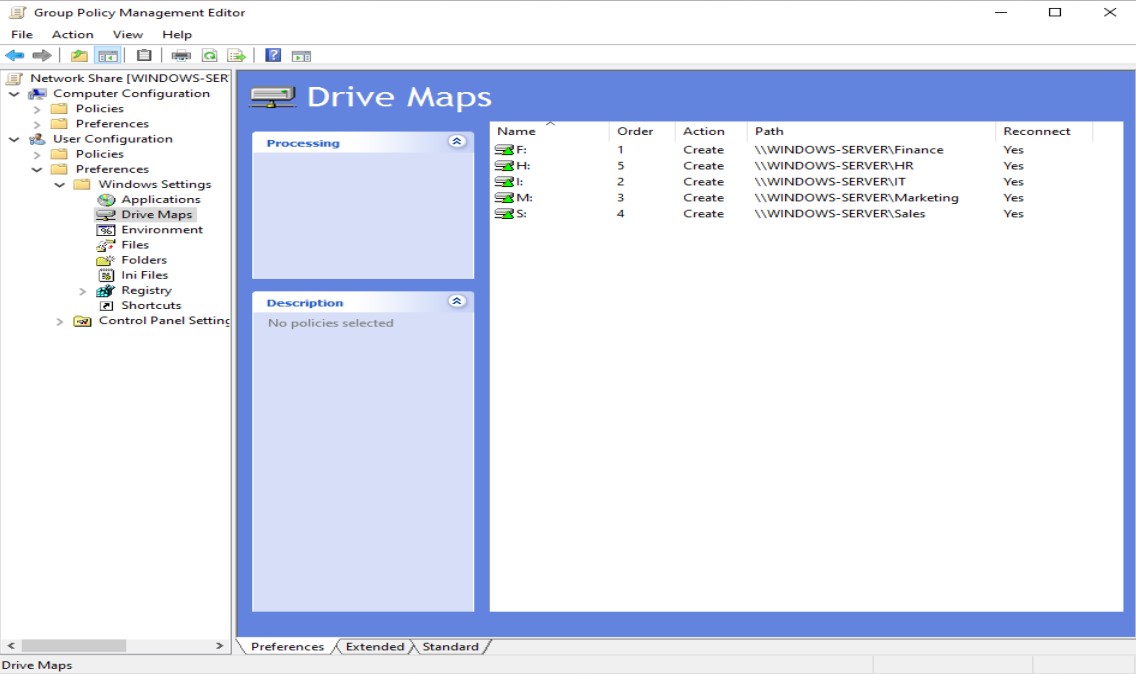
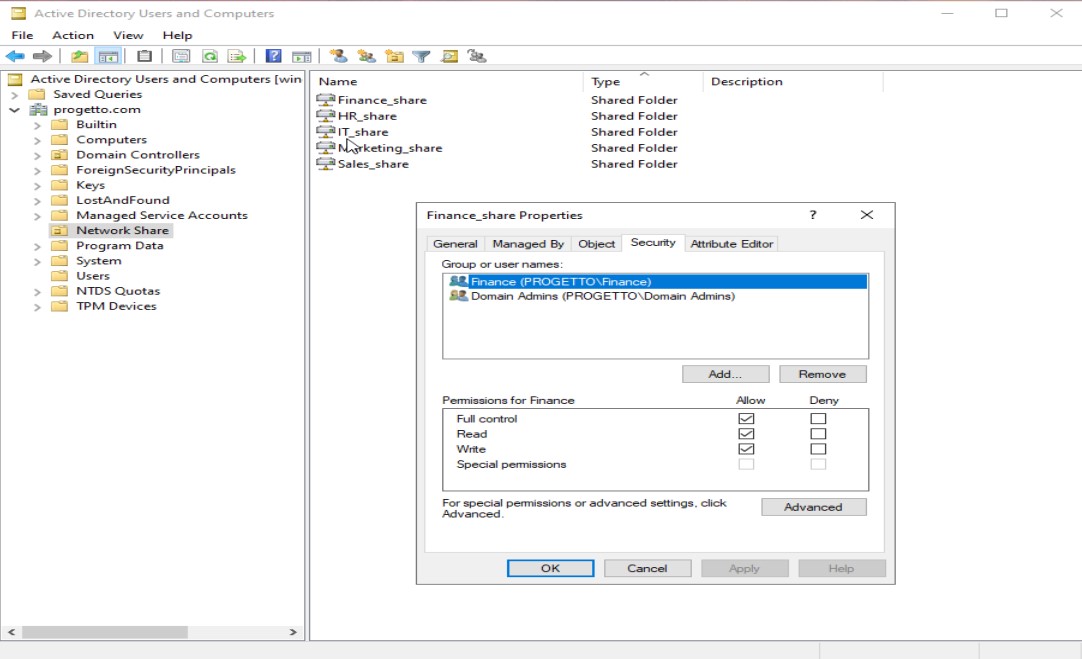
* + 1. [Script di creazione gruppi](Script/Group_create.ps1): i comandi usati consistono fondamentalmente delle seguenti istruzioni.

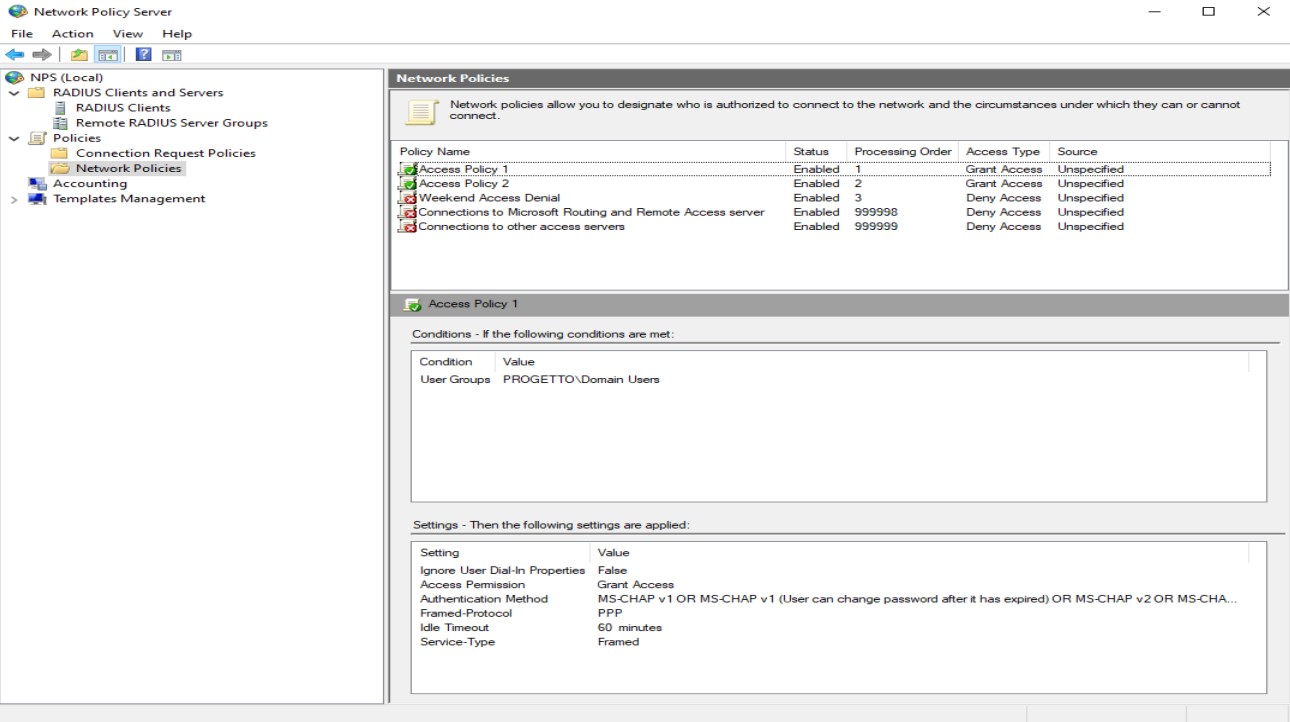
New-ADGroup -Name "NomeGruppo" -SamAccountName "NomeSAMGruppo" -GroupCategory Security -GroupScope Global -Path "CN=Users,DC=progetto,DC=com" -Description "IT Administrators Group”

È stata scelta come destinazione dei gruppi il container di default “Users” per motivi di semplicità di gestione e per evitare troppa dispersione. In contesti come numeri di risorse maggiori può essere più efficiente e conveniente organizzare i gruppi in Organizational Units, ciò comporta una migliore separazione logica e visuale ma anche la possibilità, non presente per il container di default Users, di legare direttamente a tali OU le Group Policy volute.

* 1. Creazione utenti ed aggiunta ai gruppi:

La creazione degli utenti ha avuto origine dalla definizione di un [file in formato CSV](Script/users.csv) contenente i dati iniziali necessari per i rispettivi profili. Questa soluzione è giustificata esclusivamente da necessità di flessibilità e velocità di implementazione e, contenendo dati sensibili quali la password iniziale, non rappresenta una base sicura di gestione dei dati da cui importare le informazioni di registrazione utente.

* + 1. Importare i dati del file CSV con [apposito script powershell](Script/Users_Creator.ps1): questo script itera fra le informazioni di ogni utente, assegna i valori alle variabili necessarie come parametri per il cmdlet di creazione, controlla se esista già un utente con tali valori, in caso contrario crea l’utente e successivamente lo aggiunge al gruppo specificato nella descrizione del profilo. Fra le impostazioni di creazione degli account vi è anche l’obbligo, per gli utenti, di cambiare la password di partenza dopo il primo accesso.
  1. Creazione ed applicazione delle GPO:  
     Le Group Policy sono state definite con l’obiettivo di migliorare la sicurezza di base delle risorse, sia a livello di configurazione macchina che utente. Si è cercato di applicare criteri che tenessero in considerazione le linee guida per prevenire: Broken Access Control (Deny by Default, privilegio minimo, ABAC), Security Misconfiguration, Identification and Authentication Failures, Security Logging and Monitoring Failures. È stato inoltre scelto di separare le GPO, non solo in base ai gruppi di applicazione, ma soprattutto per separare le configurazioni e facilitarne manutenzione e modifiche. È possibile trovare a [questo link](Indirizzi%20GPO.docx) gli “indirizzi specifici” per ogni impostazione descritta.
     1. Software Deployment: policy per la distribuzione automatica del software, approvato dagli admin, sulle macchine del dominio. Seguendo le [istruzioni qui riportate](https://learn.microsoft.com/en-us/troubleshoot/windows-server/group-policy/use-group-policy-to-install-software), è stato:
        + Creato un Distribution Point, contenente il pacchetto di installazione in formato msi, con gli appositi permessi di accesso (in questo caso direttamente nel domain controller, in una situazione reale in un apposito server)
        + Definita una GPO che specifichi il percorso del distribution point ed assegni quest’ultimo alle risorse di dominio.
        + All’avvio della macchina il software sarà automaticamente installato.
     2. Deny App Installation: policy per impedire agli utenti non admin l’installazione di applicativi non ammessi
        + Disattivare Windows Installer per pacchetti non distribuiti dalla GPO di cui sopra.
        + Disattivare opzione Add/Remove Program dal pannello di controllo.
     3. Deny App Execution: aggiunte policy per esecuzione di file e script che, in sinergia con le policy di distribuzione e installazione software, impediscono di eseguire materiale non presente nelle cartelle definite.
        + AppLocker: definite delle impostazioni base per bloccare script o eseguibili non riconosciuti.
     4. Account Policies: policy “enforced” in quanto deve sovrascrivere alcune impostazioni definite inizialmente dalla policy di default di AD. Tale configurazione definisce:
        + Password Policy Enhancement:
          1. Lunghezza minima della password di 12 lettere.
        + Account Lockout Policy Enhancement:
          1. Numero di tentativi di login errati prima di bloccare temporaneamente l’account: 5.
          2. Durata blocco account: 10 minuti.
          3. Reset counter di blocco: 10 minuti.
     5. Local Policies: policy applicate ad utenti non admin. Definiscono:
        + Audit Enhancement:
          1. Audit logon events success and failure: per monitorare gli eventi di accesso ai client.
          2. Audit policy change success and failure: per monitorare gli eventi di cambio policy, non ammessi, da parte degli utenti.
        + User Right Assignment:
          1. Impedito ad utenti non admin la connessione via RDP a macchine client.
          2. Impedito a non-admin di modificare System Time e System Time Zone, ciò è importante per la corretta cronologia dei log impostati per monitorare firewall, accessi, et similia.
        + Interactive Logon:
          1. Machine inactivity: impostato un timer di inattività macchina, alla fine del quale viene attivato il blocco dello schermo.
          2. Password Change: imposta un timer che porta l’utente a cambiare la password del profilo prima di una determinata scadenza.
          3. Hide Last Signed-in: nella schermata di blocco schermo, non viene riportato lo user name dell’ultimo utente che ha acceduto alla macchina.
        + Network Security:
          1. LAN Manager authentication level: imposta l'invio della sola risposta NTLMv2 e rifiuta LM e NTLM.
          2. Minimum session security for NTLM SSP based (including secure RPC) clients e server: richiede una crittografia a 128 bit. Sia sicurezza della sessione NTLMv2 che key 128 BIT.
        + User Account Control:
          1. Comportamento in caso di richiesta di elevazione dell’autorizzazione per utenti non admin: nega automaticamente le richieste di elevazione.
     6. Windows Defender Antivirus: policy configurata per tutti gli utenti che imposta delle misure base di sicurezza attuate tramite Windows Defender.
        + Real Time Protection:
          1. Abilitata protezione in tempo reale.
          2. Abilitato monitoraggio del comportamento utente.
          3. Abilitata scansione di file e allegati.
          4. Abilitato monitoraggio di file e programmi.
          5. Abilitato scanning degli script.
        + Impostazioni di scansione:
          1. Abilitata scansione e-mail.
          2. Heuristics.
          3. Abilitata scansione dispostivi USB.
          4. Impostato massimo utilizzo della CPU durante scansione.
          5. Scelto quale tipo di scansione fare e quando farla.
     7. Windows Update: policy per garantire che tutti gli aggiornamenti siano recepiti uniformemente dalle macchine nel dominio.
        + Automatic Updates: scaricare e installare automaticamente gli aggiornamenti in un momento specifico per ridurre al minimo le interruzioni.
     8. Miscellaneous: impostazioni che definiscono misure di sicurezza meno specifiche.
        + Event Log Size and Retention:
          1. Configura la dimensione dei log di Security, Application, e Sistema ad almeno128 MB.
          2. Mantiene i log almeno per 90 giorni.
        + Disabilitazione porte (USB, etc etc):
          1. Ammessa installazione (e quindi utilizzo) solo di dispositivi con uno specifico ID
          2. Disabilita installazione di dispositivi non descritti da altre policy.
        + Removable storage access:
          1. Disabilità tutti i permessi (lettura, scrittura, esecuzione) per tutte le classi di storage removibili (cd, floppy, usb, tape drives, …).
     9. Network Share: policy per mappare come drive di sistema le share di rete definite in seguito agli utenti. Oltre a definire le share come drive di sistema, permette ogni directory appaia solo al gruppo di utenti a cui è dedicata. Ciò è permesso poiché, i drive creati nelle User configuration di tale GPO, possiedono impostazioni di targetting configurabili con diversi parametri, in questo caso, per Security Group.
  2. Creazione delle share di rete:  
     Questo processo crea una directory per dipartimento e garantisce totale controllo solo agli utenti di tali gruppi ed agli admin. Vengono inizialmente create le apposite cartelle nel server (come nel caso del distribution point, dovrebbe esservi un server dedicato a questa funzione).  
     Successivamente, tramite il tool di gestione ADUC, viene istanziata una OU specifica per le share di rete. Al suo interno verranno definite le cartelle condivise in termini di percorso e Access List, per ogni dipartimento.

1. **Configurazione del Server RADIUS:**Di seguito viene descritta la configurazione di un server RADIUS e cioè di un server di autenticazione e gestione dell'accesso remoto che svolge un ruolo cruciale nella gestione della sicurezza e dell'accesso alle reti. Vengono inoltre descritte alcune policy implementate che gestiscono politiche di accesso remoto.
   1. Impostare Server Radius:
      1. Una volta scaricato ed installato il ruolo NPS tramite Server Manager, è sufficiente configurare NPS come server RADIUS tramite Network Policy Server.
   2. Configurare Policy ed eventuali Client (assenti nella nostra configurazione):
      1. Due policy di approvazione dell’accesso una specifica per utenti ed una dedicata agli amministratori.
      2. Una policy per impedire l’accesso alla rete in momenti non lavorativi, così da evitare accessi indesiderati in momenti in cui una risposta immediata da parte degli amministratori non può essere attuata.