DOKUMENTASJON AV PROSJEKT

Her er linken til repoet vårt: https://gitlab.stud.idi.ntnu.no/jovre/dcst1005-prosjekt-gruppe10

Innledning

I dette prosjektet har vi sikret On-PremiumIT sin infrastruktur. I dette løsningsforslaget skal vi presentere fremgangsmåten vår, samt forklare hvorfor vi har gjort det som vi gjør. Vi begynte med å rulle ut et produksjonsmiljø og et testmiljø, slik at vi hadde et miljø der vi kunne teste og feile før vi implementerte det i produksjonsmiljøet.

AD-struktur

På disse miljøene installerte vi Active Directory, og meldte maskinene inn i domenet. Installasjon av samt opprettelse av AD-strukturen ble utført ved bruk av skript for å sikre god navnekonvensjon og minimere sannsynligheten for menneskelig feil. AD-strukturen for bedriften vil bestå av en domenekontroller for å styre AD-en, en manager-pc til administrativt arbeid på domenekontrolleren gjennom en PSSession, en server til lagring av felles filer og en rekke klienter til bedriftens ansatte.

Opprettelse av OU

Laget OU for maskiner, brukere og grupper. Maskin og gruppe-OU'ene får så under-OU'er for hver avdeling i bedriften. Gruppe-OU'en får lokale og globale grupper, lager også grupper for avdelingene.

File-Share

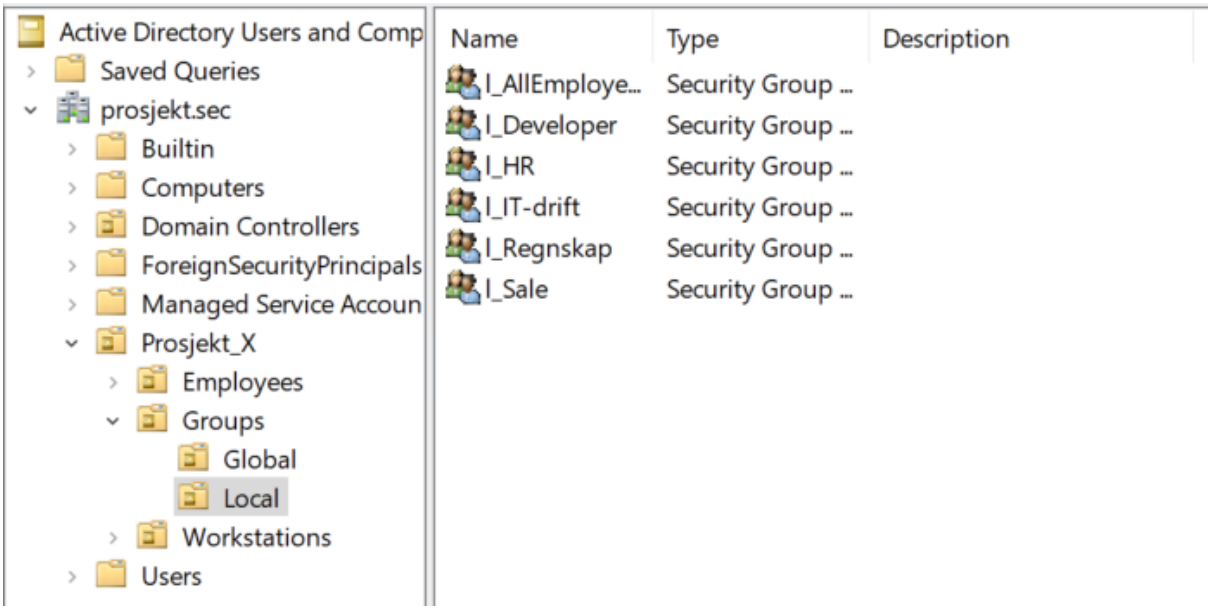
Oppretter delte filområder for hvert avdelingen. Dette fjerner den generelle tilgangen for brukere og gir kun gruppen som tilhører avdelingen avgang til dens delte filområde.

Opprettelse av brukere

Oppretter brukere via kode og csv-fil som inneholder fornavn, etternavn og departement, kode lager SAMAccountName og UPN ut i fra den infoen, passord genereres automatisk og sendes til fil med SAMAccountName, siden passord er lagret i klartekst er passordbytte ved første innlogging satt på. Brukere blir lagret i OU, og lagt i gruppe til departement. CSV-filen tømmes for å kunne putte inn nye brukere. Da kan skriptet 3-Create-users-in-bulk kjøres på nytt, for å legge til de nye brukerne.

Globale og lokale sikkerhetsgrupper

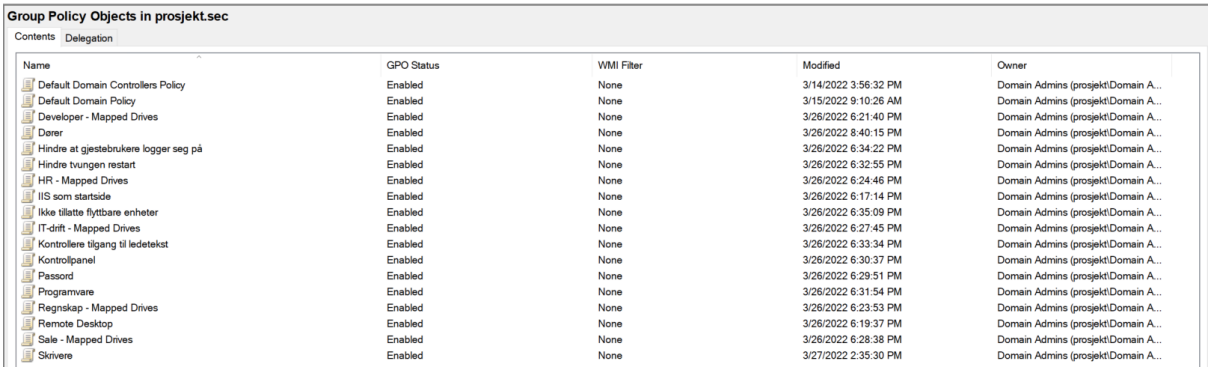
Globale og lokale sikkerhetsgrupper er viktig i en bedrift for å la de ulike avdelingene kun få rettigheter og tillatelser som angår dem. Vi har lokale sikkerhetsgrupper til hver avdeling, eks. *l_Regnskap*, som gjør at de vil få tilgang til sine respektive mapper og dører når vi knytter disse gruppene til GPO for tilgang til dører og mapper. Vi har også en lokal gruppe for alle ansatte, *l_AllEmployees*. Denne gruppen vil ha tilgang til bygget og 'Remote Desktop'. Den globale sikkerhetsgruppen er en del av den lokale sikkerhetsgruppen.



Her er en illustrasjon av de lokale sikkerhetsgruppene.

Group Policy

Group Policy er viktig å ta i bruk for å sikre bedriftens maskiner/servere og brukere.



Group Policy Objects in prosjekt.sec

Contents | Delegation

Name	GPO Status	WMI Filter	Modified	Owner
Default Domain Controllers Policy	Enabled	None	3/14/2022 3:56:32 PM	Domain Admins (prosjekt\Domain A...
Default Domain Policy	Enabled	None	3/15/2022 9:10:26 AM	Domain Admins (prosjekt\Domain A...
Developer - Mapped Drives	Enabled	None	3/26/2022 6:21:40 PM	Domain Admins (prosjekt\Domain A...
Dører	Enabled	None	3/26/2022 8:40:15 PM	Domain Admins (prosjekt\Domain A...
Hindre at gjestebrukere logger seg på	Enabled	None	3/26/2022 6:34:22 PM	Domain Admins (prosjekt\Domain A...
Hindre tvungen restart	Enabled	None	3/26/2022 6:32:55 PM	Domain Admins (prosjekt\Domain A...
HR - Mapped Drives	Enabled	None	3/26/2022 6:24:46 PM	Domain Admins (prosjekt\Domain A...
IIS som startside	Enabled	None	3/26/2022 6:17:14 PM	Domain Admins (prosjekt\Domain A...
Ikke tillatte flyttbare enheter	Enabled	None	3/26/2022 6:35:09 PM	Domain Admins (prosjekt\Domain A...
IT-drift - Mapped Drives	Enabled	None	3/26/2022 6:27:45 PM	Domain Admins (prosjekt\Domain A...
Kontrollere tilgang til ledetekst	Enabled	None	3/26/2022 6:33:34 PM	Domain Admins (prosjekt\Domain A...
Kontrollpanel	Enabled	None	3/26/2022 6:30:37 PM	Domain Admins (prosjekt\Domain A...
Passord	Enabled	None	3/26/2022 6:29:51 PM	Domain Admins (prosjekt\Domain A...
Programvare	Enabled	None	3/26/2022 6:31:54 PM	Domain Admins (prosjekt\Domain A...
Regnskap - Mapped Drives	Enabled	None	3/26/2022 6:23:53 PM	Domain Admins (prosjekt\Domain A...
Remote Desktop	Enabled	None	3/26/2022 6:19:37 PM	Domain Admins (prosjekt\Domain A...
Sale - Mapped Drives	Enabled	None	3/26/2022 6:28:38 PM	Domain Admins (prosjekt\Domain A...
Skrivere	Enabled	None	3/27/2022 2:35:30 PM	Domain Admins (prosjekt\Domain A...

Her er en illustrasjon av alle GPO bedriften må forholde seg til.

- Det første GPO vi har er å sette C:\inetpub\wwwroot\iisstart.htm som default startside i Microsoft Edge på klientene.

- Det andre GPO vi har er å tillate bedriftens ansatte å Remote Desktop til sine laptoper.

- Det tredje GPO vi har vil automatisk mappe opp delt mappe for de respektive avdelingene. Dette GPO er det fem av, én til hver avdeling. Dette vil sørge for at medlemmene av hver avdeling bare får tilgang til sine respektive mapper.

- Det fjerde GPO vi har dreier seg om passord. Her har vi satt flere betingelser når man skal opprette nytt passord. Den ene betingelsen er når de logger seg på første gang, med passordet i *userinfo.csv*, vil de måtte endre til et nytt passord ettersom vi har satt 'Minimum password age: 0 days'. I tillegg må passordet være på minst 12 tegn, og inneholde spesialtegn og stor bokstav.

- Det femte GPO vi har sørger for at ansatte ikke kan gå på kontrollpanel. Gjennom kontrollpanelet kan man kontrollere alle aspekter av datamaskinen. Så ved å moderere hvem som har tilgang til datamaskinen, kan man holde data og andre ressurser trygge.

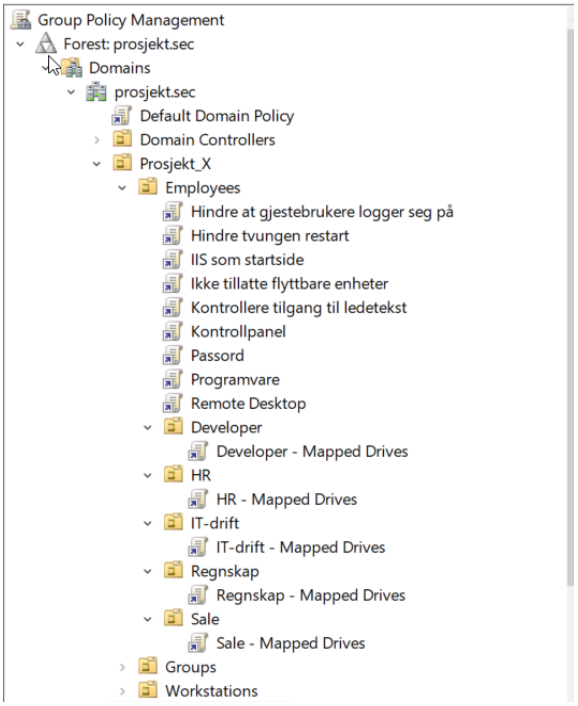
- Det sjette GPO vi har gjør at ansatte ikke kan installere programvare. Om man har friheten til å installere programvare, kan kan installere uønskede apper som kompromitterer systemet. Systemadministratorer må vanligvis rutinemessig utføre vedlikehold og rengjøring av slike systemer. For å være på den sikre siden, er det gunstig å forhindre programvareinstallasjoner gjennom gruppepolicy.

- Det syvende GPO vi har gjør at ansatte ikke blir tvunget til omstart i forbindelse med oppdateringer. Tvunget omstart er ikke uvanlig, for eksempel kan det være situasjoner der man jobber på datamaskinen sin og Windows viser en melding om at systemet må startes på nytt på grunn av en sikkerhetsoppdatering. I mange tilfeller, hvis man ikke legger merke til meldingen eller bruker litt tid på å svare, starter datamaskinen automatisk på nytt, og man mister viktig, ulagret arbeid.

- Det åttende GPO vi har er å hindre tilgang for ansatte til ledetekst. Ledetekster kan brukes til å kjøre kommandoer som gir høynivå-tilgang til brukere og unngår andre restriksjoner på systemet. Så for å sikre systemet, er det lurt å deaktivere ledetekst.

- Det niende GPO vi har hindrer at gjestebrukere kan logge inn. Gjennom en gjestekonto kan man få tilgang til sensitive data. Slike kontoer gir tilgang til en Windows-datamaskin og krever ikke passord. Aktivering av denne kontoen betyr at alle kan misbruke tilgangen til systemene.

- Det tiende GPO vil hindre ansatte å bruke flyttbare mediestasjoner. Flyttbare mediestasjoner er svært utsatt for infeksjon, og de kan også inneholde virus eller skadelig programvare. Hvis en bruker kobler en infisert stasjon til en nettverksdatamaskin, kan det påvirke hele nettverket.



Her er en illustrasjon av hvor de ulike GPO er knyttet hen.

Tjenester

Overvåking av kritiske tjenester som kjøres i bedriftens infrastruktur er viktig slik at bedriften kan fungere optimalt med minst mulig nedetid. AD burde overvåkes fordi det kobler sammen maskinene, AD avhenger også av flere tjenester som DNS, DFS Replication, osv. Disse tjenestene burde også overvåkes slik at feilsøking vil bli lettere og nedetid kortere. I tillegg overvåkes Windows Time for å synkronisere klokkene til pc-ene på et nettverk. Dette gjøres som en Task på DC1 som gjøres hvert femte minutt for å holde nedetid som skyldes tjenestene vi overvåkes minimal. I forbindelse med delte områder burde DFS overvåkes. DFS burde overvåkes fordi dette er tjenesten som muliggjør delte filområder.

Vi har valgt å overvåke prosessor, RAM og total bruken til disken. I tillegg til hvor mye nettrafikken i bits per sekund. Dette er kritiske counters å overvåke og skrives til egen .csv-fil med dato og klokkeslett når den blir tatt. Dette og overvåking av W3SVC kjøres som en ScheduledJob. Dette skulle egentlig gjøres som en ScheduledTask, men det fungerte ikke så vi da for en alternativ løsning som fungerte.

Backup

Vi valgte en løsning med både full backup og incremental backup. Full backup er viktig fordi du får da tilgang til all data på et sted for enkel oppretting av eventuelle mistede filer. Det tar imidlertid mye plass, så å ta full backup hver dag er uhensiktsmessig. Vi har valgt å schedule en full backup en gang i uken, med en incremental backup hver dag. Med et slikt oppsett går det ikke for lang tid mellom hver fulle backup slik at oppretting er relativt effektivt med tanke på størrelse, kontra for eksempel et intervall på en måned. Skulle den nyeste fulle backupen også bli skadet må man bare en uke til tilbake i tid for å opprette. Med incremental backup som supleringsbackup får man også daglig trygghet i form av små backuper som lagrer endringer mellom hver dag. Det blir noen flere backup filer å gjenopprette, men i løpet av bare en uke blir det ikke alt for mye.

Kilder

Allen, R. (2021). How To Map Network Drives With Group Policy (Complete Guide). Hentet fra: https://activedirectorypro.com/map-network-drives-with-group-policy/

Constantinos, T. (2015, 14. desember). Monitoring Domain Controller Health Status with PowerShell. Hentet fra https://askme4tech.com/monitoring-domain-controller-health-status-powershell

Huculak, M. (2021, 30. januar). How to create scheduled tasks with PowerShell on Windows 10. Hentet fra https://www.windowscentral.com/how-create-scheduled-tasks-powershell-windows-10

Microsoft. (2021, 5. oktober). How the Windows Time Service Works. Hentet fra https://docs.microsoft.com/en-us/windows-server/networking/windows-time-service/how-the-windows-time-service-works

Murphy, D. (2017). Top 10 Most Important Group Policy Settings for Preventing Security Breaches. Hentet fra: https://www.lepide.com/blog/top-10-most-important-group-policy-settings-for-preventing-security-breaches/

Normand, Y. (2020, 29. desember). Password generation in PowerShell Core (6+). Hentet fra https://dev.to/onlyann/user-password-generation-in-powershell-core-1g91

Tor Ivar Melling. (2022, 27. februar). *PowerShell og Get-Service for å overvåke status på kjørende tjenester*[Videoklipp]. Hentet fra https://www.youtube.com/watch?v=mLyc1jC05u4&ab_channel=TorIvarMelling