

6105 Windows Server og datanett

Leksjon 6a Grupper i Windows

- Lokale grupper og domenegrupper
- Gruppetyper og scopes
- Innebygde grupper



Pensum

- Kvisli: Windows Server og nettverk, kapittel 8 Grupper

Relevante lenker

Microsoft Docs:

- » [Active Directory Security Groups](#)
- » [Authentication Services: Groups](#)
- » [Authentication Services: Group Scope](#)

Andre kilder

Windows Server Brain: [Understanding Group Types and Scopes](#)

Grupper

Gruppe = samling av brukerkontoer, som

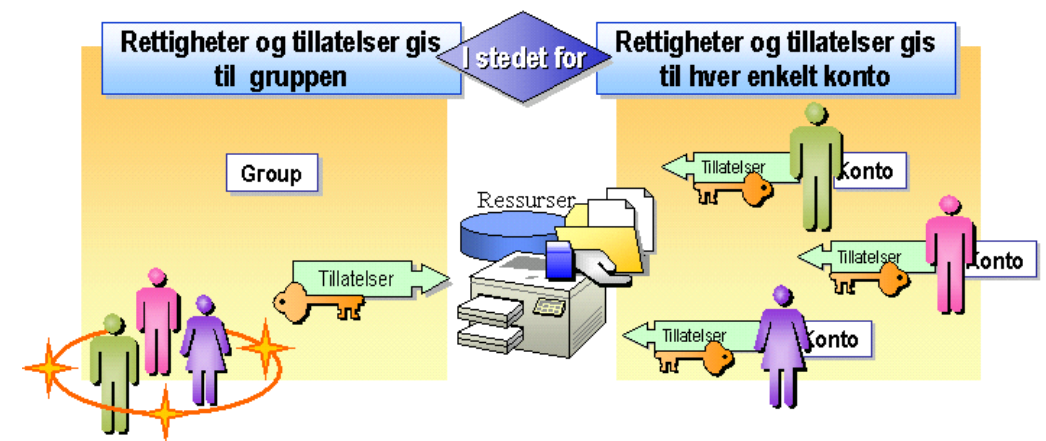
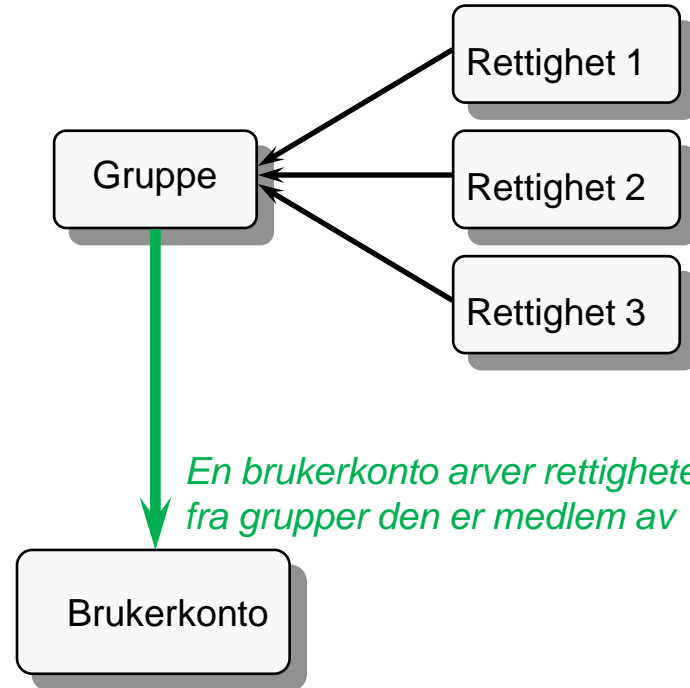
- hører organisatorisk sammen
- og / eller
- skal ha like rettigheter

Hovedhensikt

- Forenkle administrasjonen av brukere og rettigheter

Oppnås ved at

- rettigheter kan tildeles grupper i stedet for hver enkelt bruker
- rettigheter kan lett endres ved å melde brukere inn og ut av grupper



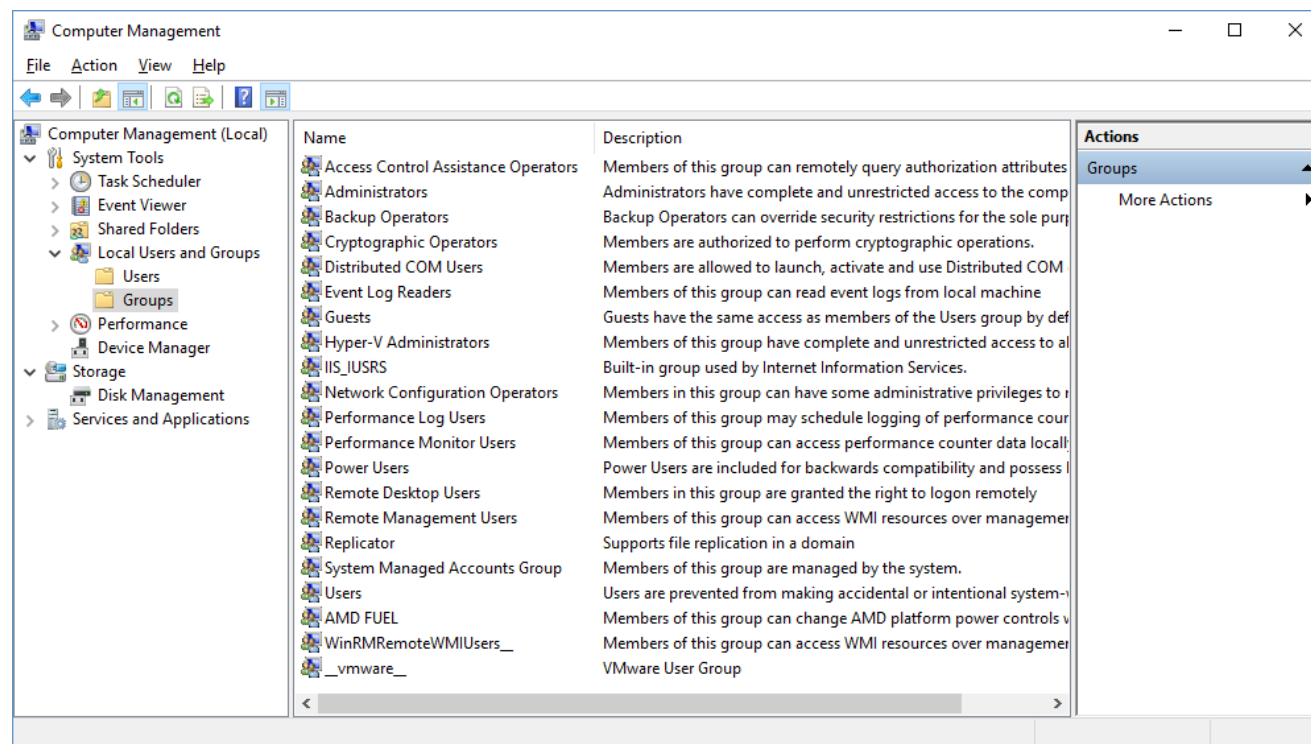
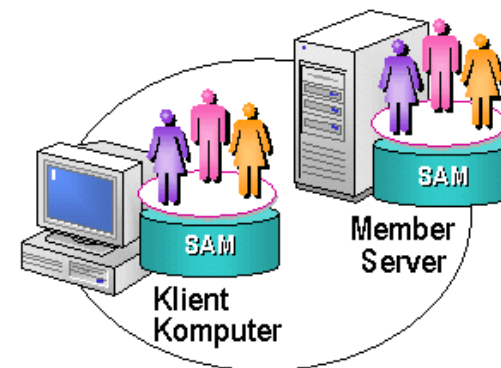
Lokale grupper

Egenskaper

- Defineres og administreres lokalt på én maskin
 - » Med verktøyet Computer Management
- Lagres i lokal SAM
- Brukes vanligvis bare i arbeidsgrupper (ikke i domener)

Innebygde lokale grupper i Windows klient

- Administrators
- Backup Operators
- Cryptographic Operators
- Guests
- IIS_IUSRS
- Network Configuration Operators
- Performance Monitor Users
- Power Users
- Remote Desktop Users
- Replicator
- Users
- m.fl.



Lokale grupper

Begrensninger

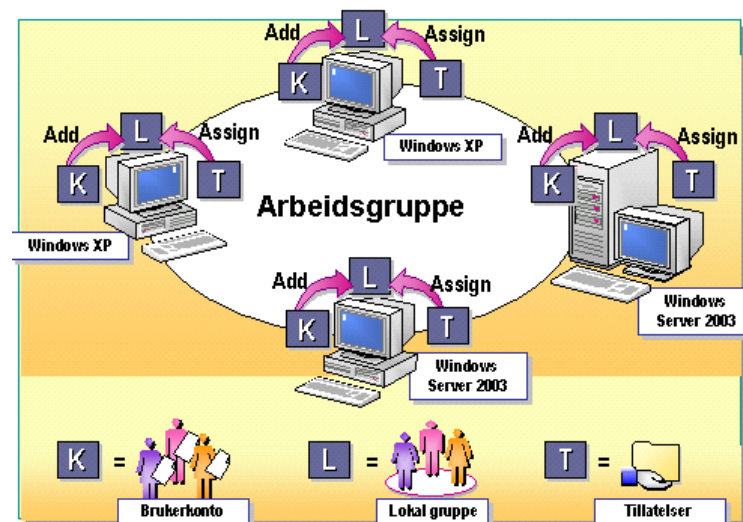
- Kan bare inneholde lokale brukerkontoer fra gruppens maskin
 - » på en medlemstjener kan lokale grupper dessuten inneholde domenekontoer og domenegrupper (se senere)
- Kan bare gis rettigheter til ressurser på gruppens maskin
- Kan ikke være medlem i noen andre grupper!

Hvem kan opprette lokale grupper?

- Medlemmer i gruppen Administrators

Arbeidsmetodikk for lokale grupper

- Opprett lokale brukerkontoer (K)
- Opprett lokale grupper (L), og meld inn kontoer som skal ha like rettigheter
- Gi tilgangsrettigheter (T) til de lokale gruppene



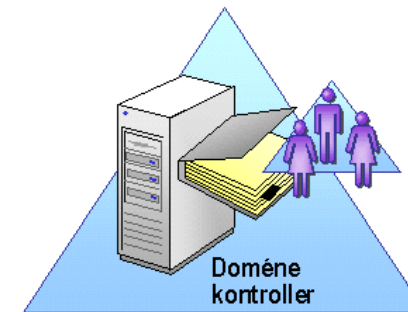
"KLT strategi" for lokale grupper

Konto → Lokal Gruppe ← Tilgangsrettighet

Domene grupper

Egenskaper

- Defineres i AD på domene kontroller
 - » Med verktøyet Active Directory Users and Computers
- Lagres i Active Directory Domain Services (AD DS)
- Kan gis rettigheter til ressurser på alle maskiner i domenet
- Kan være medlem i andre grupper

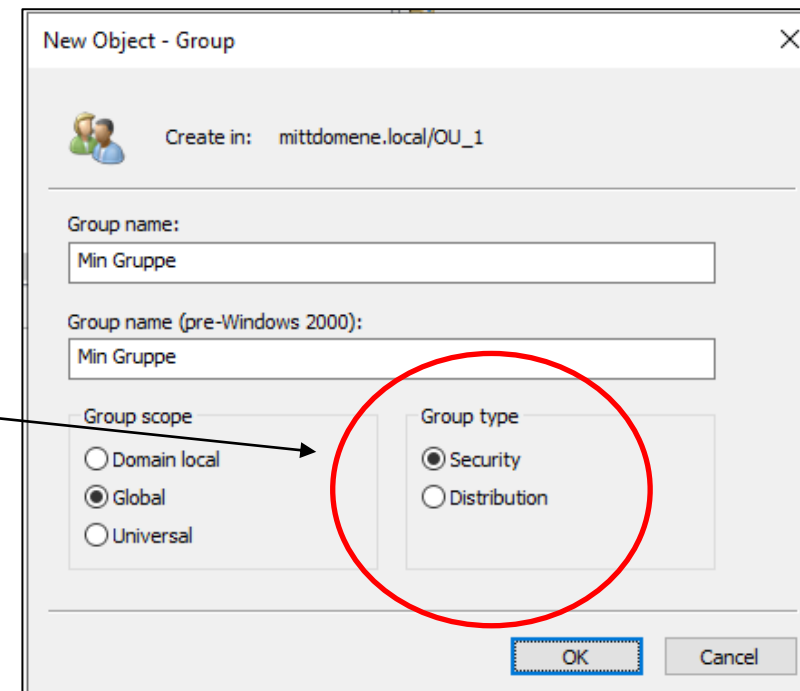


Hensikt

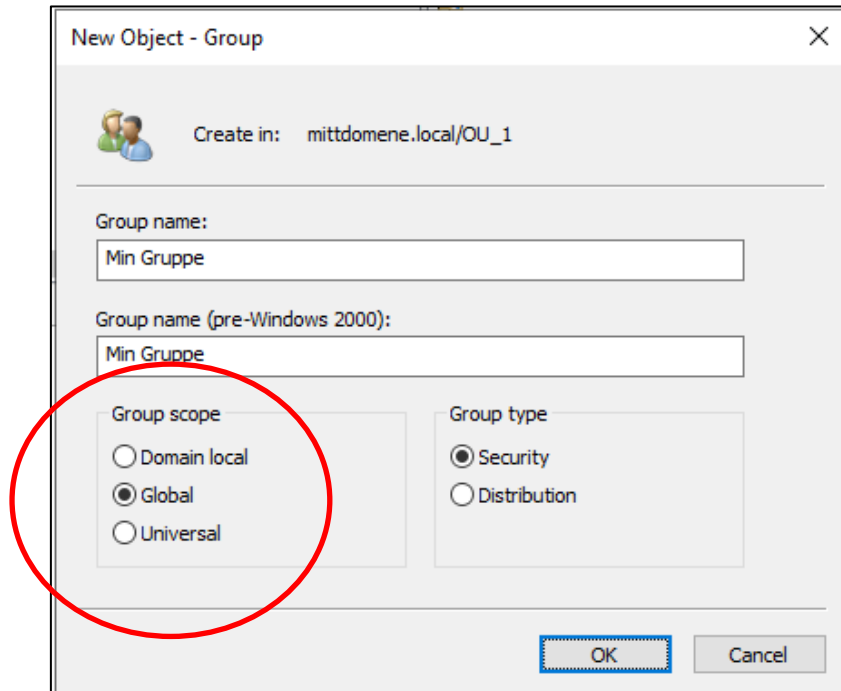
- Forenkle sentral administrasjon av brukere og rettigheter

Gruppetyper (Group type)

- Sikkerhetsgruppe (bruk denne)
 - » For å administrere tilgangsrettigheter til ressurser
- Distribusjonsgruppe (lite brukt)
 - » Beregnet for distribusjonslister i e-post
 - » Kan ikke gis tilgangsrettigheter
 - » Programmer som skal bruke disse må kunne lese AD DS



Scopes for domenegrupper



Group Scopes

Group scope	Members from same domain	Members from domain in same forest	Members from trusted external domain	Can be assigned permissions to resources
Local	U, C, GG, DLG, UG and local users	U, C, GG, UG	U, C, GG	On the local computer only
Domain Local	U, C, GG, DLG, UG	U, C, GG, UG	U, C, GG	Anywhere in the domain
Universal	U, C, GG, UG	U, C, GG, UG	N/A	Anywhere in the forest
Global	U, C, GG	N/A	N/A	Anywhere in the domain or a trusted domain

U User
C Computer
GG Global Group

DLG Domain Local Group
UG Universal Group

Tre ulike scopes for domenegrupper

- Globale grupper
- Lokale domenegrupper
- Universelle grupper

Bestemmer bl.a.

- Hvor i domenet gruppen kan brukes
- Hvilke brukere/grupper som kan være medlem
- Hvordan gruppen brukes

Scopes for domenegrupper

Globale grupper

- Brukes primært som «*rollegrupper*»
 - » Dvs. samler brukerkontoer som har felles organisasjonstilhørighet / rolle
- Vi gir vanligvis ikke tilgangsrettigheter direkte til en global gruppe!
- Kan inneholde brukere, datamaskiner og globale grupper fra eget domene
- Kan være medlem i alle domenelokale og universelle grupper

Domenelokale grupper

- Brukes primært som «*rettighetsgrupper*»
 - » Dvs. vi gir rettigheter til disse gruppene, og melder inn de som skal ha dem
- Kan gis rettigheter til alle ressurser i eget domene
- Kan inneholde alle brukere, datamaskiner, globale og universelle grupper
 - » Kan også inneholde domenelokale grupper fra eget domene.
- Kan være medlem i andre domenelokale grupper i eget domene + lokale grupper

Universelle grupper

- Brukes mest som «*rettighetsgrupper*» i store nettverk med flere domener
- Kan gis rettigheter til ressurser i alle domener (eget og andre) i en AD-skog
- Kan inneholde brukere, globale grupper og universelle grupper i hele AD-skogen.
- Kan være medlem i andre universelle grupper og domenelokale grupper i hele AD-skogen

Innebygde (predefinerte) domenegrupper

Opprettes automatisk ved installasjon av AD

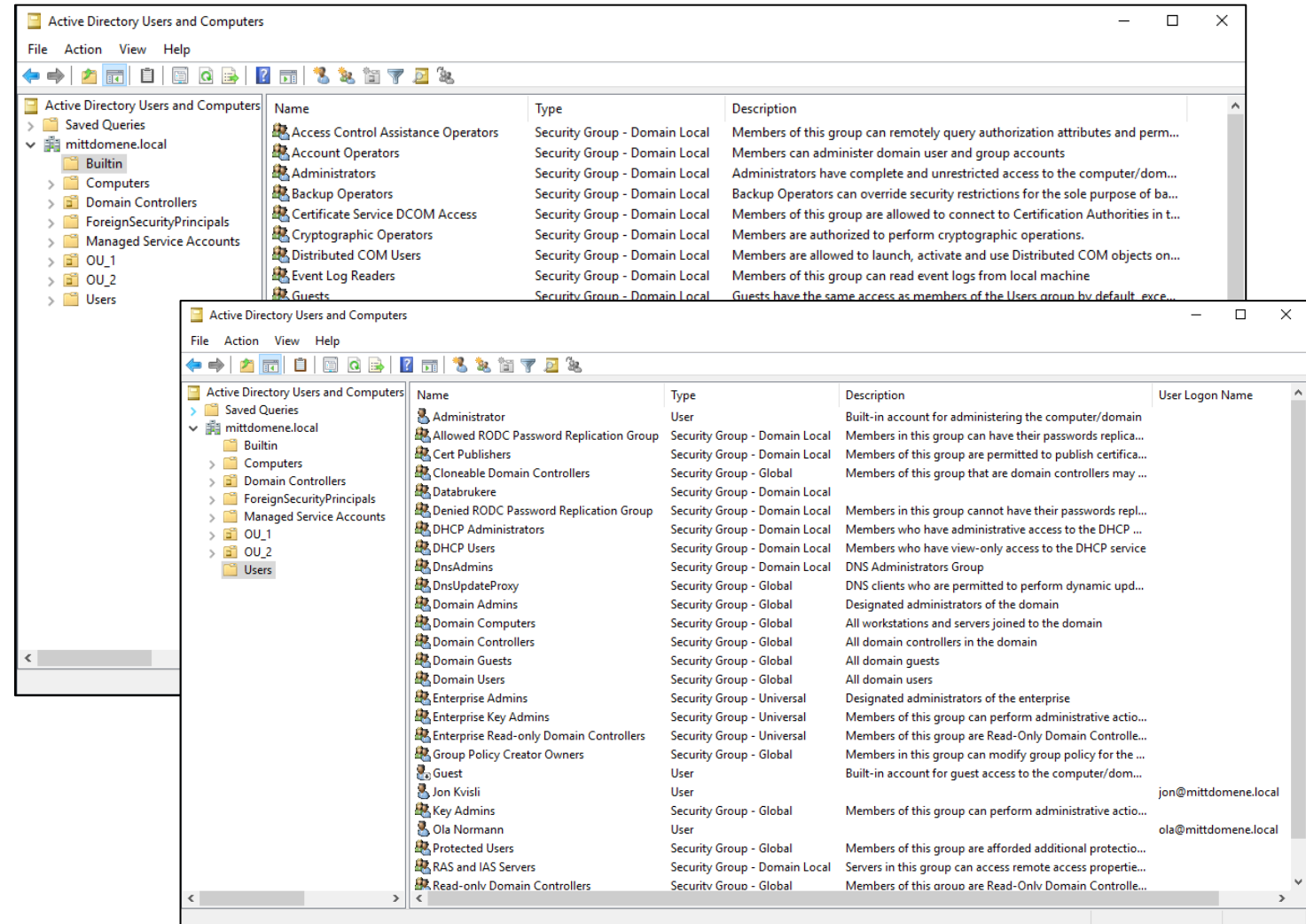
- Lagres i AD DS
- Kan ikke slettes!
- Knyttet til definerte rettigheter

Domene lokale grupper i mappen Builtin

- Account Operators
- Administrators
- Backup Operators
- Print Operators
- Remote Desktop Users
- Users

Globale grupper i mappen Users

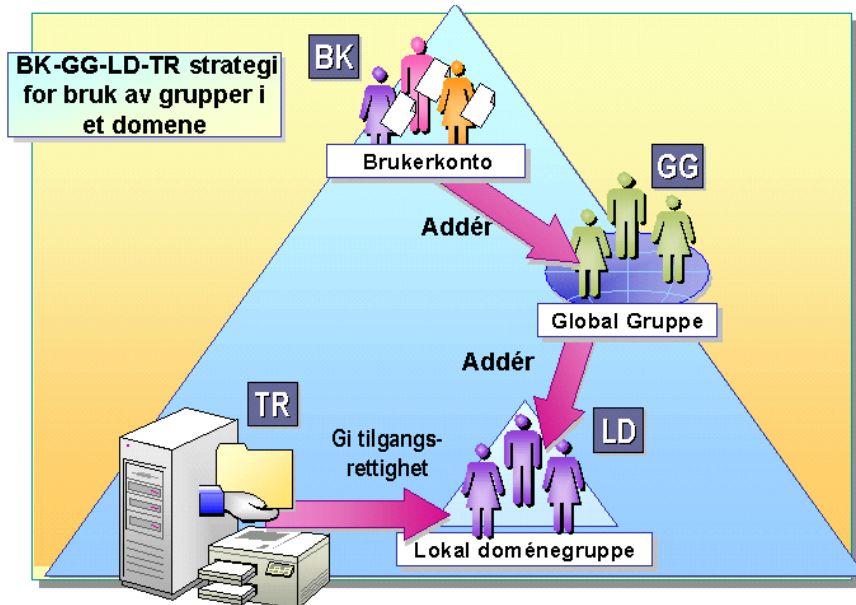
- Domain Admins
- Domain Computers
- Domain Users
- Enterprise Admins



Bruk av grupper i et domene

Arbeidsmetodikk:

- Opprett brukerkontoer (BK)
- Legg de brukerkontoene som har samme rolle / tilhørighet inn i globale grupper (GG)
- Legg de globale gruppene inn i en lokale domenegrupper (LD)
 - » Bruk en innebygget gruppe hvis det passer, eller
 - » Lag en ny lokal domenegruppe
- Gi de lokale domenegruppen tilgangsrettigheter (TR) til ressurser i domenet



BK = lag brukerkontoer

GG = legg brukerkontoer inn i global gruppe

LD = legg global gruppe inn i lokal domenegruppe

TR = tildel rettigheter til lokal domenegruppe

- Minimaliser bruk av universelle grupper
- Legg aldri brukere rett i universelle grupper
- Må være medlem av *Administrators* eller *Account Operators* for å lage domenegrupper