

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

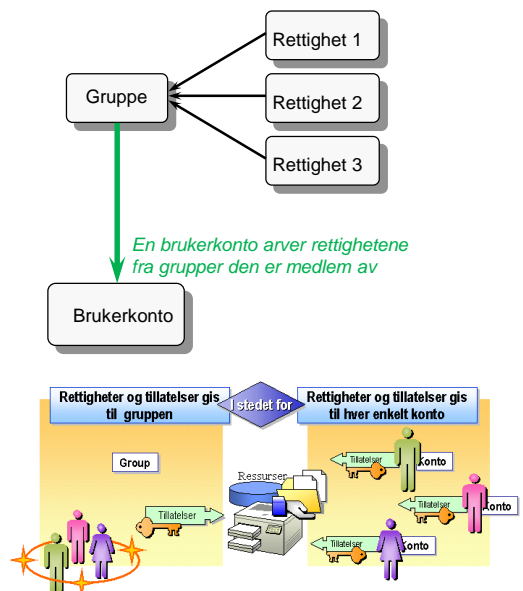
Nyttige lenker

- [Microsoft Technet: Understanding Groups](#)
- [Microsoft Technet: Local Users and Groups](#)
- [Microsoft Technet: Active Directory Security Groups](#)

1

Grupper

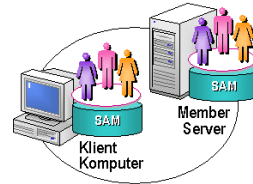
- **Gruppe = samling av brukerkontoer, som**
 - hører organisatorisk sammen
 - og / eller
 - skal ha like rettigheter
- **Hovedhensikt**
 - Forenkle nettverksadministrasjonen
- **Oppnås ved at**
 - rettigheter kan tildeles grupper i stedet for hver enkelt bruker
 - rettigheter kan lett endres ved å melde brukere inn og ut av grupper



2

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**



Name	Description	Actions
Access Control Assistance Operators	Members of this group can remotely query authorization attributes.	
Administrators	Administrators have complete and unrestricted access to the computer.	More Actions
Backup Operators	Backup Operators can override security restrictions for the sole purpose of backing up files.	
Cryptographic Operators	Members are authorized to perform cryptographic operations.	
Distributed COM Users	Members are allowed to launch, activate and use Distributed COM objects.	
Event Log Readers	Members of this group can read event logs from local machines.	
Guests	Guests have the same access as members of the Users group by default.	
Hyper-V Administrators	Members of this group have complete and unrestricted access to all Hyper-V related services.	
IIS_IUSRS	Members in this group used by Internet Information Services.	
Network Configuration Operators	Members in this group can have some administrative privileges to configure network settings.	
Performance Log Users	Members of this group may schedule logging of performance counter data.	
Performance Monitor Users	Members of this group can access performance counter data locally.	
Power Users	Power Users are included for backwards compatibility and possess limited administrative privileges.	
Remote Desktop Users	Members in this group are granted the right to logon remotely.	
Remote Management Users	Members of this group can access WMI resources over management protocols.	
Replicator	Supports file replication in a domain.	
System Managed Accounts Group	Members of this group are managed by the system.	
Users	Users are prevented from making accidental or intentional system changes.	
AMD FUEL	Members of this group can change AMD platform power controls.	
WinRMRemoteWMIUsers_...	Members of this group can access WMI resources over management protocols.	
...vmware_...	Members of this group can access WMI resources over management protocols.	
VMware User Group	Members of this group can access WMI resources over management protocols.	

6105 Windows Server og datanett

© Jon Kvisli, USN

Grupper i Windows - 3

3

Lokale grupper

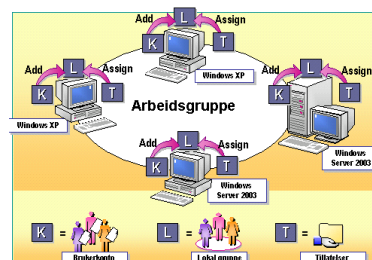
- **Begrensninger**
 - Kan bare inneholde lokale brukerkontoer fra gruppens maskin
 - » på en medlemstjener kan lokale grupper dessuten inneholde domenekontoer og domenegrupper (se senere)
 - Kan bare gis rettigheter til ressurser på gruppens maskin
 - Kan ikke være medlem i noen andre grupper!

- **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

6105 Windows Server og datanett

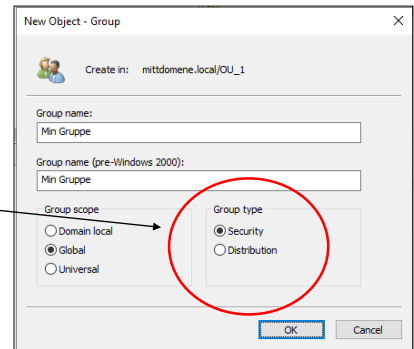
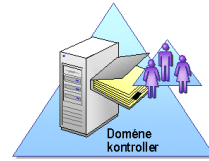
© Jon Kvisli, USN

Grupper i Windows - 4

4

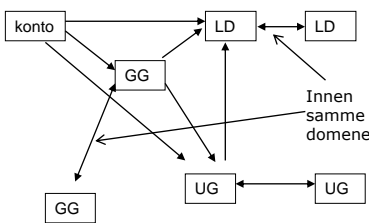
Domengrupper

- **Egenskaper**
 - Defineres på domenekontroller
 - » 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**
 - Sentralisere administrasjon av brukere og rettigheter
- **Gruppetyper**
 - **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

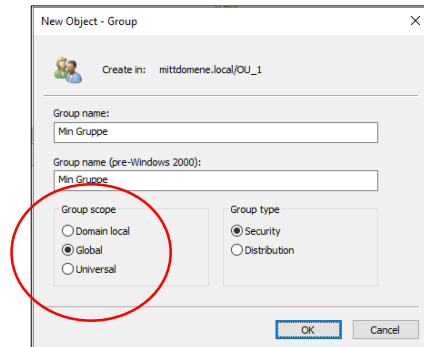


5

Scopes for domengrupper



- **Tre ulike scopes for domengrupper**
 - Globale grupper
 - Lokale domengrupper
 - Universelle grupper
- **Bestemmer**
 - hvor i nettet gruppen kan brukes
 - hvordan gruppen brukes
 - » Bl.a. hvilke objekter som kan være medlem i gruppen



6

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 kun 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

6105 Windows Server og datanett

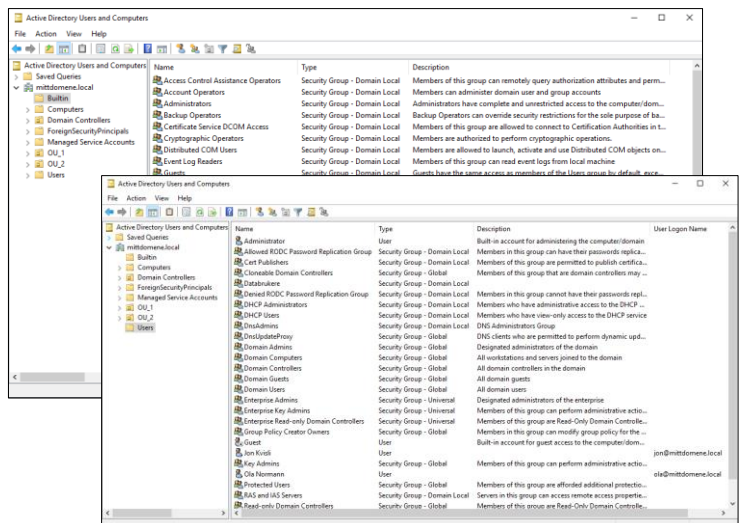
© Jon Kvisli, USN

Grupper i Windows - 7

7

Innebygde (predefinerte) domenegrupper

- **Opprettes automatisk ved installasjon av AD**
 - Lagres i AD DS
 - Kan ikke slettes!
 - Knyttet til definerte rettigheter
- **Domenelokale 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



6105 Windows Server og datanett

© Jon Kvisli, USN

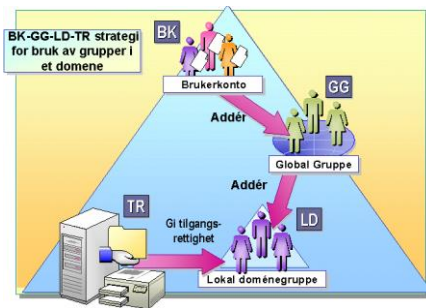
Grupper i Windows - 8

8

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