

6105 Windows Server og datanett

Labøving: Brukeradministrasjon i Active Directory

Oppgave a: Endre lokal *logon-policy* på domenekontroller

En Windows domenekontroller setter begrensninger for hvilke brukerkontoer som får lov å logge inn lokalt på **domenekontrolleren**. I en driftssituasjon er det fornuftig, men i de videre øvingene har vi bruk for å logge inn på domenekontrolleren med nye brukere som vi oppretter. Før vi kan gjøre denne øvingen, må vi derfor endre *sikkerhetspolitikken* på domenekontrolleren, slik at **alle** brukerkontoer i domenet kan logge på lokalt på domenekontrolleren:

1. Logg inn tjenermaskinen som **Administrator**.
2. Bruk *Server Manager* og menyvalget **Tools ► Group Policy Management**
3. Åpne AD skogen (*Forest:*) ► *Domains* ► ditt domene ► mappen **Domain Controllers**.

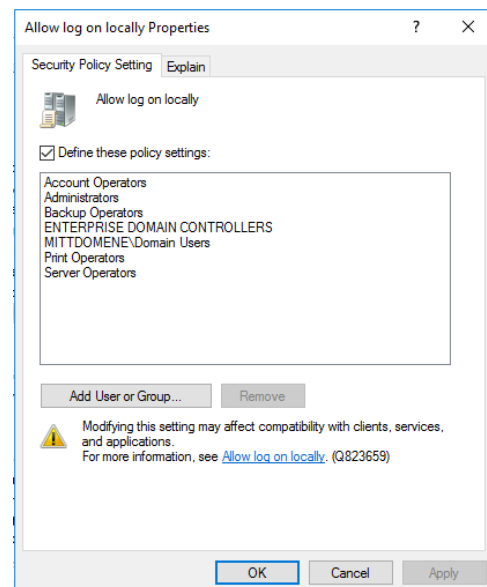
**Obs! Vær nøye med å velge riktige "mapper" i punkt 4-7!
Det er flere mapper med like navn på ulike nivåer, og lett å ta feil!**

4. Høyreklikk på **Default Domain Controllers Policy** under *Domain Controllers* og velg **Edit**.
5. Åpne **Computer Configuration ► Policies ► Windows Settings ► Security Settings ► Local Policies**.
6. Velg (markér) **User Rights Assignment**.
7. I detaljruten til høyre **dobbelklikker** du **Allow log on locally**.

Vinduet til høyre viser da hvilke brukere og grupper som kan logge på lokalt på domenekontrolleren.

8. Sjekk at det står hake foran *Define these policy settings*.
9. Kikk knappen **Add User or Group**.
10. Legg til domenegruppen **Domain Users** på denne måten:

- Klikk knappen **Browse**
- Skriv inn gruppen **Domain Users**
- Klikk knappen **Check names**
- Klikk **Ok**

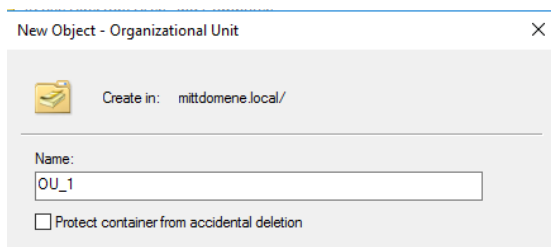


11. Klikk **Apply / OK** og lukk *Group Policy Management Editor*.
12. **Restart tjenermaskinen**. De nye policyene vil bli aktive etter omstart.
13. Sjekk at du kan logge inn på tjenermaskinen med den personlige domenebrukeren du laget i labøving 5a.
14. Logg deretter ut igjen fra denne brukeren.

Oppgave b: Lage organisasjonsenheter i AD domenet

Du skal nå opprette to *organisasjonsenheter* (OUer) i det nye domenet ditt. Dette krever administratorrettigheter for domenet.

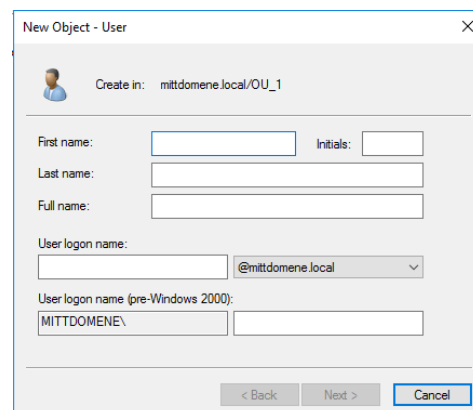
1. Logg inn på tjenermaskinen som **Administrator**
2. Bruk verktøyet *Active Directory Users and Computers*.
3. Høyreklikk domenenavnet og velg **New ► Organizational Unit**.
4. **Ta bort** krysset foran *Protect container from accidental deletion*.
5. Lag to nye organisasjonsenheter med navn **OU_1** og **OU_2** i domenet.



Oppgave c: Lage nye brukerkontoer (domenekontoer) i OUer

Brukeren **Administrator** har også rettigheter til å lage nye domenebrukere i OUene.

1. Høyreklikk **OU_1**, velg **New ► User** og opprett en domenebruker i denne OUen:
 - Fornavn: **Test**
 - Etternavn: **Domenebruker1**
 - Påloggingsnavn (*User Logon Name*): **testbruker1**
 - Passord: **xyz.123**
 - Bruker skal **måtte** endre passord ved neste pålogging.



2. Lag en ny domenebruker i **OU_2**:
 - Fornavn: **Test**
 - Etternavn: **Domenebruker2**
 - Påloggingsnavn (*User Logon Name*): **testbruker2**
 - Passord: **Password.2019**
 - Brukeren skal **ikke** kunne endre passord og passordet skal **aldri** utløpe
3. Test pålogging fra **klientmaskinen** med domenekonten **testbruker1**
Hva skjer under pålogging? _____
4. Velg **Password.2019** når du blir bedt om nytt passord.
5. Test også pålogging fra klientmaskinen med domenekonten **testbruker2**
6. Logg ut fra klientmaskinen.

Oppgave d: Endre egenskaper på domenekontoer i Active Directory

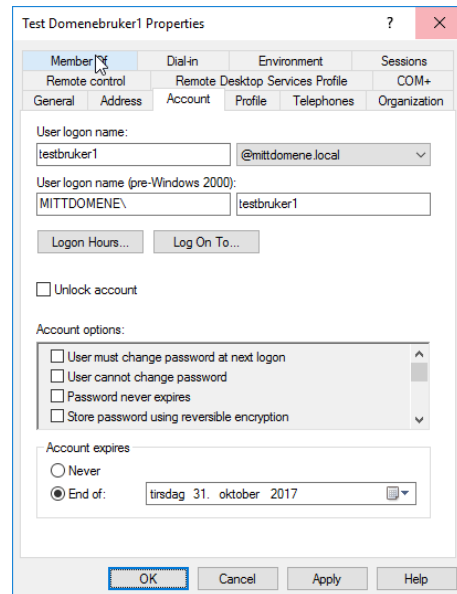
I denne oppgaven skal du endre flere egenskaper på de to domenekontoene du laget i forrige oppgave.

1. Vær pålogget tjenermaskinen som **Administrator**
2. Start programmet *Active Directory Users and Computers* og åpne mappen **OU_1**
3. Bruk menyvalg **View ► Add/remove columns...** og legg til kolonnen *User Logon Name*.
4. Organiser vinduet slik at du ser den nye kolonnen.

5. Dobbeltklikk på brukerkontoen **Test Domenebruker1 (testbruker1)**

6. Velg fanen *Account*, og gjør følgende endringer:

- Sett utløpsdato (*account expires*) til siste dato i neste måned.
- Brukeren skal bare kunne logge inn mandag til fredag mellom kl. 06 og 23 (Knappen *Logon Hours...*).
- Gi brukeren rettighet til å logge på fra din klientmaskin og tjenermaskin, men ingen andre maskiner i domenet (Knappen *Log On To...*).



7. Bruk det du har lært nå og sett følgende egenskaper på brukeren **Test Domenebruker2 (testbruker2)**
 - Gi brukeren rettighet til å logge på mandag til søndag mellom kl 23:00 og 06:00, men ellers ikke.
 - Brukeren skal kunne logge på fra alle maskiner i domenet.
 - Brukerkontoen skal utløpe dagen etter dagens dato.

Test nå brukerkontoene fra klientmaskinen etter endringene:

8. Logg inn domenet fra klientmaskinen med brukeren **testbruker1**

Dette bør gå bra (med mindre du nå sitter og jobber om natten).

9. Logg inn domenet fra klientmaskinen med brukeren **testbruker2**.

Du skal da få en melding om at du ikke kan logge deg på.

Hvorfor? _____

10. Bytt til tjenermaskinen og modifier brukeren **testbruker2** slik at du likevel får logget inn. Test at det virker.

11. Logg ut fra klientmaskinen

Oppgave e: Endre navn på brukerkontoer

Det er også mulig å endre navn på en brukerkonto i *Active Directory*.

1. Vær pålogget tjenermaskinen med brukerkontoen **Administrator**.
2. Bruk *Active Directory Users and Computers*.
3. Høyreklikk brukerkontoen **Test Domenebruker2**, velg **Rename** og endre feltet *Name* til **Test Domenebruker3**
4. Du får da automatisk opp vinduet *Rename User* for å endre andre opplysninger.
 - Bruk dette vinduet til å endre etternavn og visningsnavn (*Display name*) tilsvarende.
 - Endre også brukernavnet (*User logon name*) til **testbruker3**.
 - Pass også på å endre logon navnet for tidligere Windows versjoner (*pre-Windows 2000*).
5. Test innlogging fra klientmaskinen med den endrede påloggingsnavnet (**testbruker3**), og sjekk at det fungerer som den skal.
6. Logg ut fra fra klientmaskinen

Oppgave f: Passivisere og aktivere brukerkontoer

Administrator kan sperre tilgangen til en brukerkonto ved å *deaktivere* den:

1. Bruk *Active Directory Users and Computers* på tjenermaskinen.
2. Finn brukeren *Test Domenebruker3* (**testbruker3**).
3. Høyreklikk brukeren og velg **Disable Account**.
4. Vent 10-15 sekunder og forsøk å logge på domenet fra klientmaskinen din som **testbruker3**.
5. Bytt til tjenermaskinen igjen og *aktiver* (*Enable*) **testbruker3** igjen.
6. Sjekk at du kan logge på som **testbruker3** fra klientmaskinen din nå (etter noen sekunder).
7. Logg ut fra fra klientmaskinen

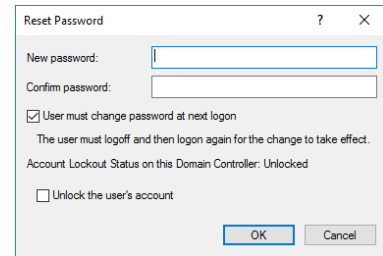
Oppgave g: Bytte passord på en brukerkonto

Brukere har en lei tendens til å glemme passordet sitt. Av sikkerhetsmessige grunner er det ikke mulig for en administrator å se hvilket passord en bruker har. I slike tilfeller er derfor løsningen å gi brukerkontoen et nytt passord:

1. Bruk *Active Directory Users and Computers* på tjenermaskinen
2. Finn fram til brukeren **Test Domenebruker 1** (**testbruker1** under *OU_1*).

3. Høyreklikk brukeren og velg **Reset password...**
4. Gi brukeren det nye passordet: **xyz.123**

Obs! Det bør stå kryss i ruten *User must change password at next login*. Dette sørger for at bruker **må** velge et nytt passord som nettverksadministrator **ikke** kjenner.

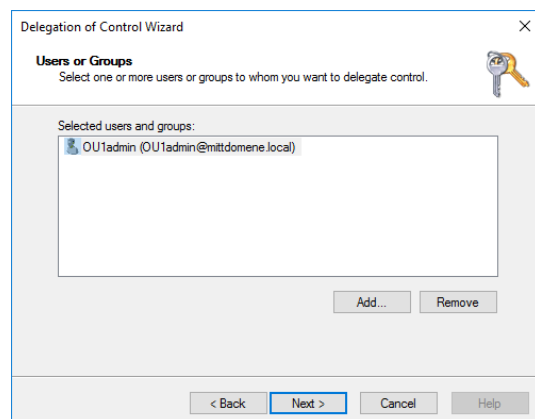


5. Logg inn på domenet fra klientmaskinen med brukerkontoen **Test Domenebruker1 (testbruker1)** og bruk det nye passordet.
Hva skjer under pålogging? _____
6. Gi brukeren et nytt passord som du husker og som tilfredsstillere kravene til passord i et Windows-domene. (Tidligere passord kan ikke brukes.)

Oppgave h: Delegere rettigheter til administrasjon av OU

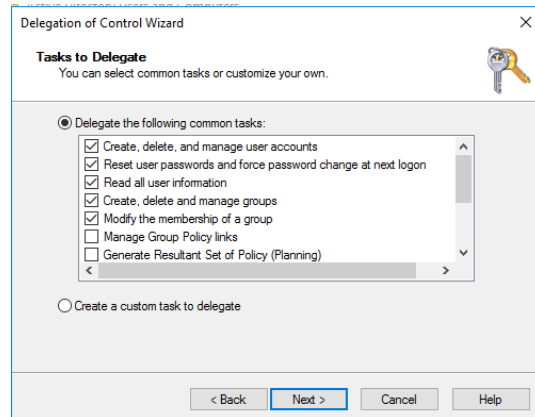
I denne oppgaven skal du først lage en ny brukerkonto som tilhører organisasjonsenheten **OU_1** i domenet. Deretter skal du *delegere* administrativt ansvar for denne OU'en til den nye brukerkontoen. På denne måten får brukeren administrative rettigheter som **bare** gjelder innen denne organisasjonsenheten. Til slutt skal du teste den nye administrative kontoen.

1. Vær pålogget tjenermaskinen med brukerkontoen **Administrator**.
2. Bruk *Active Directory Users and Computers*
3. Lag en ny domenekonto under OU_1 med disse egenskapene:
 - Gi kontoen logon-navnet **OU1admin**
 - Bruk passordet **Password.2019**
 - Bruker trenger ikke bytte passord ved innlogging.
 - Passord skal aldri utløpe.
4. Høyreklikk **OU_1**, og velg **Delegate Control**.
5. Nå starter veiviseren *Delegation of Control Wizard*.
6. Klikk **Add** og legg til den nye kontoen **OU1admin**.



7. Deleger følgende oppgaver til **OU1admin**:

- *Create, delete, and manage user accounts*
- *Reset user passwords and force password change at next logon*
- *Read all user information*
- *Create, delete, and manage groups*
- *Modify the membership of a group*



8. Lag en tilsvarende bruker **OU2Admin** som får delegert ansvar for de samme oppgavene på **OU_2**

Nå skal du teste den nye kontoen **OU2admin**.

9. Logg først ut fra tjenermaskinen og logg inn igjen med den nye kontoen **OU2admin**

10. Start **Server Manager**

11. Du må nå oppgi **OU2admin** og passord for å kjøre **Server Manager**.

12. Start *Active Directory Users and Computers*

13. Høyreklikk på **OU_1**

Hvorfor ser du ikke noen **New**-meny? _____

14. Forsøk å slette brukerkontoen **Test Domenebruker1** under **OU_1**.

Hvorfor går ikke dette? _____

15. Høyreklikk på **OU_2**

Hvilke valg har du under **New** menyen nå? _____

Hvorfor har du bare disse valgene? _____

16. Lag en ny domenebruker i **OU_2**. Velg opplysninger selv.

17. Sjekk at du får lov til å slette den nye brukeren i **OU_2** etter at den er laget

Slutt på øvingen