LAB-IT-PROSJEKTET – TEKNISKE LØSNINGER

IT-FORUM 2017

UTFORDRINGEN:

- Bruker trenger tilgang til lab-utstyr

- Bruker: «Jeg trenger tilgang til dette utstyret.»
- IT: «Hvem er du? Hva skal du ha tilgang til? Hvem har autorisert det?»

NÅSITUASJONEN

WINDOWS-PC KOBLET TIL INSTRUMENT

- Ikke-driftet PC:
  - Ansvarlige?
  - Sikret?
  - Patchet?
  - Bak brannmur?
  - Mange spørsmålstegn og svakheter...

- Klientdriftet PC
  - Windows 7 klientdrift av IT-avdelingen
  - automatisk oppdatering av OS og software
  - lokal administrator via «install» konto
  - mulighet for autologin av felles labbruker

En stadig pågående prosess for å få flere maskiner klientdriftet...

«INSTALL» KONTOEN

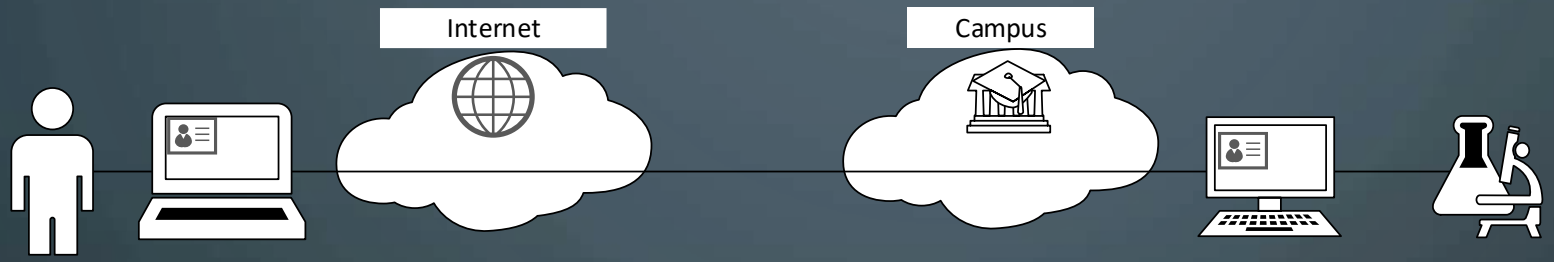
- Ulemper:
  - Kan ikke brukes til å koble til maskinen via RDP.
  - Passordet kan bli delt internt i en gruppe, ikke mulig å vite hvem som gjorde hva på maskinen.
  - Kan oppleves som tungvint.
- Fordeler:
  - Passord på avveie kan ikke brukes til noe over nettverket. Krever fysisk tilgang.
  - Enkelt å delegere admintilgang til labmaskinen.
  - Etablert praksis for UiB Windows klientdrift.

FELLES LAB-BRUKER (UIB\LAB)

- Ulemper:
  - Kan ikke brukes til å koble til maskinen via RDP.
  - En felles domenebruker som brukes på mange maskiner.
    - Ingen tilgang til lagring på nettverk
    - Kan kun logge på labmaskiner
    - Kun lokal profil
- Fordeler:
  - Passord på avveie kan ikke brukes til noe over nettverket. Krever fysisk tilgang.
  - Autologin
  - Ingen skjermsparer
  - Praktisk for å f.eks. overvåke prosesser

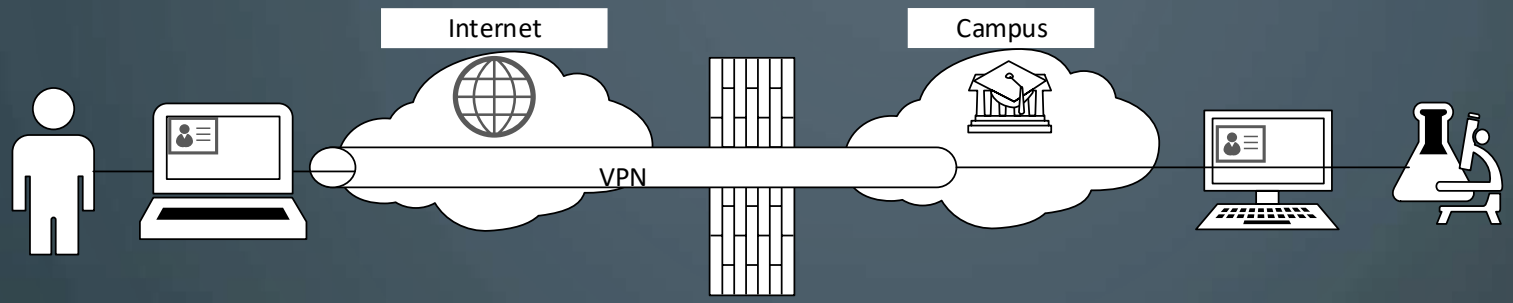
TILLEGGSUTFORDRINGEN:

- Bruker trenger tilgang til lab-utstyr fra privat utstyr utenfor campus



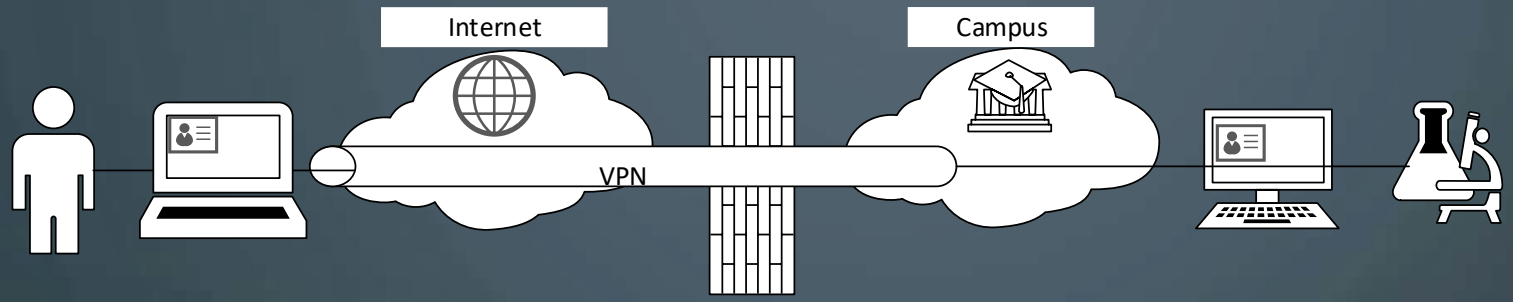
- Bruker: «Jeg trenger tilgang til dette utstyret hjemmefra.»
- IT: «Hvem er du? Har du en sikker nettverkstilkobling? Hva skal du ha tilgang til? Hvilken sesjon skal du ha tilgang til? Hvem har autorisert det?»

DAGENS LØSNING:



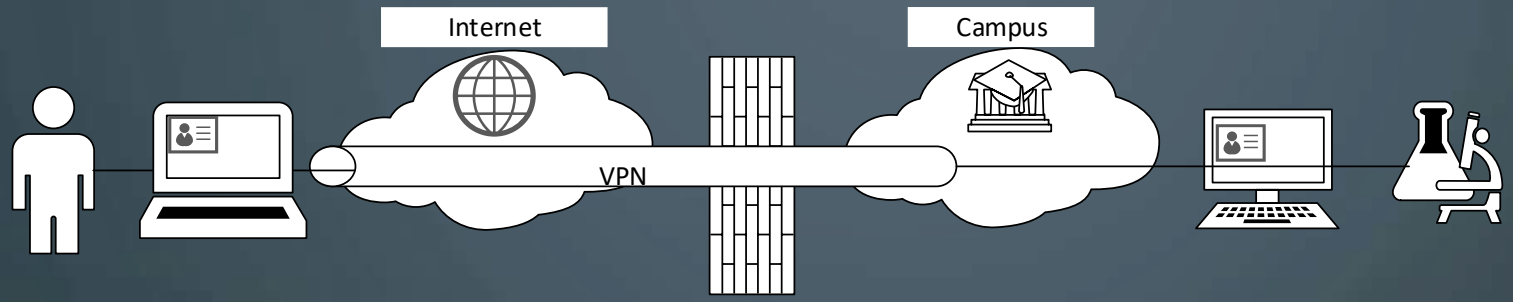
- Bruker kobler til lab-pc med Remote Desktop via VPN oppkobling
- Autentisering av bruker mot AD domene
- Sikring av forbindelsen med RDP-protokoll over VPN
- Tilgang til lab-pc/instrument via lokal gruppe på PC (Remote Desktop Users)

UTFORDRINGER VED DAGENS LØSNING:



- Bruker kan kun koble til sin egen sesjon
- Det er et uttrykt ønske om å koble til en kjørende sesjon med fellesbruker
- Krav om VPN-oppkobling er et ekstra hinder for mange brukere
- Tilgangskontroll krever mye micro-management

UTFORDRINGER VED DAGENS LØSNING:



- Blir det for tungvint å få tilgang til instrumentet kan brukere finne på lure snarveier som f.eks. TeamViewer, eller 4G-rutere!
  - Potensielle sikkerhetsrisikoer
  - Utenfor IT-avdelingens kontroll
  - Ingen mulighet for å vite hvem som gjorde hva på hvilken pc, dersom det er åpnet for at eksterne har full desktoptilgang via TeamViewer el.l.

VEIEN VIDERE?

- Windows 10
  - Vi gjør ikke mer utvikling eller tilpasning på Windows 7, alt videre arbeid har fokus på Windows 10 klientmaskiner i domene og med basisdrift i bunn.
- Remote Desktop Services
  - Brukes for å publisere RemoteApp oppkoblinger til eksisterende fysiske maskiner.
  - Trenger ikke VPN.
  - Bruker går til en webside og ser labmaskiner de er gitt tilgang til.

WINDOWS 10

- Windows 10 har vært i utvidet pilot en god stund og produksjonssettes om kort tid.
- Stabil og sikker plattform.
- Ny håndtering av lokal administratortilgang og Remote Desktop
- Mulighet for LTSB (Long Term Servicing Branch)

FORBEDRINGER I WINDOWS 10

- Maskinobjektet i Active Directory har en attributt «ManagedBy»
- Verdien her kan settes enten til en gruppe eller en bruker i AD

ADMINISTRATORTILGANG

- Dersom maskinen er med i en spesiell gruppe vil bruker/gruppe definert her bli medlem i Administrators gruppen på PC
- De som da har administratortilgang kan elevere seg til administrator etter behov ved hjelp av UAC

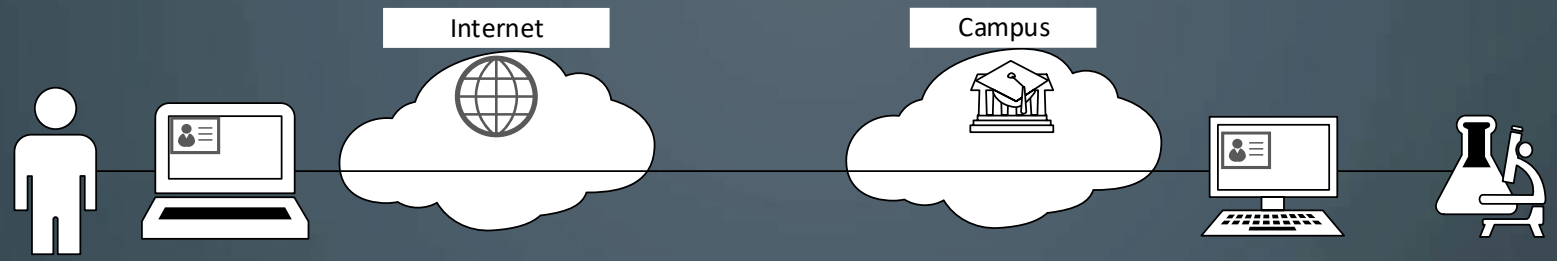
REMOTE DESKTOP TILGANG

- Som en standard er medlemmer definert her med i lokal gruppe Remote Desktop Users.
- (Medlemmer i Administrators gruppen har allerede RDP tilgang)

WINDOWS 10 LTSB

- Vanlige Windows 10 installasjoner får funksjonsoppdateringer 2 ganger i året.
- LTSB er en nedstrippet versjon av Windows 10 uten mange konsumerorienterte funksjoner som bl.a. Windows Store
- LTSB har en levetid på 10 år og nye utgaver forventes hvert 3. år
- I levetiden får LTSB kun sikkerhetsoppdateringer og ikke nye funksjoner

TILBAKE TIL TILLEGGSUTFORDRINGEN:



- Kjernen i problemet er å gi autentiserte brukere fjerntilgang til lab-pc som gjerne kjører en sesjon med felles pålogget bruker
- TeamViewer ble testet, men krevde mye micro-management og ekstern autentisering, registrering av epost i TeamViewer.
- Vi trengte en tjeneste som kunne gjøre den nødvendige magien for å autentisere en bruker og gi tilgang til en sesjon som kjører med andre

REMOTE DESKTOP SERVICES

- Bygger på RDP, kjerneteknologi innebygget i Windows siden NT 4.0
- Kjent som Remote Desktop Services siden Windows Server 2008 R2
- Har flere roller, de mest relevante for vårt formål er:
  - Remote Desktop Session Host
  - Remote Desktop Web Access

PROOF OF CONCEPT!

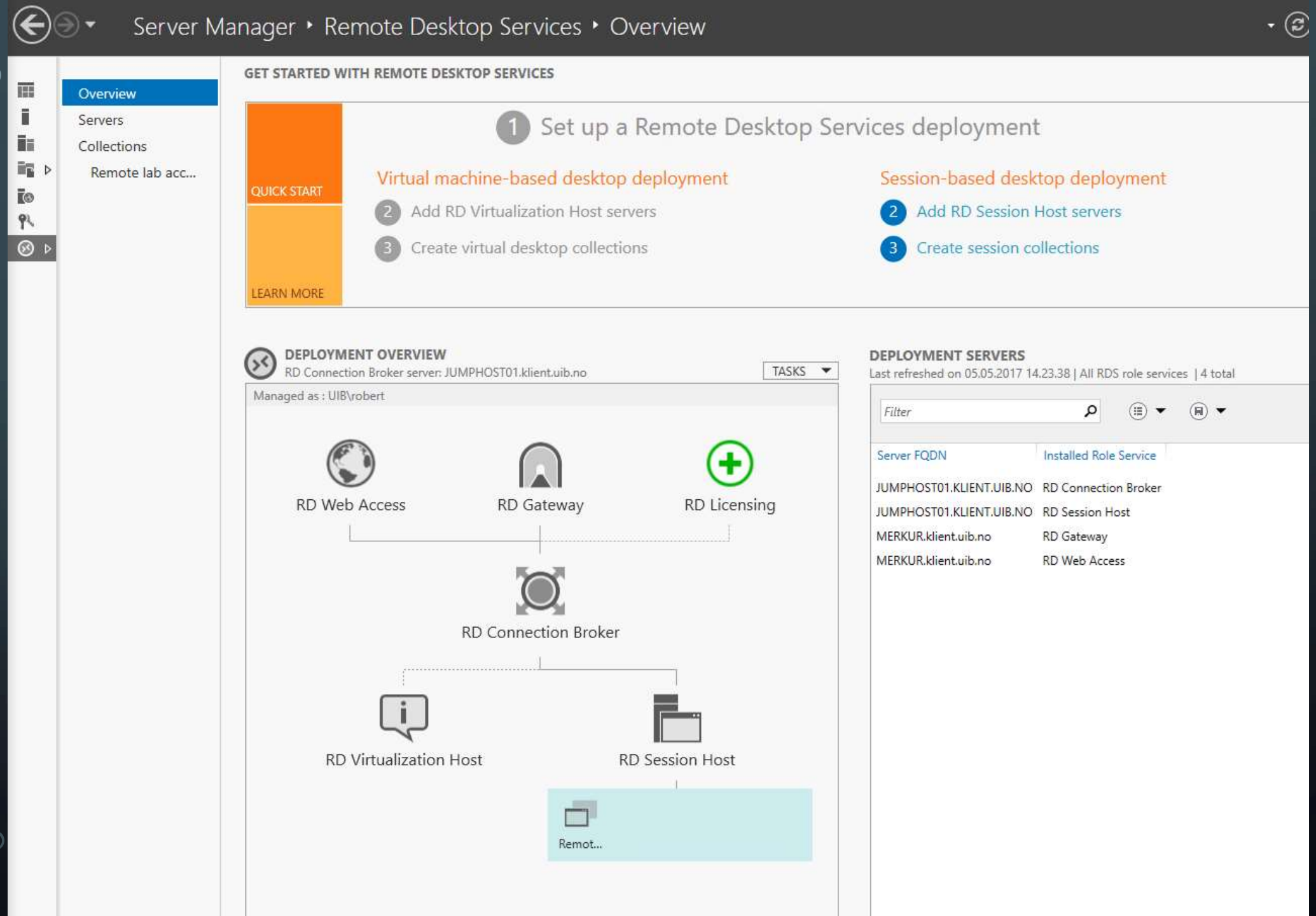
- Arbeidet som er gjort hittil er bare en POOC, og det gjenstår mye før det kan settes i produksjon.

RD WEB ACCESS

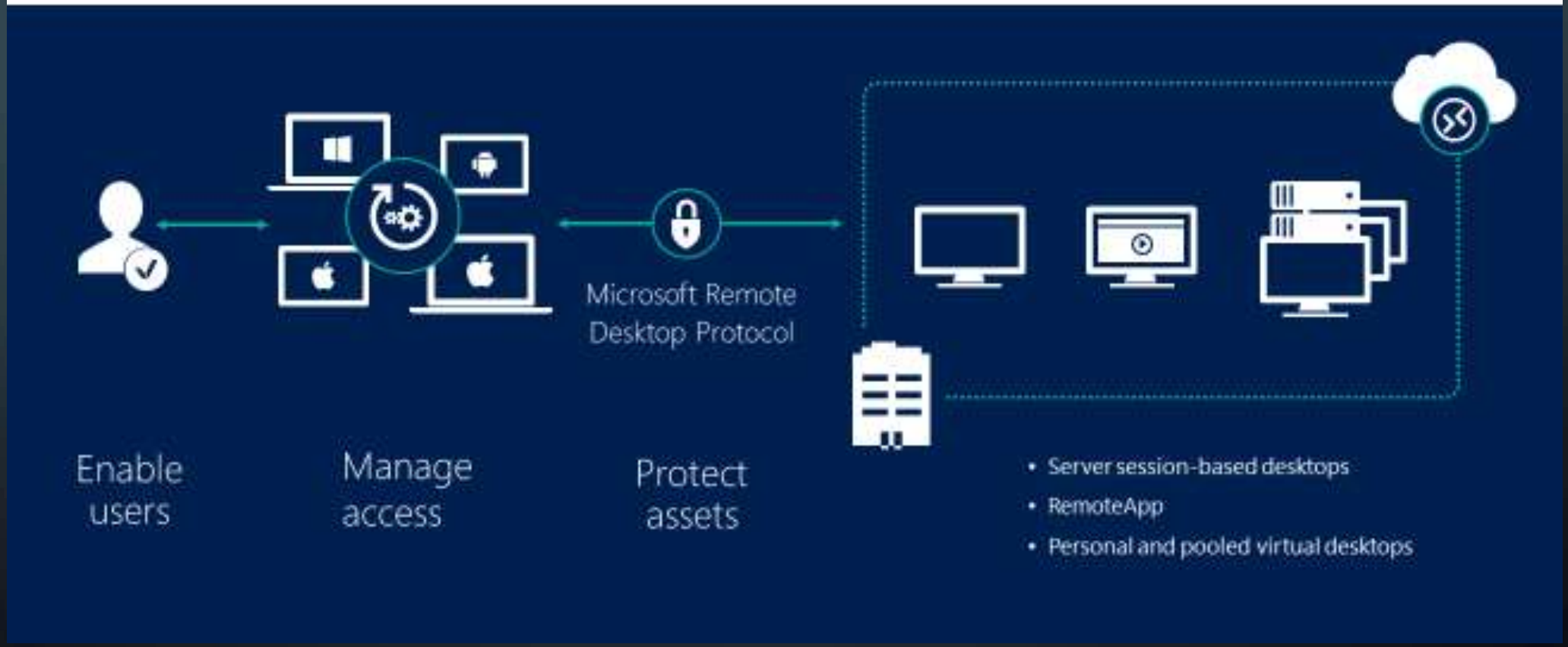
- Webserver som gir et web-grensesnitt til ressurser som bruker er gitt tilgang til.

RD SESSION HOST

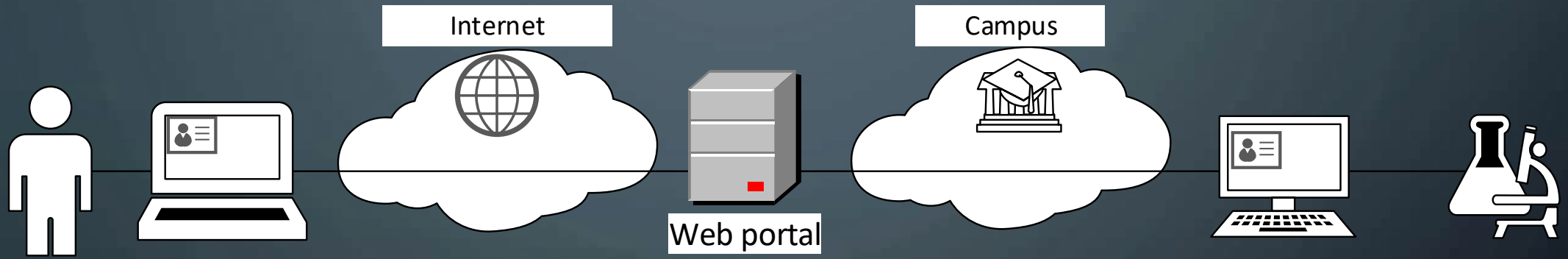
- Server med programmer publisert som RemoteApp
- I denne løsningen er programmet som publiseres, Remote Desktop med innstillinger for å koble til en spesifikk maskin med en spesifikk bruker.
- Disse RDP-sesjonene vises i webportalen RD Web Access
- Programmer defineres i Collections
- Grupper i Active Directory gir tilgang til Collections
- Lett å delegere administrasjonen av tilgang til lab-utstyr etter initielt oppsett


Server Manager ‣ Remote Desktop Services ‣ Overview
Overview
Servers
Collections
Remote lab acc...
GET STARTED WITH REMOTE DESKTOP SERVICES
QUICK START
LEARN MORE
1 Set up a Remote Desktop Services deployment
Virtual machine-based desktop deployment
2 Add RD Virtualization Host servers
3 Create virtual desktop collections
Session-based desktop deployment
2 Add RD Session Host servers
3 Create session collections
DEPLOYMENT OVERVIEW
RD Connection Broker server: JUMPHOST01.klient.uib.no
TASKS
Managed as : UIB\robert
RD Web Access
RD Gateway
RD Licensing
RD Connection Broker
RD Virtualization Host
RD Session Host
Remot...
DEPLOYMENT SERVERS
Last refreshed on 05.05.2017 14.23.38 | All RDS role services | 4 total
Filter
Server FQDN
Installed Role Service
JUMPHOST01.KLIENT.UIB.NO
RD Connection Broker
JUMPHOST01.KLIENT.UIB.NO
RD Session Host
MERKUR.klient.uib.no
RD Gateway
MERKUR.klient.uib.no
RD Web Access

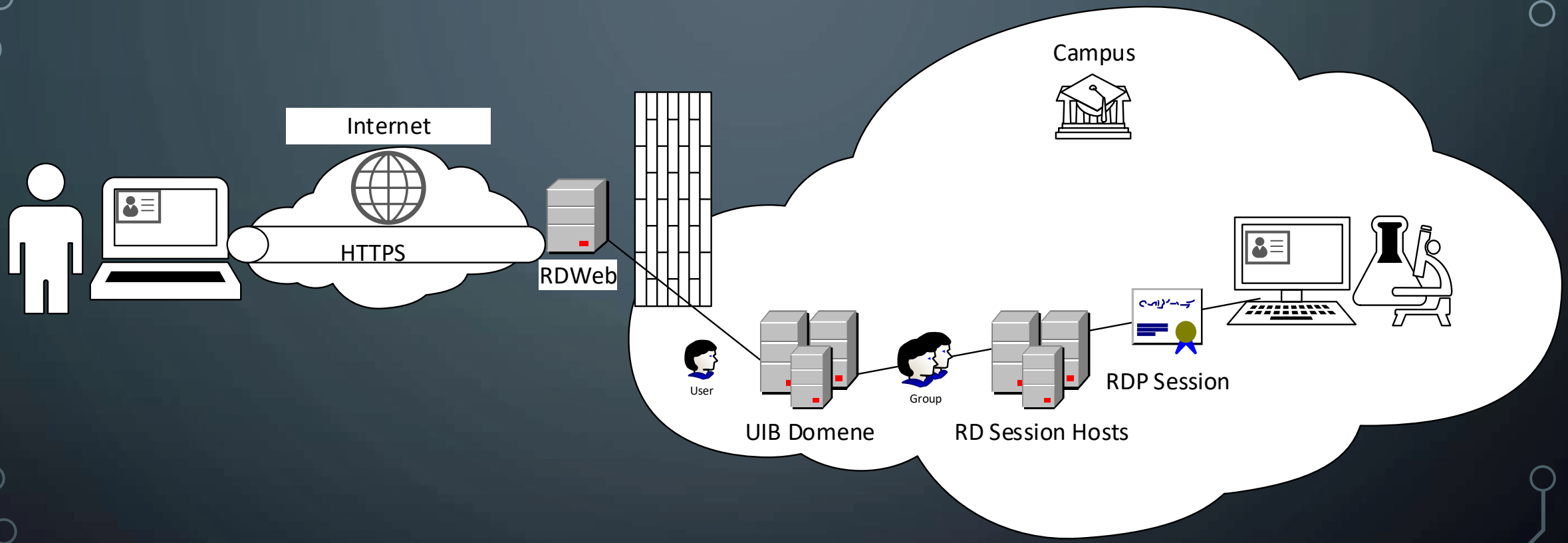
Remote Desktop Services

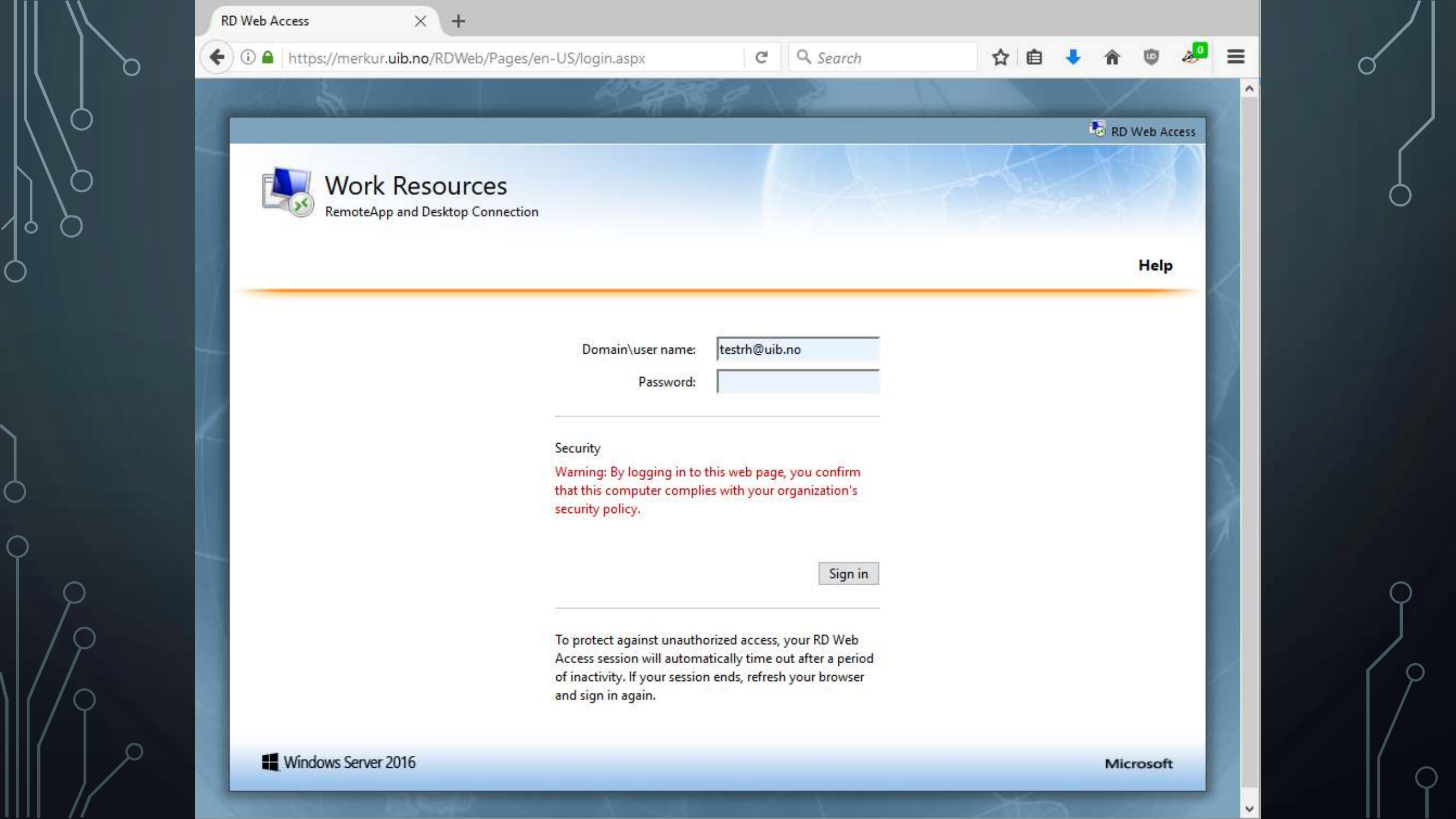


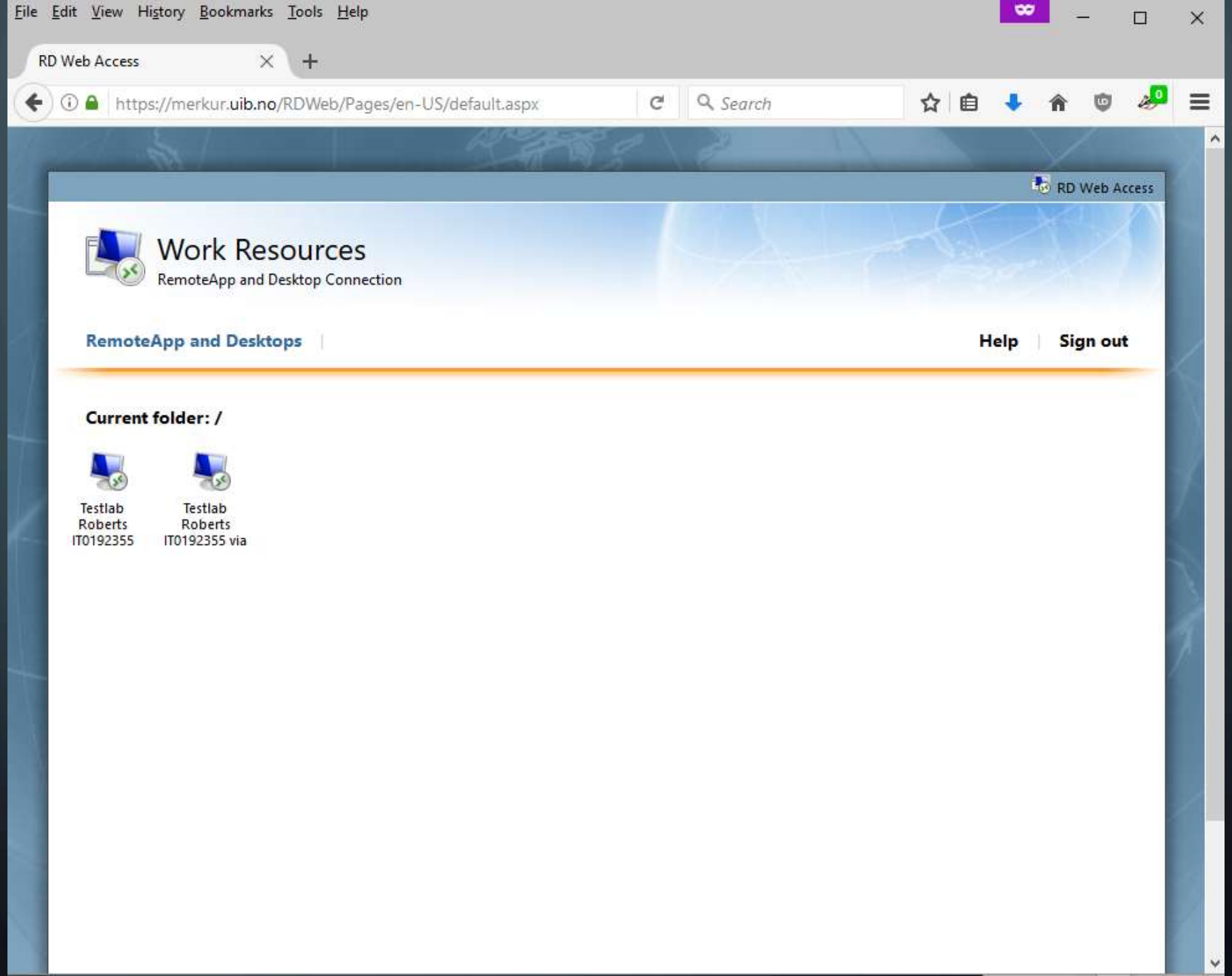
BRUKERS OPPLEVELSE:

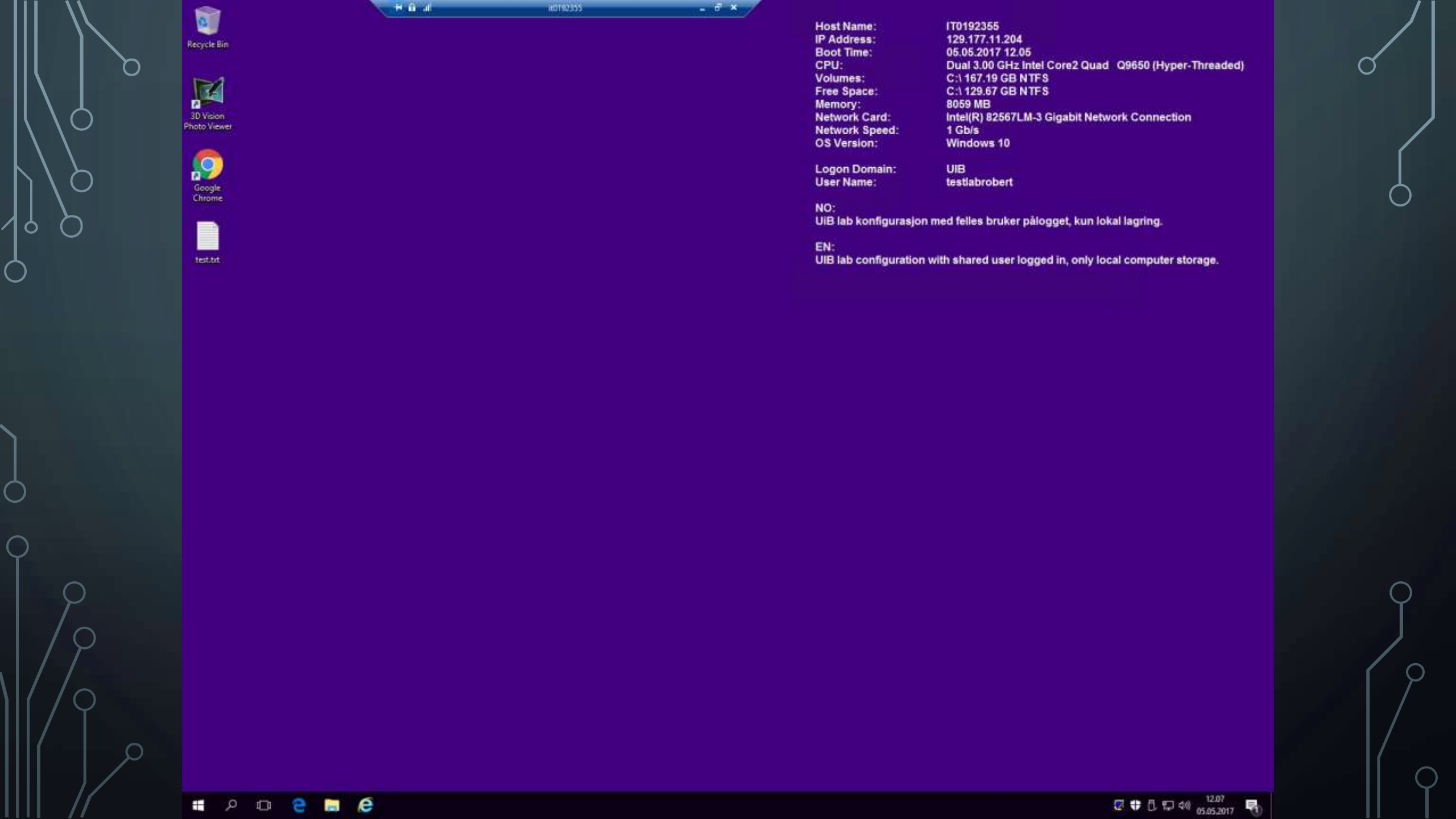


BAK KULISSENE:

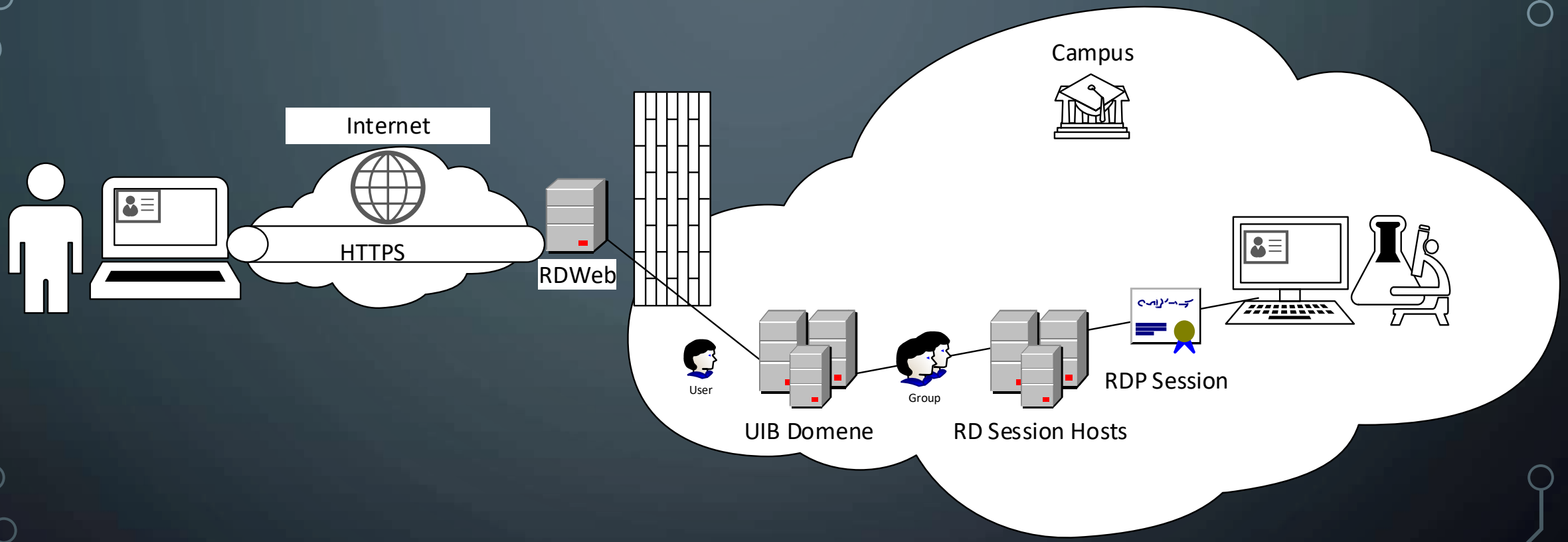



RD Web Access
https://merkur.uib.no/RDWeb/Pages/en-US/login.aspx
Search
RD Web Access
Work Resources
RemoteApp and Desktop Connection
Help
Domain\user name:
testrh@uib.no
Password:
Security
Warning: By logging in to this web page, you confirm that this computer complies with your organization's security policy.
Sign in
To protect against unauthorized access, your RD Web Access session will automatically time out after a period of inactivity. If your session ends, refresh your browser and sign in again.
Windows Server 2016
Microsoft


File Edit View History Bookmarks Tools Help
RD Web Access
https://merkur.uib.no/RDWeb/Pages/en-US/default.aspx
Search
RD Web Access
Work Resources
RemoteApp and Desktop Connection
RemoteApp and Desktops
Help
Sign out
Current folder: /
Testlab Roberts IT0192355
Testlab Roberts IT0192355 via


Recycle Bin
3D Vision Photo Viewer
Google Chrome
test.txt
IT0192355
Host Name: IT0192355
IP Address: 129.177.11.204
Boot Time: 05.05.2017 12.05
CPU: Dual 3.00 GHz Intel Core2 Quad Q9650 (Hyper-Threaded)
Volumes: C:\ 167.19 GB NTFS
Free Space: C:\ 129.67 GB NTFS
Memory: 8059 MB
Network Card: Intel(R) 82567LM-3 Gigabit Network Connection
Network Speed: 1 Gb/s
OS Version: Windows 10
Logon Domain: UIB
User Name: testlabrobert
NO:
UiB lab konfigurasjon med felles bruker pålogget, kun lokal lagring.
EN:
UIB lab configuration with shared user logged in, only local computer storage.
12.07
05.05.2017

SPØRSMÅL?


Internet
HTTPS
RDWeb
Campus
User
Group
UIB Domene
RD Session Hosts
RDP Session

REFERANSER:

- https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/welcome-to-rds

- https://ryanmangansitblog.com/2013/03/27/deploying-remote-desktop-gateway-rds-2012/