Bacheloroppgave

NTNU
Norges teknisk-naturvitenskapelige universitet
Fakultet for informasjonsteknologi og elektroteknikk
Institutt for datateknologi og informatikk

Annika Luu
Solveig Longva

Sikkerhet i virtualiseringstjenester

Bacheloroppgave i informatikk, drift av datasystemer

Mai 2021

NTNU
Kunnskap for en bedre verden

sopra steria

Annika Luu
Solveig Longva

Sikkerhet i virtualiseringstjenester

Bacheloroppgave i informatikk, drift av datasystemer
Mai 2021

Norges teknisk-naturvitenskapelige universitet
Fakultet for informasjonsteknologi og elektroteknikk
Institutt for datateknologi og informatikk

NTNU

Kunnskap for en bedre verden

Abstract

Many companies are moving from an on-premise, physical computer infrastructure to a virtual solution to ensure that their employees have the option to work from home and when traveling for business. A virtual IT infrastructure can also provide improved security when it comes to keeping confidential data safe and preventing data loss. There are numerous companies offering virtualization services currently, and it can be hard to determine which is right for one's purpose. In this thesis, we have chosen two of the most common virtualization services among businesses, VMware vSphere and Windows Virtual Desktop, and set up a test lab in order to analyze the different security features they offer. We have also chosen to look into user-friendliness and pricing, to aid the client in making the decision of which service they wish to use. The result of this analysis is that VMware is the leader when it comes to security due to their advanced network security features, while Windows Virtual Desktop is the more user-friendly option. The Windows Virtual Desktop/Azure combination is more expensive than VMware vSphere but offers more features for that price.

Overordnet innholdsfortegnelse

Bacheloroppgave, Sluttrapport

Annika Luu
Solveig Longva

Sluttrapport

Sikkerhet i virtualiseringstjenester

Versjon 1.0

Mai 2021

NTNU
Kunnskap for en bedre verden

sopra steria

Revisjonshistorie

Dato	Versjon	Beskrivelse	Forfattere
07.05.2021	0.1	Opprettelse av sluttrapport.	Annika Luu og Solveig Longva
20.05.2021	1.0	Ferdigstille sluttrapporten.	Annika Luu og Solveig Longva

Innholdsfortegnelse, sluttrapport

1.1. Forord

Denne rapporten er en sluttrapport som skrives i forbindelse med emnet IDRI3001 - Bacheloroppgave i drift av datasystemer. Prosjektgruppen består av Annika Luu og Solveig Longva. Prosjektet skal utarbeides i samarbeid med Sopra Steria hvor selskapet og NTNU AIT stiller som veileder. Dette dokumentet forklarer driftsaspektet ved prosjektoppgaven og er siste del av bacheloroppgaven som leveres ved slutten av vårsemesteret 2021.

Denne oppgaven er forankret i en reell problemstilling fra fagområdet informatikk, drift av datasystemer, *sikkerhet i virtualiseringstjenester*. Studentene har gjennom dette prosjektet tilegnet seg kunnskaper om infrastrukturen og sikkerhetsfunksjoner innen disse virtualiseringstjenestene og oppnådd egen utvikling i selvstendig prosjektarbeid.

1.1.1. Takk

Prosjektgruppen ønsker å gi stor takk til alle som har hjulpet oss gjennom utførelsen av prosjektet og kommet med gode tilbakemeldinger og støtte.

- **Vegard Widên og Kristian Næss**, våre veiledere fra Sopra Steria. Tusen takk for gode tilbakemeldinger og disponering av Microsoft Azure.
- **Stein Meisingseth**, vår veileder fra NTNU AIT samt faglærer i Drift av datasystemer. Tusen takk for god veiledning og anbefalinger for prosjektet. Ikke minst ønsker vi også å takke deg for tre år med minneverdig skolegang i drift av datasystemer.
- **Jostein Lund**, faglærer av drift av datasystemer. Tusen takk for tre år med minneverdig skolegang.

- **Ludvig Pedersen og Emil Antoni Brasø**, infrastruktur ingeniør fra Sopra Steria. Tusen takk for teknisk innsikt i Windows Virtual Desktop og Azure-miljøet.
- **Aleksander Tandberg,** avdelingsingeniør NTNU. Tusen takk for IT-støtte og disponering av VMware.
- **Marthe Hagen og Jørgen Longva**, tusen takk for korrektur av rapporten og støtte.
- **Khuong Luu og Fonne Yep**, tusen takk for motiverende ord og støtte.

Kontaktinformasjon

Tlf: 481 30 105

Epost: solvlon@stud.ntnu.no

Solveig Longva

Tlf: 413 531 40

Epost: annika.luu@ntnu.no

Annika Luu

1.2. Oppbygging av rapporten

Sluttrapporten er sammensatt av tre rapporter; forstudierapport, designrapport og driftsrapport. Første del av sluttrapporten vil gi en innføring i begrep og forkortelser som brukes i rapporten og en beskrivelse av oppgaven, slik at leseren får oversikt over hva de tre rapportene tar utgangspunkt i. Det er også vedlagt et GANTT-diagram som gir oversikt over fremgangen i prosjektet.

1.3. Definisjoner og forkortelser

Ord	Forklaring
AADDS	Azure Active Directory Domain Services
ARM	Azure Resource Manager
CAL	Client Access License
CSPM	Cloud Security Posture Management
CWPP	Cloud Workload Protection Platform
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
EDR	Endpoint Detection and Response
GPO	Group Policy Object
HA	High Availability
IaaS	Infrastructure as a Service
MFA	Multi-factor authentication
MS Azure	Tjeneste som tilbyr skybaserte datatjenester
NAT	Network Address Translation
RDP	Remote Desktop Protocol
RDS	Remote Desktop Services
SIEM	Security information and event management
SOAR	Security orchestration automated response
SOC	Security Operation Center

SSL	Secure Sockets Layer
SQL	Structured Query Language
TCO	Total cost of ownership
TCP	Transmission Control Protocol
VM	Virtuell maskin
VMware	Et selskap som tilbyr skybaserte datatjenester, programvare og tjenester for virtualisering.
VPN	Virtual Private Network
vSphere	Miljøtjeneste for VMware
WVD	Windows Virtual Desktop
XDR	Extended detection and response

1.4. Oppgavebeskrivelse

1.4.1. Case-beskrivelse

LongLuu er en bedrift med 100 ansatte. De ønsker å implementere enten WVD eller VMware vSphere på grunn av COVID-19-situasjonen. De ønsker at deres ansatte kan jobbe hjemmefra og prioriterer høyere sikkerhet i løsningen de skal velge. De benytter seg av et Windows-basert miljø. Pr. dagens dato benytter de ikke en virtualiseringstjeneste. Prosjektgruppen skal sammenligne de ovennevnte og komme med den optimale løsningen for LongLuu ut i fra hva som møter deres krav til sikkerhet, i tillegg til brukervennlighet og økonomiske faktorer. Bedriften har hørt mye om de ulike tjenestene men ingenting om sikkerhetsnivået. Begge tjenestene påstår å være sikre, men hva vil dette si? Er de så sikre som de påstår?

1.4.2. Oppgave

Prosjektgruppen skal foreta en analyse og sammenligning av Windows Virtual Desktop og VMware vSphere med fokus på sikkerhet, brukervennlighet og pris, og presentere resultatene for bedriften.

1.5. Hvordan oppgaven ble løst

Oppgaven ble løst ved hjelp av testlab-er som ble satt opp i Azure og VMware vSphere, i tillegg til demolab-er som tilbys gratis fra VMware. Prosjektgruppen henter mye informasjon direkte fra Microsoft og VMwares nettside og kan konkludere at disse er pålitelige for denne bacheloroppgaven. Vi har benyttet dette for å støtte opp resultater som vi selv har observert. Vi har også hatt jevnlig dialog med veiledere fra NTNU AIT og Sopra Steria for å få tilbakemelding underveis, slik at vi får kvalitetssikret stoffet før prosjektgruppen går videre til neste del av prosjektet.

1.6. Gjennomføring av prosjektet

Prosjektgruppen oppretter en prosjektplan for planlegging og motivasjon. Prosjektplanen starter med innsamling av nødvendige ressurser og kunnskap for å utføre prosjektet. Prosjektgruppen utarbeider rapporter underveis for å holde veilederne oppdatert. Det føres også timelister, minimum 500 +-5% for begge prosjektmedlemmer slik at prosjektgruppen overholder prosjektplanen. Prosjektet ferdigstilles den 20. mai 2021.

1.6.1. Problemer underveis

Oppsettet av Windows Virtual Desktop og VMware gikk bra etter at vi har fått tilgang til nødvendige ressurser. Problemet var at prosjektgruppen manglet tilgangsrettigheter for oppretting av Windows Virtual Desktop ettersom at vi ikke kunne koble til tenant i Azure AD. Dette ble løst etter at prosjektgruppen fikk de rette tilgangsrettighetene og opprettet WVD med AADDS. Videre hadde vi problemer med nettverkstilgang til VMware, noe som ble løst etter kommunikasjon med ansvarlig for disponeringen av virtualiseringstjenesten.

1.6.2. Måloppnåelse

Følgende mål ble definert ved start av prosjektet:

Effektmål

- Øke sikkerheten ved implementering av virtuelle tjenester.
- Trygg tilkobling ved hjemmekontor.
- Skalerbar virtualiseringsløsning.
- En kost-/nytteeffektiv løsning
- Et varslingssystem som kan oppdage innbrudd gjennom overvåkning av loggdata i systemet.

- Trusselbeskyttelse
- En logganalyse som loggfører alle uvanlige aktiviteter.

Resultatmål

- En analyse av sikkerhetsfunksjoner og kostnader i Windows Virtual Desktop og VMware vSphere.
- Prosjektet skal ferdigstilles 20. mai 2021, resultatet skal presenteres for veilederen fra NTNU AIT og Sopra Steria 27. mai 2021.
- Prosjektgruppen får en forståelse av kundenes behov.

Prosessmål

- Øke kompetansen innenfor de fagfeltene som utforskes i prosjektet.
- Øke kompetansen for samarbeid og kommunikasjon

I denne rapporten oppdager vi at både Windows Virtual Desktop og VMware, ved hjelp av deres sikkerhetsfunksjoner, egner seg til å oppnå effektmålene. De er begge skalerbare virtualiseringstjenester som støtter en trygg tilkobling ved hjemmekontor og kan øke sikkerheten i LongLuu ved implementering av en av disse virtualiseringstjenestene. Å gå fra on-premise-løsning til en løsning basert på virtualisering vil gi en kost-/nytteeffektiv løsning hvor flere ansatte kan benytte seg av de samme ressursene og minker kostnader for å opprettholde hardware i bedriften. Disse virtualiseringstjenestene har funksjoner som kan oppdage innbrudd gjennom overvåkning av loggdata i systemet og loggfører uvanlige aktiviteter. På denne måten kan de beskytte infrastrukturen mot sikkerhetstrusler. Begge tjenestene kan være til nytte for bedriften og kan tilføre denne nytten på ulike måter. De er fremdeles ulike og gruppen vil sammenligne dem i sammenligningskapittelet i driftsrapporten.

Ut i fra resultatet og prosessen underveis i dette prosjektet konkluderer gruppen med at alle målene er oppnådd i en tilfredsstillende grad.

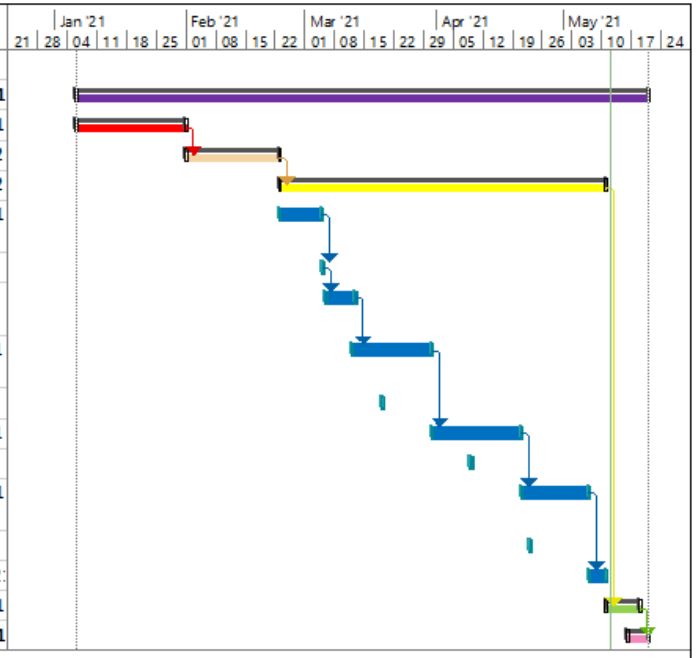
1.7. MS Project

Ved bruk av Microsoft Project utarbeides en prosjektplan som skal oppdateres jevnlig. Hensikten er å lede dem mot prosjektets mål, definert i forstudierapporten, og skal virke motiverende og gi oversikt for alle interessenter i prosjektet.

1.7.1. GANTT-diagram

Et GANTT-diagram er et søylediagram som illustrerer prosjektprosess over tid. GANTT-diagrammet skal oppdateres underveis og spiller en viktig rolle for planlegging av prosjektet ved å definere datoer for start- og sluttidspunkt av oppgavene som gjennomføres i prosjekt. Se vedlegg (1) for fullversjonen av GANTT-diagrammet.

ID	Task Mode	Task Name	Duration	Start	Finish
1					
2		**Prosjekt**	**97 days**	**Wed 06.01.2**	**Thu 20.05.21**
3		**Forstudie**	**19 days**	**Wed 06.01.2**	**Sun 31.01.21**
10		**Designrapport**	**16 days**	**Mon 01.02.2**	**Mon 22.02.2**
16		**Driftsrapport**	**55 days**	**Tue 23.02.21**	**Mon 10.05.2**
17		Innhenting av nødvendige ressurser	8 days	Tue 23.02.21	Thu 04.03.21
18		Møte 5	30 mins	Fri 05.03.21	Fri 05.03.21
19		Oppsett av WVD og VMware	6 days	Sat 06.03.21	Fri 12.03.21
20		Oppsett av sikkerhetsfunksjoner	13 days	Fri 12.03.21	Tue 30.03.21
21		Møte 6	30 mins	Fri 19.03.21	Fri 19.03.21
22		Analyse av systemene	15 days	Wed 31.03.2	Tue 20.04.21
23		Møte 7	30 mins	Fri 09.04.21	Fri 09.04.21
24		Gjennomføring og rapportskriving	12 days	Wed 21.04.21	Thu 06.05.21
25		Møte 8	30 mins	Fri 23.04.21	Fri 23.04.21
26		Avslutning	2 days	Fri 07.05.21	Mon 10.05.2
27		**Sluttrapport**	**6 days**	**Tue 11.05.21**	**Tue 18.05.21**
29		**Presentasjon**	**5 days**	**Sun 16.05.21**	**Thu 20.05.21**



Project: Bachelor_finalVersion
Date: Wed 12.05.21

Task
Split
Milestone
Summary
Project Summary
Inactive Task
Inactive Milestone
Inactive Summary
Manual Task
Duration-only
Manual Summary Rollup
Manual Summary
Start-only
Finish-only
External Tasks
External Milestone
Deadline
Progress
Manual Progress

Page 1

Figur 1 - GANTT diagram

Bacheloroppgave, Forstudierapport

Annika Luu
Solveig Longva

Forstudierapport

Sikkerhet i virtualiseringstjenester

Versjon 1.0

Januar 2021

NTNU
Kunnskap for en bedre verden

sopra steria

Innholdsfortegnelse, forstudierapport

Revisjonshistorie

Dato	Versjon	Beskrivelse	Forfattere
27.01.2021	0.1	Opprettelse av forstudierapport.	Annika Luu og Solveig Longva
04.02.2021	0.2	Endring på dokumentet basert på tilbakemelding fra veilederen.	Annika Luu og Solveig Longva
29.04.2021	0.3	Fjerne Citrix fra prosjektet.	Annika Luu og Solveig Longva
13.05.2021	1.0	Formatering.	Annika Luu og Solveig Longva

1. Introduksjon

Hensikten med denne forstudierapporten er å gi et overblikk over hva prosjektet innebærer. Den skal beskrive de ulike aspektene ved prosjektet og gi oversikt over hva planen er og hvilke målsetninger prosjektet omfatter. Den tar for seg en risikoanalyse med potensielle risikofaktorer og mulige konsekvenser. Vi vil også ta for oss en kost/nytte-analyse der vi analyserer virtualiseringstjenestene basert på deres kostnader sammenlignet med sikkerhetsfunksjoner. Til slutt vil vi komme med våre anbefalinger til videre arbeid basert på dagens situasjon og ønsker.

Målet er å gi alle parter i prosjektet et inntrykk over hva som er involvert i prosjektet, men det er viktig å nevne at det kan oppstå endringer underveis i samråd med partene som er med i prosjektet.

2. Bakgrunn for prosjektet

Prosjektgruppen ønsker å gjøre rede for sikkerhetsnivået i Windows Virtual Desktop (WVD) målt opp mot den tilsvarende virtualiseringstjeneste, VMware, da det er brukt av mange bedrifter i dag og har vært i bruk lenge. WVD er en relativt ny virtualiseringstjeneste, og dersom bedrifter skal vurdere om de vil gå over til denne tjenesten vil det være viktig å vite hvilke fordeler eller ulemper det har i forhold til tjenesten de benytter i dag. Her er det flere faktorer som må tas med i beregningen, og sikkerhet er en viktig faktor blant disse.
LongLuu er en bedrift med 100 ansatte, som i dag ikke benytter en virtualiseringtjeneste for arbeidsstasjoner og servere. De ønsker å implementere en virtualiseringstjeneste slik at de ansatte kan jobbe hjemmefra og ha tilgang på intranett på jobbreise. Bedriften benytter seg av Windows til både klienter og tjenere. De ønsker en løsning som er mest mulig kost-/nytteeffektiv og som høy grad av sikkerhet i form av overvåking av systemet, varsling, håndtering og loggføring av hendelser, samt preventive tiltak som kan hindre sikkerhetsbrudd.

2.1. Beskrivelse av problemer og behov

Sikkerhet spiller en viktig rolle i en bedrifts systemer. For å beskytte bedriftens integritet og data i høyeste grad kan man benytte seg av tjenester som stadig oppdateres etter dagens trusselbilde og dermed sikre systemene. De fleste store aktører som tilbyr virtualiseringstjenester tilbyr programvare og tilleggstjenester som kan gjøre det virtuelle systemet tryggere. Når en ny virtualiseringstjeneste kommer på markedet vil det for mange bedrifter være interessant å vurdere om denne tjenesten kan være aktuell å gå over til. Det kan derimot være vanskelig å finne informasjon om tjenesten fordi den er nylig publisert og fordi det ikke finnes like mange brukererfaringer med tjenesten. Når det kommer til sikkerhetsaspektet kan det være vanskelig å bedømme dette, da man ikke har så mye mer å gå på enn hva leverandøren har å si om det. Det er derfor vi med dette prosjektet ønsker å granske sikkerhetsnivået i WVD sammenlignet med virtualiseringstjenester som er benyttet av mange bedrifter i dag. På denne måten kan man få et innblikk i sikkerhetsgraden og om det vil være lønnsomt og trygt å migrere til WVD eller en annen tjeneste.

2.2. Hvorfor behov for virtualisering

Som nevnt har vi i dette prosjektet besluttet å trekke inn VMware for å sammenligne WVD med virtualiseringstjenester som er mye brukt blant bedrifter i dag. Det virtuelle systemet er ofte administrert av en egen IT-avdeling og/eller av en ekstern supportbedrift, i tillegg til oppdateringer og forbedringer som leverandøren selv kommer med. Sikkerhet i systemet er noe som gjerne både IT-avdelingen og leverandøren har ansvar for, avhengig av hvilken trussel det dreier seg om. Dersom noe rammer selve systemet er det ofte leverandøren som har ansvar for å tette sikkerhetshullet, for eksempel et sikkerhetshull i tjenestens innloggingsfunksjon. Om det for eksempel oppstår et sikkerhetsbrudd hvor en ansatt får tilgang på filer som vedkommende ikke skulle ha tilgang på som følge av feil rettigheter i systemet så faller dette ansvaret gjerne på de IT-ansvarlige i bedriften. I dette tilfellet vil det være viktig at systemet er designet slik at det er lett for IT-avdelingen å administrere systemet slik at slike hendelser ikke inntreffer. At tjenesten er relativt lett å administrere er altså en viktig faktor når det kommer til sikkerhet.

VMware tilbyr tjenester som gir en oversikt over potensielle sikkerhetstrusler og verktøy som kan rette opp i disse truslene. VM-ene har tilgang til virtuelle enheter, men ikke direkte tilgang til maskinvare. De kan også kun kommunisere gjennom virtuelle switcher. VMware ESXi gir også rollebasert tilgang og benytter kraftige krypteringsteknikker når det kommer til klienter og tjenere.

3. Prosjektmål

Prosjektgruppen har formulert følgende mål med utgangspunkt i case-beskrivelsen fra bedriften LongLuu. Disse målene er styrbare og målbare slik at de skal virke veiledende for prosjektgruppen under utførelsen. Disse skal brukes til å vurdere resultatet i ettertid for å sikre at prosjektgruppen leverer det er som avtalt med bedriften.

3.1. Effektmål

- Øke sikkerheten ved implementering av virtuelle tjenester.
- Trygg tilkobling ved hjemmekontor.
- Skalerbar virtualiseringsløsning.
- En kost-/nytteeffektiv løsning.
- Et varslingssystem som kan oppdage innbrudd gjennom overvåkning av loggdata i systemet.
- Trusselbeskyttelse.
- En logganalyse som loggfører alle uvanlige aktiviteter.

3.2. Resultatmål

- En analyse av sikkerhetsfunksjoner og kostnader i Windows Virtual Desktop og VMware vSphere.
- Prosjektet skal ferdigstilles 20. Mai 2021, prosjektgruppen presenterer da resultatet for veilederen og Sopra Steria den 27. mai 2021.
- Prosjektgruppen får en forståelse av kundenes behov.

3.3. Prosessmål

- Øke kompetansen innenfor de fagfeltene som utforskes i prosjektet.
- Øke kompetansen for samarbeid og kommunikasjon

3.4. Prosjektets omfang

Bedriften ønsker å implementere enten WVD eller VMware vSphere, med spesielt fokus på WVD og deres funksjoner, da dette er en relativt ny løsning hvor man ønsker å vite hvordan det stiller seg i forhold til de mer brukte tjenestene. Prosjektgruppen skal i følge case-beskrivelsen gjøre rede for VMware vSphere og Windows Virtual Desktops sikkerhetsfunksjoner og utarbeide en analyse der vi sammenligner de ovennevnte virtualiseringstjenestene.

3.5. Produktets funksjonelle egenskaper

Produktet skal være en analyse av sikkerhetsnivået i WVD og andre virtualiseringstjenester slik som VMware vSphere. Produktets funksjonelle egenskaper skal være et grunnlag for bedriftens avgjørelse av hvilken virtualiseringstjeneste de ønsker å implementere.

3.6. Prosjektets milepæler og hovedaktiviteter

Prosjektgruppen benytter MS Project for å opprette en prosjektplan som illustrerer prosjektets milepæler og hovedaktiviteter med et GANTT-diagram. Prosjektet startet den 6. januar 2021 og ferdigstilles den 20. mai 2021. Vedlegg (1).

- Forstudierapport, 28. januar 2021
- Designrapport, 19. februar 2021
- Driftsrapport, 10. mai 2021
- Sluttrapport, 20. mai 2021
- Presentasjon, 27. mai 2021

4. Interessenter og rammebetingelser

4.1. Interessentanalyse

Her beskrives alle interessenter i prosjektet, suksesskriterier og deres bidrag som inngår i prosjektperioden. Disse kan deles inn i to kategorier, eksterne og interne interessenter. Videre skal vi beskrive deres roller i prosjektet.

Eksterne interessenter:

- **Ledelsen i LongLuu.** De ønsker å implementere et system for hjemmekontor for de ansatte som er mest mulig kost-/nytteeffektivt. Ledelsen fungerer som oppdragsgiver og skal stille krav, beslutte og gi innsikt i bedriften til prosjektgruppen for å komme frem til den mest optimale løsningen.

- **Sluttbruker**
  Dette er de ansatte som berøres i det daglige. Disse bidrar med nyttig informasjon før og under prosjektet.

    - **Ved kontoret**
      De kan komme med nyttig informasjon om hvordan systemet fungerer, fordeler, ulemper og igjen gi tilbakemeldinger om forbedringsmuligheter.

    - **Hjemmekontor og på reise**
      De ansatte på reise kan koble til bedriftens intranett med VPN og får en sikker tilkobling. Disse kan komme med tilbakemeldinger om brukervennlighet ved ekstern tilkobling og tjenesteytelse.

Interne interessenter:

- **Prosjektgruppen** består av to gruppemedlemmer, Solveig Longva og Annika Luu. De har ansvar for rapportskriving, planlegging, utførelse og levering av prosjektet innen sluttdato.

- **Sopra Steria** fungerer som veileder. De bidrar med kunnskap, teknisk hjelp, tekniske ressurser og veiledning.

- **NTNU AIT** fungerer som veileder. De bidrar med kunnskap, teknisk hjelp og veiledning.

Interessent	**Suksesskriterier**	**Bidrag til prosjektet**
Eksterne		
LongLuu	Bedre system med høy sikkerhet for hjemmekontor.	Beslutning, krav og innsikt
Sluttbruker	Hjemmekontor og jobbreise gjennom en sikker tilkobling.	Tilbakemelding om tjenesteytelse, brukervennlighet, fordeler og ulemper med tjenesten, både før, under og etter prosjektet.
Interne		
Prosjektgruppen	Vellykket prosjekt	Ansvar for å presentere løsninger
NTNU AIT og Sopra Steria	Vel gjennomført prosjekt og verdifull informasjon.	Veiledning, teknisk hjelp og kunnskap.

Tabell 1 - Interessentanalyse

5. Rammebetingelser

Prosjektgruppen har utarbeidet rammebetingelser for å legge begrensninger for aktiviteter som utføres i prosjektet henhold til avtaler som ble gjort.

- Absolutt krav til ferdigdato er satt til den 20. mai 2021.
- Kostnadsrammen skal settes etter LongLuu har besluttet en virtualiseringstjeneste. Prosjektgruppen skal utarbeide en kost/nytte analyse der vi sammenligner kostnaden på de ulike virtualiseringstjenester.
- Drifts- og utviklingsmiljø: Prosjektgruppen skal benytte Microsoft Azure som tilbys av Sopra Steria.

6. Kritiske suksessfaktorer

6.1. Suksessfaktorer

Faktorer som vil være kritiske for et vellykket resultat av prosjektet:

- Nok informasjon må samles inn, blant annet ved å lese eksisterende publikasjoner, forhøre seg med personer med kunnskap innenfor området, og å utforske virtualiseringstjenestene i praksis.
- Frister for ferdigstillelse av rapporter må overholdes.
- Prosjektgruppen må ha nok kunnskap om virtualiseringstjenester for å kunne sette opp et virtuelt desktop-miljø. Dersom det er noe som er uklart/nytt, må de ha evne til å tilegne seg denne kunnskapen.
- Prosjektgruppen må ha tilgang på en virtualiseringsplattform (for eksempel Microsoft Azure).
- Bedriften må oppgi sine krav til hva som skal være med i prosjektoppgaven.
- Prosjektgruppen må ha kunnskap om de tjenestene som skal sammenlignes med WVD.

6.2. Informasjonsbehov

- Prosjektgruppen behøver jevnlige møter med representanter for bedriften, for å få tilbakemeldinger underveis og svar på spørsmål som skulle dukke opp. Før møtene settes det opp en agenda, og en av studentene fører referat for møtet. Både agenda og referat skal være tilgjengelig for alle parter. Møtene holdes etter avtale mellom alle partene.
- Dersom en av partene trenger hurtig svar på noe, kan de ringe eller ta kontakt over Teams innenfor normale arbeidstider.
- Bedriften skal holdes oppdatert om hvordan prosjektgruppen ligger an og hva som er produsert mellom møtene.
- Prosjektgruppen har behov for å benytte seg av bedriftens tekniske ressurs for å få et innblikk i hvilke aspekter ved virtualiseringstjenestene det legges vekt på av bedriften.

7. Risikoanalyse

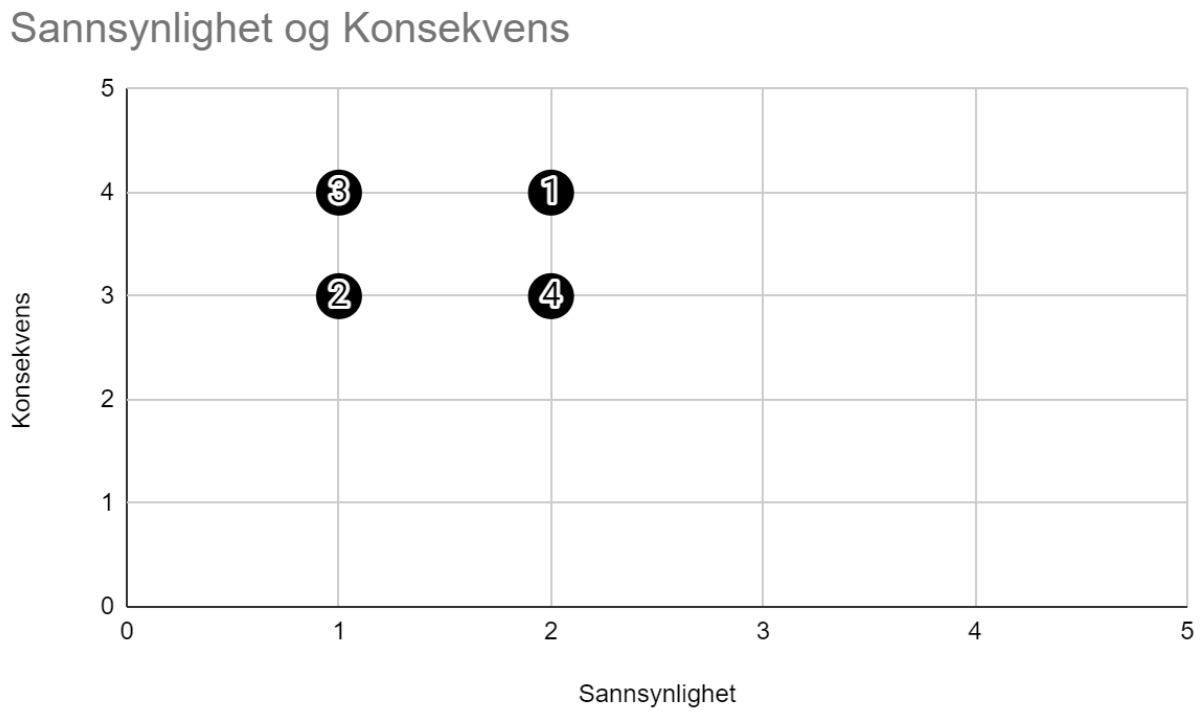
I tabellen under beskrives risikofaktorer som er knyttet til dette prosjektet. For hver faktor tar vi for oss sannsynligheten (S) for at dette inntreffer og konsekvensen(e) (K) dette kan få. Dette kan vi visualisere i et koordinatsystem, hvor tallene representerer risikofaktorens nummer i tabellen, og vi vurderer konsekvens og sannsynlighet mellom en (minst alvorlig) og fem (mest alvorlig).

Nr.	Risiko	Beskrivelse	S	K
1	Prosjektgruppen leverer ikke resultat innen tidsfrist	Dersom prosjektgruppen ikke leverer innen gitt tidsfrist vil dette kunne ansees som et tillitsbrudd da prosjektgruppen ikke klarer å levere det som er forventet, og vil gi et svekket inntrykk av prosjektgruppen. Det vil også gi forsinkelser for bedriftens arbeid med å komme til en konklusjon om hvilke systemer som skal benyttes i fremtiden og for implementasjon av dette systemet. For å unngå dette har prosjektgruppen satt opp mål og delmål i MS Project som skal oppnås innen gitte tidsrammer for å kunne holde orden på fremgangen og kunne passe på at frister overholdes.	2	4
2	Konflikt innad i prosjektgruppen	Dersom det oppstår konflikter innad i prosjektgruppen vil dette kunne skape forsinkelser og i verste fall gå utover kvaliteten på det endelige resultatet. Medlemmene i prosjektgruppen har tegnet en kontrakt mellom seg som illustrerer hva de forventer av hverandre og hvordan en eventuell konflikt skal løses på en måte som ikke går utover tidsfrister eller kvalitet.	2	3

3	Konflikt mellom prosjektgruppe og bedrift	Dersom det oppstår konflikter mellom prosjektgruppe og bedrift kan dette gå utover samarbeidet mellom partene og hindre gjennomføring av selve prosjektet. For å unngå at noe slikt inntreffer er det viktig at man holder en god dialog mellom partene, og redegjør for forventninger og planer for prosjektet på en profesjonell måte. Jevne møter kan sørge for dette, i tillegg til at det gir partene en mulighet til å bli kjent med hverandre å oppnå en god tone.	1	4
4	Misforståelser mellom prosjektgruppe og bedrift	Misforståelser mellom prosjektgruppe og bedrift kan føre til at resultatet som leveres ikke når opp til bedriftens forventninger. Igjen kan dette løses ved å ha jevnlige møter om framgangen i prosjektet og hva som er gjort så langt. Ved prosjektstart er det viktig at partene diskuterer hva som forventes av resultatet og hva som skal inkluderes i dokumentasjonen som leveres.	2	3

Tabell 2 - Risikoanalyse

Sannsynlighet og konsekvens vurdert i forhold til hverandre:



Figur 2 - Sannsynlighet og konsekvens

8. Kostnad og nytte

I forbindelse med dette prosjektet er det vanskelig å anta noe om den kvantifiserbare nytten, da denne avhenger av uforutsigbare faktorer, slik som pandemien. Dersom bruken av hjemmekontor fortsetter å være meget utbredt vil man kunne anta at nytten av en virtualiseringstjenste er stor. Dersom dette ikke er tilfellet vil det sannsynligvis være like nyttig, men det er vanskelig å si i hvor stor grad.

8.1. Kvantifiserbar nytte

Per dags dato har ikke LongLuu en virtualiseringsløsning. Det vil kunne antas at de vil tape en del på å ikke ha dette, da i lys av COVID-19-situasjonen og andre situasjoner som kan forhindre arbeid på kontor. Man kan potensielt bli hindret i å få utført arbeid dersom det ikke er mulig for bedriften å tilby hjemmekontor i en situasjon der dette er anbefalt, påbudt eller på annen måte behøvelig.

8.2. Ikke-kvantifiserbar nytte

Den ikke-kvantifiserbare nytten innebærer økt fleksibilitet blant de ansatte ved mulighet til å ha hjemmekontor. Denne nytten er vanskelig å sette et tall på, da situasjoner som medfører behov for hjemmekontor vanligvis er uforutsigbare. Dersom situasjoner som COVID-19 preger bedriften på lang sikt vil det uten tvil kunne unngå tapt arbeidskraft og økonomiske tap for bedriften som følge av tapt produktivitet, dersom de har mulighet til å jobbe hjemmefra. Det vil også lønne seg å ha en virtualiseringsløsning på plass for å kunne jobbe på reise og på offsite-møter.

Ved å gjennomgå en sammenligning av de ulike tjenestene vil det kunne gi bedriften mulighet til å ta det beste valget med tanke på kostnader sammenlignet med andre tjenester. De vil altså med høy sannsynlighet spare på sikt på å gjennomføre dette prosjektet da de får et godt grunnlag for å velge den mest egnede tjenesten.

8.3. Estimerte kostnader

8.3.1. Bruk av Windows Virtual Desktop

LongLuu eier Windows 10 Enterprise-lisenser, i tillegg til RDS CAL-lisenser med Software Assurance. Windows Virtual Desktop er inkludert i lisensen og krever dermed ikke ekstra kostnader for selve tjenesten (1).

8.3.2. Bruk av VMware vSphere

For VMware vSphere har en behov for en lisens per CPU. Per åttekjerners CPU vil man kunne ha omtrent 15 VM-er, så for en bedrift med 100 ansatte vil man da trenge minst sju lisenser. VMware vSphere koster 248 894,31 kr for sju lisenser og er en engangssum. Dette inkluderer supportkostnader (31).

8.3.3. Prissammenligning av virtualiseringstjenestene

	Kostnad (pr. år)	**Brukere**
Windows Virtual Desktop	386 386,83 (med lisens allerede eid av LongLuu)	100
VMware vSphere	248 894,31 (engangssum)	100

Tabell 3 - Prissammenligning

9. Retningslinjer og standarder

9.1. Krav til dokumentasjon

Under utførelsen skal prosjektgruppen utarbeide dokumenter som leder prosjektet mot det endelige resultatet. Det leveres en sluttrapport og en presentasjon ved slutten av prosessen. Denne rapporten vil foreligge skriftlig på PDF-format ved levering.

9.1.1. Forstudierapport

Hensikten med denne rapporten er å klargjøre bakgrunnen av prosjektet, prosjektets mål og interessenter samt gjennomføre de nødvendige undersøkelsene for at bedriften kan avgjøre om dette er et prosjekt de ønsker å fortsette med. Denne rapporten skal ferdigstilles den **28. januar 2021.**

9.1.2. Designrapport

Denne rapporten skal være en forminsket versjon av forstudierapport der vi får en overordnet oversikt av prosjektet. Frist for innlevering **19. februar 2021.**

9.1.3. Driftsrapport

I denne rapporten skal prosjektgruppen innhente nødvendig informasjon og skaffe oversikt over produktet. Frist for innlevering **10. mai 2021**

9.1.4. Sluttrapport

Sluttrapporten er den avsluttende rapporten for prosjektet. Her skal prosjektgruppen gjøre rede for hele prosjektet der de oppsummerer arbeidet samt gjøre vurderinger av måloppnåelse. Bedriften skal beslutte om videre arbeid etter prosjektet basert på denne rapporten. Frist for innlevering **20. mai 2021.**

9.1.5. Rutiner for godkjenning og revisjon

Alle rapporter skal leveres innen et bestemt tidspunkt, og disse skal gjennomgås og godkjennes av alle i prosjektgruppen. Hvert dokument avsluttes med et møte der veilederne får tilgang til dokumentet i forkant av møtet, en til tre dager, slik at de kan komme med tilbakemelding eller kommentarer for endring eller godkjenning av dokumentet.

9.2. Krav til kvalitetsgjennomganger

Prosjektgruppen ser et behov for kvalitetsgjennomganger av følgende dokumenter og aktiviteter:

9.2.1. Rapporter

Prosjektgruppen skal utarbeide rapporter og har hovedansvaret for kvalitetsgjennomgang av dokumenter som utarbeides under prosjektet. Disse rapportene skal godkjennes innad i prosjektgruppen før de kontrolleres av veilederen og Sopra Steria. Alle interessenter må være med å godkjenne en rapport før denne regnes som gyldig i prosjektet.

9.2.2. Case-beskrivelse

Alle parter i prosjektet må godkjenne case-beskrivelsen før prosjektgruppen setter i gang prosjektet.

9.2.3. Møter

Under utførelsen av prosjektet, skal det avholdes flere veiledningsmøter. Det sendes en møteinnkalling til hvert møte og disse blir referert av et medlem i prosjektgruppen. Alle interessenter skal gjennomføre en kvalitetsgjennomgang av disse for å sikre enighet i prosjektet.

9.3. Krav til standarder og metoder

9.3.1. Rapportmaler

I dette prosjektet benyttes dokumentmaler fra emnet IDRI2007 - Prosjekt og dokumentasjonsarbeid som grunnform. Disse blir tilpasset etter behov.

9.3.2. Microsoft

9.3.2.1. Microsoft Project

Dette er et prosjektstyringsprogram som benyttes for å opprette en oversiktlig prosjektplan og fremvises som et GANTT-diagram.

9.3.2.2. Word

Dette er et tekstbehandlingsprogram som benyttes for all dokumentasjon og rapportskriving.

9.3.2.3. Microsoft Teams

Teams er en kommunikasjons- og samarbeidsplattform som knytter alle parter av prosjektet i en gruppe. Her ligger all nødvendig informasjon, slik som dokumenter, kontrakter, møtereferat og lignende. Det avholdes faste møter på Teams der prosjektgruppen er ansvarlig for å oppdatere alle interessenter om fremgangen i prosjektet.

9.4. Endringshåndtering

Alle interessenter kan sende en forespørsel om endring av dokumenter i prosjektet. Disse skal behandles formelt og forretningsmessig og gjennomføres på følgende måte:

9.4.1. Utfylling av endringsmelding, dokumentér endringsinnhold

Fastsette endringen og spesifiser hvilken del av dokumentet/prosjektet det gjelder.

9.4.2. Foreta en konsekvensanalyse

Nye endringer kan føre til nye konsekvenser. Det er behov for konsekvensanalyse for å ha oversikt over mulige konsekvenser for så igjen unngå uønskede hendelser.

9.4.3. Foreta en ny kostnadsanalyse

Det er essensielt å foreta en ny kostnadsanalyse for å korrekt beregne kost/nytte ved en endring.

9.4.4. Godkjenning og aksept

Alle interessenter må godkjenne endringen før man utfører endringen.

9.4.5. Loggføring av endring

Alle endringer skal loggføres.

9.4.6. Justering av prosjektplanen

Her er det viktig med en oppdatering av prosjektplanen, GANTT-diagrammet og omorganisere prosjektet etter endringen.

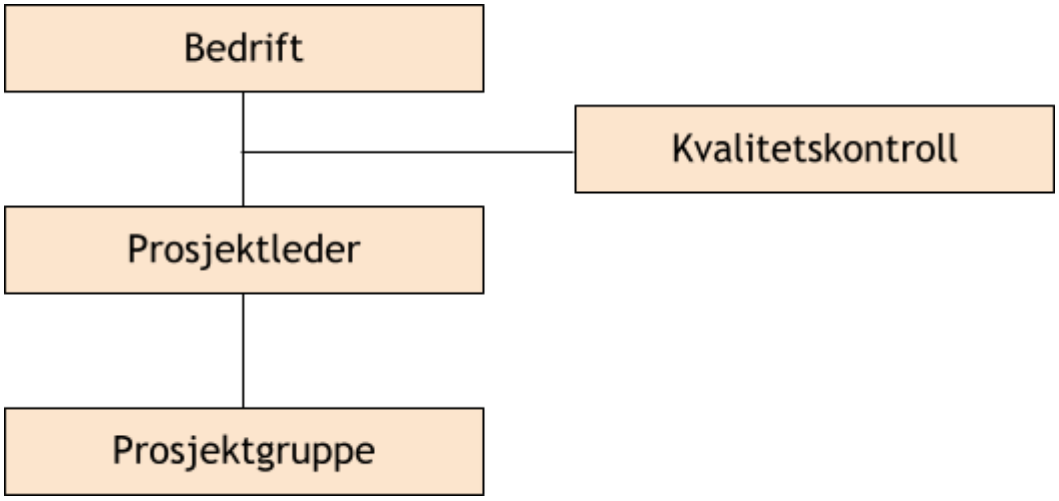
9.4.7. Informering av interessenter

Etter at prosjektgruppen har gjort rede for endringen, skal prosjektgruppen informere alle interessenter om dette.

9.4.8. Gjennomføring av endring

Dersom de ovennevnte punktene er gjennomført, kan vi gjennomføre endringen.

10. Prosjektorganisering



Figur 3 - Prosjektorganisering

Figuren over viser partene i prosjektet og arbeidsfordelingen mellom disse.

- Bedriften LongLuu er oppdragsgiveren for prosjektet og skal klargjør deres ønsker fra prosjektgruppen og hva som forventes av resultatet.
- Kvalitetskontroll vil gjennomføres av veilederne for prosjektet. Dette innebærer at de vurderer kvaliteten basert på krav fra bedriftens side. I dette tilfellet er dette Stein Meisingseth, veileder fra NTNU AIT, og Sopra Steria.
- Prosjektlederrollen rulleres mellom medlemmene i prosjektgruppen. Prosjektlederen har rolle som møteleder under veiledningsmøter i prosjekt.
- Prosjektgruppen består av to medlemmer, Solveig Longva og Annika Luu, hvor arbeidsoppgaver fordeles jevnt mellom disse.

11. Anbefaling om videre arbeid

Prosjektgruppen har gjort rede for ikke-kvantifiserbar nytte, der bedriften vil få nytte av å gå over til en virtualiseringstjeneste. Det vil være lønnsomt for bedriften på lang sikt, både med tanke på mulighet for hjemmekontor, slik at man unngår tapt arbeidskraft i situasjoner der fysisk oppmøte ikke er mulig, og jobbreiser. En virtualiseringstjeneste kan øke fleksibiliteten i bedriften samt åpne opp nye muligheter for de ansatte. I dette prosjektet vil bedriften få mulighet til å velge den sikreste løsningen og vurdere nytten opp mot dette. Følgelig vil prosjektgruppen anbefale å videreføre prosjektet med de planene som er fremlagt i forstudierapporten.

Bacheloroppgave, Designrapport

Annika Luu
Solveig Longva

Designrapport

Sikkerhet i virtualiseringstjenester

Versjon 1.0

Februar 2021

NTNU
Kunnskap for en bedre verden

sopra steria

Innholdsfortegnelse, designrapport

Revisjonshistorie

Dato	Versjon	Beskrivelse	Forfattere
19.02.2021	0.1	Opprettelse av designrapport.	Annika Luu og Solveig Longva
25.02.2021	0.2	Endring på dokumentet basert på tilbakemelding fra veiledere.	Annika Luu og Solveig Longva
29.04.2021	0.3	Fjerne Citrix fra prosjektet.	Annika Luu og Solveig Longva
13.05.2021	1.0	Formatering.	Annika Luu og Solveig Longva

Oppsett

Designrapporten inneholder en oppsummering av kundens behov og dagens systemer. Med dette utgangspunktet begrunnes valg av virtualiseringstjenester. I neste del av rapporten fortsetter vi med å beskrive tekniske detaljer og funksjoner knyttet til testmiljø og virtualiseringstjenestene. Avslutningsvis beskrives detaljer rundt selve prosjektet, det vil si dokumentasjon, prosjektplan og videre arbeid. I tillegg presenteres anbefaling for videre arbeid i dette prosjektet.

1. Innledning

Designrapporten er en overordnet oversikt over utformingen av løsningen som prosjektgruppen skal levere til kunden, i tillegg til hvordan dette utføres. Rapporten setter hovedfokus på prosjektets omfang og utførelse.

I denne rapporten finner man en innledning til selve designrapporten og en oversikt over begreper og forkortelser som brukes. Vi tar også en gjennomgang av kunden og deres situasjon, i tillegg til hvilke krav og behov de har knyttet til fremtidige systemer. Deretter beskrives de tekniske løsningene, og funksjonene i de ulike virtualiseringstjenestene redegjøres for. Avslutningsmessig gis en oppdatering på prosjektplanen og anbefaling for videre arbeid.

Hensikten med rapporten er å gi oppdragsgiver innblikk i hvordan sluttresultatet vil se ut og hvordan arbeidet foregår for å oppnå avtalte prosjektmål. Denne rapporten skal i tillegg fungere som en konseptuell beskrivelse av tekniske detaljer som vurderes når vi videre skal utføre en analyse av systemene.

2. Avgrensning

I dette prosjektet sammenligner prosjektgruppen Windows Virtual Desktop og VMware vSphere. Bedriften LongLuu ønsker å få en detaljert analyse av disse to virtualiseringstjenestene. Prosjektgruppen skal sammenligne ulike egenskaper som gir en direkte påvirkning på beslutningen for hvilken virtualiseringstjeneste bedriften vil gå for.

Under finner du en liste over egenskaper som er interessant i denne analysen.

- Kost/nytte analyse
- Sikkerhetsnivå
    - Funksjoner
- Brukervennlighet

Resultatet av dette prosjektet skal være en grundig analyse av WVD og VMware vSpheres sikkerhetsfunksjoner og deretter sammenligne deres egenskaper som er nevnt i listen over.

3. Kunde og behov

LongLuu er en bedrift som driver med regnskap for bedrifter i Norge. De har 100 ansatte som tilhører til ulike avdelinger. LongLuu ønsker å virtualisere IT-systemene sine, enten med Windows Virtual Desktop eller VMware, for å åpne opp for hjemmekontor på grunn av COVID-19-situasjonen. Bedriften har kjennskap til disse virtualiseringstjenestene men ønsker en grundig analyse av deres sikkerhetsnivå. Prosjektgruppen har fått dette oppdraget og skal undersøke samt utarbeide en sammenligning av produktenes funksjonalitet og sikkerhet. Denne rapporten skal være et beslutningsgrunnlag for en eventuell implementasjon på et senere tidspunkt.

I dag benytter LongLuu et on-premise Windows-basert miljø der all programvare er installert lokalt på arbeidsstasjonen. Bedriften mangler en virtualiseringstjeneste for arbeidsstasjoner og servere, noe som begrenser produktiviteten i dag på grunn av COVID-19. Bedriften ønsker også en sikker tilkobling til bedriftens intranett ved jobbreiser.

4. Hvorfor valg av løsning

Det eksisterer mange ulike virtualiseringstjenester for arbeidsstasjoner. I dette prosjektet har vi besluttet i samråd med oppdragsgiver at fokuset skal begrenses til tjenestene Windows Virtual Desktop og VMware vSphere. Dette begrunnes av at Windows Virtual Desktop er en relativt ny løsning som for mange bedrifter virker veldig interessant, blant annet på grunn av at man kan benytte seg av det uten ekstra kostnader for lisens dersom man allerede har eksisterende Windows-lisenser. Følgende lisenser gir tilgang til WVD:

- Microsoft 365 E3/E5
- Microsoft 365 A3/A5/Student Use Benefits
- Microsoft 365 F3
- Microsoft 365 Business Premium
- Windows 10 Enterprise E3/E5
- Windows 10 Education A3/A5
- Windows 10 VDA per user

Det er derimot lite dybdekunnskap om WVD blant mange bedrifter. Vi velger derfor å analysere sikkerhet og kost-/nytte for bedriften med Windows Virtual Desktop slik at LongLuu får den informasjonen de trenger for å avgjøre om dette er en aktuell løsning. VMware er et mer tradisjonelt valg blant bedrifter og det er derfor nyttig å sammenligne disse opp mot Windows Virtual Desktop for se hvordan disse stiller seg opp mot hverandre.

De endrede kostnadene ved å gå over til bruk av virtuelle maskiner gjennom en av de to virtualiseringstjenestene inkluderer også selve kostnaden for tjenesten. I tillegg kommer kostnader knyttet til implementering av valgt løsning. Implementering kan utføres av bedriften selv eller av eksterne konsulenter. Med riktig planlegging av implementeringsprosessen vil ikke overgangen til virtuelle arbeidsstasjoner føre til noe nedetid, da systemet kan settes opp i parallell med eksisterende løsninger.

Framtidige kostnader ved de ulike tjenestene kan sees i tabellen under. Kostnader ved bruk av ekstern konsulent kommer i tillegg om man ønsker å benytte seg av dette. Prisene er overslag og ikke absolutte tall.

	Kostnad (pr. år)
Windows Virtual Desktop	386 386,83 (med lisens)
VMware vSphere	248 894,31 (engangssum)

Figur 3 - Prissammenligning

5. Beskrivelse av tekniske løsninger

5.1. Testmiljø

For å evaluere de ulike tjenestene setter prosjektgruppen opp et testmiljø i MS Azure for vurdering av WVD, mens VMware testes lokalt. Testmiljøet benyttes for å utrede hvilke sikkerhetsfunksjoner som er tilgjengelige i tjenestene, og hvordan disse fungerer. I tillegg ser vi på hvor intuitiv installasjonen av tjenesten er og hvor brukervennlig administrasjonen av systemet er.

5.2. Verktøy og ressurser

I utførelsen av prosjektet benyttes følgende verktøy og ressurser:

- Microsoft Azure
- VMware vSphere
- MS Project
- Google Scholar

6. Løsningsbeskrivelse

Her beskriver vi viktige sikkerhetsfunksjoner (og andre relevante funksjoner for å forenkle administrasjon av systemet) knyttet til de ulike virtualiseringstjenestene, og hvilke systemkrav som må møtes for å ta disse tjenestene i bruk. I tillegg til disse sikkerhetsfunksjonene er det helt avgjørende at systemet er konfigurert med riktige tilganger og rettigheter.

6.1. Programvare, systemkrav og viktige sikkerhetstjenester

Disse løsningene krever at man har Windows 10 installert, i tillegg til de nyeste versjonene av virtualiseringstjenestene nevnt under for å kunne dra full nytte av de nyeste sikkerhetsfunksjonene. Videre er det viktig å sørge for at man inkluderer systemer som utfører viktige oppgaver når det kommer til sikkerhet. Dette gjelder altså alle virtualiseringstjenestene vi skal se på.

6.2. Forutsetninger og avhengigheter

Prosjektgruppen definerer følgende punkter som forutsetninger og avhengigheter for å oppnå effektmål, resultatmål og prosessmål som er oppgitt i forstudierapporten.

6.2.1. Innlevering

Denne rapporten skal ferdigstilles ca. den 19. februar og leveres i PDF-format som en del av den endelige rapporten den 20. mai 2021.

6.2.2. Mål

Vi er avhengig av å undersøke relevante funksjoner som blir nevnt i punkt 7.3. for å sikre at følgende mål er oppnådd ved innlevering.

- Øke sikkerheten ved implementering av virtuelle tjenester.
- Trygg tilkobling ved hjemmekontor.
- Skalerbar virtualiseringsløsning.
- En kost-/nytteeffektiv løsning
- Brukervennlig løsning

6.3. Windows Virtual Desktop

Prosjektgruppen skal sette opp en VM med Windows Virtual Desktop, med tilhørende applikasjoner og tjenester som er viktig for sikkerhetsadministrasjon.

6.3.1. FSlogix

FSlogix består av et sett av løsninger som kan forenkle bruk av Windows-miljøer (3). I Windows Virtual Desktop er det anbefalt å benytte FSLogix profile containers som brukerløsning, slik at hver brukerprofil blir lagret i en egen container. Dette kan gi bedre ytelse og gjør at OneDrive for Business støttes. I tillegg gir det mulighet til å utvide brukerprofilen med ekstra mapper.

6.3.2. Reverse connect

Reverse connect er en innebygd sikkerhetsfunksjon som brukes i Windows Virtual Desktop for å redusere risikoen ved bruk av remote desktops ved hjemmekontor og jobbreiser (4). Ved hjelp av denne teknologien kan vi kjøre virtuelle maskiner med private IP-adresser og holde disse isolert fra andre arbeidsoppgaver og nettverk.

6.3.3. Multi-factor authentication med Conditional Access

Multi-factor authentication gir et ekstra lag av sikkerhet, og må benyttes for alle brukere, både “vanlige” brukere og for administratorer (4).

6.3.4. Endpoint protection

Det er essensielt å aktivere endpoint protection i alle virtuelle maskiner i Windows Virtual Desktop for å beskyttelse klientene mot ondsinnede programvare (4). Dette gjøres ved å aktivere Windows Defender der Azure Monitoring Agents er installert og koblet opp mot Azure Security Center.

6.3.5. Azure Security Center

Det å aktivere Active Security Center åpner opp mulighet for administrasjon av sikkerhetsstatus og gir en beskyttelse mot trusler mot arbeidsbelastninger med Azure Defender (4). Dette vil effektivisere administrasjonen av sikkerhet som igjen styrker sikkerheten av hele miljøet.

6.3.5.1. Azure Defender

En innebygd tjeneste i Azure Security Center som gir trusselbeskyttelse for arbeidsbelastninger i Azure, både lokalt og i hybrid sky. Denne styrker infrastrukturen av Windows Virtual Desktop gjennom sikkerhetsvarsling der sikkerheten er effektivisert med kunstig intelligens og automatisering (5).

6.3.5.2. Secure Score

Secure score gir anbefalinger og råd for hvordan man kan øke sikkerheten i systemet (4). Disse anbefalingene oppdateres jevnlig og holder brukeren oppdatert på hva som er beste praksis når det kommer til sikkerhetsadministrasjon.

6.3.6. Azure Monitor

Med Azure Monitor kan man overvåke bruk og tilgjengelighet, og man kan sette opp varslinger for hendelser (slik som nedetid). Denne tjenesten samler inn telemetri og analyse datalogg i Log Analytics (4).

6.3.7. Screen Capture Protection

Denne funksjonen forhindrer sensitiv informasjon fra å bli tatt opp i form av opptak av skjermen eller skjermbilder fra klientens side gjennom ondsinnet programvare (4).

6.3.8. Azure Sentinel

Her ønsker vi å lagre audit logs i en SIEM løsning, Azure Sentinel for å få innsyn i brukeraktivitet og diagnostikk (26). Disse loggene omfatter blant annet:

- Azure Activity Log
- Azure Active Directory Log
- Azure Active Directory
- Session host
- Windows Virtual Desktop Diagnostic Log
- Key Vault logs

6.3.9. Integrer Azure Security Center med Azure Sentinel

Det å integrere Security Center med Azure Sentinel får vi et resultat som ligner på Security Operation Center (SOC). Sikkerhetsvarsler fra Azure Defender kan overvåkes i Azure Sentinel Workbook og kan opprette en hendelse for håndtering av en trussel.

6.4. VMware vSphere

6.4.1. Extended Detection and Response (XDR)

XDR tilbyr enhetlig plattform for gjenkjenning og respons for sikkerhetsbrudd (18). Ved hjelp av dette får man samlet og sammenlignet data fra flere kilder og ta kontroll fra ulike punkter i systemet for å kunne oppdage trusler raskere.

6.4.2. VMware vSphere HA

VMware tilbyr en tjeneste kalt VMware vSphere HA. Dette er en tjeneste som sørger for at virtuelle maskiner flyttes til en annen tjener dersom nåværende tjener krasjer. Loggfiler opprettes for slike hendelser slik at årsaken til feilen kan identifiseres (5).

6.4.3. VMware NSX

VMware NSX tilbyr funksjonalitet for å administrere virtuelle nettverk med mulighet for å implementere "zero-trust"-sikkerhet mellom VM-er og mikrosegmentering (oppdeling av datasenteret i sikkerhetssegmenter som gjør det mulig å definere sikkerhetskontroller for hvert segment) (22).

7. Krav til driftsdokumentasjon

Dokumentasjonen skal leveres på en måte som sikrer oversiktlighet og tilgjengelighet for alle parter.

- All dokumentasjon (forstudierapport, designrapport og driftsrapport) skal leveres som en sluttrapport på PDF-format innen oppgitt tidsfrist.
- All dokumentasjon skal være på norsk. Informasjon kan fortsatt hentes fra engelskspråklige kilder.
- Oppdragsgiver og IDI AIT skal ha opphavsrett til dokumentasjonen
- Før endelig innlevering skal dokumentasjonen kvalitetssikres av veileder og oppdragsgiver

8. Konklusjon

Prosjektgruppen har utformet en skisse til design for analyse av utvalgte virtualiseringstjenester. Bedriften LongLuu ønsker å vite hvilken av disse tjenestene tilbyr den mest kost-/nytteeffektive løsningen blant Windows Virtual Desktop og VMware vSphere, slik at de kan gå over fra dagens system med kun lokale arbeidsstasjoner, til et system med virtuelle maskiner slik at de kan jobbe hjemmefra og på reise.

Vi har gjort kort rede for en rekke sikkerhetsfunksjoner i de ulike løsningene som er interessante å undersøke nærmere når man skal foreta en inngående analyse og sammenligning av tjenestene. Hovedfokus ved gransking av disse tjenestene er sikkerheten, i tillegg til brukervennlighet og pris, som er viktige vurderingspunkter for bedriften.

Videre arbeid avhenger av at nok informasjon er samlet inn slik at man har et grunnlag for å utføre analysen. Neste steg i prosessen er å ta utgangspunkt i denne informasjonen og presentere dette sammenstilt for hver tjeneste, slik at man kan se dette i en sammenheng som kan gi grunnlag for vurdering av hvilken tjeneste man potensielt kan implementere i bedriften.

Bacheloroppgave, Driftsrapport

Annika Luu
Solveig Longva

Driftsrapport

Sikkerhet i virtualiseringstjenester

Versjon 1.0

Mai 2021

NTNU
Kunnskap for en bedre verden

sopra steria

Innholdsfortegnelse, driftsrapport

Revisjonshistorie

Dato	Versjon	Beskrivelse	Forfattere
15.02.2021	0.1	Opprettelse av driftsrapport.	Annika Luu og Solveig Longva
07.05.2021	0.2	Fjerning av Citrix.	Annika Luu og Solveig Longva

1. Innledning

Planen med denne rapporten er å beskrive hvordan testing av systemet foregår og hvordan dette settes opp. Driftsrapporten setter hovedfokus på fremgangsmåten og de tekniske detaljene som angår det endelige resultatet og forklarer dette for relevante interessenter.

I dette dokumentet finner man en innledning til driftsrapporten og deretter en oversikt over definisjoner og forkortelser som man bruker i rapporten. Videre går vi gjennom fire faser for å oppnå sluttresultatet. Dette involverer en beskrivelse av hvordan vi har satt opp testlab-en, hvilke sikkerhetsfunksjoner som er inkludert i testen og hvordan disse fungerer (i tillegg til hvorfor disse er inkludert), og en økonomisk analyse av de ulike løsningene. Siste fase oppsummerer resultatene og gir et overblikk over de viktigste punktene angående sikkerhet, brukervennlighet og kostnader. Til slutt går vi gjennom den oppdaterte prosjektplanen og presenterer konklusjonen for leseren hvor vi tar for oss hovedelementene fra resultatet man har kommet fram til og anbefaler videre handling basert på dette.

2. Hensikt

Hensikten med denne rapporten er å fremlegge en oversiktlig plan av prosjektet gjennom en detaljert dokumentasjon av prosessen underveis. I rapporten finner du en beskrivelse av hvordan prosjektgruppen gjennomfører prosjektet i henhold til beskrivelsen i designrapporten samt prosjektets mål som er beskrevet i forstudierapporten.

3. Innhold

Rapporten deles inn i fire faser hvor vi finner en beskrivelse av oppsettet av de to virtualiseringstjenester, en grundig undersøkelse av deres sikkerhetsfunksjoner, kostnadsanalyse og til slutt en sammenligning. Oppsett og funksjonalitet forklares og fremvises ved hjelp av figurer og skjermbilder fra testlaboratoriet som opprettes i første fase. I den økonomiske analysen av Windows Virtual Desktop og VMware vSphere tas alt knyttet kost/nytte med i betraktning. Ved siste fase sammenlignes virtualiseringstjenestene ved å analysere deres egenskaper, fordeler, ulemper, brukervennlighet, sikkerhetsnivåer og kost/nytte. Denne rapporten avsluttes med en oppsummering av de ovennevnte egenskaper og en vurdering av virtualiseringstjeneste for bedriften LongLuu.

4. Beskrivelse av faser

For å gi en god forståelse for hva fasene som gjennomgås i denne rapporten tar for seg, gir vi her en kort oppsummering av de ulike fasene og hva de innebærer.

4.1. Fase 1 - Oppsett av testlaboratoriet

I denne fasen skal prosjektgruppen vise fremgangsmåten for installasjon og oppsettet av testmiljø i Azure og VMware vSphere. Hensikten er å undersøke sikkerhetsfunksjonene som WVD og VMware leverer i testmiljøet.

4.2. Fase 2 - Sikkerhetsfunksjoner

4.2.1. WVD

Følgende sikkerhetsfunksjoner knyttet til WVD tar vi for oss i denne fasen:

- FSlogix
- Multi-Factor Authentication
- Endpoint protection
- Azure Security Center
- Secure Score
- Azure Monitor
- Azure Monitor Metrics
- Logs Analytics
- Screen Capture Protection
- Microsoft Azure Sentinel

4.2.2. VMware

I denne tjenesten trekker vi frem følgende tjenester:

- Extended Detection and Response (XDR)
- VMware vSphere High Availability

- VMware NSX

4.3. Fase 3 - Økonomisk analyse

Den økonomiske analysen bryter ned kostnadene knyttet til løsningene. For de ulike løsningene har man ulike tjenester som varierer i pris. Det er viktig å ha oversikt over disse for å vite hva man potensielt vil betale for, og om disse tjenestene er verdt kostnaden. For hver tjeneste er det flere funksjoner og tjenester man kan benytte seg av og sluttpris vil derfor variere basert på hva man velger å kjøpe. Vi trekker fram funksjonene og tjenestene som vi ser er viktig for optimal sikkerhet og presenterer kostnad for hver av disse.

4.4. Fase 4 - Sammenligne de ovennevnte

Avslutningsvis utarbeider prosjektgruppen en analyse av WVD og VMware, der alle nevnte egenskaper sammenlignes og konkluderes med en oppsummering ved slutten av driftsrapporten.

5. Fase 1 - Oppsett av testlaboratoriet

I dette prosjektet opprettes det to testmiljøer for å muliggjøre en grundig undersøkelse av deres sikkerhetsfunksjoner. Under finner man en oversikt over testmiljøene som skal opprettes:

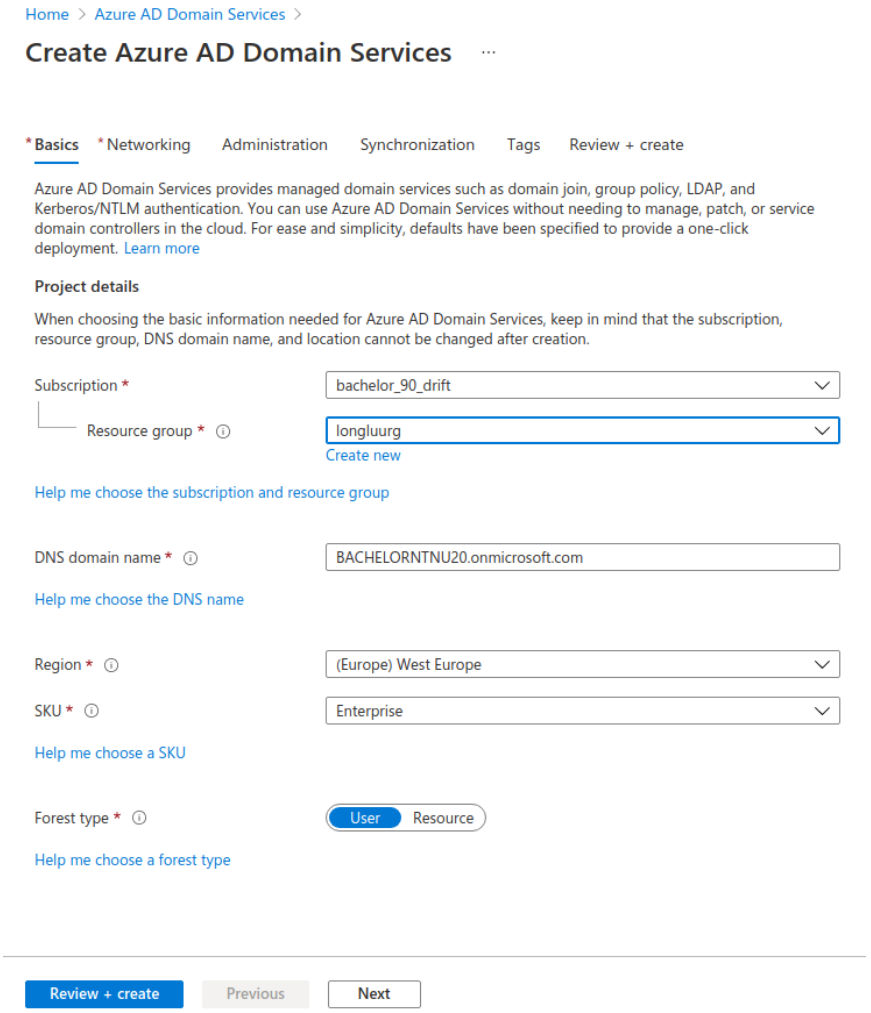
- Et miljø i Microsoft Azure som disponeres av Sopra Steria
- Et miljø i VMware vSphere som disponeres av Norges teknisk-naturvitenskapelige universitet.

5.1. Windows Virtual Desktop

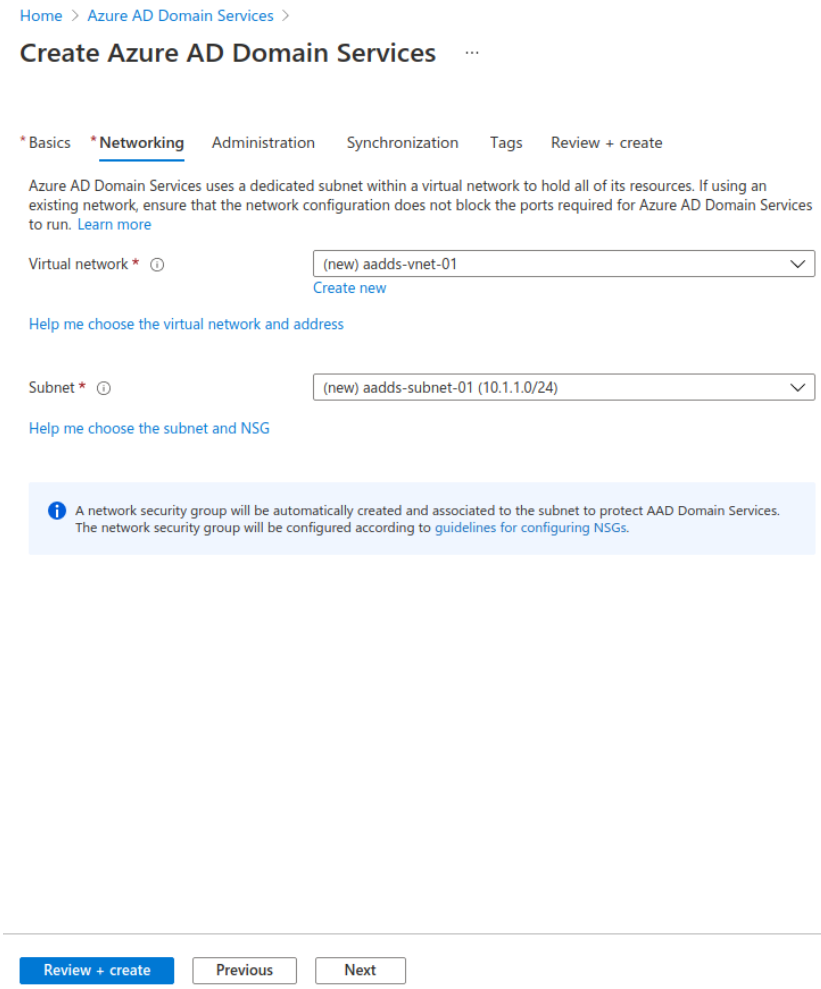
Sopra Steria disponerer ett Azure abonnement som benyttes for å opprette et testmiljø i Windows Virtual Desktop. I oppsettet går vi gjennom stegene som inngår i å sette opp en virtuell maskin i Windows Virtual Desktop, før vi ser på oppsett og konfigurasjon av sikkerhetsfunksjonene man kan benytte seg av.

5.1.1. Oppsett av virtuell maskin

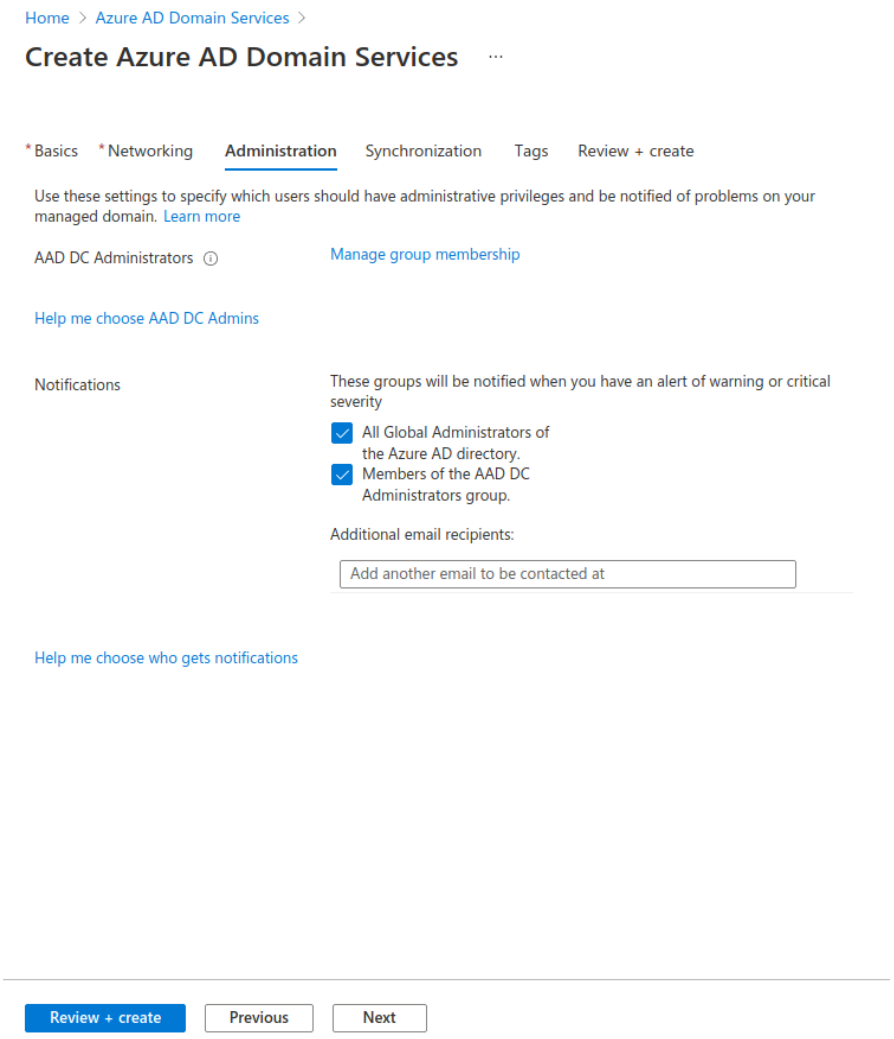
5.1.1.1. Azure Active Directory Domain Services



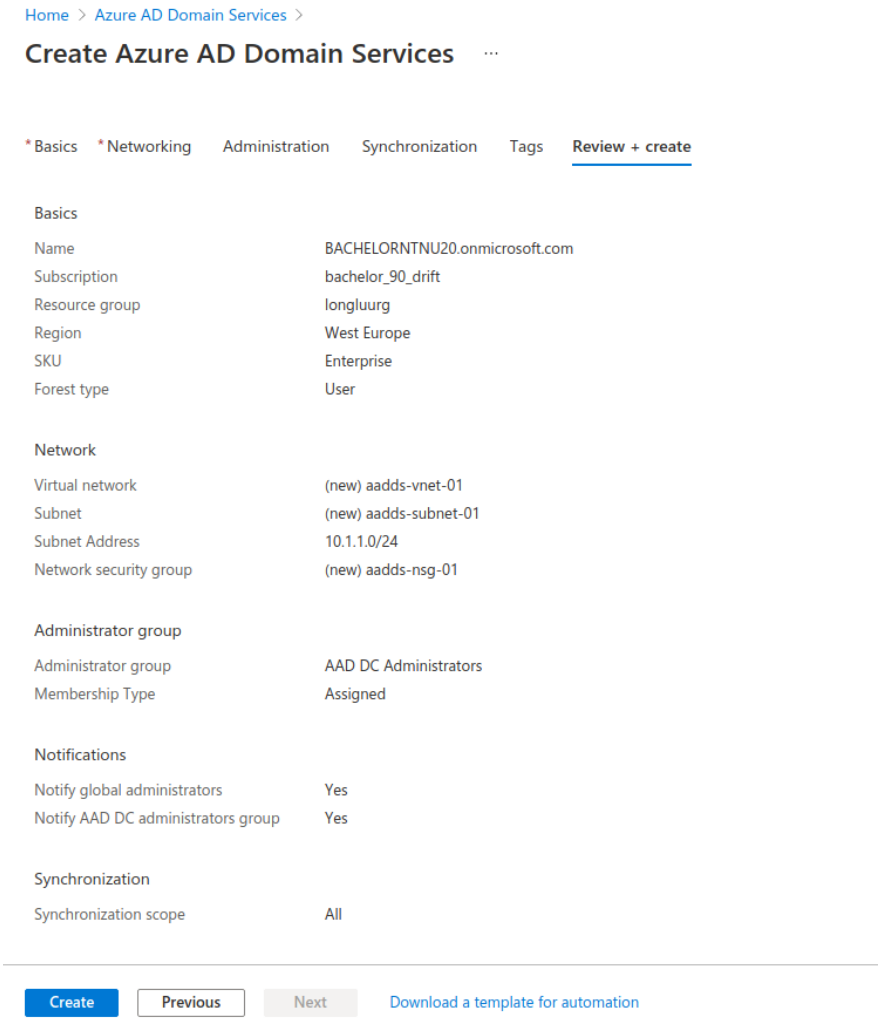
Første steg er å sette opp en domenekontroller med Azure Active Directory Domain Services (AADDS). Dette skal vi senere benytte for at maskinene skal kunne kommunisere med domenekontrolleren. Her velger vi ressursgruppe og domenenavn på tenant.



Når vi setter opp AADDS, setter vi også opp et virtuelt nettverk og velger adresseområde for subnettet.

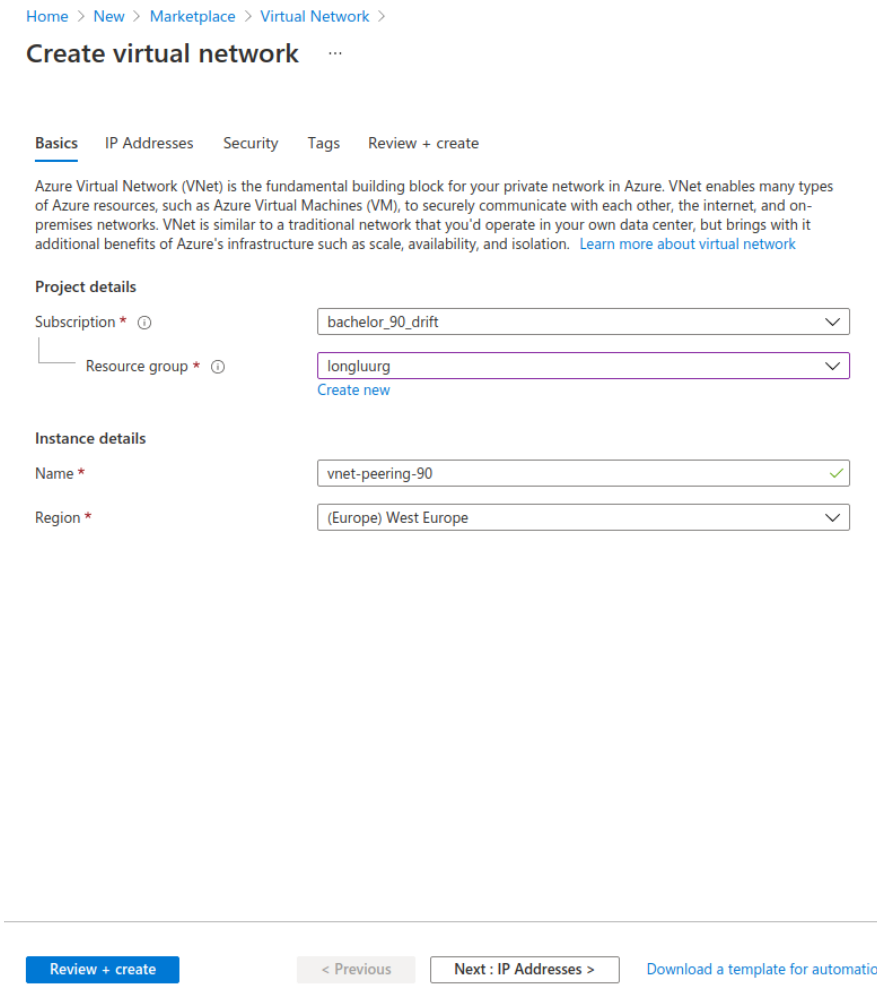


Vi velger at administratorgruppen i tenant-en skal kunne administrere domenekontrolleren.

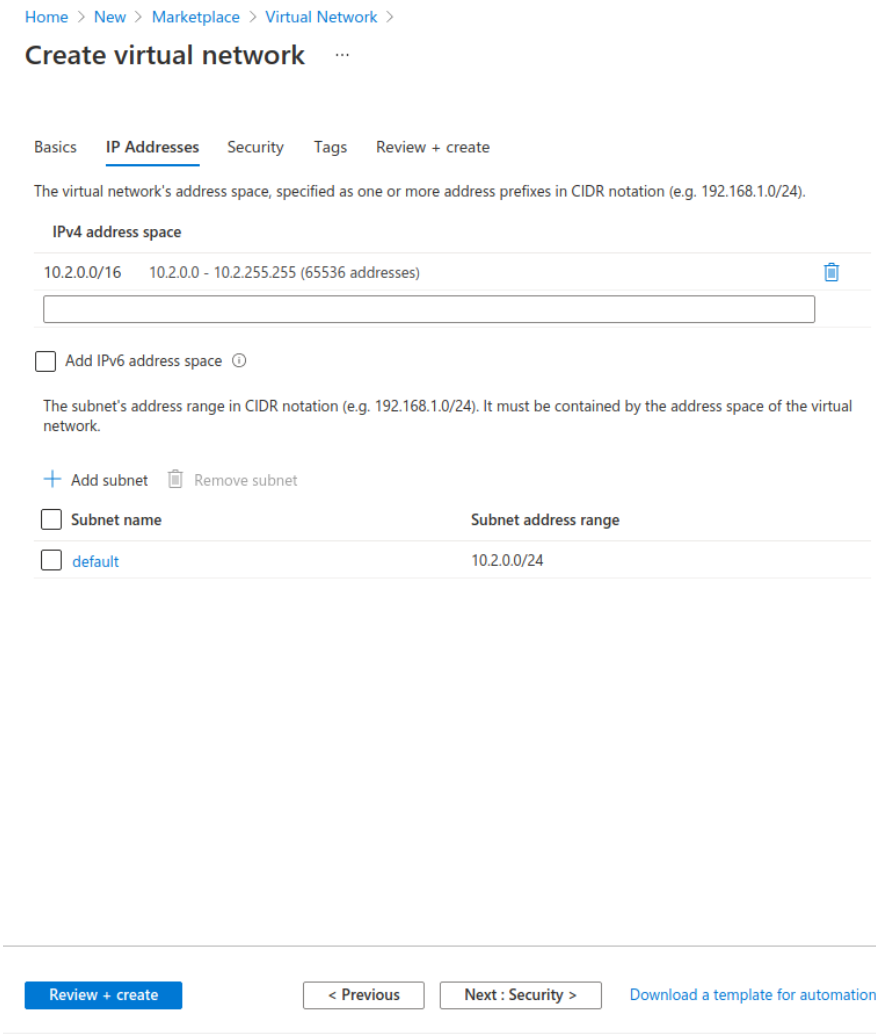


Resten av innstillingene lar vi stå som de er og velger "Review + create" for å rulle ut tjenesten.

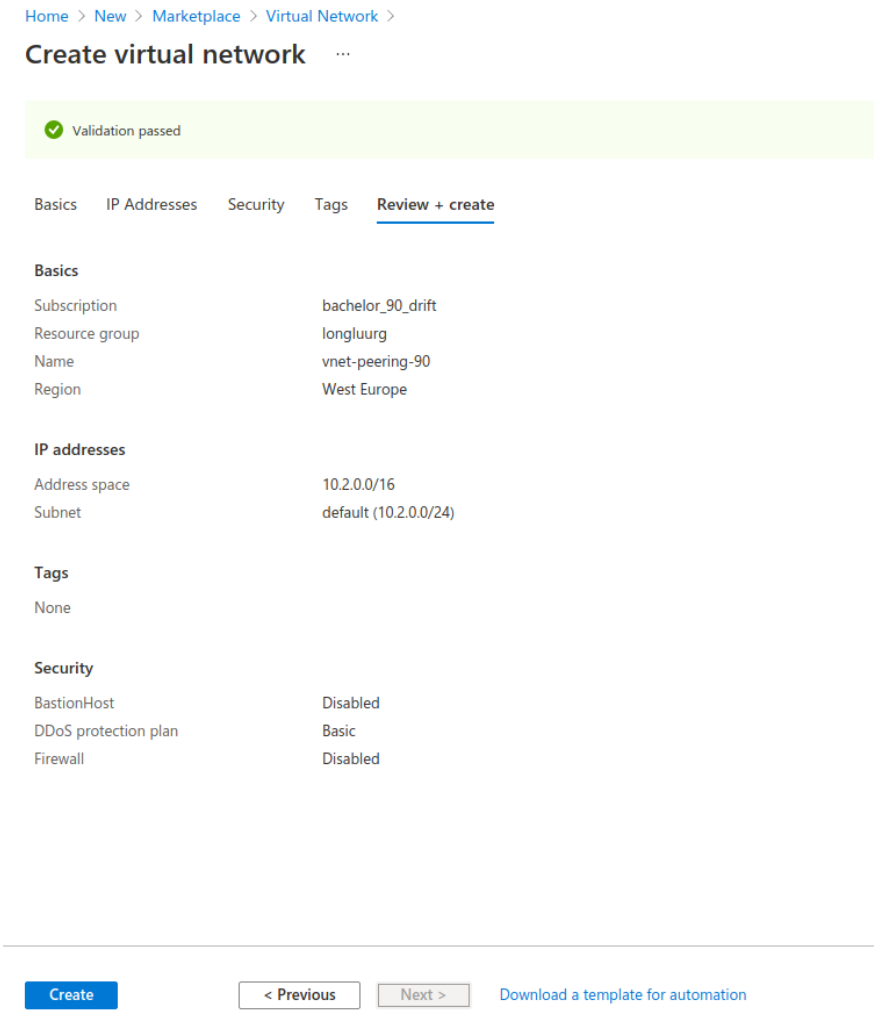
5.1.1.2. Vnet og peering



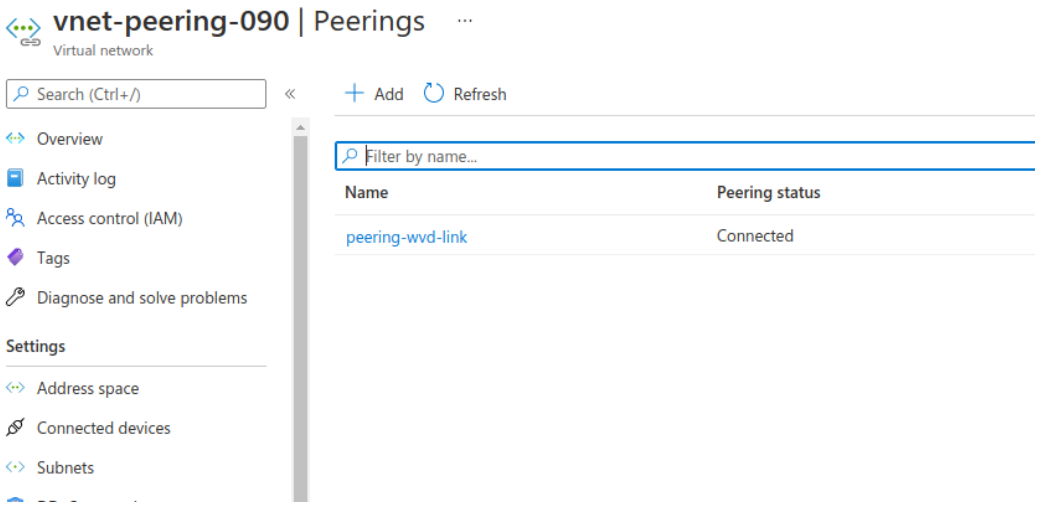
Neste steg i oppsettet er å opprette et virtuelt nettverk for de virtuelle maskinene. Dette melder vi inn i en ressursgruppe (hvor alt tilhørende de virtuelle maskinene legges). Vi gir det et navn og velger region.



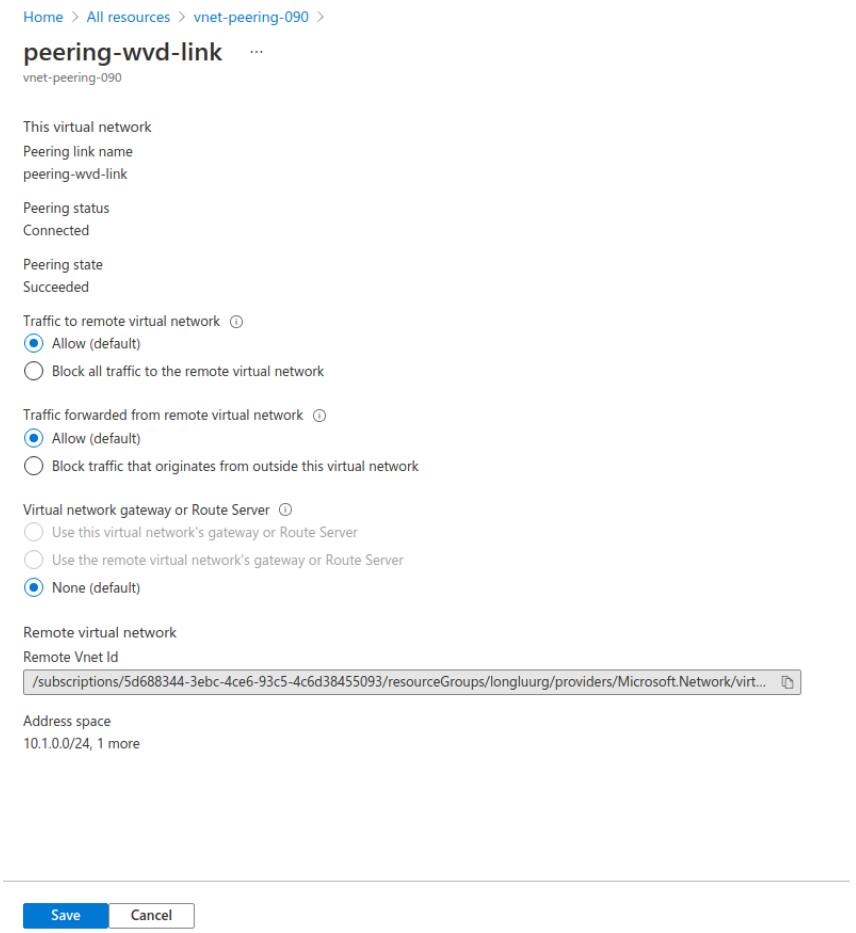
Vi velger adresseområde for det virtuelle nettverket og lar subnet stå som default.



Resten av innstillingene lar vi stå som de er og velger "Review + create" for å opprette nettverket.

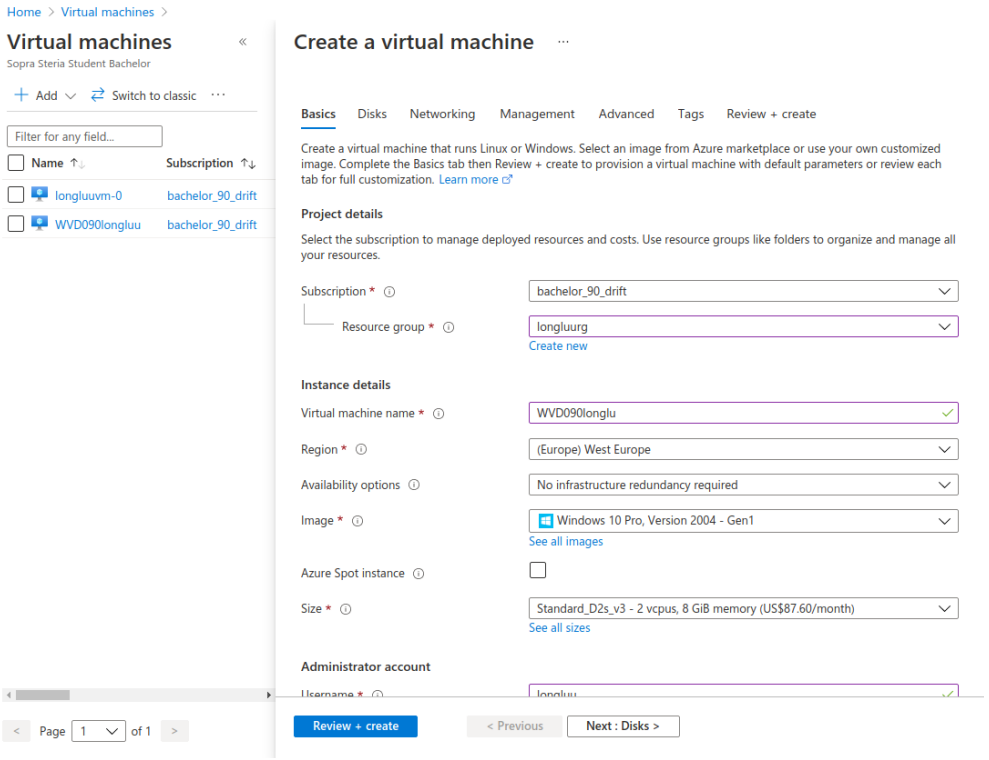


For å kunne melde maskinene inn i domenet er vi avhengig av at nettverket er koblet til og kan snakke med nettverket vi opprettet tidligere med AADDS. For å oppnå dette setter vi opp peering mellom nettverkene. Vi trykker "Add" og velger ønskede innstillinger.

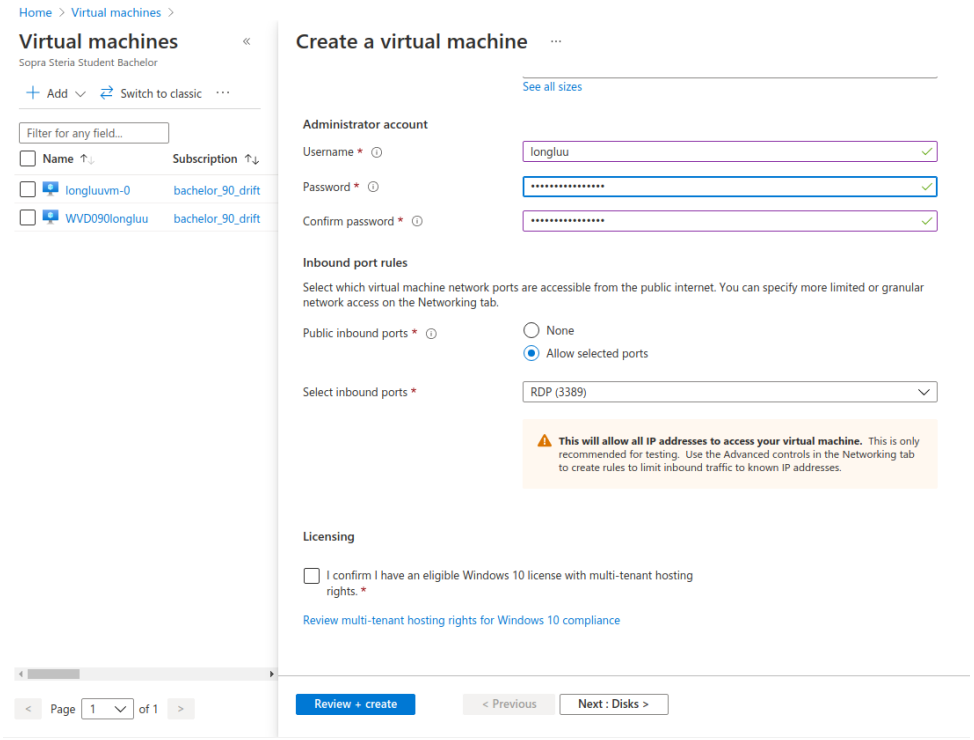


Vi gir peering-linken et navn og tillater trafikk til og fra det fjernstyrte virtuelle nettverket.

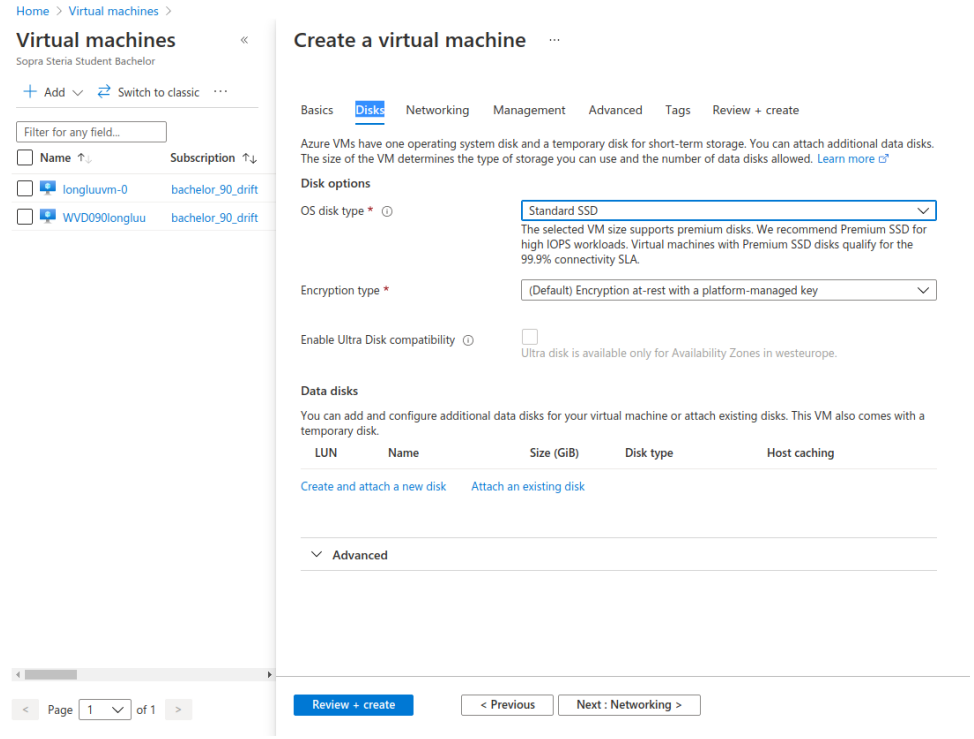
5.1.1.3. Oppsett av virtuell maskin



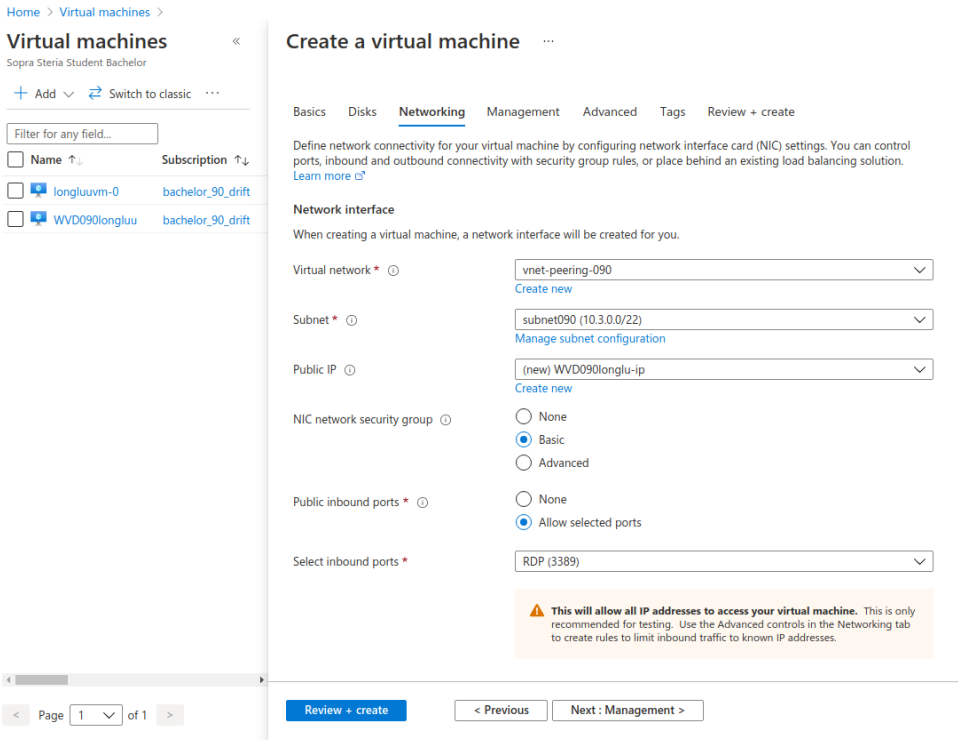
Her oppretter vi Windows 10 Pro virtuell maskin og kaller den for WVD090longlu under bachelor_90_drift-abonnementet.



Videre fyller vi inn brukerinformasjon for administrator og velger RDP tilkobling.



Ved "Disks" velger vi Standard SSD.

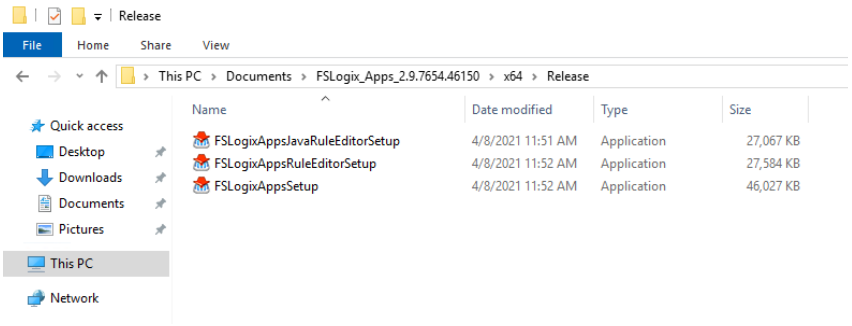


Her setter vi "Virtual network" til vnet-peering-090 og subnettet som vi opprettet tidligere. Dette nettverket kan altså snakke med nettverket til domenekontrolleren.

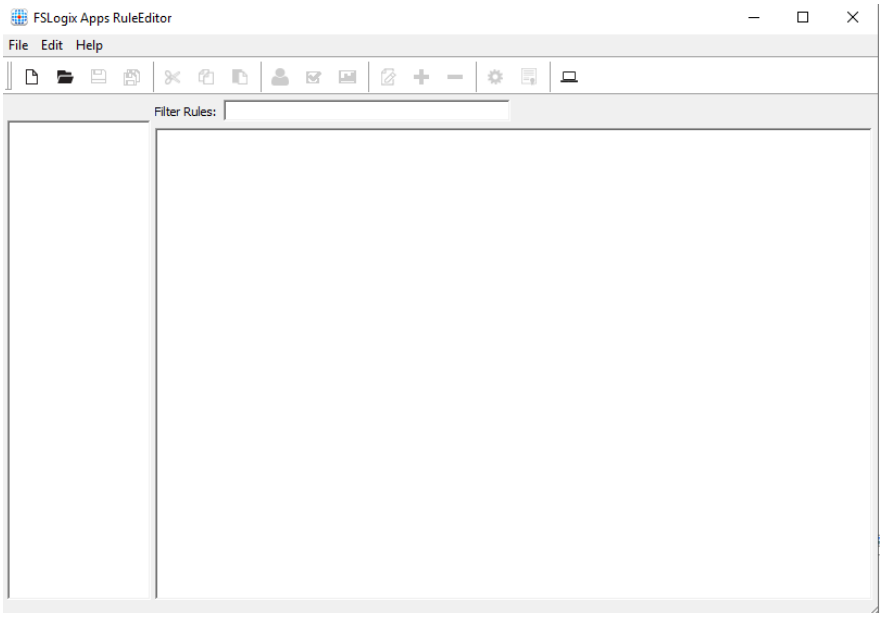
5.1.2. Oppsett av sikkerhetsfunksjoner

5.1.2.1. FSLogix

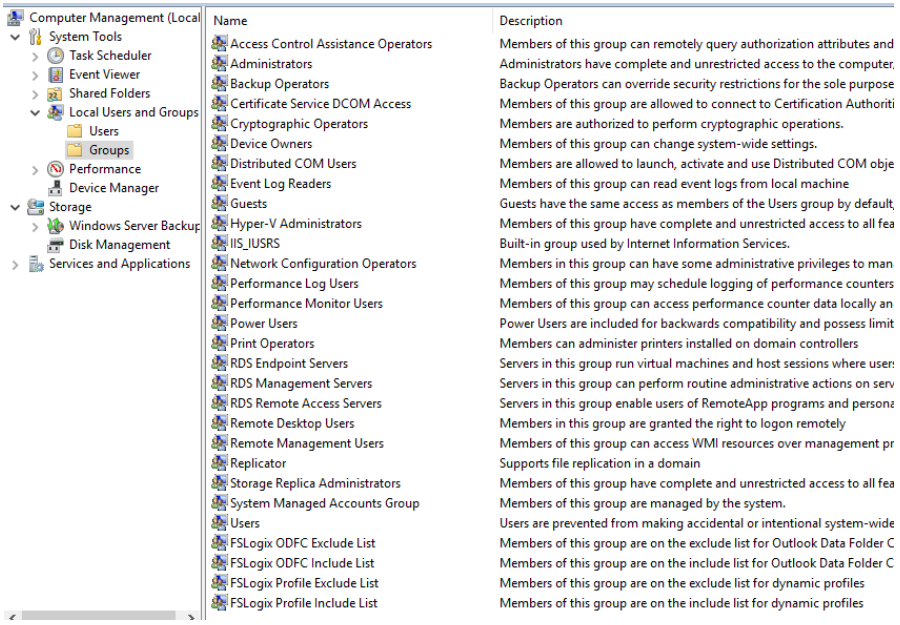
FSLogix lastes ned fra Microsofts nettside og installeres på ønsket maskin.



Her ser vi mappen med installasjonsfiler som lastes ned. FSLogix består av tre deler som kjøres og installeres hver for seg.



Etter installasjon kan tjenesten kjøres. Det er nå klart for å sette opp profile containers og egne regelsett for disse.



Man kan velge hvilke brukere som skal inkluderes i tjenesten, og hvilke som skal ekskluderes ved å legge de til i FSLogix Profile Exclude/Include List (nederst i listen på bildet over).

5.1.2.2. Reverse Connect

Reverse Connect er en tjeneste som er innebygd i alle WVD-maskiner. Det er derfor ikke nødvendig å utføre noe oppsett her.

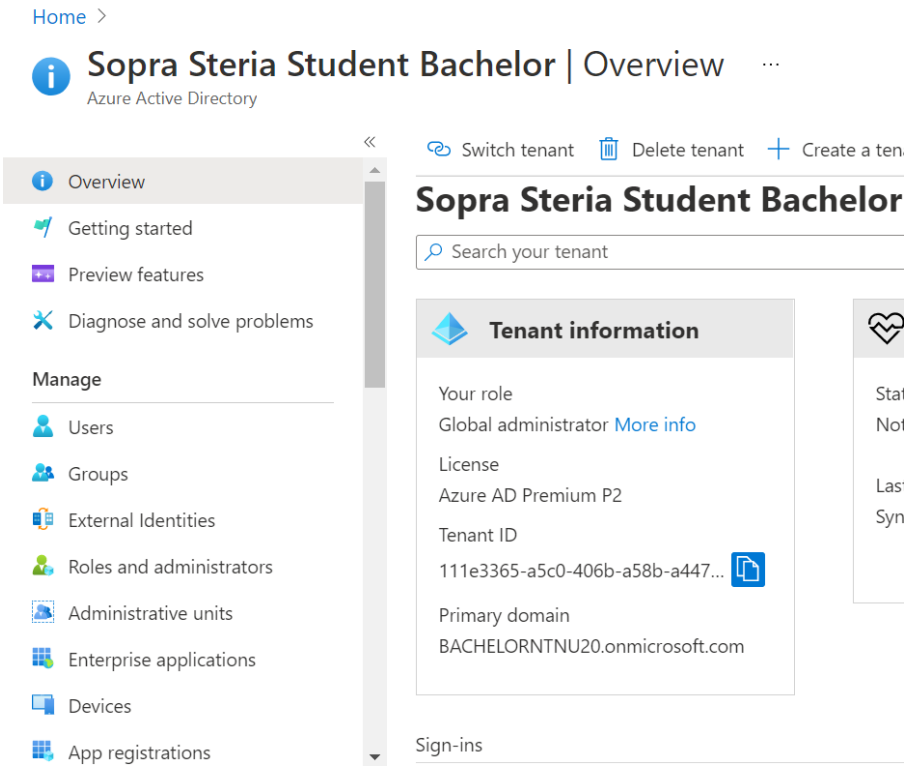
5.1.2.3. Multi-Factor Authentication

For at vi kan aktivere Multi-Factor Authentication i WVD, må vi oppfylle følgende forutsetninger:

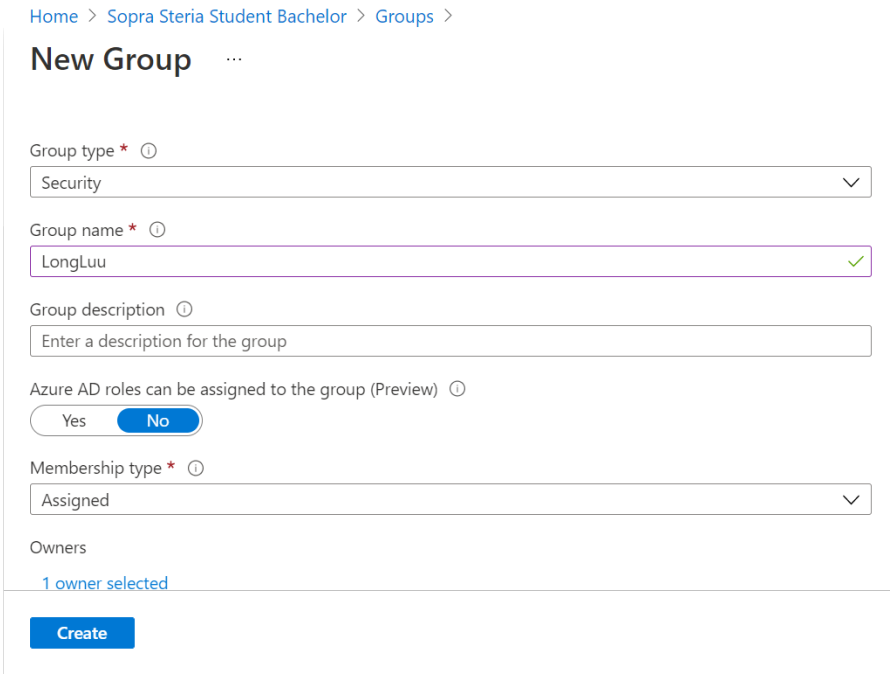
1. Tildele brukerne en lisens med Azure Active Directory Premium P1 eller P2.
2. Opprette en Azure Active Directory gruppe og legge til brukerne som gruppemedlem av gruppen.
3. Aktivere Azure Multi-factor authentication hos alle brukerne som er medlem i pkt. 2 (6).

5.1.2.3.1. Forutsetninger

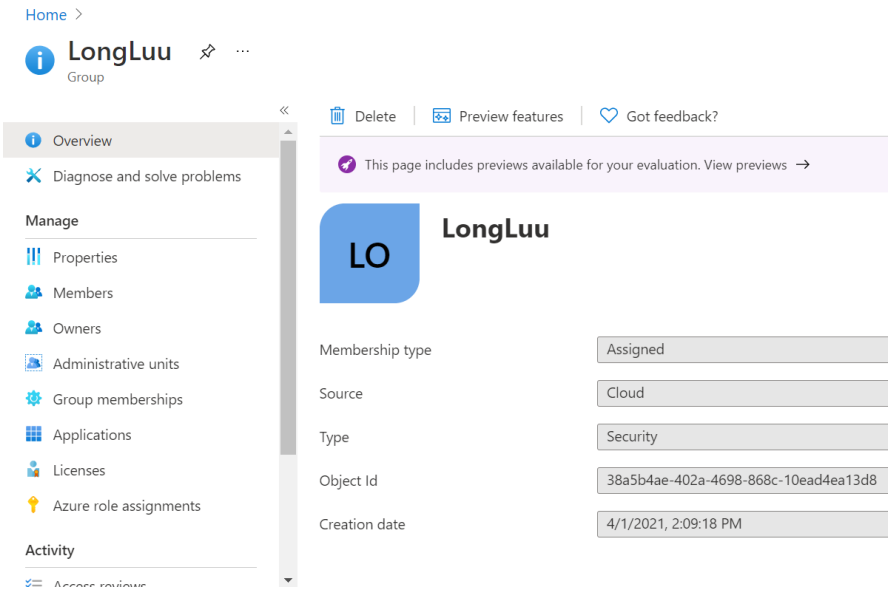
I denne delen setter vi opp punkt 2 og 3 av forutsetningene ovenfor for å aktivere Multi-Factor Authentication i Windows Virtual Desktop.



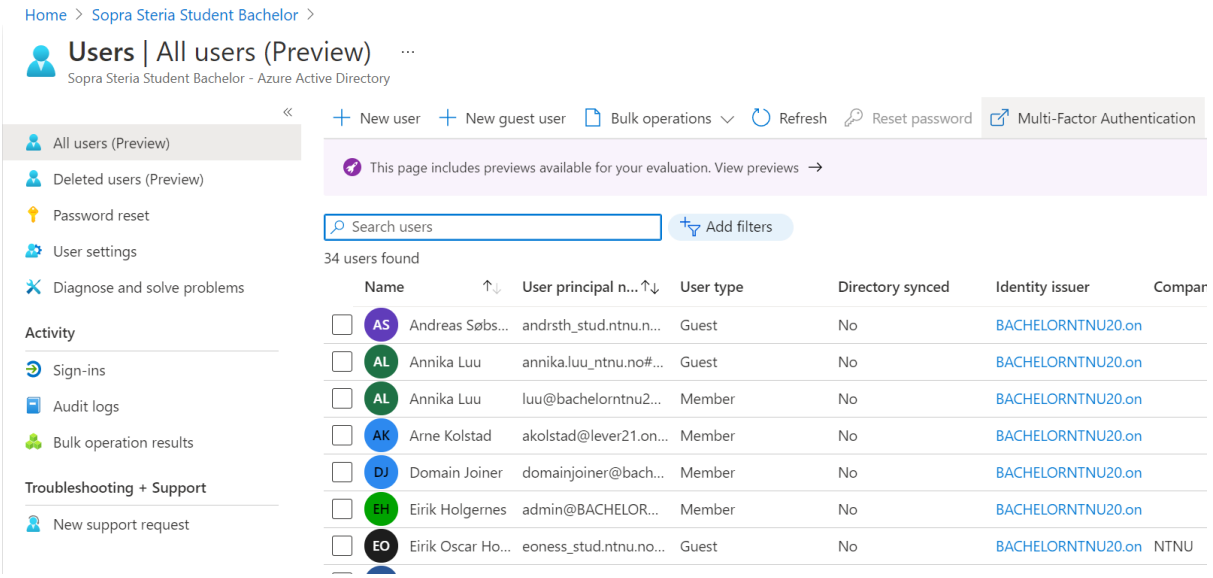
Forutsetning nr. 1 krever ikke oppsett, men tildeles av Sopra Steria. Vi ser at det er oppfylt under "Tenant information" i Azure AD.



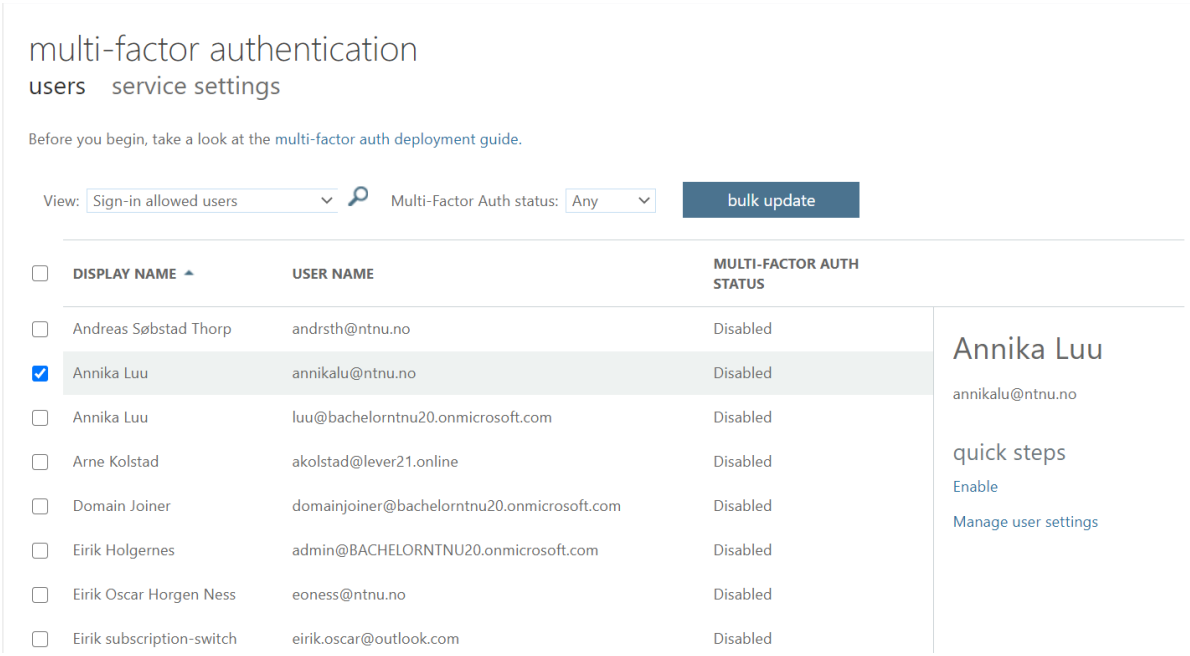
Forutsetning nr. 2 er å opprette en Azure Active Directory-gruppe. Her legger vi til medlemmer som krever en MFA-innlogging. Alle ansatte og administratorer i LongLuu må tilhøre til en gruppe med MFA-innstilling.



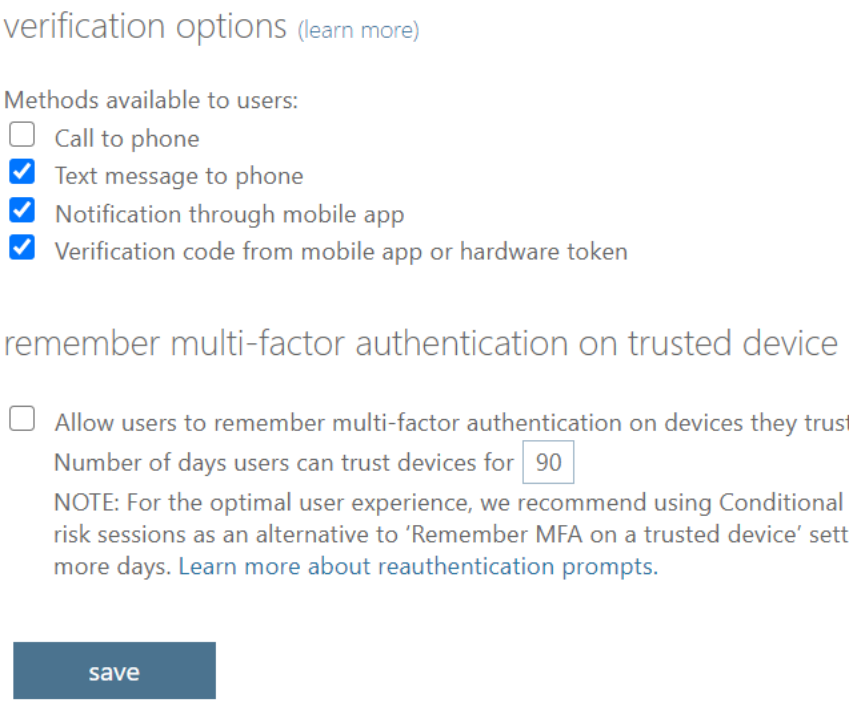
Gruppen er opprettet med følgende informasjon.



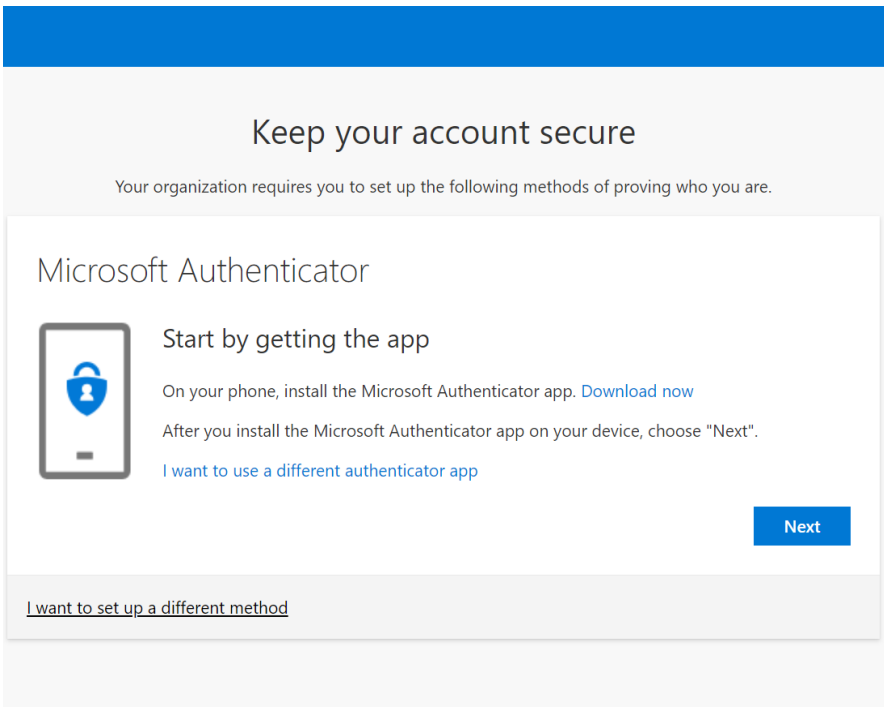
For å aktivere Azure multi-factor authentication velger vi "Users" i hovedmenyen i Azure Active Directory og klikker på "Multi-Factor Authentication" (15).



Her velger vi å teste ut en bruker og klikker på knappen "enable".

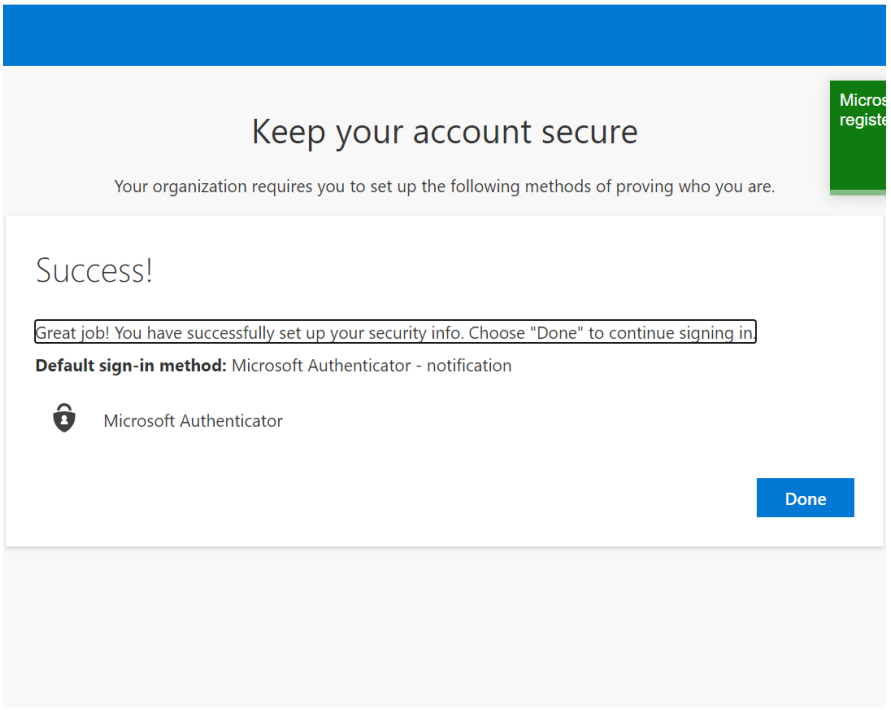


Vi klikker på "Service settings" for å velge ønskede alternativer.



Når testbrukeren logger inn, ber nettsiden om at vedkommende skal laste ned en mobilapplikasjon kalt "Microsoft Authenticator". Vedkommende kan legge til en konto ved å skanne en QR-kode.

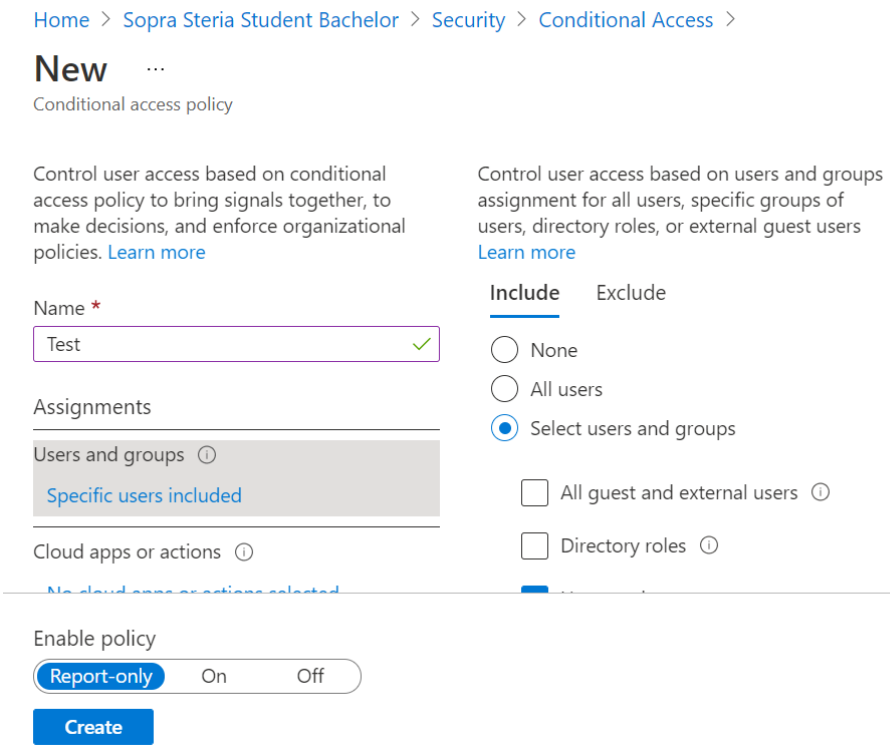
Brukeren kan deretter benytte seg av denne appen for å verifisere seg ved innlogging.



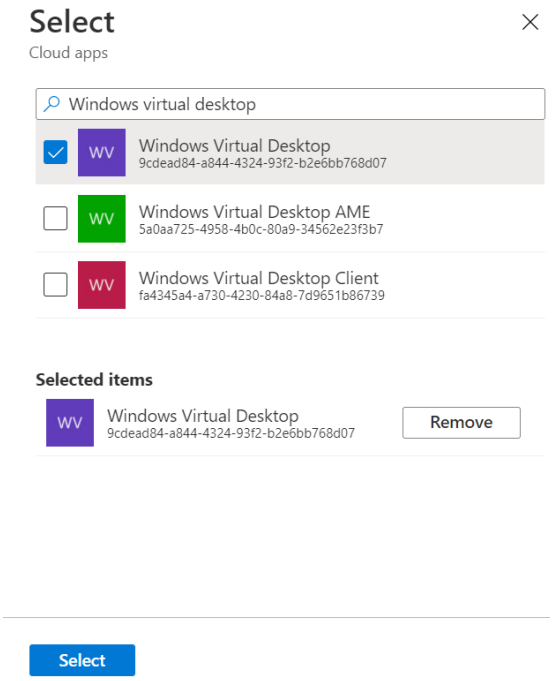
Etter registrering av konto og verifisering, får man bekreftelse om at oppsettet er vellykket.

5.1.2.3.2. MFA med Conditional Access

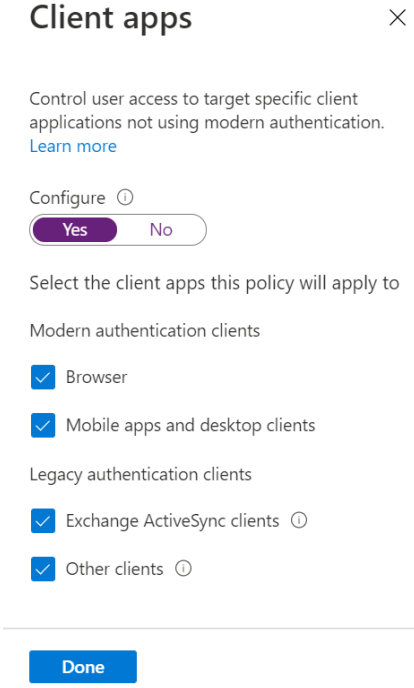
Videre setter prosjektgruppen opp Multi-Factor Authentication i Windows Virtual Desktop med Conditional Access. Dette gjøres i hovedmenyen i Azure AD. Her velger vi "Security" og deretter "Conditional Access" (6).



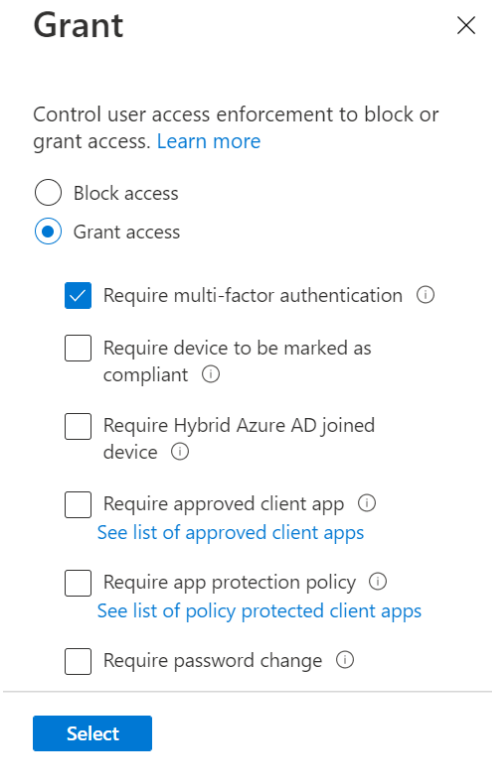
Her legger vi til den gruppen som ble opprettet i pkt. 5.1.2.3.1. og medlemmer det angår.



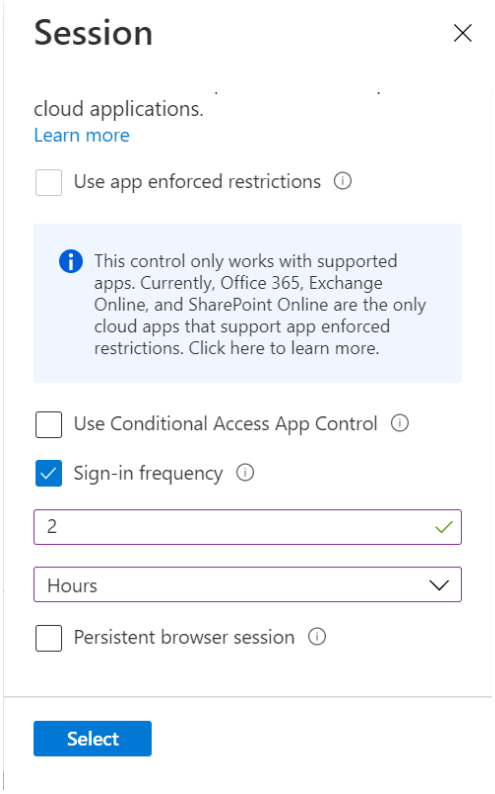
Ved Cloud apps velger vi WVD-applikasjonen og deretter "Select".



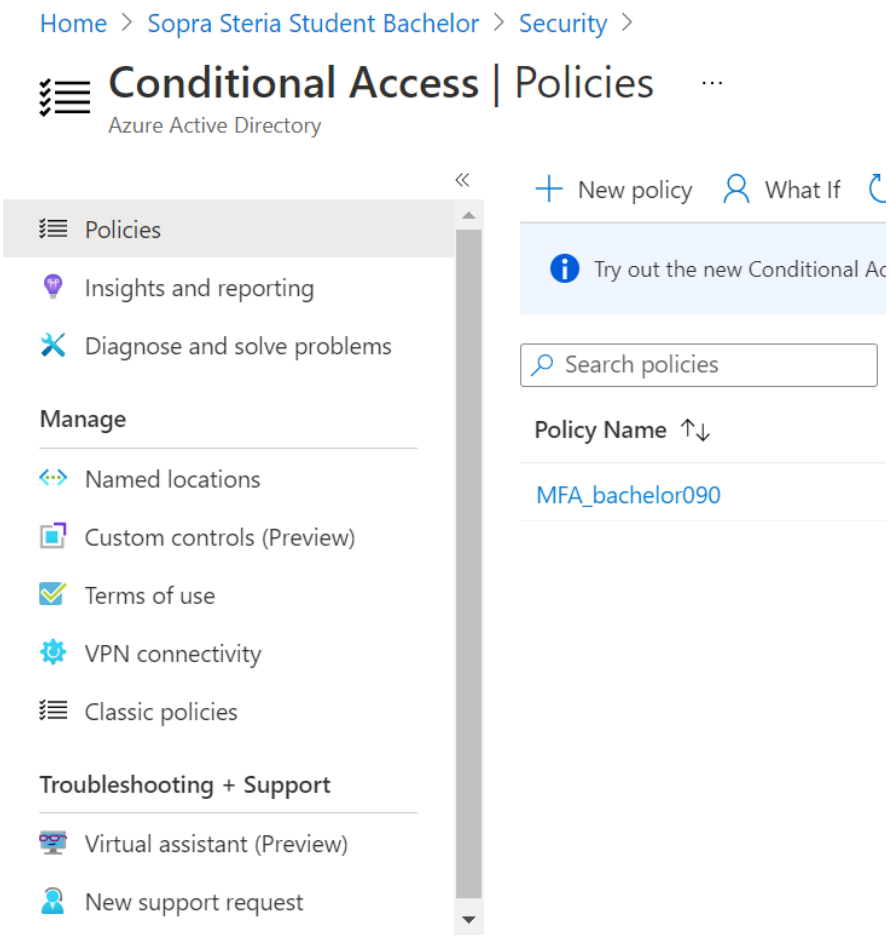
Ved Client apps velger vi å endre "Configure" til "Yes".



Vi velger "Grant access" og huker av "Require Multi-Factor Authentication".

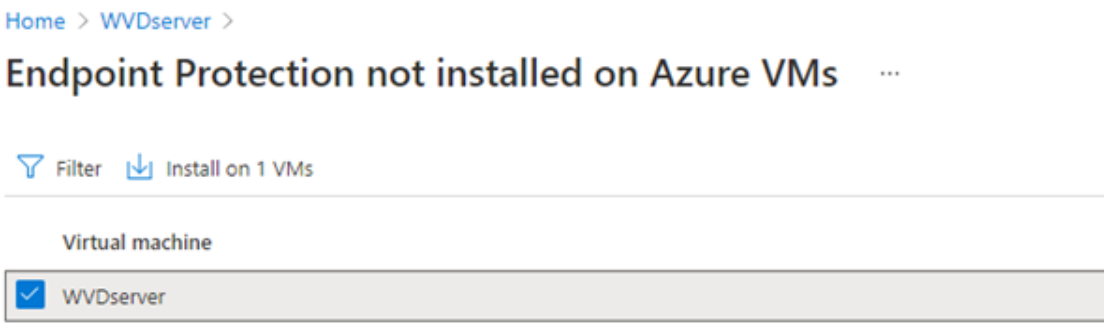


Så tildeler vi "Sign-in frequency". I dette tilfellet er det satt til to timer.

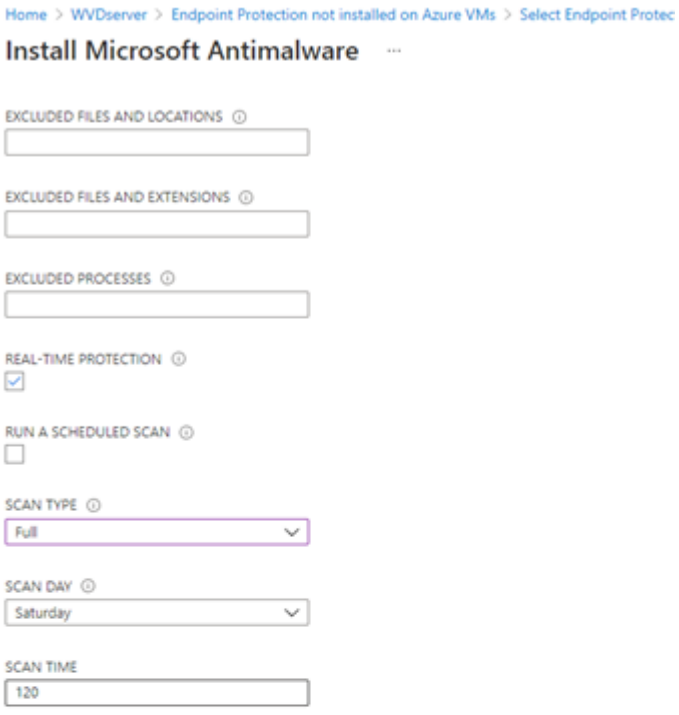


Her finner vi Conditional Access-retningslinjen. Alle ansatte og administratorer i LongLuu må verifisere seg for å logge på brukeren sin.

5.1.2.4. Endpoint Protection



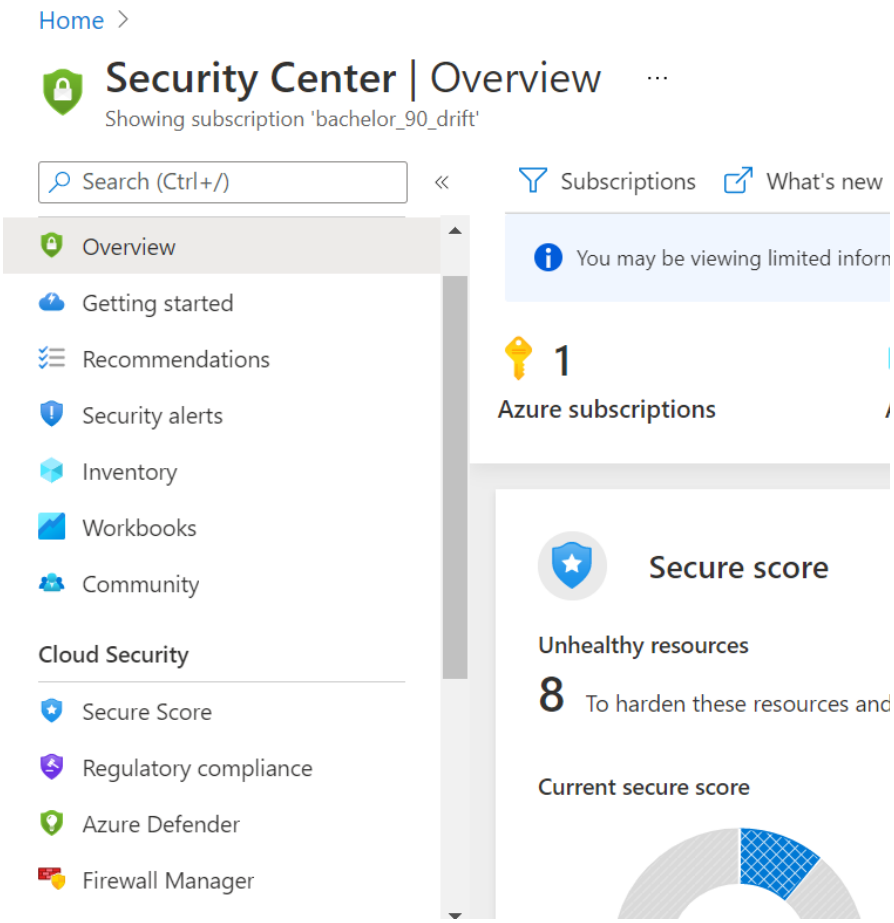
For å sette opp Endpoint Protection på virtuelle maskiner går vi inn på "Advisor Recommendations". Her blir vi varslet om at det er anbefalt å sette opp denne funksjonen dersom den ikke allerede er konfigurert. Vi får da mulighet til å installere dette via Azure.



Vi blir bedt om å velge hvilken type skanning vi ønsker og når denne skal kjøres, og ruller ut funksjonen.

5.1.2.5. Azure Security Center

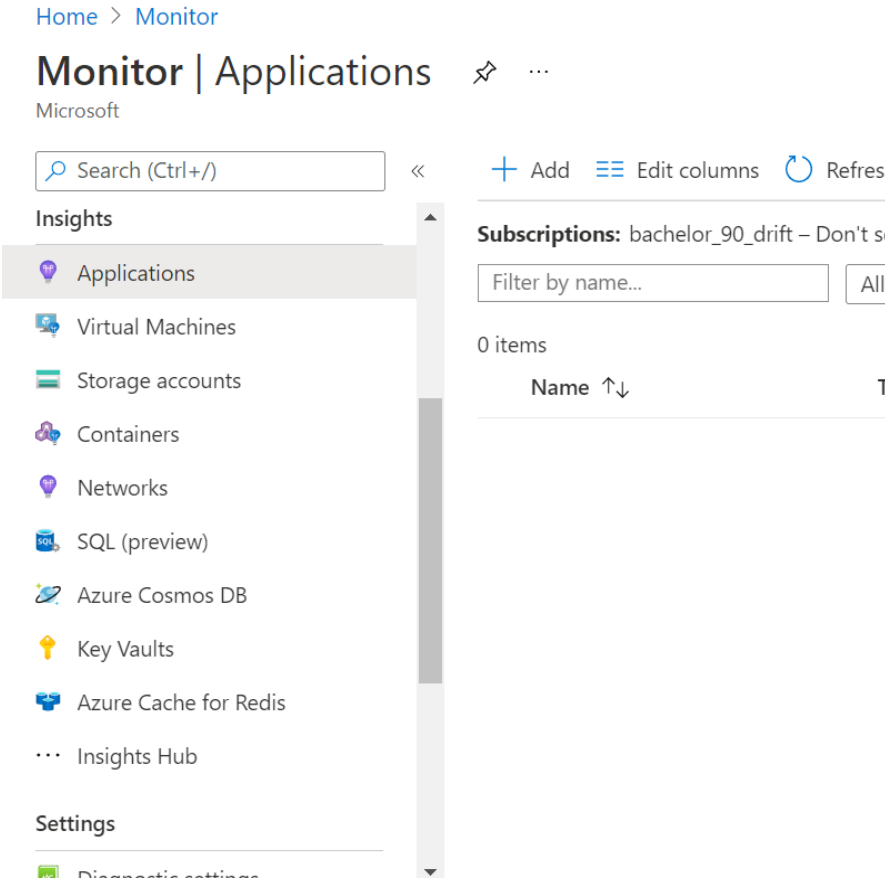
Azure Security Center er et sikkerhetsstyringssystem i Azure portalen. Det er ikke nødvendig å gjøre noe oppsett her, men vi må aktivere tjenesten på følgende måte:



Vi aktiverer Azure Security Center ved å søke "Security Center" og velge upgrade.

5.1.2.6. Azure Monitor

Azure Monitor er et innebygd system for overvåking av Azure-miljøet. Denne funksjonen søkes opp i portalen og krever ikke at vi utfører noe oppsett. I hovedmenyen får vi tilgang på de ulike insights-ene som finnes (se bilde under).

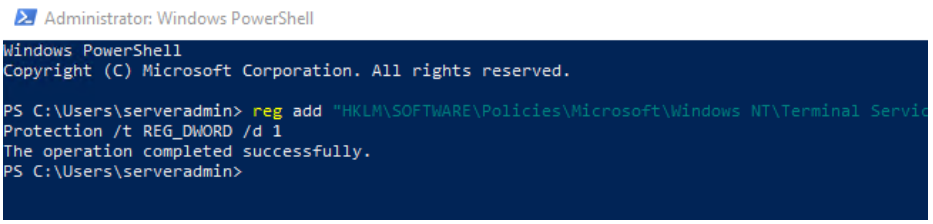


5.1.2.7. Screen Capture Protection

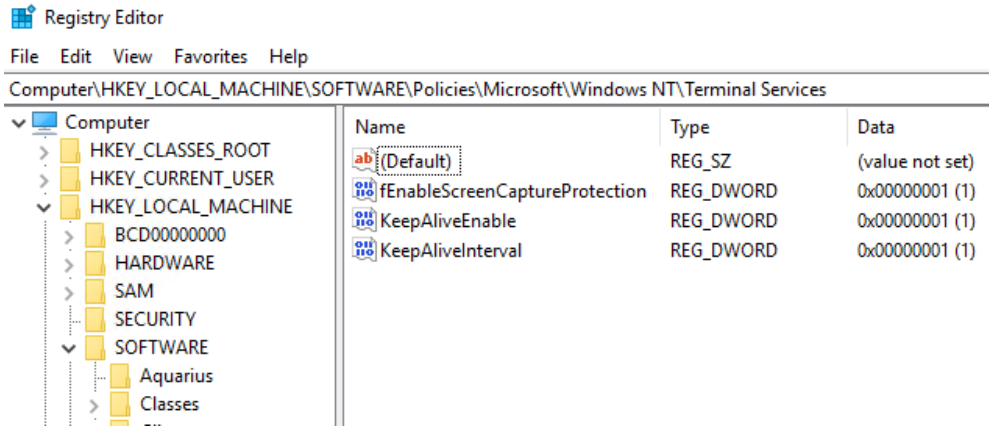
For å sette opp Screen Capture Protection må vi først legge til en regel som tillater tjenesten. Dette kan gjøres i PowerShell.

```
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services" /v fEnableScreenCaptureProtection /t REG_DWORD /d 1
```

Vi kjører kommandoen.



Nå er regelen lagt til. Vi kan åpne Registry Editor for å se dette.



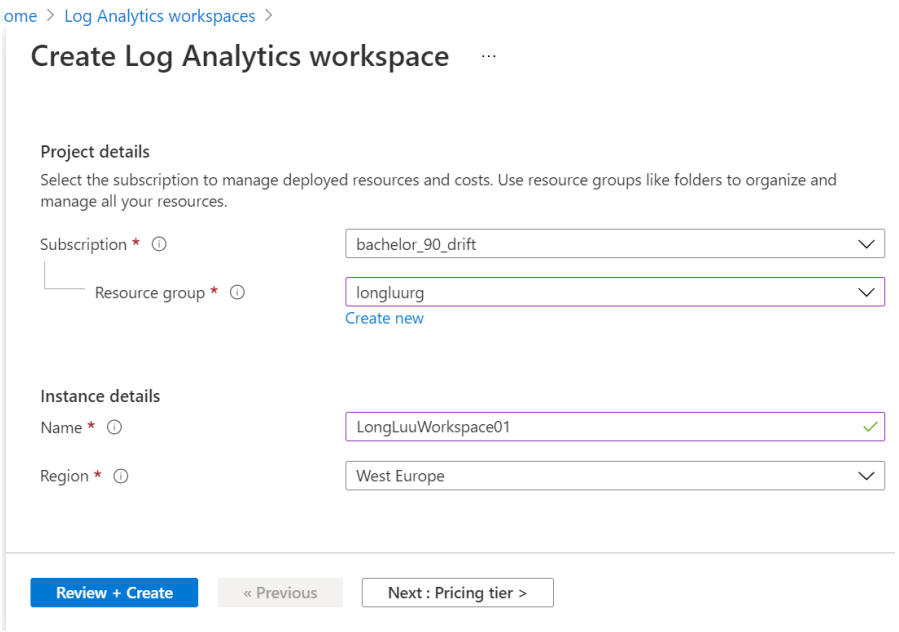
Vi ser at "EnableScreenCaptureProtection" er lagt til under Terminal Services.

5.1.2.8. Azure Sentinel

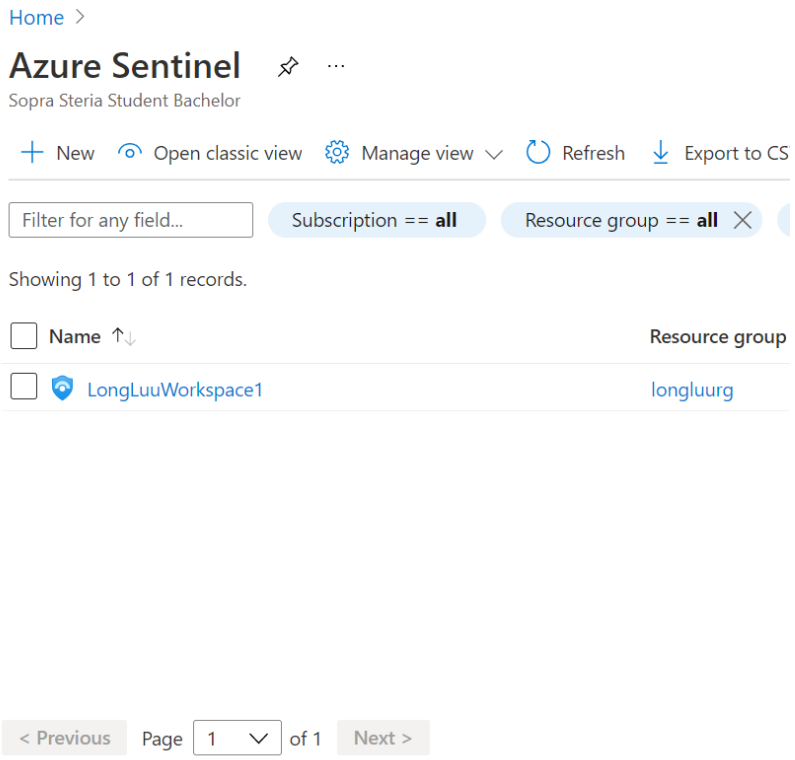
Azure Sentinel er en Security Information Event Management (SIEM) og Security orchestration automated response (SOAR)-løsning. Vi benytter Azure Sentinel for innsamling av audit logs som ble nevnt i designrapporten.

Her har vi tre globale forutsetninger:

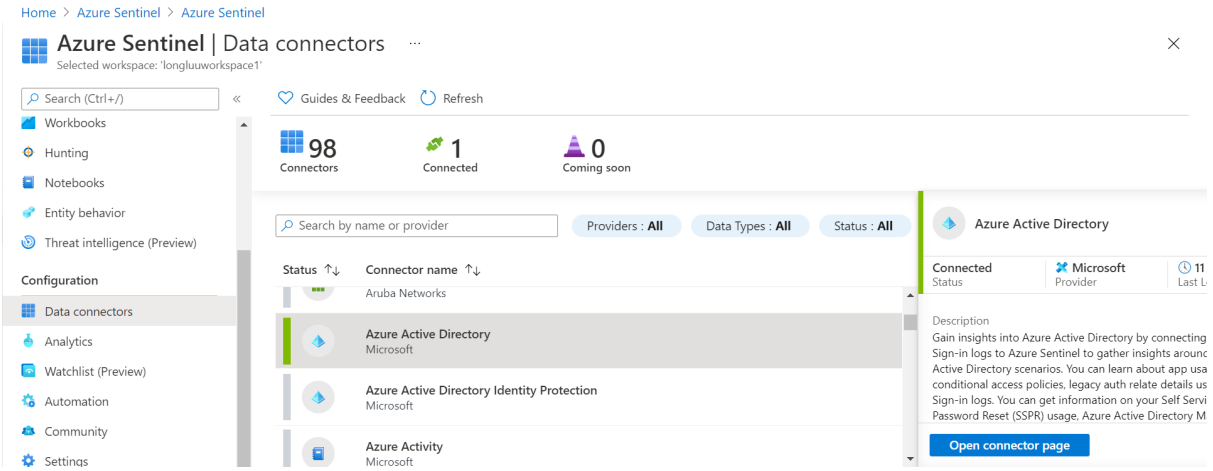
1. Vi har en aktivt Azure-abonnement der man har en "contributor" rettigheter til Azure-abonnementet og "contributor" eller leserettigheter på ressursgruppen.
2. Vi har en Log Analytics workspace (16).
3. Andre rettigheter kan være nødvendig for tilkobling av datakilder.



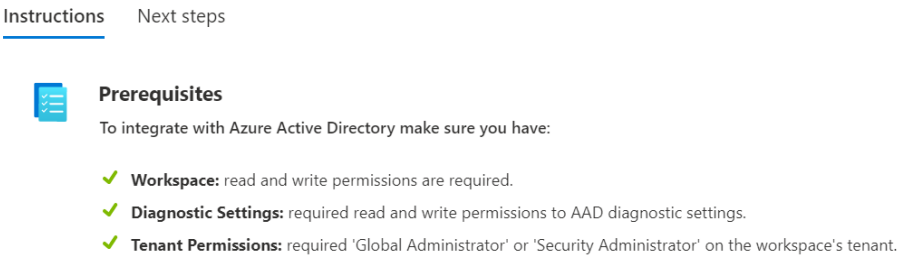
For å aktivere Azure Sentinel trenger vi å opprette en "Log Analytics workspace". Her oppretter vi en workspace for ressursgruppen, longluurg og kaller den for LongLuuWorkspace1.



I Azure Sentinel legger vi til LongLuuWorkspace1.

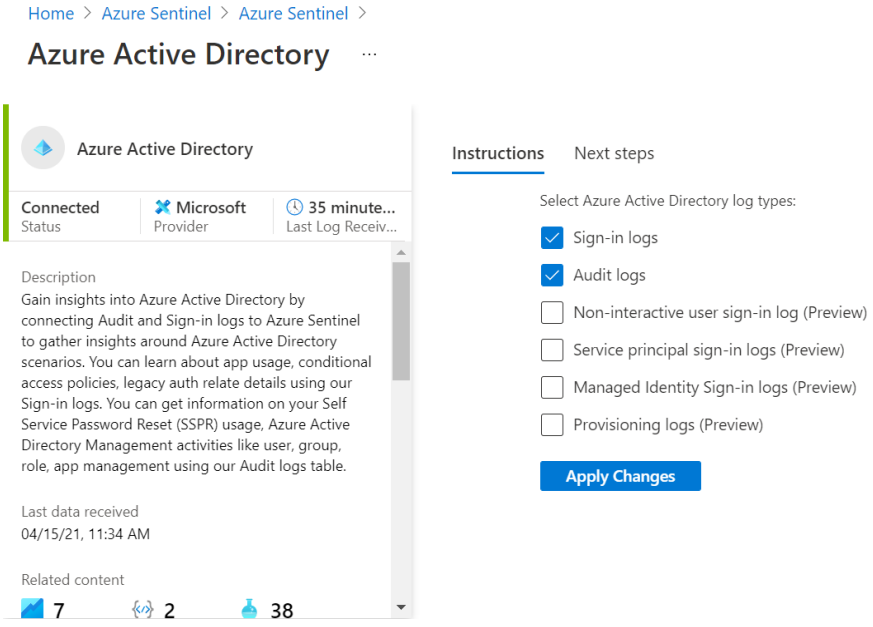


I figuren over velger vi ønsket datakilde, som i dette tilfellet er "Azure Active Directory", og deretter "Open connector page".

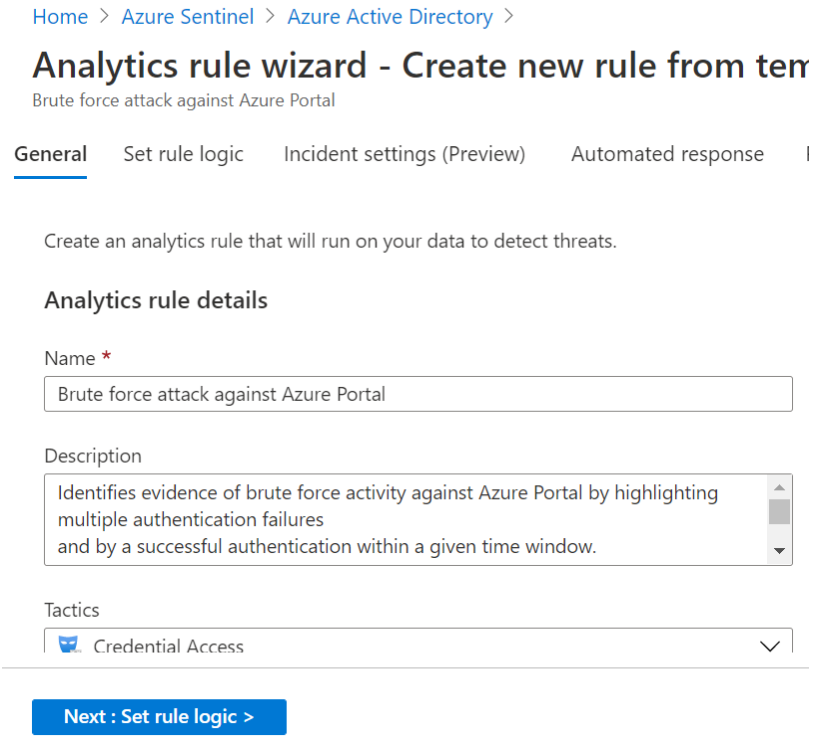


Her har vi tre forutsetninger for å koble til denne datakilden:

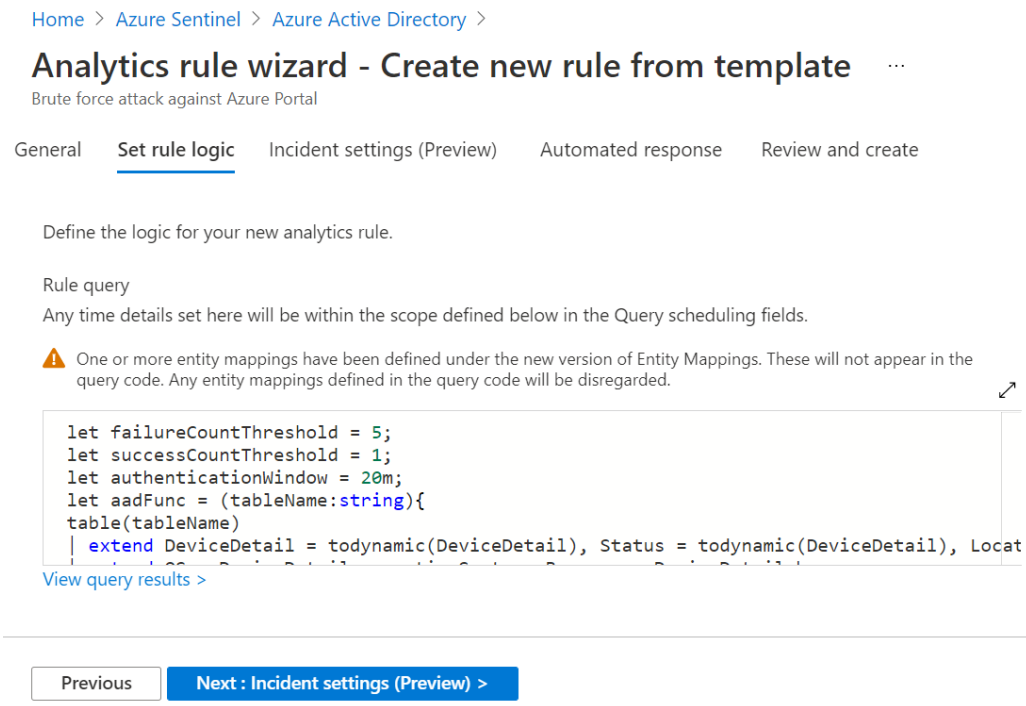
1. *Lese- og skrivetilgang til arbeidsområdet.*
2. *Lese- og skrivetilgang til AAD diagnostic settings.*
3. *Har enten "Global Administrator"-rolle eller "Security Administrator"-rolle i tenant-en.*



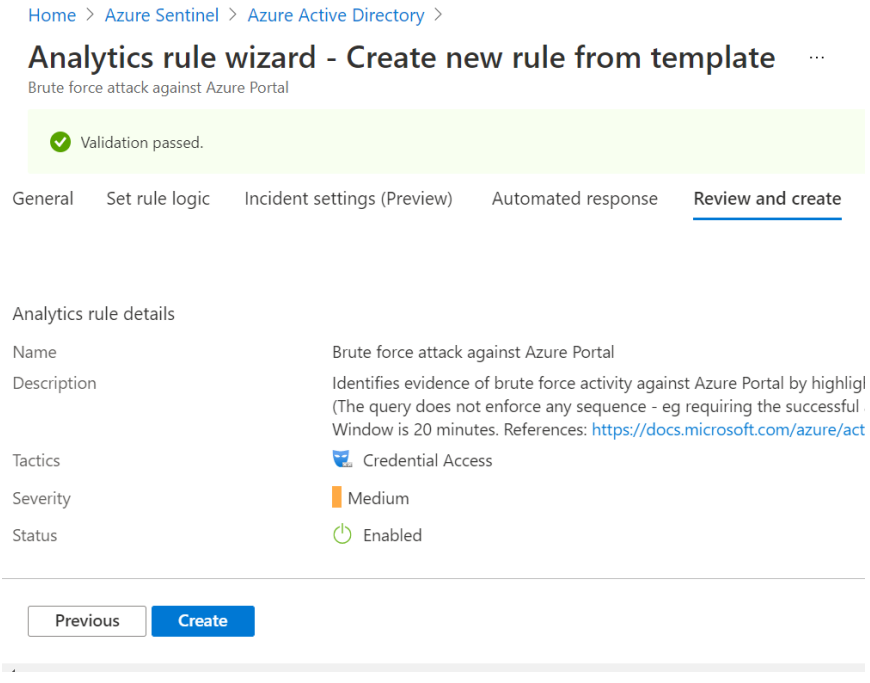
Vi huker av "Sign-in logs" og "Audit logs", og velger "Apply Changes". Vi ser at statusen er endret til "Connected".



Etter tilkobling av datakilden kan vi velge å opprette nye regler. Her velger vi "Brute force attack against Azure Portal". Denne regelen skal identifisere bevis på brute-force-aktivitet mot Azure-portalen. Dette gjøres ved å markere flere autentiseringsfeil innen et gitt tidsperspektiv.



Her ser vi scriptet til regelen.

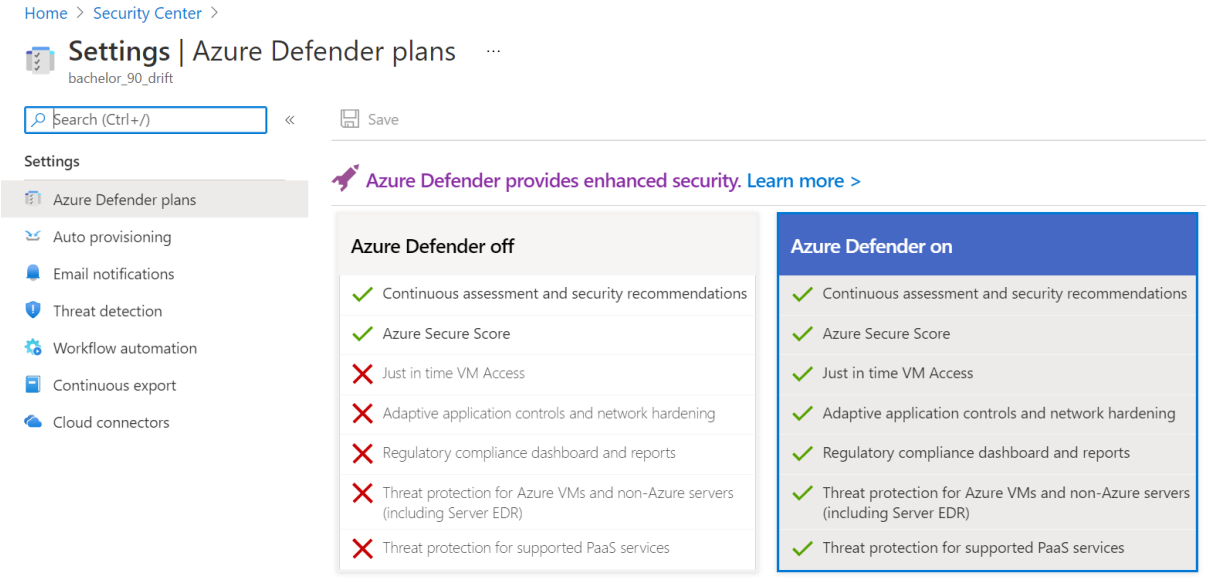


Etter at valideringen er gjennomført kan vi velge "Create".

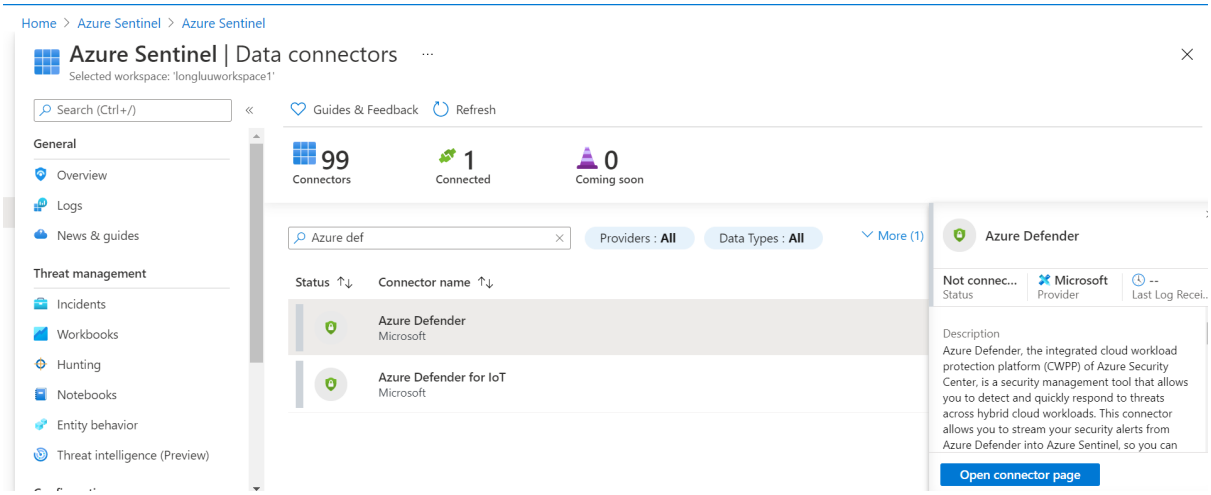
5.1.2.9. Integrasjon av Azure Security Center med Azure Sentinel

Vi integrerer Azure Security Center med Azure Sentinel og oppnår et resultat som tilsvarer en Security Operations Center (SOC). Det er to forutsetninger for å integrere Azure Security Center med Azure Sentinel (13):

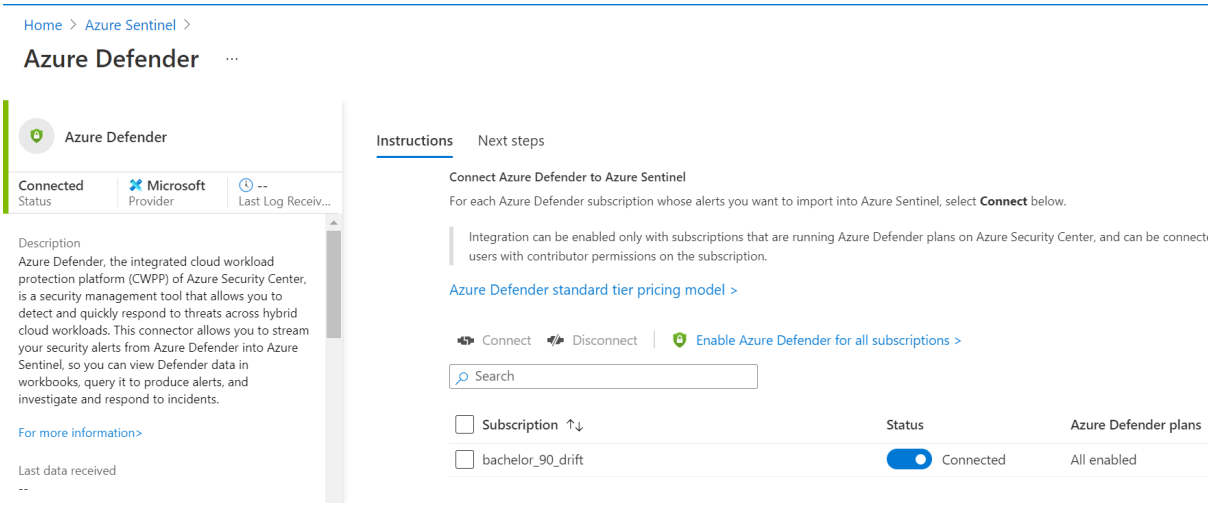
1. En bruker med Security Reader rolle av Azure abonnement.
2. Aktivere Azure Defender i Azure Security Center.



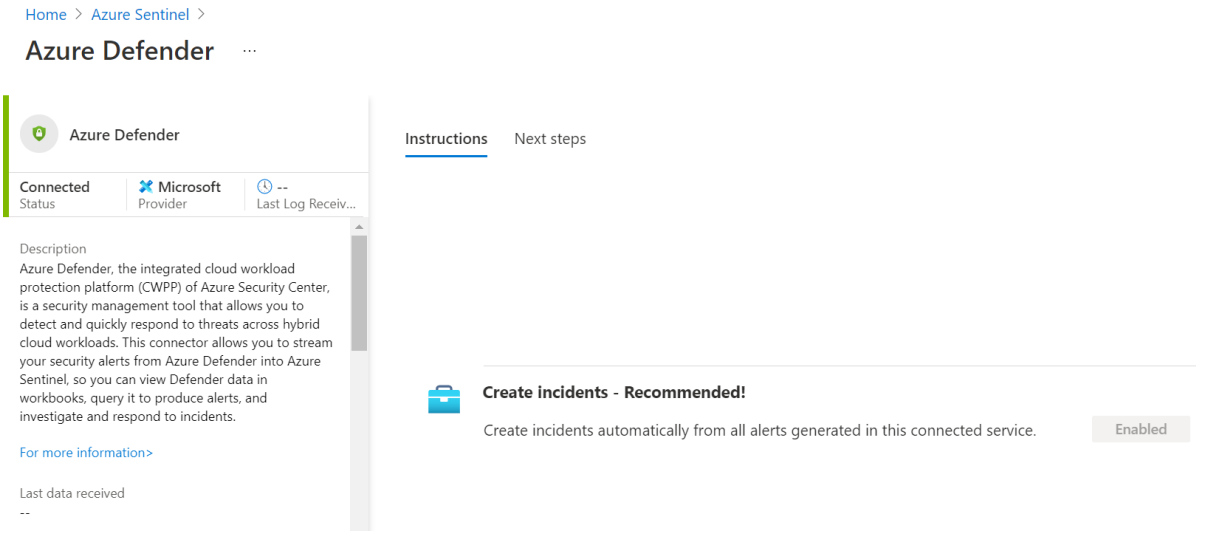
Vi går inn på Security Center, "pricing and setting" og velger det tilhørende abonnementet. Her ser vi at Azure Defender er aktivert.



Videre går vi til Azure Sentinel, "Data connectors" og søker opp "Azure Defender". Vi klikker på "Open connector page".



Vi velger det rette abonnementet og trykker på "Connect"-knappen.

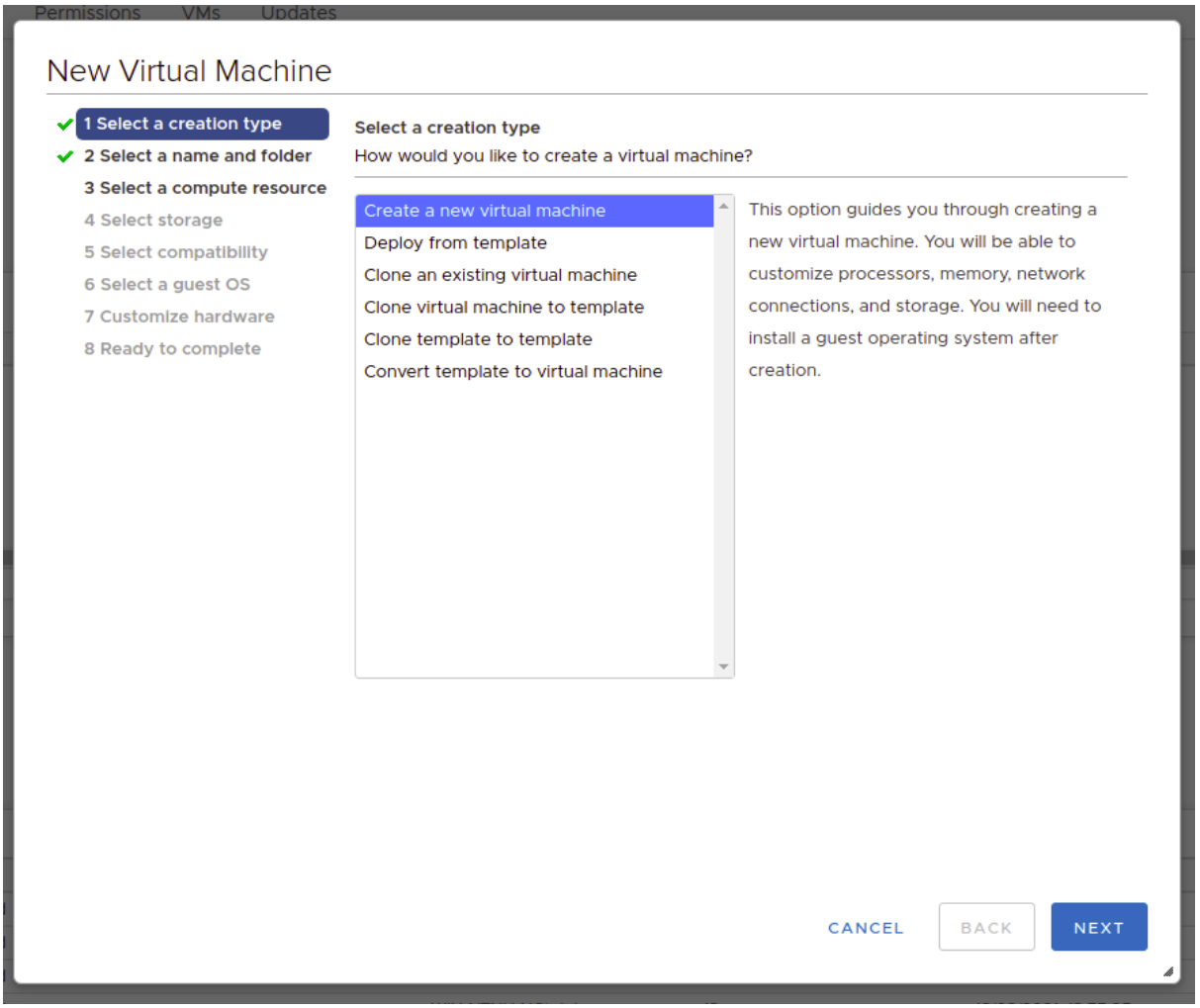


Ved "Create Incidents" velger vi aktivér-knappen for å slå på en standard funksjon som automatisk oppretter Incidents fra varsler.

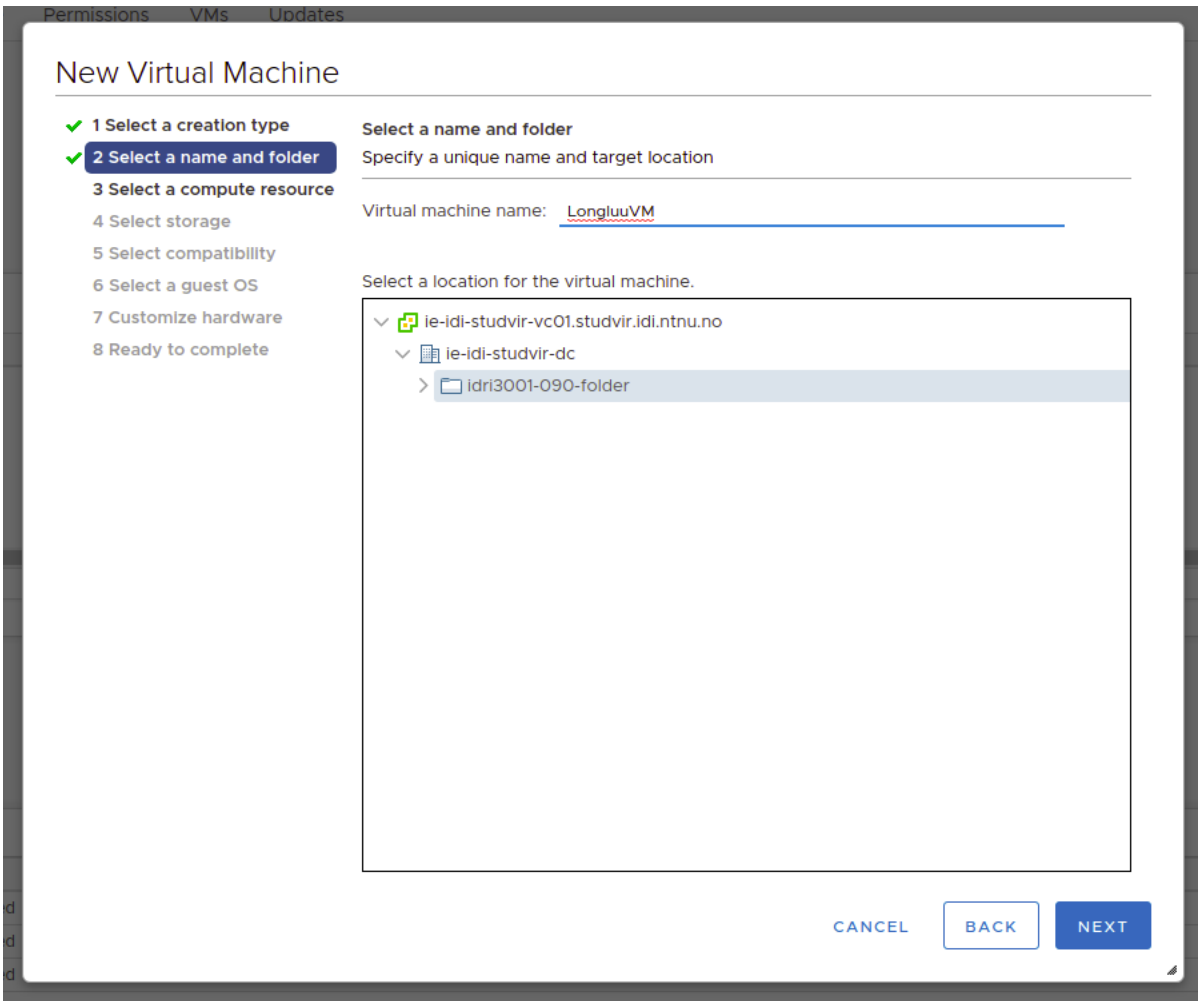
5.2. VMware vSphere

Prosjektgruppen skal opprette et testmiljø i VMware vSphere, disponeres av NTNU, for å undersøke sikkerhetsfunksjoner i virtualiseringstjenesten.

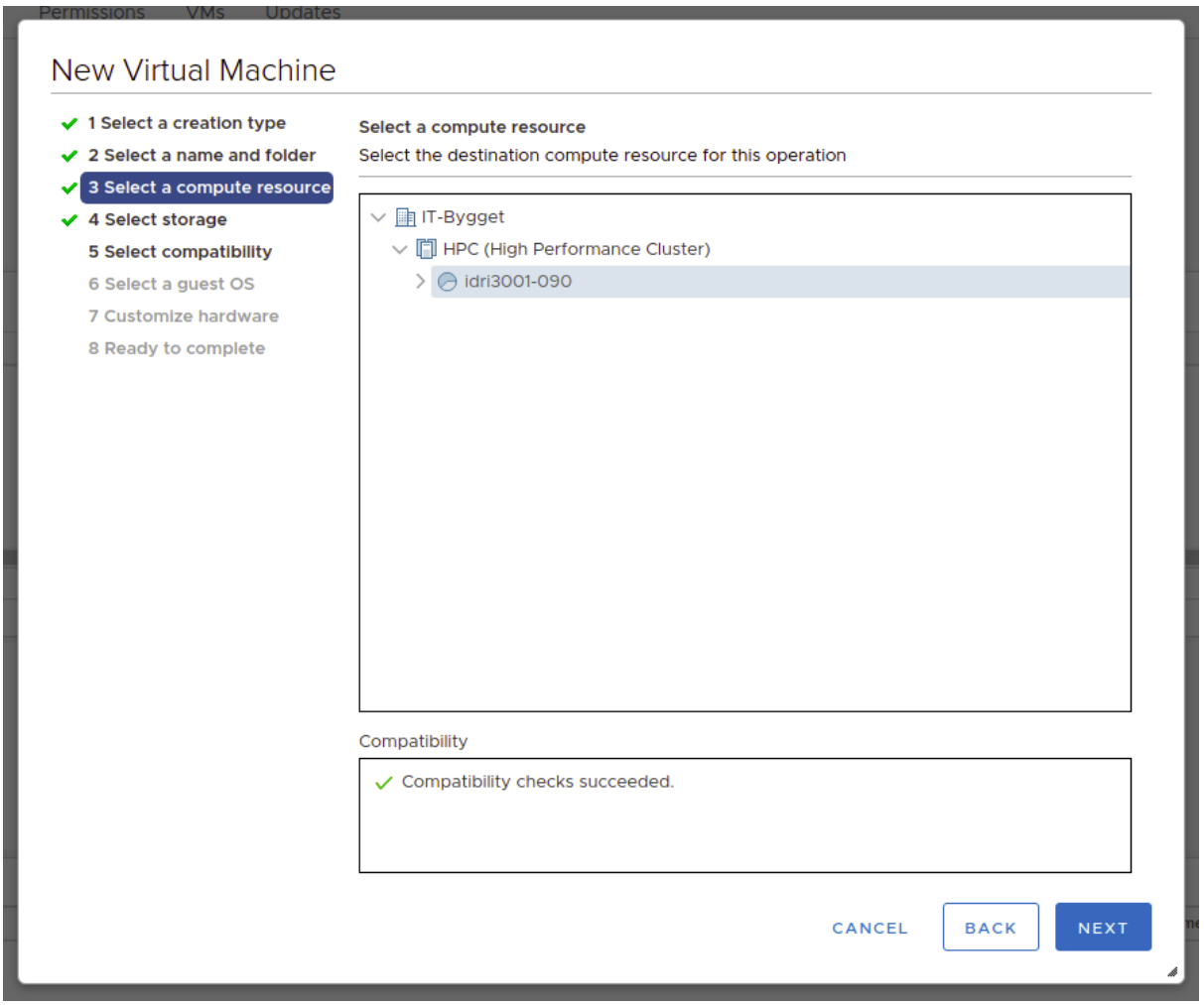
5.2.1. Oppsett av virtuell maskin



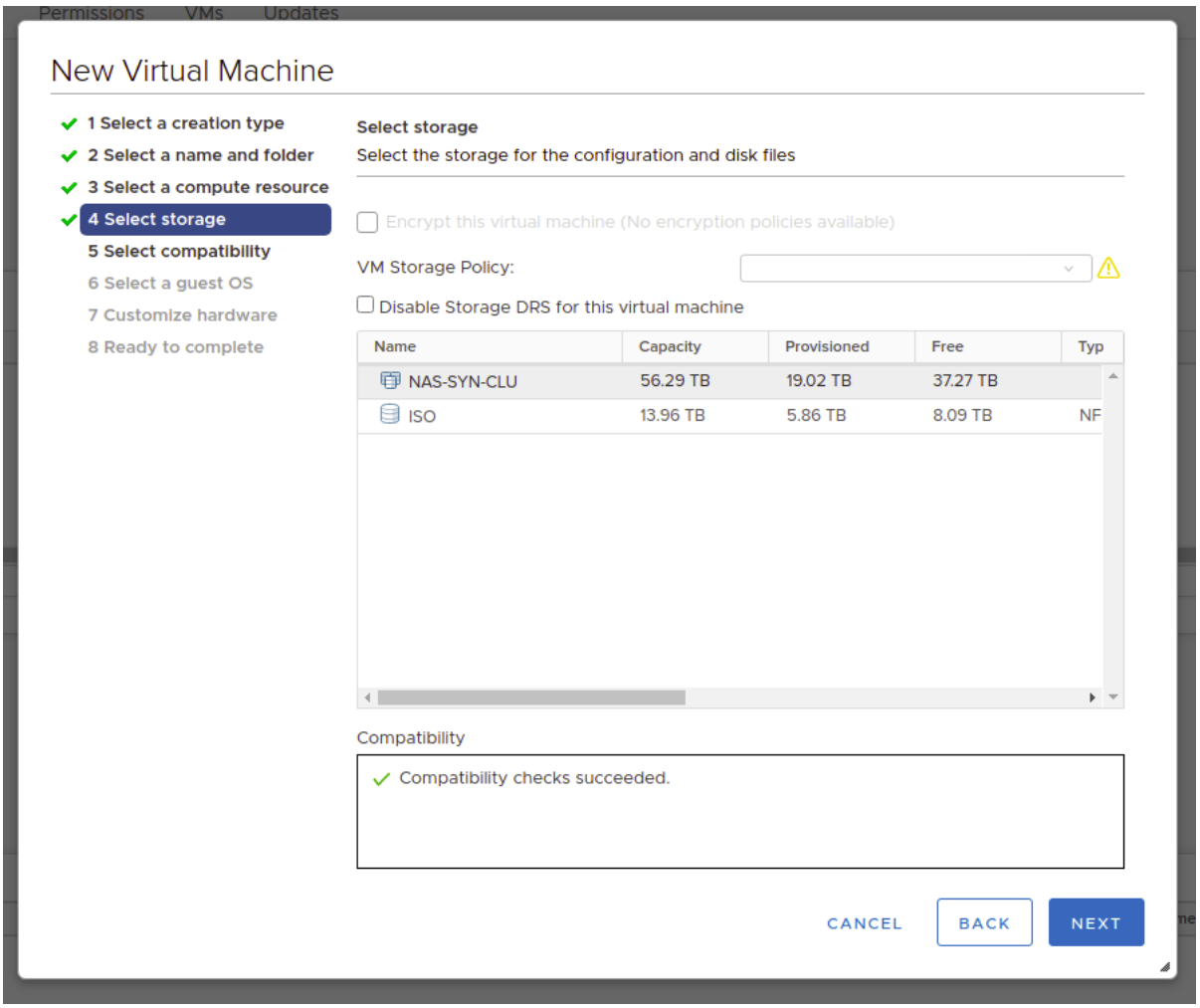
I vSphere Client opprettes en mappe for virtuelle maskiner. Her velger vi "Create a new virtual machine" og får opp som følgende.



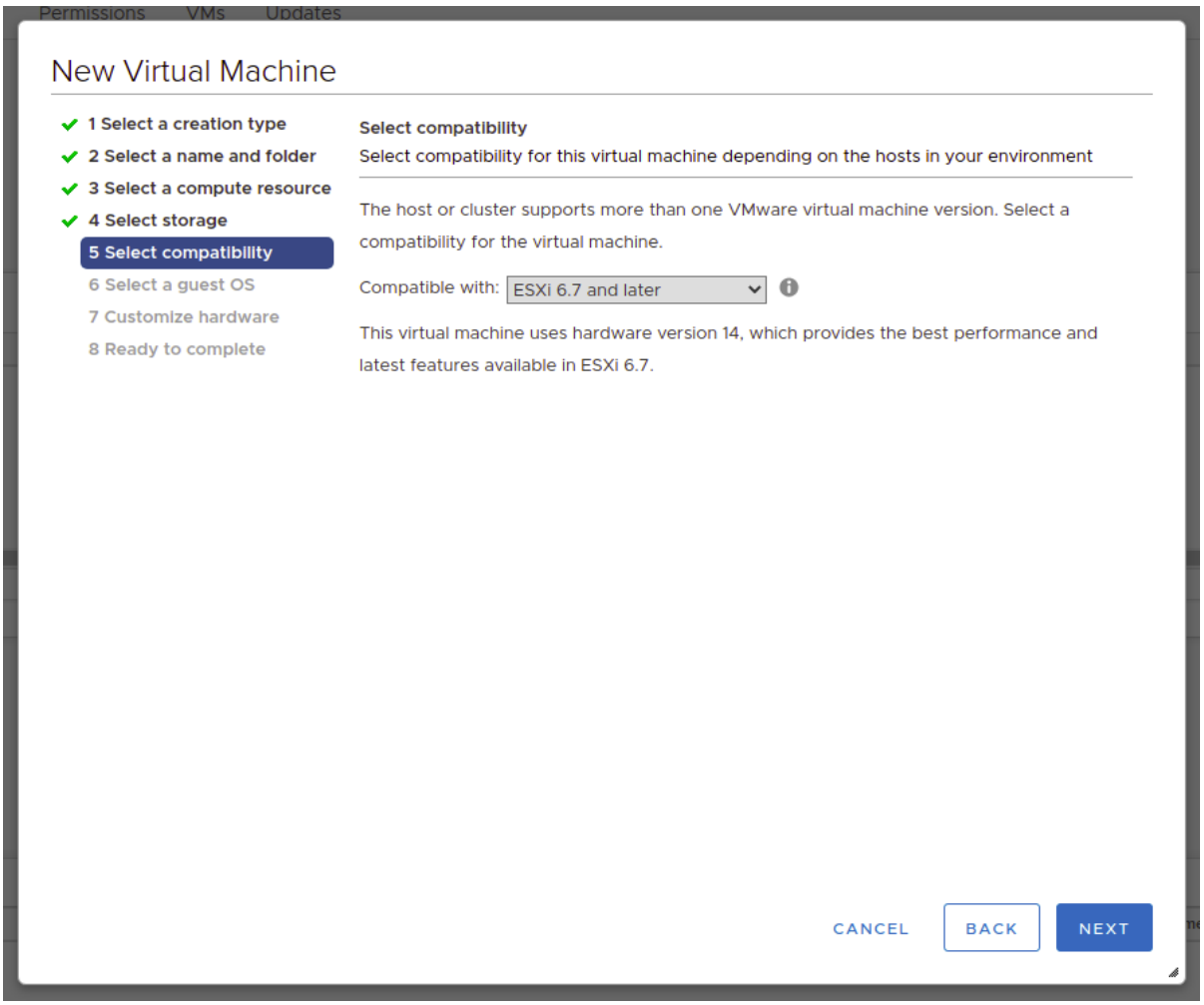
Vi gir maskinen et navn og velger mappen som ligger under domenekontrolleren.



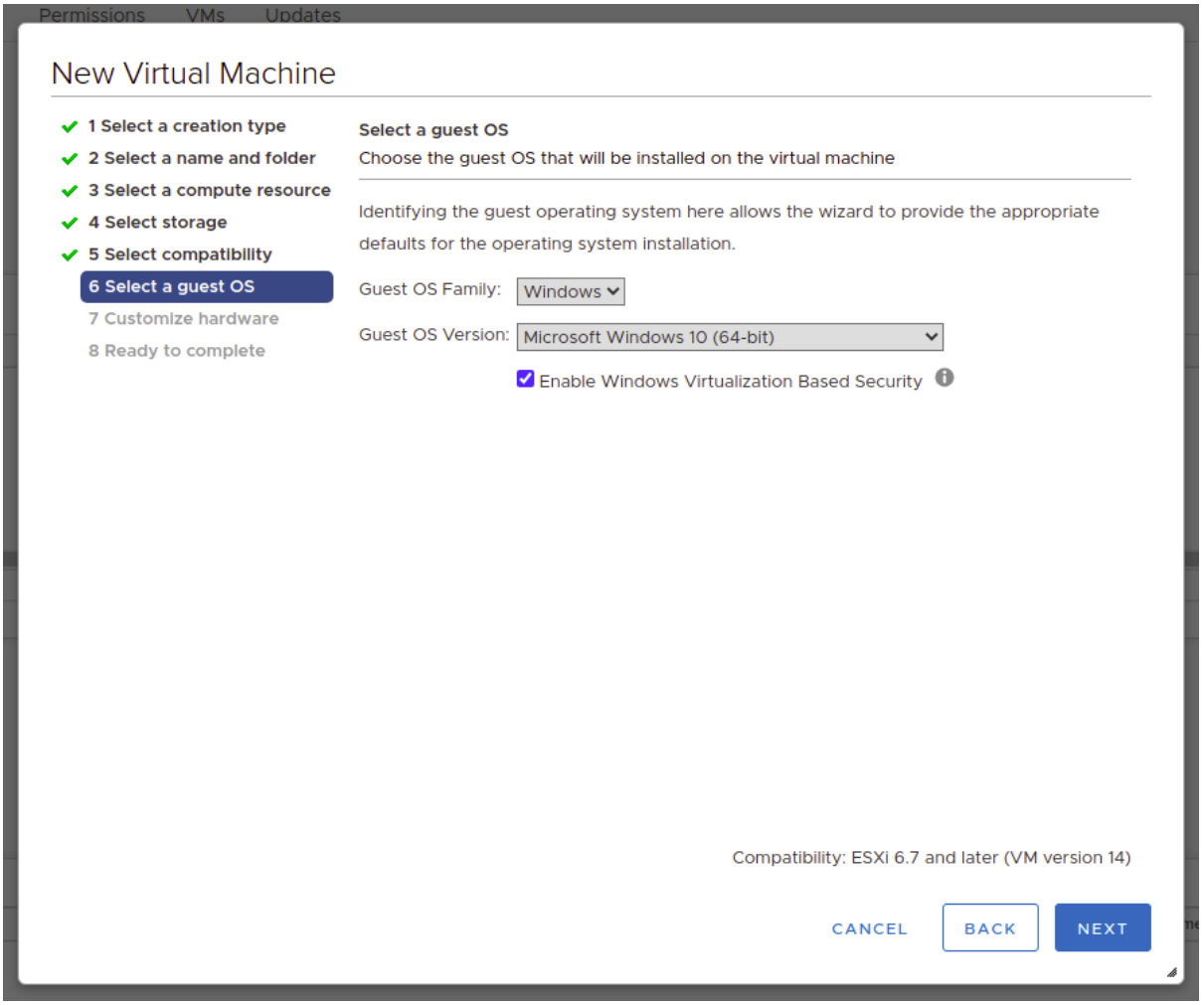
Vi velger hvor ressursene som maskinen skal benytte seg av ligger.



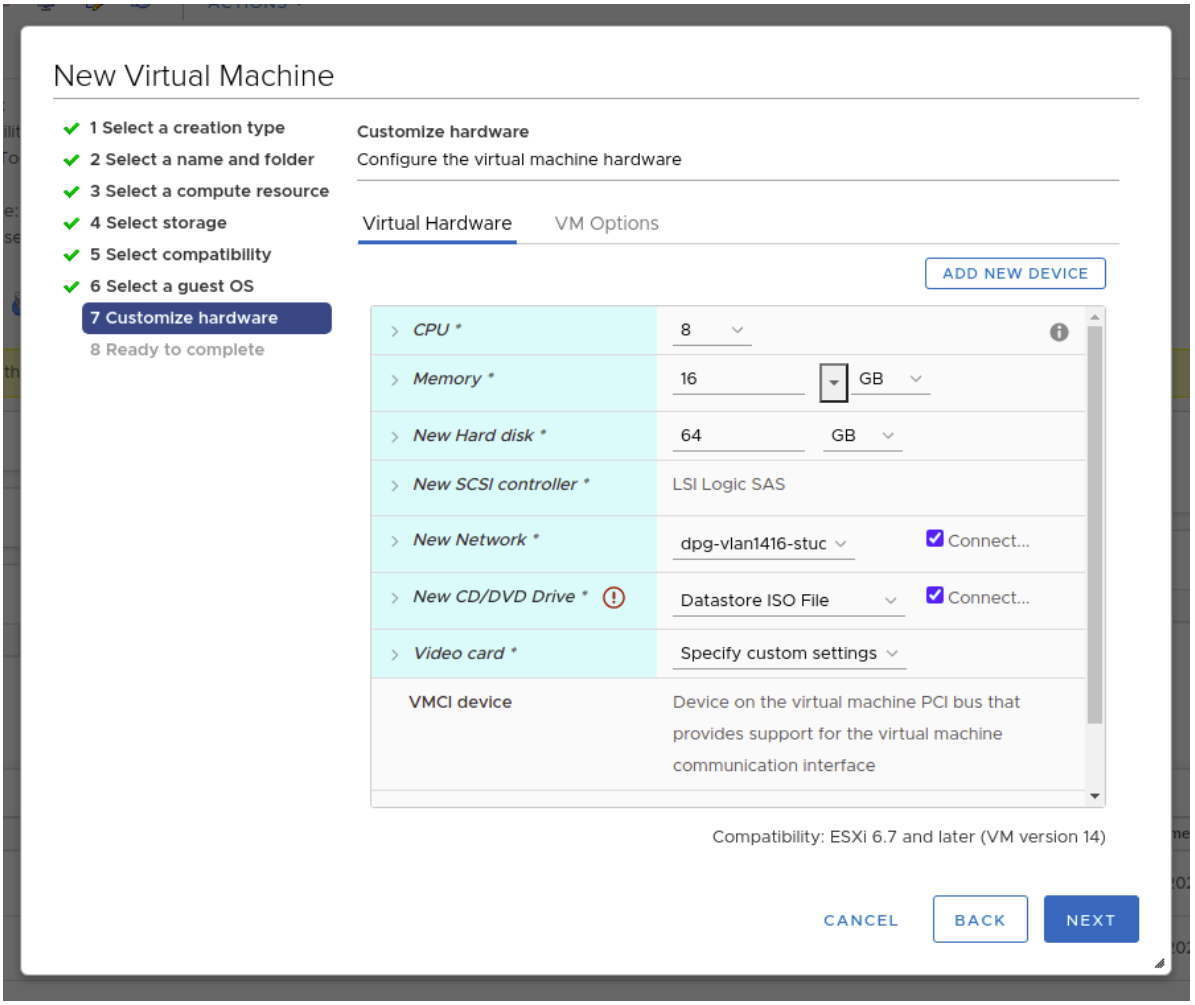
Videre velger vi lagringsenhet for maskinen.



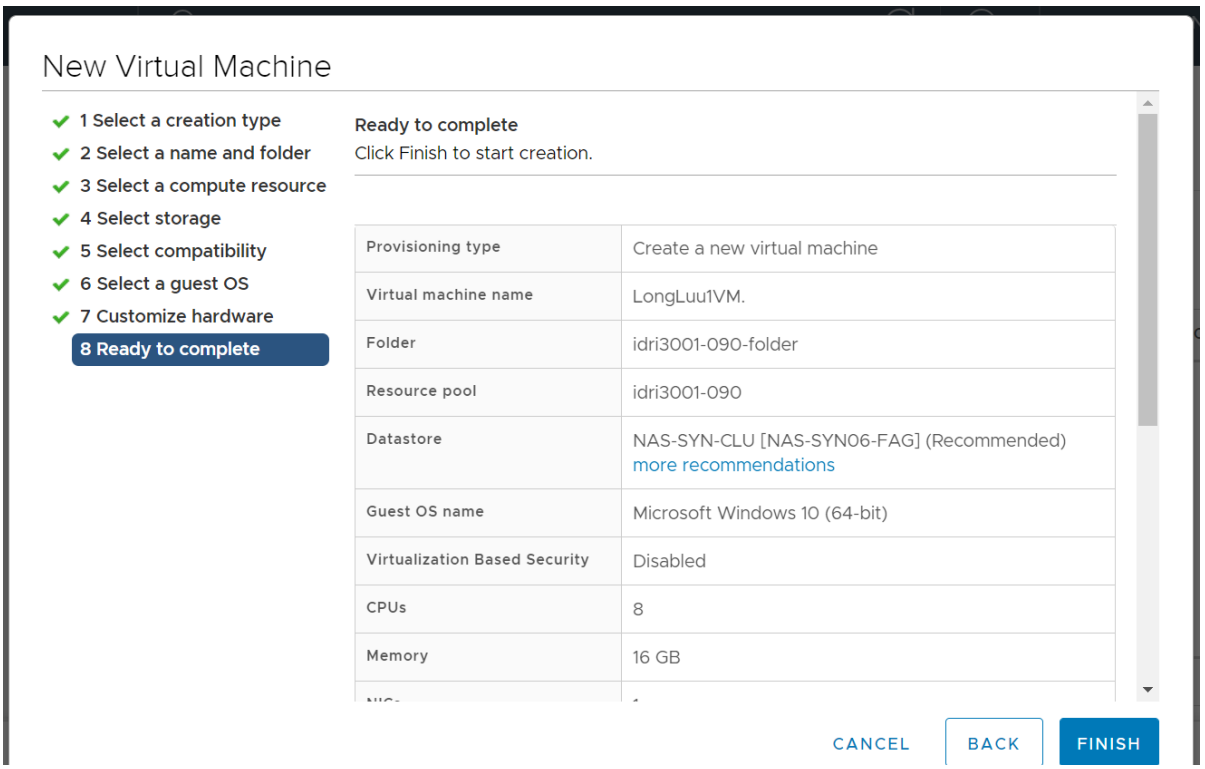
Vi velger også hvilken VMware-versjon vi ønsker å benytte for maskinen. Vi velger den nyeste versjonen, versjon 6.7+.



Vi oppretter en Windows 10 (64-bit) og huker av "Enable Windows Virtualization Based Security".



I denne fasen velger vi ønskede maskinvarer, slik som det er vist i figuren over.



Her finner man en oversikt over alle innstillingene og virtuell maskinen er klar for å bli opprettet.

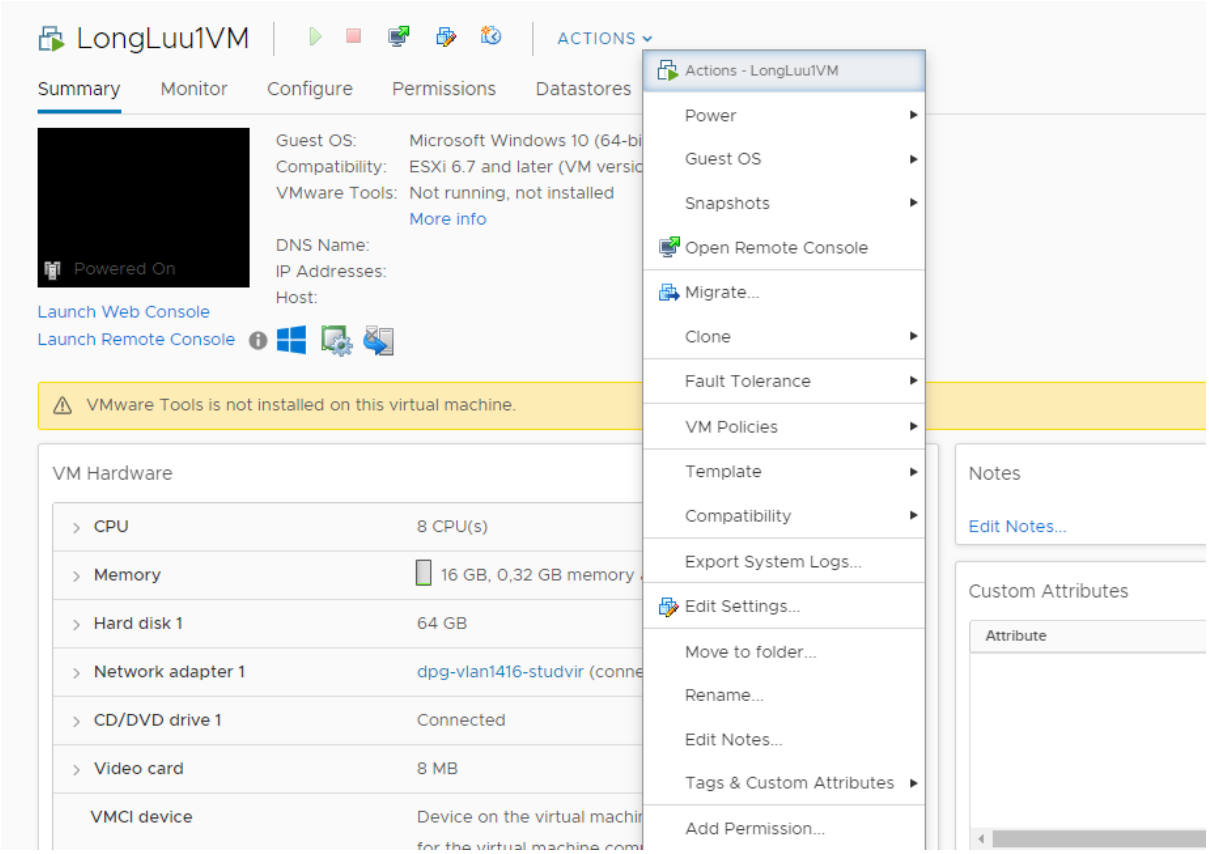
5.2.2. Oppsett av sikkerhetsfunksjoner

5.2.2.1. Extended Detection and Response (XDR)

XDR er allerede integrert i nyere versjoner av vSphere, derfor er ikke ytterligere oppsett nødvendig.

5.2.2.2. VMware vSphere High Availability

VMware vSphere HA (High Availability) er integrert i vSphere, men krever at VMware Tools er installert på VM-en som skal overvåkes for å aktiveres (9).



For å installere VMware Tools velger vi "Install VMware Tools" under "Guest OS". Dette tar kun noen sekunder. Etter dette vil HA aktiveres.

5.2.2.3. VMware NSX

For å demonstrere VMware NSX benytter vi oss av en gratis demonstrasjon fra VMware. Det er dermed ikke nødvendig å utføre noe oppsett her, annet enn å logge inn på VMware-bruker og starte demonstrasjonen.

6. Fase 2 - Sikkerhetsfunksjoner

Følgende sikkerhetsfunksjoner er nevnt i designrapporten. Her forklares funksjonaliteten til disse i detalj, da vi forklarte tekniske detaljer rundt oppsett i kapittel 7, og beskriver hvordan disse fungerer for å beskytte virtualiseringstjenesten mot angrep.

6.1. Windows Virtual Desktop

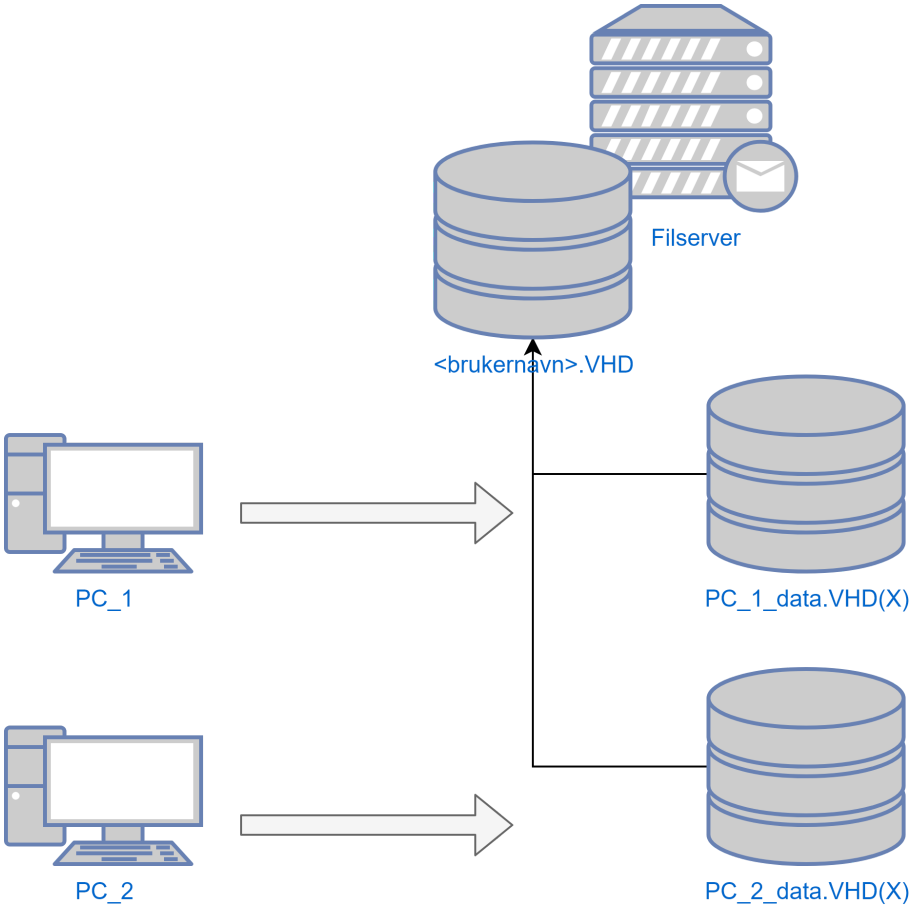
Windows Virtual Desktop er en tjeneste for skrivebord- og applikasjonsvirtualisering. De tilbyr en flerbrukerløsning med Windows 10 multi-session der flere brukere deler på ressurser fra samme maskin. Denne tjenesten har både høy fleksibilitet, skalerbarhet og er lagt opp for enkel utrulling samt administrasjon av infrastruktur. For mer informasjon kan man gå til siden under: https://docs.microsoft.com/en-us/azure/virtual-desktop/

6.1.1. FSlogix

Riktig oppsett og administrasjon av profiler og profilbeholdere er viktig for å ivareta sikkerheten i det virtuelle systemet. Man kan se for seg et scenario hvor man har hundrevis av brukere og mange ulike stillingstyper i en bedrift, hvor hver stillingstype innebærer forskjellige rettighetsnivå. I et komplisert system som dette kan det fort hende at noe blir oversett og brukere kan få uautorisert tilgang til data. Slike hendelser kan få konsekvenser av varierende grad, og kan unngås ved gode rutiner og hjelpemiddel for å administrere systemets brukere.

FSlogix er et hjelpemiddel som kan tas i bruk i et WVD-miljø som tjener nettopp dette formålet. En brukerprofil inneholder en mengde konfigurasjonsdata og innstillinger som bestemmer hva brukeren kan benytte seg av og hvordan den kan samhandle med miljøet. Noen av disse kan endres av brukeren, mens andre er bestemt av systemadministrator, for eksempel gjennom GPO-er. FSLogix fungerer slik at det lager VHD(X)-filer for brukerprofilen og lagrer disse i en

delt filmappe. Disse kan gjøres tilgjengelige gjennom nettverket når brukeren logger inn og gjøres utilgjengelige igjen når brukeren logger ut (7).

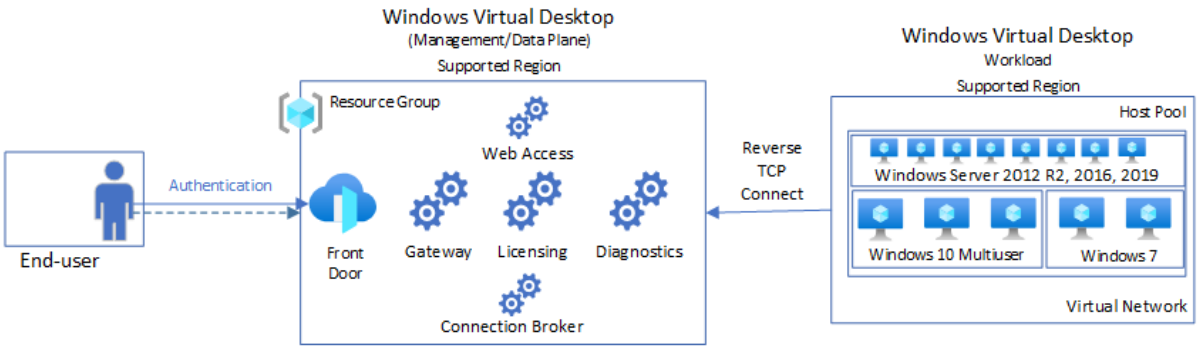


Figur 4: Her ser vi et eksempel på databehandling med FSLogix. Brukerdata blir lagret som VHD-filer på filserveren, og hentes ut ved forespørsel, altså når brukeren logger på.

FSLogix benytter seg av en cache-løsning (lagring av data for hurtig tilgang) kalt Cloud Cache. Dette innebærer at man cacher brukerprofil-filer lokalt på maskinen. Dette sørger for mindre belastning for nettverkstrafikken. Med FSLogix kan man utvide brukerprofilen til å inkludere flere mapper (9).

6.1.2. Reverse connect

Windows Virtual Desktop benytter Reverse Connect for tilkobling av Remote Desktop og transport av RDP-trafikk. Her brukes ikke TCP-listener til å motta innkommende RDP-tilkoblinger, men man bruker utgående port til Windows Virtual Desktops infrastruktur over HTTPS-tilkoblinger (11). Dette gir en sikrere tilkobling til virtuelle maskiner og kan reduserer risikoen for sikkerhetsbrudd ved hjemmekontor og jobbreiser. Her benyttes også Azure AD Conditional Access Policy, nevnt i 8.1.3., til å håndtere adgangen til Windows Virtual Desktop.



Figur 5: Figuren viser hvordan en ende-bruker får tilgang til ressurser etter MFA og illustrerer kommunikasjonen mellom Workload og Data Plane med Reverse Connect med TCP.

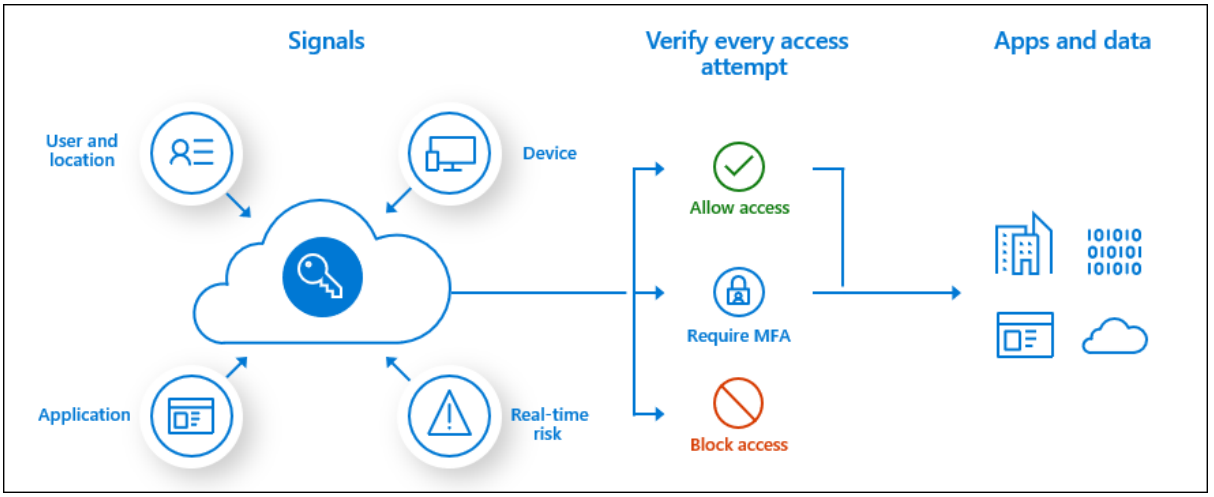
6.1.3. Multi-Factor Authentication

Multi-Factor Authentication er en autentiseringsmetode der en bruker blir bedt om en ytterligere form for identifikasjon i løpet av påloggingsprosessen. Denne funksjonen baserer seg på noe du vet, har eller er. Det vil si et passord, en mobil eller bruk av biometri til identifisering. I dette prosjektet skal brukerne benytte en applikasjon, Microsoft Authenticator, til å verifisere seg selv. Fremgangsmåten for å sette opp Microsoft Authenticator er beskrevet i pkt. 7.1.2.3.1. Denne

funksjonen må benyttes hos alle administratorer og ansatte i LongLuu. Med det mener vi at alle ansatte i LongLuu skal gjennomføre denne verifiseringen før de får tilgang til brukeren sin i Windows Virtual Desktop. Denne adgangskontrollen kan sikre ansattes identitet og hindre at ondsinnede kan misbruke en ansatts bruker (6).

6.1.3.1. Conditional Access Policy

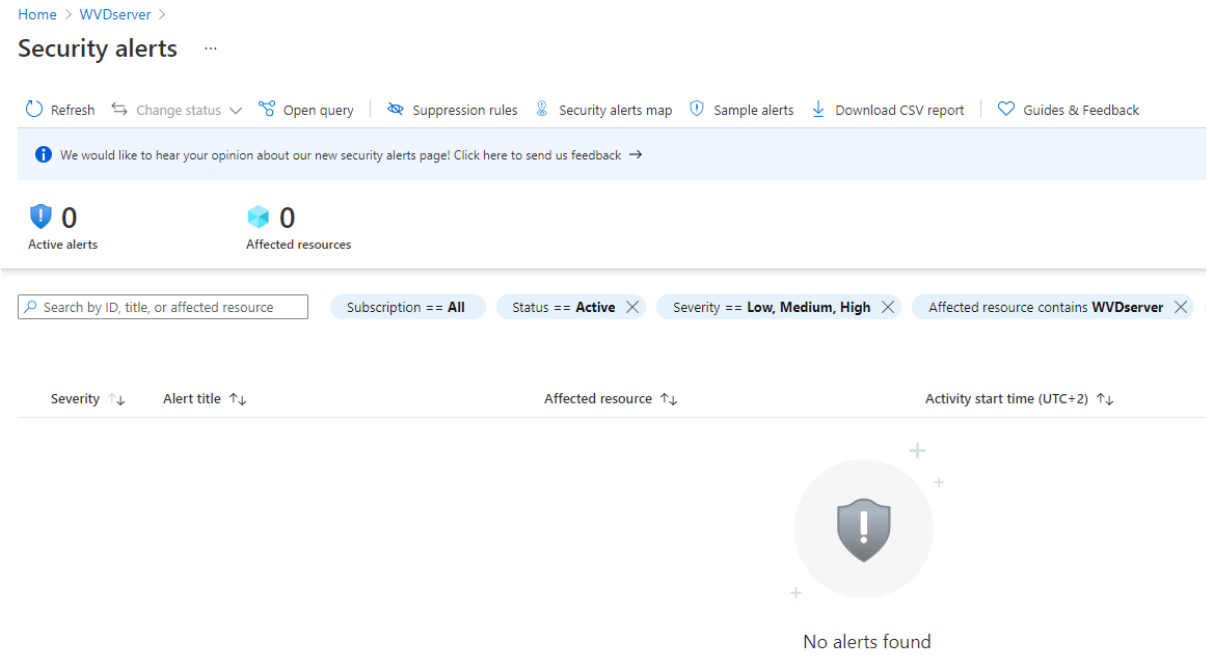
Conditional Access er et verktøy i Azure AD som samler signaler, tar beslutninger og håndhever det i organisasjonsretningslinjen. Dette verktøyet er bygd opp av if-setninger. Dersom en bruker søker om tilgang til en ressurs må brukeren fullføre en verifisering, altså Multi-Factor Authentication. Hensikten med Conditional Access policy er å gi et ekstra lag av beskyttelse slik at sensitiv informasjon ikke havner i gale hender. I tillegg gir MFA sikker fjerntilgang, slik at de ansatte i LongLuu kan øke produktiviteten ved å ha muligheten til å jobbe hvor og når som helst (6).



Figur 6: Figuren viser hvordan ulike signaler sender forespørsel om tilgang til ressursene. Signalen blir enten godkjent, stilles krav om MFA eller ikke godkjent (11).

6.1.4. Endpoint Protection

Endpoint Protection utfører automatiske trusselskanninger og varsler ved eventuell oppdagelse av dette. For mer kritiske trusler vil tiltak for å fjerne disse bli igangsatt automatisk. Det gir også brukeren mulighet til å få oversikt over potensielle trusler funnet på enhetene som Endpoint Protection er installert på og hvilke tiltak som ble satt til verks for å håndtere disse.



Figur 7 - Her vil varsler om sikkerhetstrusler vises ved en hendelse.

Ved bruk av Endpoint Protection gjennom Azure vises og konfigureres varsler angående sikkerhetshendelser i Azure Security Center, hvor man også kan velge når og hvordan maskinene skal kjøres gjennom sikkerhetssjekker (12).

6.1.5. Azure Security Center

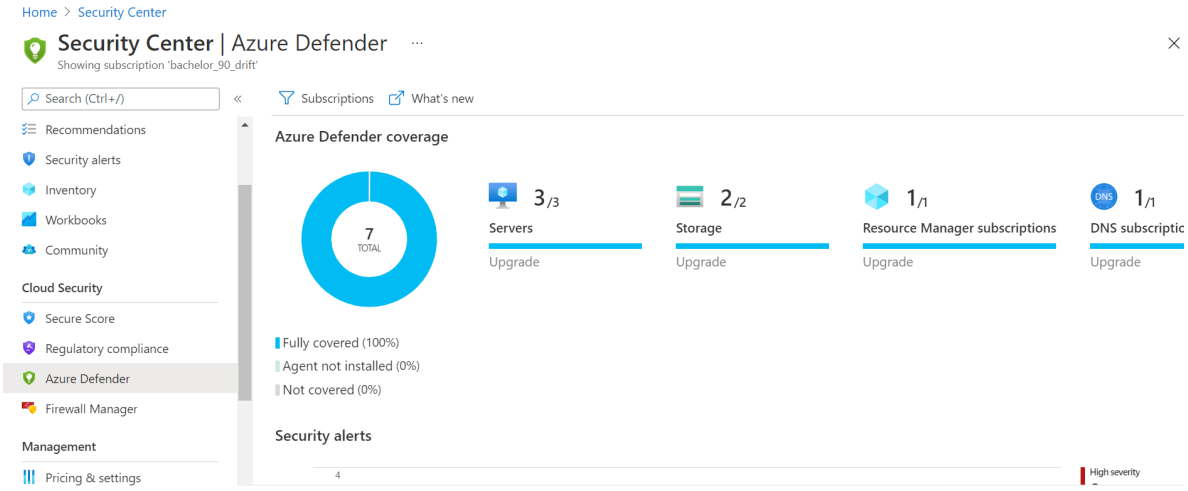
Azure Security Center er et innebygd verktøy i Azure-portalen for administrasjon av sikkerhetsstatus og beskyttelse mot trusler. Dette

verktøyet kategoriseres som en *Cloud Security Posture Management (CSPM)* og *Cloud Workload Protection Platform (CWPP)*. *CSPM* er et verktøy som fokuserer på sikkerhetsvurderinger og overvåkning av IaaS stack. Det forhindrer feilkonfigurering og styrker sikkerheten av hele infrastrukturen i Windows Virtual Desktop. *CWPP* benyttes for overvåkning og beskyttelse av sky-belastninger (25).

Alle ressurser i Windows Virtual Desktop må kobles til Azure Security Center for å forsterke sikkerhetsgraden i infrastrukturen, gjennom integrasjon i Cloud Security. Dette involverer ressurser som Azure Defender, Firewall Manager, Secure Score og Regulatory Compliance.

6.1.5.1. Azure Defender

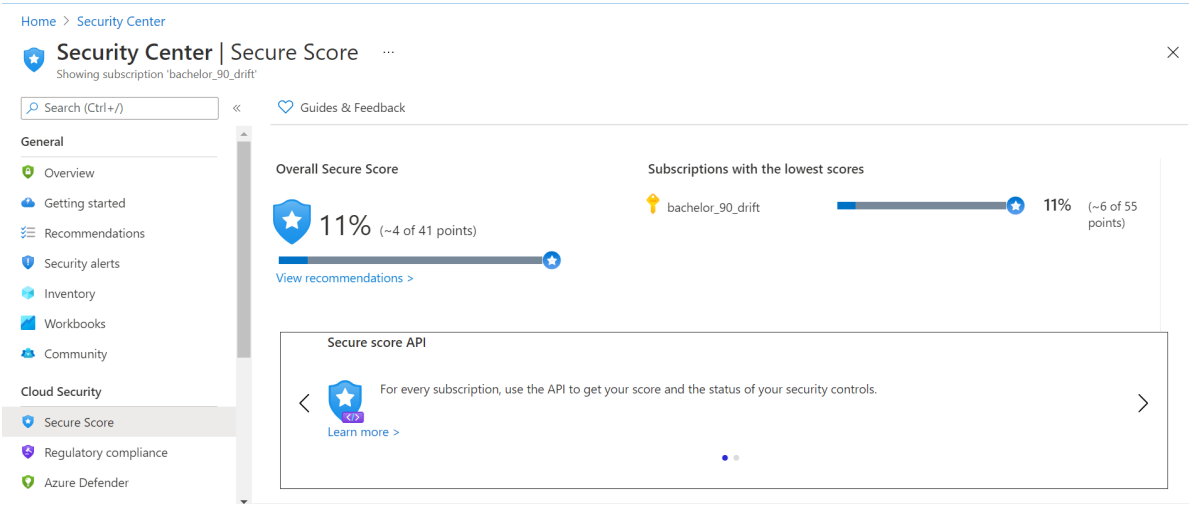
Azure Defender er et integrert verktøy i Azure Security Center som administrerer sikkerhet på tvers av serverbelastningene i Azure. Denne tjenesten gir innsikt ved å skanne gjennom hele abonnementet i Azure og tilbyr sikkerhetsvarsler og trusselbeskyttelse ved et angrep. Denne tjenesten er tilgjengelig for for servere, SQL-databaser, Storage, Key Vault, Resource Manager, Kubernetes og Container-registrer.



Figur 8 - Her finner vi en oversikt over hva Azure Defender dekker.

6.1.5.2. Secure Score

Secure Score er en tjeneste for sikkerhetsvurdering av en organisasjon i Azure Security Center. Denne tjenesten har kontroll over sikkerheten på tvers av ressurser i Azure, og man får en oppdatert rapport over sikkerhetssituasjonen for infrastrukturen til bedriften. Secure Score kommer med anbefalinger som kan beskytte systemet mot sikkerhetsangrep, slik at det er mulig å komme med forbedringer samt øke arbeidsflyt for administrering (17).



Figur 9 - Secure Score

6.1.6. Azure Monitor

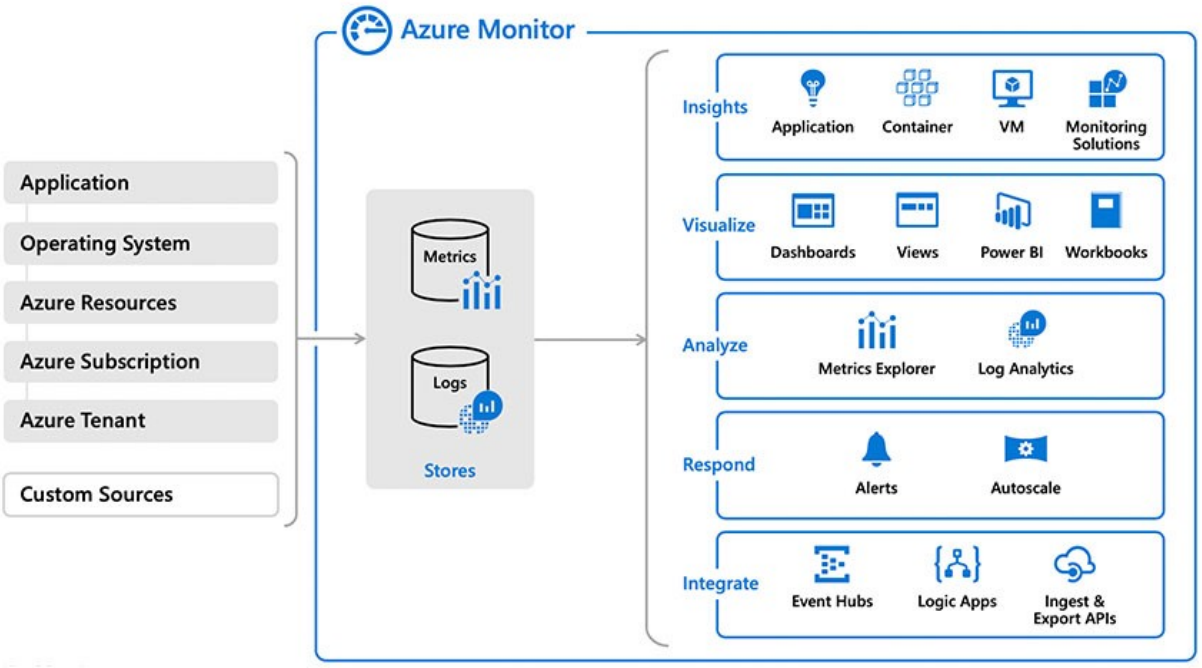
Azure Monitor er en innebygd funksjon i Azure-portalen og benyttes til å overvåke infrastrukturen i Windows Virtual Desktop. Systemet har sikkerhetsfunksjoner for overvåkning av applikasjoner og nettverk der de benytter disse dataene til å analysere og optimalisere Azure-miljøet. Data som samles av Azure Monitor kan deles inn i to hovedtyper: Metrics og Logs.

6.1.6.1. Azure Monitor Metrics

Azure Monitor fungerer ved å samle inn telemetri ved hjelp av Azure Monitor Metrics fra lokale kilder og Azure-kilder, som for eksempel fra Azure Security Center som er nevnt i pkt. 8.1.5. Disse telemetridataene er verdier som samles med jevne mellomrom og kan presentere aspekter ved systemet på et bestemt tidspunkt. Dette blir lagret i en database hvor det benyttes til å analysere ressursene i Azure og optimalisere infrastrukturen i Windows Virtual Desktop.

6.1.6.2. Logs Analytics

I tillegg til telemetri samler Azure Monitor inn loggdata. Loggdata er av ulike typer data med forskjellige egenskaper. Logs Analytics brukes for å redigere og kjøre logg-spørringer for data i Azure Monitor Logs, og kan analysere dataene direkte ved bruk av ulike innebygde verktøy i Azure. Fordelen med analysering av loggdata er at det gir sanntidsinnsikt med Azure Dashboard slik at det er mulig med rask feilsøking i Azure-miljøet.



Figur 10 - Her finner du oversikt over funksjoner i Azure Monitor.

6.1.7. Screen Capture Protection

Screen Capture Protection skjuler fjernstyringsprosesser når man tar en skjermdump. På denne måten unngår man at sensitiv informasjon blir delt med andre. Dersom man forsøker å ta bilde av skjermen vil fjernstyringsvinduet se slik ut:

Figur 11 - Screen Capture Protection

Fjernstyringsvinduet blir altså blokket ut for å hindre uautorisert tilgang til fjernstyringsverktøy (8).

6.1.8. Microsoft Azure Sentinel

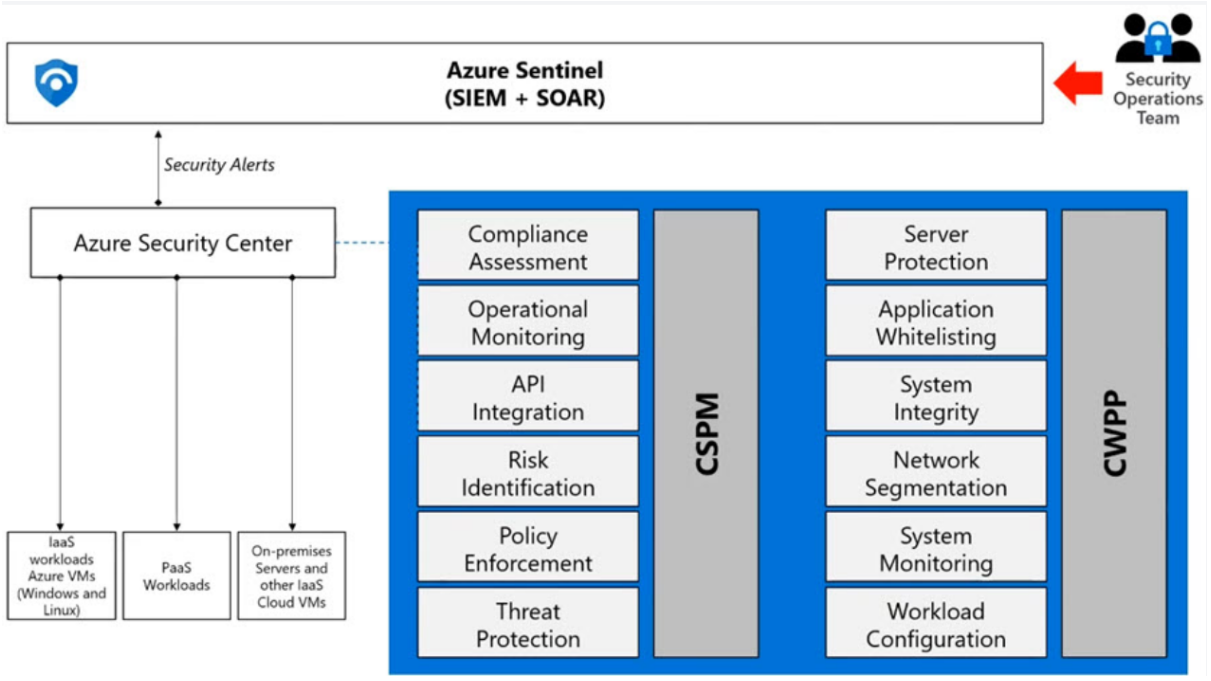
Azure Sentinel er en innebygd Security Information Event Management (SIEM) og Security Orchestration Automated Response (SOAR)-løsning i Azure. Hovedoppgaven til denne løsningen er innsamling av data, å oppdage og undersøke hendelser samt komme med en rask respons. Dette gjøres ved å koble til ulike Data Connectors, altså sikkerhetskilder, i Azure. Vi kobler til disse datakildene og benytter disse til sikkerhetsovervåkning av ressursene i Workbooks.

I dette prosjektet er vi interessert i å overvåke "audit logs" i Azure Active Directory. Audit logs i Azure AD er revisjonslogg som registrerer aktivitet hos bruker og admin i Windows Virtual Desktop. Ved å koble til "Azure Active Directory"-kilden, får vi en oversikt over

disse loggene i Workbooks og kan enkeltvis opprette en tilpasset Workbook.

6.1.9. Integrasjon av Azure Security Center med Azure Sentinel

Azure Defender er en integrert med Cloud Workload Protection Platform (CWPP). Dette verktøyet kan oppdage og svare raskt på trusler på tvers av ressurser i Azure. Når vi integrerer Azure Security Center med Azure Sentinel, vil Security Alerts som genereres av Security Center blir eksportert til Azure Sentinel. Slik kan man overvåke Defender-data i Workbooks, sende spørringer om å opprette varsler og deretter undersøke samt svare på hendelser.



Figur 12 - Dette bildet viser hva en får av å integrer Azure Security Center med Azure Sentinel.

6.2. VMware vSphere

VMware tilbyr programvare for virtualisering av blant annet servere, arbeidsstasjoner. Dette gjør det mulig å dele ressurser fra en fysisk server mellom flere virtuelle maskiner. VMware vSphere er en virtualiseringsplattform som gjør det mulig å administrere det virtuelle miljøet. Man kan lese mer om VMware vSphere her: https://www.vmware.com/no/products/vsphere.html

6.2.1. Extended Detection and Response (XDR)

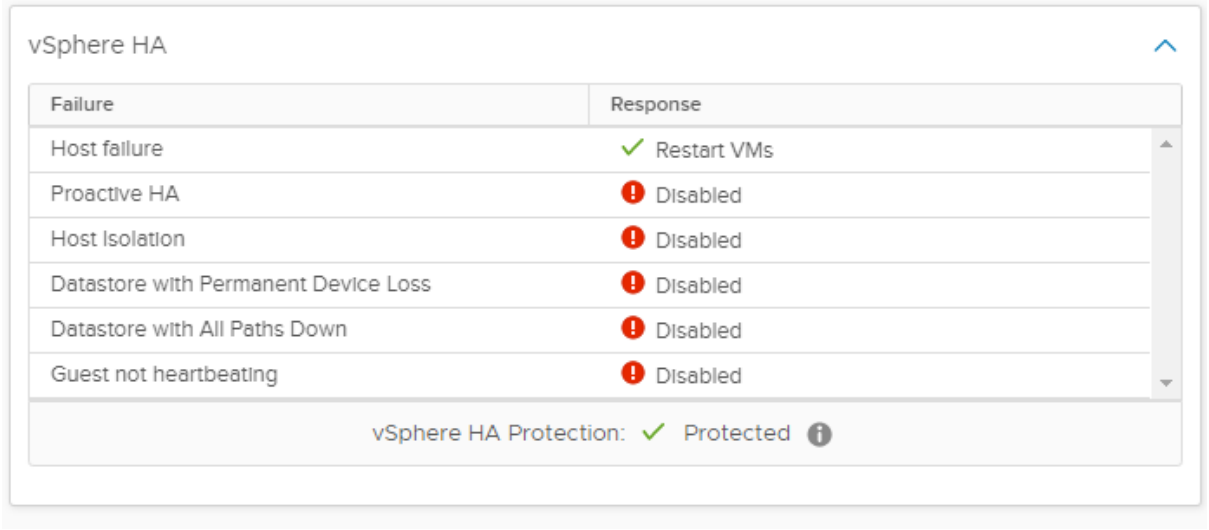
XDR er en mer avansert utgave og progresjon av Endpoint Detection and Response (EDR). EDR fjerner trusler på endepunkter og workloads, mens XDR har i tillegg utvidet det til flere sikkerhetskontrollspunkter som e-post, nettverk, servere og sky. Disse data er telemetri som blir samlet på tvers av domener og danner grunnlag for analyse der systemet tillater gruppering og prioritering av varsler. Videre blir det oppdaget trusler basert fra disse varslene, eksempelvis kan den oppdage dårlige aktører som bruker lovlige programvarer for å få tilgang til systemet. XDR kan fjerne trusler samt automatisk oppdatere sikkerhetspolitikken sin for å forhindre at samme eller lignende angrep oppstår igjen. Denne sikkerhetsteknologien utvider synlighet, fortløpende analyse, overvåkning og respons på tvers av nettverk, server og skyene i tillegg til applikasjoner og endepunkter (18).

6.2.2. VMware vSphere High Availability

Hensikten med vSphere High Availability er å samle VM-er og tilhørende tjenere til et cluster. Tjenesten overvåker tjenerne, og starter VM-ene på en alternativ tjener dersom den opprinnelige tjeneren skulle feile. HA erklærer altså en primærtjener og en eller flere sekundærtjenere. Ved å overvåke tjenerne kan HA avgjøre hvilken type feil som inntreffer og bestemme om VM-ene skal restartes på en annen tjener. Dersom feilen for eksempel ligger hos nettverket er det kanskje

ikke en løsning å flytte maskinene. Man kan selv velge hvordan HA skal respondere i dette tilfellet.

I vSphere-miljøet kan High Availability nås ved å gå inn på ressursen hvor dette er aktivert. Vi vil da se en fane som vist på bildet under, hvor det vises en liste over hvilke tjenester i HA som er aktivert for ressursen. Man får også mulighet til å velge hvilke som skal være aktive, noe som bestemmes avhengig av hvilket use case som er aktuelt. Ønsker man for eksempel et miljø som tar hensyn til potensiell nedetid grunnet tjenerfeil kan det være lurt å aktivere "Host failure", som restarter VM-ene som nevnt tidligere dersom dette inntreffer.



Figur 13 - High Availability

HA kan også overvåke applikasjoner ved å sjekke "heartbeat", og restarter VM-en hvor applikasjonen er installert ved en eventuell feil (9).

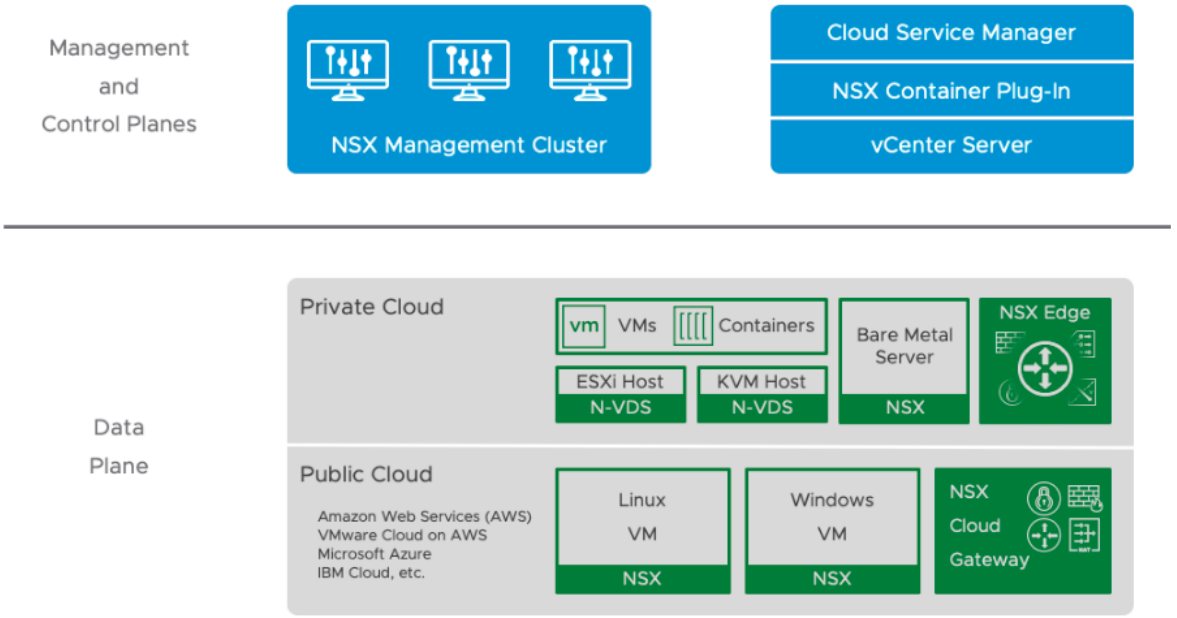
For å beskytte tjenesten finnes vSphere HA Security. Dette sørger for at konfigurasjonsdata kun er lesbart av rotbrukeren (bruker med rettighet til å lese systemfiler). Hendelser som oppstår blir også loggført og lagret. vSphere HA benytter seg av en brukerkonto opprettet av vCenter Server for å logge inn i systemet, hvor passord er

tilfeldig generert og endres periodisk. All kommunikasjon mellom vCenter Server og HA verifiseres og utføres over SSL, og HA varsler dersom en ukjent tjener forsøker å få kontakt (18).

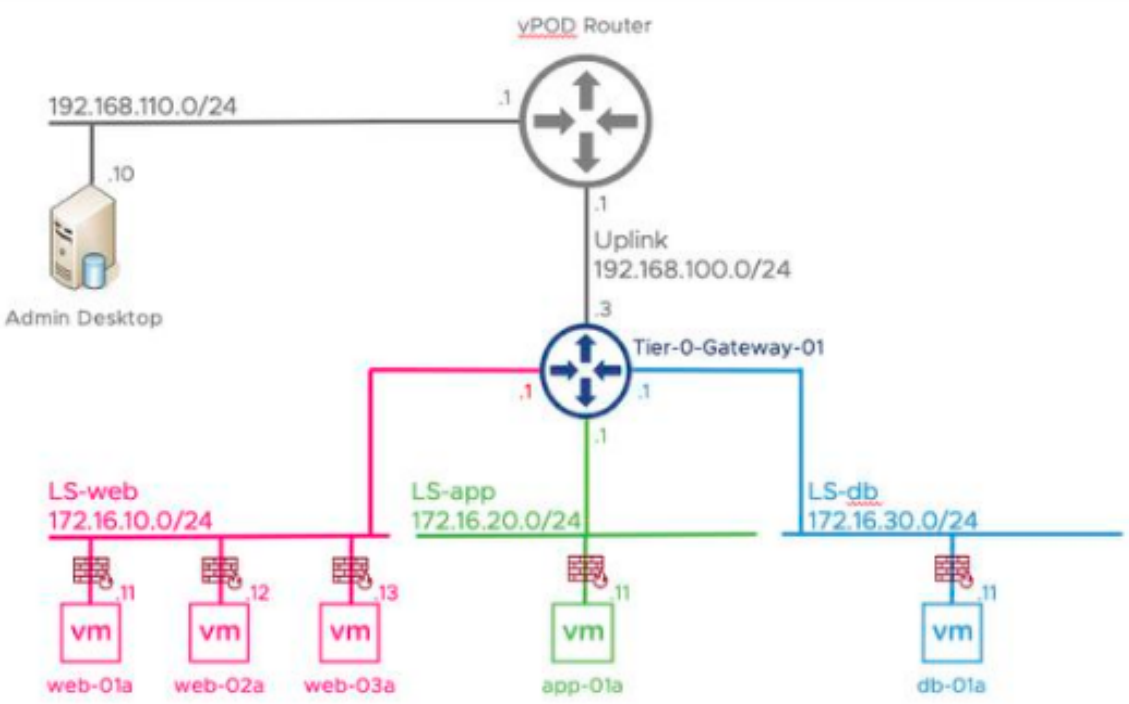
6.2.3. VMware NSX

VMware NSX er en virtualiseringstjeneste for nettverk. Den gjør det mulig å sette opp virtuelle nettverk i fysiske nettverk og på virtuelle servere. NSX kan benyttes for å dele opp nettverk i mikrosegmenter for separate arbeidsområder for å senke risiko og konsekvens ved angrep.

Vi skal nå se litt på hvordan dette kan benyttes i praksis. Først viser vi oppsettet ser ut i vår testlaboratoriet.



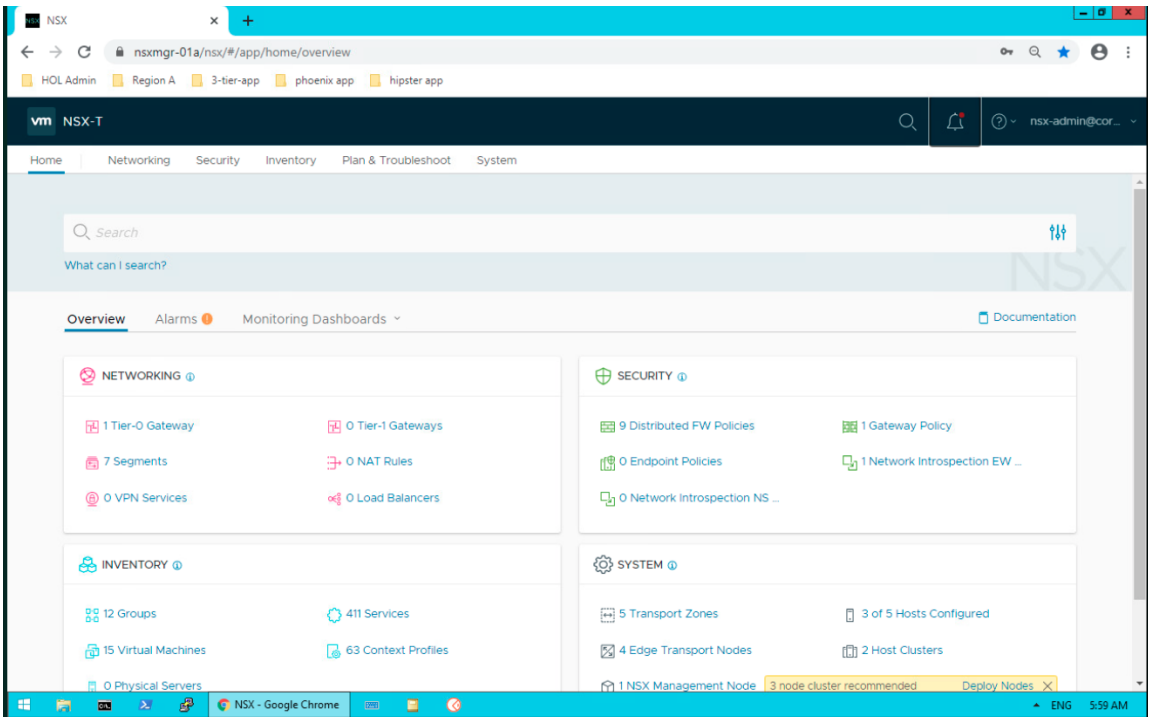
Figur 14 - Bildet over demonstrerer hvordan et VMware-miljø kan være satt opp med NSX. NSX er fordelt i et Management Cluster, Container Plug-in, NSX Cloud Gateway og NSX Edge.



Figur 15 - NSX

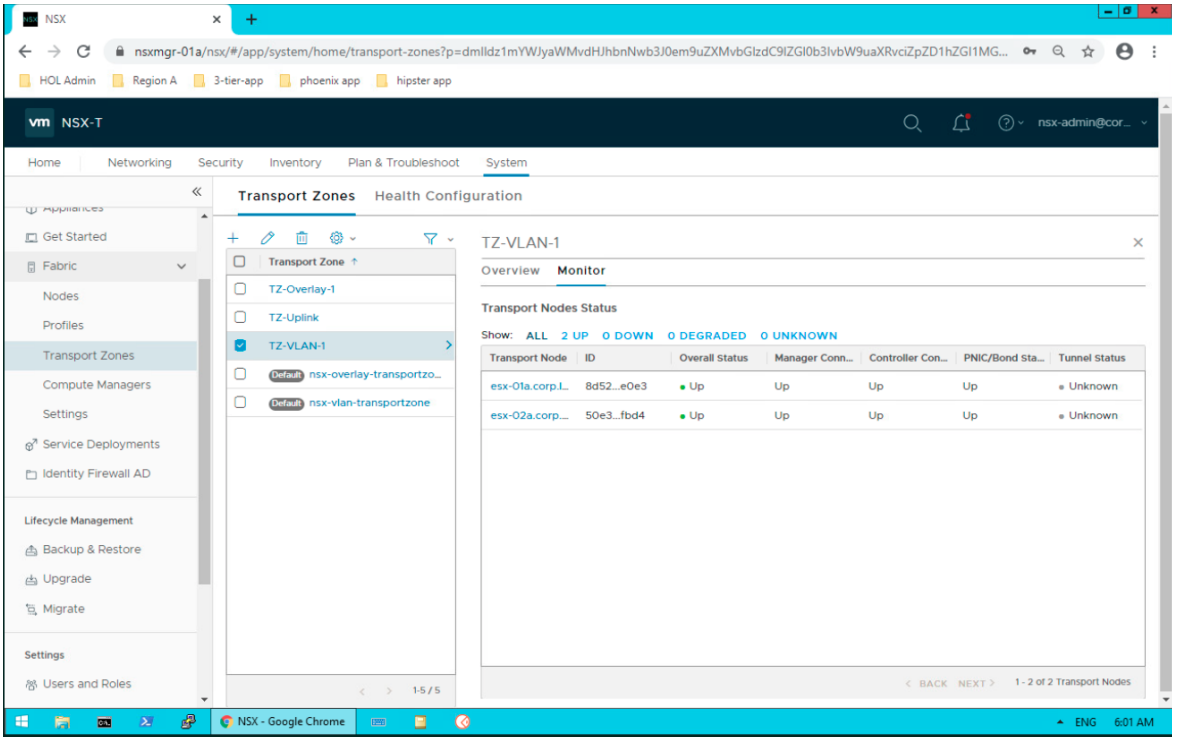
Slik er nettverket i testlaboratoriet vårt satt opp. Vi har tre ulike virtuelle nettverk som rutes gjennom en gateway, som igjen linker til ruteren, hvor en maskin kalt "Admin Desktop" er koblet til direkte.

Administrasjonskonsollen for NSX kan nås ved å logge inn på NSX-miljøet. Her kan man sette opp regler og preferanser for hvordan NSX skal beskytte nettverket og maskinene.



Figur 16 - For å administrere NSX logger vi på testbruker for NSX-miljøet. Da får vi opp konsollen hvor man kan benytte seg av de ulike tjenestene NSX tilbyr.

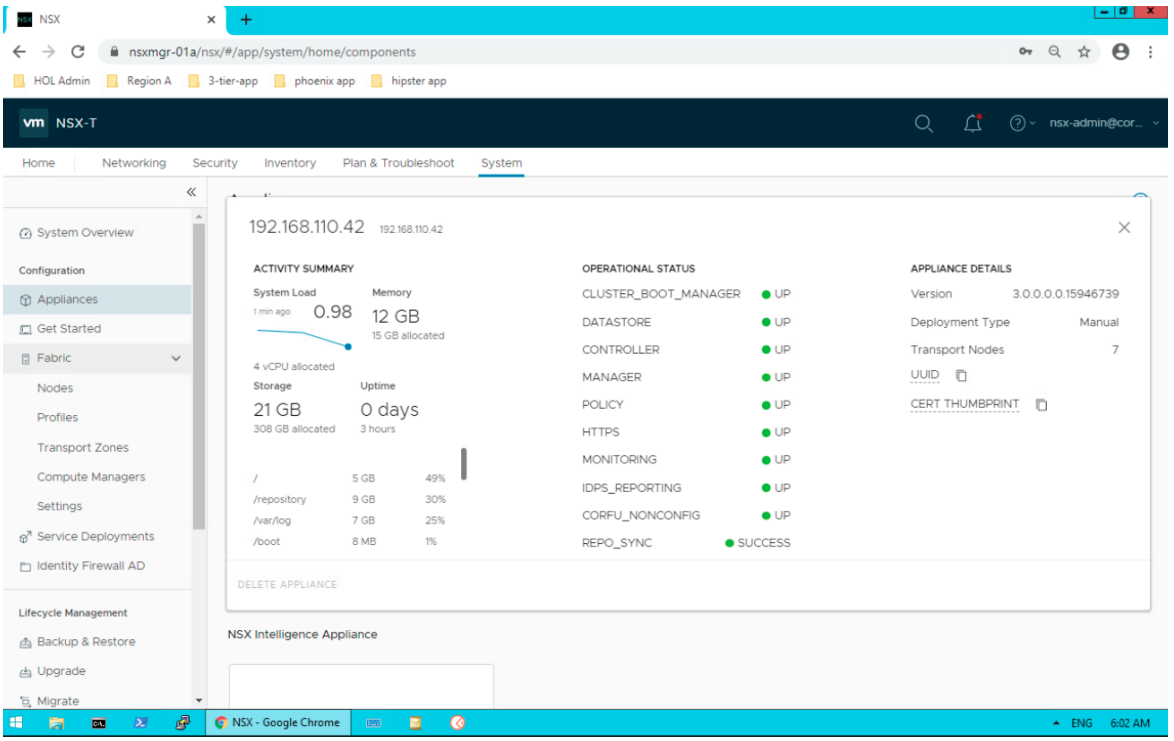
Som nevnt kan NSX benyttes for mikrosegmentering. En vanlig strategi for angrep er øst-vest-metoden, hvor angriperen finner et usikret punkt i nettverket, for eksempel en VM, og flytter seg gjennom nettverket for å bryte seg inn i andre enheter i nettverket. Dette kan være vanskelig å oppdage i tide. For å løse dette kan man altså benytte seg av mikrosegmentering, ved å fordele arbeidsoppgaver i separate nettverk som ikke kan kommunisere med hverandre.



Figur 17 - NSX

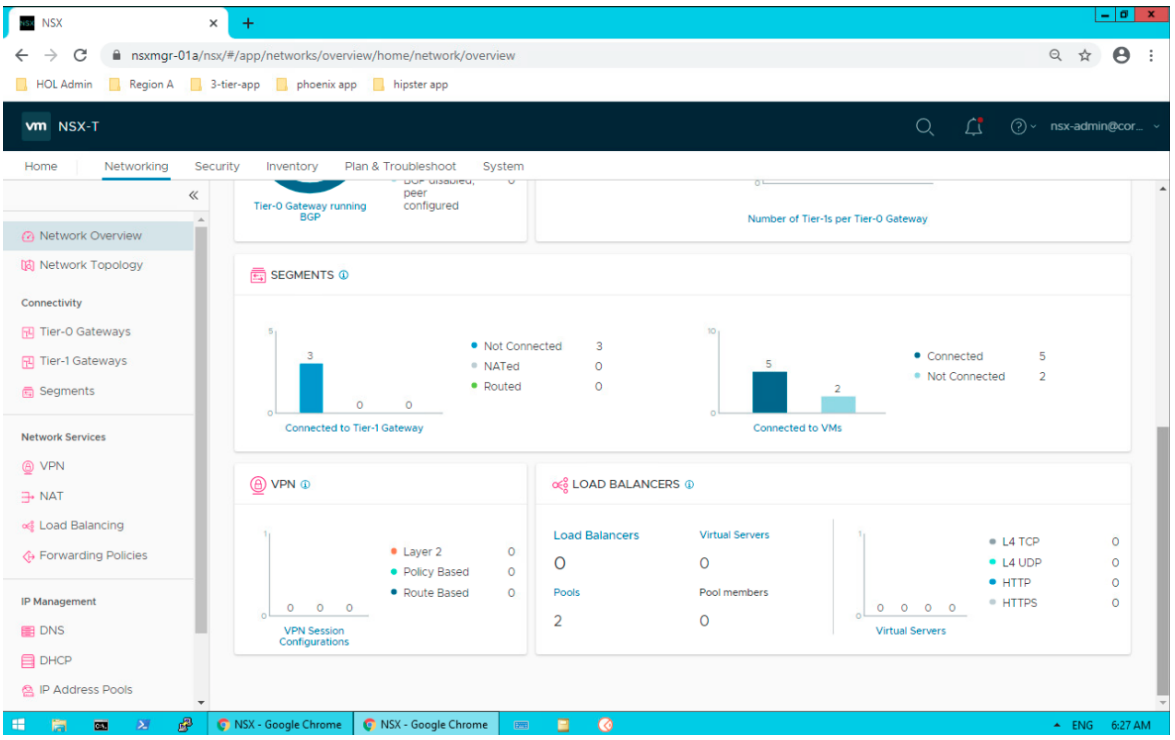
I NSX kan man overvåke status for transportsonene ved å velge "Transport Zones" under "Fabric"

NSX tilbyr også overvåking av nodene og sonene i nettverket, slik at man kan utrede problemer og bli varslet om hendelser.



Figur 18 - Videre kan man overvåke status for de ulike apparatene (appliances) ved å velge "Appliances" fra menyen.

I visse tilfeller er ulike nettverk nødt til å kunne kommunisere. I slike tilfeller benyttes IPS (Intrusion Prevention Systems) for å overvåke nettverkstrafikken og håndtere mistenkelig trafikk.



Figur 19 - Dersom man navigerer til "Networking"-fanen får man oversikt over hele nettverket, og man kan endre på konfigurasjoner for VPN, NAT, gateway, DHCP og mye mer.

Som et ekstra sikkerhetslag gjør NSX det mulig å benytte seg av anti-eksfiltrering for DNS og URL-er. Dette gjør at man kan unngå at DNS-data havner i feil hender, og blokkere usikre sider som kan infisere maskinen med virus eller tilegne seg passord (22).

7. Fase 3 - Økonomisk analyse

I denne fasen skal prosjektgruppe redegjøre for kostnader ved Windows Virtual Desktop og VMware. Det vil være en del kostnader som ikke reflekteres her i denne analysen, slik som kostnader knyttet til Windows-lisenser og maskinvare som bedriften allerede eier. Prisene under er kun estimater og ikke absolutte tall. Disse kostnadene kan variere avhengig av kjøpsdato og type avtaler som inngås med Microsoft og VMware. Prisene for Windows Virtual Desktop er hentet fra Microsoft sin egen priskalkulator (23) og VMwares kostnader er hentet fra deres nettside (31) og en tredjepart (Virtualisationwork) (24).

7.1. Windows Virtual Desktop

7.1.1. Azure Security Center, Azure Defender

Azure Security Center har en rekke gratis tjenester slik som Secure Score. Disse går under den gratis versjonen av Security Center. I denne analysen vil en stor del av kostnadene være knyttet til Azure Defender. Her har LongLuu behov for en (virtuell) server, en SQL-database og omtrent en milliard *storage transactions*. Med denne ressursinnstillingen, vil prisen bli 22 865,82 kr per år.

7.1.2. Azure Monitor

7.1.2.1. Datainntak

Som nevnt i pkt. 8.1.5., samler Azure Monitor inn telemetri og analysere disse i Log Analytics. I Log Analytics betaler en for datainntak og oppbevaring av disse. Det er behov for 100 VM-er for LongLuu der disse gjennomsnittlig inntar 2 Gb data pr. måned. Det gir en kostnad på 67 836 kr per år.

7.1.2.2. Dataoppbevaring

Innsamlet data lagres gebyrfritt i Log Analytics arbeidsområdet i 31 dager. Data som lagres etter de første 31 dagene vil man bli

belastet 1,261 kr for per Gb per måned. Data som oppbevares i Azure Sentinel-arbeidsområder er kostnadsfrie i 90 dager.
Det er svært vanlig å oppbevare data i minst to måneder, og her antar vi at LongLuu ønsker å beholde sikkerhetsdataene sine i tre måneder. Det blir 6050,76 kr per år.

7.1.3. Azure Sentinel

Vi antar at LongLuu trenger 100 Gb pr. dag for Azure Sentinel. Det er mulig å velge kapasitetsreservasjon eller pay-as-you-go. Med kapasitetsreservasjon vil det koste 1 260,58 kr per dag (20) og 435 600 kr per år. Pay-as-you-go vil koste 17,64 kr per Gb-inntak. Azure Sentinel er gratis de første 31 dagene.

7.1.4. Prisoverslag for Windows Virtual Desktop

Funksjon	**Beskrivelse**	**Kostnad pr. år**
Security Center (Azure Defender)	Pris for en server og en SQL-database	**22865,82 kr**
Azure Monitor	100 VM-er, inntar 2 Gb data pr. mnd. Dataoppbevaring i 90 dager.	**70 869,72 kr**
Azure Sentinel	100 Gb per dag.	**453 600,00 kr**
Windows Virtual Desktop	Pris med allerede eid lisens.	**386 386,83 kr**
SUM		**= 933 722,37 kr**

Tabell 4 - Prisoverslag for WVD

7.2. VMware

7.2.1. VMware vSphere

Grunnmiljøet, VMware vSphere, har en estimert kostnad på 248 894,31 kr. Dette er en engangssum og kommer med ett år med support fra VMware (31). VMware tar betalt per lisens, og man trenger en lisens per CPU. Dette er begrenset til maks 32 kjerner per CPU. Mange virtualiseringsplattformer har mer enn 32 kjerner, men dette berører casen i dette prosjektet med tanke på ressursbehov. Med 7 CPU-er holder det med færre enn 32 kjerner per CPU.

7.2.2. Extended Detection and Response (XDR)

XDR kommer integrert med VMware vSphere, og legger derfor ikke til ekstra kostnader.

7.2.3. VMware vSphere High Availability

I likhet med XDR, kommer HA integrert med VMware vSphere, og legger heller ikke til ekstra kostnader.

7.2.4. VMware NSX

VMware NSX har en (engangs)kostnad på 402 313,59 kr for sju lisenser. I likhet med VMware vSphere trenger man en lisens per CPU (24).

7.2.5. Prisoverslag for VMware

Funksjon	Beskrivelse	Kostnad (engangssum)
VMware vSphere	En lisens per CPU, LongLuu trenger (minst) 7 CPU-er	**248 894,31 kr**
Extended Detection and Response (XDR)	Innebygd i vSphere.	**0**
VMware vSphere High Availability	Innebygd i vSphere	**0**
VMware NSX	En lisens per CPU, LongLuu trenger (minst) 7 CPU-er	**402 313,59 kr**
SUM		**= 651 207,90 kr**

Tabell 5 - Prisoverslag for VMware

Totalprisen for VMware inkludert valgte sikkerhetstjenester kommer på 651 207,90 kr. Dette er en engangssum og inkluderer som nevnt i 7.2.1. ett år med support fra VMware.

8. Fase 4 - Sammenligne de overnevnte

I den fjerde fasen tar vi for oss resultatene av de tidligere fasene og sammenligner disse for å se hvordan virtualiseringtjenestene stiller opp mot hverandre.

8.1. Kost/nytte

I fase 3 har prosjektgruppen utarbeidet en økonomisk analyse av Windows Virtual Desktop og VMware. Tabellene i denne fasen viser at Total Cost of Ownership for Windows Virtual Desktop er en årlig sum på 933 722,37 kr og VMware har en engangssum på 651 207,90 kr. Prosjektgruppen baserer seg på disse tabellene og sammenligner kostnader av sikkerhetsfunksjoner i den økonomiske analysen.

LongLuu benytter Windows som operativsystem for klienter og servere for øyeblikket og har med disse lisensene allerede tilgang på WVD. Windows Virtual Desktop er et Azure-basert system og får derfor tilgang til flere funksjoner som er innebygd i Azure portalen til å opprettholde sikkerhetsstatus i infrastrukturen. I denne rapporten nevnes en del sikkerhetsfunksjoner i Windows Virtual Desktop der flere av disse er innebygd og kostnadsfrie. Andre avanserte sikkerhetsfunksjoner slik som Azure Defender, Azure Sentinel og Azure Monitor krever både lagringsplass for oppbevaring av data og eksportering av data. Dette gir en totalkostnad på 547 335,54 kr per år og anses som nødvendig for å sikre systemet på et høyt nivå.

I motsetning til Windows Virtual Desktop er VMware sine kostnader engangskostnader, og ikke årlige kostnader. VMware har en engangskostnad på 651 207,90 kr på det året en velger å implementere tjenesten. Denne kostnaden innebærer kjøp av lisenser for VMware vSphere og VMware NSX. Disse innebærer flere sikkerhetsfunksjoner som er innebygd, slik som Extended Detection and Response (XDR) og VMware vSphere High Availability som er medregnet i prisen for lisensene. Vi ser også at VMware krever forholdsvis mer administrasjon for å drifte infrastrukturen enn WVD.

Når vi sammenligner de estimerte kostnader (TCO), kan vi se at Windows Virtual Desktop koster betraktelig mer enn VMware, men kan dog være mer kost-nytte effektivt med tanke på sikkerhetsfunksjoner og innebygde funksjoner i Azure portalen. Windows Virtual Desktop tilbyr enklere administrasjon av infrastrukturen der det er høy skalerbarhet og fleksibilitet slik at LongLuu kan enkelt skalere etter behovet sitt i bedriften.

8.2. Sikkerhet

Både VMware og Microsoft tilbyr ende-til-endebasert XDR-støtte til sine miljøer. Microsoft leverer XDR som en del av Azure Defender, mens VMware leverer dette som en integrert tjeneste i vSphere. Begge kontrollerer sikkerhet knyttet til blant annet e-post, nettverk, servere og sky, og fjerner trusler som oppdages. Selve XDR-teknologien er stort sett den samme for begge tjenestene, mens Microsoft har kombinert XDR og Azure Sentinel for ytterligere tilgang til data fra andre sikkerhetselementer, slik som brannmur.

VMware vSphere håndterer feilede VM-er med High Availability, mens denne funksjonaliteten er innebygd i WVD. Ulempen her er at man ikke får samme mulighet til å velge hvordan feil skal håndteres, og man får ikke dratt nytte av applikasjonovervåkningsfunksjonen som vSphere High Availability tilbyr.

Endpoint Protection er tilgjengelig i begge løsningene, men for VMware er man nødt til å gå til anskaffelse av Carbon Black Cloud Endpoint-tjenesten fra VMware for å dra nytte av tilsvarende tjeneste som er tilgjengelig for WVD. Dette vil isåfall bli en ekstra kostnad og mer oppsett. Endpoint Protection er en del av Azure Defender og er derfor tilgjengelig i eksempelmiljøet vi har tatt for oss i dette prosjektet, i tillegg til de andre tjenestene som er tilgjengelig gjennom Azure Defender. Sikkerhetsmessig vil begge Endpoint Protection-tjenestene kunne yte tilnærmet lik grad av økt sikkerhet da de bygger på samme prinsipp.

NSX gir VMware en fordel ovenfor WVD når det kommer til nettverkssikkerhet. Det betyr ikke at nettverkssikkerheten i WVD er å regnes som utilstrekkelig, kun at VMware yter ytterligere sikkerhet på dette gjennom å tilby denne tjenesten. Begge tjenestene gir også meget gode muligheter for overvåkning av status og loggføring, WVD med Azure Monitor og Audit Logs, og VMware vSphere med High Availability og loggføring i NSX.

VMware vSphere tilbyr ikke samme funksjonalitet som WVD når det kommer til Reverse Connect, Screen Capture Protection og FSLogix. Det er mulig å konfigurere tofaktorautentisering, men de har ingen egen autetiseringsapp slik som Microsoft har med Microsoft Authenticator (26).

8.3. Brukervennlighet

Brukervennlighet er viktig for de fleste bedrifter og vil være en viktig faktor når man velger hvilken virtualiseringstjeneste man vil ta i bruk. Det kan som nevnt tidligere påvirke sikkerhet da et system som ikke er intuitivt kan føre til brukerfeil som går utover sikkerhet (slik som tildeling av feil rettigheter og uheldig sletting av data som resultat av dette). Begge løsningene vi har sett på virker til å være utviklet for å være brukervennlige, men vi vil se litt på hva som gjør de brukervennlige og hvordan de stiller i forhold til hverandre.

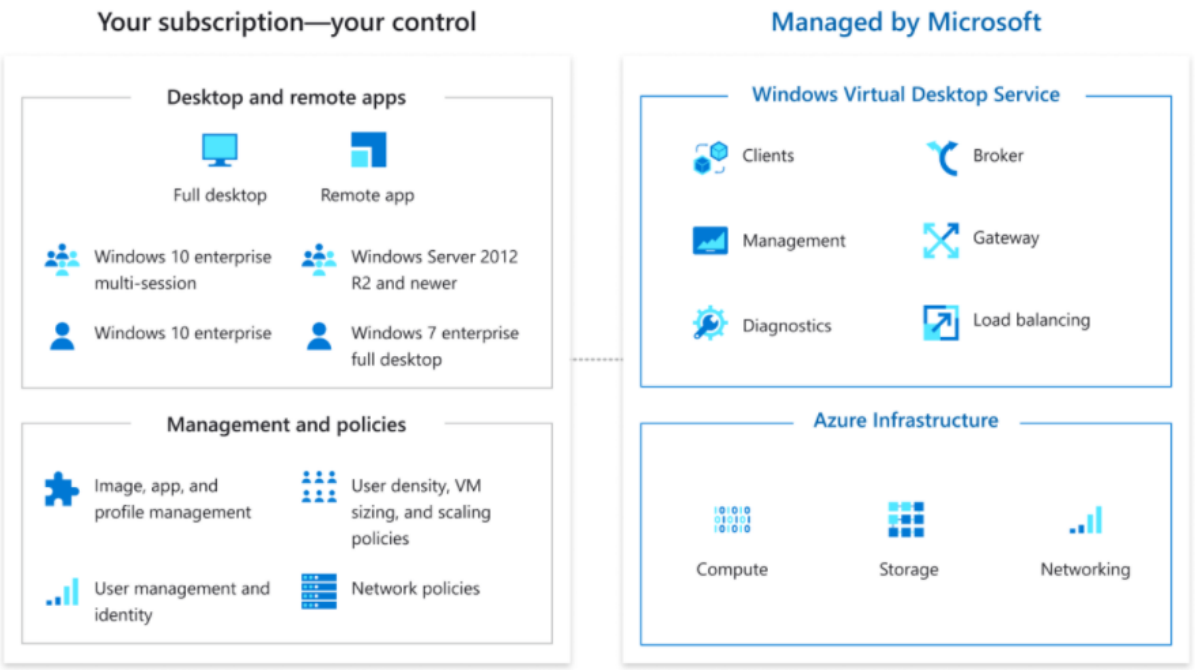
8.3.1. Windows Virtual Desktop

Windows Virtual Desktop er som nevnt et Microsoft Azure-basert system, som betyr at man kan benytte seg av en brukervennlig Azure-portal for å overvåke, administrere og opprette nye ressurser i Azure. Man får mulighet til å tilpasse portalen etter ens egen preferanse slik at man får bedre oversikt over alle ressursene sine i Azure (30).

Ansatte får tilgang til skrivebordet sitt uavhengig av lokasjon (forutsetter tilgang til internett), uten at det går på bekostning av

effektivitet og sikkerhet. Alle brukere må gjennom Multi-Factor Authentication for å få tilgang til ressursene sine. Denne funksjonen oppfyller LongLuus krav for hjemmekontor hvor sikkerheten opprettholdes på et høyt nivå.

Siden Windows Virtual Desktop er en tjeneste levert av Microsoft, finner vi en del fordeler med administrasjon av infrastrukturen. LongLuu administrerer skrivebordene, applikasjoner og retningslinjer. Microsoft har også forenklet distribusjonen av applikasjoner og løsningen er svært skalerbar, i tillegg til at de administrerer infrastrukturen i Azure knyttet til blant annet nettverk og lagring. De vedlikeholder tjenester i Windows Virtual Desktop slik at det er henholdsvis mindre krevende å drifte WVD enn VMware.



Figur 20 - Oversikt over administrasjonen av Windows Virtual Desktop (31).

8.3.2. VMware

VMware sørger for god oppetid ved hjelp av vSphere High availability slik at brukere har kontinuerlig tilgang til sin maskin. VMware NSX

forenkler også nettverkovervåkningsprossesen ved å tilby visuell oversikt over nettverket. Oppsettet av vSphere gjør det ukomplisert å konfigurere brukerrettigheter for de ulike ressursene man innehar. Man møter derimot bratt læringskurve når man først skal ta i bruk vSphere, og det er en del å sette seg inn i. Når man først har kommet i gang er bruk av dette systemet meget håndterlig, men det tar litt tid å "få inn i fingrene". Dette er noe vi selv har opplevd, og har sett eksempler på at andre også opplever (30). Her vil vi påstå at WVD er lettere å sette seg inn i da det er mer intuitivt.

8.3.3. *Infrastructure as Code*

Når det gjelder brukervennlighet er det verdt at det kan være praktisk å utføre en implementering med et script, kalt Infrastructure as Code. Vi kan benytte script for implementering av både VMware og Windows Virtual Desktop. IaC brukes til å administrere IT-infrastruktur med maskinleselige konfigurasjonsfiler. Man finner IaC som verktøy i ARM Templates. IaC kjøres som et script, hvor vi får en konsistent infrastruktur som kan forhindre menneskelige feil. Det gir også en bedre oversikt over infrastrukturen gjennom et versjonskontrollsystem. Videre er IaC gjenbrukbar; samme kode kan brukes gjentatte ganger. I tillegg er det idempotent slik at det blir orden i systemet uten at det lages flere kopier av samme script.

8.4. Oppsummering

Vi har sett på sikkerhet, pris og brukervennlighet knyttet til WVDs og VMwares virtualiseringstjenester, med økt fokus på sikkerhet. Ved å ta for seg utvalgte tjenester og funksjoner som tilbys av disse aktørene har vi gitt et bilde på hva bedriften kan forvente ved å benytte tjenestene til det de har behov for. Under har vi satt opp tabeller som kort oppsummerer resultatene av analysen av de to virtualiseringstjenestene og hvordan disse stiller opp mot hverandre basert på fokusområdene vi har gjennomgått.

	Sikkerhet	
	Vurdering	**Begrunnelse**
Windows Virtual Desktop	6/10	Relativt høy grad av sikkerhet, med forbedringspotensial innen nettverkssikkerhetsverktøy.
VMware	8/10	Viser også høy grad av sikkerhet, og stiller sterkt innenfor nettverkssikkerhet.

Tabell 6 - Oppsummering av sikkerhet

	Pris	
	Vurdering	**Begrunnelse**
Windows Virtual Desktop	7/10	Prisen er høyere enn estimatet vi har gjort for VMwaren. Man betaler periodevis og for mengden ressurser man velger å gå for. Man har også allerede tilgang om man eier Windows-lisens
VMware		Prisen er lavere enn estimatet for WVD, og man betaler en

	9/10	engangssum. Det er verdt å merke at man får mindre for prisen med tanke på verktøy og funksjoner. Ønsker man tilgang til lignende verktøy må man kjøpe disse i tillegg.

Tabell 7 - Oppsummering av pris

	Brukervennlighet	
	Vurdering	**Begrunnelse**
Windows Virtual Desktop	8/10	Azure-portalen er brukervennlig og man har tilgang på velordnede oversikter over systemet.
VMware	6/10	VMware vSphere krever litt tid å sette seg inn i, men viser seg å være brukervennlig når man har benyttet seg av tjenesten en liten stund.

Tabell 8 - Oppsummering av brukervennlighet

9. Konklusjon og videre arbeid

Hensikten med å vurdere sikkerhet i virtualiseringstjenester er å finne en løsning som gir høy grad av sikkerhet i form av overvåkning, sikkerhetsvarsling ved angrep, håndtering og loggføring av hendelser. Systemet skal utføre preventive tiltak som kan hindre sikkerhetsbrudd. Etter en grundig undersøkelse kan vi se at både Windows Virtual Desktop og VMware vSphere egner seg til å sikre den daglige driften for LongLuu. Windows Virtual Desktop er mer kostbar enn VMware, men kan gi en større fordel for LongLuu på lang sikt. VMware stiller sterkt med nettverkssikkerhet mens Windows Virtual Desktop er mer brukervennlig.

LongLuu skal etter dette prosjektet beslutte om de ønsker å implementere en av disse virtualiseringstjenestene. Videre arbeid avhenger av bedriftens beslutning for hvilken tjeneste de ønsker. Implementering kan utføres av bedriften selv eller av eksterne konsulenter. Prosjektgruppen tilbyr å stille som ekstern konsulent for implementasjon og gi support der det er ønskelig gjennom en serviceavtale.

Prosjektmedlemmene skal avslutningsvis utarbeide en sluttrapport for dette prosjektet, som ferdigstilles den 20. mai 2021. Denne skal inneholde den nyeste versjonen av forstudierapport, designrapport og driftsrapport.

4. Referanseliste

1. Windows Virtual Desktop Pricing [Internett]. Microsoft; 2021 [Hentet 25. januar 2021]. Tilgjengelig fra: https://azure.microsoft.com/en-us/pricing/details/virtual-desktop/

2. VMware vSphere Enterprise Plus [Internett]. VMware; 2021 [Hentet 29. april 2021]. Tilgjengelig fra: https://store-us.vmware.com/vmware-vsphere-enterprise-plus-284281000.html

3. What is FSLogix? [Internett]. Microsoft; 08. juli 2019 [Hentet 16. februar 2021]. Tilgjengelig fra: https://docs.microsoft.com/en-us/fslogix/overview

4. Security best practices [Internett]. Microsoft; 2021 [Hentet 13. februar 2021]- Tilgjengelig fra: https://docs.microsoft.com/en-us/azure/virtual-desktop/security-guide

5. How vSphere HA Works [Internett]. VMware; 2020 [Oppdatert: 20. juli 2020; Hentet: 13. april 2021]. Tilgjengelig fra: https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.avail.doc/GUID-33A65FF7-DA22-4DC5-8B18-5A7F97CCA536.html

6. Set up Azure multifactor authentication for Windows Virtual Desktop [Internett]. Microsoft; 10. oktober 2020 [Hentet 22. mars 2021]. Tilgjengelig fra: https://docs.microsoft.com/en-us/azure/virtual-desktop/set-up-mfa

7. Tutorial: Configure Profile Container to redirect User Profiles [Internett]. Microsoft; 28. juni 2019 [Hentet 28. mars 2021]. Tilgjengelig fra:

https://docs.microsoft.com/en-us/fslogix/configure-profile-container-tutorial

8. Granheden, T. Screen Capture Protection for Windows Virtual Desktop [Internett]. [Sted ukjent]: [Utgiver ukjent]; 22. januar 2020 [Hentet 15. mars 2021]. Tilgjengelig fra: http://www.tbone.se/2021/01/22/screen-capture-protection-for-windows-virtual-desktop/

9. Windows Virtual Desktop Profile Management [Internett]. Apps4Rent.com; 2021 [Hentet 23. april 2021]. Tilgjengelig fra: https://www.clouddesktoponline.com/blog/windows-virtual-desktop-profile-management

10. What is Conditional Access in Azure Active Directory? [Internett]. Microsoft; 21. januar 2021 [Hentet 1. mai 2021]. Tilgjengelig fra: https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview

11. Understanding Windows Virtual Desktop network connectivity [Internett]. Microsoft; 16. november 2020 [Hentet 1. mai 2021]. Tilgjengelig fra: https://docs.microsoft.com/en-us/azure/virtual-desktop/network-connectivity

12. Microsoft Endpoint Protection for Azure Customer Technology Preview Privacy Statement [Internett]. Microsoft; 2012 [Oppdatert mars 2012; Hentet 1. mai 2021]. Tilgjengelig fra: https://azure.microsoft.com/en-gb/support/legal/endpoint-protection/

13. Connect Azure Defender data to Azure Sentinel [Internett]. Microsoft; 7. september 2020 [Hentet 4. mai 2021]. Tilgjengelig fra: https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-security-center

14. Quickstart: On-board Azure Sentinel [Internett]. Microsoft; 14. oktober 2020 [Hentet 4. mai 2021]. Tilgjengelig fra:

https://docs.microsoft.com/en-us/azure/sentinel/quickstart-onboard

15. Enable per-user Azure AD Multi Factor Authentication to secure sign-in events [Internett]. Microsoft; 17. august 2020 [Hentet 5. mai 2021]. Tilgjengelig fra: https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-userstates#view-the-status-for-a-user

16. Create a Log Analytics workspace in the Azure portal [Internett]. Microsoft; 18. mars 2021 [Hentet 5. mai 2021]. Tilgjengelig fra: https://docs.microsoft.com/en-us/azure/azure-monitor/logs/quick-create-workspace

17. Microsoft Secure Score [Internett]. Microsoft; 1. mai 2020 [Hentet 5. mai 2021]. Tilgjengelig fra: https://docs.microsoft.com/en-us/microsoft-365/security/defender/microsoft-secure-score?view=o365-worldwide

18. XDR (Extended Detection and Response) [Internett]. VMware; 2021 [Hentet 14. april 2021]. Tilgjengelig fra: https://www.vmware.com/topics/glossary/content/xdr-extended-detection-and-response.html

19. vSphere HA Security [Internett]. VMware; 2021 [Oppdatert 20. juli 2020; Hentet 15. april 2021]. Tilgjengelig fra: https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.avail.doc/GUID-7442EF04-56C9-4910-ACBA-DF42E97ED311.html

20. Priser på Azure Sentinel [Internett]. Microsoft; 2021 [Hentet 18. april 2021]. Tilgjengelig fra: https://azure.microsoft.com/nb-no/pricing/details/azure-sentinel/

21. Priser på Azure Monitor [Internett]. Microsoft; 2021 [Hentet 18. april 2021]. Tilgjengelig fra: https://azure.microsoft.com/nb-no/pricing/details/monitor/

22. How Does VMware NSX Security Work [Internett]. Palo Alto Networks; 2021 [Hentet 18. april 2021]. Tilgjengelig fra: https://www.paloaltonetworks.com/cyberpedia/how-does-vmware-nsx-security-work#:~:text=VMware%20NSX%C2%AE%20is%20a,and%20within%20virtual%20server%20infrastructures.&text=As%20the%20direct%20descendent%20of,based%20on%20VMware%20vSphere%C2%AE

23. Priskalkulator [Internett]. Microsoft; 2021 [Hentet 20. april 2021]. Tilgjengelig fra: https://azure.microsoft.com/nb-no/pricing/calculator/

24. VMware NSX [Internett]. Virtual Graffiti Inc; 2021 [Hentet 20. april 2021]. Tilgjengelig fra: https://www.virtualizationworks.com/NSX.asp

25. Introduction to Azure Defender [Internett]. Microsoft; 30. september 2020; [Hentet 20. april 2021]. Tilgjengelig fra: https://docs.microsoft.com/en-us/azure/security-center/azure-defender

26. Configuring VMware Verify for Two-Factor Authentication [Internett]. VMware; 2019 [Oppdatert: 31. mai 2019; Hentet 20. april 2021]. Tilgjengelig fra: https://docs.vmware.com/en/VMware-Workspace-ONE-Access/19.03/idm-administrator/GUID-FE8A5B1C-BC17-4A5C-BC8D-614C5EE4057A.html

27. Roussey B. Pick your poison: VMware vShere VS. Microsoft Hyper-V [Internett]. Sted: Sacramento, CA; 23. november 2016 [Hentet 20. april 2021]. Tilgjengelig fra: https://techgenix.com/vmware-vsphere-vs-microsoft-hyper-v/

28. Windows Virtual Desktop [Internett]. Microsoft; 2021 [Hentet 16. april 2021]. Tilgjengelig fra: https://azure.microsoft.com/nb-no/services/virtual-desktop/#security

29. What is Infrastructure as Code [Internett]. Microsoft; 31. mars 2021; [Hentet 04. mai 2021]. Tilgjengelig fra: https://docs.microsoft.com/en-us/azure/devops/learn/what-is-infrastructure-as-code

30. Microsoft Azure-portal [Internett]. Microsoft; 2021 [Hentet 04. mai 2021]. Tilgjengelig fra: https://azure.microsoft.com/nb-no/features/azure-portal/

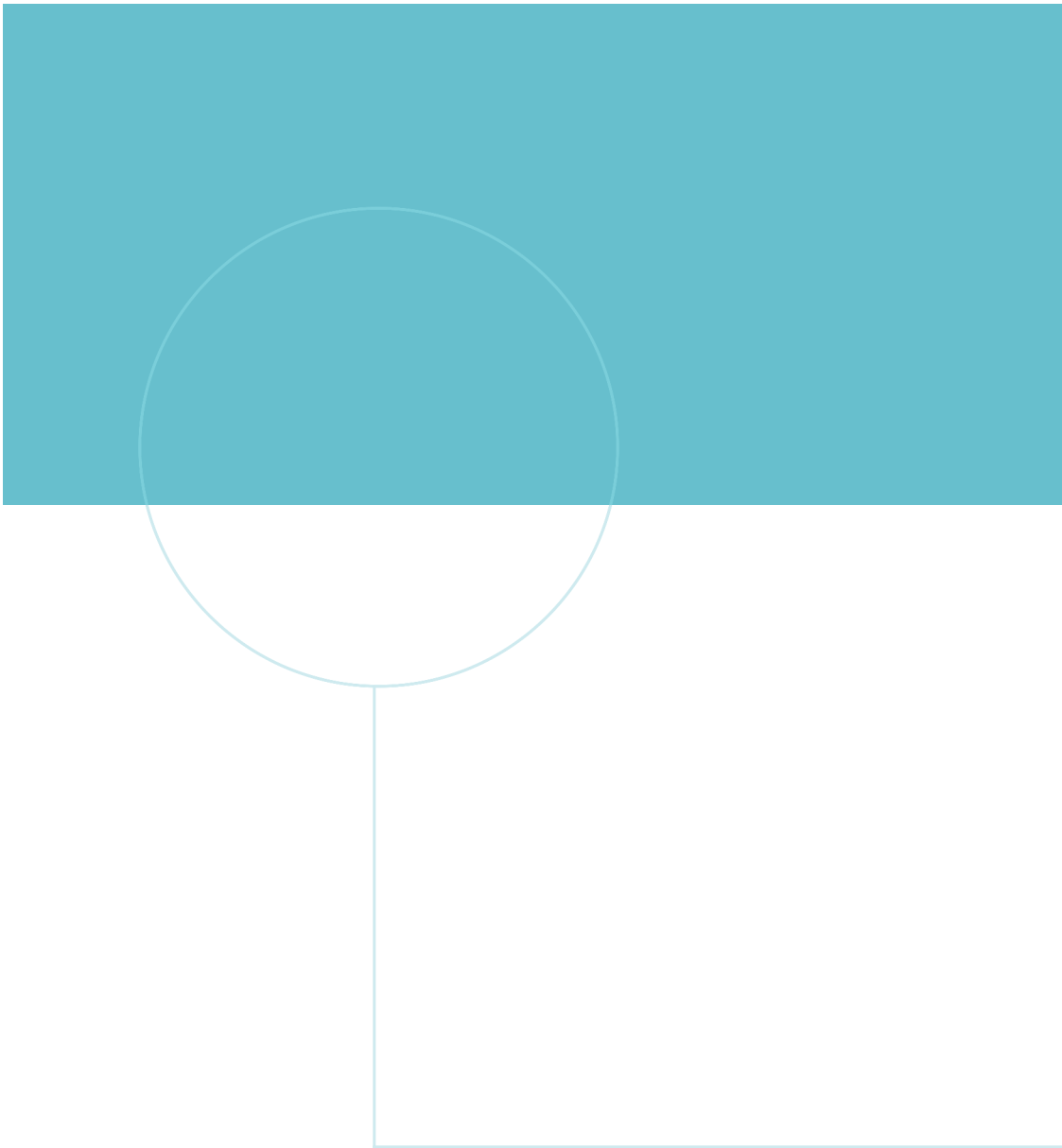
31. VMware Online Store [Internett]. VMware; 2021 [Hentet 04. mai 2021]. Tilgjengelig fra: https://store-us.vmware.com/vmware-vsphere-enterprise-plus-284281000.html

5. Figurliste

6. Tabelliste

7. Vedlegg

1. Bachelor_finalVersion.mpp, GANTT-diagram som viser prosjektplanen for bacheloroppgaven.



NTNU
Kunnskap for en bedre verden

sopra steria