Innhold

Fornying og forbetring av IT tenester hjå Bømoen internasjonale flyplass

Prosjekt

Bømoen internasjonale flyplass moderniserer sin IT-infrastruktur ved å flytte nesten alle tjenester til skyen. Dette muliggjør levering av tjenester overalt, når som helst, samtidig som infrastrukturen bygger på ei plattform som kontinuerlig oppdateres og forbedres. Ved å benytte nesten 100 % skybaserte løysingar for administrasjon av nettverk, servere og brukarar oppnås ein stabil, skalerbar og framtidsretta plattform som kan drifte flyplassen effektivt.

Mål

Modernisere IT-infrastrukturen for å sikre stabilitet, skalerbarhet og tilgjengelighet

Overføre tjenester til skyen for økt fleksibilitet og tilgjengelighet overalt

Funksjonelle krav

Brukarstyring via Entra ID for sentralisert autentisering

Automatisert utrulling av klientenheter med Intune og Autopilot

Implementere Microsoft 365 for produktivitet og kommunikasjon

Sikkerhetskopiering ihht. 3-2-1-prinsippet

Sikkerhetskrav

Implementere Zero Trust-arkitektur

Bruk av Next-Gen Firewall med trafikkinspeksjon

To-faktor autentisering med FIDO2 USB-nøkler og Windows Hello for Business

klienttrafikk skal gå gjennom kryptert Always-on VPN

Tekniske rammer

Redundans for høg oppetid på kritisk infrastruktur

Bruke skybaserte løysningar der det er best.

Lover og regler

Følge relevante sikkerhetsstandarder og personvernlover.

Tilgang til verktøy og digitale tenester

Brukarar

Alle brukarar blir oppretta i Entra ID. Dette er for å få same kilde for på logging til alle tenester og einingar. Alle administratorar blir satt opp med PIM for rolletildeling. 2 forskjellige brukarar blir oppretta for å skile på konto for dagleg bruk og administratorkontoar.

Einingar

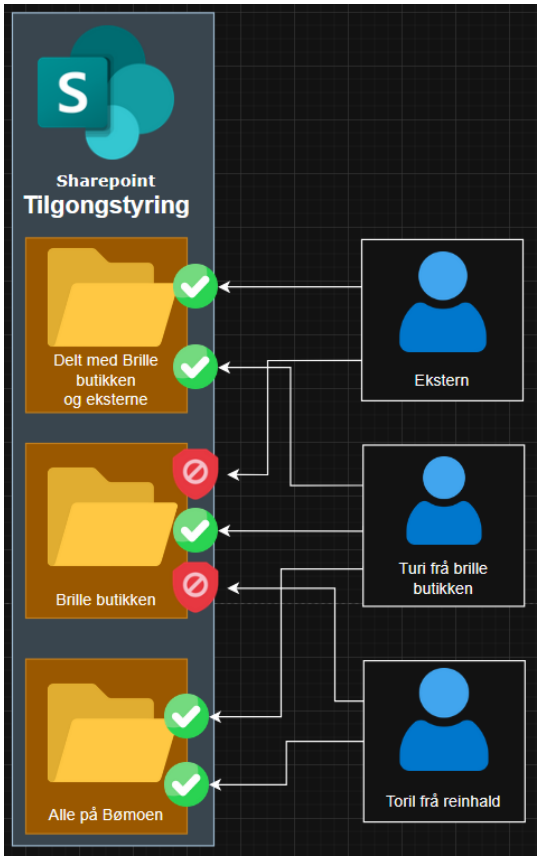
Einingane til brukarane blir innrullert med Autopilot og Intune for enkel installasjon vedlikehald og utrulling av applikasjonar på klientar sine einingar.

Tenester

Alle brukarar får Microsoft sin 365 lisens. Då får alle brukarar tilgang till Office 365 pakka, Exchange og SharePoint. Med dette kan alle nytte nettprat, E-post og filutveksling også utanfor bedriftas nettverk.

Det blir anskaffa ei brukerstøtte SAAS løysing for å enkelt drive brukerstøtte og altid ha tilgengleg ein platform for å ta imot brukarar og hjelpe dei med deira problem. Samt ein passwordmanger for å administrere password/nøklar og serfikat til tenestene.

Som kasseløysing tar eg i bruk zettle for ei simpel og modere betalingsløysing for kundar og ansatte.



Fysisk Infrastruktur

Løysinga under er satt opp får å behalde høg oppetid for å sleppe store komersielle tap under evetuell nedetid. Den kan lett skalerast opp eller ned til å tilpasse seg kundens behov om oppetid og budsjett. For eksempel innkjøp av redundante løysningar som fleire serverar, switchar, brannmurar og Internet linjer.

Serverar

Totalt blir det satt opp 4 serverar, tre som hypervisor cluster og 1 for sikkerheit kopiering av clusteret. Proxmox VE cluster blir brukt for å køyre virtuelle maskiner. Clusteret blir satt opp med CEPH for rask lagring med høg tilgjengelegheit sjølv under tap av serverar. Det blir og satt opp ein Proxmox backup server for sikkerheitskopi av Proxmox clusteret

Lokale Tenester

Det blir satt opp eit lokalt cluster for å ha moglegheit til å køyre og teste tenester lokalt skulle det bli nødvendig. Sikkerheitskopi løysinga blir satt opp på clusteret for å kunne ha ein lokal sikkerheitskopi over lang tid til ein lav pris.

Det installerast Gitlab og Semphore for å ha ein solid lagrings platform for konfigurasjon til diverse skytenester, serverar og netverksinfrastruktur. Samt dei er gode

automatisjonsverktøy for å skubbe ut konfigurasjonen. Dette blir og brukt for vedlikehald, oppdateringar og automatisere oppgåver.

Det blir og satt opp lokal Grafana og Loki for å kunne behalde loggar og data over lengre tid frå diverse kildar til ein mykje lågare kostnad.

For å dele ut IP-adresser blir det installert ein DHCP server i same cluster. For å halde dukumentasjon på kva som er kva blir det satt opp ein lokal Netbox instqanse for å dokumentere nettverket.

Netverk

Nettverksutstyret som blir kjøpt inn er HPE aruba for å best kunne nytte deira skyteneste HPE Aruba Networking Central. Aruba central blir konfigurert med «Infrastructure as code» og blir konfigurert via Semaphore med git som datakilde for all konfigurasjon. Dette er for å altid ha ein lokal versjon av konfigurasjon og lett kunne endre, oppdatere og rulle tilbake konfigurasjon.

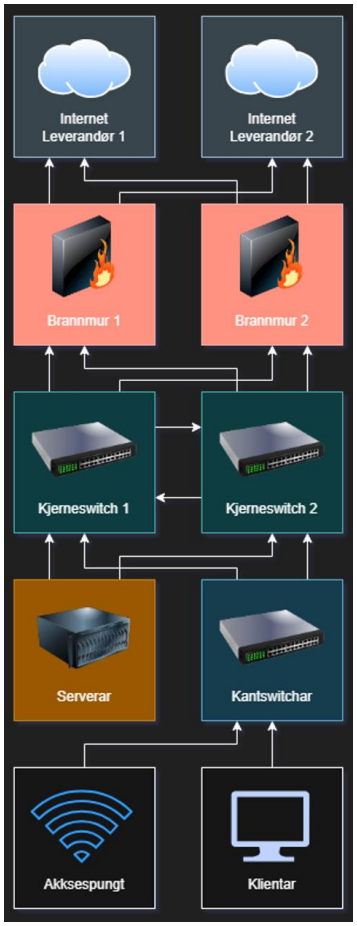
Nettverket blir satt opp med redundante kjerneswitchar for tilkopling til serverar og kantswitchar. Det blir satt opp redundante brannmurar for høgast mogleg oppetid i lag med doble Internet linjer.

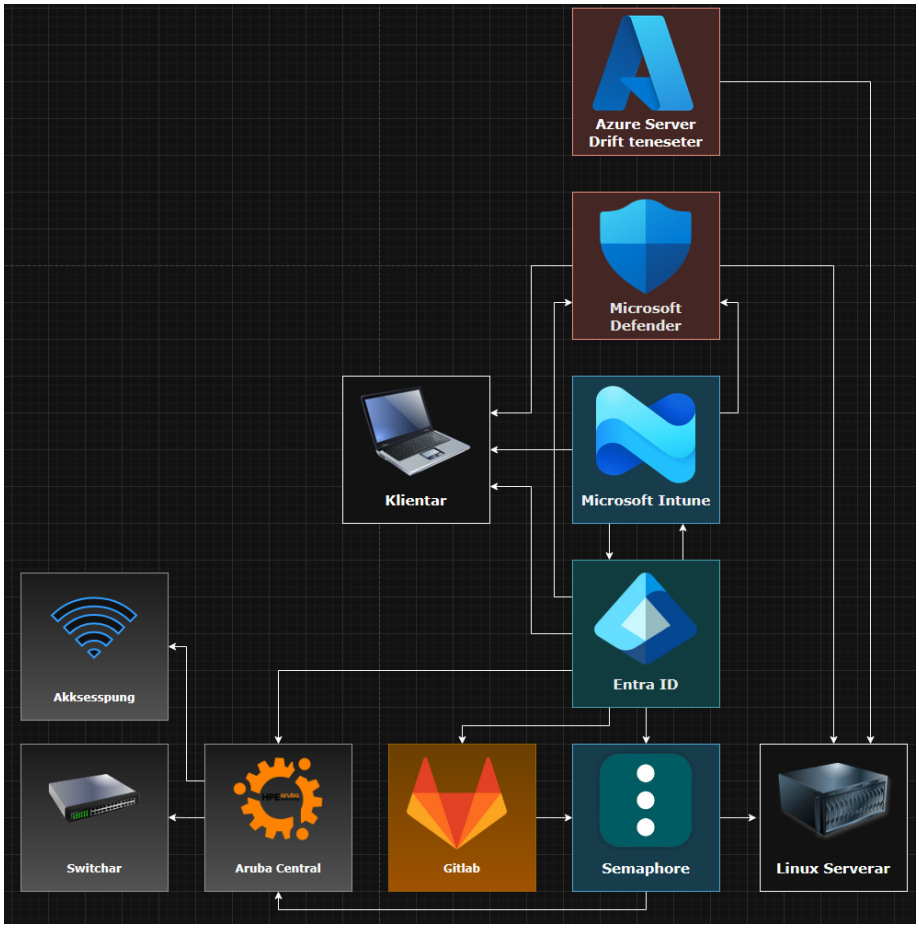
For å unngå unødvendig nedetid blir switchar og serverar sat opp med dobbel kabling slik at dei er kopla til kvar sin kjerneswitch.

Trådlaust nett vert sat opp med aksesspunkt og kompatibel kontroller for enkel administrering av alle aksesspunkta.

Sikring av maskinvare

Alt av datautstyr blir tilkopla ein online UPS for reingjering av straum, oppetid under korte straumbrud og for trygg og sikker stans i drift utan risiko for å skade på maskinvare. Kritisk netverksutstyr får nødagregat for forsyning av straum under lengre straumbrot.


Internet Leverandør 1
Internet Leverandør 2
Brannmur 1
Brannmur 2
Kjerneswitch 1
Kjerneswitch 2
Serverar
Kantswitchar
Akksespungt
Klientar


Azure Server Drift teneseter
Microsoft Defender
Klientar
Microsoft Intune
Akksesspung
Entra ID
Switchar
Aruba Central
Gitlab
Semaphore
Linux Serverar

Sikkerheit

Nettverka og sky tenestene blir konfigurert med Zero Trust og Defense in depth tankegongen. Det vil seie at ein ikkje stolar på nokon eller noko og ein skal alltid anta verste. Samt at ein skal ha fleire lag med beskyttelse og sikre kvart ledd at tenestene. Det blir gitt tilgang til kunn det som trengst til og mellom tenester i nettet.

Det blir tekke i bruk ein «Next-Gen Firewall» med støtte for dekryptering og inspeksjon av trafikk. Dette er for å kunne oppdage og stoppe skadeleg programvare og trafikk før den kan gjere skade. DNS og URL filtrering blir satt opp for å dempe phishing kampanjar og farleg trafikk til internett.

Generelt sikkerheit

Det blir tatt i bruk passkeys via fido2 USB nøklar i lag med SSO for å trygge organisasjonen. I lag med dette blir Windows Hello for Business tatt i bruk for å gi sluttbrukarar ein enklare kvardag samt ei trygg og sikker på logging. På loggin blir låst ned til klientmaskiner administrert av organisasjonen. Alle tenester blir då konfigurert med 2 faktor og organisasjonen er sikra mot blant anna phishing and andre angrepsformar. Microsoft Defender blir tatt i bruk får å overvake og stoppe angriparar. Samt det blir konfigurert til å gjere det same i skyenestar som Microsoft Office 365

Alle klientar og serverar får installert Microsoft Defender for Endpoint. Dette gir vern mot skadeleg programvare, overvaking av mistenkjeleg åtferd, og moglegheit for å blokkere uønska intern trafikk. Defender blir òg brukt til å samle og sende loggar til sentral sikkerheitsovervaking.

Klientar

Alle klientmaskiner får installert ein «Always on VPN» løysing. Det vil seie at klientar sine einingar alltid er tilkopla organisasjonens nett og alt av data går via ein krypter VPN tunnel. Einingane vil då alltid befinne seg i eit eige isolert nettverk og vere verna uansett kvar dei befinn seg. Dei er og sikrar sidan all trafikk går via ein trygg brannmur. Samtidig får brukaren tilgang til interne ressursar på ein trygg måte.

Frå eit administratorperspektiv gir dette moglegheit for enkel tilgangstyring og identifisering av brukarrelatert nettverkstrafikk. Og sikra nettet då dette vil vere einaste veg inn til tenestene ved unntak av nettet i data senteret.

Internt nettverk

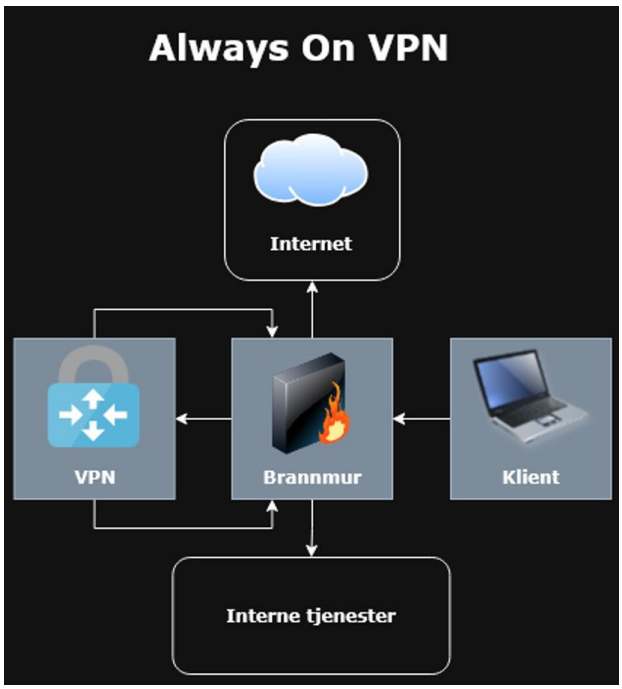
Internt nett blir segmentert i stor grad for å skile og beskytte dei forskjellige tenestene. Ved å nytte mykje segmentering i nettet får ein og køyrt meir trafikk gjennom brannmur og får separert tenestene skulle ein server bli kapra.

Netta ved unntak av klientnettverket blir satt opp i trå med VG testen og vil kunn ha tilgang til resursane som er nødvendig får å vedlikehalde og halde tenestene i gong. Proxmox sin SDN blir nytta for enkel mikrosegmentering mellom tenester der det trengst. Dette gjer det mogleg å separere trafikk internt mellom virtuelle maskiner utan behov for ekstra netverkskonfigurasjon.

Trygging av fysisk nett

Alt av fysisk nettverkstilgang, inkludert nettverksuttak, trådlaust nett og tilgang til datarom, blir sikra med RADIUS-basert autentisering. Dette sikrar at berre godkjende einingar og brukarar får tilgang til det interne nettverket. Datarom blir og sikra fysisk med låste dører.

Alt av klient einingar og serverar får diskkryptering for å sikre mot tjuveri.



Sikkerheitskopiering av data

Sikkerheitskopi er ekstremt viktig, å ha ein sikkerheitskopi på lager de det som kan redde deg eller organisasjonen. Om du skulle vere offeret for et dataangrep eller berre slette feil filer. Då gir et bra system for sikkerheitskopiering moglegheit for rask og enkel gjenoppretting av viktige og kritiske data.

Eg vel dermed å følge 3, 2, 1 standen der målet er å ha 3 kopier av dataen, på 2 forskjellige typar lagring der 1 er ekstern. Denne løysinga er trygg effektiv og gir sikkerheit sjølv i krisesituasjonar, samt fleksibilitet.

Eg vel å nytte dei 3 løysingane under for å oppnå dette. Likt for alle løysingane blir dei konfigurert som uforanderleg (immutable) samt autentisering og kommunikasjon blir haldt separat frå dei andre tenestene.

Løysingane under er skalerbar og kan utvidast etter behov raskt. Samt ein kan enkelt auke mengde sikkerheitskopiar over fleire leverandørar og lokasjonar. For å sikre sikkerheitskopiane er all pålogging seperat frå vanleg brukar og administrasjonspålogging.

Virtuelle maskiner

Av alle virtuelle maskiner blir det oppretta ein full sikkerheitskopi som blir lasta opp til Proxmox Backup Server. Dette er for å få best kvalitet mogleg på sikkerheitskopi løysinga då det er eit system designa for implementasjon med den valte hypervisoren Proxmox.

Denne nyttast grunna rask og enkel full VM gjenoppretting samt gjenoppretning av individuelle filer. Den er rask og har effektiv lagring med hjelp av snapshots. Dette gjer at ein får utnytte maskinvaren til det fulle.

Andre media

Det blir satt opp eit lokalt Minio s3 cluster for sikkerheitskopiering av all anna data. Dette kan vere data frå Office 365 eller andre skytenester som bør sikkerheitskopierast. Dette gir moglegheit for lett opp lasting og ut henting av data. Det blir konfigurert med snapshots og full kryptering som gir ekstra redundans og beskyttelse. Minio gir moglegheit for lett integrering med alle system då det nyttar s3 standaren.

Ekstern sikkerheitskopi

Som ekstern sikkerheitskopi vel eg ein skytjeneste med støtte for s3. Då det integrerast lett med allereie eksisterande system og gir fleksibilitet i val av leverandør. Skylagringa bli konfigurert til å speglast over fleire datasenter og geografiske lokasjonar for å sikre konstant tilgjengelegheit.

Kostnadsoverslag

Investeringsbudsjett

Utgift	Antall	Pris per enhet	Total
Serverar	4	kr 25 000,00	kr 100 000,00
Brannmur	2	kr 500 000,00	kr 1 000 000,00

Kjerneswitchar	2	kr 400 000,00	kr 800 000,00
Kant switchar	20	kr 12 000,00	kr 240 000,00
Nødaggregat	1	kr 100 000,00	kr 100 000,00
UPS	1	kr 100 000,00	kr 100 000,00
UPS på kant	20	kr 15 000,00	kr 300 000,00
Aksesspunkt	70	kr 2 000,00	kr 140 000,00
Anna netverksutstyr	1	kr 100 000,00	kr 100 000,00
Kjøling	1	kr 20 000,00	kr 20 000,00
PC	250	kr 9 000,00	kr 2 250 000,00
Nettbrett / Telefon	250	kr 3 000,00	kr 750 000,00
TOTAL			5 900 000,00 kr

Driftsbudsjett

Utgift	Antall	Pris per (år)	Pris per månad	Pris per år
PVE lisens	1	kr 6 000,00	kr 500,00	kr 6 000,00
PBS Lisens	1	kr 25 000,00	kr 9 000,00	kr 25 000,00
Aruba Central + Switch og AP lisens	90	kr 1 200,00	kr 9 000,00	kr 108 000,00
Lisens brannmur	2	kr 500 000,00	kr 83 333,33	kr 1 000 000,00
		Pris per (månad)		
Sky lagring (Antall GB)	40000	kr 0,05	kr 2 000,00	kr 24 000,00
Microsoft 365 E3	250	kr 300,00	kr 75 000,00	kr 900 000,00
Microsoft 365 E5 Security	250	kr 100,00	kr 25 000,00	kr 300 000,00
Sharepoint	1000	kr 4,00	kr 4 000,00	kr 48 000,00

TOTAL			kr 207 833,33	kr 2 411 000,00

Kommentar til budsjett

Prisar og frekvens av utstyr tilpassast behov og ønsker om oppetid som vurderast av kunden.

Prisar relatert til skylagrin blir regulert etter behov.

Prisar relatert til lisensar kan regulerast basert på brukarens behov.

Berekraft

Det blir kjøpt nytt datautstyr med god kvalitet som kan vare i mange år.

Nettverkutstyret blir konfigurert til å ha redusert kapasitet og bruke mindre straum i periodar med redusert bruk.

Oversikt over nødvendig tenester og utstyr

Tenester/Programvare

- Sharepoint, Onedrive
- Office 365
- Entra ID
- Intune
- Autopilot
- Aruba Central
- Microsofr Defender
- Minio
- Azure
- Grafana, loki
- Gitlab, semphore
- Proxmox
- Global Protect
- AWS S3
- Technitium
- Windows

- Ubuntu server
- Netbox

Utstyr

- Serverar
- UPS
- Brannmur
- Switchar
- Aksesspunkt
- Anna netverksutstyr
- PCar
- Nettbrett
- Mobiltelefonar

Resursar

PIM:

https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-configure

HPE Aruba networking central:

https://www.hpe.com/no/en/aruba-central.html

Zero trust:

https://www.paloaltonetworks.com/cyberpedia/what-is-zero-trust-network-access-ztna

Next Generation Firewall:

https://docs.paloaltonetworks.com/ngfw

Fido2:

https://www.microsoft.com/nb-no/security/business/security-101/what-is-fido2

Windwos Hello For Business:

https://learn.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/

Microsoft defender:

https://learn.microsoft.com/en-us/defender/

Microsoft defender for endpoint:

https://learn.microsoft.com/en-us/defender-endpoint/

VG testen:

https://gorantomte.no/vg-testen/

Immutable storage:

https://learn.microsoft.com/en-us/azure/storage/blobs/immutable-storage-overview

Proxmox backup server:

https://pbs.proxmox.com/

Minio:

https://min.io/docs/

Gjennomføring av praktisk del

Endringar I oppsett

Grunna mangel på diverse lisensar som for eksempel lissensar i aruba central og Tennant i Azure blir dessa programvarene brukt som erstatning for nemnte sky løysingar.

Ein vil oppnå same mål ved untak av mindre moglegheitar i for eksempel sikkerheitsløysinga og netverksadministasjon.

Teneste	**Ønska oppset**	**Gjennomføring under fagprøve**
Netverksadministasjon	Aruba Central	
Diverse funksjonar i microsoft skytenester	Entra, Intune, Defender, O365	
S3 lagring	Minio	Minio eller garage (grunna usikkerheit i lisensiering)
S3 sky	AWS S3	

Oppgåver som må utførast og tidsrammer

Dag / Tid	Tirsdag	Onsdag	Torsdag	Fredag	Mandag
Før lunch	Klargjering installasjonar, oppdatering av planleggingsdokument	Entra ID, conditional access, O365	Palo alto globalprotect + intune	Grafana + loki	Bonustid til det som skulle trenge meir arbeid
Etter lunch	Instalering klargering klientar og serverar. Konfigurasjon på brannmur	Intune og autopilot	Defender	Dokumentasjon	Bonustid til det som skulle trenge meir arbeid