

Practical Design 2024

Innledning	3
Domenestruktur og Serverkonfigurasjon	3
Domenekonfigurasjon.....	3
Serverroller	4
Active Directory (AD) Servere:	4
DNS Servere	5
DHCP Servere.....	6
Filservere.....	6
Applikasjonsservere	6
Bruker- og Gruppestyring	7
Active Directory Organisational Units (OUs):	7
Geografiske OUs:.....	7
Avdelingsspesifikke OUs.....	7
Grupperettigheter	8
Gruppekonfigurasjoner	8
Rettighetsstyring	8
Spesialrettigheter for Ledelse og Nøkkelpersoner	8
Sikkerhetsprotokoller for GeekGulp Refreshments	9
Nettverkssikkerhet	9
Brannmurer	9
Antivirusprogrammer.....	9
Sikker Internettbruk	9
Password og Lockout Policy.....	10
Sterkere Passordpolitikk	10
Kontoadgangs- og låsepolitikk.....	10
Datakryptering	11
Kryptering av Sensitive Områder	11
Ende-til-Ende Kryptering.....	11
Fil- og Datalagringsløsninger	11
Oppsett av Lagringsområder:.....	11
Restriksjoner og Tilgangskontroll.....	12
Tilgangskontroll og Overvåking:	12
Tilgangslogger	12
Overvåkingsverktøy	13

Regelmessig Revisjon	Feil! Bokmerke er ikke definert.
Backup og Gjenopprettingsstrategier	14
Backup løsninger	14
Brukerdata og Systemkonfigurasjoner	14
Lagringslokasjoner	14
Gjenopprettingsplaner	15
Testing av Gjenopprettingsplaner:	15
Programvareinstallasjon og Vedlikehold	15
Programvare for Regnskapsførere:	15
Windows Deployment Services (WDS)	16
Intranett og Webapplikasjoner	16
Webserver og Hosting	17
Intranettinnhold	17
Arbeidsstasjoner og Brukerenheter	18
Skrivebords konfigurasjoner	18
Skrivebords konfigurasjoner (Eksempler)	19
Sesongarbeidere	19

Innledning

I denne dokumentasjonen skal vi utforske og utforme en komplett IT-infrastruktur for GeekGulp Refreshments, et fremadstormende energidrikkselskap som står overfor en periode med betydelig vekst og ekspansjon. Med hovedkvarter i Mosvik og en planlagt utvidelse til Mjøndalen, er behovet for en robust og skalerbar IT-løsning mer presserende enn noen gang. Vår oppgave er å etablere en domenestruktur som ikke bare understøtter selskapets nåværende operasjoner, men også er klargjort for fremtidig vekst og nye ansatte.

Gjennom denne dokumentasjonen vil vi detaljert beskrive hvordan vi planlegger å opprette nødvendige servere, tjenester, bruker- og gruppestruktur, samt rettigheter som vil støtte både daglig drift og langsiktig skalerbarhet. Det vil legges spesiell vekt på sikkerhet, brukervennlighet og kostnadseffektivitet for å sikre at løsningene ikke bare er teknisk gjennomførbare, men også praktiske for GeekGulp Refreshments å vedlikeholde etter at vår direkte involvering avsluttes.

Dokumentasjonen vil også inkludere spesifikke roller og rettigheter for nøkkelpersonell som **Grank Fulli**, daglig leder som krever full tilgang til det nye domenet, Jon Johansen, IT-konsulenten som vil være ansvarlig for å drifte systemet, og andre viktige medarbeidere som vil ha spesialiserte behov og tilganger.

Domenestruktur og Serverkonfigurasjon

Domenekonfigurasjon

For GeekGulp Refreshments er det strategisk viktig å etablere en kraftig domenestruktur som støtter både nåværende og fremtidige operasjoner. Med tanke på firmaets hovedkvarter i Mosvik og den planlagte utvidelsen til Mjøndalen, tenker jeg at den mest optimale tilnærmingen vil være å sette opp et primært domene med navnet GeekGulp.local og et sekundært domene eller en «**child domain**» for den nye lokasjonen, som

Mjondalen.GeekGulp.local.

Hvorfor har jeg valgt å ha separate domener?

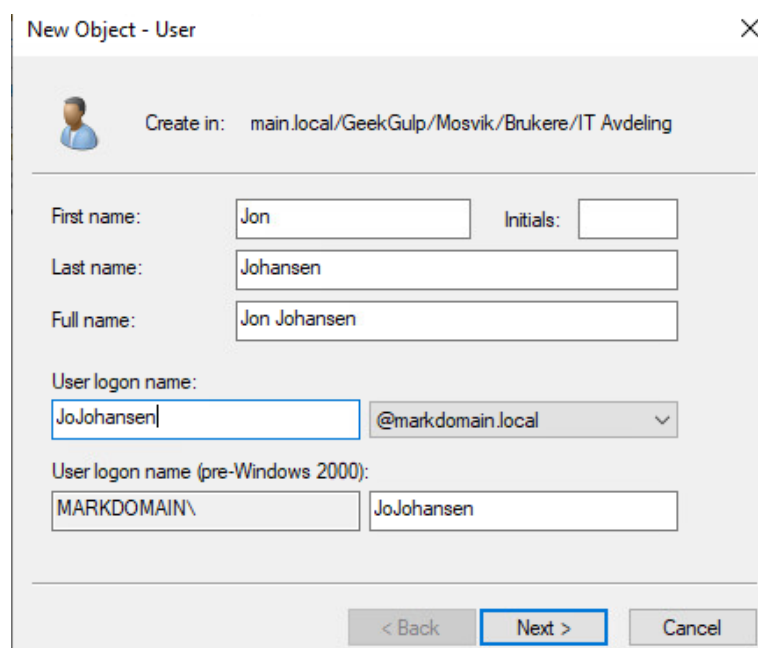
- Ved at vi har separate domener for forskjellige geografiske lokasjoner, gjør dette lettere for oss å jobbe med administrasjonen og sikkerheten. Det gjør det mulig å skreddersy tilgangskontroller og policyer som spesifikt passer for behovene til hver lokasjon. Ved å strukturere domenet på denne måten, kan GeekGulp Refreshments lettere skalere sin IT-infrastruktur i takt med bedriftens vekst, uten å forstyrre eksisterende nettverksoperasjoner.

Computer name	GeekGulpDC1
Domain	GeekGulp.local
Windows Defender Firewall	Private: On
Remote management	Enabled
Remote Desktop	Disabled
NIC Teaming	Disabled
Ethernet0	10.13.101.10, IPv6 enabled

For GeekGulp Refreshments er det kritisk å etablere en solid og lett identifiserbar serverstruktur, som reflekteres i navnet og domenemodellen. Serveren, betegnet som GeekGulpDC1, fungerer som en primær domenekontroller i domenet GeekGulp.local. Dette navnet og domenet gir en klar indikasjon på sin rolle og tilknytning til selskapet, og er avgjørende for enkel administrasjon og skalerbare i et voksende nettverksmiljø.

Navnstandard

For å sikre enkel administrasjon og identifikasjon av brukere i Active Directory, benytter GeekGulp Refreshments en klar og konsistent navnstandard. Brukerkontoer formateres med en kombinasjon av første bokstav i fornavnet og etternavn, noe som demonstreres med brukeren «**Jon Johansen**» hvis brukernavn blir «JoJohansen». Denne metoden sikrer at brukernavnene er intuitive og enkle å huske, samtidig som de forblir unike innen organisasjonen.



New Object - User

Create in: main.local/GeekGulp/Mosvik/Brukere/IT Avdeling

First name: Jon Initials:

Last name: Johansen

Full name: Jon Johansen

User logon name: JoJohansen @markdomain.local

User logon name (pre-Windows 2000): MARKDOMAIN\ JoJohansen

< Back Next > Cancel

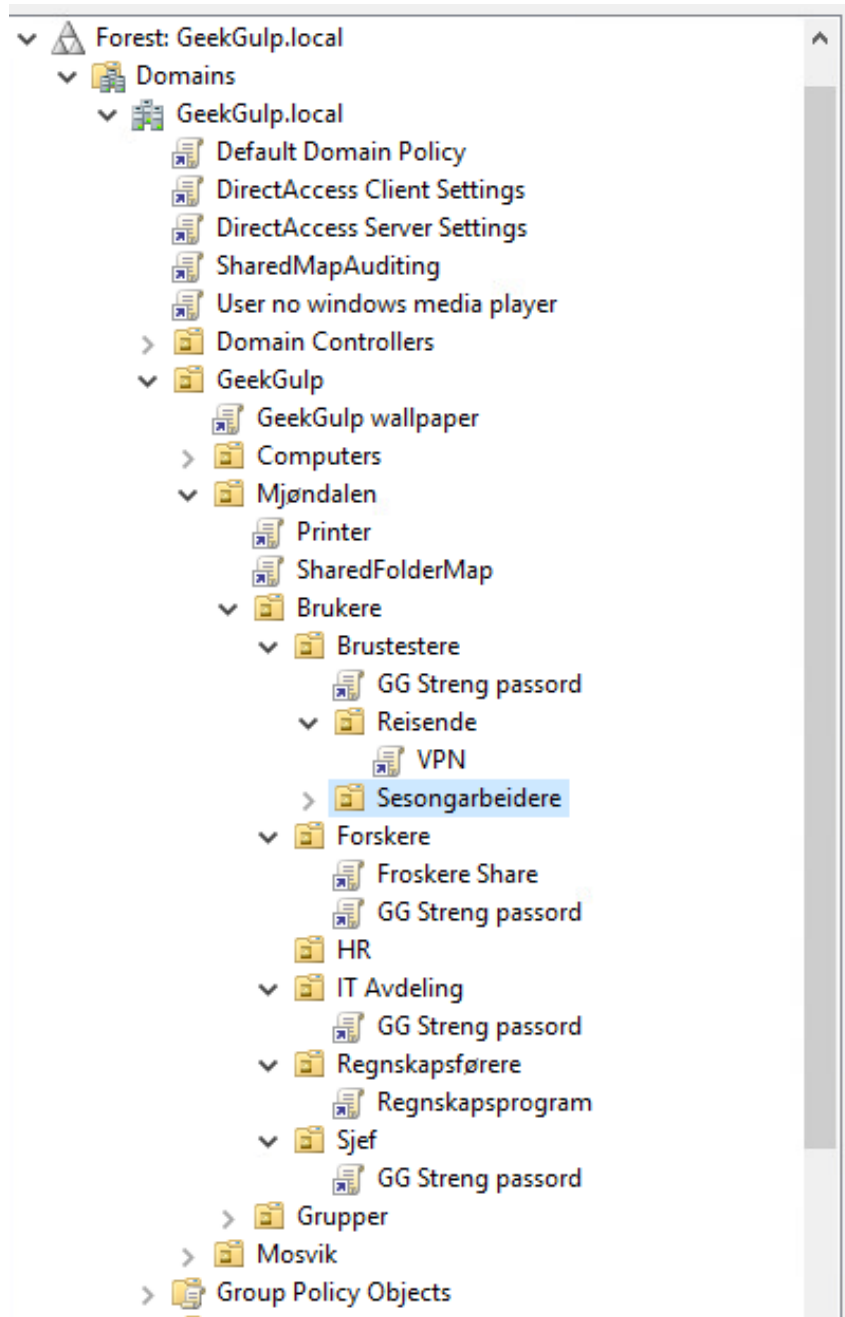
Serverroller

For å støtte domenestrukturen og den daglige driften av GeekGulp Refreshments, seg jeg nødvendig å iverksette flere kritiske serverroller:

Active Directory (AD) Servere:

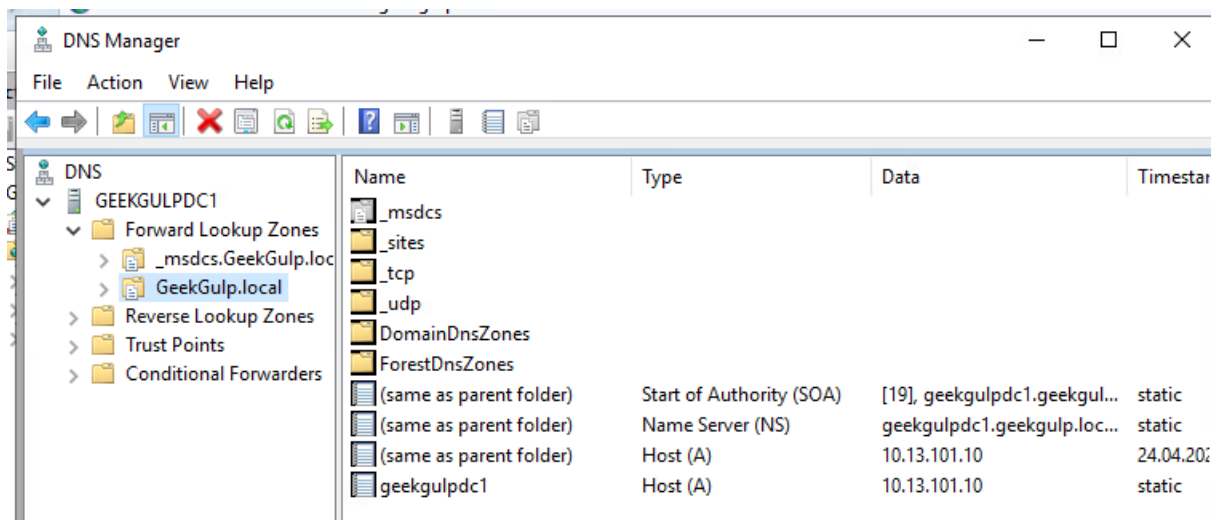
AD-serverne vil fungere som ryggraden i GeekGulp Refreshments' nettverksidentitets- og tilgangsstyring. Disse serverne vil håndtere brukerlogins, tilgangsrettigheter og policyer over hele firmaet.

Eksempel: Første eksemplet vårt kan være brukeren «**Jon Johansen**», en IT-konsulent, vil være ansvarlig for å administrere AD-serverne våre, inkludert brukeroprettelser, passordtilbakestilling, og policyhåndtering.



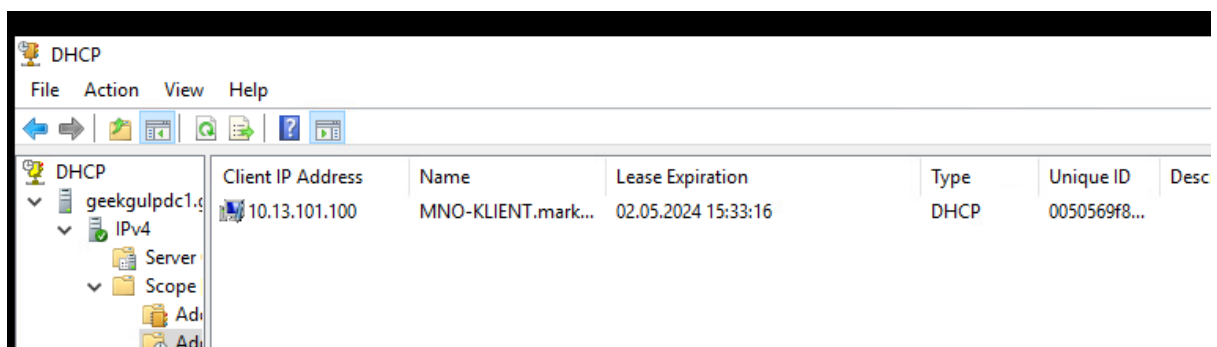
DNS Servere

DNS serverne er kritiske for å omdanne brukervennlige domenenavn (som `www.geekgulp.local`) til IP-adresser. DNS er avgjørende for intern og ekstern kommunikasjon i nettverket. Dette sikrer at ansatte kan få tilgang til interne applikasjoner så vel som internettressurser uten forsinkelser. Litt lengre ned viser jeg et eksempel på hvordan DNS serveren vår kan se ut.



DHCP Servere

DHCP-serverne automatisk tildele IP-adresser til klientmaskiner og enheter innen nettverket, noe som reduserer administrative oppgaver og mulige feilkonfigurasjoner. For konfigureringen til Geek Gulp, vil automatisk IP-adresse tildeling forenkle prosessen med å legge til nye enheter i nettverket, noe som er spesielt nyttig gitt den planlagte veksten og hyppige tillegg av sesongarbeideres utstyr.



Filservere

Filserverne vil være ansvarlige for lagring og forvaltning av alle delte data, noe som sikrer at ansatte har tilgang til nødvendige filer og ressurser. Et eksempel kan være regnskapsførerne brukerne våre. I dette tilfellet vil Fritjof Hoel og Barbro Lefdal (regnskapsførerne) vil ha tilgang til dedikerte delte mapper på filserveren hvor de kan lagre og hente økonomiske rapporter og dokumenter.

Applikasjonsservere

Disse serverne vil hoste diverse forretningsapplikasjoner som er nødvendige for de daglige operasjonene til GeekGulp Refreshments, inkludert regnskapsprogrammer og interne applikasjoner.

Spesialiserte servere for hver rolle sikrer optimal ytelse og effektivitet ved å tillate at hver server er konfigurert for spesifikke oppgaver. Ved å ha dedikerte servere for kritiske funksjoner som AD og DNS, kan GeekGulp Refreshments sikre høyere nivåer av redundans og sikkerhet, noe som er avgjørende for å beskytte mot datatap og sikkerhetstrusler.

Et eksempel som kan vise til dette er følgende: En server kan være dedikert til å kjøre et regnskapsprogram tilgjengelig som en .msi-fil, noe som sikrer at regnskapsførerne alltid har tilgang til oppdaterte applikasjoner og data. Dette vil gjøre hele prosessen enklere, da vi har kun et server dedikerte til disse type oppgaver.

Backup Servere: Vi kan også planlegge ekstra backup servere både onsite og offsite for kritiske servere som vårt AD og filserver, noe som sikrer kontinuerlig tilgjengelighet selv under hardwarefeil eller i katastrofesituasjoner. For DNS og DHCP serverne våre, kan vi for eksempel implementere **failover clustering** for å sikre høy tilgjengelighet og lastbalansering. Dette vil være spesielt kritisk i Mosvik hvor hoved serverparken ligger.

Bruker- og Gruppestyring

Active Directory Organisational Units (OUs):

For å effektivt administrere brukere og datamaskiner innen GeekGulp Refreshments, er det viktig å strukturere Active Directory (AD) med Organisational Units (OUs) som reflekterer selskapets interne struktur og geografiske plassering.

Eksempel (Mosvik OU): Inneholder OUs for hver avdeling som IT, HR, og regnskapsførere. For eksempel, Jon Johansen, IT-konsulent, vil ha administrative rettigheter innen IT OU for å håndtere nettverksressurser og sikkerhetspolicyer.

Eksempel (Mjøndalen OU): Som en ny lokasjon vil denne OU strukturen hjelpe med å rulle ut spesifikke konfigurasjoner som reflekterer behovene til ansatte der, og kan ha mer tilpassede sikkerhetsinnstillinger basert på mindre fysisk sikkerhet sammenlignet med hovedkontoret.

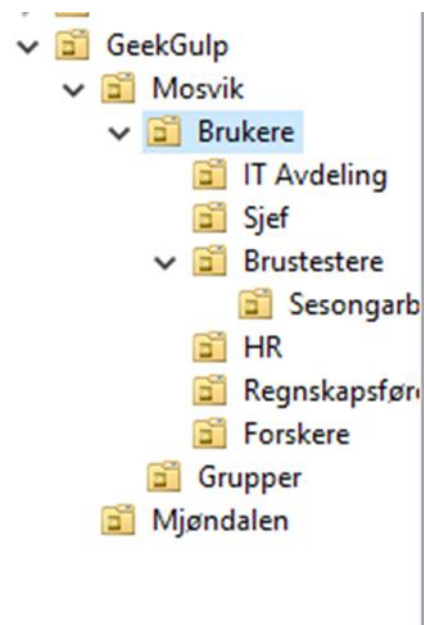
Geografiske OUs:








Vi kan også opprette separate OUs for Mosvik og Mjøndalen. Dette vil tillate lokasjonsspesifikk policyhåndtering og tilgangskontroll, noe som er spesielt viktig ettersom selskapet vokser og ekspanderer til nye områder.

Avdelingsspesifikke OUs

Innenfor hver geografisk OU, kan vi opprette underenheter for IT, HR, regnskapsførere, brustestere og forskere. Dette sikrer at hver avdeling kan administreres separat med tilpassede policyer og tilgangsrettigheter.

Ved å dele opp OUs etter geografisk lokasjon og avdeling, kan IT-administratorene våre enklere håndtere brukerrettigheter og -policyer, noe som er kritisk for sikkerhet og overholdelse av interne regler. Det forenkler prosesser som brukeradministrasjon, distribusjon av programvare og sikkerhetsoppdateringer, da disse kan håndteres målrettet per OU.



Name	Type	Desc
 GR_Brustestere	Security Group...	
 GR_Forskere	Security Group...	
 GR_HR	Security Group...	
 GR_IT Avdeling	Security Group...	
 GR_Regnskapsf...	Security Group...	
 GR_SESONG	Security Group...	
 GR_Sjef	Security Group...	

Grupperettigheter

For å sikre effektiv og sikker tilgang til ressurser og data, er det nødvendig å definere klare grupperettigheter basert på brukerroller og arbeidsoppgaver.

Eksempler:

- **IT Gruppe:** Gir tilgang til serverrom, nettverkskonfigurasjoner, og avanserte systeminnstillinger. Dette er kritisk for personer som

Jon Johansen, som må kunne reagere raskt på IT-utfordringer.

- **HR Gruppe:** Gir tilgang til sensitive personellfiler og lønnsinformasjon. Tobias Flænderssen, HR-ansvarlig, bruker disse rettighetene til å administrere ansattdata, inkludert ansettelser, oppsigelser og kontrakts endringer.

Gruppekonfigurasjoner

Vi kan også opprette sikkerhetsgrupper som IT, HR, Regnskapsførere, Brustestere og Forskere i AD. I tillegg, kan vi tilordne nødvendige tilgangsrettigheter til disse gruppene basert på deres funksjonsbehov.

Rettighetsstyring

Når det gjelder rettighetsstyring, kan vi tilpasse tilgangsnivåene slik at de reflekterer den faktiske nødvendigheten for tilgang i hverdagen, for eksempel gir HR tilgang til personellfiler, mens IT-administratorer har tilgang til serverrom og kritiske systemer. Vi kan også definere grupper med spesifikke tilganger som reduserer risikoen for uautorisert tilgang og mulige sikkerhetsbrudd. Disse vil da begrense muligheten for utilsiktet eller ondsinnet dataendring.

Spesialrettigheter for Ledelse og Nøkkelpersoner

Nøkkelpersoner som Grank Fulli trenger utvidede rettigheter for å utføre sine roller effektivt. Her kommer jeg med noen tidlige eksempler:

Grank Fulli (Daglig Leder): Som daglig leder, trenger Grank Fulli tilgang til alle områder av nettverket for å kunne overvåke bedriftsoperasjoner, økonomiske rapporter og ansattinformasjon. Dette inkluderer spesielle administrative rettigheter som gir ham muligheten til å se over alle avdelingenes aktiviteter.

Forskning OU: Dr. Peppa Tune, kjemiker og forsker, trenger spesielt høye sikkerhetstiltak og tilgang til sensitive forskningsdata. Dette innebærer krypterte lagringsløsninger og begrenset tilgang for andre brukere.

Med dette bak tankene, kan vi konkludere med at ledere og nøkkelpersoner må kunne håndtere bredere aspekter av organisasjonens operasjoner uten begrensninger, noe som krever bredere tilgangsrettigheter. Ved å bruke **Group Policy Objects (GPOs)**, kan vi innføre regler som automatisk iverksetter de nødvendige sikkerhetsinnstillingene for hver gruppe basert på deres OU-tilhørighet. Dette inkluderer automatisk konfigurasjon av skrivebordsmiljøer, applikasjonstilganger, og nettverkstilgangskontroller.

På den andre siden, har vi sesongarbeidere. For disse kan spesielle GPOer settes opp for å automatisk begrense tilgangen deres til internett og visse applikasjoner når de logger på systemet, og sikre at deres arbeidsstasjoner er låst ned til kun de nødvendige funksjonene.

Denne tilnærmingen sikrer at alle avdelinger og nøkkelpersoner har de rettighetene de trenger for å utføre sine jobber effektivt, samtidig som den opprettholder organisasjonens sikkerhetsstandarder. Det gjør det også lettere for IT-avdelingen å administrere og overvåke nettverksaktivitet og brukertilganger sentralt.

Sikkerhetsprotokoller for GeekGulp Refreshments

For å beskytte GeekGulp Refreshments mot mulige trusler og sikre integriteten og konfidensialiteten til selskapets data, er det avgjørende å iverksette grundige sikkerhetsprotokoller. Disse tiltakene bør omfatte alt fra nettverkssikkerhet til spesifikke retningslinjer for passordhåndtering og kryptering av data. La oss se nærmere på de:

Nettverkssikkerhet

Brannmurer

Vi kan installere og konfigurere brannmurer for å kontrollere inngående og utgående nettverkstrafikk basert på forhåndsdefinerte sikkerhetsregler. Dette inkluderer å sette opp egnede brannmursregler som blokkerer uønsket trafikk og mulig skadelige forbindelser. Som et eksempel kan vi se nærmere på **Forskningavdelingen**. Vi kan implementere spesifikke regler som sikrer at all inngående og utgående trafikk til forskningsdatabaser er nøye filtrert og monitorert, noe som beskytter mot uautorisert tilgang og datatap.

Antivirusprogrammer

Antivirusprogrammer kan sikre at alle endepunkter og servere er utstyrt med oppdaterte antivirusprogrammer for å oppdage og nøytralisere skadelig programvare. Når det gjelder vår gruppe med IT-avdelingen, kan vi sørge for at avanserte antivirusprogrammer er installert med høy prioritet for oppdateringer, gitt at disse systemene ofte er mål for cyberangrep på grunn av deres administrative tilganger.

Sikker Internettbruk

Jeg tenker at et annet alternativ som kan være bra og nyttig er å utdanne ansatte (alt fra IT-avdelingen til sesongarbeiderne) gjennom regelmessige kurs og oppdateringer om beste praksiser for sikker internettbruk. Dette inkluderer opplæring i hvordan identifisere phishing-forsøk og andre vanlige cybertrusler. For sesongarbeiderne kan det være guides man kan lese før man starter på selve jobben eller kurs man kan ta på nett.

Vi kan konkludere med at robuste brannmurer og antivirusprogrammer er første linje i forsvar mot eksterne angrep. Opplæring i sikker internettbruk er kritisk for å redusere risikoen for menneskelige feil, som ofte er den svakeste leddet i sikkerhetskjeden.

Password og Lockout Policy

Sterkere Passordpolitikk

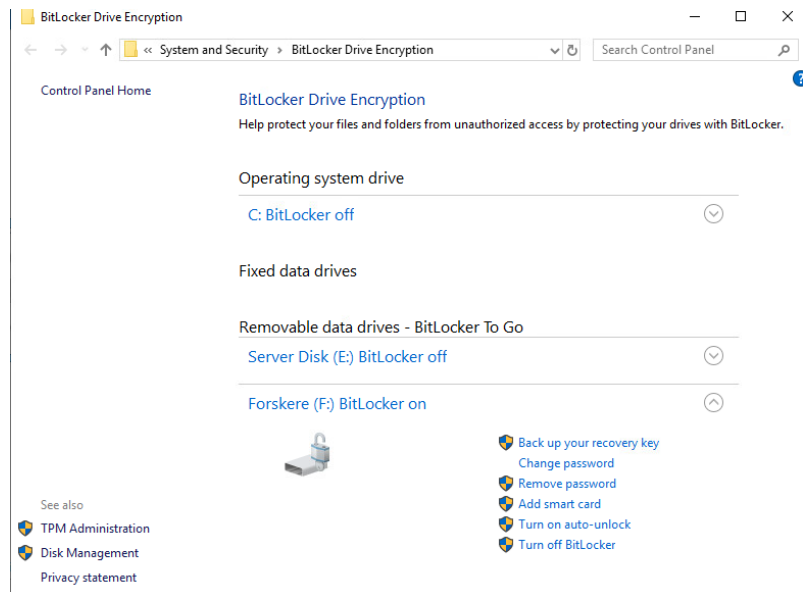
Vi kan også implementere en passord policy som krever komplekse passord (minimumslengde, inkludering av tall, store og små bokstaver, og spesialtegn) for alle brukere, med ytterligere forsterkninger for IT-avdelingen og andre brukere med tilgang til kritiske systemer.

Kontoadgangs- og låsepolitikk

Når det gjelder adgang til kontoene, kan vi sette opp en låsepolitikk der kontoer midlertidig låses etter flere mislykkede innloggingsforsøk for å hindre brute-force angrep.

Eksempler

- **Sterkere Passordpolitikk (ledelse, HR, osv.):** Daglig leder Grank Fulli og andre i ledergruppen bør ha ekstra komplekse passordkrav gitt deres tilgang til alle bedriftens kritiske systemer og data.
- **Kontoadgangs- og låsepolitikk (sesongarbeidere):** Innfør strenge låsepolitikker som krever administrativ godkjenning for å låse opp kontoer, siden disse brukerkontoene er mer utsatt for kompromittering på grunn av deres sporadiske bruk.



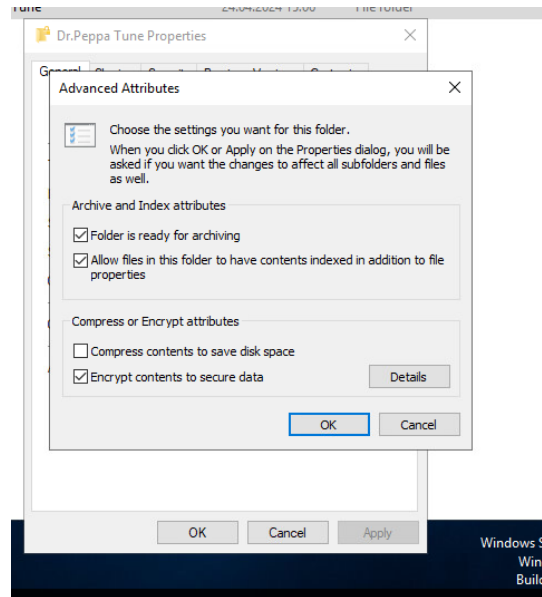
Sterke passord og effektive låsepolitikker reduserer risikoen for uautorisert tilgang betraktelig. Låsepolitikker beskytter mot automatiserte angrepsforsøk og sikrer at sensitive brukerkontoer forblir sikre.

Datakryptering

Kryptering av Sensitive Områder

Vi har kommet til krypterings-delen i oppgaven. Her kan vi sikre at alle data knyttet til forskningsavdelingen og HR er kryptert både i hvile og under overføring ved bruk av sterke krypteringsstandarder som AES (Advanced Encryption Standard) for å kryptere filsystemer og databaser.

Eksempel (forsyningsavdelingen): Dr. Peppa Tune og hennes team jobber med sensitive og verdifulle forskningsdata. Kryptering av deres datalagringsområder er essensielt for å beskytte mot industriell spionasje.



Ende-til-Ende Kryptering

Når det gjelder Ende-til-Ende kryptering, kan vi implementere ende-til-ende kryptering for all datakommunikasjon som involverer sensitiv informasjon.

Eksempel (HR-Avdelingen): Vi kan sikre at all kommunikasjon som involverer personopplysninger, fra intervjuer til ansattvurderinger, er kryptert fra ende til ende for å opprettholde konfidensialitet og overholde personvernlovgivningen.

Forskningsdata kan inneholde følsom og verdifull informasjon som krever høyeste nivå av sikkerhet for å forhindre industriell spionasje. HR-data inneholder personlig informasjon som må beskyttes for å overholde personvernlover og -forskrifter.

Disse sikkerhetstiltakene er ikke bare nødvendige for å beskytte mot eksterne trusler, men de hjelper også med å bygge en kultur av sikkerhet og ansvarlighet internt. Ved å sette standarder og implementere strenge sikkerhetstiltak, kan GeekGulp Refreshments sørge for at de ikke bare beskytter sin egen virksomhet, men også styrker tilliten blant ansatte, kunder og partnere.

Fil- og Datalagringsløsninger

Oppsett av Lagringsområder:

For å håndtere data effektivt og sikkert hos GeekGulp Refreshments, er det viktig å nøye planlegge og konfigurere lagringsområdene. Dette omfatter å definere nettverkslagringsområder (NAS eller SAN) for hver avdeling, tilrettelagt med de nødvendige sikkerhets- og tilgangskontrollene.

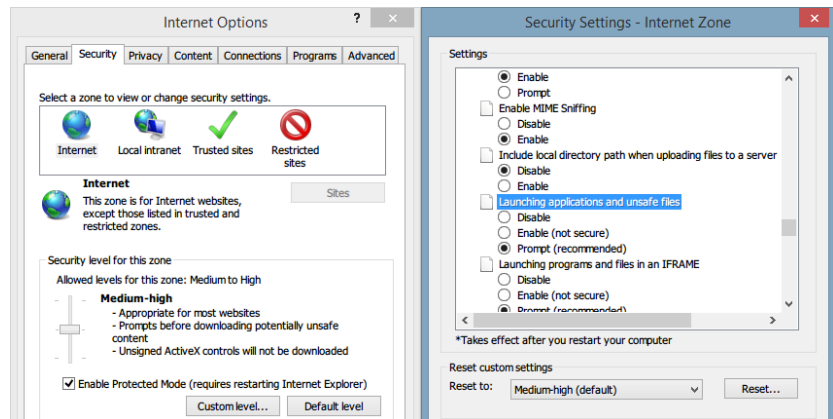
Vi kan opprette ulike lagringsområder. La oss se nærmere på dem:

- **Avdelingsspesifikke Lagringsområder:** Vi oppretter separate lagringsområder for hver avdeling, for eksempel IT, HR, forskning, og regnskap. Dette sikrer at filer og data er organisert og lett tilgjengelig for autoriserte brukere.

- **Geografisk Distribusjon:** I tilfelle av flere lokasjoner, som Mosvik og Mjøndalen, bør vi vurdere lokasjonsspesifik lagring for å redusere latency og sikre data tilgjengelighet selv ved nettverksutfall.

Restriksjoner og Tilgangskontroll

Vi setter opp detaljerte tilgangsrettigheter basert på brukernes rolle i organisasjonen. For eksempel, mens forskere får full tilgang til forskningsdata, bør andre avdelinger kun ha leserettigheter, om nødvendig.



Eksempel: Dr. Peppa Tune, en forsker og kjemiker hos GeekGulp, trenger en sikker og lett tilgjengelig lagringsplass for forskningsdata. En dedikert NAS-enhet settes opp for forskningsavdelingen med krypterte volumer for å sikre sensitiv informasjon om nye produktformler.

Tilgangskontroll: Bare medlemmer av forskningsavdelingen, samt utvalgte medlemmer fra IT for teknisk støtte, har tilgang til denne NAS-enheten. Dr. Tune får administrative rettigheter innen dette området for å kunne håndtere filene effektivt.

Eksempel (HR): Tobias Flændersen, HR-ansvarlig, trenger et sikkert system for lagring av ansattfiler, kontrakter og sensitive personopplysninger. HRs lagringsområde på et SAN opprettes med høy tilgjengelighet og redundans for å minimere risiko for datatap.

Tilgangskontroll: HR-avdelingen får eksklusiv tilgang til dette området med spesielle rettigheter for å legge til, endre og slette dokumenter. Tilgang for andre avdelinger er sterkt begrenset og overvåkes nøye.

Velorganiserte lagringsområder forbedrer produktiviteten ved å gjøre det enklere for ansatte å finne og benytte nødvendige data. Ved å sette restriksjoner basert på avdeling og nødvendighet, reduseres risikoen for uautorisert tilgang og potensielle datalekk.

Tilgangskontroll og Overvåking:

En effektiv tilgangskontroll kombinert med omfattende overvåking er essensielt for å beskytte organisasjonens data mot interne og eksterne trusler.

Tilgangslogger

Vi implementer en rekke løsninger for logging av alle tilgangsforsøk til sensitive datalagringsområder. Dette inkluderer hvem som har tilgang til hva, samt tidspunkt for tilgangen. Her er noen eksempler som jeg kom på:

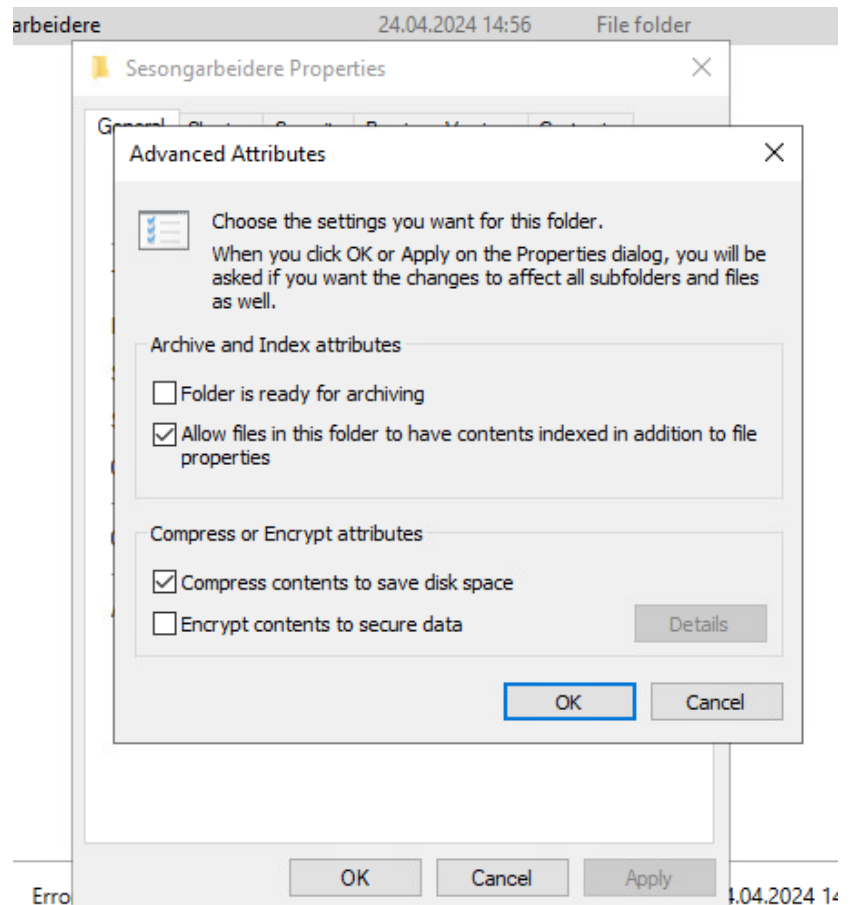
- **IT-Avdelingen:** For IT-avdelingen, ledet av Jon Johansen, kan det settes opp detaljerte logger for tilgang til serverrom og nettverksutstyr. Alle tilgangsforsøk til kritiske infrastrukturer logges og overvåkes via SIEM-systemer.
- **Sesongarbeidere:** For sesongarbeidere kan de implementeres en automatisert loggfunksjon som registrerer hver gang en enhet kobles til eller fra nettverket. Dette hjelper med å spore og verifisere bruk av IT-ressurser av sesongarbeidere, som kun har tilgang til bestemte tider av året.

Overvåkingsverktøy

Bruk av overvåkingsverktøy som SIEM (Security Information and Event Management) systemer kan hjelpe oss å analysere tilgangslogger og varsle oss om uvanlige eller mistenkelige adferdsmønstre. Her er det noen eksempler:

- **Regelmessige Sikkerhetsrevisjoner:** For alle avdelinger, inkludert de som håndterer sensitive data som forskning og HR, kan det planlegges regelmessige sikkerhetsrevisjoner for å evaluere effektiviteten av de implementerte sikkerhetstiltakene.
- **Reaksjon på Sikkerhetsbrudd:** I tilfelle av et sikkerhetsbrudd, vil detaljerte overvåkingslogger fra SIEM-systemet hjelpe IT-avdelingen med å raskt identifisere kilden og omfanget av bruddet, slik at rask respons og nødvendige tiltak kan iverksettes.

Ved å overvåke og logge tilgang til data, kan organisasjonen raskt identifisere og reagere på uautoriserte tilgangsforsøk. For sektorer som håndterer sensitive data, spesielt innen HR og finans, hjelper dette med å opprettholde compliance med relevante personvernslover og industrireguleringer.

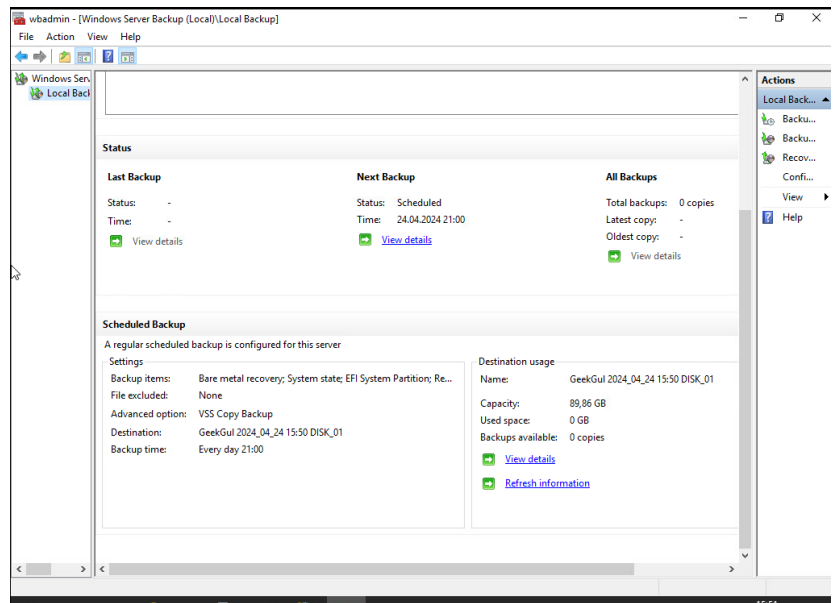


Backup og Gjenopprettingsstrategier

For å sikre kontinuitet og beskyttelse av data i tilfelle av tekniske feil, menneskelige feil eller katastrofale hendelser, er det avgjørende for oss (GeekGulp Refreshments) å implementere robuste backup- og gjenopprettingsstrategier.

Backup løsninger

Før vi bestemmer oss for hva som helst, er det viktig å se gjennom hvilke data som er kritiske og må backes opp. Dette inkluderer finansielle data, forskningsdata, brukerdata, og systemkonfigurasjoner.



Eksempel (Finansiell data): Regnskapsførerne Fritjof Hoel og Barbro Lefdal genererer viktige finansielle rapporter daglig. Disse dataene skal backes opp hver time onsite for å sikre at ingen kritisk informasjon går tapt i løpet av arbeidsdagen. En daglig offsite backup sikres også for å beskytte mot lokale skader som brann eller oversvømmelse.

Eksempel (Forskningsdata): Dr. Peppa Tune arbeider med sensitive forskningsdata som kan ha stor kommersiell verdi. Disse dataene krypteres og backes opp flere ganger om dagen både onsite og offsite, med særlig oppmerksomhet på sikkerheten til lagringsmediet og dataintegriteten under overføring og lagring.

Brukerdata og Systemkonfigurasjoner

Alle brukerprofiler og systeminnstillinger vil backes opp ukentlig for å raskt kunne gjenopprette operativsystemer og brukerinnstillinger i tilfelle maskinvarefeil eller cyberangrep.

Backupfrekvens: Vi kan fastsette hvor ofte dataene skal sikkerhetskopies basert på deres viktighet og hvor ofte de endres. Kritiske systemer kan kreve daglig eller til og med timevis backup, mens mindre kritiske systemer kan backes opp ukentlig. I vårt tilfelle har vi valgt å gjøre det hver dag kl. 21 (da ingen er på kontoret eller alle er hjemme)

Lagringslokasjoner

- **Onsite Backup:** Vi kan benytte onsite backup-løsninger som raskt kan gjenopprette systemer og minimere nedetid i tilfelle systemfeil.
- **Offsite Backup:** Vi kan også benytte offsite backup-løsninger, inkludert skybaserte tjenester, for å beskytte mot lokale katastrofer som brann eller naturkatastrofer. Dette sikrer at dataene er trygge og tilgjengelige selv hvis det primære kontoret blir utilgjengelig.

Ved å ha regelmessige onsite og offsite backups reduseres risikoen for betydelig datatap dramatisk. Hyppige backups sikrer at du kan gjenopprette til en nylig tilstand med minimalt datatap, noe som er kritisk for forretningsoperasjoner.

Gjenopprettingsplaner

Vi kan også lage detaljerte, trinn-for-trinn gjenopprettingsprosedyrer for ulike scenarioer, fra enkel filgjenoppretting til fullstendig systemrekonstruksjon.

Testing av Gjenopprettingsplaner:

Gjennomføring av regelmessige tester av gjenopprettingsplanene sikrer at de fungerer som forventet. Dette inkluderer både bordøvelser og faktiske gjenopprettingsøvelser.

Eksempel (fil igjen oppretting): En ansatt ved et uhell sletter en viktig presentasjon timer før et viktig møte. IT-avdelingen, ledet av Jon Johansen, bruker den siste timens backup for å raskt gjenopprette filen, minimerer forstyrrelsen og sikrer at presentasjonen går som planlagt.

Eksempel (fullstendig Systemrekonstruksjon): En virusinfeksjon tar ned flere systemer i IT-avdelingen. Med forhåndsutviklede og regelmessig testete gjenopprettingsprosedyrer, kan IT-teamet raskt gjenopprette alle berørte systemer til den siste kjente gode konfigurasjonen innen timer, drastisk reduserer mulig nedetid og tap av produktivitet.

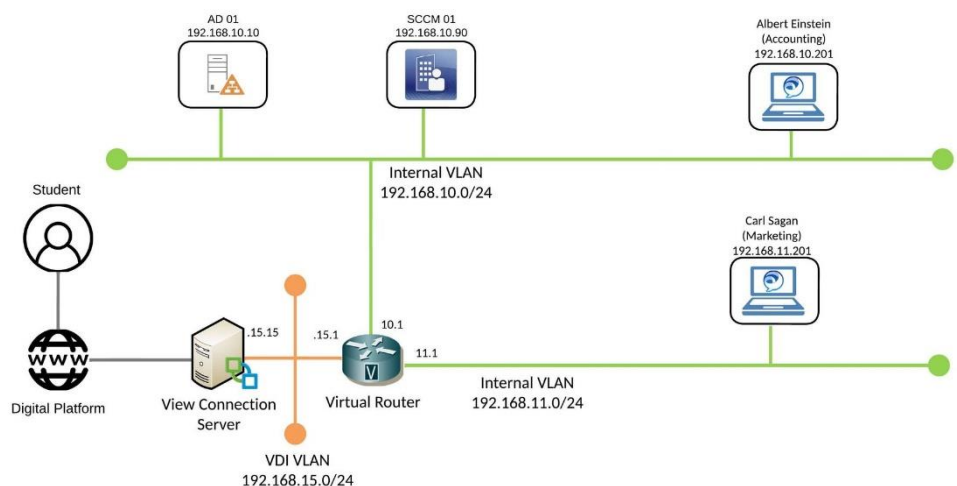
Grundig dokumenterte og regelmessig testete gjenopprettingsplaner sikrer at selskapet raskt kan komme tilbake til normal drift etter et datatap. Effektive og raskt gjennomførbare gjenopprettingsplaner minimerer nedetid, noe som beskytter selskapet mot omfattende økonomiske og operative skader.

Programvareinstallasjon og Vedlikehold

For å sikre oss for en effektiv og sikker programvarehåndtering innen GeekGulp Refreshments, er det viktig å implementere automatiserte systemer for installasjon og vedlikehold av programvare. Dette omfatter spesielt regnskapsprogramvare og operativsystemer, som er avgjørende for daglig drift og datasikkerhet.

Programvare for Regnskapsførere:

Automatisering: Bruk av automatiseringsverktøy for å installere regnskapsprogramvare som Microsoft Dynamics, vil være nødvendig for regnskapsførerne Fritjof Hoel og Barbro Lefdal. Disse verktøyene kan være basert på gruppepolicyer eller administrasjonsverktøy som Microsoft System Center Configuration Manager (SCCM), som tillater installasjon og oppdateringer å rulles ut sentralt uten å forstyrre brukeren.



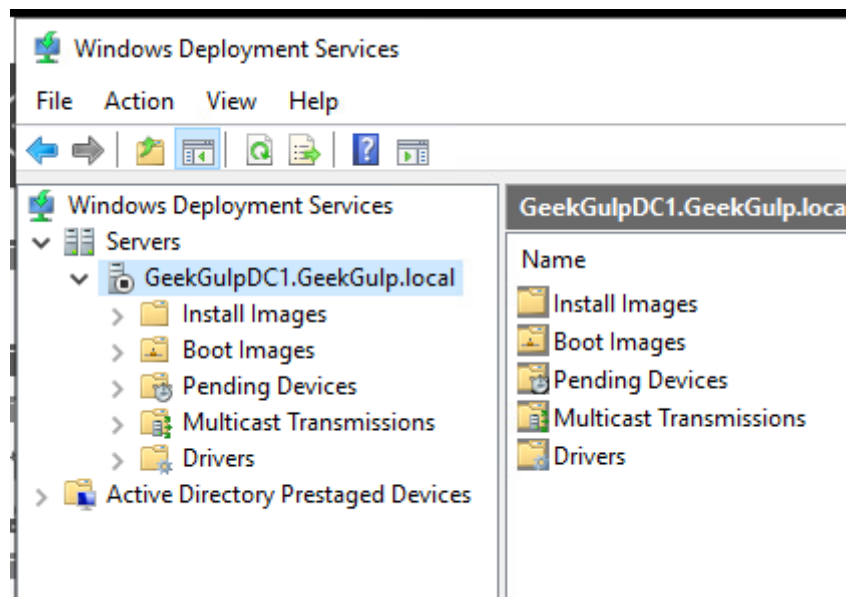
Versjonshåndtering og Oppdateringer: Implementering av en sentralisert tjeneste for å holde regnskapsprogramvaren oppdatert med de siste sikkerhetspatchene og funksjonsoppdateringene. Dette sikrer at programvaren ikke bare er effektiv, men også sikker mot nyeste trusler.

Automatisering av disse reduserer tidsbruken og potensielle feil som kan oppstå ved manuell installasjon. Oppdateringer sikrer at programvaren er beskyttet mot kjente sårbarheter, noe som er kritisk for å håndtere sensitiv finansiell informasjon.

Windows Deployment Services (WDS)

Nettverksbasert OS

Distribusjon: Vi setter opp Windows Deployment Services på en sentral server, for eksempel GeekGulpDC1, for å tillate enkel og rask distribusjon av Windows-operativsystemer til nye og eksisterende maskiner over nettverket. Dette inkluderer konfigurasjon av boot og install images som kan tilpasses ulike brukergrupper innen firmaet.



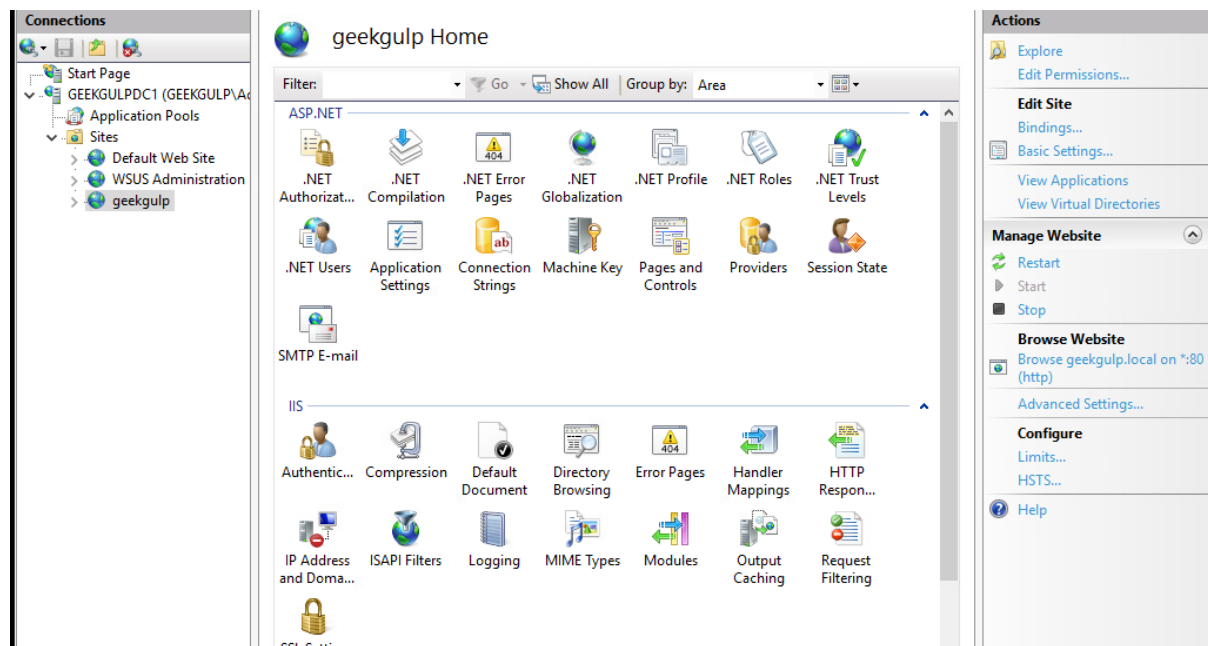
Prekonfigurering og Bildetilpasning: Vi forbereder og tilpasser installasjonsbilder til spesifikke avdelingsbehov. For eksempel, kan bildene for regnskapsavdelingen inkludere forhåndsinstallert regnskapsprogramvare, mens IT-avdelingen kan ha avanserte nettverksverktøy og sikkerhetsprogrammer.

WDS tillater IT-avdelingen å raskt sette opp nye maskiner eller gjenopprette eksisterende maskiner til en kjent god konfigurasjon, noe som reduserer nedetid og øker produktiviteten. Ved å bruke standardiserte bilder sikrer man at alle systemer er konfigurert likt, noe som reduserer kompatibilitetsproblemer og forenkler feilsøking og support. For å understøtte de sesongbaserte arbeidernes behov, kan det spesifikke konfigurasjoner ved hjelp av WDS settes opp for å automatisk installere og konfigurere de begrensede systemene de bruker hver sommer, med de nødvendige restriksjonene allerede på plass (f.eks., blokkering av tilgang til internett og visse applikasjoner).

Intranett og Webapplikasjoner

For å støtte intern kommunikasjon og informasjonsdeling effektivt, er det essensielt for oss (GeekGulp Refreshments) å implementere et robust og funksjonelt intranett. Dette omfatter

både teknisk konfigurasjon av hosting-infrastruktur og nøye planlegging av innholdet som skal tilbys. Her er et bilde av hvordan dette kan se ut.



Webserver og Hosting

Serverkonfigurasjon: Vi velger og setter opp dedikerte servere eller virtuelle maskiner som skal kjøre Windows Server med Internett Information Services (IIS) for å hoste intranettet. Vi sørger for at serverne er skalert etter antatt belastning og antall samtidige brukere.

IIS Innstillinger: Vi konfigurerer IIS for å håndtere webapplikasjonene, inkludert oppsett av flere applikasjonspooler for å isolere forskjellige applikasjoner for bedre sikkerhet og stabilitet. Til slutt aktiverer vi også de funksjoner som komprimering for å forbedre lastetider og HTTPS for sikker dataoverføring.

En godt konfigurert webserver sikrer høy tilgjengelighet og gode responstider for intranettet, noe som er kritisk for brukertilfredshet og produktivitet. Riktig konfigurerte IIS-innstillinger og isolerte applikasjonspooler hjelper med å beskytte sensitive data og forebygge potensielle sikkerhetstrusler.

Intranettinnhold

Innholds struktur: Vi kan planlegge strukturen på intranettet nøye for å sikre at det er lett navigerbart og brukervennlig. Opprett seksjoner for nyheter, HR-ressurser, bedriftspolicyer, ansattportaler og lønningsinformasjon. Litt lengre oppe er det et eksempel på hvordan dette kan se ut.

Dynamisk og Interaktivt Innhold: Integrering av interaktive elementer som diskusjonsforum, interne bloggsider og mulighet for ansatte til å kommentere eller bidra med innhold kan være en stor fordel for Geek Gulp. Dette fremmer en inkluderende og samarbeidspreget bedriftskultur.

Tilpasset Innhold: Dette sikrer at innholdet kan personaliseres basert på brukernes roller og interesser. For eksempel, at ledere får tilgang til ledelsesrapporter mens vanlige ansatte får tilgang til generelle selskapsoppdateringer og HR-dokumenter.

Et rikt og engasjerende intranett øker sannsynligheten for at ansatte vil bruke plattformen aktivt, noe som forbedrer intern kommunikasjon og samarbeid. Ved å gi ansatte enkel tilgang til nødvendig informasjon og ressurser, som lønningsinformasjon og personalhåndbøker, spares tid og forbedres den generelle effektiviteten.

Arbeidsstasjoner og Brukerenheter

For å sikre konsistens og sikkerhet på tvers av alle arbeidsstasjoner hos GeekGulp Refreshments, er det viktig å iverksette standardiserte skrivebords konfigurasjoner og spesielle tilpasninger for sesongarbeidere. Disse tiltakene hjelper med å opprettholde kontroll over IT-miljøet og sikre at alle brukere har de ressursene de trenger for å være produktive, samtidig som unødvendige risikoer unngås.

Name	Allowed Permissions	Inherited
GEEKGULP\Domain Admins	Edit settings, delete, modify security	No
GEEKGULP\Enterprise Admins	Edit settings, delete, modify security	No
NT AUTHORITY\Authenticated Users	Read (from Security Filtering)	No
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Read	No
NT AUTHORITY\SYSTEM	Edit settings, delete, modify security	No

Policy	Setting	Comment
Desktop Wallpaper	Enabled	

Skrivebords konfigurasjoner

Standardisert Bakgrunn: Setter opp en policy via Group Policy i Active Directory for å standardisere skrivebordsbakgrunnen på alle firmaets maskiner. Bruk firmaets logo eller et annet firmarelatert bilde som bakgrunn for å fremme merkevaren og gi et enhetlig utseende.

Innstillinger og Programvare: Konfigurer standardprogramvarepakker som skal installeres på alle arbeidsstasjoner, som Office-pakken, nettlesere, og nødvendig kommunikasjonsverktøy. Sørg for at alle nødvendige innstillinger som nettverkskonfigurasjoner og sikkerhetsinnstillinger er forhåndskonfigurert.

Skrivebords konfigurasjoner (Eksempler)

- Dr. Peppa Tune, som jobber i forskningsavdelingen, vil ha spesifikke programvarer knyttet til forskning og analyse forhåndsinstallert på sin arbeidsstasjon.
- Jon Johansen, IT-konsulent, vil ha administrative verktøy og avansert diagnostisk programvare tilgjengelig på sin maskin.

Sesongarbeidere

Restriktiv Tilgang: Vi kan bruke Group Policy for å sette opp en begrenset brukerprofil som automatisk brukes på sesongarbeideres maskiner. Disse profilene skal begrense tilgangen til internett og blokkere tilgang til systeminnstillinger og visse applikasjoner som ikke er relevante for deres jobbfunksjoner.

Programvare Restriksjoner: Vi konfigurerer applikasjonskontrollpolitikker som forhindrer installasjon og bruk av ikke-godkjent programvare, slik som spill eller medieprogrammer som Windows Media Player. (som på Centric sine PCer)

Sesongarbeiderne bruker laptopen som kun er aktivert om sommeren, og disse maskinene skal ha en konfigurert oppstart som ikke tillater tilgang til verktøy som kan kompromittere sikkerheten eller distrahere fra arbeidet.

Ved å standardisere bakgrunner og innstillinger, reduseres risikoen for sikkerhetsbrudd ved at alle maskiner opprettholder grunnleggende sikkerhetsstandarter. For sesongarbeidere hjelper restriksjonene med å holde fokus på jobbrelevante oppgaver og forhindrer misbruk av firmaets ressurser.