Bacheloroppgave

Myhre, Marius Ibenfeldt & Lien, Tormod Haus

Utvikle verktøy for konsolidering og analyse av nodeinformasjon fra Domstoladministrasjonens nettverk.

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

NTNU
Kunnskap for en bedre verden

Myhre, Marius Ibenfeldt & Lien, Tormod Haus

Utvikle verktøy for konsolidering og analyse av nodeinformasjon fra Domstoladministrasjonens nettverk.

Bacheloroppgave i Informatikk, drift av datasystemer
Veileder: Tor Ivar Melling
Mai 2019

NTNU
Kunnskap for en bedre verden

Myhre, Marius Ibenfeldt & Lien, Tormod Haus

Utvikle verktøy for konsolidering og analyse av nodeinformasjon fra Domstoladministrasjonens nettverk.

Bacheloroppgave i Informatikk, drift av datasystemer
Veileder: Tor Ivar Melling
Mai 2019

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

Innhold

Vedlegg

Sluttrapport

Bacheloroppgave 015

Våren 2019

Marius Myhre

Tormod Lien

IDRI3001 Bacheloroppgave i drift av datasystemer

20. Mai. 2019

DOMSTOL ADMINISTRASJONEN

NTNU
Kunnskap for en bedre verden

Revisjonshistorie

Dato	Versjon	Beskrivelse	Forfatter
14.05.2019	0.1	Opprettet dokumentet	Prosjektgruppen
15.05.2019	0.2	Kap. 1, 2 og 3.	Prosjektgruppen
18.05.2019	0.3	Ferdigstilt for veiledning	Prosjektgruppen
20.05.2019	0.4	Ferdigstilt etter tilbakemelding	Prosjektgruppen

Innholdsfortegnelse

Tabelliste

Ordliste

Ord	Beskrivelse
SaaS	Software as a service. Gir brukere mulighet til å koble til og bruke skybaserte apper over internett. Det vil si at en leier bruken av et program som driftes av leverandøren.
SCCM	System Center Configuration Manager
CPPM	ClearPass Policy Manager
AMP	Airwave Management Platform
Aruba-tjenestene	ClearPass og Airwave

1. Introduksjon

Sluttrapporten er det siste dokumentet i bachelorprosjektet, og skal oppsummere arbeidet som er gjort. Dokumentet beskriver først oppgaven, deretter hvordan den er løst, og refleksjoner rundt hvordan prosjektet har gått.

2. Oppgavebeskrivelse

Punktet beskriver oppgaven som prosjektgruppen har gjennomført, og de personene som har vært involvert i oppgaven.

2.1 Kort beskrivelse av oppgaven

Bachelorprosjekt 015 er gitt av Domstoladministrasjonen, ved Øyvin Moe. Oppgaven handler om å forbedre nettverkssikkerheten i domstolene, og består av tre deler:

- Powershell-script for uthenting og analyse av nodeinformasjon
- En database som lagrer informasjonen og resultatene fra analysen
- En nettside som visualiserer informasjonen som befinner seg i databasen

Den originale arbeidstittelen til oppgaven, "teknisk, sosial og fysisk informasjonssikkerhet – analyse og tiltak hos Domstoladministrasjonen", var veldig åpen, og av de mulige områdene oppgaven kunne ta for seg valgte prosjektgruppen å fokusere på nettverkssikkerhet. Med god hjelp fra teknikere hos DA og veilederne, kom prosjektgruppen fram til problemstillingen: "Utforske mulighetene for, designe og produsere et verktøy for automatisk analyse av nodeinformasjon fra SCCM, Clearpass og Airwave". Etter hvert ble oppgaven mer rettet mot innsamlingen av nodeinformasjon, og oversikten over nodene i nettverket, med analyse av informasjonen som ble hentet.

2.2 Personer involvert i oppgaven (Utenom prosjektgruppen)

Navn	**Rolle**
Øyvin Moe	Oppgavestiller
Tor-Ivar Melling	Veileder
Ansatte i DA	Innspill og tilbakemeldinger underveis i oppgaven
Referansegruppe 042	Korrekturlesning av dokumentasjon

Tabell 1: Involverte personer

3. Hvordan ble oppgaven løst

Ved prosjektstart i Januar benyttet prosjektgruppen seg av de første ukene på å planlegge hvordan prosjektet skulle gjennomføres. I løpet av uke 2 og 3 ble det gjennomført flere møter med ansatte på DA, da oppgaven fortsatt var veldig åpen. Prosjektgruppen hadde valgt nettverkssikkerhet som temaet på oppgaven, og gjennom møtene ble problemstillingen formulert.

Etter problemstillingen ble formulert, gikk arbeidet framover, med forstudierapporten som første punkt. Når denne var ferdig begynte prosjektgruppen på designrapporten, og etter det begynte utviklingen av selve verktøyet. I løpet av utviklingen ble driftsdokumentet skrevet, og etter det var ferdig, ble sluttrapporten skrevet, og presentasjonen utført.

3.1 Metoder og standarder

Metode/Standard	Bruksområde
Trello	Trello ble benyttet for å gi god oversikt over arbeidsoppgavene som skulle utføres, var under utvikling og de som var ferdige. Verktøyet ga også god oversikt over hvem som skulle gjøre hva og tidsfrister som skulle overholdes. På denne måten har Trello vært en viktig motivasjonsfaktor for prosjektgruppen.
GitHub	GitHub ble benyttet for versjonskontroll i tillegg til at det la til rette for synkront arbeid med kode.
Navnestandarder	Maler og standarder fra NTNU er benyttet for navngivning av dokumenter. Møtereferat er navngitt på formen M*øtereferat ÅÅÅÅ-MM-DD.* Møteinnkallinger er navngitt på formen *Møteinnkalling ÅÅÅÅ-MM-DD.*
Programmeringsstandarder	Prosjekgtruppen har benyttes seg av lower camelCase for navgivning av variabler. Funksjoner har blitt navngitt med verb fra verblisten (Microsoft Docs, 2018) til PowerShell.

Tabell 2: Metoder og standarder

3.2 Bruk av litteratur og internett

Ettersom verktøyet skulle hente informasjon fra SCCM, Aruba Airwave, og Aruba Clearpass, var det nødvendig å finne ut av hvilke grensesnitt man kunne benytte seg av for å utføre uthentingen. For SCCM var det enkelt å benytte seg av Powershell Remoting (Microsoft Docs, 2018). For Aruba-tjenestene var det nødvendig å finne dokumentasjonen til Airwave og Clearpass, spesielt punktene for deres APIer. For Airwave benyttet prosjektgruppen seg av det innebygde XML-APIet (Aruba, 2019), og for Clearpass benyttet prosjektgruppen seg av den innebygde REST-APIet (Aruba, 2019).

3.3 Oversikt over ressurser som er brukt

Det er ikke benyttet fysisk maskinvare i prosjektet ettersom prosjektgruppen har benyttet seg av virtualisert miljø hos NTNU for hosting av servere og maskiner for kjøring av PowerShell skripts. Videre har prosjektgruppen benyttet seg av Azure WebApp og Azure SQL som er skyløsninger og driftes av Azure. Azure WebApp ble benyttet for å hoste nettsiden som ble utviklet, og Azure SQL er en SQL-database.

3.4 Oversikt over programvare som er brukt

Program	Beskrivelse	Formål i prosjektet
GitHub	Versjonskontroll	Skriving av kode for PowerShell skripts og utvikling av nettside.
Microsoft Azure	SaaS-basert tjeneste for IT-infrastruktur.	Hosting av nettside og database.
Office 365	Programvare for produktivitet.	Et eget Sharepoint-område ble benyttet som samhandlingsplattform mellom prosjektgruppen, veileder og oppgavestiller. Benyttet av prosjektgruppen for intern samhandling i dokumentasjonsarbeidet. Outlook ble brukt for møtevirksomhet og e-postutvekslinger mellom interessentene.
Visual Studio Code	Teksteditor med terminal	Skriving av kode for PowerShell skripts og utvikling av nettside.
MS Project	Prosjektstyringsverktøy	Benyttet for å utforme Gant-diagram
Moqups	Webapp for laging av mockups og wireframes	Lage wireframe for nettsiden i design
MS Visio	Visualiseringsverktøy	Benyttet for å lage diagrammer som forklarer nettverk og dataflyt.

Tabell 3: Brukt programvare

3.5 Fordeling av arbeidet

I løpet av prosjektet har det ikke vært noe spesifikk fordeling av arbeidet blant medlemmene på prosjektgruppen. I løpet av de forskjellige rapportene har begge medlemmene skrevet på det meste, og i løpet av utviklingen har begge medlemmene programmert og dokumentert. Det utviklet seg en viss fordeling der Marius tok seg av Airwave og Clearpass, og Tormod tok seg av SCCM og databasen. Her ble også hoveddelen av dokumentasjon på de forskjellige delene utført av den som utviklet den. Prosjektgruppen har likevel arbeidet på tvers, og de forskjellige løsningene medlemmene har kommet fram til har blitt forklart til den andre, så begge har god forståelse av den komplette løsningen. I møter har det vært en fast fordeling, der Tormod har vært ordstyrer, og Marius har vært referent.

3.6 Dokumentasjon for prosjektet

Rapporter

Dokument	Beskrivelse
Forstudierapport	Starten av projektet med analyse av dagens løsning i Domstoladministrasjonen og hva som kan gjøres for å forbedre den.
Designdokument	Konseptuell beskrivelse av EnVy og hvordan det skal utvikles.
Driftsdokument	Detaljert beskrivelse av implementasjon og videreutvikling av EnVy.
Sluttrapport	Oppsummering av prosessen og resultatet av prosjektet.

Tabell 4: Rapporter

Vedlegg

Dokument	Beskrivelse
Avtaler	Avtale mellom de ulike partene som er involvert i prosjektet. De avtalene som er inngått er mellom: • NTNU og Oppgavestiller • Medlemmene i prosjektgruppen
Møteinnkallinger	Innkalling til veiledningsmøter for oppgavestiller, veileder og prosjektgruppen. Inneholder agendaen for møtet, lenke til siste møtereferat og lenke til eventuell dokumentasjon som skal leses til møtet.
Møtereferat	Møtereferater fra veiledningsmøter, og andre møter prosjektgruppen har holdt i løpet av prosjektets gang.
Timeliste	Ukentlig timeliste som viser timebruk for prosjektgruppens medlemmer og ukesrapporter som sier hva som er gjort gjeldende uke og planen for neste uke
Fremdriftsplan	Gantt-diagram som viser prosjektgruppens plan for arbeidsoppgaver og tidsbruk.

Tabell 5: Vedlegg

4. Gjennomføring av prosjektet

I dette kapittelet kommer prosjektgruppens refleksjoner rundt hvordan prosjektet har blitt gjennomført. Det beskrives hva som gikk bra, hva som gikk dårlig, hva som kunne gått bedre, hvordan tekniske problemer ble løst, hvilke begrensninger løsningen har, og til slutt en vurdering av prosjektgruppens måloppnåelse etter gjennomføring av prosjektet.

4.1 Hva som gikk bra

Punktet beskriver det prosjektgruppen mente gikk bra med prosjektgjennomføringen.

4.1.1 Utforming av oppgaven

Oppgavebeskrivelsen fra start av var veldig åpen, og ga prosjektgruppen stor frihet til å velge oppgaven selv. Gjennom et par møter helt i starten av prosjektet ble oppgaven låst ned til uthenting og analysering av informasjon fra SCCM, Clearpass og Airwave, noe som gjorde at prosjektgruppen hadde et veldefinert startpunkt allerede et par uker inn i prosjektet.

4.1.2 Veiledningsmøter

Veiledningsmøtene prosjektgruppen har fått, har vært til ekstremt stor hjelp. Det at både oppdragsgiver og veileder har deltatt aktivt gjorde det veldig enkelt å få tilbakemelding på det arbeidet som hadde blitt gjort, og anbefalinger til hva som skulle gjøres videre. Møtene har som regel skjedd med en til to ukers mellomrom, og det har vært veldig motiverende å jobbe mot hvert møte, og planlegge slik at man har noe ferdig til hvert veiledningsmøte.

4.1.3 Samhandlingsverktøy

Trello har blitt brukt veldig flittig av prosjektgruppen og har vært til stor hjelp for å holde oversikt over arbeidsoppgaver og arbeidsinndeling. Det har også vært god motivasjon i å kunne benytte sjekklister.

GitHub ble benyttet for samskriving av kode. For selve utviklingen har dette vært det viktigste verktøyet. Prosjektgruppen har også dratt god nytte dette verktøyet i form av versjonskontroll og backup.

For samskriving av dokumentasjon har SharePoint fungert bra, med unntak av en liten periode preget av tregheter og nedetid.

4.1.4 Fordelingen av arbeidsoppgaver

Gjennom prosjektet har det ikke vært en fast fordeling av arbeidet. I all hovedsak ble oppgavene fordelt ved at hvert medlem valgte en oppgave fra listen i Trello, noe som gjorde at hvert medlem alltid hadde noe å gjøre, og begge kunne arbeide på forskjellige ting. Medlemmene har forskjellige kunnskaper, og ved å velge oppgaver som man hadde god kunnskap i fra før, eller oppgaver som var mere utfordrende, fikk begge medlemmene utnyttet den kunnskapen de hadde og de fikk gjort vanskeligere oppgaver som ga stor lærdom.

4.1.5 Arbeidsmoral

I starten av prosjektet ble prosjektgruppen enige om at man skulle møte opp hos Domstoladministrasjonen klokken 9, og arbeide fram til rundt 4, hver dag dette var mulig. Dette har fungert veldig bra, der man har fått arbeidet med prosjektet likt som man ville jobbet med et prosjekt i en bedrift. Det ble alltid utført arbeid på prosjektet hver dag, noe som gjorde at mengden kvelds- og helgejobbing ble minimert, slik at arbeidsmoralen til prosjektgruppen alltid har vært høy.

4.1.6 Læring underveis i prosjektet

I løpet av prosjektet har prosjektgruppen lært veldig mye. For å kunne utføre oppgaven var det flere elementer som måtte gjennomføres, som ingen på prosjektgruppen kunne fra før: APIer, formatering og sammenstilling av data, tilkobling til databaser i Powershell, PHP, og mye mer. Gjennom dette prosjektet har prosjektgruppen måtte lære seg hvordan ting fungerte, og hvordan man skulle sette sammen de forskjellige delene til å løse oppgaven som ble gitt.

4.2 Hva som gikk dårlig

Prosjektgruppen satte opp ett eget testmiljø for å tilsvare Domstoladministrasjonens oppsett. Her oppstod det tidlig problemer med å få Aruba Airwave til å fungere ettersom VMWare ikke støttet tredjeparts svitsjer. Dette problemet ble det brukt for mye tid på, da prosjektgruppen var innbitt på å finne en løsning. Etter mye tidsbruk ble oppsett av Airwave lagt død etter samtaler med veileder.

Testmiljøet har ikke blitt brukt nok til å rettferdiggjøre tidsbruken på oppsettet av det. Tidlig i prosjektet var planen å simulere en "miniversjon" av domstolenes nettverk, men i løpet av prosjektets gang benyttet prosjektgruppen seg heller av generert data. Dette medførte at testmiljøet kun ble brukt til å teste uthenting av informasjon.

4.3 Hva som kunne gått bedre

Under utviklingen av EnVy burde prosjektgruppen vært flinkere til å dokumentere driftsdokumentet. Dette medførte at prosjektgruppen måtte ha en rekke lange arbeidsdager mot slutten av prosjektet for å få dokumentasjonen opp på ønsket nivå.

Utviklingen av nettsiden ble påbegynt for sent. Mye av fokuset ble lagt på å få innhenting og formatering av data til å bli bra, og det ble derfor ikke lagt nok fokus på nettsiden. Dette medførte flere av ideene som kom ved utviklingen av det visuelle måtte legges på is og heller dokumenteres som muligheter for videreutvikling.

De to siste rapportene, Driftsdokument og Sluttrapport, burde vært levert tidligere til veiledere for gjennomlesning slik at tidspresset ikke ble like stort på både veileder, oppgavestiller og prosjektgruppen. Dette var et resultat av at dokumentasjon av driftsdokument ikke ble arbeidet godt nok med under utviklingsfasen.

4.4 Hvordan har tekniske problemer blitt løst

I løpet av prosjektet har prosjektgruppen møtt mange tekniske problemer. Dersom problemet var mangel på kompetanse, benyttet prosjektgruppen seg i hovedsak av internett for å hente informasjon og prøve å forstå hvordan problemet skulle løses. Dersom den individuelle informasjonshentingen ikke fant et svar, ble den andre parten involvert, og prosjekgruppen sammen prøvde å finne en løsning eller workaround.

Flere av de tekniske problemene prosjektgruppen møtte var bugs i kode vi skrev. Planen var fra starten å benytte GitHubs "issues"-funksjonalitet, men ettersom prosjektgruppen alltid jobbet på samme kontor, ble problemer tatt opp i dialog, og løst på stedet.

4.5 Hvilke begrensinger har systemet

EnVy har ved prosjektets slutt ingen mulighet for live-uthenting av informasjon fra tjenestene. I starten av prosjektet ble det gjort et valg at man skulle hente informasjonen en gang daglig, slik at man hver dag ville få en oppdatert database med informasjon om hvilke enheter som befinner seg i nettverket. For å kunne utføre live-uthenting vil det være nødvendig med store endringer i programmet, noe som prosjektgruppen ikke la i scopet til prosjektet.

4.6 Vurdering av måloppnåelse

I dette punktet vurderes hvor godt prosjekgruppen har oppnådd de målene som ble definert i forstudie- og designrapporten.

4.6.1 Fremdriftsplan

Fremdriftsplanen er et Gantt-diagram, og ble brukt som en grov tidsramme gjennom hele prosjektet. Diagrammet beskriver ikke i detalj hva som skal gjøres, men viser hva prosjektgruppen til enhver tid skulle arbeide med. Denne planen ble laget i forstudiet, og var et godt hjelpemiddel for å tidlig få en god oversikt over det arbeidet som skulle gjøres. Planen har blitt fulgt relativt godt gjennom hele prosjektet, med unntak av at opplæring ikke ble aktuelt da bestilte servere ankommer etter prosjektets slutt. Den andre forskjellen er at tidsbruken på utvikling ble en del lengre og arbeidet med hovedrapporten ble dermed kortet ned.

4.6.2 Prosessmål

Prosessmålene som prosjektgruppen satte var følgende:

Prosjektgruppen skal:

- Oppnå karakteren A
- Øke sin kompetanse innen informasjonssikkerhet
- Forbedre samarbeid- og kommunikasjonsevner
- Tilegne seg nyttige erfaringer fra arbeidslivet

Prosjektgruppen føler de har gjennomført de tre siste prosessmålene. Begge deltagerne har økt sin kompetanse innen informasjonssikkerhet, både gjennom arbeidet med utviklingen, men spesielt gjennom kontakten med de som faktisk arbeider i feltet hos Domstoladministrasjonen. Gjennom arbeidet har prosjektgruppen formidlet hva de holder på med til interessentene hos Domstoladministrasjonen, og har samarbeidet innad for å gjennomføre et vanskelig prosjekt. Til slutt har begge deltagerne fått mange nyttige erfaringer fra arbeidslivet, da vårt prosjekt har blitt behandlet av Domstoladministrasjonen som et internt prosjekt. Det første punktet kan ikke prosjektgruppen si så mye om, annet enn vi selv føler vi har gjort en veldig god jobb med prosjektet.

4.6.3 Resultatmål

Resultatmålene som prosjektgruppen satte var følgende:

Prosjektgruppen skal:

- Lage et verktøy som henter, sammenligner, og formaterer nodeinformasjon fra SCCM, Clearpass, og Airwave.
- Lage et Dashboard for fremstilling av data.
- Lage et verktøy som varsler ved potensielle trusler.
- Levere verktøyet og dokumentasjonen senest 20. Mai 2019.

Alle fire målene ble oppnådd. Det første punktet ble oppnådd gjennom skriptene som ble utviklet. Dashboardet ble gjennomført i form av nettsiden, og varslingen ble gjort gjennom automatisk analyse av informasjon, som blir vist i dashboardet. Tidsfristene ble overholdt, og innlevering den 20. Mai gjennomføres, med presentasjon av prosjektet den 28. Mai.

4.6.4 Risikoanalyse

I risikoanalysen kom prosjektgruppen fram til 11 hendelser som kunne negativt påvirke konsekvensene:

1. Ting tar lengre tid enn forventet
    - Det ble brukt for mye tid på oppsett av testmiljø. Dette gjorde at vi startet med utviklingen senere enn planlagt. I tillegg ble det brukt for lang tid på utviklingen. Selv om ting tok lengre tid, klarte prosjektgruppen å utføre alt som skulle utføres i oppgaven.
2. Problemer med utstyr brukt til å utføre prosjektet
    - Det var ingen problemer med utstyret til prosjektgruppen. Det var noen dager der SharePoint var nede, men da ble arbeid som ikke behøvde SharePoint utført.
3. Prosjektgruppen klarer ikke utvikle løsning
    - Det har i løpet av prosjektet vært flere veisperrer der prosjektgruppen har måtte løse vanskelige problemer, men alle problemer ble løst.
4. Tap av data med implementasjon av løsning
    - I løpet av prosjektets gang har prosjektgruppen benyttet testmiljøet for å teste bruken av EnVy, og det er ingen muligheter for tap av data når løsningen skal implementeres,
5. Nedprioritering av prosjektet fra Domstoladministrasjonen sin side
    - Prosjektet ble ikke nedprioritert av Domstoladministrasjonen.
6. Løsningen har ingen nytte for oppgavestiller
    - Gjennom mye kommunikasjon med de som skal ta i bruk løsningen hos Domstoladministrasjonen har prosjektgruppen lagd en løsning som har nytteverdi hos oppgavestiller.
7. Sykdom blant veiledere
    - Det har ikke vært noen problemer som har oppstått av sykdom blant veiledere.
8. Tap av data hos prosjektgruppen
    - Data har ikke blitt tapt hos prosjektgruppen. Prosjektgruppen har i løpet av prosjektet tatt ukentlige lokale backups av alt materiale, og alt har blitt lagret i SharePoint og hos GitHub.
9. Kortvarig sykdom og fravær
    - Det har vært ett tilfelle av kortvarig sykdom hos prosjektgruppen, der Marius fikk influensa. Dette har ikke hatt store konsekvenser.
10. Langvarig sykdom og fravær
    - Det har ikke vært noen tilfeller av langvarig sykdom eller fravær.
11. Intern misnøye i prosjektgruppen
    - Det har ikke vært intern misnøye hos prosjektgruppen.

4.6.5 Forskjeller mellom planlagt og utført arbeid

Prosjektet var planlagt å produsere:

- Verktøy for konsolidering og analyse av nodeinformasjon fra SCCM, Aruba Airwave og Aruba Clerapass.
- Dashboard løsning for visualisering av nodeinformasjon med analyse.
- Maler for bruk av PowerBI

De to første punktene er produsert i form av PowerShell-skript for konsolidering og analyse av nodeinformasjon, og nettsiden som Dashboard løsning. Maler for PowerBI utgikk da Domstoladministrasjonens prosjekt for å innføre PowerBI ikke kom til å bli ferdig innen prosjektets slutt. Konsolideringen og analysen ble gjennomført som planlagt, og nettsiden visualiserer både nodeinformasjonen som er hentet, og resultatene av anaylsene som ble utført.

4.6.6 Timeregnskap

Timeregnskapet benytter seg av arbeidsarter som er inspirert av fremdriftsplanen. Disse arbeidsartene er:

- Forstudie
- Møte
- Testmiljø
- Design
- Utvikling
- Driftsdokument
- Sluttrapport
- Presentasjon

For hver uke ble det ført hvor mange timer som ble brukt på de ulike arbeidsartene, i tillegg til en statusrapport for hva som ble gjort gjeldende uke og plan for den kommende uken. Tidsrammen på prosjektet ble satt til 500 timer per person i prosjektgruppen. Det var et slingringsmonn på 10 prosent, og prosjektgruppen satte et mål på 514 timer per person for å gi medlemmene litt ekstra motivasjon. For å nå dette målet hadde prosjektgruppen satt seg et mål om å bruke ca. 28 timer hver uke på prosjektet.

4.6.7 Kommentarer

Samarbeidet mellom medlemmene i prosjektgruppen har vært veldig bra. Begge partene hadde like ambisjoner til hva dette bachelorprosjektet skulle være: En A. Med utgangspunkt i dette har begge partene møtt opp når de skulle, og arbeidet veldig godt med prosjektet. Der det har vært avvik fra planen, enten i form av at man ikke kan møte opp eller at man må dra tidligere, har man gitt beskjed i god tid, gjerne gjennom Facebook. Dette er noe prosjektgruppen mener har fungert veldig godt.

Det har vært veldig gøy å kunne utføre dette prosjektet hos og for Domstoladministrasjonen. Ved å kunne utføre en oppgave som faktisk ønskes, og å vite at verktøyet kom til å bli tatt i bruk, har det å arbeide med Domstoladministrasjonen vært veldig motiverende. I tillegg til motivasjon, har det å jobbe i en faktisk bedrift ført til unike problemstillinger og løsninger. Der prosjektgruppen i en skoleoppgave kunne stått fritt til å velge løsninger, har Domstoladministrasjonen sine egne krav til hvilke programmer som skal brukes, noe som var utfordrende, og veldig lærerikt.

Til slutt vil prosjektgruppen takke oppgavestiller Øyvin Moe, og veileder Tor Ivar Melling, for god kommunikasjon og veldig gode tilbakemeldinger i løpet av prosjektet. Begge veilederne har gått “above and beyond” det som kreves av en veileder i et bachelorprosjekt, noe som har vært kritisk for at prosjektet ble gjennomført så bra som det ble gjort.

5. Referanser

Microsoft Docs (2018) *Approved Verbs for PowerShell Commands.* Available at: https://docs.microsoft.com/en-us/powershell/developer/cmdlet/approved-verbs-for-windows-powershell-commands (Accessed: 1 May 2019).

Microsoft Docs (2018) *Running remove commands*. Avaliable at: https://docs.microsoft.com/en-us/powershell/scripting/learn/remoting/running-remote-commands?view=powershell-6 (Accessed: 4 March 2019).

Aruba Support Center (2019) *Airwave 8.2.8 API Guide*. Avaliable at: https://support.arubanetworks.com/Documentation/tabid/77/DMXModule/512/Command/Core_ViewDetails/Default.aspx?EntryId=32983 (Accessed: 14 May 2019)

Aruba Support Center (2019) *ClearPass Guest User Guide (Revision 01).* Avaliable at: https://support.arubanetworks.com/Documentation/tabid/77/DMXModule/512/Default.aspx?EntryId=33705 (Accessed: 14. May 2019)

Forstudierapport

Bacheloroppgave 015 *Marius Myhre*

Våren 2019 *Tormod Lien*

IDRI3001 Bacheloroppgave i drift av datasystemer

20. Mai. 2019

DOMSTOL ADMINISTRASJONEN

NTNU
Kunnskap for en bedre verden

Revisjonshistorie

Dato	Versjon	Beskrivelse	Forfatter
14.01.2019	0.1	Opprettet dokumentet	Prosjektgruppen
16.01.2019	0.2	La til ulike kapittel og punkter som skulle under hvert kapittel.	Prosjektgruppen
17.01.2019	0.3	Intro ferdig utkast. Bakgrunn ferdig utkast. Prosjektmål påbegynt.	Tormod
18.01.2019	0.4	Videre utarbeiding av dokumentet	Prosjektgruppen
23.01.2019	0.5	Videre utarbeiding av dokument	Prosjektgruppen
25.01.2019	0.6	Klargjort for gjennomlesning	Prosjektgruppen
28.01.2019	0.7	Førsteutkast ferdigstilt	Prosjektgruppen
30.01.2019	0.8	Endringer etter veiledningsmøte	Prosjektgruppen
31.01.2019	0.9	Siste gjennomgang av innhold	Prosjektgruppen
01.02.2019	0.10	Forslag til ferdigstillelse	Prosjektgruppen
04.02.2019	0.11	Fullført interessentanalyse	Prosjektgruppen

Innholdsfortegnelse

Figurliste

Tabelliste

Ordliste

Ord	Beskrivelse
DA	Domstoladministrasjonen
NTNU	Norges teknisk-naturvitenskapelige universitet
SCCM	System Center Configuration Manager
Aruba Airwave	Tjeneste for overvåking av svitsjer og aksesspunkter i et nettverk
Aruba Clearpass	Tjeneste for adgangskontroll i et nettverk
Aruba-tjenestene	Samlebetegnelse for Aruba Airwave og Aruba Clearpass.
Node	Alle komponenter i et nettverk
DHCP	Dynamic Host Connection Protocol

1. Introduksjon

Forstudierapporten er den innledende rapporten i bachelorprosjektet. Prosjektet vil gå ut på å utvikle et verktøy som behandler enhetsinformasjon fra SCCM, Airwave og Clearpass. Selve løsningsforslaget vil bli nærmere forklart i den neste rapporten.

Hensikten med forstudierapporten er å legge et godt grunnlag slik at de kommende fasene i prosjektet kan løses på best mulig måte. Dette dokumentet vil forklare hva oppgavestiller ønsker å forbedre med dagens sikkerhetsløsning og hva prosjektgruppen kan bidra med. Videre vil det gis råd om hva som trengs av ressurser for å gjennomføre prosjektet.

1. **Introduksjon** forklarer hensikten med dokumentet
2. **Bakgrunn** for prosjektet forklarer hvorfor denne oppgaven ble til i form av oppavestiller problemer og behov.
3. **Prosjektmål** viser hvilke mål prosjektgruppen og oppavestiller skal jobbe mot i dette prosjektet.
4. **Interessenter og rammebetingelser** utforsker de ulike partene som direkte eller indirekte vil bli påvirket av prosjektet i tillegg til å se på rammene for prosjektet som f.eks. kostnader og tidsbruk.
5. **Kritiske suksessfaktorer** viser hvilke faktorer som er essensielle for resultatet til prosjektet.
6. **Risikoanalyse** avdekker hva som kan gå galt i prosjektet, sannsynligheten for at dette skjer og mulige tiltak for å redusere risikoen eller håndtere utfallet.
7. **Kost/nytte-analyse** avdekker det økonomiske utfallet for oppgavestiller, og om prosjektet er faktisk er økonomisk gjennomførbart.
8. **Retningslinjer og standarder** presenterer retningslinjene og standardene som prosjektgruppen må forholde seg til gjennom prosjektets gang.
9. **Prosjektorganisering** viser partene som vil være involvert i prosjektet, samt arbeidsfordelingen mellom disse.
10. **Anbefaling om videre arbeid** avdekker hva som burde skje videre ut ifra alt man har tilegnet seg av informasjon under forstudiet.
11. **Utstyrsliste** forklarer hva slags utstyr som er benyttet og i hvilken sammenheng.
12. **Kilder** viser de kildene prosjektgruppen har benyttet seg av for å innhente informasjon.

2. Bakgrunn for prosjektet

Domstoladministrasjonen er den administrative overbygningen for domstolene, og har ansvar for IKT-systemene som brukes. Alle domstolene i Norge har en egen IKT-ressurs med varierende IKT-kompetanse, som drifter lokalt IKT-utstyr og utfører enkel administrasjon av infrastruktur. Monitorering og behandling av domstolenes nettverk og de ulike nodene i nettverket er en del av domstoladministrasjonens arbeidsoppgaver.

Domstolene i Norge har nylig gjennomført en digitaliseringsprosess som har medført store endringer når det gjelder informasjonssikkerheten. Dokumenter som tidligere ble skrevet ut og deretter makulert lagres nå digitalt og skal være tilgjengelig “on the go". Dette har medført store endringer for Domstoladministrasjonen når det gjelder IKT-systemene de forvalter. Eventuelle svakheter i nettverket kan dermed være katastrofale.

Bakgrunnen for dette prosjektet er nettopp å forbedre nettverkssikkerheten til Norges domstoler. De ønsker at prosjektgruppen skal lage et verktøy som gir en bedre oversikt over nodeinformasjonen man kan få tak i fra Airwave, Clearpass og SCCM. Det er også ønsket utforsking av funksjonalitet i Aruba-tjenestene i tillegg til anbefalinger om mulige endringer av dagens løsning.

Informasjonssikkerhet er veldig viktig, og man har sett en stor økning i fokus på dette området de siste årene rundt omkring i verden. I 2016 skrev Norsis om en undersøkelse, utført av Vanson Bourne, hvor ni av ti toppledere i mellomstore norske bedrifter forventer datasikkerhetsbrudd. I undersøkelsen sa de norske beslutningstakerne at de regner med at kostnaden av et sikkerhetsbrudd vil være på i gjennomsnitt tre millioner kroner, hvor blant annet tap av omdømme og produksjon er inkludert (NorSIS, 2016). Dersom dette stemmer vil det lønne seg for organisasjoner å investere i riktige tiltak på forhånd. Bedret nettverksikkerhet vil med andre ord være en viktig del av å ivareta datasikkerheten, og kan på lang sikt være kostnadsbesparende.

2.1 Beskrivelse av problemer og behov

Dette delkapittelet beskriver problemer med nåværende løsning og hvilke behov som er uttrykt fra oppgavestiller.

2.1.1 Beskrivelse av problemer med dagens tjenester

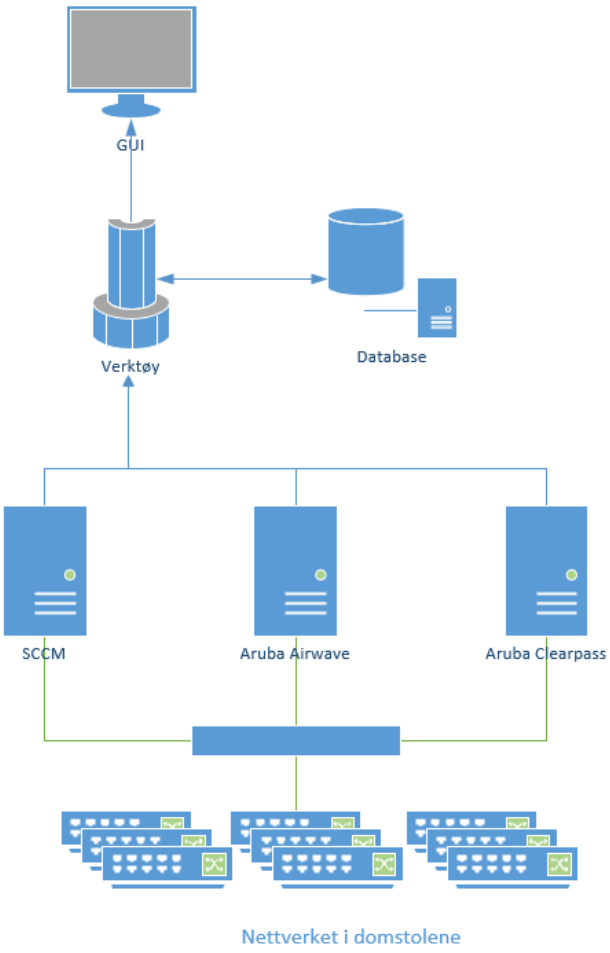
- Enkelte data som hentes ut fra Aruba-tjenestene er uoversiktlige
- Det eksisterer ingen verktøy for å sammenlikne nodeinformasjon som hentes fra SCCM, Airwave og Clearpass.

2.1.2 Beskrivelse av behov

I dagens løsning er det behov for:

- En enkel og effektiv måte å få oversikt over samlet data fra SCCM, Clearpass og Airwave
- Automatisk rapportering av eventuelle uønskede noder i nettverket
- Informasjon og anbefalinger angående bruks- og tilpasningsmuligheter av Clearpass, ettersom at tjenesten er nylig implementert

Figuren under viser relasjonen mellom nettverket, tjenestene som skal bli brukt, og verktøyet som skal utvikles.



Figur 1:Visualisering av løsningen

2.2 Beskrivelse av dagens systemer og rutiner

Domstoladministrasjonen administrerer nettverket for alle landets domstoler, og har derfor veldig mange noder å følge med på. Dagens oppsett av nettverk er todelt hvor selve domstol-nettet kun er internt og gjestenettet kan nå ut mot internett. Denne oppdelingen gjør at det interne nettet ikke kan nås fra utsiden.

For å monitorere gjestenettverket anskaffet Domstoladministrasjonen Aruba Airwave, og nå helt nylig har de anskaffet Aruba Clearpass for å bedre nettverksoversikten og adgangskontrollen på det interne nettet. Disse to tjenestene snakker ikke sammen per dags dato. Ettersom at Clearpass er helt nytt har de ikke fått utforsket alle mulighetene til det nye systemet. Dette kan med andre ord medføre endringer i bruken av systemet samtidig som prosjektet gjennomføres.

Aruba Airwave overvåker svitsjer og aksesspunkter i nettverket. Dette vil si at Domstoladministrasjonen kan følge med ytelse og pålitelighet for disse nodene. Airwaven logger også nettverkstrafikken som går i nettet, med typen nettverkstrafikk og destinasjonen til trafikken for hver enkelt bruker. I dagens oppsett monitorerer Airwave totalt 232 switcher, av disse er det 184 Aruba switcher, og det er 48 cisco switcher.

Dersom noen kobler seg på det interne nettet sendes det en DHCP forespørsel som fanges opp av Aruba Clearpass. Clearpass logger hvilke enheter som kobler seg til, og hva slags autentisering som er brukt. Per dags dato er det ikke mulig å behandle disse enhetene ved hjelp av Clearpass men dette vil i nær fremtid endre seg. Regler er satt opp for autentisering, men er ikke blitt implementert.

Automatisk behandling av disse enhetene ved hjelp av Clearpass er planlagt implementert i løpet av prosjektperioden.

For å administrere klientmaskinene i domenet til domstolene i Norge benyttes SCCM. SCCM brukes for å oppdatere klientmaskiner, deployere operativsystem til nye maskiner, sette sikkerhetsregler for maskiner, og overordnet ha oversikt over enhetene i domenet. Domstoladministrasjonen administrer ca. 3 000 klienter som er fordelt rundt om i de ulike domstolene i Norge. Det benyttes en egen server for tynnklienter, som hovedsakelig utfører utrulling av konfigurasjonsfiler til tynnklientene. Fordelingen mellom tykk- og tynnklienter er ca. 50/50.

Domstoladministrasjonen har ansatt en hovedansvarlig for driften av SCCM, og en hovedansvarlig for driften av nettverk.

3. Prosjektmål

Dette kapittelet beskriver målene for prosjektet basert på problemene og ønskene som er dokumentert. Prosjektets effektmål, resultatmål og prosessmål beskriver de ulike målene som skal nås for at prosjektet skal bli en suksess.

3.1 Effektmål

Følgende punkter ønskes å bli oppnådd:

- Uttrekk og analyse av hvilke enheter som er på nettet fra SCCM, Airwave, og Clearpass skal ikke ta mer enn 1 minutt.
- Konsolidering og sammensetting av informasjonen skal gjøres automatisk, og skal ikke ta mer enn 1 minutt.
- Redusere tidsbruken per sikkerhetsrevisjon med 20 timer.
- Redusere tidsbruken i oppfølgingsarbeidet etter en sikkerhetsrevisjon med 8 timer i året.

3.2 Resultatmål

Prosjektgruppen skal:

- Lage et verktøy som henter, sammenligner, og formaterer nodeinformasjon fra SCCM, Clearpass, og Airwave.
- Lage et Dashboard for fremstilling av data.
- Lage et verktøy som varsler ved potensielle trusler.
- Levere verktøyet og dokumentasjonen senest 20. Mai 2019.

3.3 Prosessmål

Prosjektgruppen ønsker å:

- Oppnå karakteren A
- Øke sin kompetanse innen informasjonssikkerhet
- Forbedre samarbeid- og kommunikasjonsevner
- Tilegne seg nyttige erfaringer fra arbeidslivet

3.4 Prosjektets omfang

Prosjektet skal:

- Utvikle et verktøy i testmiljø levert av NTNU.
- Basere seg på informasjon som kan hentes fra SCCM, Clearpass, og Airwave.
- Levere et verktøy som vil fungere på de systemene Domstoladministrasjonen benytter i dag.
- Gjennomføre en kort brukerveiledning for nettverk- og klientadministrator.

3.5 Verktøyets funksjonelle egenskaper

Verktøyet skal:

- Automatisk innhente informasjon fra SCCM, Airwave og Clearpass
- Automatisk konsolidere og sammenligne informasjonen for å finne eventuelle sikkerhetsproblemer
- Formatere utdata på en oversiktlig og lettleselig måte.

3.5.1 Ikke funksjonelle egenskaper og krav

- Verktøyet skal dokumenteres på en forståelig og tilfredsstillende måte

3.6 Prosjekts milepæler og hovedaktiviteter

Prosjektet deles inn i ulike faser basert på aktivitetene som skal gjennomføres:

Forstudiefase (14.01.19 - 13.02.19)

- Oppstart av prosjektet og definering av oppgaven.
- Opprettelse av samhandlingsplattform og avtaler
- Utforming av forstudierapport

Designfase (13.02.19 - 04.03.19)

- Utforming av løsningsdesignet

Utviklingsfase (05.03.19 - 30.04.19)

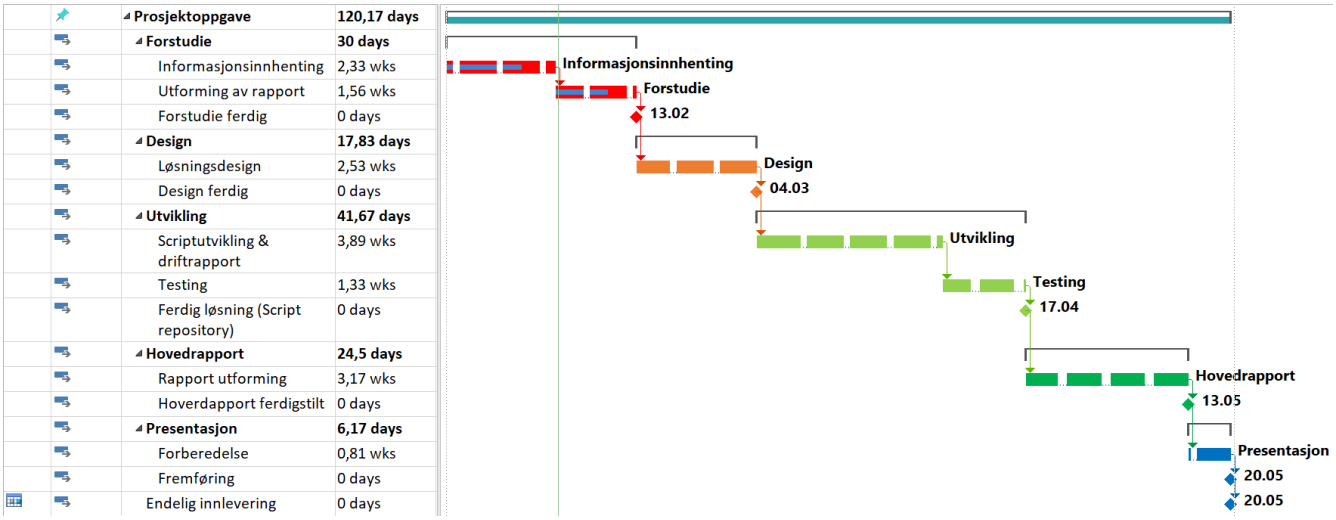
- Utvikling av verktøyet.
- Siste test av verktøyet.
- Utforming av sluttrapport.

Avslutningsfase (30.04.19 - 20.05.19)

- Ferdigstilling av verktøyet og dokumentasjonen
- Innlevering av prosjektet
- Presentasjon av prosjektet

Ukentlig arbeidsmengde er lagt opp til 28 timer. Arbeidsfordelingen for de ulike dagene vil se slik ut for prosjektgruppen:

- Mandag: 09:00 – 16:00
- Onsdag: 09:00 – 16:00
- Torsdag: 09:00 – 16:00
- Fredag: 09:00 – 16:00



Figur 2: Gantt-diagram for prosjektet. Original er vedlagt

Gantt-diagrammet viser planen for tidsbruk per aktivitet som prosjektgruppen skal gjennomføre. De ulike aktivitetene er satt opp basert på de dokumentene som skal leveres og fremføringen. Utformingen av driftsdokument skjer samtidig som løsningen utvikles. Testing blir kontinuerlig utført under utviklingsfasen, og det er planlagt en ekstra testfase etter utviklingsfasen er gjennomført.

4. Interessenter og rammebetingelser

Kapittelet forklarer hvem som er interessentene for prosjektet og de rammebetingelsene som setter grensene for prosjektets livssyklus.

4.1 Interessentanalyse

Oppgavestiller

Oppgavestiller er Domstoladministrasjonen, representert av Øyvin Moe (Rådgiver ved Domstoladministrasjonen).

Sikkerhetsansvarlige

- Informasjonssikkerhetsansvarlig

Sluttbrukere

- Nettverksansvarlig
- Klientadministrator
- Brukersenteret

Prosjektgruppen

- Marius Myhre
- Tormod Lien

Veileder

Veileder for prosjektet er Tor Ivar Melling.

4.1.4 Eksterne interessenter

EKSTERNE INTERESSENTER	SUKSESSKRITERIER	BIDRAG TIL PROSJEKTET
OPPGAVESTILLER	Implementasjon av den nye løsningen som gir enklere drift av dagens systemer	Bidrar med informasjon og bistand slik at prosjektgruppen er best mulig rustet til å besvare oppgaven.
INFORMASJONSSIKKERHETSANSVARLIG	Økning i den totale sikkerheten i nettverket til domstolene	Bidrar med informasjon og bistand slik at prosjektgruppen er best mulig rustet til å besvare oppgaven.
NETTVERKSANSVARLIG	Bedre oversikt over enheter i nettverket	Bidrar med teknisk informasjon og bistand slik at prosjektgruppen får god forståelse for dagens bruk av Airwave, og Clearpass
KLIENTADMINISTRATOR	Bedre oversikt over enheter i nettverket	Bidrar med teknisk informasjon og bistand slik at prosjektgruppen får forståelse for dagens bruk av SCCM
BRUKERSENTERET	Bedre oversikt over enheter i nettverket	Bidrar med informasjon og bistand slik at prosjektgruppen er best mulig rustet til å besvare oppgaven.

*Tabell **1**: Eksterne interessenter med deres bidrag og suksesskriterier*

4.1.5 Interne interessenter

INTERNE INTERESSENTER	SUKSESSKRITERIER	BIDRAG TIL PROSJEKTET
PROSJEKTGRUPPEN	Løse oppgaven i samsvar med satte mål og rammebetingelser.	Besvarelse av oppgaven
VEILEDER	Jevnlige møter slik at veileder kan følge med og komme med innspill ved behov	Veiledning

*Tabell **2**: Interne interessenter med deres bidrag og suksesskriterier*

4.2 Rammebetingelser

Delkapittelet beskriver de rammebetingelsene som prosjektgruppen må forholde seg til i prosjektarbeidet.

4.2.1 Krav til ferdigstillelse

Kravet for ferdigstillelse av prosjektet er 20.mai.2019

4.2.2 Kostnadsramme

Prosjektets kostnadsramme er på 990 000,- kroner

4.2.3 Tidsbruk

Prosjektet har en tidsramme på 500 arbeidstimer per prosjektmedlem, med et slingringsmonn på +- 10%. Dette tilsvarer en maksimal tidsbruk på 1100 arbeidstimer for prosjektgruppen samlet sett.

5. Kritiske suksessfaktorer

Kapittelet beskriver de faktorene som er avgjørende for at prosjektet skal bli en suksess.

5.1 Suksessfaktorer

Suksessfaktorer for **oppgavestiller**:

- Verktøyet bidrar til å bedre oversikten over sårbarheter i nettverket.
- Verktøyet bidrar til å tette sårbarheter i nettverket.
- Verktøyet blir en effektiv måte å innhente nodeinformasjon på.

Suksessfaktorer for **informasjonssikkerhetansvarlig:**

- Godt dokumentert arbeid slik at man lett kan sette seg inn i hva som er gjort.
- Verktøyet bidrar til å bedre oversikten over klientsituasjonen i domenet og nettverket til domstolene og Domstoladministrasjonen.

Suksessfaktorer for **nettverksansvarlig og klientadministrasjonsansvarlig**:

- Bortfall av arbeid som ville vært nødvendig for å skape en tilsvarende løsning
- Løsning skal enkelt gi oversikt over eventuelle noder som kan være en sikkerhetsrisiko
- Lett forståelige scripts som gir en god oversikt over utdata.
- God dokumentasjon av arbeid og løsningsforslag

Suksessfaktorer for **brukersenter:**

- Verktøyet skal gi enkel oversikt over enheter på nettverket, for å hjelpe brukesenteret i sine oppgaver.

Suksessfaktorer for **prosjektgruppen**:

- Forbedre sine kunnskaper innen informasjonssikkerhet
- God kommunikasjon internt i prosjektgruppen
- Samarbeidsavtalen følges som avtalt
- Levere en løsning som overholder gitte krav

Suksessfaktorer for **veileder:**

- Prosjektet gjennomføres på en god måte.
- Ha løpende dialog med prosjektgruppen.
- Kvaliteten på arbeidet er tilfredsstillende.

Felles suksessfaktorer for **oppgavestiller og prosjektgruppen**:

- God kommunikasjon mellom oppgavestiller, prosjektgruppen og veileder slik at eventuelle endringer i prosjektets mål og rammer kan avdekkes.

5.2 Informasjonsbehov

Veiledere

Veileder fra NTNU, Tor Ivar Melling, og veileder fra Domstoladministrasjonen, Øyvin Moe, vil ha behov for statusoppdateringer, som vil komme i form av møter med prosjektgruppen. I startperioden skjer disse møtene ukentlig, og utover prosjektets gang vil disse møtene komme med hyppigere eller mindre hyppige intervaller. Møteinnkalling til veiledere skal sendes ut minst tre dager i forveien. Møtereferat skal føres av prosjektgruppen og legges ved neste møteinnkalling.

Oppgavestiller

Veileder og kontaktperson fra Domstoladministrasjonen, Øyvin Moe, har behov for informasjon om prosjektets gang, noe som vil skje gjennom statusmøter som beskrevet under veiledere samt en løpende dialog med prosjektgruppen. Prosjektgruppen er tildelt et kontor en etasje over oppgavestiller, men vil etter planen flytte ned i umiddelbar nærhet til oppgavestillers kontor. Dersom oppgavestiller og studentene ikke er i umiddelbar nærhet av hverandre kan oppgavestiller nås på telefon og mail.

Nettverksansvarlige

Nettverksansvarlige vil ha behov for informasjon om hva prosjektgruppen arbeider med, for å sikre at det prosjektgruppen gjør er hensiktsmessig og relevant. Mot slutten av prosjektet vil nettverksansvarlig ha behov for en gjennomgang av løsningen.

Prosjektgruppen

Prosjektgruppen har behov for hjelp og veiledning fra veiledere til hvordan de best mulig kan gjennomføre prosjektet. Der prosjektgruppen har behov for nærmere informasjon om Domstoladministrasjonen, vil dette kunne gjøres ved å kontakte Øyvin, eller eventuelt avtale møter med relevante interessenter direkte. I tillegg vil det være behov for prosjektgruppen å få informasjon underveis i prosjektet fra nettverksansvarlig og klientadministrator, slik at prosjektgruppen utvikler et verktøy det er behov for.

6. Risikoanalyse

Risikoanalysen tar for seg sannsynligheten for at en hendelse skal inntreffe, samt konsekvensene dersom den blir en realitet. Deretter tar analysen for seg mulige tiltak som reduserer sannsynligheten og/eller konsekvensene for de ulike hendelsene.

6.1 Beskrivelse av tabellen

Tabellen gir en oversikt over de ulike risikoene. For hver hendelse blir det gitt en beskrivelse av hva hendelsen er og hvilke konsekvenser den kan få. Det settes poeng for sannsynligheten for at hendelsen inntreffer og for konsekvensen dersom den inntreffer. Til slutt blir det beskrevet hvilke tiltak som vil bli satt i verk for å redusere risikofaktoren for hendelsen

Risikofaktoren til en hendelse vil være produktet av sannsynligheten og konsekvensen. Her måles sannsynlighet på en skala fra 1 til 5, basert på hvor ofte hendelsen kan forekomme, og konsekvens på en skala fra 1 til 4, basert på alvorlighetsgraden om hendelsen inntreffer.

S = Sannsynlighet

K = Konsekvent

RF = Risikofaktor

Sannsynlighet:

- 5 – Flere ganger i uken.
- 4 – En gang i uken.
- 3 – En-to ganger i måneden.
- 2 – To til fire ganger i halvåret.
- 1 – En eller færre ganger i halvåret

Konsekvens:

- 5 – Alvorlige konsekvenser for prosjektet
- 4 – Store konsekvenser for prosjektet
- 3 – Moderate konsekvenser for prosjektet
- 2 – Små konsekvenser for prosjektet
- 1 – Minimale problemer for prosjektet

Hendelser:

Prosjektspesifikke risikoer:

1. Uforventet tidsnød
2. Problemer med utstyr (personlig PC, Testmiljø, etc.)
3. Prosjektgruppen klarer ikke utvikle løsningen
4. Tap av data ved implementasjon av løsning
5. Domstoladministrasjonen nedprioriterer prosjektet
6. Prosjektgruppen utvikler et verktøy det ikke er behov for.

Ufrivillige risikoer:

7. Sykdom blant veiledere
8. Tap av data hos prosjektgruppen
9. Kortvarig sykdom

10. Langvarig sykdom
11. Intern misnøye i prosjektgruppen

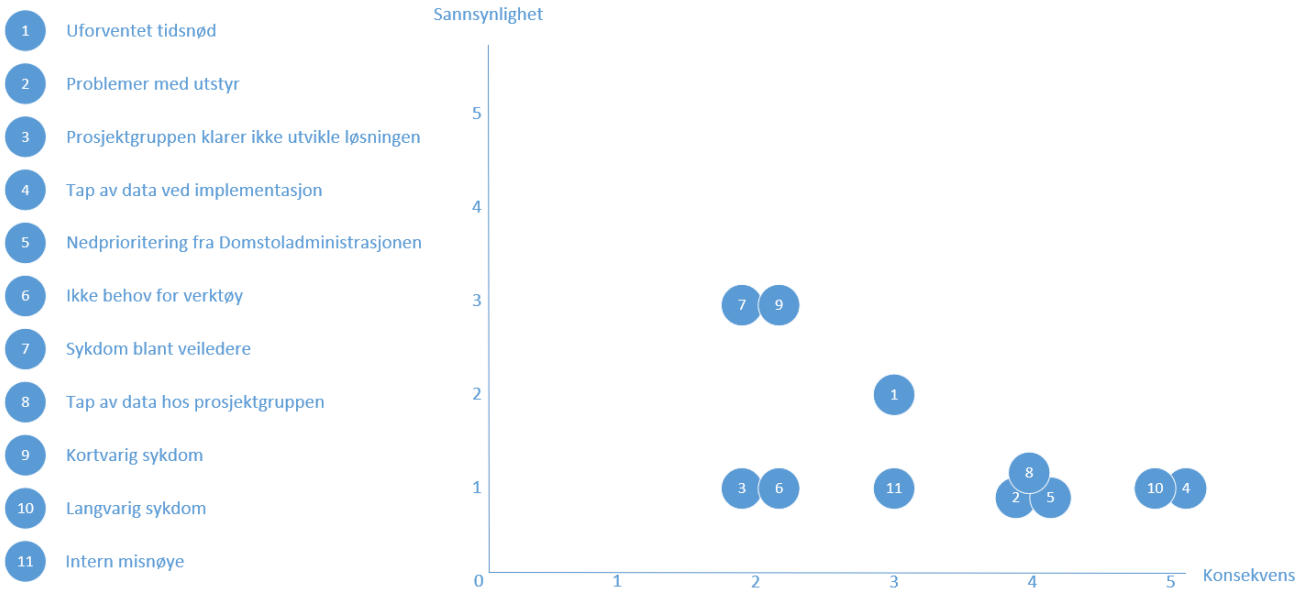
HENDELSE	BESKRIVELSE	S	K	RF	TILTAK
1	Ting tar lengre tid enn forventet, noe som kan gjøre at det blir tidsnød mot slutten av prosjektet	2	3	6	For å unngå tidsnød planlegges alle oppgaver med en sikkerhetsmargin, og prosjektgruppen holder ukentlige møter med veiledere for å få god oversikt på hva som er gjort, og hva som må gjøres
2	Problemer med utstyr brukt til å utføre prosjektet. Dette kan være personlige pcer, laboppsett fra NTNU, eller annet utstyr som ikke fungerer slik som det skal	1	4	4	Utstyr som blir brukt til prosjektet skal holdes oppdatert, og skal behandles med respekt. Dersom en av prosjektgruppens maskiner får store problemer, har prosjektgruppen alternative maskiner som kan benyttes (Stasjonære pcer, andre laptopper).
3	Prosjektgruppen klarer ikke utvikle løsning de har funnet. Dette kan være mangel på for eksempel PowerShell-kompetanse, eller at det viser seg etter utforskning at det ikke er mulig å gjennomføre planlagt løsning.	1	2	2	Om det viser seg i løpet av en senere fase i prosjektet at det ikke kan utformes som planlagt, har prosjektgruppen "backup"-løsninger som kan utnyttes for å svare på oppgaven. I tilfellet manglende kompetanse, er det ansatte hos Domstoladministrasjonen og NTNU som har gode kunnskaper i PowerShell. Disse kan benyttes for å få hjelp til utførelse.
4	Tap av data ved implementasjon av løsning. Dette vil i hovedsak være ved bruk av PowerShell-script, som kan om disse er utformet med feil, få store konsekvenser for systemet til Domstoladministrasjonen. Andre typer tap av data kan være feilkonfigurering av ClearPass eller AirWave, som kan føre til at disse må tilbakestilles.	1	5	5	Ved å teste løsninger i lab-oppsett hos NTNU vil eventuelle feil bli funnet før script eller konfigurasjoner blir gitt over til Domstoladministrasjonen. I tillegg er det avtalt av både Lars og Geir Hugo at eventuelle script skal leses over og testes av de før disse blir satt ut i produksjonsmiljø.
5	Dersom Domstoladministrasjonen nedprioriterer prosjektet vil det være vanskelig for prosjektgruppen å gjennomføre prosjektet. Om det blir vanskelig å få tak i nødvendig informasjon fra veileder eller andre interessenter vil kvaliteten på verktøyet	1	4	4	For å unngå nedprioritering er det viktig at prosjektgruppen har løpende kommunikasjon med Domstoladministrasjonen om hva som blir gjort, og hvilken nytteverdi som skapes. I tillegg er det viktig å tidlig sette opp et testmiljø slik at

	som prosjektgruppen skal utvikle ikke være like god som den kan være.				arbeidet med prosjektet kan fortsette selv om Domstoladministrasjonen mister interessen.
6	Dersom prosjektgruppen utvikler et verktøy Domstoladministrasjonen ikke har behov for, vil det være unødvendig tidsbruk for oppgavestiller.	1	2	2	Løpende kommunikasjon med interessentene fra Domstoladministrasjonen
7	Sykdom blant veiledere som gjør at prosjektgruppen ikke får hjelpen de trenger for å utføre prosjektet.	3	2	6	Ved å ha to veiledere, en fra NTNU og en fra Domstoladministrasjonen er det liten sannsynlighet for at begge veilederne blir syke til samme tid. Ved eventuell sykdom meldes dette til møtedeltagerne via mail.
8	Tap av data hos prosjektgruppen, for eksempel data fra SharePoint-området som blir korrupt og all informasjon der blir tapt	1	4	4	For å forhindre katastrofal tap av data ved feil hos SharePoint, vil all data som lagres der bli backet opp på en ekstern harddisk hos prosjektgruppen. Hver Fredag tas en full backup av innholdet av SharePoint-siten.
9	Kortvarig sykdom og fravær som gjør at deltagere i prosjektgruppen ikke kan møte opp. Kortvarig defineres som maks 1 uke.	3	2	6	Opprettholde god hygiene og godt kosthold. Ved kortvarig sykdom vil den berørte melde fra som anvist i samarbeidskontrakten, og vil så godt som mulig arbeide hjemmefra. For å unngå at denne sykdommen blir gitt til andre vil den syke holde seg hjemme.
10	Langvarig sykdom og fravær	1	5	5	Dersom et medlem av prosjektgruppen får langvarig sykdom eller skade, vil den så godt som mulig forsøke å arbeide med prosjektet hjemme. Dersom det er alvorlig sykdom/skade, vil veildere bli informert så fort som mulig.
11	Intern misnøye i prosjektgruppen.	1	3	3	Dersom det oppstår misnøye skal eventuelle uenigheter løses så fort som mulig. Uenigheter som prosjektgruppen ikke klarer å håndtere internt skal løses ved hjelp av veileder.

*Tabell **3**: Risikovurdering*

6.2 Visualisering av risikofaktorer

Grafen er en visuell fremvisning av risikofaktorene nevnt i tabellen over. X-aksen er konsekvens, og Y-aksen er sannsynlighet. Elementer som er lenger ned og til venstre har lavere risikofaktor, og elementer lenger opp og til høyre har høyere risikofaktor.



Figur 3: Risikofaktorer

7. Kost/nytte analyse

Kapittelet tar for seg en analyse av prosjektet og ser om det er økonomisk ansvarlig å gjennomføre det. Analysen fokuserer på Domstoladministrasjonens kostnader og nytte ved prosjektet.

7.1 Kvantifiserbar- og ikke-kvantifiserbar nytte

Med utgangspunkt i effektmålene for prosjektet, viser prosjektgruppen til følgende kvantifiserbar- og ikke-kvantifiserbar nytte for Domstoladministrasjonen og prosjektgruppen.

Effektmål:

- Uttrekk og analyse av hvilke enheter som er på nettet fra SCCM, Airwave, og Clearpass skal ikke ta mer enn 1 minutt.
- Konsolidering og sammensetting av informasjonen skal gjøres automatisk, og skal ikke ta mer enn 1 minutt.
- Redusere tidsbruken per sikkerhetsrevisjon med 20 timer.
- Redusere tidsbruken i oppfølgingsarbeidet etter en sikkerhetsrevisjon med 8 timer i året.

Kvantifiserbar nytte:

- Beregnet kroneverdi ved at nettverk- og klientansvarlig hos Domstoladministrasjonen ikke trenger å bruke 1 000 timer på å produsere en tilsvarende løsning.
    - Prosjektgruppen går her ut ifra at de har en lønn på kr 550 000,- noe som tilsvarer en timelønn på 291,59,-. Det antas at innleide konsulenter har en medført kostnad på kr 1 400,- per time. Prosjektgruppen antar også at nettverk- og klientansvarlig ville utviklet samme produktet på halve tiden pga. mer kunnskap og erfaring.
        - 250 timer x 291,59 kr = 72 897,5 kr
        - 250 timer x 1400 kr = 350 000 kr
- Beregnet kroneverdi ved at sikkerhetsrevisjoner tar kortere tid.
    - Prosjektgruppen antar at det er 5 personer som deltar på revisjonen. Reduksjonen i tidsbruk med tanke på nettverksanalysen antas til å være en reduksjon på 20 arbeidstimer for revisjonsgruppen. Det blir her antatt at det hentes inn konsulenter som har en medført kostnad på kr 1 400,- per time. Sikkerhetsrevisjoner skjer hvert fjerde år.
        - 5 personer x 1400 kr x 20 timer = 140 000 kr
- Sikkerhetsrevisjoner fører også til tiltak som man skal måle virkningsgraden/effekten av. Dette etterarbeidet vil ta kortere tid med bedre oversikt. Prosjektgruppen går dermed ut ifra at man vil årlig spare 8 timer på dette arbeidet.
    - Dette tilsvarer 30 x 291,59 kr = 8 747,7 kr.
- Skulle samme jobben som verktøyet utfører blitt gjort manuelt ville det tatt ca 56 timer. Dette arbeidet antas å bli gjort en gang i måneden.
    - 28 timer x 291,59 kr = 8 164,52 kr
    - 28 timer x 1 400 kr = 39 200 kr
    - 12 x (8 164 + 39 200) = 568 374,24 kr

Ikke-kvantifiserbar nytte:

- Verktøyet vil gi nettverksansvarlige bedre oversikt over enheter i nettverket
- Verktøyet vil gi nettverksansvarlige et godt utgangspunkt for videreutvikling av løsninger som bruker data fra Airwave, Clearpass og SCCM

- Der verktøyet kan oppdage klientmaskiner som bruker en eldre versjon av Windows, vil man kunne iverksette tiltak for å stoppe bruk av utdatert programvare. Dette vil øke sikkerheten, og kan spare penger i form av lisenskostnader, og det vil være mindre sjanse for innbrudd ved utnyttelse av sikkerhetshull i gammel programvare.

7.2 Bortfall av direkte kostnader

Prosjektet skal ikke erstatte eksisterende løsninger, og vil derfor ikke innebære bortfall av direkte kostnader.

7.3 Estimerte kostnader

Estimert medført kostnad for konsulentarbeid av prosjektgruppen er 900 kr. Maksimalt antall timer per person er 550.

900 kr x 550 = 495 000 kr

495 000 kr x 2 = 990 000

Maksimale konsulentkostnader for prosjektgruppen ved maks antall arbeidstimer blir: 990 000 kroner.

7.4 Sammenstilling av kost/nytte

Delkapittelet visualiserer de tallene prosjektgruppen har kommet frem til i de øvrige delkapitlene under punkt 7. Tabellen gir et klart bilde av at dette ikke er et dyrt prosjekt. Over en 5-års periode viser tabellen at de eneste kostnadene er utviklingskostnadene som er anskaffelseskostnaden av prosjektgruppen. Når det gjelder sum nytte av prosjektet etter 5 år viser tabellen at dette tilsvarer ca. summen av å ansette en ekstra ansatt.

	År 1	År 2	År 3	År 4	År 5	Sum
Kvantifiserbar nytte	kr 458 747,70	kr 577 121,94	kr 577 121,94	kr 577 121,94	kr 717 121,94	kr 2 907 235,46
Bortfall kostnader	kr 0,00	kr 0,00	kr 0,00	kr 0,00	kr 0,00	kr 0,00
Sum Nytte	**kr 458 747,70**	**kr 577 121,94**	**kr 577 121,94**	**kr 577 121,94**	**kr 717 121,94**	**kr 2 907 235,46**
Utviklingskostnader	kr 990 000	kr 0,00	kr 0,00	kr 0,00	kr 0,00	kr 990 000,00
Sum kostnader	**kr 990 000,00**	**kr 0,00**	**kr 0,00**	**kr 0,00**	**kr 0,00**	**kr 990 000,00**
Beregnet nytte (Nytte - kostnader)						**kr 1 917 235,46**

*Tabell **4**: Kost/nytte*

8. Retningslinjer og standarder

Kapittelet vil ta for seg de retningslinjer og standarder som skal følges gjennom prosjektets livssyklus.

8.1 Krav til dokumentasjon

Tabellen under tar for seg en kort beskrivelse av de ulike dokumentene som skal produseres av prosjektgruppen. Samtlige dokumenter skal lagres i SharePoint.

DOKUMENT	FRIST	FORMAT	BESKRIVELSE
SAMARBEIDSAVTALE	17.01	.docx	Retningslinjer for samarbeidet internt i prosjektgruppen.
FORSTUDIERAPPORT	13.02	.docx	En beskrivelse av prosjektet og Domstoladministrasjonen.
DESIGNDOKUMENT	04.03	.docx	En konseptuell beskrivelse av løsningen.
SLUTTRAPPORT	20.05	.docx	En oppsummering av prosjektet og arbeidsprosessen. Vurderer om målene er oppnådd eller ikke.
SCRIPT	15.05	.ps1	En kort forklaring av de ulike scriptene som er utviklet.
MØTEINNKALLING	To dager før møtet	.docx	Innkalling følger malen fra NTNU. De lagres på SharePoint og vises til med lenke i møteinnkallingen som gjøres via epost.
MØTEREFERAT	En dag etter møtet	.docx	Referat følger malen fra NTNU. De skal lagres på SharePoint. Referat fra forrige møte skal vises til med lenke i neste møteinnkallingsdokument.
TIMELISTE	Hver fredag	.xlsx	Oversikt over arbeidstimene, samt en ukentlig oversikt som beskriver hva som er gjort.

*Tabell **5**: Retningslinjer for dokumentasjon*

8.2 Krav til kvalitetsgjennomganger

Tabellen under tar for seg kravene til kvalitetsgjennomganger av dokumenter og løsning.

DOKUMENT	HVEM	HVORDAN
FORSTUDIERAPPORT	Veiledere, prosjektgruppe	Gjennomgås og godkjennes på ukentlige møter med veiledere fra NTNU og DA. Etter rapport er ferdigstilt skal den godkjennes av veileder og oppgavestiller
DESIGNDOKUMENT	Veiledere, prosjektgruppe	Gjennomgås og godkjennes på ukentlige møter med veiledere fra NTNU og DA. Etter rapport er ferdigstilt skal den godkjennes av veileder og oppgavestiller
HOVEDRAPPORT	Veiledere, prosjektgruppe	Gjennomgås og godkjennes på ukentlige møter med veiledere fra NTNU og DA. Etter rapport er ferdigstilt skal den godkjennes av veileder og oppgavestiller
LØSNINGER	Veiledere, prosjektgruppe, Lars/Geir Hugo	Gjennomgås og godkjennes på ukentlige møter med veiledere fra NTNU og DA. Etter godkjenning av veiledere, skal løsninger leveres til Lars & Geir Hugo, for godkjenning.
SLUTTRAPPORT	Veiledere, prosjektgruppe	Gjennomgås og godkjennes på ukentlige møter med veiledere fra NTNU og DA. Etter rapport er ferdigstilt skal den godkjennes av veileder og oppgavestiller

*Tabell **6**: Krav til kvalitetsgjennomganger*

8.3 Krav til standarder og metoder

8.3.1 Navnestandarder

- Møtereferat skal navngis på formen: Møtereferat DD.MM.ÅÅÅÅ
- Møteinnkallinger skal navngis på formen: Møteinnkalling DD.MM.ÅÅÅÅ
- Endelig innlevering skal være i PDF format, med oppgavenummeret til oppgaven som navn (015.pdf)

8.3.2 Programmeringsstandarder

I utgangspunktet vil all programmering foregå med Windows PowerShell. All programmering skal utføres med fokus på lesbarhet, vedlikehold, og konfigurabilitet, slik at eventuelt etterarbeid med scriptene som blir laget blir enklest mulig.

- Funksjoner som blir laget skal navngis med vanlig PowerShell Verb-Substantiv navngivning. Verbet skal si hvilken handling som cmdletten utfører, og substantivet skal si hvilken ressurs handlingen blir utført på.
    - Eksempel: Hent-DataFraAirWave
    - Merk her at det brukes norske verb, ikke verb fra verblisten i PowerShell. Dette er for å få god klarhet i hva som er laget av prosjektgruppen, og hva som er native-funksjoner i PowerShell.
- Variabler som brukes skal benytte lower camelcase, med liten bokstav på første ord, og stor bokstav på resten.
    - Eksempel: navnPåVariabel

8.3.3 Dokumentmaler

Vi bruker dokumentmaler utgitt av NTNU institutt for datateknologi og informatikk (NTNU IDI, 2012). Malene inkluderer forstudie, designdokument, samarbeidsavtaler, driftsdokument, sluttrapport, møteinnkallinger, og møtereferat. Timelister føres i Excel, og det er her ikke brukt mal.

8.3.4 Utviklingsverktøy

- Tekstdokumenter
    - Word Online i SharePoint blir brukt til samskriving av tekstdokumenter
    - Microsoft Word 2016 bruker for utforming og design av tekstdokumenter
- Gantt-diagram/prosjektplaner
    - Microsoft Project 2016
- Testoppsett
    - VCenter oppsett levert av NTNU brukes for testing av løsninger
- Script
    - Windows PowerShell Integrated Scfipting Environment (ISE)
- Timelister
    - ExcelOnline i Sharepoint blir brukt til samskriving av timelister
    - Microsoft Excel 2016 blir brukt for utforming og design av timelister

8.3.5 Testoppsett

Som testlab benyttes et VCenter-miljø satt opp på NTNU sine datasystemer. Det blir her satt opp et oppsett som skal best mulig etterligne Domstoladministrasjonens systemer, med SCCM, Airwave, og ClearPass.

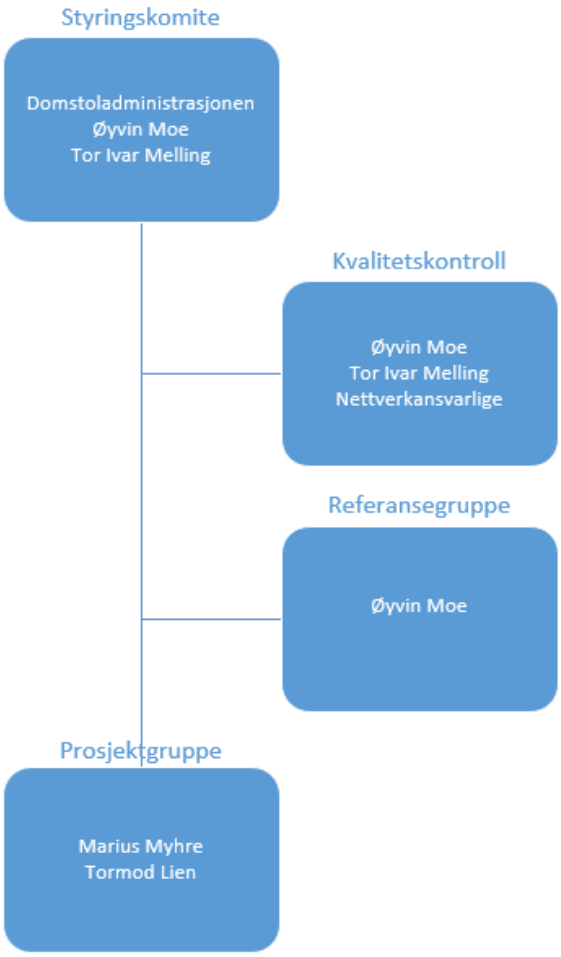
8.4 Endringshåndtering

Gjennom prosjektets gang er det forventet at endringsønsker vil kunne komme fra oppavestiller, brukere, veiledere, eller prosjektgruppen. Alle endringsforespørsler skal håndteres på følgende måte:

1. Dokumenter endringens innhold
    a. Dokumentasjon lagres i SharePoint, under dokumenter/Endringsforespørsler
2. Analyser konsekvensene for prosjektet
3. Beregn eventuell kostnad/nytte
4. Godkjenn og aksepter endringen
    a. Endringer skal godkjennes av oppavestiller og prosjekgruppen
5. Loggfør endringen
6. Juster planene
7. Informer interessenter
8. Gjennomfør endringen

9. Prosjektorganisering

Kapittelet tar for seg organiseringen av de involverte partene i prosjektet samt å se på arbeidsfordelingen innad i prosjektgruppen. Oversiktsbilde blir fremstilt i figur 9.1



Figur 4: Prosjektorganisering

Oppgavestiller:

Domstoladministrasjonen

Styringskomite:

Domstoladministrasjonen, Øyvin Moe (Veileder DA), Tor Ivar Melling (Veileder NTNU)

Kvalitetskontroll:

Gruppens veiledere (Øyvin Moe & Tor Ivar Melling) får ansvar for kvalitetskontroll av samtlige rapporter. Gruppens veiledere samt Lars & Geir Hugo får ansvar for kvalitetskontroll av script/tekniske løsninger som blir utviklet.

Referansegruppe:

Veileder fra Domstoladministrasjonen, Øyvin Moe, får rolle som referansegruppe.

Prosjektleder/Arbeidsfordeling:

Prosjektleder blir rotert på månedlig basis, der det starter i januar med Marius som leder. Ettersom prosjektgruppen bare består av to medlemmer, er det ingen behov for faste roller eller arbeidsoppgaver. I hovedsak vil arbeid fordeles likt, og om det er nødvendig med fordeling av arbeidsoppgaver vil dette bli gjort når nødvendig.

10. Anbefaling om videre arbeid

Vi vil anbefale at dette prosjektet videreføres til designfasen med de planene som er lagt fram i forstudierapporten. Grunnen til dette er at ut ifra de tallene og informasjonen som er kommet frem i dette dokumentet har Domstoladministrasjonen god nytte av å få prosjektet gjennomført.

11. Utstyrsliste

Prosjektgruppen vil benytte seg av egne bærbare datamaskiner, ekstra skjermer vil bli gjort tilgjengelig av Domstoladministrasjonen. Et virtuelt testmiljø blir gjort tilgjengelig av NTNU, slik at prosjektgruppen har en testlab å benytte seg av.

12. Kilder

NorSIS (2016) *Informasjonssikkerhet er mye mer enn teknologi.* Available at: https://norsis.no/10524-2/ (Accessed: 17. January 2019)

NTNU IDI (2012) *Maler og standarder*. Available at: http://iie.ntnu.no/fag/maler-standarder/ (Accessed: 01. February 2019)

Designdokument

Bacheloroppgave 015 *Marius Myhre*

Våren 2019 *Tormod Lien*

IDRI3001 Bacheloroppgave i drift av datasystemer

20. Mai. 2019

DOMSTOL ADMINISTRASJONEN

NTNU
Kunnskap for en bedre verden

Revisjonshistorie

Dato	Versjon	Beskrivelse	Forfatter
06.02.2019	0.1	Opprettet dokumentet	Prosjektgruppen
07.02.2019	0.2	Kap 3 og 4	Tormod
13.02.2019	0.3	Kap 5 og 6	Tormod
14.02.2019	0.4	Kap 7	Tormod
18.02.2019	0.6	Oppdatert info	Prosjektgruppen
27.02.2019	0.7	Oppdatert info	Prosjektgruppen
28.02.2019	0.8	Oppdatert info	Prosjektgruppen
09.03.2019	0.9	Korrekturlesing	Prosjektgruppen
10.05.2019	1.0	Ferdig formatert	Prosjektgruppen

Innholdsfortegnelse

Figurliste

Ordliste

Ord	Beskrivelse
Løsningen	Løsningen på problemstillingen. Består av verktøyet, databaseløsningen, og visualiseringsløsningen.
Verktøyet	Prosjektgruppens PowerShell-script for uthenting og analyse av data.
Databaseløsning	Prosjektgruppens løsning for lagring av data etter analyse og datagrunnlag for visualiseringsløsning.
Visualiseringsløsning	Prosjektgruppens løsning for visualisering av data fra databaseløsning.
SCCM	System Center Configuration Manager
Aruba Airwave	Tjeneste for overvåking av svitsjer og aksesspunkter i et nettverk
Aruba Clearpass	Tjeneste for adgangskontroll i et nettverk
Aruba-tjenestene	Samlebetegnelse for Aruba Airwave og Aruba Clearpass
Node	Komponent i nettverk
Nodeinformasjon	Informasjon om en komponent i et nettverk
DHCP	Dynamic Host Connection Protocol
DHCP-request	Forespørsel om IP-adresse fra klient til ruter
Dashboard	Informasjonadministrasjonsverktøy som framviser data visuelt
PowerShell	Scriptspråk utviklet av Microsoft for å automatisere arbeidsoppgaver på windowsmaskiner
PowerShell Remoting	Utføre PowerShell-kommandoer fra en annen maskin
SQL	Structured Query Language
Trello	Samarbeidsverktøy
GitHub	Verktøy for samarbeid og versjonskontroll av kode
Azure Stack	Skytjeneste levert av Microsoft
PowerBI	Analyse- og visualiseringsverktøy
HTML	Hyper Text Markup Language
CSS	Cascading Style Sheet
PHP	PHP: Hypertext Preprocessor
API	Application Programming Interface
REST	Representational state transfer
RESTful API	API som benytter seg av REST-teknologi
Access Token	“Passord” for å kunne få informasjon fra et API

1. Innledning

Designdokumentet beskriver løsningen som prosjektgruppen skal utvikle. Løsningen består av et verktøy for innhenting og analyse av data, databaseløsning og visualiseringsløsning. Dokumentet inneholder en beskrivelse av oppgavestiller og deres behov og avgrenser løsningens egenskaper ut ifra disse ønskene. Deretter beskrives hvilke krav som settes for løsningen og prosjektgruppens strategi og metode for å utvikle det. Til slutt beskrives de tekniske løsningene som er valgt, og det forklares hvordan disse benyttes i løsningen.

2. Om Oppgavestiller og behov

2.1 Oppgavestiller

Domstoladministrasjonen er den administrative overbygningen for domstolene, og har ansvar for IKT-systemene som brukes. Alle domstolene i Norge har en egen IKT-ressurs med varierende IKT-kompetanse, som drifter lokalt IKT-utstyr og utfører enkel administrasjon av infrastruktur. Monitorering og behandling av domstolenes nettverk og de ulike nodene i nettverket er en del av domstoladministrasjonens arbeidsoppgaver.

Domstolene i Norge har nylig gjennomført en digitaliseringsprosess som har medført store endringer når det gjelder informasjonssikkerheten. Dokumenter som tidligere ble skrevet ut og deretter makulert lagres nå digitalt og skal være tilgjengelig “on the go". Dette har medført store endringer for Domstoladministrasjonen når det gjelder IKT-systemene de forvalter. Eventuelle svakheter i nettverket kan dermed være katastrofale.

Dagens oppsett av nettverk er todelt hvor selve domstol-nettet kun er internt og gjestenettet kan nå ut mot internett. Denne oppdelingen gjør at det interne nettet ikke kan nås fra utsiden. For å monitorere gjestenettverket anskaffet Domstoladministrasjonen Aruba Airwave, og nå helt nylig har de anskaffet Aruba Clearpass for å bedre nettverksoversikten og adgangskontrollen på det interne nettet. Disse to tjenestene snakker ikke sammen per dags dato. Ettersom at Clearpass er helt nytt har de ikke fått utforsket alle mulighetene til det nye systemet. Dette kan med andre ord medføre endringer i bruken av systemet samtidig som prosjektet gjennomføres.

Aruba Airwave overvåker svitsjer og aksesspunkter i nettverket. Dette vil si at Domstoladministrasjonen kan følge med ytelse og pålitelighet for disse nodene. Airwave logger også nettverkstrafikken som går i gjestenettet, med typen nettverkstrafikk og destinasjonen til trafikken for hver enkelt bruker. I dagens oppsett monitorerer Airwave totalt 232 switcher, av disse er det 184 Aruba switcher, og det er 48 cisco switcher.

Dersom noen kobler seg på det interne nettet sendes det en DHCP-forespørsel som fanges opp av Aruba Clearpass. Clearpass logger hvilke enheter som kobler seg til, og hva slags autentisering som er brukt. Per dags dato er det ikke mulig å behandle disse enhetene ved hjelp av Clearpass men dette vil i nær fremtid endre seg. Regler er satt opp for autentisering, men er ikke blitt implementert. Automatisk behandling av disse enhetene ved hjelp av Clearpass er planlagt implementert i løpet av prosjektperioden, men dette er ikke en del av prosjektets omfang.

For å administrere klientmaskinene i domenet til domstolene i Norge benyttes System Center Configuration Manager. SCCM brukes for å oppdatere klientmaskiner, deployere operativsystem til nye maskiner, sette sikkerhetsregler for maskiner, og overordnet ha oversikt over enhetene i domenet. Domstoladministrasjonen administrer ca. 3 000 klienter som er fordelt rundt om i de ulike domstolene i Norge. Det benyttes en egen server for tynnklienter, som hovedsakelig utfører utrulling av konfigurasjonsfiler til tynnklientene. Fordelingen mellom tykk- og tynnklienter er ca. 50/50.

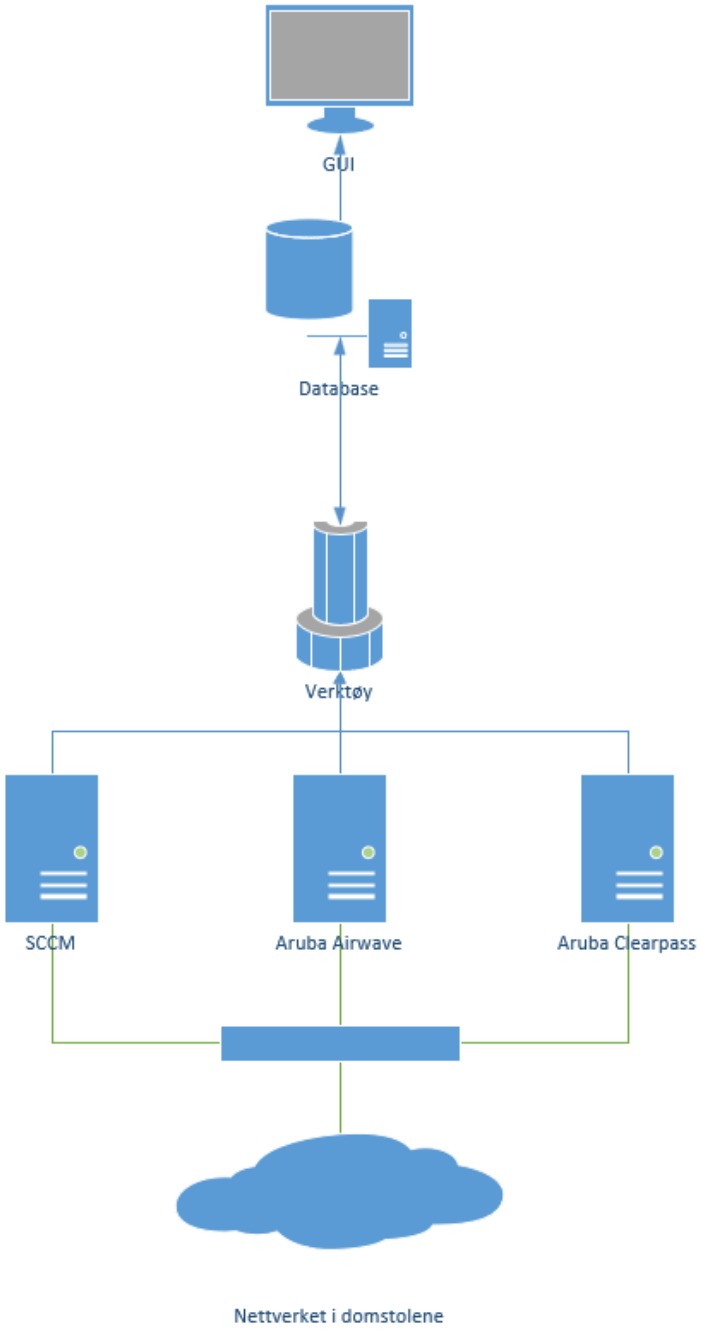
Domstoladministrasjonen har ansatt en hovedansvarlig for driften av SCCM, og en hovedansvarlig for driften av nettverk.

2.2 Behov

Oppgavestiller har behov for:

- En enkel og effektiv måte å få oversikt over samlet data fra SCCM, Clearpass og Airwave.
- Automatisk rapportering av eventuelle trusler oppdaget i nettverket.

Figuren under viser relasjonen mellom nettverket, tjenestene som skal bli brukt, verktøyet, databaseløsningen og visualiseringsløsningen som oppgavestiller ønsker.



Figur 1: Visualisering av design

3. Avgrensning

Kapittelet beskriver ønskene oppgavestiller har til prosjektet.

3.1 Verktøy for konsolidering og analyse av nodeinformasjon

Oppgavestiller ønsker et verktøy som konsoliderer og analyserer nodeinformasjon fra SCCM, Airwave og Clearpass. Verktøyet skal hente ut informasjon som allerede ligger lagret på disse tjenestene, utføre analyser, og legge inn nodeinformasjonen og resultater fra analysen i en Azure database. Verktøyet skal *ikke* behandle eller administrere systemene informasjonen hentes fra, og verktøyet skal *ikke* utføre tiltak dersom trusler blir funnet i analysen. Verktøyet skal fungere automatisk, uten input fra brukere, og skal kunne utføre innhenting, analyse, og utsending av informasjonen på planlagte tidspunkt.

3.2 Databaseløsning

Oppgavestiller ønsker en databaseløsning slik at data blir lagret på en måte som er fleksibel med tanke på fremtidige utvidelser. Databaseløsningen skal være en SQL-database. Data skal bli lagret her etter den er analysert, og skal hentes ut av visualiseringsløsningen.

3.2 Visualiseringsløsning

Oppgavestiller ønsker en visualiseringsløsning for å kunne lese informasjonen som verktøyet finner. Løsningen skal kunne vise fram all informasjonen som er lagret i databasen. Visualiseringsløsningen skal kunne nås over Domstolenes interne nettverk, og gi den informasjonen som er nødvendig for brukeren. Visualiseringsløsningen skal gjøre det mulig å visualisere informasjonen med grafer og figurer, uten store mengder brukerinput.

4. Krav til løsningen

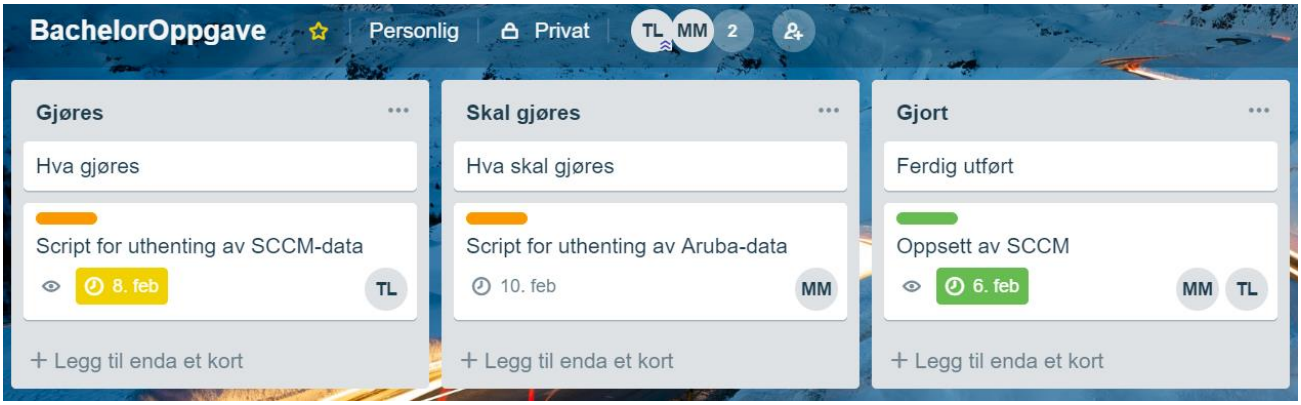
- Verktøyet skal utvikles ved hjelp av PowerShell-script.
- Verktøyet skal benytte seg av en SQL-database i Domstoladministrasjonens Azure Stack.
- Verktøyet må være utviklet slik at enkeltdeler av verktøyet kan brukes i isolasjon.
- Visualiseringsløsningen skal utvikles ved hjelp av Javascript og HTML.
- Løsningen skal være godt dokumentert slik at det blir enkelt å videreutvikle løsningen.

5. Strategi og metode

For å oppnå best mulig resultat av prosjektet er prosjektgruppen avhengig av god organisering og kommunikasjon. Dette kapittelet beskriver hvordan prosjektgruppen ønsker å benytte seg av Trello og GitHub for å oppnå dette.

5.1 Trello

Trello er et samarbeidsverktøy som prosjektgruppen bruker til å vise hva som gjøres, skal gjøres, er gjort og hvem som gjør hva.



Figur 2: Trello

Prosjektgruppen benytter Trello som en tavle med lister og klistrelapper. Listene prosjektgruppen bruker, som vises i eksempelbildet over, er "Gjøres", "Skal gjøres", og "gjort". I hver liste legges det til "kort" som tilsvarer klistrelapper hvis man skulle gjort dette med en virkelig tavle. Disse klistrelappene inneholder en aktivitet, fargekode for å vise sammenheng mellom aktiviteter, dato for når gjøremålet skal være ferdig og hvem som skal delta på aktiviteten. Hver klistrelapp plasseres ut ifra hvor aktiviteten befinner seg i arbeidsprosessen, og flyttes etter hvert som den endrer status.

Dette verktøyet gjør at prosjektgruppen kan se tavlen uansett hvor de befinner seg ettersom at man har en virtuell tavle istedenfor en fysisk tavle på kontoret. Det er også mulig å invitere veileder, oppgavestiller og andre interessenter som skulle ønske å følge med på prosjektets fremgang.

5.2 GitHub

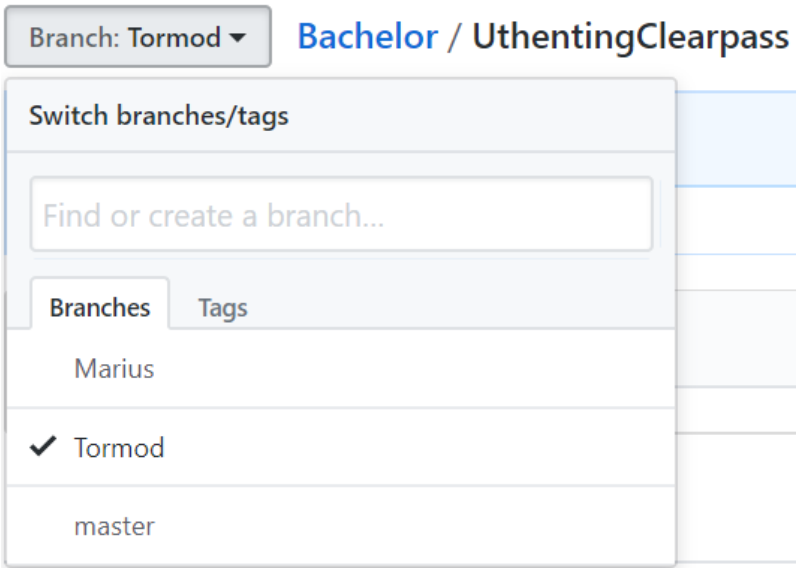
GitHub vil bli benyttet for versjonskontroll og samskriving av script til verktøyet. Prosjektgruppen utnytter da en fleksibel plattform hvor gruppemedlemmene har tilgang til scriptene uansett hvor de måtte befinne seg.

Med tanke på sikkerhet så går prosjektgruppen inn for å benytte Student Developer Pack levert av GitHub Education (GitHub Education, 2019). Dette gir prosjektgruppen to år med gratis tilgang på private GitHub repository. Prosjektgruppen kan så invitere de partene som skal ha tilgang til dette repositoryet.

Prosjektgruppen valgte GitHub pga tidligere erfaringer, og funksjonaliteten til samarbeidsverktøyet vil bli benyttet på følgende måte:

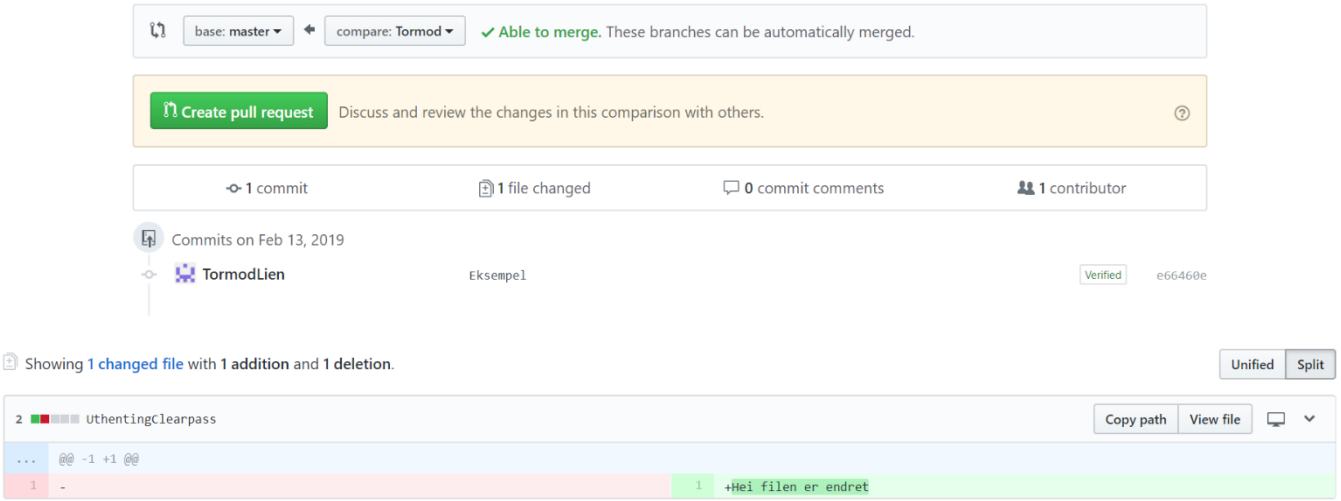
Branch benyttes for å skille mellom master-branch og de branchene som prosjektgruppen arbeider på. Dette vil si at hvert gruppemedlem har sin egen branch som endringer blir utført på, før det så gjøres forespørsel om å innføre endringene mot master-branch. En branch er altså en kopi av master-branch. I bildet under vises oppsettet til prosjektgruppen hvor master-branch tilsvarer siste samling av endringer. Tormod og Marius tilsvarer midlertidige filer, hvor endringer blir utført, som vil bli

merget(slått sammen) med master-branch. På denne måten blir det ryddig og god oversikt over fil-versjoner og loggføring av arbeid.



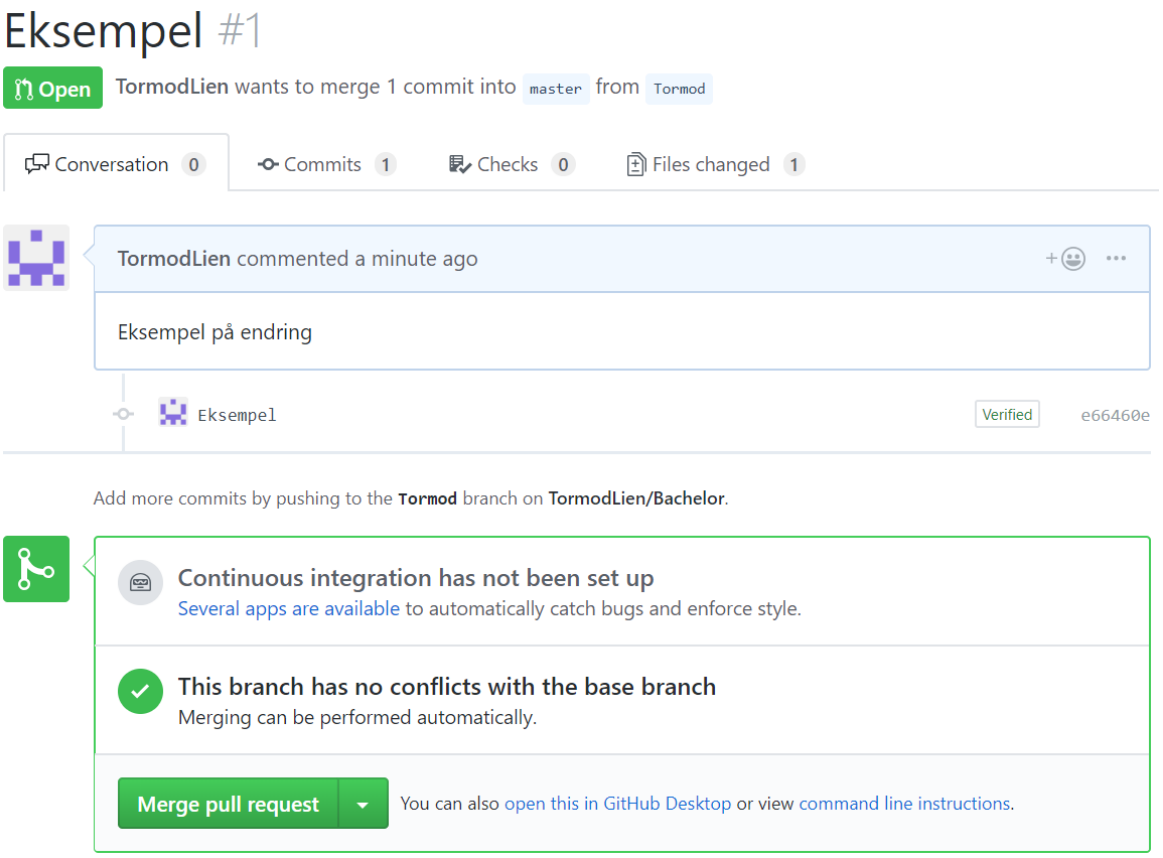
Figur 3: GitHub Branch

Commit benyttes ved at en endring er gjort på en branch, og disse endringene er ønsket å innføre på master-branch. Dette kan være alt fra endrede, slettede eller nye filer i repositoriet. Når en "Commit" er utført, så vil de utførte endringene vises som i bildet under:



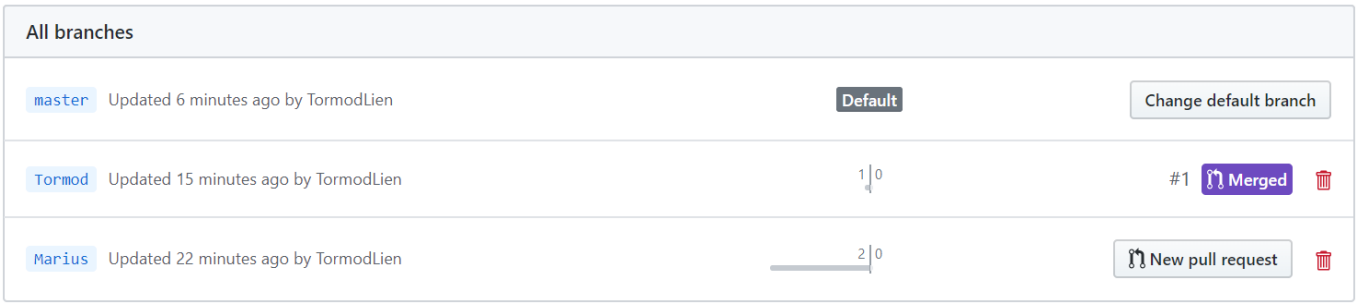
Figur 4: GitHub Commit

Push/pull benyttes for å synkronisere de ulike branchene. Her er det også muligheter for å diskutere disse endringsforslagene før branchen "merges"(slå sammen) med master-branch. I større prosjekter kan det være lurt å ha en prosjektleder som tar seg av sammenslåingen, men i dette prosjektet har alle medlemmene i prosjektgruppen administrator-rettigheter. Bildet under viser hvordan det ser ut når prosjektgruppen pusher endringer til en branch og prøver å merge dette med master-branch.



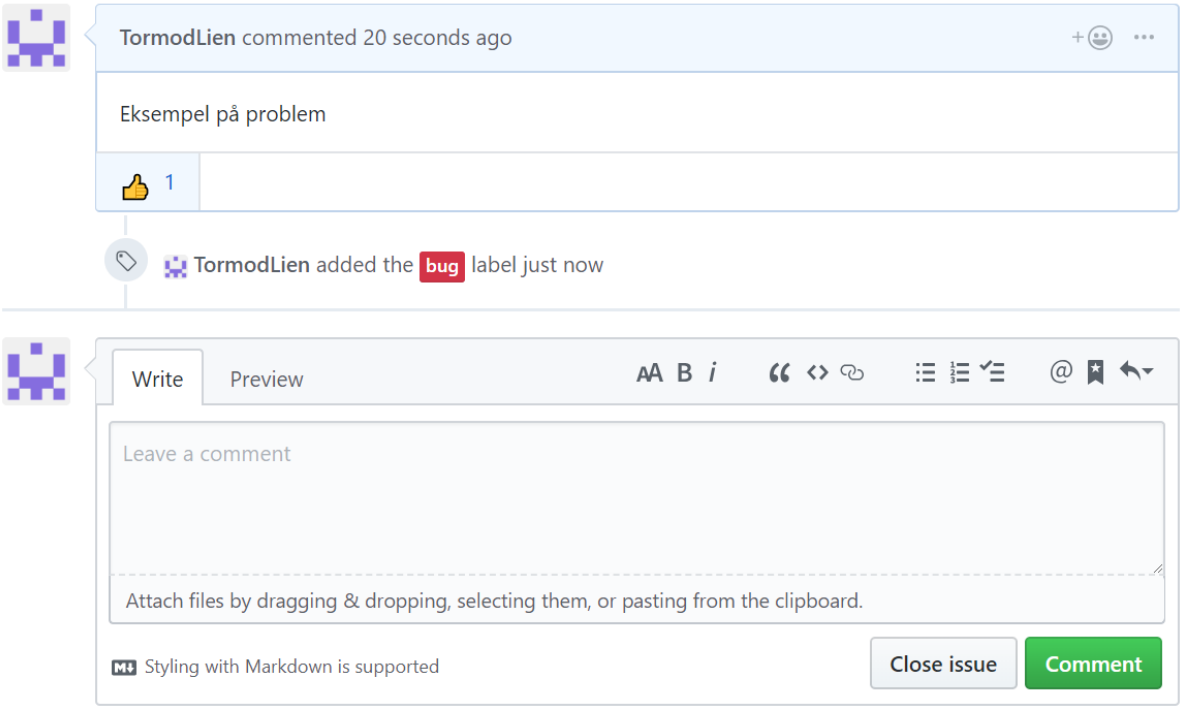
Figur 5: GitHub Push/pull

Når branchen er merget med master-branch ser det ut som i bildet under. Her er "Tormod" oppdatert mot master. Marius er ikke oppdatert, og må benytte seg av "Pull request" for å synkronisere seg opp mot master-branch. Dette er veldig viktig slik at prosjektgruppen alltid arbeider på oppdaterte branches.



Figur 6: Pull request

Issues benyttes av prosjektgruppen for å informere om problemer som oppstår. Det som rapporteres her er de problemene som ikke kan løses med en gang. På denne måten blir det også enklere for gruppemedlemmene å hjelpe hverandre. Bildet under viser hvordan det ser ut når en feil er blitt rapportert. Alle problemer som blir rapportert skal ha en beskrivelse av problemet i tillegg til en merkeknagg som gjør det enklere å kategorisere de ulike problemene.



Figur 7: GitHub Issues

5.2.1 Standarder for prosjektet.

Prosjektgruppen har satt følgende standarder til bruk av GitHub:

- Utfør alltid pull request fra master-branch før man endrer på scripts.
- Alle endringer skal utføres i egen branch.
- Alle endringer i egen branch skal testes før det merges med master-branch.
- Alle endringer skal ha en god beskrivelse av hva som er gjort.

6. Valg av tekniske løsninger

Kapittelet beskriver de tekniske løsningene som prosjektgruppen benytter seg av for å løse problemstillingen.

6.1 Microsoft PowerShell

PowerShell er et kommandovindu(skall) og OOP-språk (Object-oriented Programming). Det er en del av .NET rammeverket. Grunnideen med PowerShell var at alle Microsoft-produkters administrator-funksjonalitet skulle kunne gjøres gjennom et kommandoskall. De ulike produktene kommer fortsatt med GUI-basert admin-funksjonalitet, men disse har ofte begrensninger som man ikke har dersom man benytter kommandoskallet. I tillegg til administrasjon av Microsoft-produkter kan PowerShell brukes som et objektorientert scriptspråk. Prosjektgruppen har som mål å bruke PowerShell som språk for å hente ut informasjon fra SCCM, ClearPass og AirWave, legge inn informasjonen i en SQL-datbase på Domstoladministrasjonens Azure Stack, og analysere informasjonen som blir funnet.

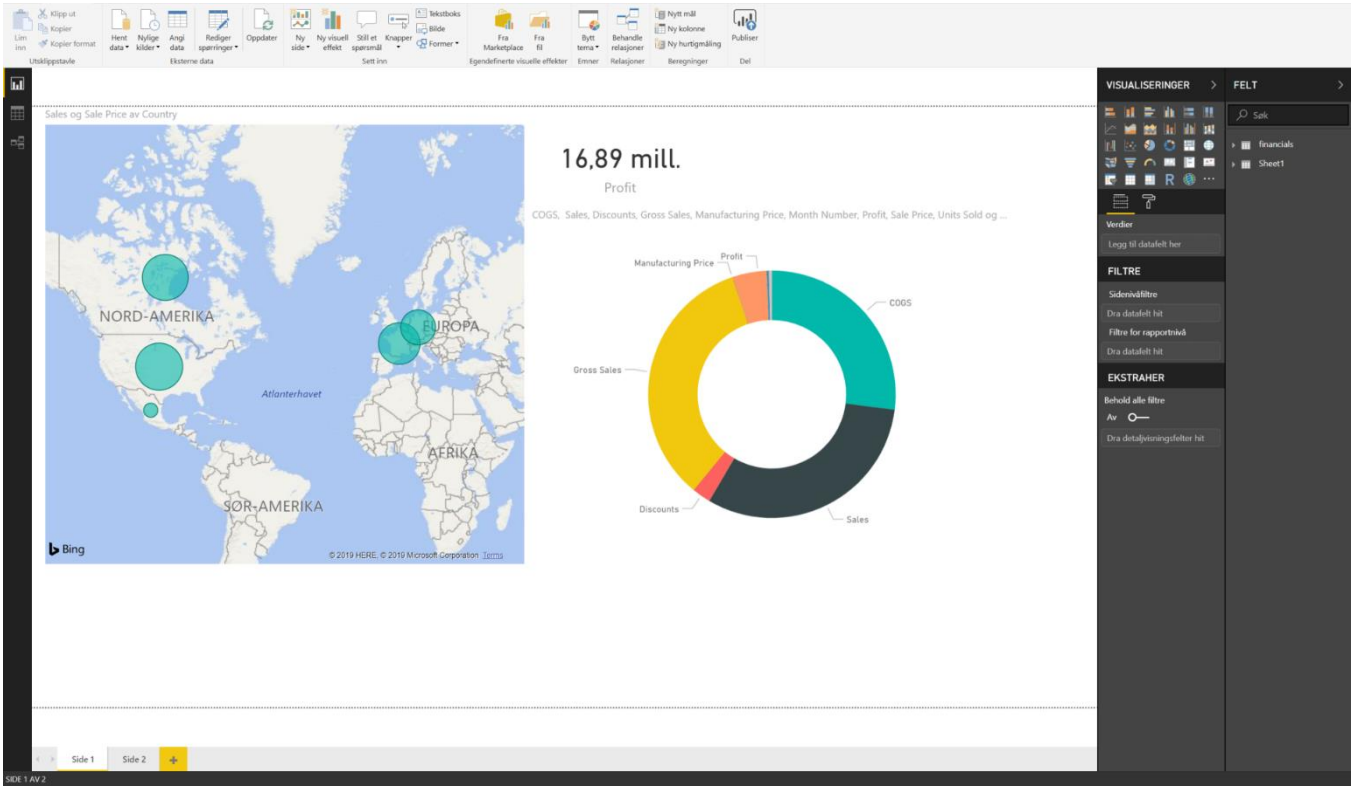
6.2 Azure Stack SQL

Azure Stack er en egen autonom sky, helt eller delvis frakoblet fra internett og offentlig sky. En SQL-server legges i denne lokale skyen slik at data ikke blir lagret utenfor landets grenser. På denne måten Domstoladministrasjonen selv kontrollere adgangen til egen data. Domstoladministrasjonen har allerede en Azure Stack, som blir driftet av Evry og er lokalisert på Gjøvik, hvor de har eksisterende oppsett med oppkobling mot databaseløsning gjennom en gateway. Prosjektgruppen vil benytte seg av dette eksisterende oppsettet. Ved å benytte Azure Stack kan også databasen flyttes opp i skyen dersom det skulle bli ønskelig i fremtiden.

6.3 Power BI

Miscrosoft Power BI er programvare for visualisering og analyse av data. Det kan ta for seg data fra hundrevis av on-premise og skybaserte kilder, for eksempel Dynamics 365, Saleforce, Azure SQL DB, Excel og SharePoint. Videre er det enkelt å visualisere denne dataen i form av grafer og tabeller. Dette gjør at prosjektgruppen kan benytte seg av denne applikasjonen for å visualisere dataen som er samlet fra SCCM, Aruba Airwave & Clearpass. Bildet under viser hvordan Dashboard kan tilpasses ved valg av data og visualiseringmetode. Selve rapporten som eksporteres viser kun det som er

rammet inn på det hvite arket.



Figur 8: Power BI

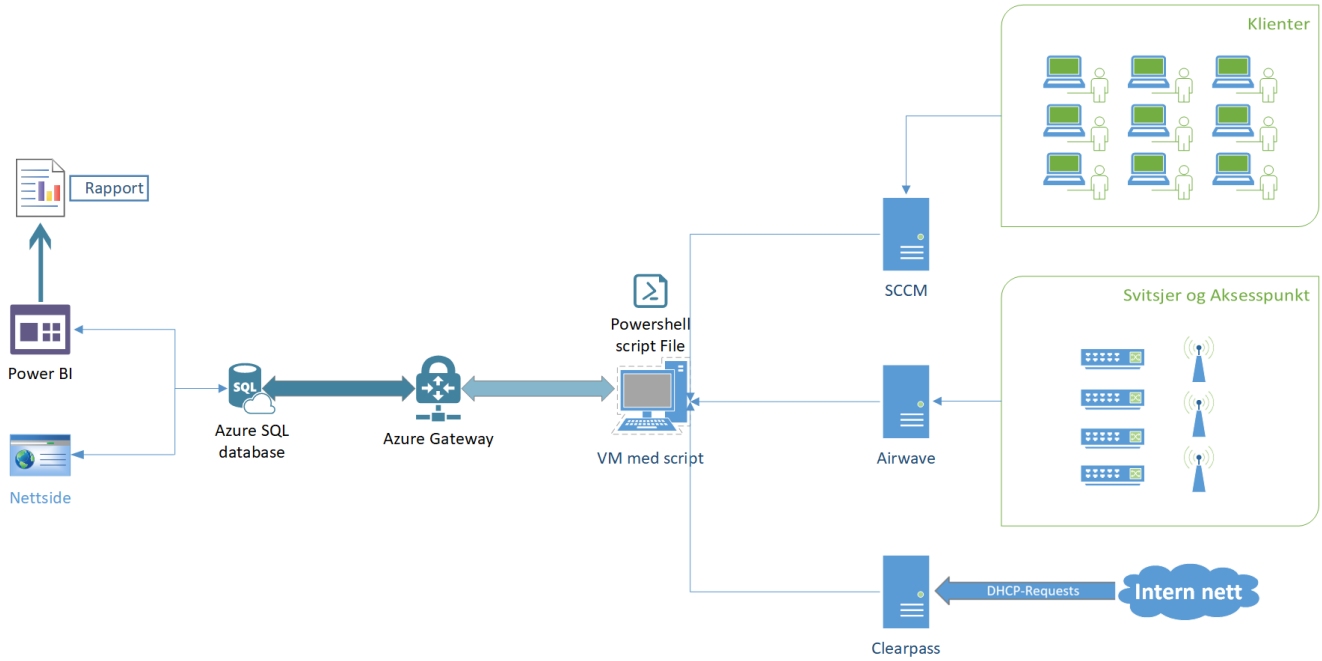
6.3 Nettside

Selv om PowerBI er den mest effektive løsningen for å visualisere informasjonen, ønsker Domstoladministrasjonen at prosjektgruppen utvikler en nettside som kan brukes for å visualisere informasjonen som er lagret i databasen. Ønsket er uttrykt da PowerBI ikke nødvendigvis blir implementert i Domstoladministrasjonen, og om det blir implementert kan dette ta sted lang tid etter prosjektets slutt. Noen ansatte vil ikke ha behov for å benytte seg av power bi, eller har ikke tilgang til det, og da er en nettside ønskelig. Nettsiden skal kunne hente informasjonen som ligger i databasen, og skal gi brukerne en enklere måte å se informasjonen enn å hente det direkte fra databasen.

For å lage nettsiden benyttes HTML og CSS for utforming av nettsiden, og PHP for å hente informasjon fra databasen. PHP er valgt ettersom prosjektgruppen tidligere har erfaring med PHP for utvikling av dynamiske nettsider.

7. Løsningsbeskrivelse

Kapittelet beskriver hvordan de utvalgte tjenestene benyttes til å implementere prosjektgruppens verktøy.

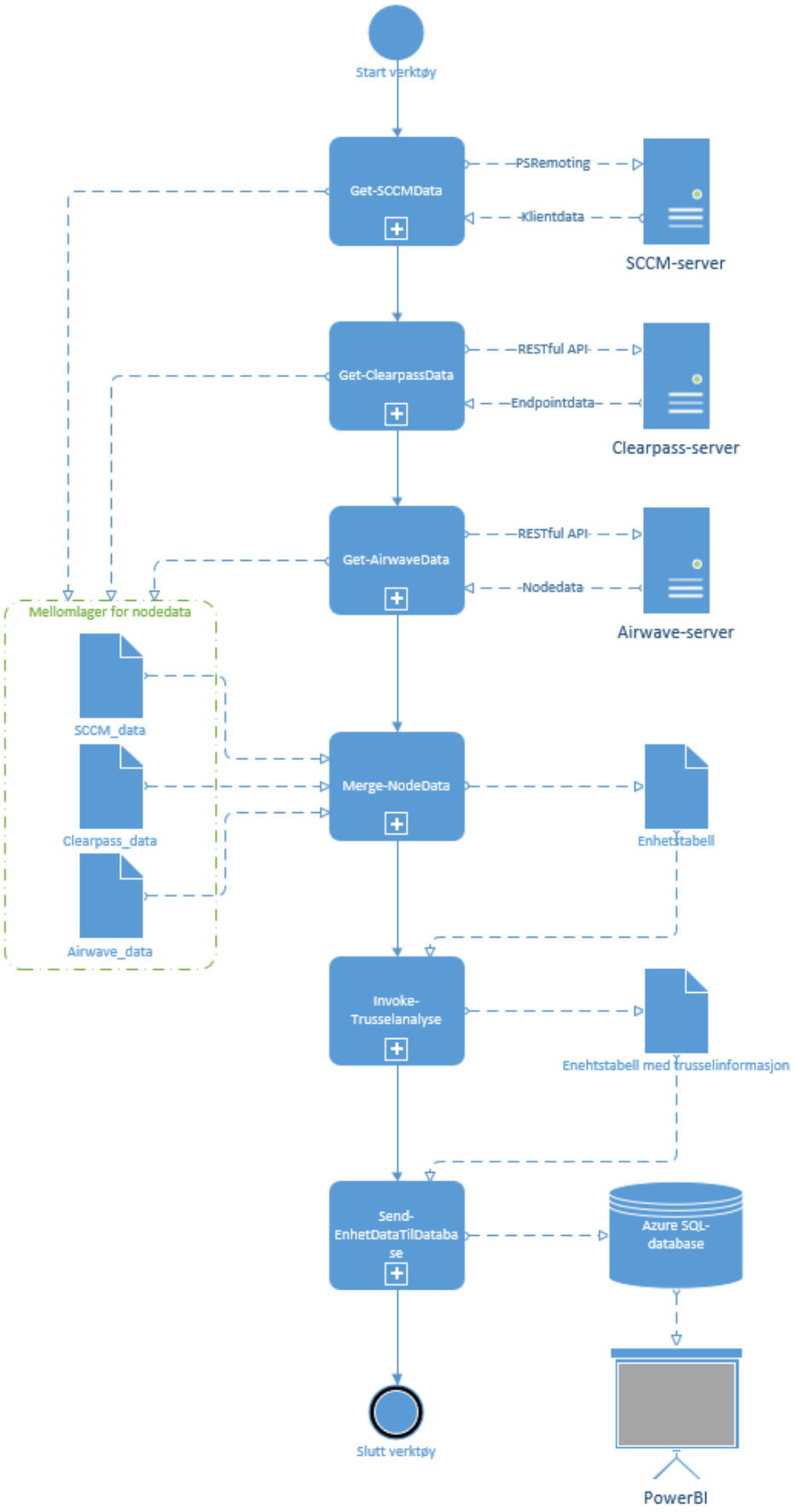


Figur 9: Løsningsbeskrivelse

Bildet over viser hvordan prosjektgruppen ser for seg løsningen. SCCM har data fra klientene rundt om i Norges domstoler. Airwave monitorerer svitsjer og aksesspunkter til gjestenettet. Clearpass loggfører alle DHCP-Requests som gjøres på det interne nettet. Verktøyet, som består av PowerShell script, vil ligge på en maskin som har tilgang til disse tjenestene. Scriptet vil her hente ut relevant data fra disse tjenestene før deretter å konsolidere dataen. Konsolidert data blir da overført gjennom en gateway til Azure Stack og SQL-databasen som befinner seg der. Deretter vil Domstoladministrasjonen kunne benytte seg av Power BI eller nettsiden til å visualisere dataen som befinner seg i databasen.

7.1 Datainnhenting og databehandling

For innhenting og behandling av informasjonen fra SCCM, Airwave og Clearpass benyttes Microsoft PowerShell. For å hente informasjon fra SCCM benytter scriptet seg av PowerShell Remoting, der scriptet kobler seg opp mot SCCM-tjeneren og henter ut informasjonen. For å hente informasjon fra Aruba-tjenestene benytter scriptet seg av RESTful-APIer innebygd i tjenestene. For å sikre modularitet i scriptet er hver funksjon frittstående, og kalles der de er nødvendige.



Figur 10: Dataflyt

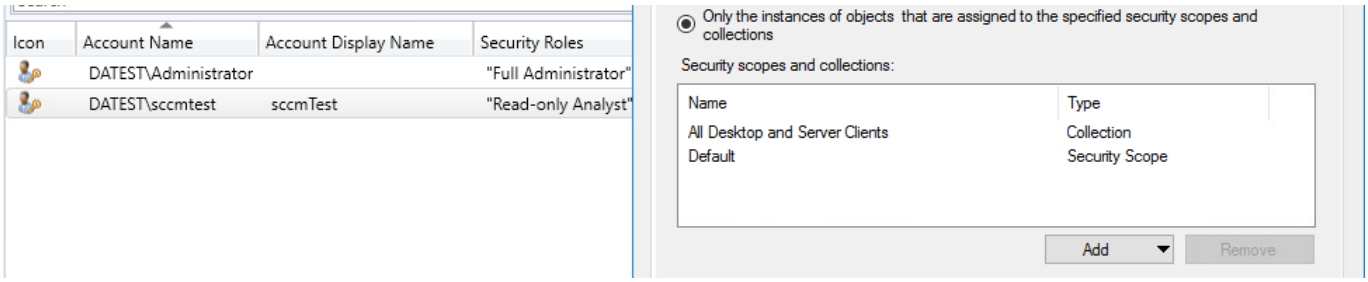
Bildet over viser den overordnede flyten i verktøyet. Først hentes all informasjonen ut med uthentingsfunksjonene for tjenestene, og informasjonen som blir hentet legges i et mellomlager. Deretter behandler sammenslåingsfunksjonen informasjonen som ligger i mellomlageret, og lager en frittstående enhetstabell med all informasjonen som er hentet. Enhetstabellen blir deretter brukt i trusselanalysen, som finner mulige trusler basert på informasjonen i tabellen, og legger inn et merke på enhetene i tabellen dersom analysen fant en trussel. Til slutt brukes et script som sender informasjonen i enhetstabellen med trusselinformasjon til databasen.

7.1.1 Datainnhenting

Før informasjonen kan analyseres må den bli hentet fra de tre forskjellige tjenestene som benyttes. Ettersom informasjonen fra de tre tjenestene er formatert forskjellig, og det ikke er én metode for å hente ut informasjon fra alle tre, benytter verktøyet en uthentingsfunksjon per tjeneste.

7.1.1.1 SCCM

SCCM har en oversikt over de enhetene som er en del av domenet. For å hente ut denne informasjonen benytter vi oss av en bruker med sikkerhetsrollen "Read-only Analyst". Denne servicebrukeren har dermed ikke rettigheter til å endre på noe i SCCM, men kan hente ut informasjon. For å begrense hva denne brukeren ser så er kun relevante "devicecollections" valgt som synlig. Denne sikkerhetstilpasningen er viktig å utføre ettersom det ikke er ønskelig at denne brukeren kan endre på dagens system.



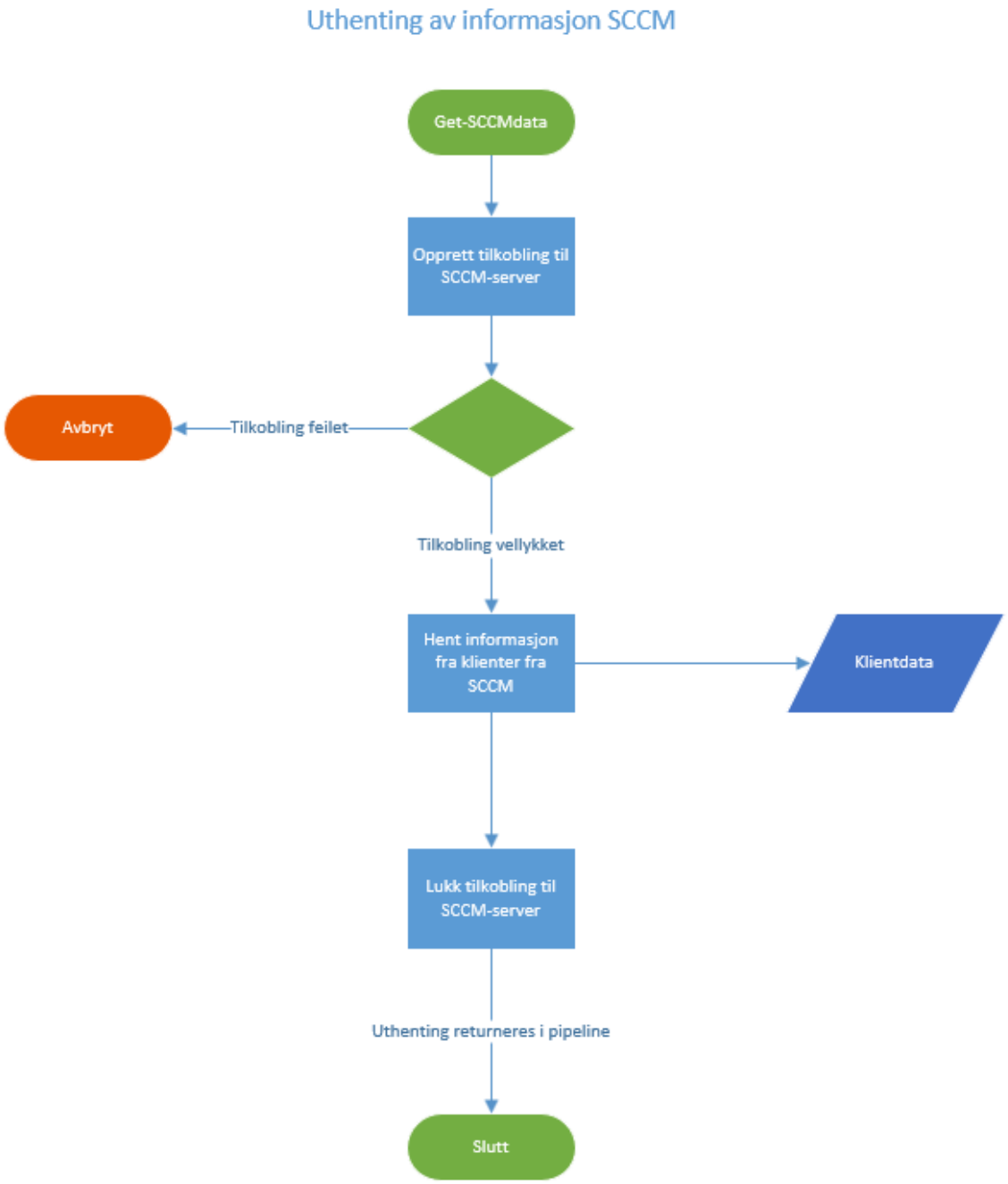
Figur 11: SCCM Read-only Analyst

Denne brukeren blir da benyttet for å fjernkoble seg inn på SCCM-serveren, uavhengig av hvor verktøyet kjøres, og deretter kjøre script for uthenting av klientinformasjon.

Uthenting av informasjon fra SCCM vil se ut som følger for hver enhet i domenet:

```
SmsProviderObjectPath          : SMS_R_System.ResourceId=16777224
IPAddresses                    : {10.0.0.28, fe80::e8be:ebfc:3b6e:7658}
LastLogonTimestamp             : 28.02.2019 12.44.06
LastLogonUserName              : sccmtest
MACAddresses                   : {00:50:56:B1:B9:FD}
Name                           : REMOTETOSCCM
OperatingSystemNameandVersion  : Windows 10
ResourceId                     : 16777224
SID                            : S-1-5-21-3051587635-922086871-3517838963-1122
```

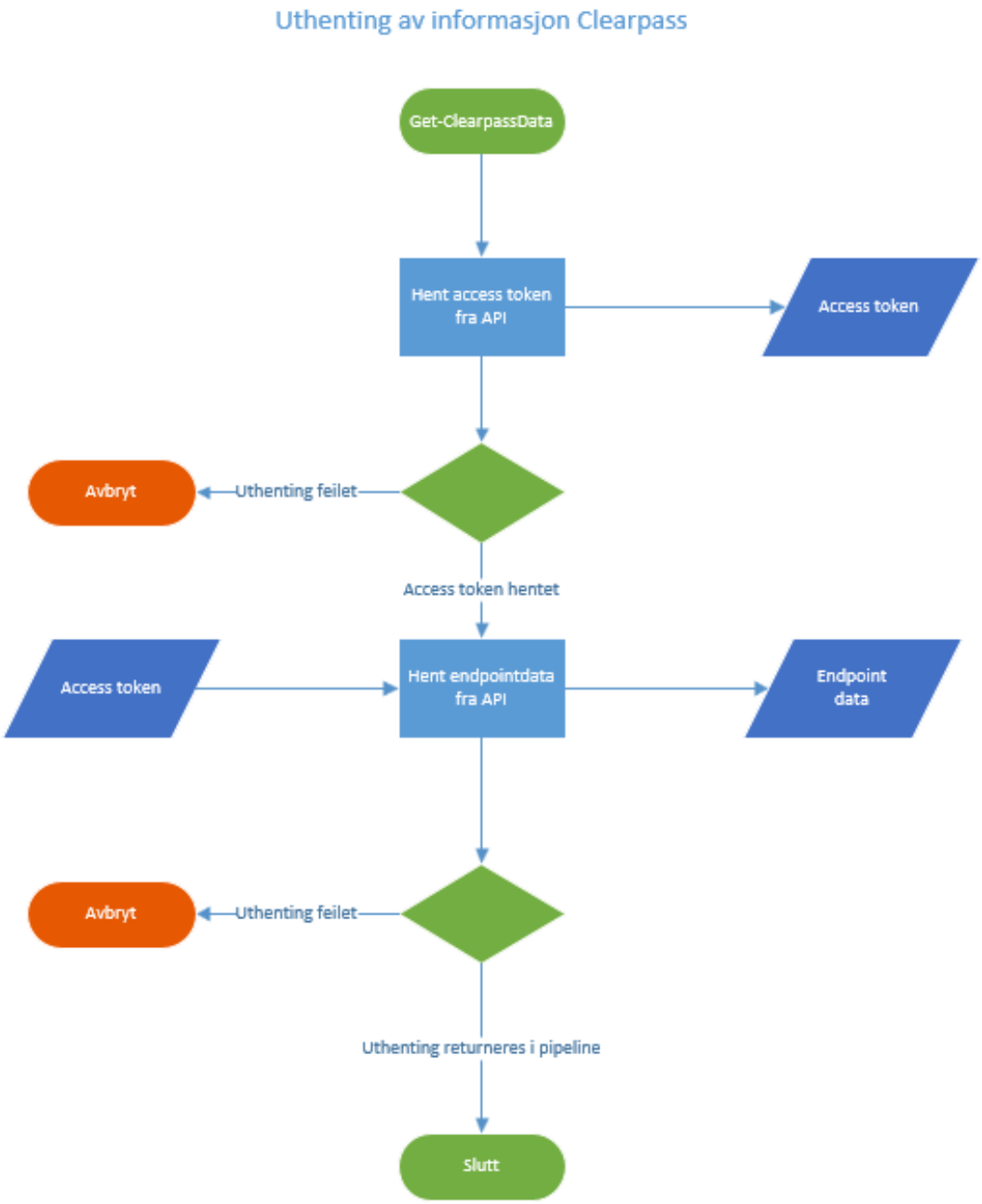
Figur 12: SCCM data



Figur 13: SCCM uthenting

7.1.1.2 Clearpass

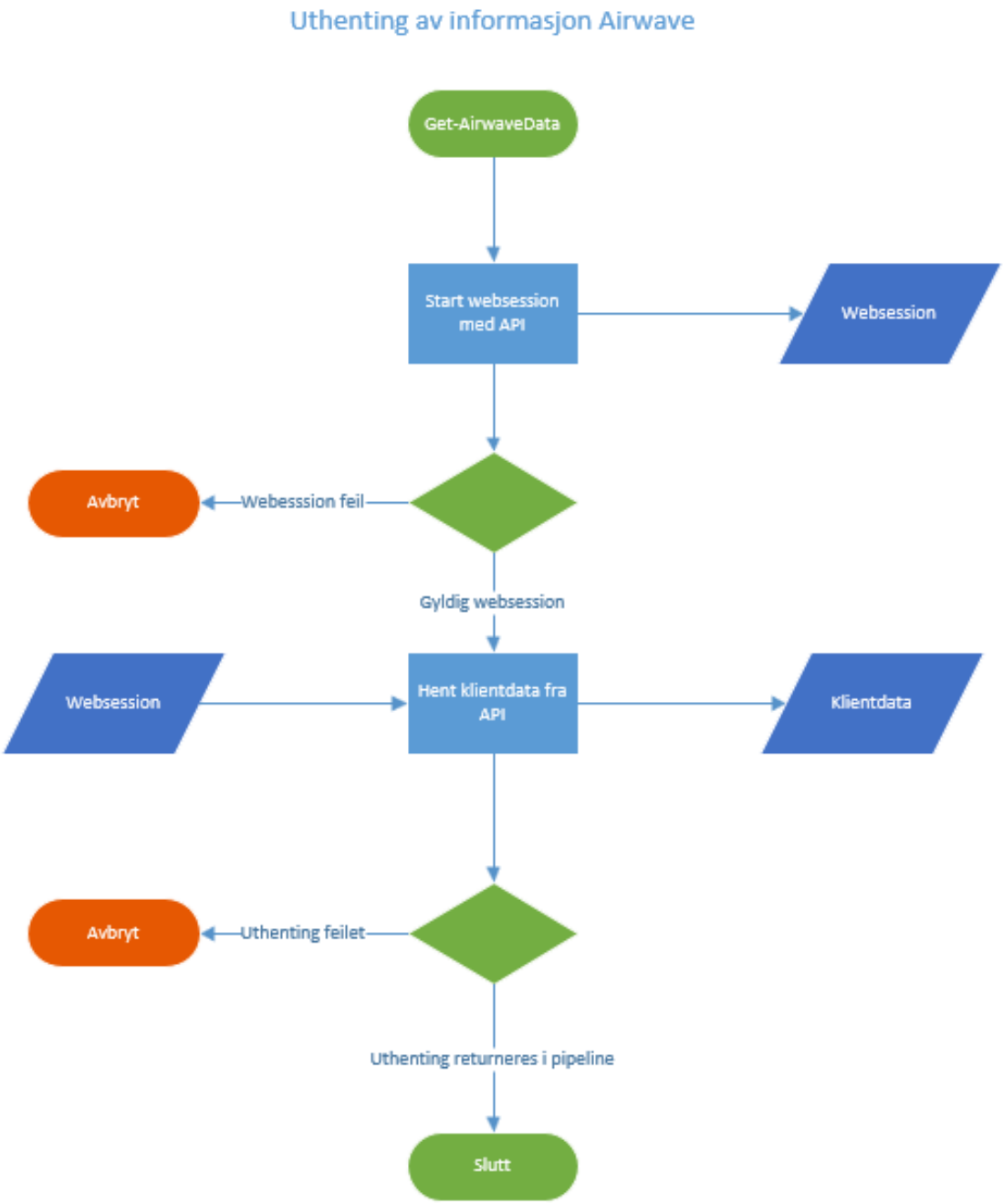
Clearpass fanger opp DHCP-forespørsler som går på internnettet, og lagrer enhetsinformasjon basert på DHCP-forespørselen, som vi henter ut ved hjelp av det innebygde RESTful APIet. Det er nødvendig å sette opp en regel i Clearpass som automatisk legger inn informasjonen vi er ute etter i attributtlisten til hver enhet før man kan eksportere informasjonen med API. Scriptet henter deretter en access token fra APIet, og benytter metoden GET endpoints for å hente ut informasjon på alle enheter. Denne dataen blir deretter returnert i PowerShell-pipelinen.



Figur 14: Clearpass uthenting

7.1.1.3 Airwave

Airwave logger trafikken i nettverket ved å få informasjon fra switchene som styrer datatrafikken i nettverket. For å eksportere denne dataen benyttes den innebygde RESTful APIet i Airwave. Scriptet starter en websession med APIet, og benytter denne sessionen for å hente ut siste rapport av en spesifisert type i XML-format. Denne rapporten blir deretter returnert i PowerShell-pipelinen.



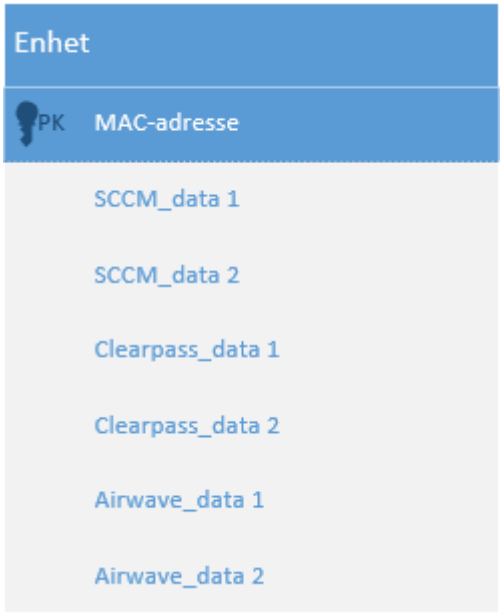
Figur 15: Airwave uthenting

7.1.2 Databehandling

Databehandlingen i verktøyet baserer seg på å først konsolidere informasjonen fra tjenestene til en enhetstabell, analysere enhetene i enhetstabellen, og å sende informasjonen til azure-databasen.

7.1.2.1 Om enhetstabellen

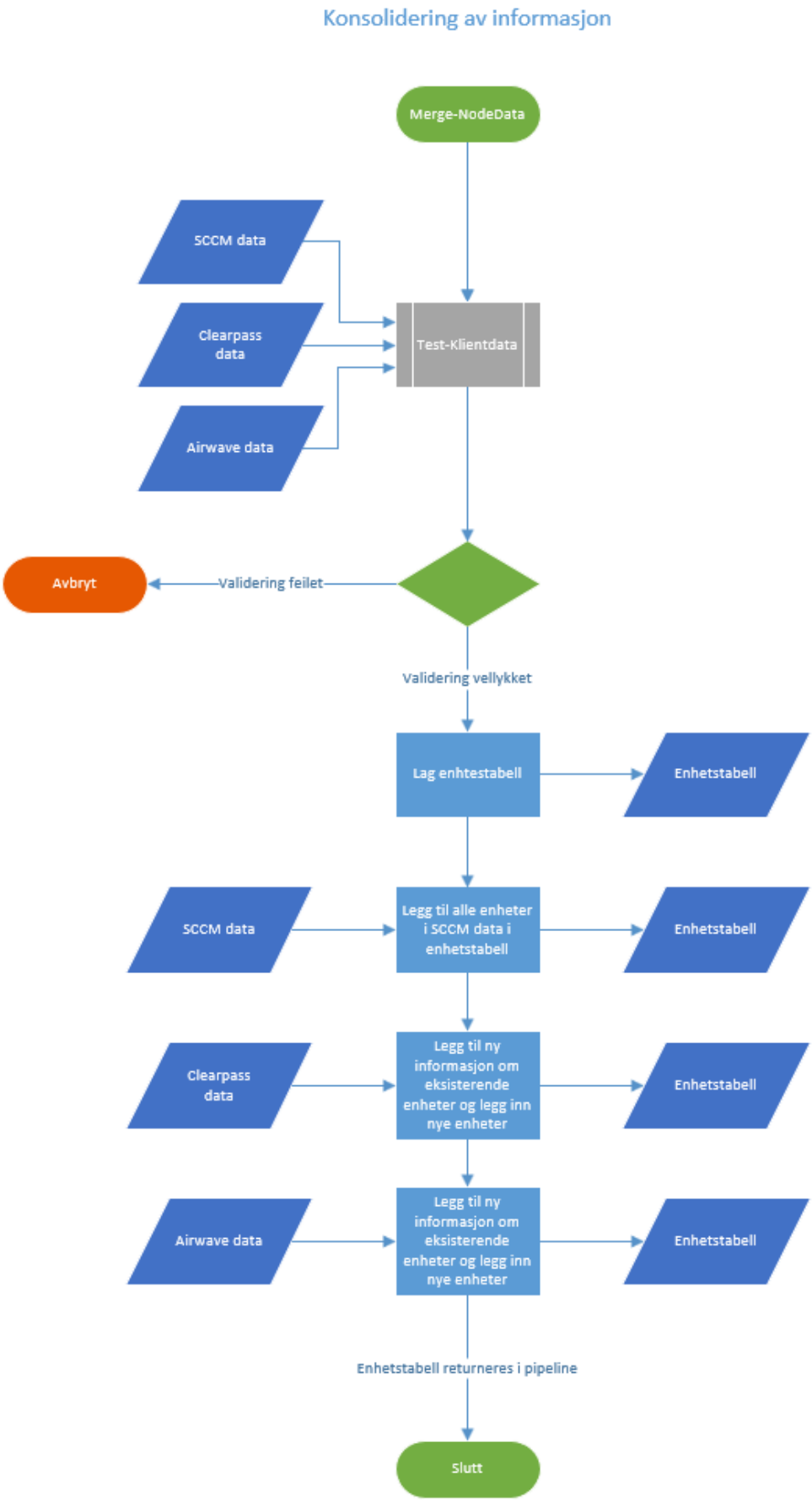
For å simplifisere analysen og innsendingen til databasen, blir rådataen fra tjenestene konsolidert til tabellen prosjektgruppen har valgt å kalle "Enhet". Enhetstabellen er et array som inneholder objekter. Hver enhet i tabellen inneholder all informasjon som er hentet fra tjenestene som angår enheten, og tabellen inneholder alle enhetene som er hentet ut fra tjenestene. Enhetstabellen gjør analysen av informasjonen mye enklere, da man har et entydig format på informasjonen, og man enkelt kan analysere hver enhet sekvensielt. Enhetstabellen kan sammenliknes med en SQL-tabell, og kan visualiseres som en tabell:



Figur 16: Enhetstabell

7.1.2.2 Konsolidering av informasjon

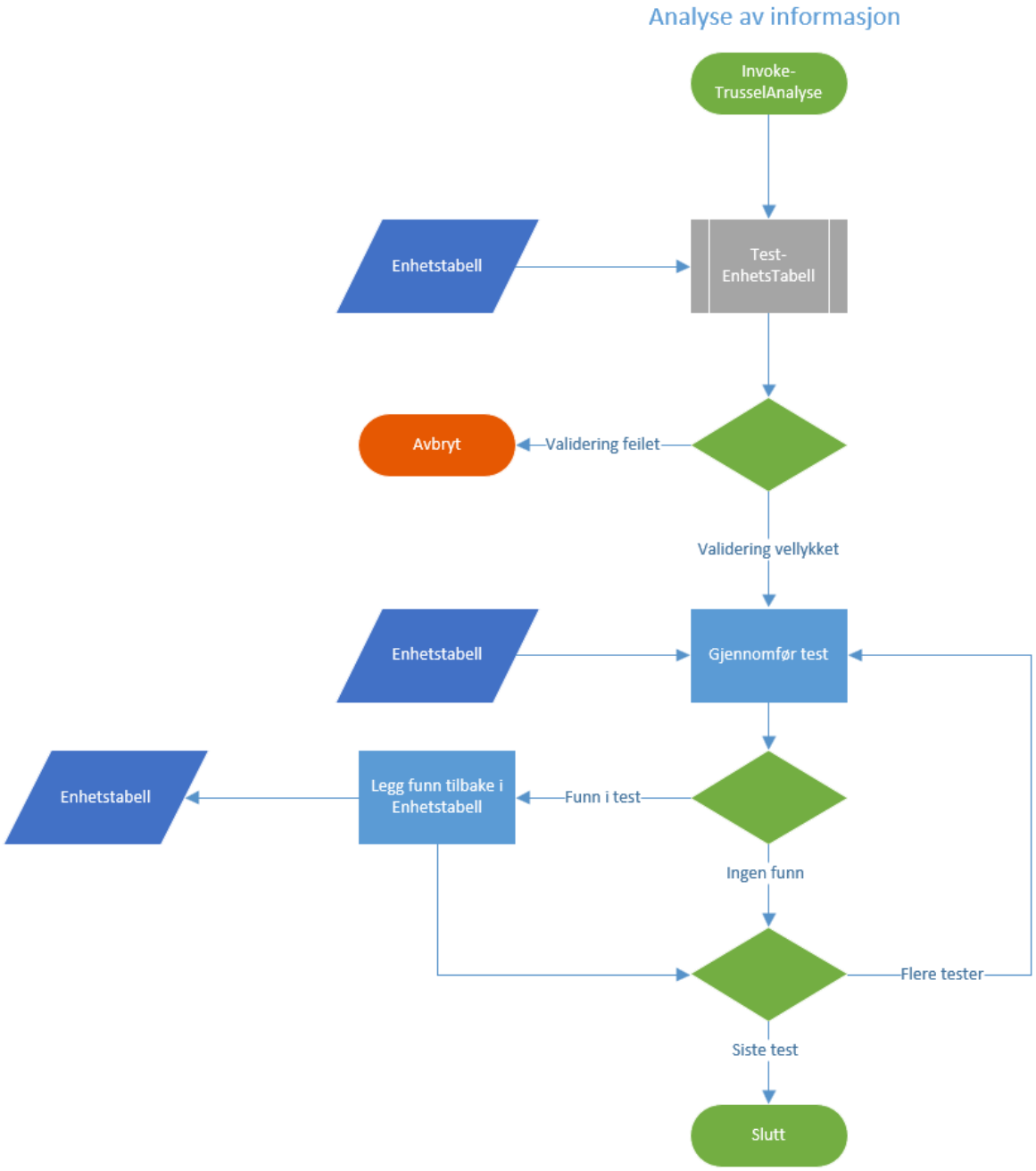
Etter at informasjonen fra de tre tjenestene er hentet, er det nødvendig å konsolidere informasjonen til ett format, slik at den kan analyseres enklere. Konsolideringsfunksjonen starter med å teste informasjonen fra de tre tjenestene, for å se at formatet er riktig slik at enhetstabellen kan bli bygd ut fra den. Deretter initialiseres enhetstabellen, og funksjonen legger inn informasjonen fra tjenestene. Enhetstabellen er et array av PowerShell-objekter. Objektene består av en unik MAC-adresse, og informasjonen fra de forskjellige tjenestene. Dersom informasjon om en enhet ikke finnes fra en eller to av kildene, vil det kun lagres informasjon om at enheten ikke har blitt oppdaget av den tjenesten det gjelder, men all informasjon fra tjenester som fant enheten vil bli lagret som normalt. Funksjonen returnerer enhetstabellen i PowerShell-pipelinen.



Figur 17: Konsolidering av informasjon

7.1.2.3 Analyse av informasjon

Etter at konsolideringsfunksjonen har laget en enhetstabell kan denne sendes videre til analysefunksjonen. Denne funksjonen starter med å validere at enhetstabellen som er sendt inn er gyldig, og begynner deretter å utføre tester på informasjonen. Hver test gjennomføres sekvensielt, og dersom testen finner mulige trusler basert på informasjonen til en enhet i tabellen, legges det inn som et attributt til objektet. Etter at alle testene er gjennomført vil enhetstabellen med trusselinformasjon returneres i PowerShell-pipelinen.

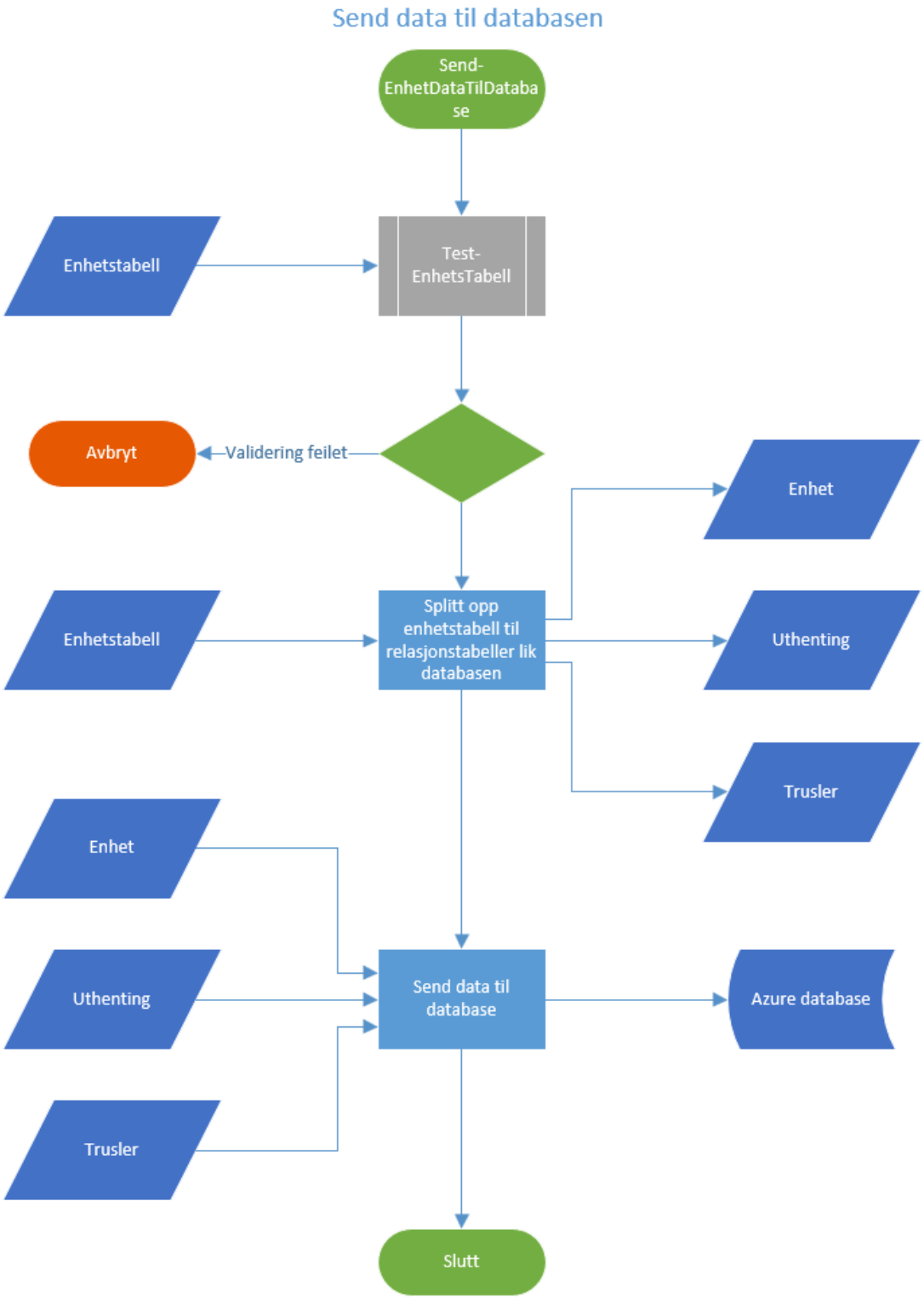


Figur 18: Analyse av informasjon

7.1.2.4 Send analysert informasjon til database

Til slutt vil verktøyet sende informasjonen i enhetstabellen med trusselinformasjon til databasen. For å gjøre dette valideres først enhetstabellen som blir sendt inn til funksjonen, før funksjonen splitter

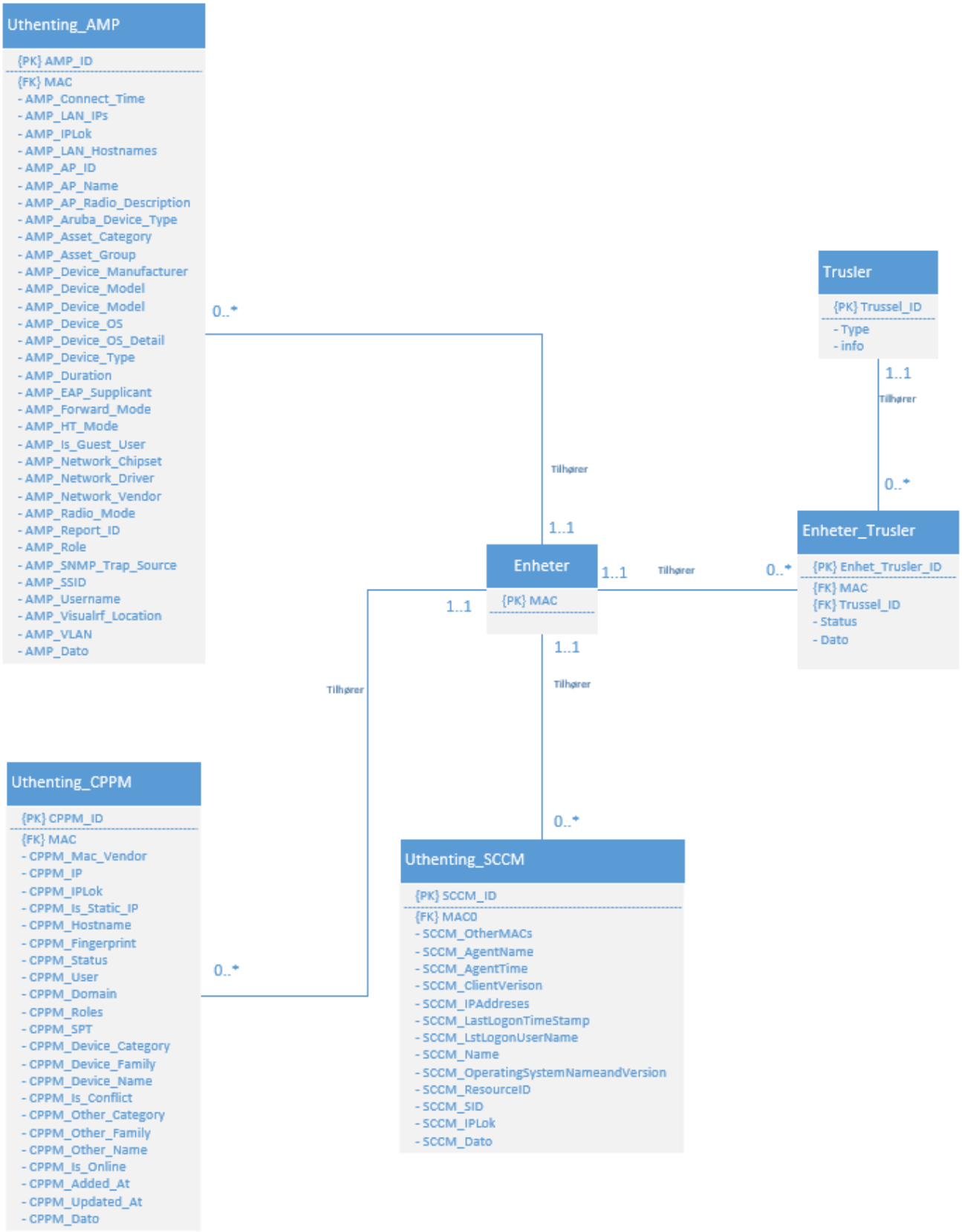
ut informasjonen i enhetstabellen til nye tabeller som samsvarer med tabellene i databasen. Deretter kjører funksjonen informasjonen ut til databasen.



Figur 19: Send data til databasen

7.2 SQL-database i Azure Stack

Prosjektgruppen skal lagre analysert data i en SQL-database med følgende oppsett:



Figur 20: Databasen

Databasen blir satt opp med tabellene og informasjonen som vist i bildet over. Det er egne tabeller for de ulike tjenestene det hentes data fra. Grunnen til dette er at data knyttet til en MAC-Adresse kan være forskjellig mellom de ulike tjenestene. Deretter har vi en samling av alle enheter som

loggføres. I "Trusler" tabellen legges inn de ulike truslene som prosjektgruppen klarer å finne, og disse kobles opp mot tabellen "Enheter_Trusler" for å få en historikk når det gjelder de ulike enhetene og deres trusselbilde. Databasen er satt opp slik at Domstoladministrasjonen i fremtiden kan utvide med flere datakilder.

7.3 PowerBI

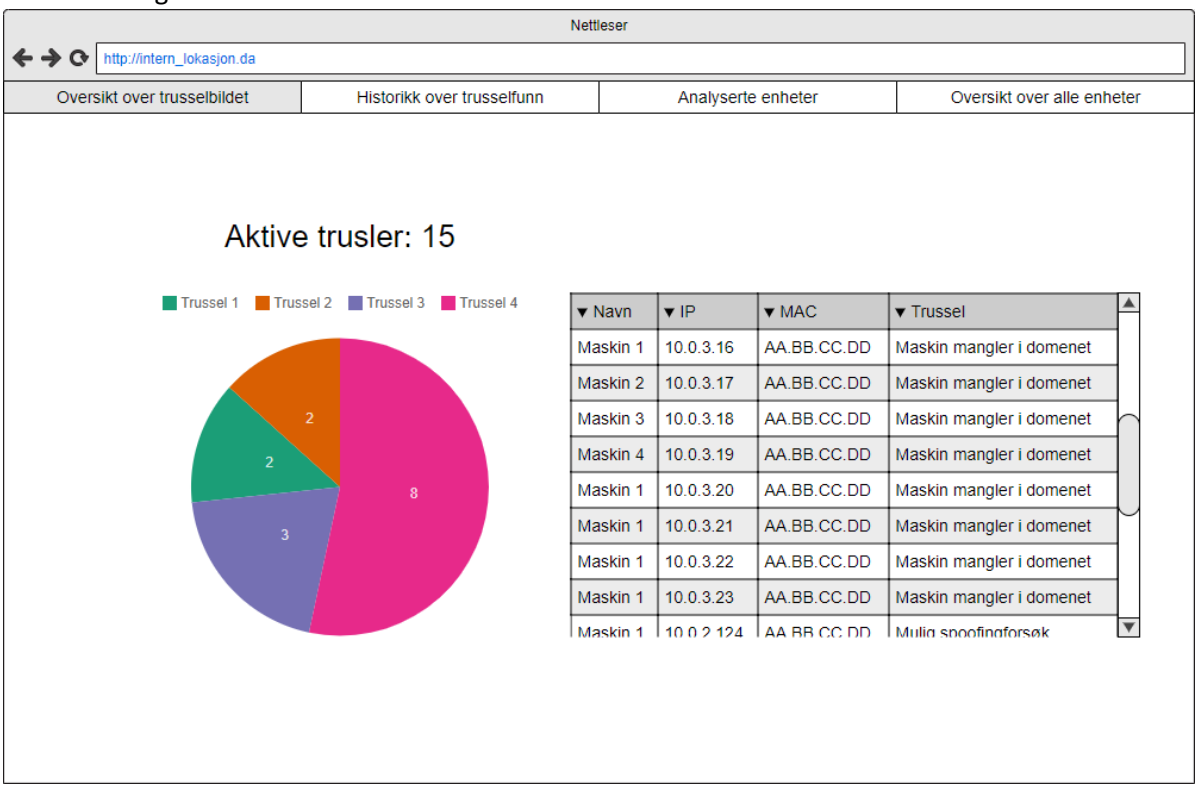
Ettersom PowerBI er en ferdig løsning som leveres av Microsoft, skal prosjektgruppen kun designe rapportmaler og dashboards som gjør det mulig å ta i bruk programmet for visualisering av informasjonen. Prosjektgruppen skal designe de dashboards som blir sett på som nødvendige for å visualisere informasjonen. Dette skal gjøres med følgende planlagte løsninger:

- Dashboard som gir overblikksinformasjon om trusselbildet i nettverket.
- Dashboard som gir historikk over trusselfunn over tid.
- Rapport med oversikt over alle enheter i nettverket.
- Rapport med detaljert informasjon over alle nåværende trusler.

7.4 Nettside for visualisering

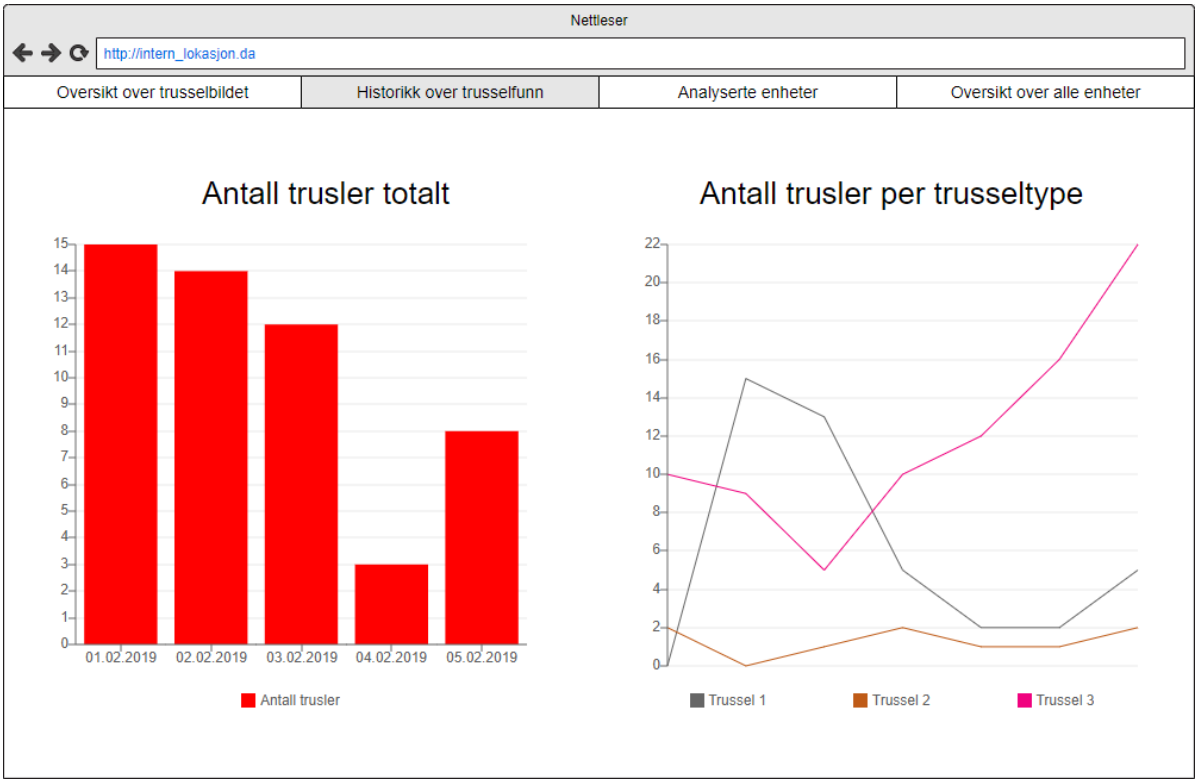
Nettsiden skal inneholde følgende funksjonalitet:

Forside som gir oversikt over trusselbildet:



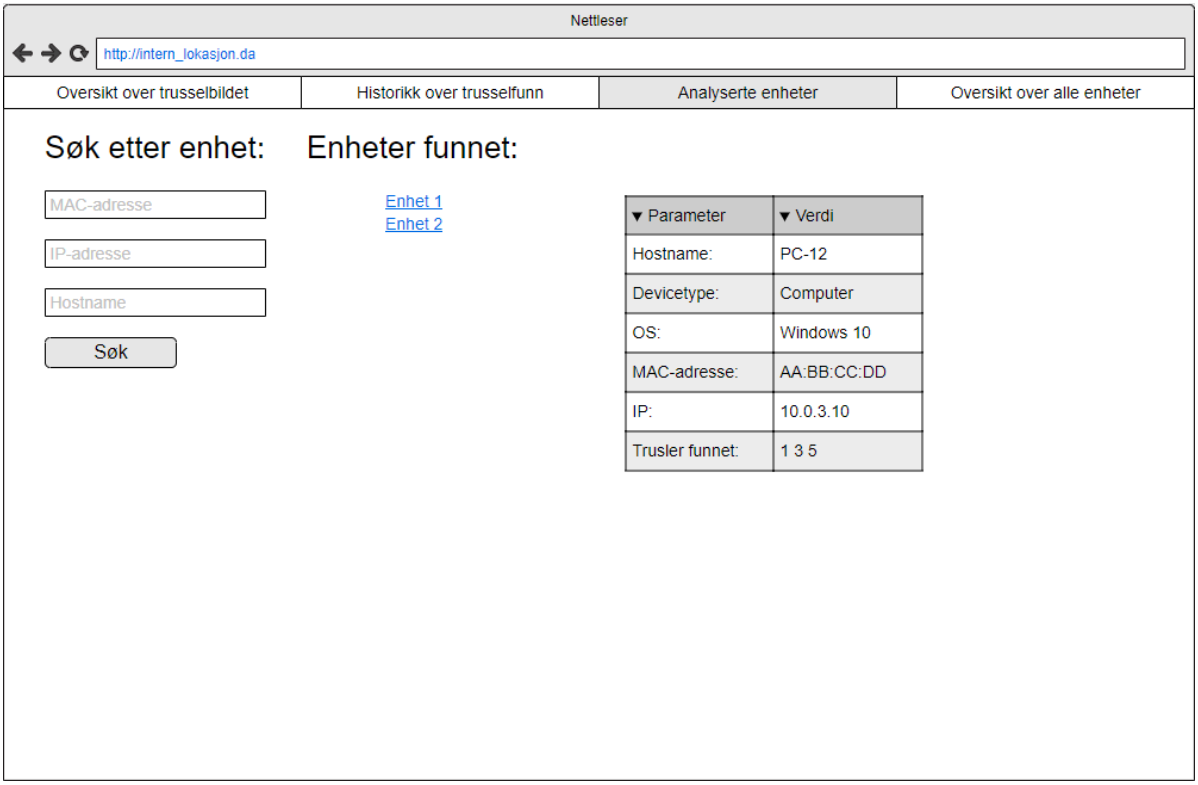
Figur 21: Nettside Trusler

En side som viser en graf av trusselfunn over tid:



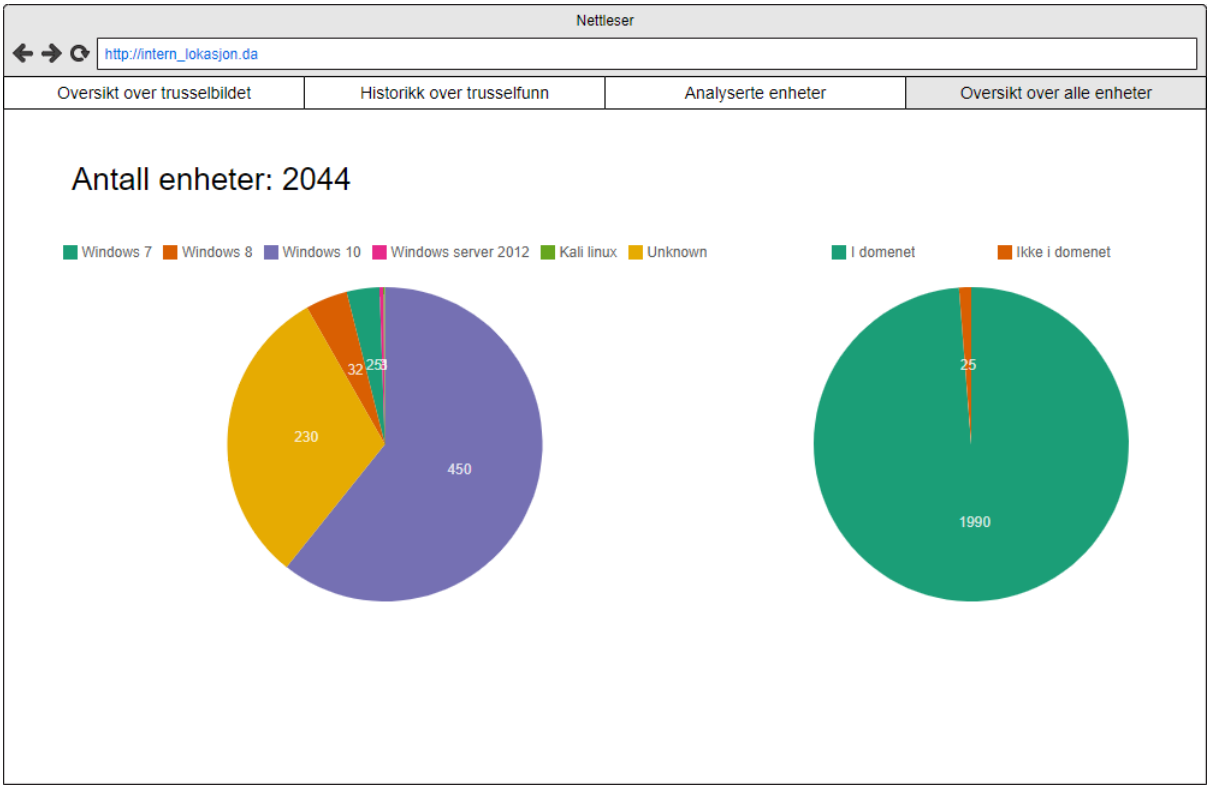
Figur 22: Nettside Grafer

En side som lar brukere se informasjonen om enheter som er analysert:



Figur 23: Nettside søk

En side som viser oversiktsbildet over alle enheter i nettverket:



Figur 24: Nettside oversikt

8. Deltakere

Prosjektgruppen består av Tormod Haus Lien og Marius Ibenfeldt Myhre.

Oppgavestiller og veileder fra Domstoladministrasjonen er Øyvin Moe, faglig leder for brukersenteret ved Domstoladministrasjonen.

Veileder fra NTNU er Tor Ivar Melling.

9. Kilder

GitHub Education. (2019). *GitHub Education*. Available at: https://education.github.com/ (Accessed: 13. February 2019)

Carina Grøttem (2016) *Derfor bør du vite hva Windows PowerShell er i stand til*. Available at: https://itavisen.no/2016/09/22/derfor-bor-du-vite-hva-windows-powershell-er-i-stand-til/ (Accessed: 13. February 2019)

Microsoft. (2019). *What is Power BI?* Available at: https://powerbi.microsoft.com/en-us/what-is-power-bi/ (Accessed: 13. February 2019)

Driftsdokument

Bacheloroppgave 015 *Marius Myhre*

Våren 2019 *Tormod Lien*

IDRI3001 Bacheloroppgave i drift av datasystemer

20. Mai. 2019

DOMSTOL ADMINISTRASJONEN

NTNU
Kunnskap for en bedre verden

Revisjonshistorie

Dato	Versjon	Beskrivelse	Forfatter
06.02.2019	0.1	Opprettet dokumentet	Prosjektgruppen
27.03.2019	0.2	“Sccm analyst” og “SQL Service-account”	Prosjektgruppen
08.05.2019	0.3	Oppsett av delkapitler	Prosjektgruppen
09.05.2019	0.4	Prerequesites og tilpassing av eget miljø	Prosjektgruppen
10.05.2019	0.5	Kap 2	Prosjektgruppen
11.05.2019	0.6	Kap 4	Prosjektgruppen
12.05.2019	0.7	Kap 3	Prosjektgruppen
13.05.2019	0.8	Kap 5	Prosjektgruppen
14.05.2019	0.9	Ferdigstilling av innhold i dokument	Prosjektgruppen
15.05.2019	0.10	Endringer etter veiledningsmøte	Prosjektgruppen
18.05.2019	0.11	Ferdigstilling av innhold etter tilbakemelding.	Prosjektgruppen

Innholdsfortegnelse

Figurliste

Tabelliste

Ordliste

Ord	Beskrivelse
SCCM	System Center Configuration Manager
AMP	Airwave Management Platform
CPPM	ClearPass Policy Manager
Aruba-tjenestene	Airwave og Clearpass
Service Account	Bruker som kun har de rettighetene som trengs av en tjeneste
EnVy	Navnet på verktøyet. “EnhetsVy”
JS	JavaScript
NodeJS	Eksekverer JavaScript-kode ved hjelp av Google V8-motoren. Dette gjør at JavaScript kan kjøres på serveren.
HTML	HyperText Markup Language. Programmeringsspråk for strukturering av nettside.
CSS	Cascading Style Sheets. Programmeringsspråk for definering av utseende til HTML-kode.
ADDS	Active Directory Domain Services. Katalogtjeneste for håndtering av brukere, brukerrettigheter og ressurskontroll.
SASS	Syntactically awesome style sheets

1. Introduksjon

Dette dokumentet beskriver hvordan verktøyet EnVy skal benyttes. Dokumentet er delt opp i fem deler, utenom introduksjonen: Installasjonsguide, Backend, Frontend, Teknisk forklaring av kode, og videreutvikling.Installasjonsguiden tar for seg alt som må gjøres for å installere EnVy, slik at det kan bli tatt i bruk. Backend forklarer hvordan det sluttbruker ikke trenger å se fungerer; hva skriptene gjør, og hvordan databasen fungerer. Frontend beskriver nettsiden som brukes for å visualisere dataen EnVy samler inn. Gjennom skjermbilder og tekstlig forklaring beskrives hvordan man kan benytte nettsiden. Under teknisk forklaring av kode beskrives all kode i detalj, slik at teknikere kan enkelt sette seg inn i virkemåten til verktøyet. Til slutt kommer videreutvikling, som tar for seg noen muligheter for videreutvikling av EnVy.

2. Installasjonsguide

Kapittelet beskriver hvilke prerequisites EnVy har, hvordan man skal installere EnVy, og hvordan man tilpasser EnVy til sitt miljø.

2.1 Prerequisites

Delkapittelet beskriver hvilke prerequisites som må være på plass før EnVy kan brukes.

2.1.1 SCCM

Her beskrives hva som må gjøres i SCCM

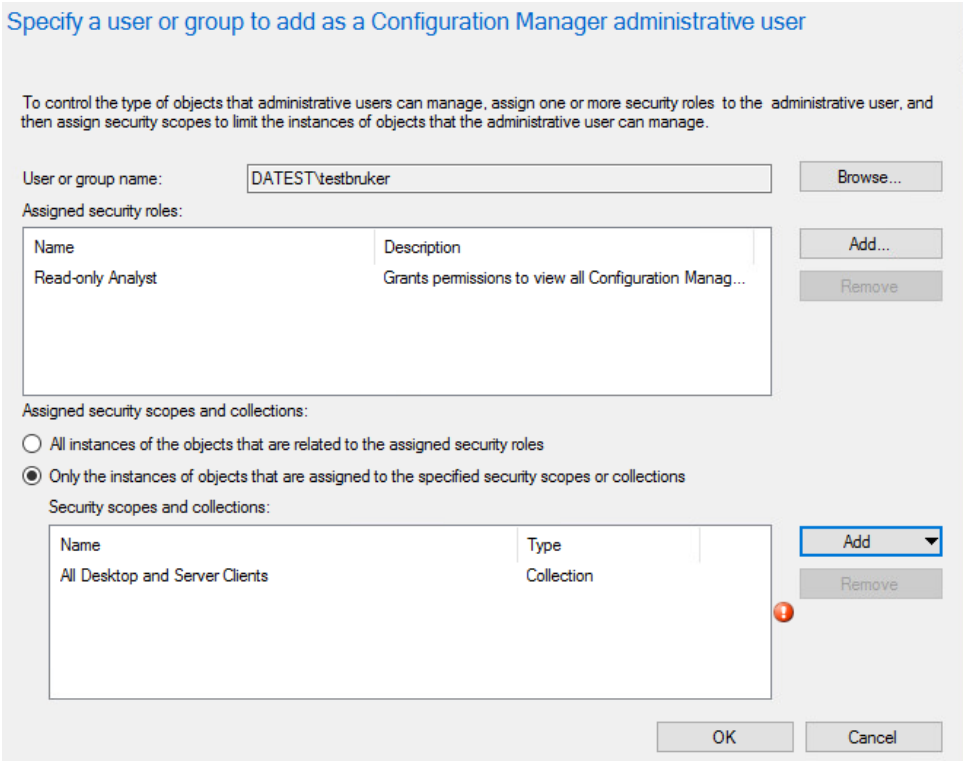
2.1.1.1 Lage SCCM Read-only Analyst

For å kunne hente data fra SCCM må det opprettes en bruker med begrensede rettigheter. Det eneste denne brukeren burde ha mulighet til er å hente ut data fra en spesifikk samling, eller collection som det heter i SCCM, av enheter. Derfor opprettes en "Read-only Analyst".

For å opprette en "Read-only Analyst" må det opprettes en serviceaccount i ADDS. Når dette er gjort kan man legge til denne serviceaccounten som SCCM analyst. Det gjøres på følgende måte:

Naviger til **Administration > Security > Administrative Users**.

Velg så **Add User or Group** og legg til servicebrukeren som skal benyttes. Velg så **Read-only Analyst** som security role, og legg til kun ønskede Collections i security scope. Eksempel i bildet under:



Figur 1: Read-only Analyst

Administrative Users vil da se slik ut:

Icon	Account Name	Account Display Name	Security Roles
	DATEST\Administrator		"Full Administrator"
	DATEST\sccmtest	sccmTest	"Read-only Analyst"

Figur 2: Administrative Users

Denne brukeren vil da kun ha lesetilgang fra angitt Collection.

2.1.1.2 Lage spørring i SCCM

For å hente ut ønsket data om enhetene i en spesifikk Collection så må det lages en SQL-spørring.

For å lage ny spørring i SCCM går man til **Monitoring > Queries > Create Query**.

Videre må query gis et navn, og dette navnet er viktig å skrive ned ettersom det også må skrives inn i "Configuration.ini". Neste steg er å trykke på **Edit Query Statement > Show Query Language**

I **Query Statement** skriver man inn følgende spørring for å hente ut ønsket data:

Query Statement:

```
select SMS_R_System.Name, SMS_R_System.MACAddresses,
SMS_R_System.IPAddresses,
SMS_R_System.OperatingSystemNameandVersion,
SMS_R_System.SID, SMS_R_System.ResourceId,
SMS_R_System.LastLogonUserName,
SMS_R_System.LastLogonTimestamp, SMS_R_System.ClientVersion,
SMS_R_System.AgentName, SMS_R_System.AgentTime from
SMS_R_System
```

Figur 3: SCCM Spørring

Det siste valget som må gjøres er valg av **Collection Limiting**. Her velger man den Collection det ønskes å hente data fra. Velg **Browse > Device Collections**. Trykk deretter på Collection det ønskes å hente data fra og fullfør veilederen. Det er viktig å avgrense til en Collection slik at belastningen på serveren blir så lav som mulig, men også at det ikke blir hentet ut unødvendig data. Unødvendig data vil kunne redusere oversikten man tilegner seg ved å benytte EnVy.

2.1.2 Aruba Airwave

For å kunne hente ut informasjon fra Airwave, benytter EnVy seg av det innebygde XML-apiet til Airwave. Det er nødvendig å lage en rolle med de rette tilgangene, og en api-bruker som benytter den rollen. For å hente ut informasjonen må API-brukeren deretter definere og kjøre rapporten som skal hentes.

2.1.2.1 Lage rolle for API service account

For å kunne gi en bruker i Airwave riktige rettigheter, er det nødvendig å lage en rolle. Rollen som blir beskrevet her har minimumskravet for å kunne hente ut en rapport.

For å lage rollen logger du deg inn i Airwave sitt webgrensesnitt som en bruker som har tilgang til å lage nye roller. Naviger deg så til:

AMP Setup > Roles > Add new role

Skriv inn admin-passord i boksen på toppen, og lag en rolle med følgende spesifikasjoner:

Name	Eksempel: API-reader
Enabled	Yes
Type	Device Manager
Device Access Level	Monitor (Read only)
Top Folder	Top
RAPIDS	None
VisualRF	Read Only
UCC	No
Traffic Analysis	No
Aruba Controller Single Sign-on Role	Disabled
Display client diagnostics screens by default	No
Allow user to disable timeout	No
Allow reboot of devices	No
Allow creation of guest users	No

Tabell 1: AMP rolle

Denne rollen vil nå kun ha read-tilgang, og kan benytte seg av API-et.

2.1.2.2 Lage API service account

For å kunne hente ut en rapport gjennom Airwave sitt API er det nødvendig å lage en bruker med riktige rettigheter.

For å lage brukeren logger du deg inn i Airwave sitt webgrensesnitt med en bruker som har tilgang til å lage nye brukere. Naviger deg så til:

AMP Setup > Users > Add New User

Skriv inn admin-passord i boksen på toppen, og skriv brukernavn og passord for brukeren, og velg rollen du lagde tidligere (Eksempel: API-Reader)

Brukernavnet til service accounten skal legges inn i konfigurasjonsflen (configuration.ini), under [AirWave], på AMP_APIUserName. Passordet kan enten legges inn i klartekst i konfigurasjonsfilen, under [AirWave], på AMP_APIpWord, eller passordet kan krypteres, og path til passordet kan legges på AMP_APIpWordPath. For instrukser til hvordan man kan kryptere passord, se kapittel 2.2.4 Kryptering av passord.

2.1.2.3 Lage rapport

For å hente informasjon fra Airwave, benytter EnVy seg av Airwave-APIet sin latestreport-API. Det er derfor nødvendig å lage en rapport som samler informasjonen EnVy skal hente.

For å lage rapporten logger du deg inn i Airwave sitt webgrensesnitt med brukeren du lagde i det tidligere steget. Naviger deg så til:

Reports > Definitions > Add New Report Definition

Lag deretter en rapport med følgende spesifikasjoner:

Title	Eksempel: nodeInformasjonsrapport
Type	Client Inventory
Group	-- All Groups --
Folder	-- All Folders --
Filter On	Devices
Device Search Filter	
Device Search Exclude Filter	
Filter by device type	-- All Device Types --
Summarize report by	Ingen (Trykk på knappen Unselect All som er rett under -- All Device Types --)
Classification	All
Device Type	All
AOS Device Type	All
Manufacturer	All
Model	All
OS	All
OS Detail	All
Network Chipset	All
Network Driver	All
EAP Supplicant	All
Asset Group	All
Asset Category	All
Include detauls about every client	Yes
Limit to active devices	No (Include all devices)
Schedule	Hvor ofte rapporten skal genereres (Gjerne en gang om dagen)
Generated report visibility	By Role
Email report	No
Export report	No

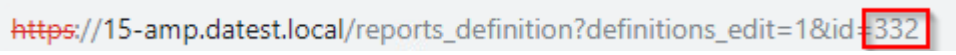
Tabell 2: AMP rapport spesifikasjoner

Deretter trykk "**Add and run**" for å lagre og kjøre rapporten med en gang.

Det vil være nødvendig for konfigurasjonen av EnVy å ha rapport-ID til denne rapporten. Den kan man finne ved å gå til følgende side:

Reports > Definitions

Og trykk på **blyanten** ved rapporten du lagde. I URL-en til siden vil ID-en stå:



Figur 4: AMP ReportID

Denne ID skal legges inn i konfigurasjonsfilen (configuration.ini) under [AirWave], på AMP_ReportID.

2.1.3 Aruba Clearpass

For å hente ut informasjon fra Aruba Clearpass benytter EnVy seg av det innebygde REST-APIet til Clearpass.

2.1.3.1 Lag API-klient

For å kunne hente ut informasjon fra Clearpass er det nødvendig å lage en API-klient som EnVy kan koble seg til. Dersom deres Clearpass-instans allerede har en API-klient konfigurert, er det mulig å benytte den, men det anbefales å lage en ny API-klient for EnVy.

For å sette opp API-klienten logger du inn på Clearpass sitt webgrensesnitt med en administratorbruker. Deretter går du til **Clearpass Guest**, og navigerer deg til:

Administration > API Services > API Clients

Og trykker her på **Create API client**.

Lag en API-klient med følgende spesifikasjoner:

Client ID	Unik streng som identifiserer klienten
Description	En beskrivelse av klienten
Enabled	True
Operator Profile	Read-Only Administrator
Grant Type	Client credentials (grant_type=client:credentials)
Access Token Lifetime	10 minutter

Tabell 3: Clearpass API-klient spesifikasjoner

Når man velger Grant Type: Client credentials vil en Client Secret dukke opp. Denne må skrives ned, da den skal brukes for å autentisere seg mot API-et. (Merk at bildet under har en annen client secret enn din API-client.)

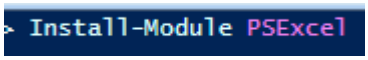
Figur 5: Clearpass client secret

Trykk deretter på Create API Client.

Client ID må skrives inn i konfigurasjonsfilen (configuration.ini) under [ClearPass], på CPPM_APIClientID. Client Secret kan enten legges inn som klartekst i konfigurasjonsfilen, på CPPM_APIClientSecret, eller den kan krypteres til en fil, og stien til passordet kan legges på CPPM_APIClientSecretPath. For instrukser til hvordan man kan kryptere et passord, se kapittel 2.2.4 Kryptering av passord.

2.1.4 Moduler som må installeres

EnVy benytter seg av modulen "PSExcel" for å kunne hente inn DHCP-scopes fra en .xlsx-fil. Det er nødvendig å installere denne på maskinen som skal kjøre skriptene for uthenting, og analyse. For å installere modulen, benyttes følgende kommando i PowerShell:



Figur 6: PSExcel modul

Merk her at dersom maskinen som skal kjøre EnVy ikke har tilkobling til internett, kan det være nødvendig å laste ned og installere modulen manuelt. Dersom dette er nødvendig, kan modulen lastes ned fra PowerShellGallery.

2.2 Installasjon

Delkapittelet tar for seg installasjonen av EnVy. Det er gjort et skille mellom oppsett av database og tilpasning av EnVy for å gi god oversikt.

2.2.1 PowerShell-Script

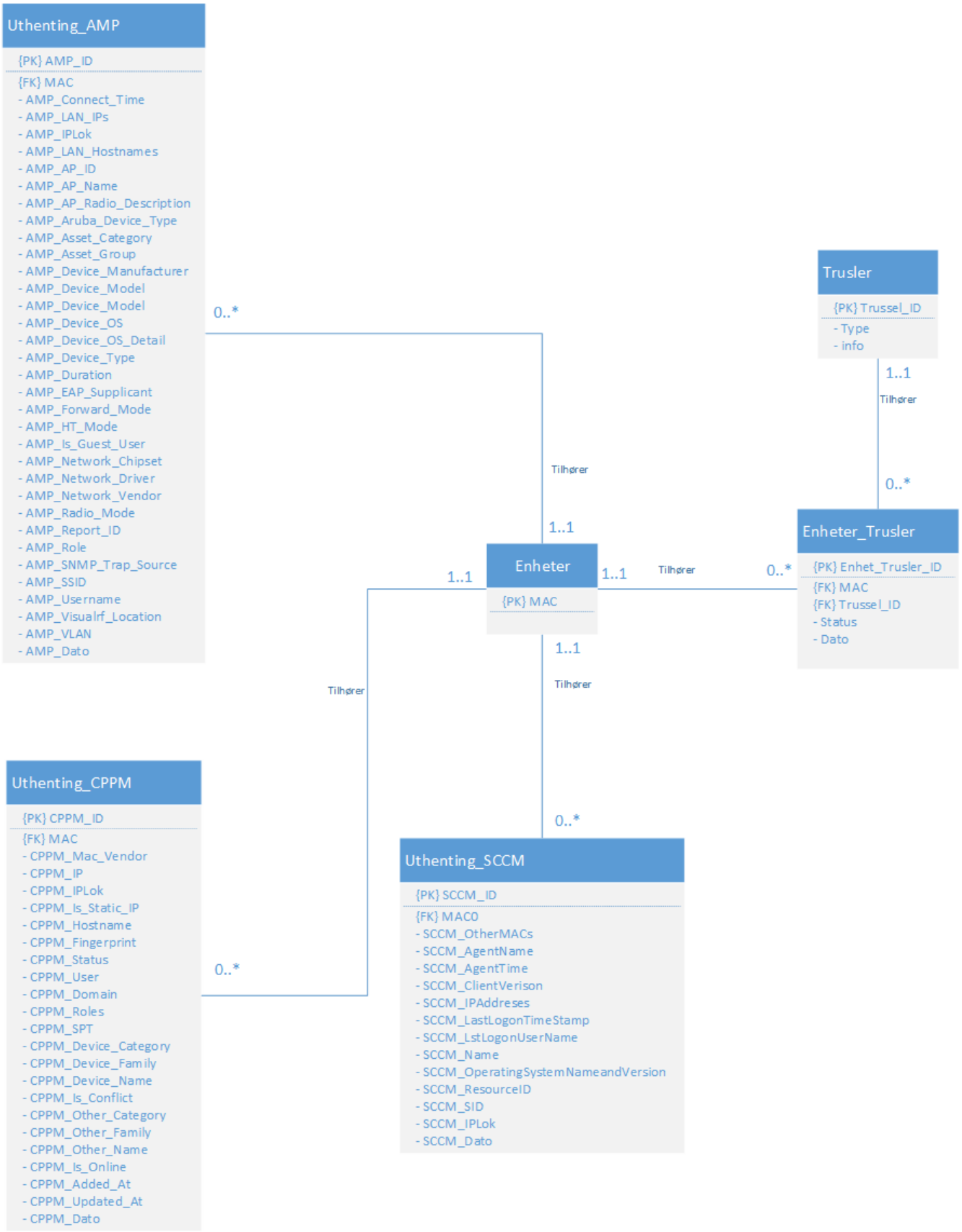
Powershell-skriptene som skal benyttes for daglig bruk av EnVy ligger i mappen EnVy_PS. Her er det filene "hent utdata.ps1" og "analyser lagretdata" som skal benyttes i daglig drift. Disse kan enten kjøres manuelt, eller de kan automatiseres. Det er mange måter å automatisere kjøring av PowerShell-skript, og prosjektgruppen anbefaler å benytte scheduled-job, da Domstoladministrasjonen enkelt kan tilpasse tidspunkt og frekvens på uthentingene. Merk at filene ikke bør flyttes fra mappen de ligger i, da EnVy benytter seg av relative filstier, som kan slutte å fungere dersom filene flyttes.

2.2.2 Database

EnVy er utviklet for å koble seg til en Microsoft SQL-database. Dette vil si at databasen kan ligge enten på en på en lokal server, eller i Azure. Oppsett av tabeller og brukere skjer ved hjelp av "InitSQL.ps1".

2.2.2.1 Initialisering

Initialisering av databasen skjer ved å benytte skriptet "InitSQL.ps1". Når dette skriptet kjøres vil en bli bedt om å skrive inn brukernavn og passord på administratorbruker til databasen. Deretter blir en bedt om å skrive inn navn og passord på servicebruker. Passordet blir lagret som securestring i ønsket sti. Denne securestringen vil bli brukt videre av EnVy når data hentes ut eller sendes inn til databasen. Når passordet lagres på denne måten så kan det kun dekrypteres til klartekst av brukeren som kryperte passordet, i tillegg til at det må gjøres på samme maskin hvor det ble kryptert. Dersom EnVy skulle bli flyttet til en annen maskin, vil dette si at passordet må krypteres til fil på nytt. Databasen blir deretter opprettet og blir seende ut som i bildet under. PK betyr "Primary Key" og FK betyr "Foreign Key".



Figur 7: Databasen

2.2.2.2 Brukere

Det opprettes to ulike brukere i "InitSQL.ps1". Den første brukeren som opprettes er serviceaccounten som en selv skriver inn brukernavn og passord til. Denne brukeren vil bli brukt av EnVy til å hente data fra og sende til databasen. Serviceaccounten blir satt opp til å kun ha rettigheter til å utføre "Select" og "Insert" setninger mot databasen. Dette er gjort med tanke på sikkerheten til databasen, slik at brukeren kun kan sende inn ny data og hente ut gammel data. Oppsettet til databasen vil dermed ikke kunne endres med denne brukeren, og den vil heller ikke ha mulighet til å slette data.

Den andre brukeren som opprettes er "NettsideBruker". Denne brukeren opprettes for at nettsiden skal kunne kommunisere med databasen. Nettsiden benytter denne brukeren til å hente ut relevant data for de ulike visualiseringsjobbene. Denne brukeren blir satt opp med rettighetene til å utføre "Select" setninger mot databasen. Ettersom nettsiden kun henter data fra databasen så vil alle andre rettigheter slås av. På denne måten vil det ikke være mulig å utnytte denne brukeren til å endre på noe i databasen.

2.2.2.3 Trusler

Det siste som skjer i skriptet "InitSQL.ps1" er at truslene det letes etter blir ført inn i tabellen "Trusler" i databasen. På denne måten blir det også testet om serviceaccount fungerer.

2.2.3 Nettside

Koden for nettsiden benytter seg av PHP, NodeJS og html. Når webserveren er oppe, lastes alt i mappen EnVy_nettside opp til webserveren.

2.2.4 Kryptering av passord

Ettersom EnVy behøver forskjellige passord for å kunne kjøre, kan det være ønskelig å ikke lagre disse i klartekst i konfigurasjonsfilen. For å hjelpe til med dette, benyttes funksjonene Protect_Passord og Unprotect_Passord.

For å kryptere passordet til API-brukeren på Airwave, Client-secret til Clearpass, og databasepassord, benyttes funksjonen Protect_Passord. Denne funksjonen vil konvertere en plaintext-string til en securestring, og dersom punktet Secretmode er satt til File i konfigurasjonsfilen, vil EnVy automatisk dekryptere passordene for bruk. De krypterte passordene kan lagres i en fil, og path til filen kan legges inn i konfigurasonsfilen, på punktene CPPM_APIClientSecretPath, AMP_APIpWordPath, og Database_PasswordPath.

2.2.4.1 Eksempel på kryptering

For å kryptere passordet "Passord1!", og lagre det i mappen C:\EnVy_PS\secret\AMPSecret.txt, kan man kjøre følgende kommando i Powershell. Merk her at man må legge inn funksjonen i terminalen, enten ved å kjøre "hent scripts.ps1", eller "stottefunksjoner.ps1".

"Password1!" | Protect-Passord | Out-File –FilePath C:\EnVy_PS\secret\AMPSecret.txt

Når dette er gjort, kan vi se at innholdet i filen er kryptert:

```
01000000d08c9ddf0115d1118c7a00c04fc297eb010000004610a00c88361c4fa6be62547c7cb67c000000000200000000000106600000001000020000000c0391a04e695d85e02ffe95ee724ad9457f4ef56cc49e74fca725cac45ba3fd4000000000e800000000200002000000060ad9dbaf15e0364343b72a250958c19c90ec914fdf93bfbc3d2287a23312f6c20000000b8433b20ccd0ca45f0e3a7a402a1931db22143efd4fca05698bff7311976ee95400000002df18c693eb9e749943a8e552a528dff6b413a07996f71d5e77f1fc3d7ccb8ee2335f2aa2b5b7a76cdebaf9a41f481701ef0421064525783e1d682a1c2d95680
```

Figur 8: Kryptert passord til fil

2.3 Tilpass eget miljø

For å tilpasse EnVy til ditt eget miljø må man endre på filen configuration.ini, kjent som "konfigurasjonsfilen". Filen er en tekstfil som består av flere seksjoner, og flere attributter for hver seksjon, som vil tilpasse EnVy til ditt miljø. Konfigurasjonsfilen inneholder kommentarer som forklarer, men her følger det også en detaljert beskrivelse av hvert attributt:

Attributt	Eksempelverdi	Tillatte verdier	Forklaring
Generelt			
Secretmode	Plain	Plain, File	Plain betyr at EnVy forventer at et passord blir skrevet i klartekst videre i konfigurasjonsfilen, der passord eller andre hemmeligheter blir skrevet. File betyr at EnVy forventer en path til en tekstfil, som inneholder et MS-securestring-kryptert passord i en fil, som ligger i pathen.
MellomLagerSize	7	Heltall	Antall filer som skal lagres i lokalt mellomlager for analysering.
RelPaths	True	True, False	Boolean som bestemmer om filepaths i konfigurasjonsfilen er relative til hovedmappen, eller absolutte.
PathTilAnalyser	\Analyser	Tekststreng	Filepath til mappen hvor analysene ligger. Basert på RelPaths skal denne verdien være en relativ eller absolutt path.
PathTilMellomlager	D:\EnVy\Mellomlager	Tekststreng	Filepath til mappen hvor mellomlageret skal ligge. Basert på RelPaths skal denne verdien være en relativ eller absolutt path.

Tabell 4: Generelle tilpasninger

Attributt	Eksempelverdi	Tillatte verdier	Forklaring
ClearPass			
CPPM_URL	https://15-cppm.datest.local:443	Tekststreng	URL til Clearpass-serveren.
CPPM_ApiClientID	TestClient1	Tekststreng	Navnet du ga API-klienten du lagde i Clearpass
CPPM_APIClientSecret	hV5wceohg5GMlPLnAz81e2VjwmNL7XL81Am6xHqlfQ26	Tekststreng	API-nøkkelen som ble vist når du lagde API-klienten i clearpass. Denne attributten brukes dersom SecretMode er plain.
CPPM_APIClientSecretPath	\Secret\CPPMSecret.txt	Tekststreng	Filepath til filen som holder den krypterte API-nøkkelen til API-klienten. Denne attributten brukes dersom SecretMode er File. Basert på RelPaths skal denne verdien være en relativ eller absolutt path.
CPPM_allowedTimeFrame	18:00-06:00	hh:MM-hh:MM	Tidsrommet hvor EnVy har lov til å kontakte Clearpass-serveren og hente data. Dersom verdien som skrives inn er 00:00-00:00 vil EnVy alltid hente data fra serveren. Denne attributten brukes dersom EnVy skal kjøre flere ganger om dagen, men CPPM-serveren ikke kan belastes i spesifikke tidsrom.

Tabell 5: Clearpass tilpasninger

Attributt	Eksempelverdi	Tillatte verdier	Forklaring
AirWave			
AMP_URL	Https://15-amp.datest.local:443	Tekststreng	URL til Airwave-serveren
AMP_APIUserName	apiUser	Tekststreng	Navnet til API-brukeren du lagde for Airwave
AMP_APIpWord	H4Vdor4#vm	Tekststreng	Passordet til API-brukeren i klartekst. Denne attributten brukes dersom SecretMode er plain
AMP_APIpWordPath	\secret\		Filepath til filen som inneholder det krypterte passordet til API-brukeren. Denne attributten brukes dersom SecretMode er File. Basert på RelPaths skal denne verdien være en relativ eller absolutt path.
AMP_ReportID	332	Heltall	RapportID til rapporten du lagde tidligere. For instrukser på hvordan man finner denne, se kapittel 2.1.2 - Aruba Airwave > Lage rapport
AMP_AllowedTimeFrame	19:00-02:00	hh:MM-hh:MM	Tidsrommet hvor EnVy har lov til å kontakte Airwave-serveren og hente data. Dersom verdien som skrives inn er 00:00-00:00 vil EnVy alltid hente data fra serveren. Denne attributten brukes dersom EnVy skal kjøre flere ganger om dagen, men Airwave-serveren ikke kan belastes i spesifikke tidsrom.

Tabell 6: Airwave tilpasninger

Attributt	Eksempelverdi	Tillatte verdier	Forklaring
SCCM			
SCCM_URL	15-sccm2.datest.local	Tekststreng	URL til SCCM-serveren.
SCCM_Query	EnVyQuery	Tekststreng	Navnet til Queryen du lagde for EnVy i SCCM
SCCM_Sitecode	ST1	Tekststreng	Sitecode til SCCM-siten
SCCM_AllowedtimeFrame	01:00-04:00	hh:MM-hh:MM	Tidsrommet hvor EnVy har lov til å kontakte SCCM-serveren og hente data. Dersom verdien som skrives inn er 00:00-00:00 vil EnVy alltid hente data fra serveren. Denne attributten brukes dersom EnVy skal kjøre flere ganger om dagen, men SCCM-serveren ikke kan belastes i spesifikke tidsrom.

Tabell 7: SCCM tilpasninger

Attributt	Eksempelverdi	Tillatte verdier	Forklaring
Database			
Azure_UserName	EnVyBruker	Tekststreng	ServiceAccount på databasen som EnVy skal bruke for innsending. Spesifiseres i løpet av initialiseringsscriptet.
Azure_password	BEff54#dde	Tekststreng	Passordet til service-accounten som EnVy skal bruke for innsending, i klartekst. Denne attributten brukes dersom SecretMode er plain
Azure_PasswordPath	\secret\AzureSecret.txt	Tekststreng	Filepath til filen som inneholder det krypterte passordet til service-accounten EnVy skal bruke for innsending. Denne attributten brukes dersom SecretMode er File. Basert på RelPaths skal denne verdien være en relativ eller absolutt path.
Azure_SQLServer	Da-test-sql.database.windows.net	Tekststreng	URL til databasen.
Azure_port	1433	Heltall	Porten som skal brukes for å koble seg til databasen
Azure_DatabaseNavn	Da-test-sql	Tekststring	Navnet på databasen på databaseserveren.

Tabell 8: Database tilpasninger

Attributt	Eksempelverdi	Tillatte verdier	Forklaring
SQL			
SQL_BatchSize	25	1-1000	Antallet enheter som skal sendes inn på en gang i hver SQL-setning. Brukes for å optimalisere INSERT-setninger. Optimalt er ifølge våre undersøkelser 25 enheter per spørring.

Tabell 9: SQL batch tilpasning

3. Oversikt over backend

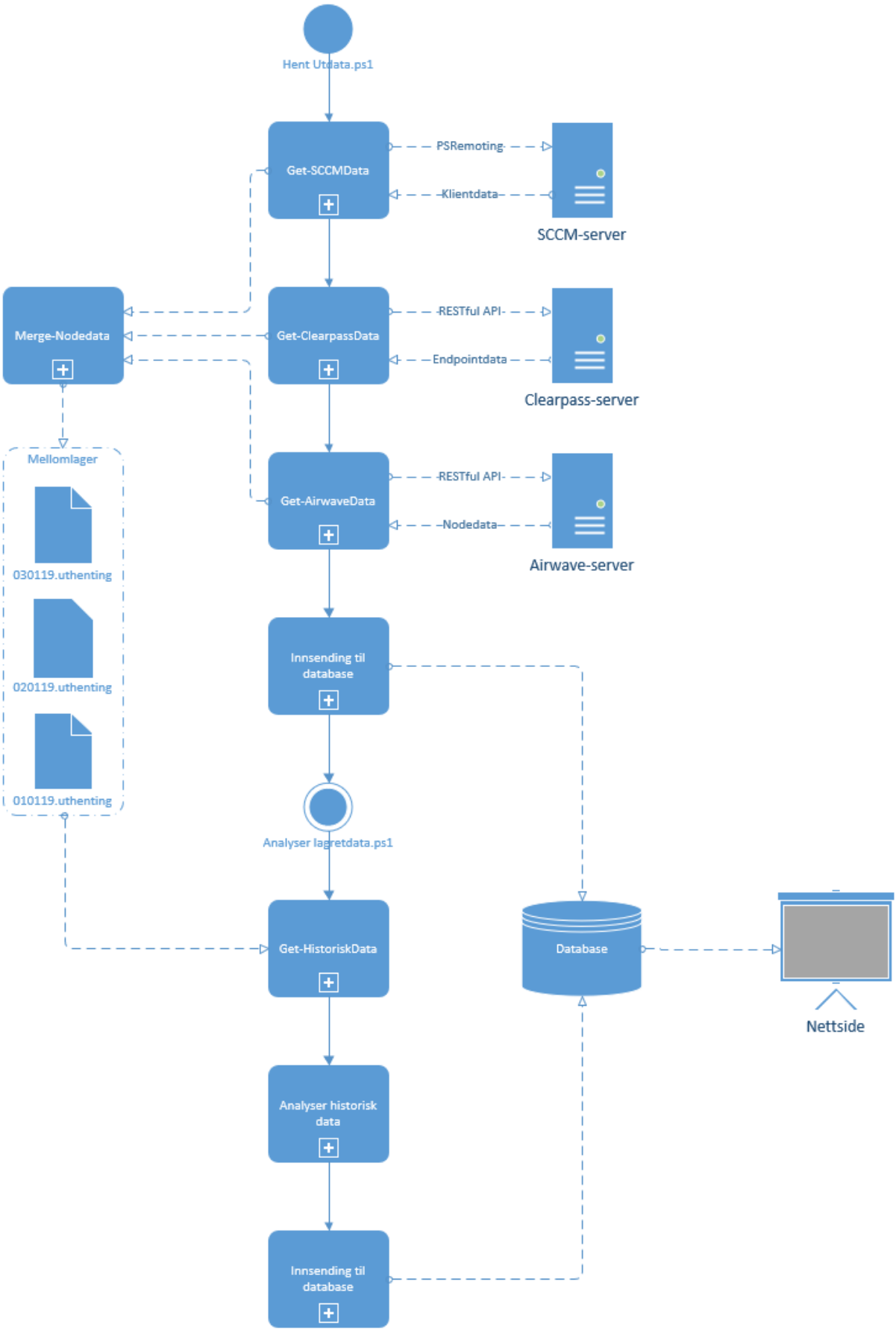
Kapittelet beskriver backenden til EnVy; Dataflyten i skriptene, og databasen.

3.1 Dataflyt

EnVy benytter seg i hovedsak av to hovedscript. Ett script som henter data fra de tre tjenestene: Hent Utdata.ps1, og ett script som analyserer dataen som er hentet: Analyser lagretdata.ps1.

Hent Utdata.ps1 vil benytte seg av informasjonen fra konfigurasjonsfilen, og hente data fra de tre kildene. Dataen som hentes vil formateres for videre bruk, og den blir sammenstilt til et kombinert objekt som samler informasjon om samme enheter fra de forskjellige tjenestene. Deretter vil to ting skje: Først lagres den kombinerte informasjonen til et lokalt mellomlager som benyttes for analyse av informasjonen, og deretter sendes den samlede dataen til databasen.

Analyser Lagretdata.ps1 kjører etter at Hent Utdata er ferdig, og vil hente inn all informasjon som er mellomlagret på den lokale maskinen, og utføre alle analyser som ligger i mappen /analyser på den. Resultatene fra analysen blir formatert, og sendes inn til databasen.



Figur 9: Dataflyt

3.2 Henting av data

Uthenting av data blir utført med ulike skripts for de tre ulike tjenestene det hentes nodeinformasjon fra.

SCCM.

For å hente nodeinformason fra SCCM benyttes skriptet "Get-SCCMKlienter.ps1". Skriptet kan deles opp i to deler hvor første delen er oppkobling mot SCCM-server og andre del er en kommando som kjøres på server. Oppkoblingen skjer ved å benytte PSSession, og sesjonen avsluttes etter kommando er kjørt på server og nodeinformasjon er hentet ut. Kommandoen kjøres på server ved hjelp av "Invoke-Command", som igjen benytter "Invoke-CMQuery" for å kjøre ønsket spørring som er opprettet i SCCM.

SCCM benytter seg av "Kerberos Authentication", noe som gjør at dette skriptet må kjøres av en bruker som er "Administrative User" i SCCM. Eksempel på hvordan man lager en slik bruker beskrives under punkt 2.1.1.

Airwave.

For å hente nodeinformasjon fra Airwave benyttes funksjonen Get-AMPClients. Skriptet benytter seg av PowerShell-cmdleten Invoke-RestMethod for tilkobling til Airwave-serveren. Først benyttes innloggingsAPIet for å lagre en websession, og denne benyttes for å hente ut den mest nylige rapporten av spesifisert type.

Clearpass.

For å hente nodeinformasjon fra Clearpass benyttes funksjonene Get-CPPMApiAccessToken, og Get-CPPMEndpoints. Først hentes en OAuth 2.0 Bearer Token med Get-CPPMApiAccessToken, som blir brukt i Get-CPPMEndpoints for å hente ut informasjonen fra CPPM-serveren. APIet som benyttes er "/api/insight/endpoint", som vil hente ut all enhetsinformasjon Endpoints har.

3.3 Formatering av data

For å kunne benytte nodeinformasjonen fra de tre tjenestene, må data som hentes formateres til samme format. Etter at informasjon er hentet fra en kilde, vil skriptet loope gjennom de hentede enhetene, og formatere de som powershell-objekter. Deretter blir enhetene lagt i en tabell, som kan benyttes av de andre skriptene i EnVy.

3.4 Sammenstilling av data

Etter at nodeinformasjon fra de tre tjenestene er hentet, vil dette sammenstilles til ett objekt som inneholder alle unike MAC-adresser og all nodeinformasjon som er hentet om hver MAC-addresse. Sammenstillingen gjøres av funksjonen Merge-Nodedata. Først lages en dyp-kopi av informasjonen som er hentet, og funksjonen looper gjennom alle uthentinger som er sendt inn til funksjonen. For hver uthenting går den gjennom hver enhet, og samler all informasjonen som ligger i hver uthenting i det nye objektet som består av alle hentede mac-addresser med all hentet informasjon for hver mac-addresse. Da den sammenstilte dataen inneholder alle mac-addresser som ble hentet fra de tre tjenestene, er det denne som benyttes når EnVy sender mac-addresser til Enheter-tabellen i databasen.

3.5 Mellomlager

Den sammenstilte informasjonen mellomlagres i mappen \mellomlager, med formatet YYYY-MM-DD.uthenting. Informasjonen blir konvertert til JSON før lagring, og konvertert tilbake fra JSON når den skal brukes til analyser av dataen. Konfigurasjonsfilens "MellomLagerSize" bestemmer hvor mange uthentinger som skal lagres i mellomlageret.

3.6 Analyse av data

Analysen av informasjonen skjer separat fra uthentingen, og gjøres med scriptet "Analyser lagretdata.ps1". Analysen benytter seg av funksjonen Get-HistoriskData, som henter den historiske dataen som ligger lagret i mellomlageret, og Merge-HistoriskData, for å samle all informasjonen fra .Uthenting -filene til en enhetstabell, og til slutt funksjonen Test-Enhetstabell, som går gjennom alle enheter i enhetstabellen, og utfører alle analyser på hver enhet. Resultatene fra analysene blir deretter sendt til databasen, i tabellen Enheter_Trusler. Analysene som utføres blir beskrevet i kapittel 2.7.1 og 2.7.2

3.6.1 Uadministrerte enheter

Formålet med denne analysen er å finne enheter som er koblet på det interne nettet, men som ikke blir administrert av SCCM. Dersom en enhet ikke administreres av SCCM kan en risikere at enheten blir utdatert, noe som er et sikkerhetsbrudd man ønsker å finne. For hver enhet som sendes inn til analysen, ser analysen om enheten har blitt funnet i SCCM, eller bare i Airwave/Clearpsas. Dersom enheten er funnet i SCCM blir den administrert, men om den ikke har blitt funnet er det en uadministrert enhet, og resultatet lagres i databasen.

3.6.2 IP-lokasjon

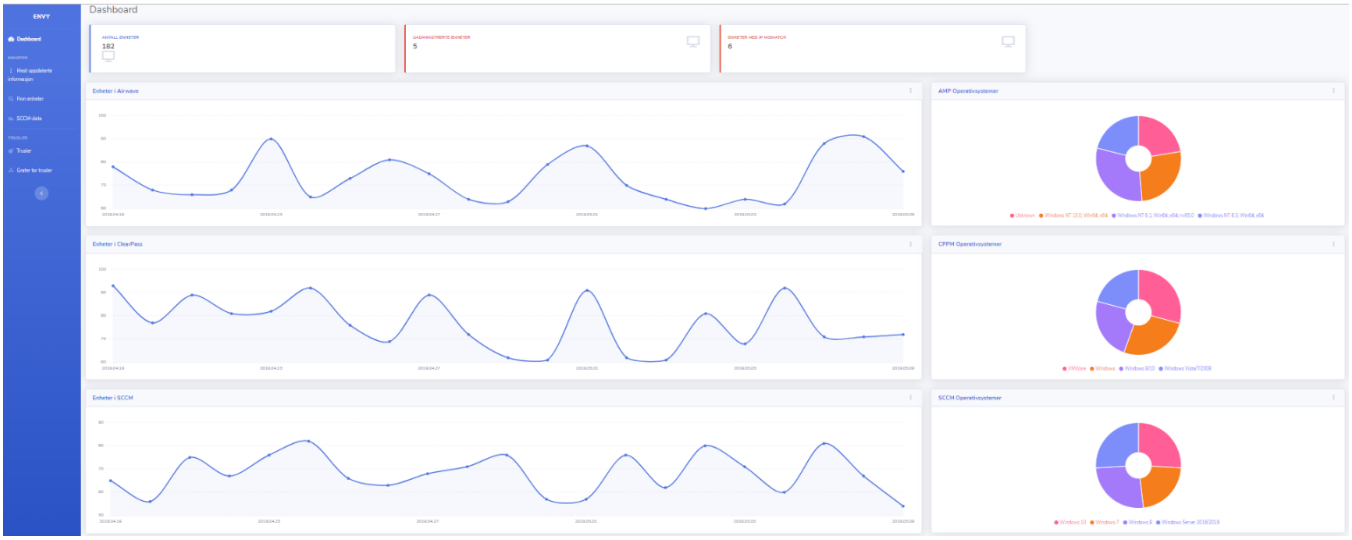
Analyse av IP-lokasjon utføres ved å benytte skriptet "Analyse_IPRange.ps1". Skriptet henter ut nyeste informasjon om hver enhet og sjekker om IPLok propertyen stemmer mellom de ulike tjenestene. Dersom det ikke er samme IPLok i siste uthenting fra de ulike tjenestene blir enheten flagget med "IP-Mismatch", og vil bli sendt inn som en trussel til databasen.

4. Oversikt over frontend

Kapittelet beskriver hva nettsiden viser og hvordan den benyttes. For å gi god oversikt er de ulike sidene som sluttbruker delt opp i hvert sitt delkapittel.

4.1 Dashboard

Dashbordet gir en oversikt over aktiviteten i nettverket. Dette er filen “index.html”.



Figur 10: Dashboard

Antall Enheter

Viser antall enheter som er loggført i databasen. Teksten og skjermen er interaktiv, og vil sende bruker til siden “Mest oppdaterte informasjon”.

Uadministrerte enheter

Viser antall enheter som er i nettverket, men som ikke blir administrert av SCCM. Tallet representerer antallet som ble funnet sist gang analysen ble utført. Når en analyse utføres blir data fra den siste uken analysert. Teksten og skjermen er interaktiv, og vil sende bruker til siden “Trusler”.

Enheter med IP-mismatch

Viser antall administrerte enheter i nettverket som har byttet IP-lokasjon den siste uken. Også her representerer tallet antallet som ble funnet sist gang analysen ble utført, og analysert data er fra de siste 7 dagene. Teksten og skjermen er interaktiv, og vil sende bruker til siden “Trusler”.

Enheter i Airwave, Enheter i Clearpass, og Enheter i SCCM

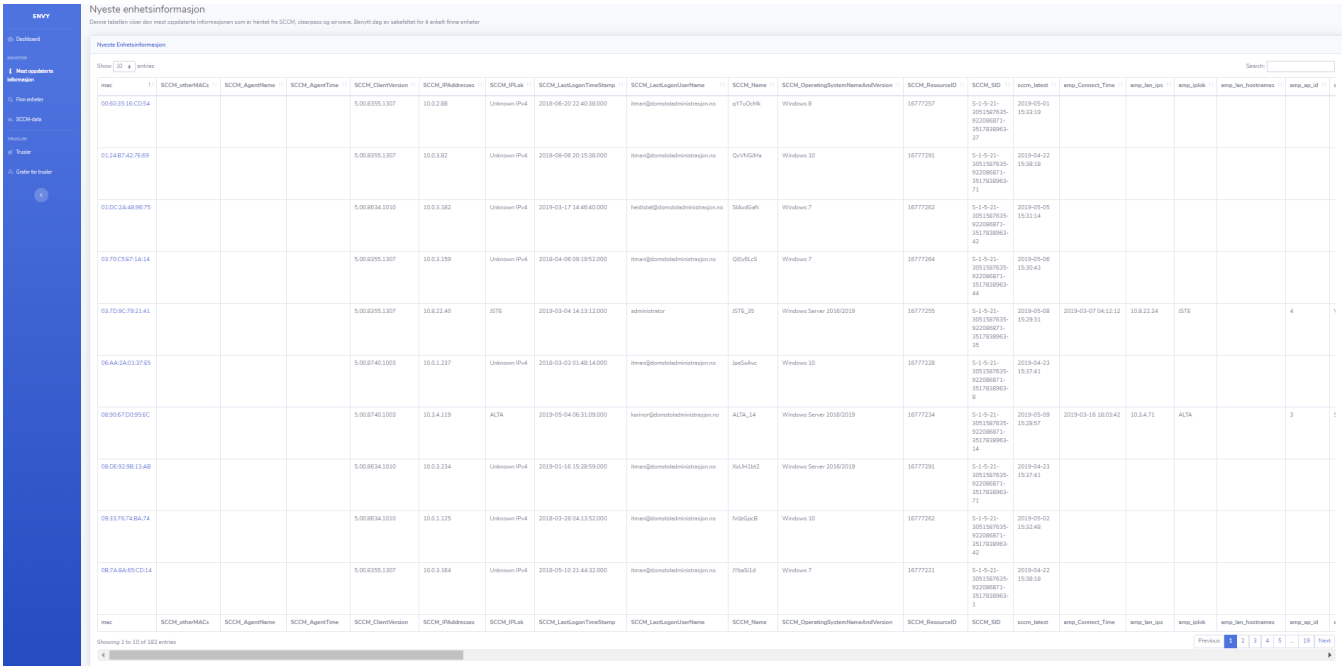
Viser en historisk oversikt over hvor mange enheter som ble loggført fra de ulike tjenestene. Data representerer alle uthentinger fra tjenestene som er blitt sendt til databasen. Hver uthenting blir markert som et punkt på grafen og viser antall enheter dersom en holder over punktet.

AMP-, CPPM- og SCCM operativsystemer

Viser alle operativsystemer som ble funnet i siste uthenting fra de ulike tjenestene. For å se antallet enheter med de ulike operativsystemene holder en over ønsket OS, og antallet vil deretter vises.

4.2 Mest oppdaterte informasjon

Siden viser alt av data som befinner seg i databasen. Dette er filen “nyesteinfo.php”.

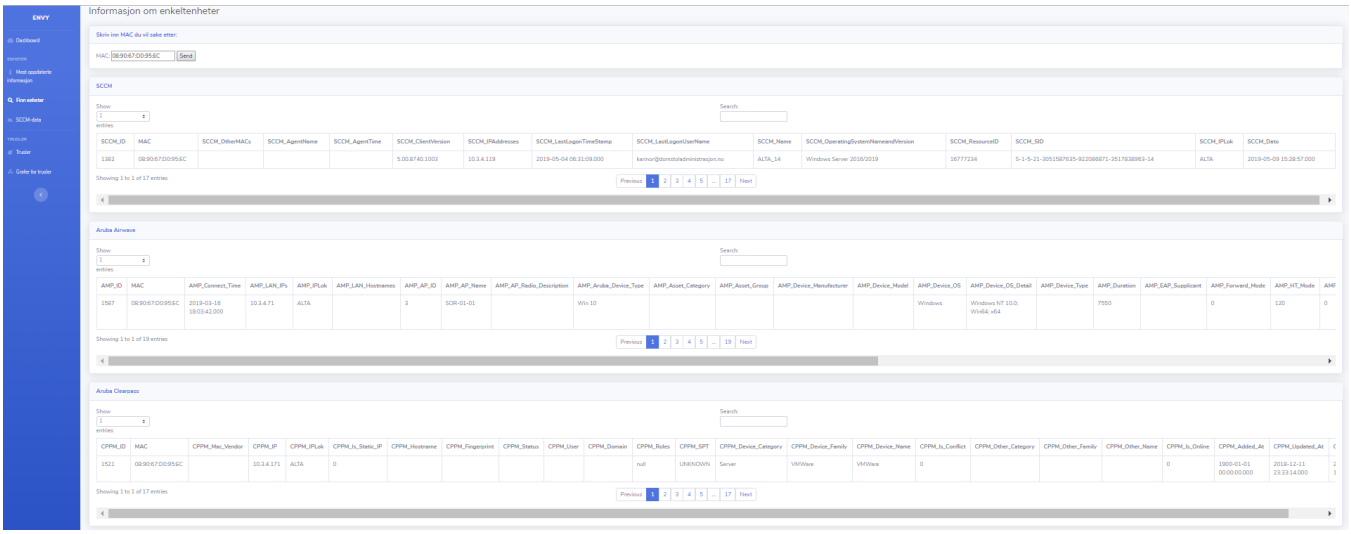


Figur 11: Mest oppdaterte informasjon

Øverst til venstre er det et alternativ over hvor mange enheter en ønsker å vise per side, og nederst til høyre kan en bla mellom de ulike sidene. Søkefeltet oppe til høyre kan benyttes til å søke gjennom dataen, og alle enheter med informasjon som matcher søket vil bli vist i tabellen. Antall enheter med ønsket søk vises nede til venstre. Dersom det ikke skrives inn noe i søkefeltet vil alt av data vises, og antall enheter i databasen vil vises nede til venstre. Alle MAC-adresser er interaktive, og vil sende bruker til "Finn enhet" med valgt MAC-adresse som søk.

4.3 Finn enheter

Denne siden viser alt av data som er lagret om en spesifikk enhet. Dette er filen "finnEnkeltenhet.php".

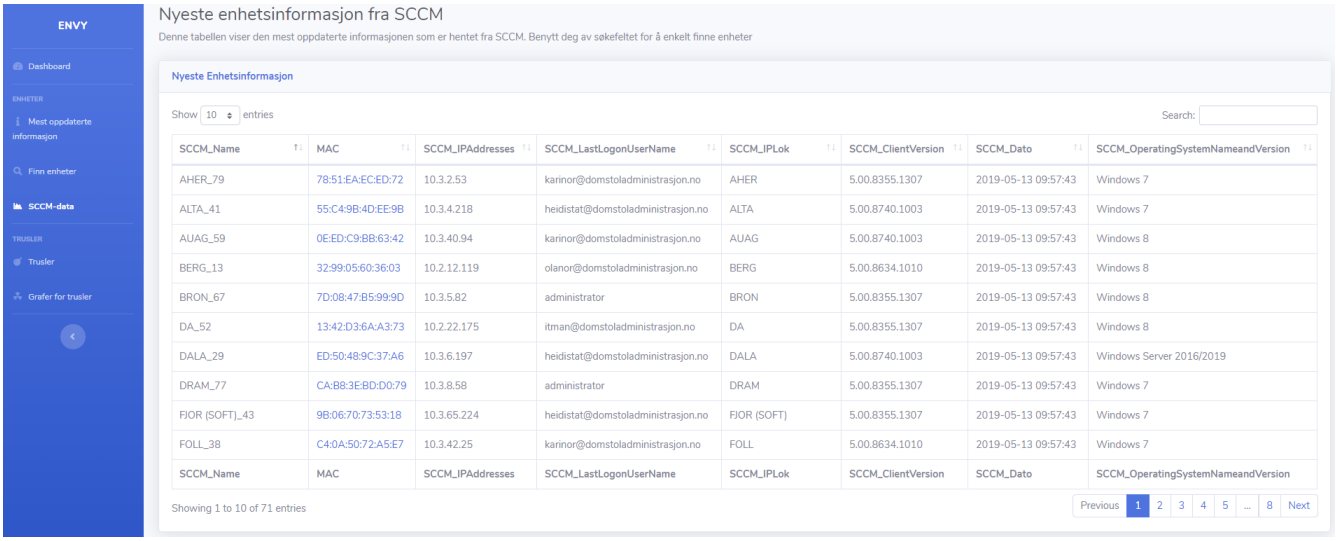


Figur 12: Finn enheter

Øverst til venstre er det et søkefelt. Dette søkefeltet benyttes til å søke etter en spesifikk MAC-adresse. Når en så trykker på "Send" vil all data om denne enheten vises i tabellene nedenfor. Tabellene er delt opp slik at det skilles mellom uthentingsinformasjon fra de 3 ulike tjenestene, SCCM, Airwave og Clearpass. Hver linje i disse tabellene tilsvarer en uthenting fra en av disse tjenestene. I toppen av hver tabell er det mulighet for å velge hvor mange uthentinger en ønsker å se på siden i tillegg til at det er søkefunksjonalitet. Antall enheter som matcher søket vil vises nede til venstre i alle tabellene.

4.4 SCCM-data

Siden viser alle enheter som ble funnet i siste uthenting fra SCCM. Dette er filen “SCCMData.php”.

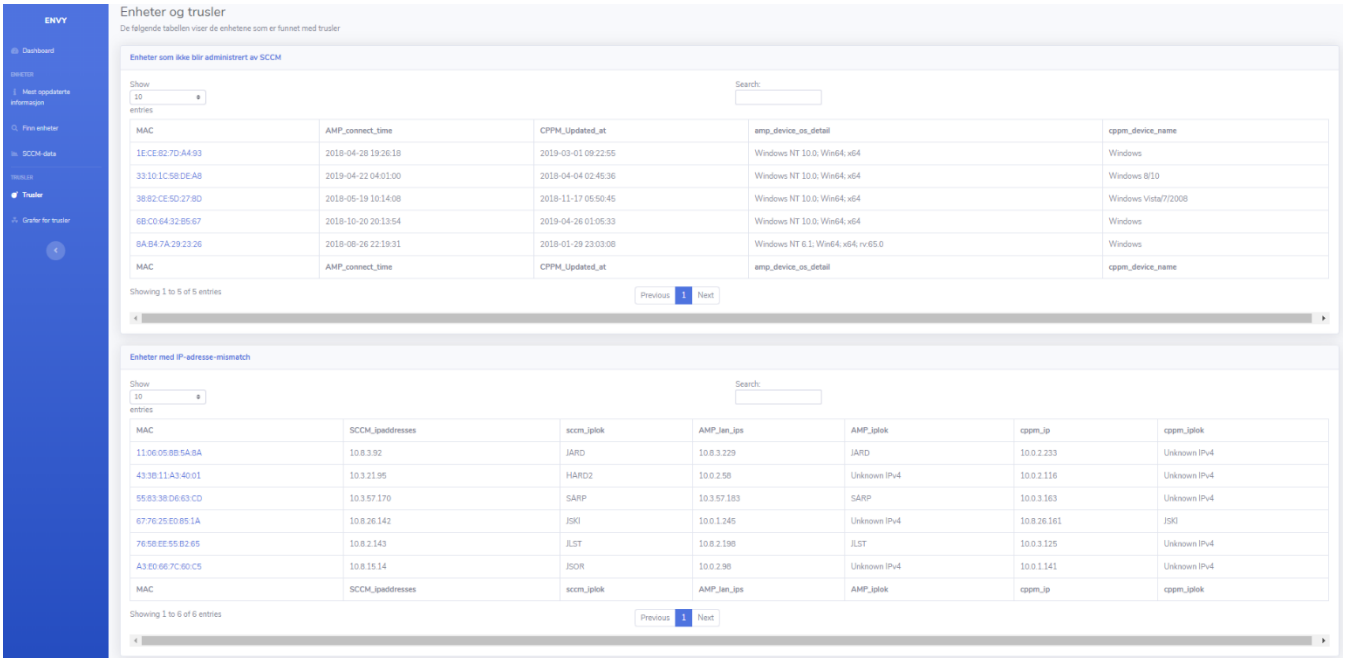


Figur 13: SCCM-data

Øvert stil venstre er det valgmulighet for å angi hvor mange enheter en ønsker å se om gangen. Oppe i høyre hjørne er det et søkefelt som kan benyttes til å søke etter den informasjonen en ønsker å se. Antall enheter som matcher søket vises så nede i venstre hjørne. Nede i høyre hjørne kan en bla mellom de ulike sidene dersom søket har resultert i flere enheter enn det er valgt at skal vises på siden. Data som hentes ut her er noe av informasjonen om hver enhet som ble funnet i siste uthenting fra SCCM.

4.5 Trusler

Siden viser enheter som er flagget som mulige trussel-enheter. Dette er filen “EnheterTrusler.html”.

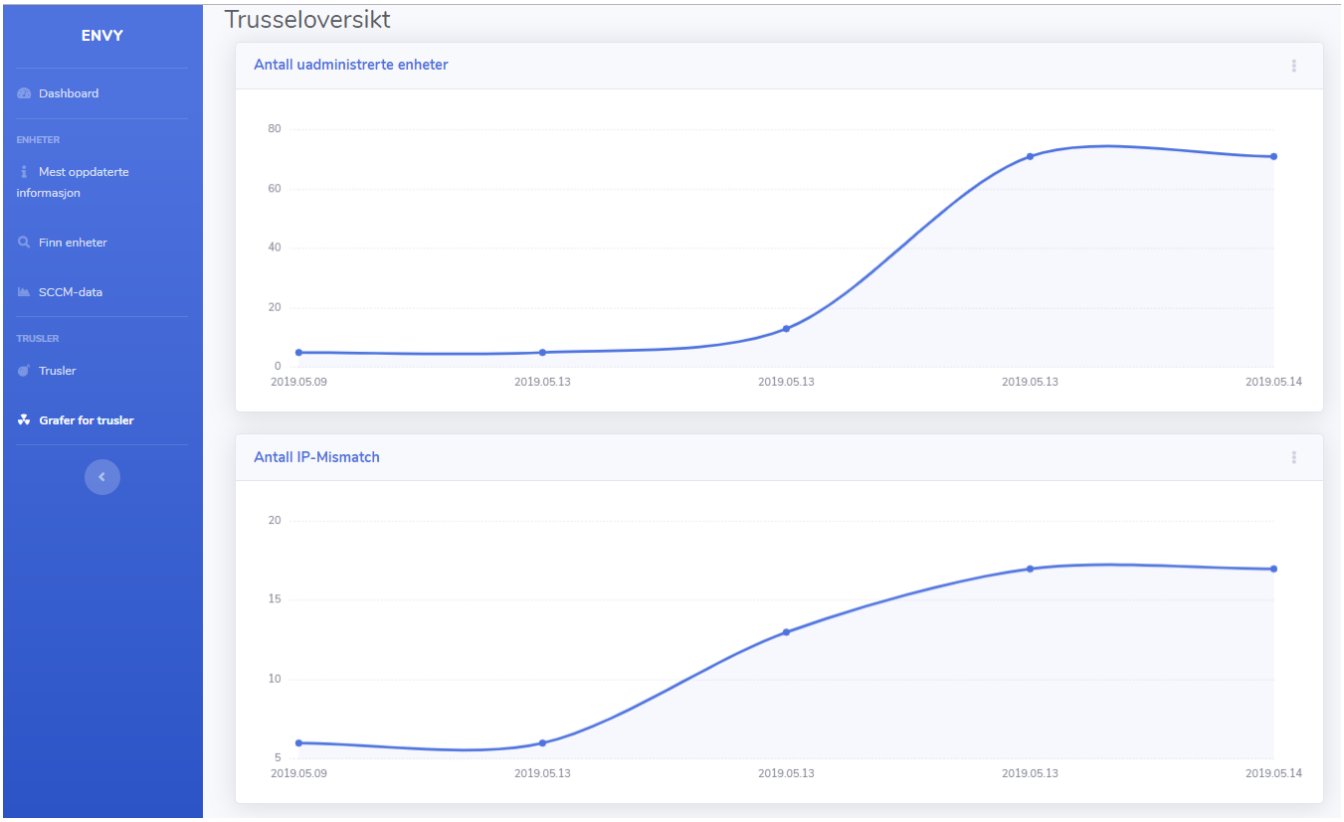


Figur 14: Trusler

Denne siden er delt i to tabeller som representerer de to truslene EnVy leter etter. Øverste tabellen viser alle enheter som ble flagget som “uadministrert” sist gang en analyse ble gjennomført. Nederste tabellen viser alle enheter som ble flagget med truselen “IP-mismatch” sist gang en analyse ble gjennomført. Begge disse tabellene har en valgmulighet oppe i høyre hjørne hvor en kan velge hvor mange enheter en ønsker å se per side. Videre har de en søkefunksjonalitet hvor en kan søke etter spesifikk informasjon, og antall enheter som matcher dette søket vil vises nede i venstre hjørne i begge tabellene. På bunnen av begge tabellene er det funksjonalitet for å bla mellom sidene dersom søket returnerer flere enheter enn antallet som vises på en side. Alle MAC-adresser i begge tabellene er interaktive og sender bruker til siden “Finn enheter” med valgt MAC-adresse som søk.

4.6 Grafer for trusler

Siden viser en oversikt over antall trusler som er funnet hver gang en analyse er blitt gjennomført. Dette er filen "TruslerGraf.html".



Figur 15: Grafer for trusler

Denne siden viser to grafer som representerer antall trusler som er funnet hver gang en analyse er gjennomført. Øverste grafen viser antall enheter som er flagget som uadministrert hver gang en analyse er blitt gjennomført. Den nederste grafen viser antall enheter som er flagget med IP-Mismatch hver gang en analyse er blitt gjennomført. For å se nøyaktig antall enheter per analyse så holder en over ønsket punkt på grafen og antall enheter vil vises i en boks.

5. Teknisk forklaring av kode

Her følger en mer teknisk forklaring av koden til EnVy. Denne forklaringen er skrevet for teknikere, som ønsker å sette seg mer inn i hva de ulike skriptene og funksjonene gjør. Delkapitlene er delt opp i PowerShell og Nettside for å gi et godt skille mellom det som skjer frem til data blir sendt til databasen, og det som skjer når data blir hentet ut fra databasen for visualisering.

5.1 PowerShell

Delkapittelet beskriver de PowerShell-skriptene som EnVy benytter seg av, og er oppdelt til å samsvare med mappestrukturen til koden for å gi god oversikt.

5.1.1 Universalt

Punktet tar for seg de skriptene som sporadisk benyttes i andre skript.

Format-IPLok.ps1

Skriptet definerer funksjonen Format-IPLok. Funksjonen tar inn en IP-addresse, og fjerner den siste gruppen med nummer fra addressen (10.0.0.xxx -> 10.0.0.). Dette brukes for å finne lokasjonen til en IP-addresse med hjelp av tabellen fra Format-IPTable.

Format-IPTable.ps1

Skriptet definerer funksjonen Format-IPTable. Funksjonen henter en liste over IP-scopes og lokasjonen som tilhører fra et eksternt XLSX-dokument, og benytter modulen “psexcel” for å hente informasjonen. Deretter formateres informasjonen til en hashtable, der hver IP-addresse er knyttet til lokasjonen fra XLSX-dokumentet.

Merge-HashtableMacsIps.ps1

Skriptet definerer funksjonen Merge-HashtableMacsIps. Funksjonen benyttes i testsammenheng, og tar inn en hashtable med MAC-addresser (Fra New-HashTableOfMacs), og en hashtable med IP-addresser og lokasjoner (Fra Format-IPTable), og kombinerer disse slik at hver MAC-addresse blir knyttet til en IP-addresse. Dette gjøres for å generere mer realistisk data i testsammenheng.

Stottefunksjoner.ps1

Skriptet definerer mange støttefunksjoner som benyttes i flere av de resterende funksjonen i EnVy.

ConvertFrom-UnixTime

Konverterer et tidspunkt fra unix-timestamp til et DateTime-objekt

New-RandomMac

Genererer en tilfeldig MAC-addresse. Brukes i testsammenheng

New-HashTableOfMacs

Genererer et hashtable med MAC-addresser, med verdien $false knyttet til hver MAC-addresse. Brukes i testsammenheng. Funksjonen genererer et hashtable da det er mer effektivt å fjerne elementer fra et hashtable enn et vanlig array. Brukes i testsammenheng.

New-RandomIP

Genererer en tilfeldig IP i rangen 10.0.1.25 - 10.0.4.250

New-RandomDate

Genererer en tilfeldig DateTime mellom 1/1/2018 og nå. Brukes i testsammenheng.

New-RandomString

Genererer en tilfeldig tekststreng med lengde 10. Brukes i testsammenheng.

Get-AnalyseListe

Henter alle .ps1-filer som ligger i anvist mappe. Listen med navnet til .ps1-filene returneres i et array, og brukes for å utføre analyser.

Get-ConfigFil

Henter konfigurasjonsfilen, og parser denne til et hashtable.

Clone-Object

Funksjon som utfører en deep-copy av et objekt. Funksjonen brukes for å kopiere et hashtable, slik at man kan gjøre endringer på det nye hashtablet, uten å endre originalkopien. (CosmosKey, 2011)

Protect-Passord

Funksjon som konverterer et plaintext-passord til en securestring. Brukes for å lagre et passord kryptert, slik at EnVy kan bruke det. Merk at for at det skal kunne dekrypteres, må det passordet krypteres av samme bruker, og på samme maskin, som det dekrypteres på.

Unprotect-Passord

Funksjon som konverterer en securestring til plaintext. Brukes for å hente et kryptert passord. Funksjonen kan kun dekryptere passordet dersom det ble kryptert av samme bruker, på samme maskin.

Format-MAC

Formaterer en MAC-addresse fra formen AABBCCDDEEFF til AA:BB:CC:DD:EE:FF

IsInAllotedTime

Funksjon som ser om et tidspunkt er mellom to andre tidspunkt. Brukes for å finne ut om en uthenting kan ta sted basert på AllowedTimeFrame-punktene i konfigurasjonsfilen.

Remove-DataEldreEnn1Uke

Funksjon som fjerner filer som er eldre enn anvist fra en mappe. Brukes for å fjerne gamle filer i mellomlageret.

Flip-HashTable

Funksjon som tar inn et hashtable, og returnerer et nytt hashtable der verdiene fra input-hashtable nå er nøkler, og nøklene fra input-hashtable nå er verdier.

Test-Lagringsplass.ps1

Skriptet definerer funksjonen Test-Lagringsplass. Funksjonen tester om ønsket lagringsplass eksisterer, og dersom det ikke gjør det, lager den mappen.

5.1.2 SQL

Dette punktet tar for seg de skriptene som benyttes for å kommunisere med sql-server.

Group-SQLInnsending.ps1

Skriptet deler opp arrays som sendes inn slik at de kan sendes videre til funksjonene som lager SQL-spørringer for innsending til databasen. Per dags dato grupperes alle SQL-innsendinger til ett element per innsending. Funksjonen er nesten i mål, men grunnet tidspress ble det ikke prioritert av prosjektgruppen å ferdigstille denne funksjonen.

New-DBNettsideBruker.ps1

Skriptet lager funksjonen New-DBNettsideBruker som returnerer spørringen for å opprette en databasebruker for login som nettsiden benytter. Funksjonen blir brukt i "InitSQL.ps1".

New-DBUserReadWriteRoleQuery.ps1

Skriptet lager funksjonen New-DBUserToReadWriteRoleQuery som returnerer spørringen for å legge serviceaccaount til i rollene "db_datareader" og "db_datawriter". Funksjonen blir brukt i "InitSQL.ps1".

New-DBUserToServiceAccount.ps1

Skriptet lager funksjonen New-DBUserToServiceAccount. Denne funksjonen returnerer spørringen for å opprette en login mot databasen for serviceaccounten. Det er denne brukeren EnVy vil benytte seg av for å sende data inn til databasen. Funksjonen som lages i dette skriptet blir brukt i "InitSQL.ps1".

New-EditServiceAccountRettigheter.ps1

Skriptet lager funksjonen New-EditServiceAccountRettigheter. Denne funksjonen returnerer spørringen som tilpasser rettighetene til serviceaccounten. Spørringen vil gi tilgang til å benytte "Select" og "Insert" som vil si at brukeren kan sende inn data og hente ut data fra databasen. Funksjonen som lages i dette skriptet blir brukt i "InitSQL.ps1".

New-NettsideBrukerReadRole.ps1

Skriptet lager funksjonen New-NettsideBrukerReadRole. Funksjonen returnerer spørringen som legger nettsidebrukeren til i rollen "db_datareader". Funksjonen blir brukt i "InitSQL.ps1".

New-NettsideBrukerRettigheter.ps1

Skriptet lager funksjonen New-NettsideBrukerRettigheter. Denne funksjonen returnerer spørringen som tilpasser rettighetene til nettsidebrukeren. Spørringen vil gi brukeren tilgang til å kun benytte "Select" som vil si at brukeren kun kan hente ut data fra databasen. Funksjonen som lages i dette skriptet blir brukt i "InitSQL.ps1".

New-NettsideLogin.ps1

Skriptet lager funksjonen New-NettsideLogin som returnerer spørringen som oppretter login mot databasen. Nettsiden vil benytte seg av denne login. Funksjonen som lages i dette skriptet blir brukt i "InitSQL.ps1".

New-ServiceAccountAzure.ps1

Skriptet lager funksjonen New-ServiceAccountAzure som returnerer spørringen som oppretter login mot databasen for serviceaccount. EnVy vil benytte seg av denne login. Funksjonen som lages i dette skriptet blir brukt i "InitSQL.ps1".

New-SqlQuery funksjoner:

Underliggende skripts lager en funksjon hver som benyttes hver gang data blir hentet ut eller skal sendes inn i tabellene i databasen. Det er en funksjon for hver av tabellene i databasen, og grunnen til dette er at SQL-strengen som benyttes mot databasen må formateres til å matche tabellene i databasen. Disse funksjonene blir med andre ord foret med data som skal sendes inn til ønsket tabell og funksjonen returnerer SQL-strengen som benyttes for å sende inn data databasen.

- New-SqlQueryAMP.ps1
- New-SqlQueryCPPM.ps1
- New-SqlQueryEnheter.ps1
- New-SqlQueryEnheterTrusler.ps1
- New-SqlQuerySCCM.ps1
- New-SqlQueryTrusler.ps1

New-SQLTable funksjoner:

Underliggende skripts lager en funksjon hver som benyttes i "InitSQL.ps1" for å opprette tabellene som skal eksistere i databasen. Funksjonene returnerer en SQL-streng hver for de ulike tabellene. Navnet på funksjonene er identisk navnet på skriptet.

- New-SQLTableAMP.ps1
- New-SQLTableCPPM.ps1
- New-SQLTableEnheter.ps1
- New-SQLTableEnheterTrusler.ps1
- New-SQLTableSCCM.ps1
- New-SQLTableTrusler.ps1

Send-QueryToDatabase.ps1

Skriptet lager funksjonen Send-QueryToDatabase. Funksjonen kobler seg opp mot databasen og sender inn ønsket spørring. Dersom det blir spurt om å hente ut data sjekkes det om data blir hentet ut, og dersom det blir der så returneres denne dataen. Denne funksjonen blir benyttet hver gang data skal sendes inn eller hentes ut fra databasen.

Test-SqlConnection.ps1

Skriptet lager funksjonen Test-SqlConnection. Funksjonen tester oppkobling mot databasen, og returnerer resultatet. Dersom oppkobling er vellykket returneres "true", og dersom oppkobling mislykkes returneres "false"

5.1.3 AMP

Punktet tar for seg de skriptene som benyttes for uthenting og formatering av nodeinformasjon fra AMP.

Get-AMPData.ps1

Skriptet definerer funksjonen Get-AMPClients. Denne funksjonen kobler seg til Airwave-serveren, og returnerer rapporten som skal hentes, i XML-format. Dersom rapporten som hentes er den som ble definert i oppstartsguiden, vil innholdet som skal benyttes ligge i rapportens ".report.pickled_user_inventory", som sendes til Format-AMPData.

Format-AMPData.ps1

Skriptet definerer funksjonen Format-AMPClient. Denne funksjonen tar inn en rapport fra Get-AMPData, og formaterer denne til å bli et array med PSCustomObjects. I tillegg til å legge inn attributtene som ligger i rapporten, vil denne funksjonen også legge på ekstra attributter, som IP-lokasjon, og dato for uthentingen. Til slutt returneres et array med formaterte objekter, som kan sendes videre til en av SQL-funksjonene, eller Merge-NodeData.

5.1.4 CPPM

Punktet tar for seg de skriptene som benyttes for uthenting og formatering av nodeinformasjon fra Clearpass.

Get-CPPMApiAccessToken.ps1

Skriptet definerer funksjonen Get-CPPMApiAccessToken. Denne funksjonen kontakter API-klienten på Clearpass-serveren, og mottar et adgangstoken som kan brukes til å utføre uthenting av data i funksjonen Get-CPPMEndPoints.

Get-CPPMEndpoints.ps1

Skriptet definerer funksjonen Get-CPPMEndpoints. Denne funksjonen benytter adgangstokenet som ble hentet av Get-CPPMApiAccessToken, til å kontakte Clearpass sitt /insight/endpoint API. Som standard vil funksjonen hente ut all informasjon om alle endpoints som er funnet i løpet av de siste 24-timene, men tidsrammen kan endres med inputen startTime. Rådataen som hentes av denne funksjonen kan sendes direkte inn til Format-CPPMEndpoints, for å formatere dataen til et brukbart format.

Format-CPPMEndpoints.ps1

Skriptet definerer funksjonen Format-CPPMEndpoints. Denne funksjonen tar inn rådata fra Get-CPPMEndpoints, og formaterer denne til å bli et array med PSCustomObjects. I tillegg til å legge inn attributtene som ble hentet fra APIet, vil denne funksjonen også legge på ekstra attributter, som ip-lokasjon, og dato for uthenting. Til slutt returneres et array med formaterte objekter, som kan sendes videre til en av SQL-funksjonene, eller Merge-NodeData.

5.1.5 SCCM

Punktet tar for seg de skriptene som benyttes for uthenting og formatering av nodeinformasjon fra SCCM.

Get-SCCMKlienter.ps1

Skriptet definerer funksjonen Get-SCCMKlienter. Denne funksjonen åpner en PSSession mot SCCM-serveren, med kerberos-authentication. Dette betyr at brukeren som kjører funksjonen må være en bruker som har minimum de tilgangen service-brukeren som er beskrevet i kapittel 2.1.1. Gjennom remote-sessionen som er laget vil funksjonen utføre SQL-spørringen som er beskrevet i 2.1.1, og rådataen som hentes kan sendes direkte videre til Formater-SCCMData.

Formater-SCCMData.ps1

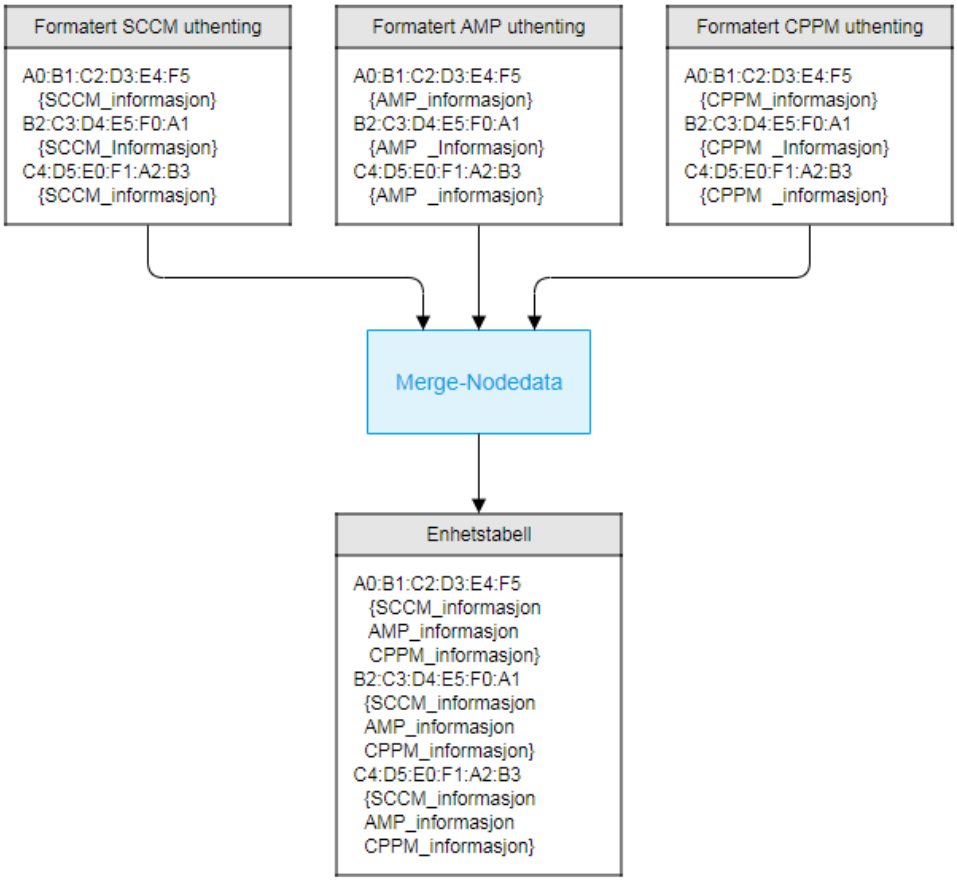
Skriptet definerer funksjonen Formater-SCCMData. Denne funksjonen tar inn rådata fra Get-SCCMKlienter, og formaterer denne til å bli et array med PSCustomObjects. I tillegg til å legge inn attributtene som ble hentet med Queryen, vil denne funksjonen også legge på ekstra attributter, som IP-lokasjon, og dato for uthenting. Til slutt returneres et array med formaterte objekter, som kan sendes videre til en av SQL-funksjonene, eller Merge-NodeData.

5.1.6 Databehandling

Dette punktet tar for seg alle skriptene som benyttes for å behandle den formaterte dataen som er hentet fra uthetningsfunksjonene.

Merge-NodeData.ps1

Skriptet definerer funksjonen Merge-NodeData. Denne funksjonen tar inn en samling av formaterte datasett fra en eller flere av formateringsfunksjonene (Formater-SCCMData, Format-AMPData, Format-CPPMEndpoints), og kombinerer disse til en enhetstabell, som samler informasjon fra de tre kildene, basert på MAC-addressen til enhetene. Formålet med dette er å kunne finne ut hvor mange unike enheter det finnes totalt fra alle uthentingene, og for å kunne enklere loope gjennom dataen i løpet av analysene. I løpet av skriptet “Hent Utdata.ps1” vil EnVy mellomlagre informasjonen i enhetstabellen lokalt på maskinen, og enhetstabellen vil bli brukt for å sende informasjonen til tabellen “Enheter” i databasen.



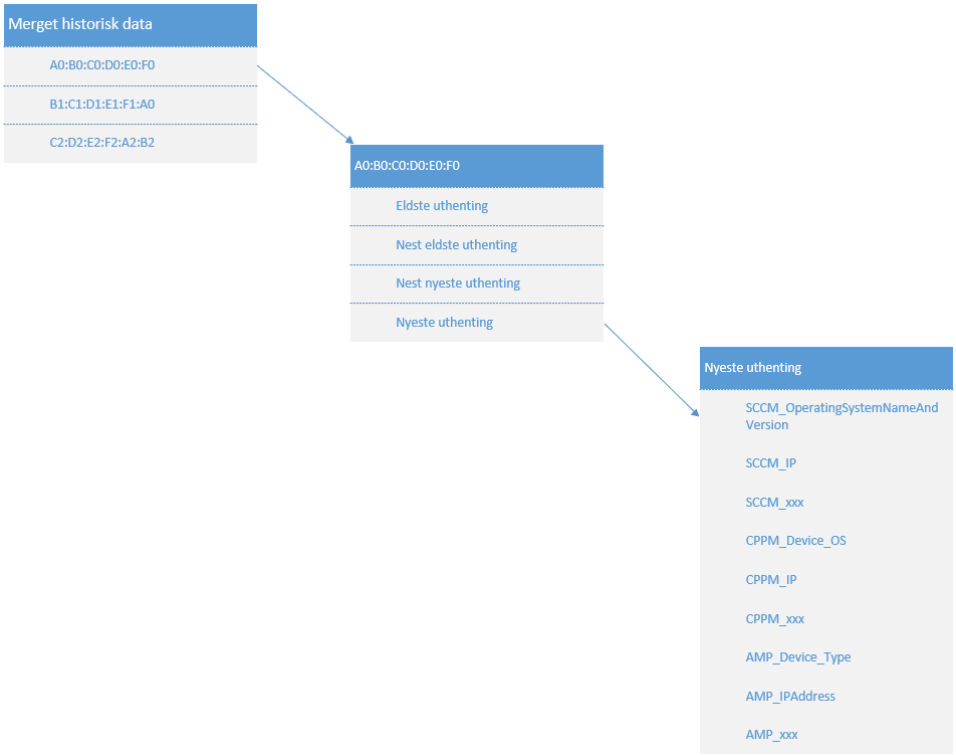
Figur 16: Merge-NodeData

Get-HistoriskData.ps1

Skriptet definerer funksjonen Get-HistoriskData. Funksjonen henter innholdet i alle ".uthenting"-filer som ligger i mellomlageret, og returnerer et array som inneholder alle uthentingene. Dette arrayet blir brukt i funksjonen Merge-HistoriskData.

Merge-HistoriskData.ps1

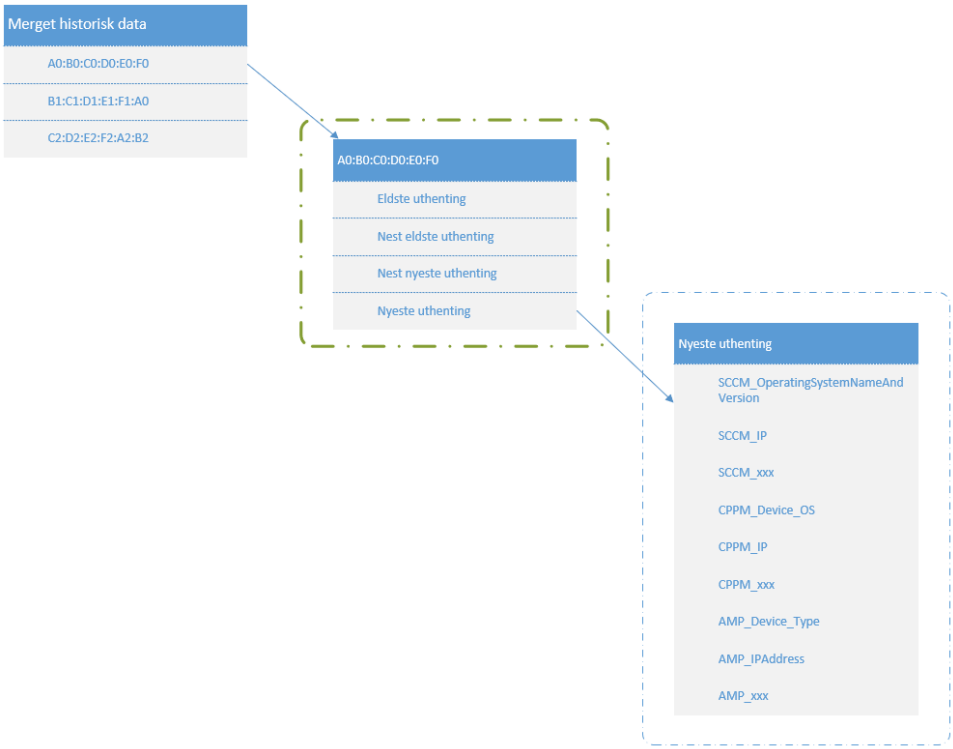
Skriptet definerer funksjonen Merge-HistoriskData. Funksjonen sammenstiller all informasjonen som ble hentet av Get-HistoriskData, til en enhetstabell som inneholder alle uthentinger for hver mac-addresse, som beskrevet i figur xx. Enhetstabellen her blir sendt til Test-EnhetsTabell, for å utføre analyse av informasjonen som er lagret.



Figur 17: Merge-HistoriskData

Test-EnhetsTabell.ps1

Skriptet definerer funksjonen Test-EnhetsTabell. Funksjonen vil gå gjennom enhetstabellen produsert av Merge-HistoriskData, og utføre alle tester som er funnet av funksjonen Get-AnalyseListe. Hver analysefunksjon vil få sendt inn et array av uthentinger, som er spesifikke til en enhet, som vist i figur XZ.



Figur 18: Test-EnhetsTabell

Format-AnalyseResultat.ps1

Skriptet definerer funksjonen Format-Analyseresultat. Funksjonen går gjennom resultatene fra Test-EnhetsTabell, og formaterer resultatene til en redusert enhetstabell som inneholder enhetene som det ble funnet trusler på, og informasjon om truslene som ble funnet. Denne enhetstabellen kan deretter bli sendt videre til Group-SQLInnsending > New-SqlQueryEnheterTrusler > Send-QueryToDatabase.

5.1.7 Analyser

Dette punktet tar for seg alle analyser som utføres på den lagrede informasjonen. Alle analyser er egne funksjoner, som kan utføres utenfor den vanlige flyten til EnVy om ønskelig.

Analyse-EnhetManglerIDomene.ps1

Skriptet definerer funksjonen Analyse-EnhetManglerIDomene. Funksjonen er en analyse som skal fastslå om en enhet som er funnet i en av uthentingene som ligger i mellomlageret, ikke er blitt administrert av SCCM. For å gjøre dette går den gjennom datasettet, og dersom den ikke finner en SCCM-uthenting, returnerer den at trusselen er funnet.

Analyse-IPRange.ps1

Skriptet definerer funksjonen Analyse-IPRange. Funksjonen er en analyse som skal fastslå om en enhets IP-lokasjoner matcher. For å gjøre dette ser analysen gjennom datasettet og sammenligner IP-lokasjonene som er funnet. Dersom de ikke matcher, returnerer analysen at trusselen er funnet.

5.1.8 Overliggende skript

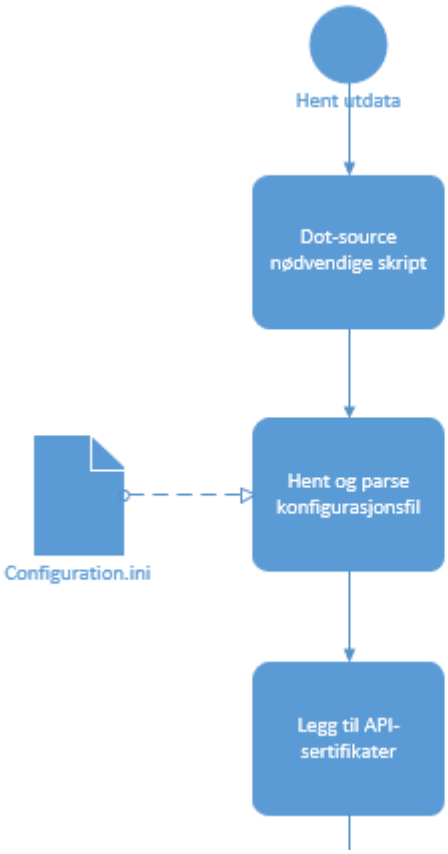
Dette punktet tar for seg de overliggende scriptene, som benytter funksjonene til å utføre innhenting og analyse av informasjon. Skriptene “Hent utdata” og “Analyser lagretdata” er hoveddelen av EnVy, og utfører til sammen den daglige bruken av EnVy.

Hent Scripts.ps1

Skriptet vil hente alle skript i alle undermapper, og kjøre disse. Brukes i testsammenheng for å initialisere alle skriptene i terminalen. Er ikke nødvendig å bruke i daglig drift.

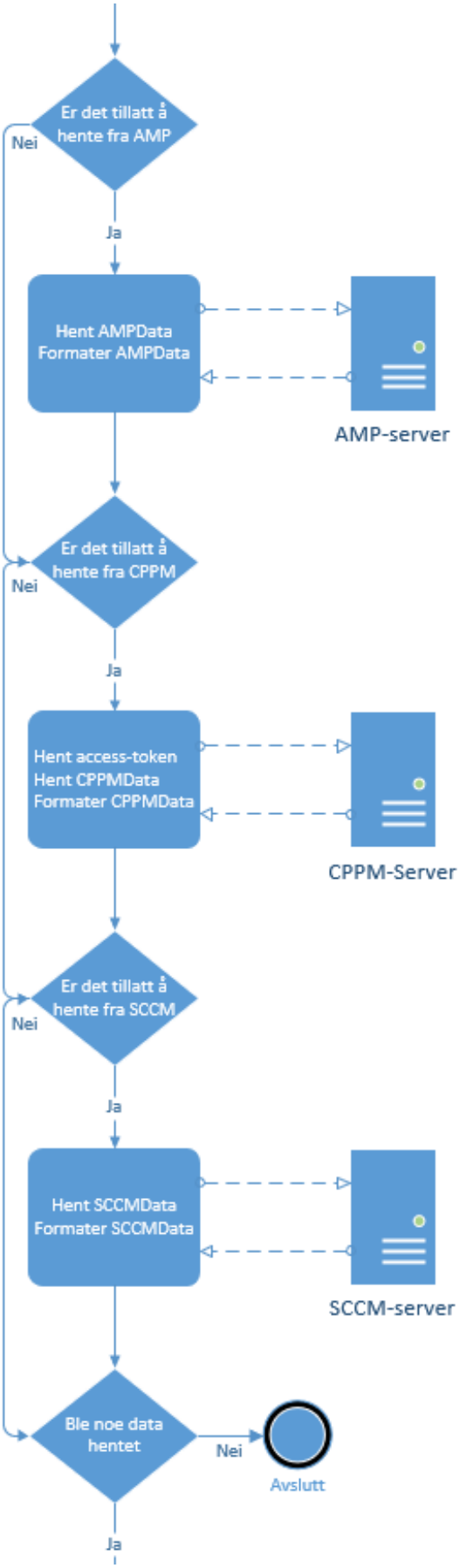
Hent utdata.ps1

Hovedskriptet som utfører informasjonshentingen til EnVy. Skriptet starter med å dot-source alle skript i undermappene. Deretter hentes og parses konfigurasjonsfilen, og alle nødvendige punkter lagres som variabler. Som siste del av initialiseringen legges det til nødvendige sikkerhetssertifikater, slik at EnVy kan koble seg til APIene til Clearpass og Airwave.



Figur 19: Hent utdata, del 1

Etter initialiseringen utføres uthentinger for Airwave, Clearpass, og SCCM sekvensielt. Dersom AllowedTimeFrame-punktene fra konfigurasjonsfilen ikke tillater uthenting, vil skriptet ikke hente ut informasjon fra de påvirkede kildene.

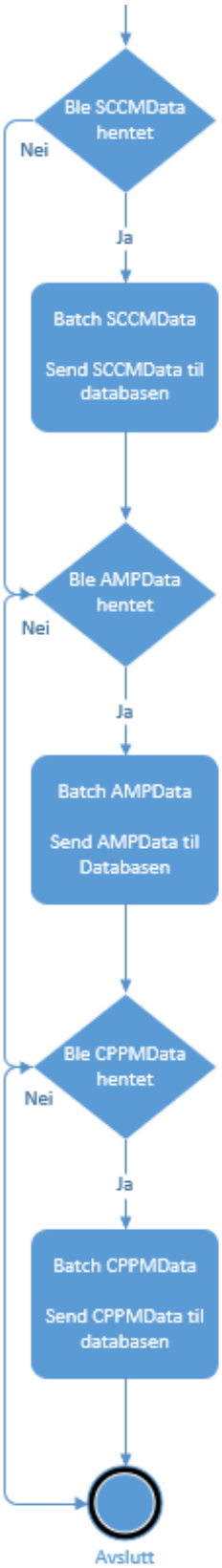


Figur 20: Hent utdata, del 2

Etter å ha hentet all tilgjengelig informasjon, merges informasjonen, og den mergede informasjonen blir mellomlagret.

Figur 21: Hent utdata, del 3

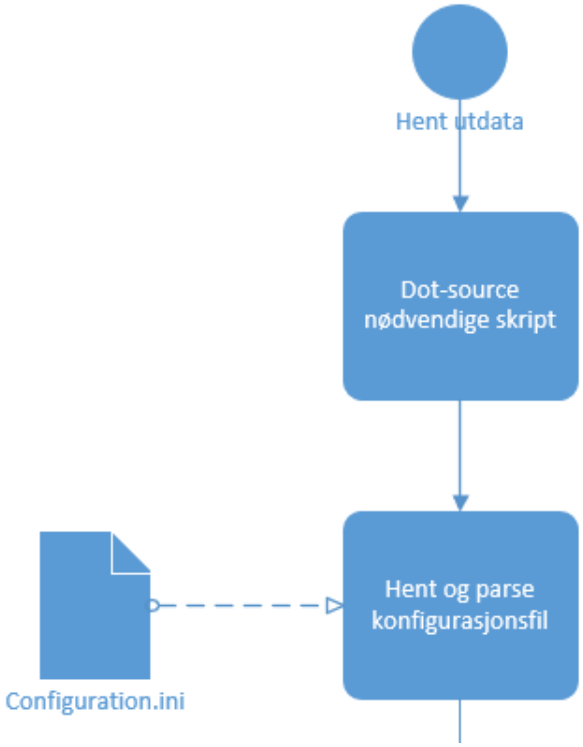
Til slutt blir informasjonen sendt til databasen. Først sendes listen av unike MAC-addresser til tabellen enheter i databasen. Deretter sendes SCCM-, Airwave-, og Clearpass-data inn sekvensielt.



Figur 22: Hent utdata, del 4

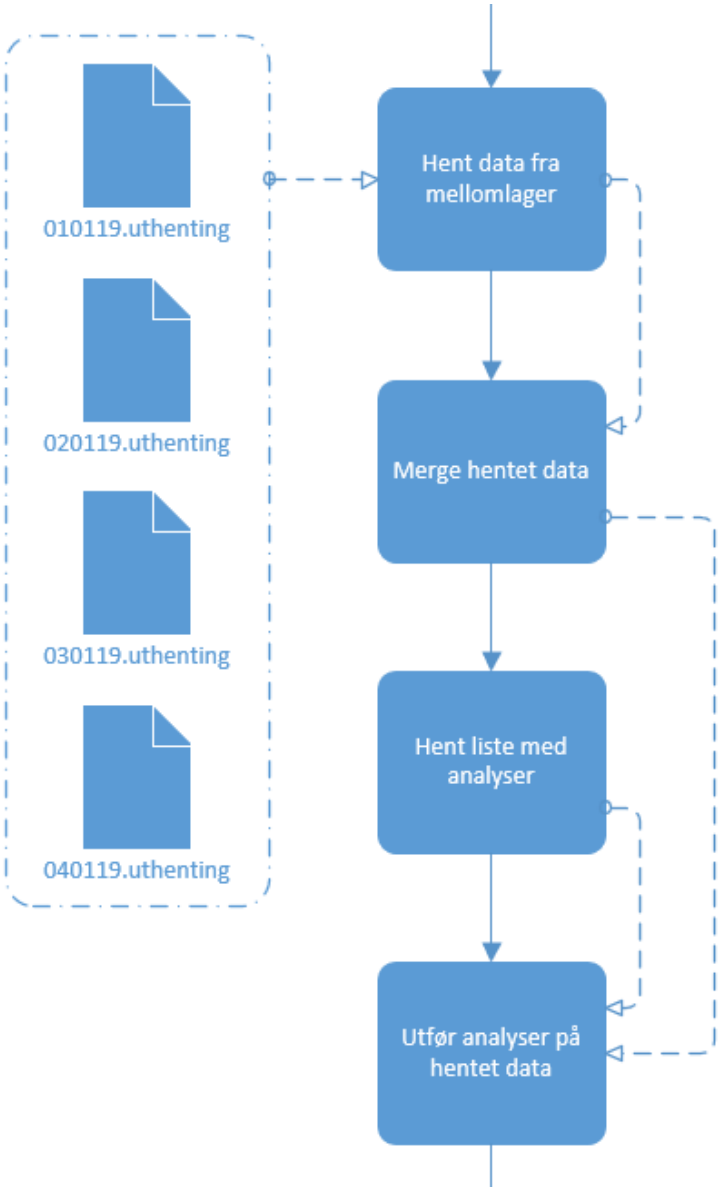
Analyser lagretdata.ps1

Hovedskriptet som utfører analysen til EnVy. Skriptet starter med å dot-source alle skript i undermappene. Deretter hentes og parses konfigurasjonsfilen, og alle nødvendige punkter lagres som variabler.



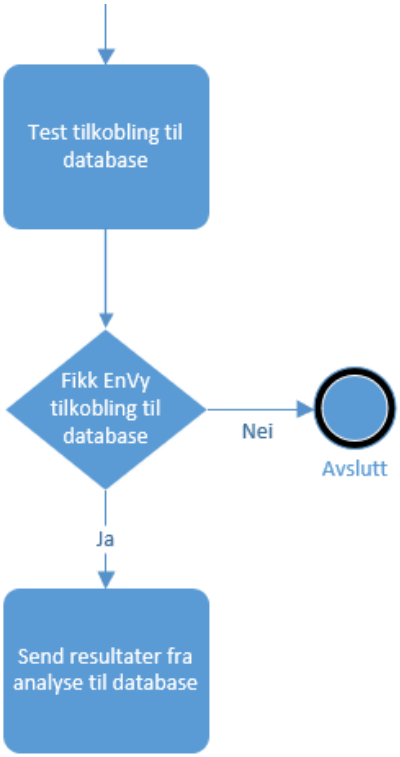
Figur 23: Analyser lagret data, del 1

Etter initialiseringen hentes all historisk data fra mellomlageret, og informasjonen merges. Listen med analyser som skal utføres hentes, og skriptet kjører Test-Enhetstabell for å analysere dataen.



Figur 24: Analyser lagret data, del 3

Etter formatering, sendes resultatet til tabellen Enheter-Trusler i databasen.



Figur 25: Analyser lagret data, del 4

InitSQL.ps1

Skriptet benyttes for å initialisere databasen slik at tabeller og brukere samsvarer med EnVy. De truslene det letes etter blir her sendt inn i databasen, og dette gjøres som en test på at servicebrukeren fungerer. Det er tiltenkt at dette er det første skriptet som kjøres ved implementasjon av EnVy. Hvordan dette skriptet fungerer er godt beskrevet i punktet 2.2.2 Database og underliggende punkter.

Lag-TestData.ps1

Skript som brukes i testsammenheng. Skriptet benytter generatorfunksjonene for å generere uthentinger. For hver dag som skal genereres blir et sett med uthentinger laget, og disse mellomlagres og sendes til databasen. Etter å ha generert mengden data som er spesifisert, utføres analyser på den genererte dataen, og resultatet fra analysene sendes til databasen. Dette skriptet blir ikke brukt i daglig bruk av EnVy, men kan brukes for testing og videreutvikling.

5.1.9 Generatorer

Punktet tar for seg generering av data for testing av EnVy. De tre funksjonene benyttes i Lag-TestData, og genererer data i tilsvarende format som en faktisk uthenting.

New-AMPFakeData

Skriptet definerer funksjonen New-AMPFakeData. Brukes i testsammenheng. Funksjonen genererer et sett med data som tilsvarer en formatert uthenting fra Airwave. Alle attributter som er generert tilsvarer det som ville blitt hentet av Airwave, for å best mulig kunne etterligne en faktisk uthenting.

New-CPPMFakeData

Skriptet definerer funksjonen New-CPPMFakeData. Brukes i testsammenheng. Funksjonen genererer et sett med data som tilsvarer en formatert uthenting fra Clearpass. Alle attributter som er generert tilsvarer det som ville blitt hentet fra Clearpass, for å best mulig kunne etterligne en faktisk uthenting.

New-SCCMFakeData

Skriptet definerer funksjonen New-SCCMFakeData. Brukes i testsammenheng. Funksjonen genererer et sett med data som tilsvarer en formatert uthenting fra SCCM. Alle attributter som er generert tilsvarer det som ville blitt hentet av SCCM, for å best mulig kunne etterligne en faktisk uthenting.

5.2 Nettside

Delkapittelet beskriver koden som EnVy benytter seg av for å visualisere data, og er oppdelt til å samsvare med mappestrukturen til koden for å gi god oversikt. Nettsiden er utviklet ut ifra malen SB Admin 2 (Start Bootstrap, 2019). Denne malen benytter seg av NodeJS og Gulp, noe som må installeres på vertsmaskinen til nettsiden. Videre har prosjektgruppen utviklet deler av nettsiden i PHP, noe som gjør at maskinen også må kunne kjøre dette. Valget falt på denne malen da den hadde god dokumentasjon og var enkel å tilpasse eget bruk. Prosjektgruppen fikk også benyttet tidligere erfaringer med PHP og JavaScript ved å benytte denne malen.

5.2.1 CSS

CSS-filene i mappen CSS er hentet fra malen SB Admin 2, og blir brukt på de ulike nettsidene for å tilpasse utseende i form av farger, skrifttype, skriftstørrelse, rammer, avstander mellom bokser osv.

5.2.2 JavaScript

Punktet tar for seg alle Javascript-filer i mappen JS.

Dashboard grafer:

Underliggende skript lager grafene som vises i "Index.html". Disse skriptene benytter seg av PHP-skript for å hente inn data fra databasen. Denne dataen blir så brukt til å lage labels som vises under grafen og tilhørende punkter som utgjør selve grafen.

- Amp-area.js - Lager "Enheter i Airwave" og benytter seg av "GetAntallAMP.php".
- Cppm-area.js - Lager "Enheter i Clearpass" og benytter seg av "GetAntallCPPM.php"
- Sccm-area.js - Lager "Enheter i SCCM" og benytter seg av "GetAntallSCCM.php"

Grafer for trusler:

Underliggende skript lager grafene som vises i "TruslerGraf.html". Disse skriptene benytter seg av PHP-skript for å hente inn data fra databasen. Denne dataen blir så brukt til å lage labels som vises under grafen og tilhørende punkter som utgjør selve grafen.

- Ip-area.js - Lager "Antall IP-Mismatch" og benytter seg av "GetAntallIP.php"
- Uadm-are.js - Lager "Antall uadministrerte enheter" og benytter seg av "GetAntallUadm.php"

Chart-pie-maker.js

Skriptet definerer funksjonen MakeChart(). Funksjonen er en modifisert versjon av SB Admin 2 sin pie-chart-demo.js. Først blir en subfunksjon, recColortable definert. Denne subfunksjonen vil øke størrelsen på et array med farger til det er nok farger til å kunne farge inn hver skive av et pie-chart. Deretter hentes informasjon fra databasen, og funksjonen utformer et pie-chart basert på informasjonen som hentes. Denne funksjonen benyttes i index.html.

Datatables-init.js

Skriptet kaller DataTables sin JQuery plugin, og brukes på sider hvor det benyttes dataTables.

HentfraDatabase.js

Skriptet definerer flere funksjoner som benyttes for å hente informasjon fra databasen.

GetSingle()

Funksjonen tar inn en SQL-spørring, og en divID. Spørringen blir sendt til GetSingle.php, og resultatet blir lagt i innerHTML til div-en med valgt divID.

GetHard()

Funksjonen tar inn en divID, og utfører spørringen i HentAltHardt.php. Resultatet av spørringen blir formatert som en tabell, og lagt i InnerHTML til div-en med valgt divID.

GetThreat()

Funksjonen tar inn filepath til en PHP-fil, og en divID. Spørringen i PHP-filen blir utført, formatert som en tabell, og lagt i innerHTML til div-en med valgt divID.

Getenhet()

Funksjonen tar inn en MAC-addresse, navnet på en kilde informasjon hentes fra, og en divID. MAC-addressen og navnet på kilden blir sendt til GetEnhet.php, og resultatet av spørringen blir formatert som en tabell, og lagt i div-en med valgt divID sin innerHTML.

Sb-admin2.js og Sb-admin2.min.js

Disse er javascriptfiler som blir brukt av malen, SB Admin 2. Disse er ikke modifisert fra malen.

5.2.3 PHP

Punktet tar for seg de PHP-filene som benyttes for å hente ut data fra databasen.

Connect.php

Skriptet åpner en PDO-connection til databasen, for å hente ut data. Det er i denne filen passordet til service-acocunten til nettsiden lagres. Denne filen blir benyttet av alle andre PHP-filer som skal koble seg til databasen.

JsonSporring.php

Skriptet definerer funksjonen JsonSporring. Funksjonen benytter seg av connect.php til å åpne en tilkobling til databasen, og kjører deretter spørringen som ble sendt inn som input i funksjonen. Svaret fra spørringen encodes som JSON, og blir echoet ut av funksjonen. Til slutt lukkes tilkoblingen til databasen. Funksjonen benyttes der reultatet av en spørring skal vises i en figur. Spørringene som sendes inn ligger i følgende php-filer:

- GetSCCMOS.php - Henter antall enheter med hvert OS fra SCCM
- GetAMPOS.php - Henter antall enheter med hvert OS fra AMP
- GetCPPMOS.php - Henter antall enheter med hvert OS fra CPPM
- GetAntallSCCM.php - Henter antall enheter fra SCCM per dato
- GetAntallAMP.php - Henter antall enheter fra AMP per dato
- GetAntallCPPM.php - Henter antall enheter fra CPPM per dato
- GetAntallIP.php - Henter antall enheter med IP-mismatch per dato
- GetAntallUadm.php - henter antall uadministrerte enheter per dato

TabellSporring.php

Skriptet definerer funksjonen TabellSporring. Funksjonen benytter seg av connect.php til å åpne en tilkobling til databasen, og kjører deretter spørringen som ble sendt inn som input i funksjonen. Svaret fra spørringen blir deretter lagt inn i en HTML-tabell, og hele tabellen blir echoet ut av funksjonen. Til slutt lukkes tilkoblingen til databasen. Funksjonen benyttes der resultatet av spørringen skal vises i en datatable. Spørringene som sendes inn ligger i følgende php-filer:

- GetNyesteSCCM.php - Henter lettlest data fra den siste uthentingen fra SCCM.
- GetTrussel1.php - Henter alle enheter fra den nyeste analysen, der analysen fastslo at enheten ikke ble administrert av SCCM
- GetTrussel2.php - Henter alle enheter fr aden nyeste analysen, der analysen fastslo at enheten hadde IP-mismatch
- HentAltHardt.php - Henter alle enheter med alle verdier, fra siste innsending

GetSingle.php

Skriptet vil utføre spørringen som sendes inn i $_REQUEST-variablen. Skriptet returnerer en enkelt verdi, og er ment å brukes for spørringer som kun skal returnere en enkelt verdi, som antallet totale enheter. Benyttes av javascript-funksjonen GetSingle(), som ligger i HentfraDatabase.js.

GetEnhet.php

Skriptet vil hente ut all informasjon om en enkeltenhet, basert på en MAC-addresse som sendes inn i $_REQUEST[“q”], fra kilden som baseres på $_REQUEST[“k”]. Informasjonen som hentes vil bli formatert i en HTML-tabell, som blir echoet ut. Benyttes av javascript-funksjonen Getenhet(), som ligger i HentfraDatabase.js

5.2.4 SCSS

I mappen SCSS ligger SASS-filer som er brukt av malen SB Admin 2 for å endre utseende til nettsiden. Disse er ikke modifisert fra malen.

5.2.5 Vendor

I mappen vendor ligger alle filer som kommer direkte fra malen SB Admin 2. Disse er ikke modifisert fra malen, og inneholder følgende:

- Bootstrap
- Charts.js
- Datatables
- Fontawesome-free
- Jquery
- Jquery-easing

5.2.6 Overliggende kode

Punktet tar for seg koden som befinner seg ytterst i mappestrukturen.

De ulike nettsidene:

Underliggende html og php filer er de sidene som sluttbruker vil se. Disse filene er bygd opp av html for å dele opp det som skal vises, css for å tilpasse utseende i form av farger, skriftstørrelse osv, PHP for uthenting av data fra databasen og javascript for fremstilling av figurer. Nettsidene er laget ut ifra rammeverket Bootstrap og malen SB Admin 2.

- Index.html
- TruslerGraf.html
- Nyesteinfo.php
- FinnEnkeltenhet.php
- Sccmdata.php
- EnheterTrusler.html

Gulpfile.js

Dette er et driftsverktøy som fulgte med malen, men kan være nyttig dersom EnVy skal videreutvikles. Verktøyet kan benyttes til å bundle javascript eller css, minifisere libraries og stylesheets eller refreshe nettsiden når en fil blir lagret.

SB Admin 2 License

Lisensfilen til malen SB Admin 2. Malen er utgitt under en MIT License, som tillater all bruk av software, så lenge lisensfilen er med.

Package-lock.json

Dette benyttes av NodeJS og sier eksakt versjon av hver modul som skal installeres. Dette gjør at når og hvor EnVy installeres ikke har noe å si ettersom en vil få samme resultatet hver gang.

Package.json

Dette benyttes av NodeJS og sier hvilke moduler som skal installeres. Her oppgis det ikke hvilken versjon, noe som vil si at her installeres kun minstekravet for modulen.

Readme.md

Readme for malen SB Admin 2. Filen inneholder brukerveiledning for tilpasning av malen.

6. Videreutvikling

EnVy er utviklet basert på PowerShell Best Practices (Jones, Penny, Perz, Bennet & Powershell Community, 2019), en uoffisiell guide på hvordan man skal utvikle god kode. Dette er gjort for å sikre gode muligheter for vedlikehold og etterutvikling. Uten å gjøre store endringer i verktøyet, men med noe scriptarbeid, kan man legge inn nye datakilder, analyser, og nettsider.

6.1 Nye datakilder

Ettersom EnVy er laget for å finne noder i nettverket, er det nødvendig at alle enheter som skal bli hentet av EnVy har en MAC-addresse.

For å legge til nye datakilder må man først lage en funksjon som tilsvarer Get-AMPData\Get-SCCMData\Get-CPPMData. Funksjonen må hente informasjonen fra den nye datakilden, slik at powershell kan behandle den. Deretter må informasjonen som er hentet bli formatert til et array med PSCustomObjects der informasjonen som hentes blir gjort til attributter i objektet. Når dette er gjort vil den formaterte informasjonen kunne sendt med til merge-nodedata, og EnVy vil sende dette til databasen.

Etter å ha laget funksjonene må man oppdatere “Hent Utdata.ps1”, og legge inn uthenting- og formateringsfunksjonene. I tillegg kan man gå inn i Merge-Nodedata.ps1, og legge til en identifiserende verdi, som gjør at dataen enklere kan bli benyttet i analyser senere.

Database

6.2 Nye analyser

For å legge inn nye analyser er det viktig å vite hvordan informasjonen som blir sendt til analysene ser ut. Informasjonen som sendes til analysene er et array med objekter, som inneholder alle uthentinger som skjedde i løpet av en dag. Analysen må derfor enten gå gjennom arrayet som blir sendt inn, eller hente ut ett spesifik datapunkt, som for eksempel den siste uthentingen.

Til sist er det nødvendig å vite hva EnVy forventer å få som svar fra en analyse. Alle analyser må returnere følgende: @($trusselD, $resultat). Her må trusselID samsvare med trusselID til trusler analysen finner, i databasetabellen “Trusler”.

6.3 Nye nettsider

For å legge inn nye nettsider kan man benytte seg av de allerede eksisterende nettsidene og skriptene, og modifisere disse til å vise det ønskede resultatet.

6.4 Anbefalinger til videre arbeid

Delkapittelet tar for seg prosjektgruppens anbefalinger til Domstoladministrasjonen om videre arbeid med EnVy.

6.4.1. Server-side processing av datatables på nettsiden

I datatabellene på nettsiden er det mye data som må lastes inn. Dersom mengden data som hentes fra databasen blir stor, kan dette påvirke ytelsen til nettsiden. Datatables.net har innebygde funksjoner for Server-side processing, noe som kan implementeres dersom mengden data eventuelt begynner å påvirke ytelsen til nettsiden (Datatables.net, 2019).

6.4.2. Ferdigstilling av Group-SQLInnsending.ps1

Funksjonen Group-SQLInnsending er nesten ferdigstilt, men grunnet tidspress ble den ikke prioritert ferdig til prosjektets ende. Om funksjonen ferdigstilles vil man kunne sende flere enn en enhet inn i

databasen per spørring, og ifølge prosjektgruppens undersøkelser er den mest effektive størrelsen på en innsending 25 enheter.

6.4.3 Nye analyser og datakilder

EnVy er godt rustet til å behandle nye datakilder, og å utføre nye analyser. Dersom verktøyet skal brukes, kan det være lønnsomt å hente informasjon fra andre datakilder, som Citrix eller antivirusprogrammer, enten for å utføre analyser på informasjonen, eller bare for å samle all informasjonen på en plass.

6.4.4 Effektivisering av SQL-kode

Mange av scriptene som benyttes i "InitSQL.ps1" er veldig like og kan gjøres mer effektive. Samme kode blir brukt flere ganger istedenfor at det er opprettet en felles funksjon. Dette ble ikke prioritert ettersom skriptene kun benyttes en gang for initialisering av databasen.

7. Kilder

Don Jones, Matt Penny, Carlos Perez, Joel Bennet og PowerShell Community (2019). *The Unofficial PowerShell Best Practices and Style Guide.* Available at: https://github.com/PoshCode/PowerShellPracticeAndStyle (Accessed: 05. March 2019)

DataTables.net (2019). *Server-side processing (5,000,000 rows).* Avaliable at: https://datatables.net/extensions/scroller/examples/initialisation/server-side_processing.html (Accessed: 13. April 2019)

Start Bootstrap (2019). *SB Admin 2*. Available at: https://startbootstrap.com/themes/sb-admin-2/ (Accessed: 29. April 2019)

NodeJS (2019). NodeJS. Available at: https://nodejs.org/en/ (Accessed: 29. April 2019)

CosmosKey (2011). *Deep copy a dictionary (hashtable) in PowerShell*. Avaliable at: https://stackoverflow.com/a/7475744 (Accessed: 15.05.2019)

Kildekode

Kildekoden er lagt ved som en zippet fil. Koden er delt opp mappene EnVy_PS, som inneholder PowerShell-skript, og EnVy_Web, som inneholder kildekoden for nettsiden.

Avtaler

Avtale mellom partene

Bedrift/virksomhet: Domstoladministrasjonen

Student(ene): Tormod H. Lien og Marius I. Myhre

og

NTNU, IDI AIT

Studentprosjekt 15 - Informasjonssikkerhet Domstoladministrasjonen

Gjennomføring
Studenten skal gjennomføre et studentprosjekt i samarbeid med bedriften/virksomheten. IDI AIT veileder arbeidet faglig. Det er utarbeidet retningslinjer for gjennomføring av studentprosjekt som beskriver oppgavefordeling og hvordan studentprosjekter gjennomføres. Retningslinjene tar også opp ansvarsfraskrivelse, opphavsrettigheter og tilgjengelighet med muligheter for individuelle avtaler.

Ansvarsfraskrivelse
Instituttet er ikke ansvarlig for eventuelle ødeleggelser som studenten måtte påføre oppgavestillers utstyr direkte eller som følge av programvare studenten lager og/eller bruker, eller som studenten på annen måte medvirker til.

Opphavsrett og tilgjengelighet
Når ikke annet er avtalt, eier studenter selv den IPR (immaterielle rettigheter) de skaper som en del av studier/studieopphold ved IDI AIT. Alle resultater er åpent tilgjengelig. Opphavsretten reguleres av Åndsverksloven. Avtaler som inngås mellom IDI AIT og studenter skal som minimum sikre instituttet rett til å bruke generert IPR til utdannings- og forskningsformål. IDI AIT skal også motta en vurderingskopi av arbeidet inkludert eventuell kildekode.

Marker med kryss det som gjelder denne oppgaven:

- ☐ Normalsituasjonen: Studentene har selv alle rettigheter knyttet til resultatet fra bacheloroppgaven, med de unntak som er beskrevet over.
- ☐ Oppdragsgiveren har rettighetene og kan utnytte produktet kommersielt og videreutvikle produktet/metoden. Instituttet vil ikke utnytte produktet kommersielt, men vil kunne arbeide videre med den grunnlagskompetansen som er vunnet gjennom prosjektet, som beskrevet over.
- ☐ Resultatene fra arbeidet legges ut som OpenSource iht lisens _____ (Se http://creativecommons.no/lisenser).
- ☒ Bacheloroppgaven (det skriftlige arbeidet) skal være undergitt utsatt offentliggjøring i 3 (maks 3) år.

Oppdragsgiver er selv ansvarlig for å avtale håndtering av eventuelle konfidensielle opplysninger med veileder/sensor og studenten(e).

Denne avtalen er underskrevet i 3 – tre - eksemplarer hvor partene skal ha hver sin.

9.1.19 Trondheim
(dato, sted)

Bedrift/virksomhet	Veileder ved IDI AIT	Student(ene)

Samarbeidsavtale

For bacherloroppgave for Domstoladministrasjonen vår 2019

Sted: Domstolsadministrasjonen, Trondheim.
Dato: 14.01.2019
Medlemmer: Marius Myhre, Tormod Lien

Mål

Effektmål

1. **Samarbeide effektivt**
    a. For å oppnå dette vil vi høre på hverandres meninger og forslag, for å komme fram til den beste løsningen på problemer.
2. **Løsningsorientert adferd**
    a. Om det oppstår problemer som stopper fremgangen i prosjektet, vil vi stoppe de oppgavene vi holder på med, for å løse problemet som har oppstått, eller finne en vei rundt problemet.
3. **Faglig utvikling**
    a. Vi ønsker begge å utvikle vår faglige kompetanse innen nettverkssikkerhet, og alle andre relevante fagområder gjennom bachelorprosjektet.

Resultatmål

4. **Oppnå karakteren A**
    a. Vi har begge like forutsetninger for prosjektet, og har som mål å oppnå karakteren A på det fullførte bachelorprosjektet.
5. **Overholde tidsfrister**
    a. Om det settes tidsfrister for arbeid, skal disse overholdes. Den overordnede tidsfristen for innlevering av bachelorprosjektet skal overholdes. For oppgaver som har tidsfrist, vil disse bli opprettet som oppgaver i SharePoint
6. **Fullføre bachelorprosjektet**
    a. For å oppnå målet med å fullføre bachelorprosjektet er det viktig at vi oppmuntrer hverandre og er engasjerte når vi jobber med oppgaven.

Prosedyrer

7. **Vanlig arbeidsuke**
    a. Med mindre annet spesifiseres av en av partene, møter begge opp hos DA alle ukedager utenom Tirsdag, og begge jobber med prosjektet fra 9-4 (med unntak av matpause).
8. **Møteinnkallinger**
    a. Ved innkalling til interne (bare Tormod og Marius) møter, gjøres dette via Facebook. Møteinnkallingen er ansett som sett dersom Facebook sier den er sett.
    b. Ved innkalling til møter med veiledere (Tor Ivar Melling, Øyvin Moe) skal man benytte seg av Outlook til å innkalle møtet. Agenda for møtet skrives i et word-dokument i SharePoint, og deles med link i møteinnkalling. Om nye ting blir lagt til på møteinnkalling, skal dette opplyses med ny mail, slik at alle deltakende på møtet blir opplyst om dette.
9. **Varsling ved fravær**
    a. Dersom man kommer for sent, skal dette opplyses om ved første anledning i melding på Facebook.
    b. Dersom man ikke kan møte opp, skal dette opplyses om ved første anledning i melding på Facebook.

c. Det er også mulig å varsle fravær muntlig, dersom det er mulig. Det skal være muntlig godkjenning av begge parter for at fraværet er godkjent.

10. **Dokumenthåndtering**
    a. Alle dokumenter som brukes i forhold til bachelorprosjektet skal lagres i SharePoint. Om dokumenter som ikke kan redigeres i SharePoint benyttes, skal disse bli lagret i SharePoint så snart arbeidet er ferdig.
11. **Innlevering**
    a. Før innlevering skal begge samles for å gå gjennom besvarelsen, for å forsikre seg om at det ikke er skrivefeil, og at dokumentets oppbygning er forståelig og riktig.

Opptreden

12. **Oppmøte og forberedelse**
    a. Oppmøtetidspunkt senest som avtalt
    b. Dersom det er avtalt stoff som skal bli gått gjennom før man møtes, forventes det at begge har lest gjennom stoffet.
    c. Er man syk, eller man har andre grunner for fravær, skal dette meldes til den andre personen så fort som mulig, gjennom Facebook.
    d. Uanmeldt fravær blir å anse som avtalebrudd.
13. **Engasjement**
    a. Bruk av PC til ikke-relaterte oppgaver som forstyrrer den andre er ikke tillat. Det er lov å ta pauser, men disse skal ikke virke forstyrrende
    b. Musikk mens man arbeider er lov, men dette må være på et volum som er lavt nok til at det er mulig å kontakte deg verbalt i vanlig toneleie.
    c. Det forventes at man er tilstedeværende og deltakende når man jobber.
14. **Avtalebrudd eller uenighet**
    a. Dersom det oppstår avtalebrudd eller store uenigheter, skal partene først forsøke å løse dette innbyrdes, på en diplomatisk måte. Dersom det ikke er mulig å løse problemet innbyrdes, skal man informere veileder, og sette opp et møte for å løse problemet.

Signatur:
Marius Myhre - *Marius Myhre*
Tormod Lien – Tormod Lien

Møteinnkallinger

Innkalling til møte: Bacheloroppgave

Dato og tid: Onsdag 09.01.19 kl. 10 – 11.
Sted: Kontor, 4.etasje, NTNU Kalvskinnet
Følgende personer innkalles: Tor Ivar Melling, Øyvin Moe, Tormod Lien og Marius Myhre
Agenda:

- Sak nr. 01/2019 - Godkjenning av innkalling
- Sak nr. 02/2019 - Godkjenning av agenda
- Sak nr. 03/2019 - Planlegging av bacheloroppgave
- Sak nr. 04/2019 - Eventuelt

Møtet planlegges avsluttet ca. Kl. 11.
Ta kontakt med undertegnede dersom du ikke har anledning til å komme.

Med vennlig hilsen:
Marius Myhre Trondheim, 07.01.2019

Innkalling til møte: Bacheloroppgave

Dato og tid: Onsdag 16.01.19 kl. 10 – 11.
Sted: Kontor, 4.etasje, NTNU Kalvskinnet.
Følgende personer innkalles: Tor Ivar Melling, Øyvin Moe, Tormod Lien, Marius Myhre
Agenda:

- Sak nr. 06/2019 - Godkjenning av innkalling
- Sak nr. 07/2019 - Godkjenning av referat fra forrige møte
- Sak nr. 08/2019 - Godkjenning av agenda
- Sak nr. 09/2019 - Gjennomgang av det vi har kommet fram til så langt med forstudie
- Sak nr. 10/2019 - Foreløpig plan fram til neste møte
- Sak nr. 11/2019 - Eventuelt

Referat fra forrige møte finner dere ved å bruke følgende lenke: https://studntnu.sharepoint.com/:w:/s/TeamSite/8792/ETQlRhUSJmVAtpOPXj0kMnABiizkpWwZF1C79fIQTUSDMQ?e=BMaBip
Møtet planlegges avsluttet ca. Kl. 11.
Ta kontakt med undertegnede dersom du ikke har anledning til å komme.

Med vennlig hilsen:
Tormod Lien

Trondheim, 09.01.2019

Innkalling til møte: Bacheloroppgave

Dato og tid: Onsdag 23.01.19 kl. 10 – 11.
Sted: Kontor, 4.etasje, NTNU Kalvskinnet
Følgende personer innkalles: Tor Ivar Melling, Øyvin Moe, Tormod Lien og Marius Myhre
Agenda:

- Sak nr. 12/2019 - Godkjenning av innkalling
- Sak nr. 13/2019 - Godkjenning av referat fra forrige møte
- Sak nr. 14/2019 - Godkjenning av agenda
- Sak nr. 15/2019 - Foreløpig problemstilling
- Sak nr. 16/2019 - Gjennomgang av det som er gjort siden forrige møte
- Sak nr. 17/2019 - Foreløpig plan til neste møte
- Sak nr. 18/2019 - Eventuelt

Referat fra forrige møte finner dere ved å bruke følgende lenke: https://studntnu.sharepoint.com/:w:/s/TeamSite/8792/EUnpt7HFyI9NrecB0pcmVZIB4sTAuhNnY96Ng3n6-RVCiw?e=RjmaNC
Møtet planlegges avsluttet ca. Kl. 11.
Ta kontakt med undertegnede dersom du ikke har anledning til å komme.

Med vennlig hilsen:
Marius Myhre

Trondheim, 09.01.2019

Innkalling til møte: Bacheloroppgave

Dato og tid: Onsdag 30.01.19, kl. 10-11.
Sted: Kontor, 4.etasje, NTNU Kalvskinnet.
Følgende personer innkalles: Øyvin Moe, Tor Ivar Melling, Tormod Lien og Marius Myhre
Agenda:

- Sak nr. 19/2019 - Godkjenning av innkalling
- Sak nr. 20/2019 - Godkjenning av referat fra forrige møte
- Sak nr. 21/2019 - Godkjenning av agenda
- Sak nr. 22/2019 - Gjennomgang av viktigste endringer av forstudierapporten
- Sak nr. 23/2019 - Foreløpig plan til neste møte
- Sak nr. 24/2019 - Eventuelt

Det ønskes at samtlige medlemmer har lest gjennom forstudierapporten før møtet, slik at alle deltagende har grunnlag for å diskutere eventuelle endringer som skal gjøres i forstudierapporten. Her ønsker prosjektgruppen at veiledere spesielt leser gjennom kapittel 2 og 3, da disse er kapitlene prosjektgruppen er mest usikre på.
Forstudierapporten finner dere på denne lenken: https://studntnu.sharepoint.com/:w:/s/TeamSite/8792/EcyIYAsjN8xAldsNF9ojV04B1KDArxfYJQ901ZkzJ0QCbw?e=eocsGY
Eller dere kan gå inn i SharePoint-siten, til: Dokumenter/Forstudie/Forstudierapport.docx
Referat fra forrige møte finner dere på denne lenken: https://studntnu.sharepoint.com/:w:/s/TeamSite/8792/EYIA96tt1EBFoXLkHWtJzLEBVxavNuoYwX3ccYh_4WNRuQ?e=Phgzu7
Møtet planlegges avsluttet ca. Kl. 11.
Ta kontakt med undertegnede dersom du ikke har anledning til å komme

Med Vennlig Hilsen:
Marius Myhre Trondheim, 25.01.2019

Innkalling til møte: Bacheloroppgave

Dato og tid: Onsdag 06.02.19, kl. 10-11.
Sted: Kontor, 4.etasje, NTNU Kalvskinnet.
Følgende personer innkalles: Øyvin Moe, Tor Ivar Melling, Tormod Lien og Marius Myhre
Agenda:

- Sak nr. 25/2019 - Godkjenning av innkalling
- Sak nr. 26/2019 - Godkjenning av referat fra forrige møte
- Sak nr. 27/2019 - Godkjenning av agenda
- Sak nr. 28/2019 - Gjennomgang av viktigste endringer av forstudierapporten
- Sak nr. 29/2019 - Foreløpig plan til neste møte
- Sak nr. 30/2019 - Eventuelt

Forstudierapporten finner dere på denne lenken: https://studntnu.sharepoint.com/:b:/s/TeamSite/8792/EYRaaBK0W3tOoIAoMT7PzEsBk_YCXBRGkvyDLDs3TjT52A?e=gpLu73
Referat fra forrige møte finner dere på denne lenken: https://studntnu.sharepoint.com/:w:/s/TeamSite/8792/EX2NnT0kpQVEoM_CpgAxMv0BYOgQCbt_1zxA3ECaVytaUQ?e=qO4o9c
Møtet planlegges avsluttet ca. Kl. 11.
Ta kontakt med undertegnede dersom du ikke har anledning til å komme

Med Vennlig Hilsen:
Tormod Lien

Trondheim, 01.02.2019

Innkalling til møte: Bacheloroppgave

Dato og tid: Tirsdag 26.02.19, kl. 09-10.
Sted: Møterom, Domstoladministrasjonen, Dronningensgate 2.
Følgende personer innkalles: Øyvin Moe, Tor Ivar Melling, Tormod Lien og Marius Myhre
Agenda:

- Sak nr. 31/2019 - Godkjenning av innkalling
- Sak nr. 32/2019 - Godkjenning av referat fra forrige møte
- Sak nr. 33/2019 - Godkjenning av agenda
- Sak nr. 34/2019 - Gjennomgang av enkelte punkter i designdokumentet.
- Sak nr. 35/2019 - Azure sql-database fra NTNU?
- Sak nr. 36/2019 - Foreløpig plan til neste møte
- Sak nr. 37/2019 - Eventuelt

Designdokumentet finner dere på denne lenken: https://studntnu.sharepoint.com/:w:/s/TeamSite/8792/EYeFRAu-OqlHvLPPLc1-RbsBsKetNmUyhZ4YCQ212H1Iow?e=Lxxt2e
Referat fra forrige møte finner dere på denne lenken: https://studntnu.sharepoint.com/:w:/s/TeamSite/8792/EX-TYxh4MtxGiPjbxrLBFssBDZvDX6GR7zwZ9xULMGnQJA?e=uTLEb9
Møtet planlegges avsluttet ca. Kl. 10.
Ta kontakt med undertegnede dersom du ikke har anledning til å komme

Med Vennlig Hilsen:
Tormod Lien

Trondheim, 25.02.2019

Innkalling til møte: Bacheloroppgave

Dato og tid: Tirsdag 12.03.19, kl. 09-10.
Sted: Møterom, Domstoladministrasjonen, Dronningensgate 2.
Følgende personer innkalles: Øyvin Moe, Tor Ivar Melling, Tormod Lien og Marius Myhre
Agenda:

- Sak nr. 1 - Godkjenning av innkalling
- Sak nr. 2 - Godkjenning av referat fra forrige møte
- Sak nr. 3 - Godkjenning av agenda
- Sak nr. 4 - Gjennomgang av utkast til designdokument
- Sak nr. 5 - Azure Stack fra NTNU
- Sak nr. 6 - Foreløpig plan til neste møte
- Sak nr. 7 - Eventuelt

Det er ønskelig om veiledere kunne ha lest gjennom deisgndokumentet, slik at de kan komme med innspill og mangler i dokumentet.
Designdokumentet finner dere på denne lenken: https://studntnu.sharepoint.com/:w:/s/TeamSite/8792/EYeFRAu-OqlHvLPPLc1-RbsBsKetNmUyhZ4YCQ212H1Iow?e=f84naN
Referat fra forrige møte finner dere på denne lenken: https://studntnu.sharepoint.com/:w:/s/TeamSite/8792/EfRElkiIAT1Kso-UNJvz-qsBw__hggFP1F4HdgHmPjQiNw?e=yE8IaB
Møtet planlegges avsluttet ca. Kl. 10.
Ta kontakt med undertegnede dersom du ikke har anledning til å komme

Med Vennlig Hilsen:
Tormod Lien

Trondheim, 07.03.2019

Innkalling til møte: Bacheloroppgave

Dato og tid: Tirsdag 19.03.19, kl. 09-10.
Sted: Møterom, Domstoladministrasjonen, Dronningensgate 2.
Følgende personer innkalles: Øyvin Moe, Tor Ivar Melling, Tormod Lien og Marius Myhre
Agenda:

- Sak nr. 1 - Godkjenning av innkalling
- Sak nr. 2 - Godkjenning av referat fra forrige møte
- Sak nr. 3 - Godkjenning av agenda
- Sak nr. 4 - Gjennomgang av utkast til designdokument
- Sak nr. 5 - Azure Stack fra NTNU
- Sak nr. 6 - Foreløpig plan til neste møte
- Sak nr. 7 - Ny møtedag fra og med April
- Sak nr. 8 - Eventuelt

Designdokumentet finner dere på denne lenken: https://studntnu.sharepoint.com/:w:/s/TeamSite/8792/EYeFRAu-OqlHvLPPLc1-RbsBsKetNmUyhZ4YCQ212H1Iow?e=SFc2eF
Referat fra forrige møte finner dere på denne lenken: https://studntnu.sharepoint.com/:w:/s/TeamSite/8792/EeptDhgwzJRFk1nVCwF3DbcB_Sp6an9vf9ynNs3iAKSRuw?e=ZqR7J5
Møtet planlegges avsluttet ca. Kl. 10.
Ta kontakt med undertegnede dersom du ikke har anledning til å komme

Med Vennlig Hilsen:
Tormod Lien Trondheim, 18.03.2019

Innkalling til møte: Bacheloroppgave

Dato og tid: Onsdag 10.04.19, kl. 09-10.
Sted: Møterom, Domstoladministrasjonen, Dronningensgate 2.
Følgende personer innkalles: Øyvin Moe, Tor Ivar Melling, Tormod Lien og Marius Myhre
Agenda:

- Sak nr. 1 - Godkjenning av innkalling
- Sak nr. 2 - Godkjenning av referat fra forrige møte
- Sak nr. 3 - Godkjenning av agenda
- Sak nr. 4 – Visning av produktet så langt.
- Sak nr. 5 – Tilgang til kostnadsoversikt av database
- Sak nr. 6 – Driftsdokumentet – forklaring av script?
- Sak nr. 7 - Foreløpig plan til neste møte
- Sak nr. 8 - Eventuelt

Referat fra forrige møte finner dere på denne lenken: https://studntnu.sharepoint.com/:w:/s/TeamSite/8792/ESu_MY93xzZMkqBGGn756DYBS9pB2AxPbH7xF5p1PHR_cA?e=DTfOXq
Møtet planlegges avsluttet ca. Kl. 10.
Ta kontakt med undertegnede dersom du ikke har anledning til å komme.

Med Vennlig Hilsen:
Tormod Lien

Trondheim, 08.04.2019

Innkalling til møte: Bacheloroppgave

Dato og tid: Torsdag 02.05.19, kl. 09-10.
Sted: Møterom, Domstoladministrasjonen, Dronningensgate 2.
Følgende personer innkalles: Øyvin Moe, Tor Ivar Melling, Tormod Lien og Marius Myhre
Agenda:

- Sak nr. 1 - Godkjenning av innkalling
- Sak nr. 2 - Godkjenning av referat fra forrige møte
- Sak nr. 3 - Godkjenning av agenda
- Sak nr. 4 – Visning av nettside
- Sak nr. 5 – Eventuelt

Referat fra forrige møte finner dere på denne lenken: https://studntnu.sharepoint.com/:w:/s/TeamSite/8792/EedX-qdSEspIhG3RCv6SszwBBwPvCBuxC0NosWBpVOZOTg?e=hKtgLm
Møtet planlegges avsluttet ca. Kl. 10.
Ta kontakt med undertegnede dersom du ikke har anledning til å komme.

Med Vennlig Hilsen:
Tormod Lien

Trondheim, 29.04.2019

Innkalling til møte: Bacheloroppgave

Dato og tid: Torsdag 09.05.19, kl. 09-10.
Sted: Møterom, Domstoladministrasjonen, Dronningensgate 2.
Følgende personer innkalles: Øyvin Moe, Tor Ivar Melling, Tormod Lien og Marius Myhre
Agenda:

- Sak nr. 1 - Godkjenning av innkalling
- Sak nr. 2 - Godkjenning av referat fra forrige møte
- Sak nr. 3 - Godkjenning av agenda
- Sak nr. 4 - Visning av nettside
- Sak nr. 5 - Designdokument
- Sak nr. 6 - Driftsdokument
- Sak nr. 7 - Eventuelt

Referat fra forrige møte finner dere på denne lenken: https://studntnu.sharepoint.com/:w:/s/TeamSite/8792/EXgWCiTVh0FPlRAL1aUt60kBtbkI8UzOOEXj5Xyuha4T2A?e=gwBl3o
Møtet planlegges avsluttet ca. Kl. 10.
Ta kontakt med undertegnede dersom du ikke har anledning til å komme.

Med Vennlig Hilsen:
Tormod Lien Trondheim, 06.05.2019

Innkalling til møte: Bacheloroppgave

Dato og tid: Onsdag 15.05.19, kl. 09-10.
Sted: Møterom, Domstoladministrasjonen, Dronningensgate 2.
Følgende personer innkalles: Øyvin Moe, Tor Ivar Melling, Tormod Lien og Marius Myhre
Agenda:

- Sak nr. 1 - Godkjenning av innkalling
- Sak nr. 2 - Godkjenning av referat fra forrige møte
- Sak nr. 3 - Godkjenning av agenda
- Sak nr. 4 - Driftsdokument
- Sak nr. 5 - Eventuelt

Referat fra forrige møte finner dere på denne lenken: https://studntnu.sharepoint.com/:w:/s/TeamSite/8792/EYMKqIuM5gZHmm7gdEwHvfsB2g-zayXJI7OZ30211JXh0A?e=jXBv72
Vi ønsker at dere leser driftsdokumentet til møtet. Driftsdokumentet kan dere finnet dere på denne lenken: https://studntnu.sharepoint.com/:w:/s/TeamSite/8792/EVLHWnB73OFIuqEKa-6vBtMBa6TvXfyKxH6Z96_T5XgKrw?e=K8V6LQ
Møtet planlegges avsluttet ca. Kl. 10.
Ta kontakt med undertegnede dersom du ikke har anledning til å komme.

Med Vennlig Hilsen:
Tormod Lien Trondheim, 13.05.2019

Møtereferat 09.01.19

Dato: 09.01.2019
Sted: NTNU Kalvskinnet, Teknologibygget 4.etg.
Til stede: Tor Ivar Melling, Øyvin Moe, Marius Myre & Tormod Lien.

Forkortelsesliste:
"DA" - Domstolsadmistrasjonen

Sak 1 - Godkjenning av innkalling
Innkalling godkjent av alle tilstedeværende

Sak 2 - Godkjenning av agenda
Agenda godkjent av alle tilstedeværende

Sak 3 – Planlegging bacheloroppgave
Generelle ting som ble tatt opp i løpet av møtet

- Problemstilling vil mest sannsynelig endres i løpet av bacheloroppgaven
- Typisk nettverkssikkerhet er det de trenger mest, som medfører at de kommer til å gjøre det selv uavhengig av oss. Dette gjør at det kan være vi starter på noe som de allerede jobber på, eller at de allerede har gjort noe av det vi tenker kan være interessant.
- Ofte er den grundige researchen gjennom oppgaven som er viktigst. Det er ok å "prøve og feile", så lenge vi har gjort prøvingen og feilingen på et godt grunnlag. Det er en bedømmelse om prosess. Trenger ikke nødvendigvis suksess.
- Det er ikke død og liv å få svaret vi ser for oss i starten.
- Karaktervurdering.
- Forventningene til alle involverte.

Angående oppgaveskriving

- https://innsida.ntnu.no/oppgaveskriving
    - Mye nyttig informasjon angående hvordan skrive problemstilling, oppgaven, osv.
- Vi kommer til å bruke referanser. Her er det gunstig å bruke et program som Zotero
    - https://www.zotero.org/
- Tor Ivar er mer en veileder i prosessen å skrive en oppgave, enn i det tekniske. Kan selfølgelig spørre om tekniske spørsmål, men de hos domstolen vet best.
- Oppgavens gang:
    - Start med å finne ut av hva oppgaven skal være
    - Går deretter over til informasjonshenting
    - Etter informasjonshenting skal man begynne å utføre oppgaven
    - Til slutt skal man skrive en evaluering av det som er gjort, med konklusjon.
- Oppgaven skal i all hovedsak svare på problemstillingen. Er da ikke nødvendig med ekstremt detaljert "brukerguide" (ala stein) med bilder med mindre det faktisk er hensiktsmessig, og gir merverdi. Unngå unødvendig "filler".
    - Her kan ting som nettverksdiagram og lignende være relevante bilder, men skjermbilder som går gjennom prosessen av det vi har gjort er mindre relevant.
- Mulig ønske om en scriptrepository.

- Etter forstudiet er ferdig, må problemstillingen fastsettes (løst). Dette kan gjerne gjøres i plenum på et møte.

Om forstudiet

- Søk på nettet etter inspirasjon til hva som kan gjøres. Om vi har fokus på for eksempel scripting mot SCCM, kan man søke i google og se hva som har blitt gjort før. Mest sannsynlig har ting blitt gjort før.
- Vet lite om systemet til DA og vil dermed bruke en del tid i starten på å sette oss inn i dette.

Om oppgaven.

- Ta med Tor Ivar og Øyvin i prosessen å skrive problemstillingen
- Tittelen på prosjektet (altså det som står som tittel på innleveringen) blir IKKE "Teknisk, sosial, og fysisk informasjonssikkerhet – Analyse og Tiltak hos domstolsadministrasjonen". Det blir noe som vi finner på som er mer relevant i forhold til oppgaven.
- De på *DA* benytter seg av SCCM, så det kan være relevant å høre med deres SCCM-type for å finne ut hvilke muligheter som finnes.
- Det er muligheter for å snakke med Tor Ivar om oppsett av testmiljø på skolen, for div testing.
- Et kjapt eksempel på noe vi snakket med DA om var et script-repository for dem, for å automatisere kliensikkerhet.

Div. Adm

- Legg ved viktig informasjon som skal leses før møter i møteinnkallinger, slik at Tor Ivar og Øyvin får tid til å lese seg opp på det viktige som skal leses. Vise godt til hva som skal leses slik at man ikke må lese 400 sider.
- Tor Ivar skal sende oss en eksempeloppgave som vi kan se på for å finne inspirasjon til hvordan man skal skrive en bachelor.
- Vi skal unngå å benytte oss av e-post, eller våre egne skytjenester som dropbox eller google drive til lagring av dokumenter, da det kan inneholde sensitiv informasjon fra *DA*. Vi skal benytte oss i hovedsak av Sharepoint, og hvis det blir relevant, kan vi sette opp Git.

Sak 4 – eventuelt

Alle tilstedeværende skriver under dokument fra NTNU angående bacheloroppgaven.
Signering av taushetserklæring vil skje ved en av de første anledningene hvor vi er hos *DA*.

Møte angående nettverket - 04.01.2019

Dato: 09.01.2019
Sted: Domstoladministrasjonen, kontor i 2. Etg.
Til stede: Tormod, Marius, Geir Hugo, Tran, Øyvin Moe

Referat

Kjell-arne og tommy (annen sikkerhet) – typ kassert utstyr etc.

De synes ethical hacking social engineering hørtes interresant ut

Om klientene DA bruker

- Bruker stasjonære og bærbare PCer, samt tynnklienter
    - Mest aktuelle i forhold til sikkerhet er bærbare, da disse beveger seg inn og ut av bygg osv., men stasjonære og tynnklienter holder seg på en plass.
- Operativsystem er Windows 7 og Windows 10
    - Hovedparten er fortsatt Windows 7
- Bytter ut PCer hvert tredje år
    - Bruker i dag et Excel-ark for registrering av "leasing" av PCer
        - Serienr, merke, navn, etc.

Om SCCM

- Geir Hugo benytter seg av SCCM for å rulle ut sikkerhetspatcher og oppdateringer til applikasjoner, samt utrulling av programvare og OS.
- Configurationitems og baseline kan brukes med Powershell for å finne sårbarheter.
    - Kjører et script, om det finner en sårbarhet kan et annet script kjøres som remedier situasjonen.
    - Geir Hugo har ikke begynt med dette enda
    - Veldig relevant for oss.
- Et script kan lese eventview, og om det finner en sårbarhet, kan det automatisk fiske det med et annet script
- Geir holder på å sette opp en CMDB, der han skal legge inn alle maskiner. Her kan man bruke powershell for å querye AD, hente alle maskinobjekt for å importere det i CMDB, bruker computerlist for å importere til CMDB, har en CSV-fil med masse info som han importerer til CMDB.
- Kan kjøre query mot SCCM-databasen for å hente ut alle maskiner, og deretter kjøre en query mot symantec og hente alle maskiner. Ser deretter hvilke maskiner som ikke har symantec antivirus, og installere dette.

Møtereferat 16.01.19

Dato: 16.01.2019
Sted: NTNU Kalvskinnet, Teknologibygget 4.etg.
Til stede: Tor Ivar Melling, Øyvin Moe, Marius Myre & Tormod Lien.

Sak 1 - Godkjenning av innkalling
Innkalling godkjent av alle tilstedeværende

Sak 2 - Godkjenning av agenda
Agenda godkjent av alle tilstedeværende

Sak 3 - Godkjenning av møtereferat fra forrige møte
Referat godkjent av alle tilstedeværende

Sak 4 – Gjennomgang av det vi har kommet fram til så langt med forstudie
Har laget en foreløpig tidslinje for prosjektet
(Se https://studntnu.sharepoint.com/:u:/s/TeamSite/8792/EVBAOwEBfNxIpCq0FstujWQBKeyF4rly9UAPb4K0kMqw-g?e=5GGOeu)
Går gjennom det vi har kommet fram til med Baselines, har funnet ut hva det er, og hvordan det kan brukes til sikkerhetsformål
Venter på møte med Lars om nettverk for å videre komme fram til en problemstilling

Sak 5 - Foreløpig plan fram til neste møte
Tor Ivar setter opp virtuell lekebinge til oss.

Sak 6: Eventuelt
Fornuftig å bruke starten på å hente inn informasjon, for å lettere se hvor vi ønsker å ta oppgaven
Domstoladministrasjonen har ingen direkte nytte av å se hvordan tidsplanen ble i forhold til estimatet, men det kan være god egenverdi for oss.

Møtereferat - Møte om nettverk

Dato og sted: 16.01.19, 1230, DA, møterom Kristiansand
Til stede: Marius Myhre, Tormod Lien, Øyvin Moe, Lars

Informasjon fra Lars

Om DA/domstolenes nettverk

- Totalt 825 trådløse aksesspunkt, 232 switcher
- Switchene er i hovedsak Aruba switcher, noe gammelt cisco er fortsatt igjen
- Nettet på DA er satt opp slik at det lokale intern-nettet ikke har WAN-tilgang. Gjestenettet har WAN, men ethernettilkobling og trådløst hovednett er kun LAN.
- I dag blir alt av trafikk tunnelert over til Evry, som gjør alt bak der.
    - Ønsker å skille mellom intern-trafikk og internett-trafikk fra gjestenettet, for å unngå overbelastning
- Alle lokasjonene er i samme nett, forskjellige VLAN
    - 10.x.x.x nett
- Trådløsnettet er ikke subnettet, bare intern-nettet
- DA har et såkalt "Geriljanett", ikke i noe form for DMZ, men har tilgang til utverden. I dag brukes det kun som lab, men om for eksempel nettet går ned har det blitt brukt av andre.
    - Lite sikkerhetsrisk i dag, da det ikke er noe kobling mellom gerilja og intranett, men kan være muligheter for forbedring

Aruba Airwave

- DA benyttes seg av Airwave for portmonitorering og oppestatus av switcher
    - Brukes ikke til sikkerhet enda
- Kan gjennom airwave få ut mange forskjellige rapporter
    - Port-rapporter
    - Client sessions
    - Health report
    - Mye mer
- Airwaven kjøres i dag kun på det trådløse nettet.
    - Kan få en trafikkoverview gjennom airwave
    - Airwave gir god oversikt over trådløsnettet
- Mange APIer på Aruba/Airwave, kan se på formatering av data ut fra API

Clearpass

- DA benytter seg av Clearpass for aksesskontroll
    - Blir noe lite brukt i dag, er ikke ut i prod
- Alle DHCP requests blir forwarded til Clearpass, som logger og får informasjon fra enhetene gjennom DHCP-requesten.
- Kjører i dag ingen discovery, kun gjennom DHCP-polling
- Clearpass er i hovedsak en RADIUS-server, men også mer
- Benyttes for å sette wired-policy, der swticher legges inn som godkjente devices i ClearPass, nettverksregler blir satt opp i clearpass, og blir pushet ut til switchene
- Autentisering går i hovedsak på dot1x, om dette feiler går den over til macauth. Skal i framtiden sette opp userauth.
- Clearpass er i all hovedsak ikke brannmur, men man kan sette opp veldig mye regler, da per user, per port, eller på andre grunnlag.
- Clearpass autentiserer hver mac-adresse, på hver port.
- KAn hente inn informasjon om hva som plugges inn, om det er godkjent eller ikke, filtrere på det man vil.
- Ettersom det brukes DHCP-requests for å finne enheter, kan ting som ligger på fast IP, som f.eks kortterminaler i kantiner på bygg ikke dukke opp i clearpass

- Clearpass har muligheten for flere forskjellige discovery-metoder for å finne enheter
- Om clearpass har pumpet ut regler til en switch, vil alt switchen gjør rapporteres inn til clearpass. Dataen profileres, og kjøres gjennom alle relevante regler, for å se hva som stemmer, og hva som ikke stemmer. Her er det, grunnet DHCP-basert discovery, mulig at vi bare får se at noe er rart med en MAC-adresse, og ingen annen info, noe som kan gjøre det vanskelig å finne ut av hva som har skjedd
- Clearpass regler er i hovedsak ACL, som gjør at switchene blir "dumme" brannmurer.

Om oppgaven vår

- Krysschecking av data fra Clearpass, Airwave, og SCCM
- Det kan være interessant å scripte en løsning for å hente ut og formatere data fra Clearpass/Airwave/SCCM. Fra Clearpass får man en XML-fil som er vanskelig å lese, kan formatere og vise utdata på en ryddig og pen måte.
- Se på hvilke APIer som finnes, se hvilken data man kan få ut, hvordan den kan formateres, hvordan den kan hjelpe sikkerheten (automatisk varsling ved mulige angrep, automatisk feilrapportering, etc)
- Sette opp varsling i Airwave om den finner rogue entry, løpende hente ut og formatere inforamsjon om rogue entry, feilmeldinger, angrepsforsøk, etc, lage historikk på når/hvor/hva har skjedd

Møtereferat fra møte 23.01.19

Dato og tid: Onsdag 23.01.19, kl 10:00 – 11:00
Sted: NTNU Kalvskinnet 5. etasje
Til stede: Tormod Lien, Marius Myhre, Øyvin Moe
Frafall: Tor Ivar Melling

Sak nr. 1 - Godkjenning av innkalling

Godkjent

Sak nr. 2 - Godkjenning av referat fra forrige møte

Godkjent

Sak nr. 3 - Godkjenning av agenda

Godkjent

Sak nr. 4 - Foreløpig problemstilling

Prosjektgruppen presenterte sin foreløpige problemstilling: Utforske mulighetene for, designe og produsere et system for automatisk analyse av enhetsinformasjon fra SCCM, Clearpass og Airwave. Den foreløpige problemstillingen ble godkjent av oppgavestiller.

Sak nr. 5 - Gjennomgang av det som er gjort siden forrige møte

Deler av forstudiet ble gjennomgått av prosjektgruppen. Det ble foreslått å ta med flere interessenter, som Informasjonssikkerhetsansvarlig og personvernsansvarlig fra Domstoladministrasjonen, samt brukersenteret. Det ble også foreslått å ikke binde navnene til de ansvarlige, men heller bruke titler. Rammebetingelsene ble gjennomgått, og det ble oppklarert hvilke kostnader som skal bli tatt med fra Domstoladministrasjonen sin side: Anta at alle systemer som blir brukt finnes fra før, og skal dermed ikke bli tatt med i kost/nytte analysen.
Effektmål ble gjennomgått, og det ble kommet fram til forskjellige metoder for å måle effekten av prosjektet. Eksempler er "Månedlige uttrekk av hvilke enheter som er på nettverket skal ikke ta mer enn x minutter", eller "Konsolidering og sammensetting av informasjon skal ikke ta mer enn x minutter". Det ble også diskutert muligheten for eventuelle "før og etter" undersøkelser, der man spør hvor lett det er å gjøre noe i dag, mot hvor lett det er etter de har benyttet det nye systemet.
Prosessmål for prosjektgruppen ble diskutert, der det ble kommet fram til å splitte opp flere av målene, og eventuelt legge inn nye mål basert på hvor vi ønsker å være om x måneder.
Suksessfaktorer ble diskutert. Her kom det fram at de som skal ha suksessfaktorer er interessentene fra interessentanalysen. Det går greit i suksessfaktorene å ha overordnede mål for oppgavestiller, og å ha spesifikke mål for spesifikke interessenter i DA, som brukesenteret.
Prosjektorganisering ble diskutert. Her kom vi fram til å sette inn Lars og Geir Hugo under kvalitetskontroll, under navnet "Nettverksansvarlige", så lenge det blir forklart i underteksten at de kun skal kvalitetskontrollere verktøyet. Det ble også diskutert å få inn en annen gruppe til å være referansegruppe, der vi kunne lese over deres rapport, og motsatt for å få best mulig tilbakemelding.
I kost/nytte analysen kan det være greit å høre med nettverksansvarlige, å høre hvor lang tid de mener de ville brukt på å gjøre jobben verktøyet skal gjøre manuelt, for å få best mulig utgangspunkt.

Sak nr. 6 - Foreløpig plan til neste møte

Foreløpig plan til neste møte er ferdigstilling av forstudierapporten for tilbakemelding, og å ferdigstille testmiljøet så fremt at vi får tilgang på lisenser til Aruba-tjenestene.

Sak nr. 7 - Eventuelt

Det er ikke nødvendig å utnevne prosjektleder, men det kan være greit å skrive at vi bytter hver måned eller noe liknende, bare for å ha gjort det. '
Testmiljøet er nede, da host-licence på host 14 som vi bruker har gått ut.

Møtereferat - Bacheloroppgave

Dato og tid: Onsdag 30.01.19, kl. 10:00 – 10:55.
Sted: Møterom, 4. etasje, NTNU Kalvskinnet,
Til stedet: Øyvin Moe (oppgavestiller), Tor Ivar Melling (veileder), Tormod Lien, Marius Myhre
Frafall: Ingen

Sak nr. 1 - Godkjenning av innkalling

Godkjent

Sak nr. 2 - Godkjenning av referat fra forrige møte

Godkjent

Sak nr. 3 - Godkjenning av agenda

Godkjent

Sak nr. 4 - Gjennomgang av forstudie

Forstudiet ble gjennomgått og endringsforslag ble gitt til prosjektgruppen. Rapporten var jevnt over litt for lite spesifikk og tunglest. Endringsforslag ble notert av prosjektgruppen, og en utskrift med noterte forslag ble gitt til prosjektgruppen av veileder fra Domstoladministrasjonen. Spørsmål prosjektgruppen hadde angående kost/nytte analysen ble besvart.

Sak nr. 5 - Foreløpig plan til neste møte

Planen for neste uke ble gjennomgått. Planen vil være å utbedre forstudierapporten i henhold til endringsforslag gitt på møtet, slik at forstudiet er ferdig til neste veiledningsmøte (06.02.19). Testmiljø er planlagt å være satt opp til neste veiledningsmøte.

Sak nr. 6 - Eventuelt

First for innlevering er 20. Mai 2019
Veileder tok opp muligheten for å samarbeide med en annen bachelorgruppe når det gjelder korrekturlesning av dokumenter. Oppgavestiller sier at dette er en god ide, så lenge det ikke deles konfidensiell informasjon i dokumentene.
Kontorsituasjonen på Domstoladministrasjonen ble diskutert med tanke på at prosjektgruppen per dags dato sitter i 3.etg, men planen er å flytte ned til 2.etg.

Møtereferat fra møte 06.02.19

Dato og tid: Onsdag 06.02.19, kl 10:00 – 10:40
Sted: Kontor, 4. etasje, NTNU Kalvskinnet.
Til stede: Tor Ivar Melling, Marius Myhre & Tormod Lien
Frafall: Øyvin Moe (Avtalt frafall)

Sak nr. 1 - Godkjenning av innkalling.

Godkjent

Sak nr. 2 - Godkjenning av referat fra forrige møte.

Godkjent

Sak nr. 3 - Godkjenning av agenda.

Godkjent

Sak nr. 4 - Gjennomgang av viktigste endringer av forstudierapporten.

Formatering av dokumentet i form av sideskifte, figurliste og tabelliste ble godkjent.
Kapittel 2, bakgrunn og behov, ble gjennomgått og godkjent. Figur og forbedret beskrivelse ble lagt til siden forrige møte.
Kapittel 3, mål, ble gjennomgått og godkjent. Mer konkrete mål ble lagt til siden forrige møte.
Interessentanalysen ble gjennomgått og godkjent. Siste interessent fikk sette opp egne suksesskriterier på mandag.
Prosjektgruppen sier seg fornøyd med forstudierapporten

Sak nr. 5 - Foreløpig plan til neste møte.

Starte på designdokumentet samt å arbeide med oppsett av testmiljøet.

Sak nr. 6 - Eventuelt.

Prosjektgruppen har ikke rettigheter til å deploye VM ved hjelp av OVF-filer. Disse rettighetene ble tilpasset i møtet, men det er usikkert om endringene vil løse problemet for prosjektgruppen. Dersom det ikke løser problemet er en alternativ løsning avtalt hvor prosjektgruppen sender filer til veileder som vil gjøre disse filene tilgjengelig i vCenteret for prosjektgruppen. Oppsett av rettigheter ble utført i henhold til følgende guide: https://kb.vmware.com/s/article/2105932.

Møtereferat fra møte 26.02.19

Dato og tid: Tirsdag 26.02.19, kl. 09:00 – 10:00
Sted: Møterom 2. etg. Domstoladministrasjonen, Dronnigens Gate 2
Til stede: Tor Ivar Melling, Øyvin Moe, Tormod Lien, Marius Myhre
Frafall:

Sak nr. 1 - Godkjenning av innkalling.

Godkjent

Sak nr. 2 - Godkjenning av referat fra forrige møte.

Godkjent

Sak nr. 3 - Godkjenning av agenda.

Godkjent

Sak nr. 4 - Gjennomgang av enkelte punkter i designdokumentet

Kapittel 2, om oppgavestiller og behov - Det går fint å kopiere det som er skrevet i tidligere dokumenter, da hvert dokument er alenestående.

Sak nr. 5 - Azure SQL-Database fra NTNU

For å teste databaseløsnigen er det viktig for prosjektgruppen å ha tilgang til Azure. Dette skal Tor Ivar finne ut av, og etter hvert gi prosjektgruppen tilgang til NTNUs Azure-miljø.

Sak nr. 6 - Foreløpig plan til neste møte.

Planen til neste gang er å fortsette med designdokumentet, slik at det forhåpentligvis blir mulig å starte utviklingen av selve løsningen i løpet av neste uke. I løpet av neste uke (uke 10), skal prosjektgruppen pitche løsningen sin til DA.

Sak nr. 7 - Eventuelt.

Det kom opp et spørsmål angående datalagring; Kan vi lagre den informasjonen vi får ut og fortsatt være i henhold til loven/gdpr?

Dette er noe prosjektgruppen er nødt til å finne ut av.

Firmware for swtich – Prosjektgruppen skal emulere en switch i VmWare-testmiljøet. For å få til dette må Tor Ivar muligens hjelpe til med å laste opp filer som er nødvendige i vCenteret, da dette ikke fungerer for prosjektgruppen.

Møtereferat fra møte 12.03.19

Dato og tid: Tirsdag 12.03.19, kl 09:00 – 10:00
Sted: Kontor, 4. etasje, NTNU Kalvskinnet.
Til stede: Tor Ivar Melling, Marius Myhre, Tormod Lien
Frafall:

Sak nr. 1 - Godkjenning av innkalling.

Godkjent

Sak nr. 2 - Godkjenning av referat fra forrige møte.

Godkjent

Sak nr. 3 - Godkjenning av agenda.

Godkjent

Sak nr. 4 - Gjennomgang utkast designdokument

En god løsning å skille ut hva løsningen, verktøyet, databaseløsning og visualseringsløsning er
Ikke fornorske Github-ord
Kan skrive litt hvorfor vi velger eks. Powershell.
Kan være greit med feilrapportering dersom

Sak nr. 5 - Azure Stack fra NTNU

****Viktig****
Tor Ivar må purre på Stein Meisingseth for å få tilgang til NTNU sin Azure Stack.
****/Viktig****

Sak nr. 6 - Foreløpig plan til neste møte.

Utvikling

Sak nr. 7 - Eventuelt.

Sharepoint har vært tregt
Driftsdokumentet kan ha bilder der det er hensiktsmessig, ikke kjør en “stein”-rapport, med 500 sider med bilder.
Filer fra sharepoint som skal til Vcenteret er vanskelig.

Møtereferat fra møte 19.03.19

Dato og tid: Tirsdag 19.03.19, kl 0900 - 1000
Sted: DA Møterom Kristiansand
Til stede: Tor Ivar, Øyvin, Marius, Tormod
Frafall:

Sak nr. 1 - Godkjenning av innkalling.

Godkjent

Sak nr. 2 - Godkjenning av referat fra forrige møte.

Godkjent

Sak nr. 3 - Godkjenning av agenda.

Godkjent

Sak nr. 4 – Gjennomgang av utkast til designdokumentet

Kommentarer til designdokumentet: Formatering mangler, men dette kommer når dokumentet ferdigstiller.
Om bedriften – Airwave logger kun gjestenettet
3.2 - Intranett er en nettside, Internt nett/internnett.
Den nye "I forhold til" er nå "da"
Remote seg inn, forklar bedre
API-EN eller API-ET, ikke begge.

Sak nr. 5 - Azure Stack

Saken utgår, da problemet var løst før møtet.

Sak nr. 6 - Ny møtedag fra og med april

Møtetid er fleksibelt. Onsdag klokken 9 passer for begge, men Tor Ivar kan endre om det er nødvendig. Øyvin sin beste dag er onsdag.

Sak nr. 7 - Foreløpig plan til neste møte.

Fortsett å utvikle.

Sak nr. 8 - Eventuelt.

Vi sladder ut live-data fra DA, slik at vi ikke lagrer deres data
Sluttrapporten: Anbefaling av videre arbeid, og begrensinger for prosjektet
Legg inn opplæring og overlevering i gantt. Planlegg hvordan DA skal få produktet.

Møtereferat fra møte 10.04.2019

Dato og tid: Ondsag 10.04.19, kl 09:00 – 10:00
Sted: Kontor, 4. etasje, NTNU Kalvskinnet.
Til stede: Tor Ivar, Øyvin, Tormod, Marius
Frafall:

Sak nr. 1 - Godkjenning av innkalling.

Godkjent

Sak nr. 2 - Godkjenning av referat fra forrige møte.

Godkjent

Sak nr. 3 - Godkjenning av agenda.

Godkjent

Sak nr. 4 - Visning av produktet så langt

Ser bra ut, viktig å vise fram til teknikere for å få tilbakemelding fra de som vet hvordan det fungere.

Sak nr. 5 - Tilgang til kostnadsoversikt

Ingen svar fra stein, Tor Ivar kan gå til stein å se over.

Sak nr. 6 - Driftsdokumentet – forklaring av scripts

Trenger ikke kopiere inn hele scriptet inn i driftsdokumentet. Kan godt ha en kjapp oversikt over hvilke script som finnes og hva de gjør, og deretter vise til koden hvor vi har god comment based help.

Sak nr. 7 - Foreløpig plan til neste møte.

Bli ferdig med alle script (igjen)

Sak nr. 8 - Eventuelt

Møtereferat fra møte 19.03.19

Dato og tid: Tirsdag 29.04.19, kl 0900 - 1000
Sted: DA Møterom Kristiansand
Til stede: Tor Ivar, Øyvin, Marius, Tormod
Frafall:

Sak nr. 1 - Demo av verktøyet.

Fremvisning av verktøyet.

Sak nr. 2 - Planen videre

Ferdig med alle scripts denne uken og arbeide med nettside fremover.

Møtereferat fra møte 02.05.2019

Dato og tid: Torsdag 02.05.19, kl. 0900 - 1000
Sted: Møterom Tønsberg, 2. etasje, Domstoladministrasjonen.
Til stede: Tor Ivar, Øyvind, Tormod, Marius
Frafall:

Sak nr. 1 - Godkjenning av innkalling.

Godkjent

Sak nr. 2 - Godkjenning av referat fra forrige møte.

Godkjent

Sak nr. 3 - Godkjenning av agenda.

Godkjent

Sak nr. 4 - Visning av nettside

Nettsiden ser bra ut. Prosjektgruppens beslutning om å benytte PHP og javascript, med open-source templates som datatables.net, charts.js og bootstrap støttes av veiledere, da tiden ikke tillater å lage alt fra bunnen av, eller sette seg inn i nodejs.

Sak nr. 5 - Foreløpig plan til neste møte.

Gjøre ferdig nettside, og begynne på avsluttende dokumentasjon. Siste cutoff for utvikling er 10. Mai

Sak nr. 6 - Eventuelt.

Presentasjon blir hos DA, tid kommer. Ingen hard tidsramme på presentasjonen, rundt 20 min med 10 min til spørsmål (totalt 30) er vanlig, men ingen problemer med å pushe til 30 min presentasjon og 10 min. spørsmål om nødvendig.
Flytt neste møte til torsdag.

Møtereferat fra møte 09.05.19

Dato og tid: Torsdag 09.05.19, kl 09:00 – 10:00
Sted: Møterom Tønsberg, 2. etasje, Domstoladministrasjonen
Til stede: Tor Ivar, Øyvin, Tormod, Marius
Frafall:

Sak nr. 1 - Godkjenning av innkalling.

Godkjent

Sak nr. 2 - Godkjenning av referat fra forrige møte.

Godkjent

Sak nr. 3 - Godkjenning av agenda.

Godkjent

Sak nr. 4 - Visning av nettside

Nettsiden virker godt, og viser den informasjonen som er forventet.

Sak nr. 5 - Designdokument

- Nettsiden ser ikke nøyaktig ut som den ble beskrevet i designdokumentet. Er det nødvendig å gå tilbake å revidere konsepttegningene?
    - Trenger ikke revidere driftsdokumentet for å endre concept-art eller liknende. Driftsdokumentet er
- PowerBI blir ikke implementert i tide for prosjektet, skal prosjektgruppen endre designdokumentet for å reflektere dette?
    - Avslutt heller driftsdokumentet med å si at konklusjonen var at powerbi ikke ble implementert i tidsrommet til prosjektet
- Databasen var antydet i designdokumentet til å være en azure-database, men det er bestilt en mssql windows server database. Er det nødvendig å endre designdokumentet for å reflektere dette?
    - Trenger ikke endre designdokumentet, så lenge det bli skrevet i driftsdokumentet hva det faktisk er.

Sak nr. 6 - Driftsdokument

- Brukerveiledning av selve nettsiden, skal denne være overfladisk, eller gå godt inn på hvordan man benytter en nettside generelt?
    - De som skal benytte nettsiden er teknisk anlagt, og skriv brukerveiledningen for dem.
- Oppsett av driftsdokument: skal det være bygd opp rundt steg i prosessen å benytte EnVy, eller bygd opp rundt individuelle moduler i EnVy?
    - Vi kan ta en vurdering av det, kan gjerne skrive i toppen hvordan dokumentet er bygd opp. Ikke så viktig hvilken som velges.

Sak nr. 7 - Foreløpig plan til neste møte.

Førsteutkast klar på mandag.
Neste møte Onsdag 15. Mai

Sak nr. 8 - Eventuelt.

Dato for fremføring:
28. Mai, klokken 9.

Møtereferat fra møte 15.05.19

Dato og tid: Onsdag 15.05.19, kl 09:00-10:00
Sted: Domstoladministrasjonen
Til stede: Tormod, Marius, Øyvin, Tor Ivar
Frafall:

Sak nr. 01/2019 - Godkjenning av innkalling.

Godkjent

Sak nr. 02/2019 - Godkjenning av referat fra forrige møte.

Godkjent

Sak nr. 03/2019 - Godkjenning av agenda.

Godkjent

Sak nr. 04/2019 - Gjennomgang av driftsdokument

Mere informasjon i introduksjonen
Mer informasjon om hva som kommer i hvert kapittel
Mye bedre beskrivelser for hvert kapittel.
Forklar hvorfor noe skal gjøres, ikke bare hva som skal gjøres

Korrekturlesing: Veldig mye skriveleif og rare formuleringer.
Bra dybde på teknisk forklaring.
Punktet JS

Sak nr. 05/2019 - Foreløpig plan til neste møte.

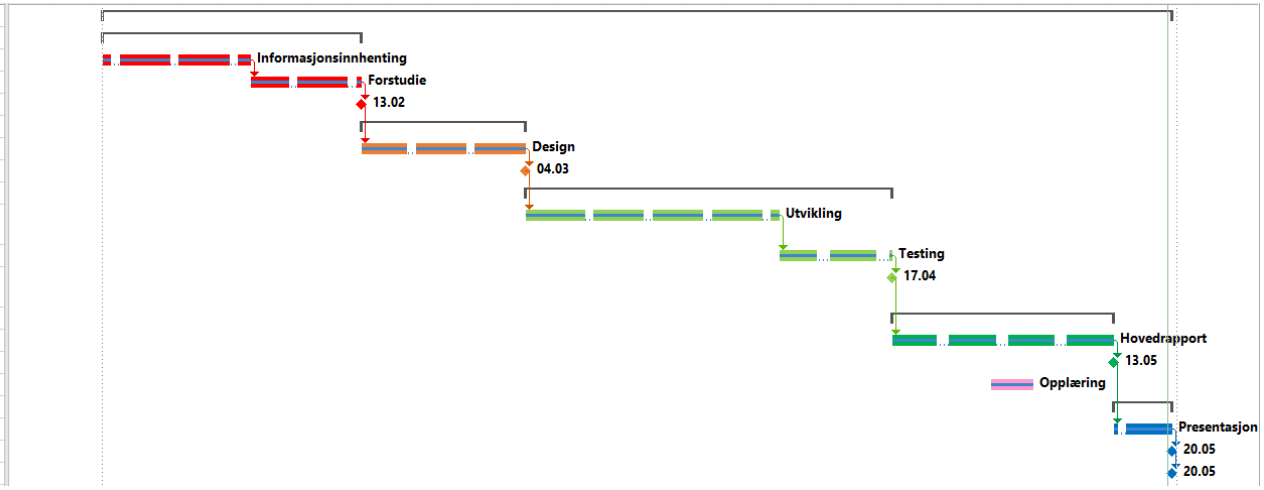
Sak nr. 06/2019 - Eventuelt.

Gjerne vis figurer
Usikker om hva vi skal ta med på forsiden, kan være greit å ikke skrive noe tittel eller problemstilling eller noe slikt.

Fremdriftsplan

Fremdriftsplanen er laget i MS Project og ligger vedlagt som filen BachelorTidsplan.mpp

✓		**Prosjektoppgave**	**120,17 days?**	**Mon 14.01.19**	**Mon 20.05.19**
✓		**Forstudie**	**30 days**	**Mon 14.01.19**	**Wed 13.02.19**
✓		Informasjonsinnhenting	2,33 wks	Mon 14.01.19	Thu 31.01.19
✓		Utforming av rapport	1,56 wks	Thu 31.01.19	Wed 13.02.19
✓		Forstudie ferdig	0 days	Wed 13.02.19	Wed 13.02.19
✓		**Design**	**17,83 days**	**Wed 13.02.19**	**Mon 04.03.19**
✓		Løsningsdesign	2,53 wks	Wed 13.02.19	Mon 04.03.19
✓		Design ferdig	0 days	Mon 04.03.19	Mon 04.03.19
✓		**Utvikling**	**41,67 days**	**Tue 05.03.19**	**Wed 17.04.19**
✓		Scriptutvikling & driftrapport	3,89 wks	Tue 05.03.19	Wed 03.04.19
✓		Testing	1,33 wks	Thu 04.04.19	Wed 17.04.19
✓		Ferdig løsning (Script repository)	0 days	Wed 17.04.19	Wed 17.04.19
✓		**Hovedrapport**	**24,5 days**	**Wed 17.04.19**	**Mon 13.05.19**
✓		Rapport utforming	3,17 wks	Wed 17.04.19	Mon 13.05.19
✓		Hoverdapport ferdigstilt	0 days	Mon 13.05.19	Mon 13.05.19
✓		**Opplæring**	6,17 days?	Mon 29.04.19	Fri 03.05.19
✓		**Presentasjon**	**6,17 days**	**Mon 13.05.19**	**Mon 20.05.19**
✓		Forberedelse	0,81 wks	Mon 13.05.19	Mon 20.05.19
✓		Fremføring	0 days	Mon 20.05.19	Mon 20.05.19
✓		Endelig innlevering	0 days	Mon 20.05.19	Mon 20.05.19



Timelister

Marius

	Mandag	Tirsdag	Onsdag	Torsdag	Fredag	Lørdag	Søndag	SUM
Uke 2	2	0	2	2	4	0	2	12
Uke 3	7	0	7	0	6	0	0	20
Uke 4	7	2	7	1	6	0	0	23
Uke 5	6	2	6	6	5	0	0	25
Uke 6	7	2	7	0	0	0	0	16
Uke 7	0	0	0	0	0	0	3	3
Uke 8	7	7	7	7	3	0	0	31
Uke 9	7	3	7	7	2	0	0	26
Uke 10	7	2	7	7	2	1	0	26
Uke 11	5	6	5	7	0	0	0	23
Uke 12	6	8	7	7	6	0	0	34
Uke 13	0	7	7	7	7	0	0	28
Uke 14	7	0	7	7	6	0	0	27
Uke 15	7	0	8	6	6	0	0	27
Uke 16	0	0	0	0	0	0	0	0
Uke 17	0	0	7	7	7	0	0	21
Uke 18	9	0	8	9	6	4	4	40
Uke 19	11	4	12	12	11	8	4	62
Uke 20	10	10	6	4	4	10	4	48
Uke 21	11							11
SUM								503
Tid igjen								11

Tormod

	Mandag	Tirsdag	Onsdag	Torsdag	Fredag	Lørdag	Søndag	SUM
Uke 2	2	0	2	0	0	2	2	8
Uke 3	7	0	7	5	6	0	0	25
Uke 4	1	0	7	1	6	0	0	15
Uke 5	7	0	6	6	5	0	0	24
Uke 6	7	0	7	7	0	0	0	21
Uke 7	0	0	7	7	5	0	0	19
Uke 8	7	7	7	7	4	0	0	32
Uke 9	7	3	7	7	0	0	0	24
Uke 10	7	2	7	7	2	1	0	26
Uke 11	7	6	5	7	3	0	0	28
Uke 12	7	8	7	7	6	0	0	35
Uke 13	0	7	7	7	7	0	0	28
Uke 14	7	0	7	7	6	0	0	27
Uke 15	7	0	8	8	6	0	0	29
Uke 16	0	0	0	0	0	0	0	0
Uke 17	0	0	7	10	7	4	3	31
Uke 18	9	0	7	9	4	4	4	37
Uke 19	12	1	4	12	11	4	2	46
Uke 20	10	10	6	1	4	10	8	49
Uke 21	11							11
SUM								515
Tid igjen								-1

Uke 2

Marius

Timer uke	12		Timer totalt	12		Resterende	502
Arbeidsart	**Mandag**	**Tirsdag**	**Onsdag**	**Torsdag**	**Fredag**	**Lørdag**	**Søndag**
Forstudie				2	4		2
Møte	2		2				

Tormod

Timer uke	8		Timer totalt	8		Resterende	506
Arbeidsart	**Mandag**	**Tirsdag**	**Onsdag**	**Torsdag**	**Fredag**	**Lørdag**	**Søndag**
Forstudie						2	2
Møte	2		2				

Ukens arbeid:

- Klassemøte med Stein på Mandag
- Oppstartsmøte med Tor Ivar og Øyvin på Onsdag
- Helgen ble brukt til å lese seg opp på nettverk, gamle leksjoner og youtube videoer.

Plan for neste uke:

- Starte med forstudierapporten og informasjonsinnhenting.
- Møte med Geir hugo & Lars angående nettverk og SCCM.

Uke 3

Marius

Timer uke	20		Timer totalt	32		Resterende	482
Arbeidsart	**Mandag**	**Tirsdag**	**Onsdag**	**Torsdag**	**Fredag**	**Lørdag**	**Søndag**
Forstudie	6		5		6		
Møte	1		2				

Tormod

Timer uke	25		Timer totalt	33		Resterende	481
Arbeidsart	**Mandag**	**Tirsdag**	**Onsdag**	**Torsdag**	**Fredag**	**Lørdag**	**Søndag**
Forstudie	6		5	5	6		
Møte	1		2				

Ukens arbeid:

- Møte med Geir Hugo og Tran på mandag angående SCCM.
- Sett på mulighetene når det gjelder SCCM og Baselines
- Veiledningsmøte på Onsdagen hvor det ble diskutert litt om hvordan prosjektet lå an og plan frem til neste møte
- Møte med Lars på onsdag angående nettverksadministrasjon og tjenestene som brukes.
- Sett på muligheter når det gjelder Aruba tjenestene Airwave og Clearpass.
- Kommet i gang med forstudierapporten

Plan for neste uke:

- Fortsette arbeidet med forstudierapporten.
- Begynne med oppsettet av testlab.

Uke 4

Marius

Timer uke	23		Timer totalt	55		Resterende	459
Arbeidsart	**Mandag**	**Tirsdag**	**Onsdag**	**Torsdag**	**Fredag**	**Lørdag**	**Søndag**
Forstudie			6	1	6		
Møte			1				
Testmiljø	7	2					

Tormod

Timer uke	15		Timer totalt	48		Resterende	466
Arbeidsart	**Mandag**	**Tirsdag**	**Onsdag**	**Torsdag**	**Fredag**	**Lørdag**	**Søndag**
Forstudie	1		6	1	6		
Møte			1				

Ukens arbeid:

- Mandag ble brukt til å starte med oppsett av test miljøet
- Onsdag hadde vi møte med Øyvin og resten av dagen ble brukt til å utarbeide forstudierapporten
- Fredag brukte vi litt tid på å stille Lars noen spørsmål før vi så nesten ferdigstillte forstudierapporten

Plan for neste uke:

- Ferdigstille forstudierapporten
- Sette opp fullstendig testmiljø
- Teste ut Aruba Tjenestene

Uke 5

Marius

Timer uke	25		Timer totalt	80		Resterende	434
Arbeidsart	**Mandag**	**Tirsdag**	**Onsdag**	**Torsdag**	**Fredag**	**Lørdag**	**Søndag**
Forstudie	4		5	6	4		
Møte			1				
Testmiljø	2	2			1		

Tormod

Timer uke	24		Timer totalt	72		Resterende	442
Arbeidsart	**Mandag**	**Tirsdag**	**Onsdag**	**Torsdag**	**Fredag**	**Lørdag**	**Søndag**
Forstudie	7		5	6	5		
Møte			1				

Ukens arbeid:

- Mandag ble brukt til å sette opp deler av testmiljøet samt å ferdigstille et førsteutkast for veiledningsmøtet på onsdagen.
- Onsdag ble brukt til å ha møte angående forstudierapporten, og resterende av dagen ble brukt til å utbedre rapporten i henhold til endringsforslag.
- Torsdag ble brukt til å ferdigstille forstudierapporten.
- Fredag ble brukt til å ferdigstille forstudierapporten for godkjenning på neste veiledningsmøte. Testmiljø ble også videreutviklet i form av SQL.

Plan for neste uke:

- Godkjenning av forstudierapport.
- Sette opp fullstendig testmiljø.

Uke 6

Marius

Timer uke	16		Timer totalt	96		Resterende	418
Arbeidsart	**Mandag**	**Tirsdag**	**Onsdag**	**Torsdag**	**Fredag**	**Lørdag**	**Søndag**
Forstudie	7						
Møte			1				
Testmiljø		2	6				

Tormod

Timer uke	21		Timer totalt	93		Resterende	421
Arbeidsart	**Mandag**	**Tirsdag**	**Onsdag**	**Torsdag**	**Fredag**	**Lørdag**	**Søndag**
Forstudie	7						
Møte			1				
Design			6	7			

Ukens arbeid:

- Mandag ble brukt på ferdigstilling av forstudierapporten
- Onsdag ble brukt på veiledningsmøte og innledende arbeid på designrapporten
- Torsdag ble brukt til videre arbeid på designrapporten

Plan for neste uke:

- Sette opp testmiljø og arbeide med designrapporten

Uke 7

Marius

Timer uke	3		Timer totalt	99		Resterende	415
Arbeidsart	**Mandag**	**Tirsdag**	**Onsdag**	**Torsdag**	**Fredag**	**Lørdag**	**Søndag**
Design							
Testmiljø							3

Tormod

Timer uke	19		Timer totalt	112		Resterende	402
Arbeidsart	**Mandag**	**Tirsdag**	**Onsdag**	**Torsdag**	**Fredag**	**Lørdag**	**Søndag**
Design			6	5	2		
Testmiljø			1	2	3		

Ukens arbeid:

- Onsdag ble brukt på å arbeide med designrapporten og oppsett av Power BI Desktop
- Torsdag ble brukt til å arbeide med designrapporten og oppsett av SQL-server
- Fredag ble brukt til å abeide med designrapporten og oppsett av SQL-server

Plan for neste uke:

- Konfigurere Aruba tjenestene
- Teste PowerBI opp mot SQL.
- Komme med forslag til løsning

Uke 8

Marius

Timer uke	31		Timer totalt	130		Resterende	384
Arbeidsart	**Mandag**	**Tirsdag**	**Onsdag**	**Torsdag**	**Fredag**	**Lørdag**	**Søndag**
Design							
Testmiljø	7	7	7	6	3		
Møte				1			

Tormod

Timer uke	32		Timer totalt	144		Resterende	370
Arbeidsart	**Mandag**	**Tirsdag**	**Onsdag**	**Torsdag**	**Fredag**	**Lørdag**	**Søndag**
Design	1		1				
Testmiljø	6	7	6	6	4		
Møte				1			

Ukens arbeid:

- Mandag ble hovedsaklig brukt til oppsett av testmiljø
- Tirsdag ble brukt til planlegging av verktøy og oppsett av testmiljø
- Onstag ble brukt til å arbeide med testmiljø
- Torsdag ble brukt til å arbeide med testmiljø. Hadde også møte med Evry angående valg av databaseløsning. Azure stack database/virtualisert sql.
- Fredag ble brukt til å arbeide med testmiljø. Clearpass-API og SCCM.

Plan for neste uke:

- Møte med DA og Microsoft hvor vi får informasjon som vil avgjøre valg av dashboard løsning
- Arbeide med designdokument og testmiljø.

Uke 9

Marius

Timer uke	26		Timer totalt	156		Resterende	358
Arbeidsart	**Mandag**	**Tirsdag**	**Onsdag**	**Torsdag**	**Fredag**	**Lørdag**	**Søndag**
Design			2				
Testmiljø	7		4	6	2		
Utvikling			1	1			
Møte		3					

Tormod

Timer uke	24		Timer totalt	168		Resterende	346
Arbeidsart	**Mandag**	**Tirsdag**	**Onsdag**	**Torsdag**	**Fredag**	**Lørdag**	**Søndag**
Design							
Testmiljø	7		5	5			
Utvikling			2	2			
Møte		3					

Ukens arbeid:

- Mandag ble brukt til å tilpasse testmiljøet.
- Tirsdag ble brukt til veiledningsmøte og møte med brukersenteret.
- Onsdag ble brukt til scripting og testmiljø.
- Torsdag ble brukt til scripting og testmiljø.

Plan for neste uke:

- Møte på onsdag angående valg av løsning
- Reell start på utviklingen
- Ferdigstilling av designdokument
- Ferdigstille testmiljø

Uke 10

Marius

Timer uke	26		Timer totalt	182		Resterende	332
Arbeidsart	**Mandag**	**Tirsdag**	**Onsdag**	**Torsdag**	**Fredag**	**Lørdag**	**Søndag**
Design	3		2	3	2	1	
Testmiljø	3						
Utvikling	1		3	4			
Møte		2	2				

Tormod

Timer uke	26		Timer totalt	194		Resterende	320
Arbeidsart	**Mandag**	**Tirsdag**	**Onsdag**	**Torsdag**	**Fredag**	**Lørdag**	**Søndag**
Design	3		2	3	2	1	
Testmiljø	3						
Utvikling	1		3	4			
Møte		2	2				

Ukens arbeid:

- Mandag ble brukt til å utvikle script i tillegg til å se på designdokument og testmiljø.
- Tirsdag ble brukt til å forberede fremføring for pitching av ide for DA.
- Onsdag ble brukt til å pitche ide for DA, utvikle script og skrive på designdokumentet.
- Torsdag ble brukt til å skrive på designdokumentet og utvikle script.
- Fredag og Lørdag ble brukt til å utføre korrekturlesning av designdokument

Plan for neste uke:

- Bli ferdig med scripts for uthenting av data fra SCCM, Airwave og Clearpass

Uke 11

Marius

Timer uke	23		Timer totalt	205		Resterende	309
Arbeidsart	**Mandag**	**Tirsdag**	**Onsdag**	**Torsdag**	**Fredag**	**Lørdag**	**Søndag**
Utvikling	5	4	5	7			
Møte		2					

Tormod

Timer uke	28		Timer totalt	222		Resterende	292
Arbeidsart	**Mandag**	**Tirsdag**	**Onsdag**	**Torsdag**	**Fredag**	**Lørdag**	**Søndag**
Utvikling	7	4	5	7	3		
Møte		2					

Ukens arbeid:

- Mandag ble brukt til å lage script for SCCM og CPPM.
- Tirsdag ble brukt til veiledningsmøte og utvikling av script for SCCM og CPPM.
- Onsdag ble brukt til utvikling av script for CPPM.

Plan for neste uke:

- Starte på scripts for analyse av data

Uke 12

Marius

Timer uke	34		Timer totalt	239		Resterende	275
Arbeidsart	**Mandag**	**Tirsdag**	**Onsdag**	**Torsdag**	**Fredag**	**Lørdag**	**Søndag**
Utvikling	6	6	7	7	6		
Møte		2					

Tormod

Timer uke	35		Timer totalt	257		Resterende	257
Arbeidsart	**Mandag**	**Tirsdag**	**Onsdag**	**Torsdag**	**Fredag**	**Lørdag**	**Søndag**
Utvikling	7	6	7	7	6		
Møte		2					

Ukens arbeid:

- Mandag ble brukt til å utvikle scripts for uthenting av data.
- Tirsdag ble brukt til å utvikle scripts for sammenslåing av data
- Onsdag ble brukt til å utviklde scripts for sammenslåing av data
- Tordsdag ble brukt til å utvikle scripts for sammenslåing av data
- Fredag ble brukt til å utvikle scripts for analyse av data, og oppsett av Azure SQL database.

Plan for neste uke:

- Send ferdig analysert testdata til database

Uke 13

Marius

Timer uke	28		Timer totalt	267		Resterende	247
Arbeidsart	**Mandag**	**Tirsdag**	**Onsdag**	**Torsdag**	**Fredag**	**Lørdag**	**Søndag**
Utvikling		7	7	7	7		
Møte							

Tormod

Timer uke	28		Timer totalt	285		Resterende	229
Arbeidsart	**Mandag**	**Tirsdag**	**Onsdag**	**Torsdag**	**Fredag**	**Lørdag**	**Søndag**
Utvikling		7	7	7	7		
Møte							

Ukens arbeid:

- Tirsdag til Torsdag ble brukt til å lage scripts for merging og analyse av data
- Fredag ble brukt til å lage script for SQL-innsending

Plan for neste uke:

- Ferdig med alle script.
- Starte på visualisering.

Uke 14

Marius

Timer uke	27		Timer totalt	294		Resterende	220
Arbeidsart	**Mandag**	**Tirsdag**	**Onsdag**	**Torsdag**	**Fredag**	**Lørdag**	**Søndag**
Utvikling	7		7	7	6		
Møte							

Tormod

Timer uke	27		Timer totalt	312		Resterende	202
Arbeidsart	**Mandag**	**Tirsdag**	**Onsdag**	**Torsdag**	**Fredag**	**Lørdag**	**Søndag**
Utvikling	7		7	7	6		
Møte							

Ukens arbeid:

- Mandag ble brukt til å lage script mot databasen og merging av data.
- Onsdag ble brukt til å lage script for merging og analyse av data.
- Torsdag ble brukt til å lage script for merging og analyse av data.
- Fredag ble brukt til å lage script for merging og analyse av data.

Plan for neste uke:

- Ferdigstille script for merging og initialisering av database.

Uke 15

Marius

Timer uke	27		Timer totalt	321		Resterende	193
Arbeidsart	**Mandag**	**Tirsdag**	**Onsdag**	**Torsdag**	**Fredag**	**Lørdag**	**Søndag**
Utvikling	7		8	6	6		

Tormod

Timer uke	29		Timer totalt	341		Resterende	173
Arbeidsart	**Mandag**	**Tirsdag**	**Onsdag**	**Torsdag**	**Fredag**	**Lørdag**	**Søndag**
Utvikling	7		8	8	6		

Ukens arbeid:

- Mandag ble brukt til å ferdigstille formatering av sccm data og starte på script for uthenting i reelt miljø.
- Onsdag ble brukt på skripting
- Tordag ble brukt på skripting
- Fredag ble brukt på å videreutvikle skript og vise fram det vi hadde til Lars og Andre

Plan for neste uke:

- Bli ferdig med alle scripts for analyse

Uke 16

Marius

Timer uke	0		Timer totalt	321		Resterende	193
Arbeidsart	**Mandag**	**Tirsdag**	**Onsdag**	**Torsdag**	**Fredag**	**Lørdag**	**Søndag**

Tormod

Timer uke	0		Timer totalt	341		Resterende	173
Arbeidsart	**Mandag**	**Tirsdag**	**Onsdag**	**Torsdag**	**Fredag**	**Lørdag**	**Søndag**

Ukens arbeid:
- Påskeferie

Plan for neste uke:
- Ferdigstille alt av scripts og starte på visualisering

Uke 17

Marius

Timer uke	21		Timer totalt	342		Resterende	172
Arbeidsart	**Mandag**	**Tirsdag**	**Onsdag**	**Torsdag**	**Fredag**	**Lørdag**	**Søndag**
Utvikling			6	7	7		
Møte			1				

Tormod

Timer uke	31		Timer totalt	372		Resterende	142
Arbeidsart	**Mandag**	**Tirsdag**	**Onsdag**	**Torsdag**	**Fredag**	**Lørdag**	**Søndag**
Utvikling			6	10	7	4	3
Møte			1				

Ukens arbeid:

- Onsdag ble brukt til veiledningsmøte og start på visualisering.
- Torsdag ble brukt til å ferdigstille funksjonalitet i alle scripts.
- Fredag ble brukt til å starte på utvikling av nettside.

Plan for neste uke:

- Plan for mandag: Ta et valg mellom PHP og NodeJS.
- Plan for Tirsdag: Ha klart en alpha-versjon av nettsiden klar til møte neste dag.
- Plan for resterende dager: Utvikle nettsiden.

Uke 18

Marius

Timer uke	40		Timer totalt	382		Resterende	132
Arbeidsart	**Mandag**	**Tirsdag**	**Onsdag**	**Torsdag**	**Fredag**	**Lørdag**	**Søndag**
Utvikling	9		8	8	6	4	4
Møte				1			

Tormod

Timer uke	37		Timer totalt	409		Resterende	105
Arbeidsart	**Mandag**	**Tirsdag**	**Onsdag**	**Torsdag**	**Fredag**	**Lørdag**	**Søndag**
Utvikling	9		7	8	4	4	4
Møte				1			

Ukens arbeid:

- Mandag ble brukt til å velge PHP fremfor NodeJS.
- Onsdag ble brukt til å utvikle nettside.
- Torsdag ble brukt til veiledningsmøte og utvikling av nettside.
- Fredag ble brukt til ryddin og kommentering av kode.

Plan for neste uke:

- Helt ferdig med alt av kode
- Ferdig førsteutkast av driftsdokumentet

Uke 19

Marius

Timer uke	62		Timer totalt	444		Resterende	70
Arbeidsart	**Mandag**	**Tirsdag**	**Onsdag**	**Torsdag**	**Fredag**	**Lørdag**	**Søndag**
Utvikling	11	4	12	11			
Møte				1			
Driftsdokument					11	8	4

Tormod

Timer uke	46		Timer totalt	455		Resterende	59
Arbeidsart	**Mandag**	**Tirsdag**	**Onsdag**	**Torsdag**	**Fredag**	**Lørdag**	**Søndag**
Utvikling	12		4	11			
Møte		1		1			
Driftsdokument					11	4	2

Ukens arbeid:

- Mandag ble brukt til å fikse nettside og kommentering av kode.
- Onsdag ble brukt til bugfix av kode
- Torsdag ble brukt til siste bugfix av kode (Faktisk ferdig scripts)
- Fredag ble brukt til å skrive på driftsdokument

Plan for neste uke:

- Ferdig førsteutkast av driftsdokument til mandag
- Ferdig driftsdokument til torsdag
- Ferdig med Sluttrapporten til Søndag
- Mandag 20.05.19 blir brukt til finpuss og innlevering

Uke 20

Marius

Timer uke	48		Timer totalt	492		Resterende	22
Arbeidsart	**Mandag**	**Tirsdag**	**Onsdag**	**Torsdag**	**Fredag**	**Lørdag**	**Søndag**
Møte			1				
Driftsdokument	10	10	3		4	1	
Sluttrapport			2			9	4
Presentasjon				4			

Tormod

Timer uke	49		Timer totalt	504		Resterende	10
Arbeidsart	**Mandag**	**Tirsdag**	**Onsdag**	**Torsdag**	**Fredag**	**Lørdag**	**Søndag**
Møte			1				
Driftsdokument	10	10	3		4	1	
Sluttrapport			2			9	8
Presentasjon				1			

Ukens arbeid:

- Mandag ble brukt til å lage førsteutkast av driftsdokumentet
- Tirsdag ble brukt til å videreutvikling av driftsdokumentet
- Onsdag ble brukt til å ferdigstille driftsdokumentet etter veiledning
- Torsdag ble brukt til å starte på presentasjonen
- Fredag ble brukt til rettlesning og formatering av driftsdokumentet
- Lørdag ble brukt til å arbeide med sluttrapporten
- Søndag ble brukt til å ferdigstille sluttrapporten etter tilbakemelding

Plan for neste uke:

- Ferdig bachelor

Uke 21										
Marius						**Tormod**				
Timer uke	11	Timer totalt	503	Resterende	11	Timer uke	11	Timer totalt	515	Resterende	-1
Arbeidsart	**Mandag**					**Arbeidsart**	**Mandag**				
Sluttrapport	7					Sluttrapport	7				
Presentasjon	4					Presentasjon	4				

Ukens arbeid:

• Mandag ble brukt til å ferdigstille oppgaven for levering og ferdigstilling av presentason.