

BACHELOROPPGAVE:

SkyHiGh Feide

FORFATTERE:

Fredrik Magnussen

Håkon Tvedt

Morten H. Singstad

DATO:

15.05.2013

Sammendrag av Bacheloroppgaven

Tittel:	Norwegian title.	Nr: -
		Dato: 15.05.2013
Deltakere:	Fredrik Magnussen	
	Håkon Tvedt	
	Morten H. Singstad	
Veiledere:	Hanno Lagweg	
Oppdragsgiver:	Erik Hjelmås, Høgskolen i Gjøvik	
Kontaktperson:	Erik Hjelmås, erikh@hig.no	
Stikkord	Norway, Norsk	
Antall sider: 13	Antall vedlegg:	Tilgjengelighet: Åpen
Kort beskrivelse av bacheloroppgaven: This should be in Norwegian, I thought I would add some more text to make sure that it ran over multiple lines. I will need to check the page number feild as it probably should be just the core pages without the appendices. Currently it returns the last page of the whole document. If I cannot work it out, I will provide two inputs, gmtnumberpages and gmtappnumber. That should do the job.		

Summary of Graduate Project

Title:	SkyHiGh Feide	Nr: -
		Date: 15.05.2013
Participants:	Fredrik Magnussen	
	Håkon Tvedt	
	Morten H. Singstad	
Supervisor:	Hanno Lagweg	
Employer:	Erik Hjelmås, Høgskolen i Gjøvik	
Contact person:	Erik Hjelmås, erikh@hig.no	
Keywords	Thesis, Latex, Template, IMT	
Pages: 13	Appendixes:	Availability: Open
	Short description of the main project: This is the short description of a bachelor thesis	

Innhold

Innhold	vii
Figurer	ix
Tabeller	xi
1 Innledning	1
1.1 Bakgrunn	1
1.2 Oppgavebeskrivelse	2
1.3 Rapportorganisering	2
1.4 Beskrivelser	4
1.5 Formål	4
1.6 Målgruppe	4
1.6.1 Prosjektets målgruppe	4
1.6.2 Rapportens målgruppe	4
1.7 Avgrensning	5
1.8 Prosjektgruppens kunnskap	5
1.9 Roller	5
2 Kravspesifikasjon	1
2.1 Brukerbeskrivelse	1
2.1.1 Omgivelser	1
2.1.2 Systemets brukere	1
2.1.3 User stories	2
2.1.4 Primærmål	2
2.1.5 Sekundærmål	2
2.2 Detaljert kravspesifikasjon	3
2.2.1 Funksjonelle krav	3
2.2.2 Use case diagram	3
2.2.3 Høynivå use case	5
2.2.4 Detaljert use case	9
2.2.5 Funksjon	12
2.2.6 Struktur og tverr-relasjoner	13

Word count: 123

Figurer

1	Use case diagram 1	3
2	Use case diagram 2	4
3	Detaljert usecase	9
4	Detaljert usecase	10
5	Detaljert usecase	11
6	Et eksempel på innlogging med feide	12
7	Hvordan autentiseringen foregår	12
8	Hvor går autentiseringstrafikken	13

Tabeller

1 Innledning

1.1 Bakgrunn

Autentisering, er i dag et stort tema. Det er mye snakk på at det blir for mange brukernavn og passord å huske. Det diskuteres også at dette skader sikkerheten av data. Grunnen til dette er at brukerne lager seg lettere passord, lagrer passord på telefonen, post-it-lapper og mange andre finurlige måter. Dette er ingen heldig situasjon, men det er veldig forståelig at det blir sånn.

En av løsningene på dette er FEIDE[?]. Denne løsningen er kunnskapsdepartementets svar på problemet. Denne løsningen er kun innenfor utdanningssektoren i Norge, men det vil være en stor reduksjon i hvor mange brukernavn og passord som må huskes.

Det er derfor blitt et ønske fra Erik Hjelmås fra Høgskolen i Gjøvik å integrere dette på skyløsningen til skolen. Openstack-skyløsningen ved HiG skal i første omgang være tilgjengelig for ansatte og fag. Det er flere fag som bruker VM-er i undervisningen (Ethical Hacking And Penetration Testing [?], Systemadministrasjon [?] og Database- og applikasjonsdrift [?]).

Ønsker fra arbeidsgiver

- Sentral innlogging for VM-er.
- Skal kunne bruke brukernavn og passord som man har ellers på skolen.

Nåværende løsning er at det står to servere som har lokale brukere. Disse opprettes om vedlikeholdes i passwd- og shadowfilene. Dette er en tungvint løsning ved når man ønsker å utvide VM-systeme for bruk av flere ved HiG.

1.2 Oppgavebeskrivelse

Hensikten ved bacheloroppgaven SkyHiGhFeide er at vi skal integrere modul i Openstack som autentiserer mot Feide (Openstack er et “open source cloud computing”-prosjekt). Denne løsning vil gjøre at man kan bruke allerede brukernavn og passord som man har i Feide. Flere tjenester i undervisningssektoren i Norge bruker Feide, målet til kunnskapsdepartementet er at alt innen skole-Norge skal autentiseres mot Feide. Ved denne modul-integreringen i Openstack vil det da bli en standard i innlogging.

Vi skal sette opp et rack med Openstack-løsning som skal kjøre VM-systemet for skolen. Dette vil bedre ytelse og effektiviteten ved bruk av VM på HiG. Vi skal sette opp autentiseringen mot horizon-plattformen på kontrollernoden i Openstack. Denne skal kjøre autentisering mot keystone-plattformen i Openstack, som er autentiseringstjenesten i Openstack.

- Sette opp SkyHiGh løsningen og oppdatere denne til siste versjon av OpenStack.
- Utrede og realisere rollebasert identitetshåndtering og tilhørende FEIDE-autentisering.

1.3 Rapportorganisering

1. Innledning - Et lite innblikk i rapporten. Gir en kort overordnet oversikt av hvordan rapporten er strukturert og hva den inneholder.
2. Kravspesifikasjon - Her dokumenteres kravene som arbeidsgiver har satt for hvordan systemet skal fungere med autentisering mot Openstack.
3. Teoretisk grunnlag Openstack - Her gir en grundig inføring i hvordan autentiseringen fungerer i Openstack. Dette er viktig for å få forståelse for hvor og hvordan vi skal kunne integrere Feide-autentisering.
4. Teoretisk grunnlag Feide - Her gir vi en grundig inføring og forklaring av hvordan Feide-autentisering fungerer. Veldig viktig for forståelse av hvordan vi skal kunne autentisere mot Openstack.
5. Design - Går mer inn på designet autentiseringen i Openstack og Feide, samt detaljert design som er utbedret av kravspesifikasjonen.
6. Gjennomføring - Her vil det bli detaljert, dokumentert og godt beskrivende forklaring på hvordan vi gjennomfører prosjektet.
7. Drifrutiner - Her gir vi en forklaring på hvordan det skal vedlikeholdes og oppdateres for å opprettholde sikkerhet og brukervennlighet.
8. Drøting - Vi diskuterer om det finnes andre og kanskje bedre muligheter i forhold til autentisering. Litt nøyere drøfting det vi har gjort kontra andre. Spør oss selv om sikkerheten blir svekket.
9. Avsluttning - Konklusjonen fra oppgaven, hvordan resultatet ble og hvordan utførelsen ble gjort.
10. Bibliografi og litteraturliste - En oversikt over referanser og tekster som er brukt i denne rapporten, samt en liste over komplekse ord.

11. Vedlegg - Dokumentering av figurer, tabeller til rapporten. Andre vedlegg: Prosjektplan, script, dagslogg og referater fra diverse møter.

1.4 Beskrivelser

Her kommer noen regler og beskrivelser på hvordan spesielle ord brukes i rapport og blir forklart.

Vi-ordet refereres til prosjektgruppen vår som består av Fredrik Magnussen, Håkon Tvedt og Morten H. Singstad. Når vi snakker om arbeidsgiver, er det Erik Hjelmås. Hanno Langweg refereres som veileder.

- Forkortelser vil bli beskrevet i sitt fulle navn i fotnoten.
- Andre spesielle ord vil få et eksponentnummer som kan refereres til litteraturlisten.
- Kommandoer og script vil ha denne fonten ved navn Courier new, på scriptene vil det også være syntax-farger.
- For kildehenvisning benytter vi oss av vancouver-stilen [?]
- Ord som er relevant å forklare i teksten vil ikke bli nevnt i litteraturlisten.

1.5 Formål

Formålet med å integrere FEIDE-autentisering i Openstack vil være en forenklet hverdag for brukerne av SkyHiGh[?], ved at de kan logge inn med brukernavn og passord som de har fra før. Det skal være rollebasert innlogging. Da mener vi at det skal være forskjellige rettigheter hvis en ansatt logger inn kontra en student. Det viktigste er at det fungerer ved HiG, men hvis mulig skal vi lage en integrering som skal kunne brukes for andre Openstack-brukere. Dagens innlogging består av to servere som lagrer nye brukernavn og passord i passwd- og shadow-filene. Ugunstig ved at man må legge til nye brukere for hvert semester samt slette de gamle.

Formålet skal også være å øke sikkerheten. Ved at brukerne får enda et nytt brukernavn og passord å huske, så er det stor sannsynlighet at brukerne skriver ned passordet på mobil, post-it-lapp eller andre steder som svekker sikkerheten. Ved at man kan bruke brukernavn og passord som brukerne har fra før, så trenger man ikke huske nye data, samt at det er større sannsynlighet for at brukerne ikke trenger å skrive informasjonen ned.

1.6 Målgruppe

1.6.1 Prosjektets målgruppe

Målgruppen for prosjektet er HiG. Det skal være en løsning som først og fremst er rettet for å fungere her. I første omgang for de ansatte med fagene som krever VM-er, deretter for alle ansatte ved skolen. Hvis en framtidig utvidelse av SkyHiGh skulle komme, så er det ønskelig at løsningen skal være tilgjengelig for enkeltstudenter.

1.6.2 Rapportens målgruppe

Rapporten er myntet på at det skal være dokumentert utførelse av prosjektet til arbeidsgiver. Derav skal det være mulig for andre interesserte å kunne se hva vi har gjort, for så å kunne integrere løsningen selv hvis ønskelig. Rapporten er også i hovedsak en ut-

danning. For oss som gruppe, så er dette en erfaring vi kan bringe med oss videre inn i arbeidslivet.

1.7 Avgrensning

Hovedmålet for oppgaven er at det skal være fungerende innlogging til Openstack mot Feide. Nødløsning er at vi får en løsning som kun fungerer for denne skolen gjennom å autentisere med LDAP-registeret til skolen. Dokumentasjon for dette vil også vedvare for at andre interessenter skal kunne bruke nødløsningen hvis de selv bruker LDAP. Siden vi er drift-studenter, ser vi det også vesentlig at vi automatiserer det som kan automatiseres.

Deretter så er det tid som avgrenser hva vi får gjort. Ønsket er å få satt opp et rack med kjørende Openstack-løsning med integrert Feide-autentisering. Bonusmål: Overvåking og implementering av SkyHiGh Adm-modulen.

1.8 Prosjektgruppens kunnskap

Prosjektgruppens faglige bakgrunn er den samme. Fredrik Magnussen, Håkon Tvedt og Morten H. Singstad går alle tre “Drift av nettverk- og datasystemer” ved HiG. Vi har brukt VM-er i fag og lært hvordan de blir opprettes, samt hvordan de opprerer på en maskin. Men kunnskap i hvordan Openstack-løsningen fungerer er heller liten. Heller ikke autentisering i seg selv har vi noen faglige kunnskaper ved.

Det vi har av faglige kunnskaper som kan hjelpe oss er grunnforståelse og god teknisk innsikt. Programmeringskunnskapen vi har opparbeidet oss her på skolen vil også komme godt til nytte med tanke på script. Scriptene vil i all hovedsak lages for å automatisere installasjonen av Openstack, som er drøftet i Vedlegg A.

Vi er derfor nødt til å tilegne oss mye kunnskap fra bunnen av. Innenfor Feide, Openstack og nye programmeringsspråk. Vi er nødt til å sette oss grundig inn i hvordan Openstack autentiserer brukerne sine.

1.9 Roller

Arbeidsgiveren våres er Erik Hjelmås, ansatt ved HiG som førsteamanuensis. Kunnskapen til arbeidsgiver angående Feide vil ikke kunne være noen stor ressurs. Men erfaringsmessig kan han bidra oss med å lete på rett plass og stille de rette spørsmålene for å kunne få den kunnskapen vi trenger. Arbeidsgiver er også en stor ressurs ved materialistiske behov.

Veileder Hanno Langweg som også er ansatt ved HiG som førsteamanuensis, kommer til å være en sterk ressurs innenfor hvordan prosjektet bør gjennomføres. Bidrag med hvordan vi bør prioritere i et så stor prosjekt og hjelpe oss med å nå de målene vi har satt oss.

Rolleinndeling under prosjektarbeidet:

- Morten H. Singstad
Valgt som leder for prosjektgruppa. Vil være den som er kontaktperson og som har det overordna ansvaret for gruppen og oppgavene.

- Fredrik Magnussen
Webansvarlig.
- Håkon Tvedt
Ansvaret for alt som har med installasjoner.

Når alt kommer til alt, så er vi en samarbeidende prosjektgruppe som hjelper hverandre og er ydmyke i rollene. Vi er bestemte, men har ingen ovenfra-og-ned-holdning ovenfor hverandre.

2 Kravspesifikasjon

Vi skal få inn en tjeneste under et allerede eksisterende rammeverk. Med det må vi beskrive de kravene som må opprettholdes for at vi skal kunne få en suksessfull integrering med ny autentisering. Vi skal også beskrive detaljert hendelsesløpet for en autentisering innenfor rammeverket, eksisterende og det vi vil integrere.

Allerede eksisterende materiale vi kan se på er dokumentasjon på Openstack keystone-modulen og Feide-dokumentasjon.

2.1 Brukerbeskrivelse

2.1.1 Omgivelser

Som nevnt tidligere, så skal autentiseringstjenesten integreres. Det skal skje på et allerede eksisterende system, som allerede har en annen autentiseringstjeneste. Selve Openstack-systemet samkjøres mellom flere servere. Det er stykket opp i moduler for ytelse og funksjonalitet. Den modulen vi skal jobbe på er “Controller noden”, den kjører noen moduler som vi skal jobbe med og derfor må sette oss ekstra nøye inn i.

- Horizon - Webinterfacet til Openstack-systemet. Der er brukergrensesnittet som brukes for å kunne lage, endre, slette og kjøre VM-ene, det er også her innloggingen ligger.
- Keystone - Tar seg av hvilke prosesser og VM-er som tilhører hvem. Derfor har også den en finger med i autentiseringen.

2.1.2 Systemets brukere

Det er tre grupper med brukere mot tjenesten vi skal integrere. De har alle forskjellige roller og autoritet innen systemet.

- Studenter/brukere - De har kun lov til å kunne lage, endre, slette og bruke VM-er. De har også restriksjoner på ytelse og mengde plass som kan brukes.
- Ansatte - Forskjellen fra studentene er at de ansatte har ikke restriksjon på ytelse og mengde data.
- It-tjenesten - Gruppen som har mest tilgang, men av den praktiske grunn at de har vedlikeholdsarbeidet. De har også rettigheter som de overnevnte.

Opplæringen ved å bruke tjenesten er minimal. Vi skal jobbe med innloggingen. Noe absolutt alle har vært borti før, med tanke på at det er noe av det første du må gjøre når du kommer til HiG.

2.1.3 User stories

2.1.4 Primærmål

Stikkord	logge inn på domene
Beskrivelse	Brukeren vil at man skal kunne skrive inn et gitt domene og komme til log in-skjermen. I dette tilfelle er domene allerede ordnet: skyhigh.hig.no.

Stikkord	logge in med Feide
Beskrivelse	Kunden vil at brukeren må logge seg inn ved å bruke eksisterende brukernavn og passord.

Stikkord	Forskjellige roller
Beskrivelse	<p>Kunden ønsker at det skal være forskjell på hvilke roller man har når man logger in. De ansatte som trenger VM-er i undervisninger trenger gjerne litt ekstra ytelse, dette i forhold til at det kan være mange studenter i et emne og må derfor delegere ut mange VM-er. Hvis ansatte bare vil bruke et par VM-er så trenger de ikke rettigheter utover det vanlige.</p> <p>Det vil bli satt opp to forskjellige roller:</p> <ul style="list-style-type: none"> • Ekstra rettigheter • Normal rettigheter

2.1.5 Sekundærmål

Stikkord	Installere Openstack
Beskrivelse	Openstack skal bli HiG sin skyløsning. Skolen bruker en del VM-er og trenger mer ytelse på de. Derfor blir løsningen å sette opp eget.

Stikkord	Installere Openstack
Beskrivelse	Openstack skal bli HiG sin skyløsning. Skolen bruker en del VM-er og trenger mer ytelse på de. Derfor blir løsningen å sette opp eget.

Stikkord	Installere Adm-modulen
Beskrivelse	Kunden ønsker også, hvis tid, at vi skal få installert Adm-modulen som bachelorgruppa SkyHiGh Adm lagde.

Stikkord	Automatisert innstallasjon
Beskrivelse	Med tanke på vedlikehold så vil det være enkelt og greit med en automatisert innstallasjon. F.eks. hvis det blir satt inn en "Compute node" til, så skal det kun være å boote en usbpinne som tar seg av hele installasjonen.

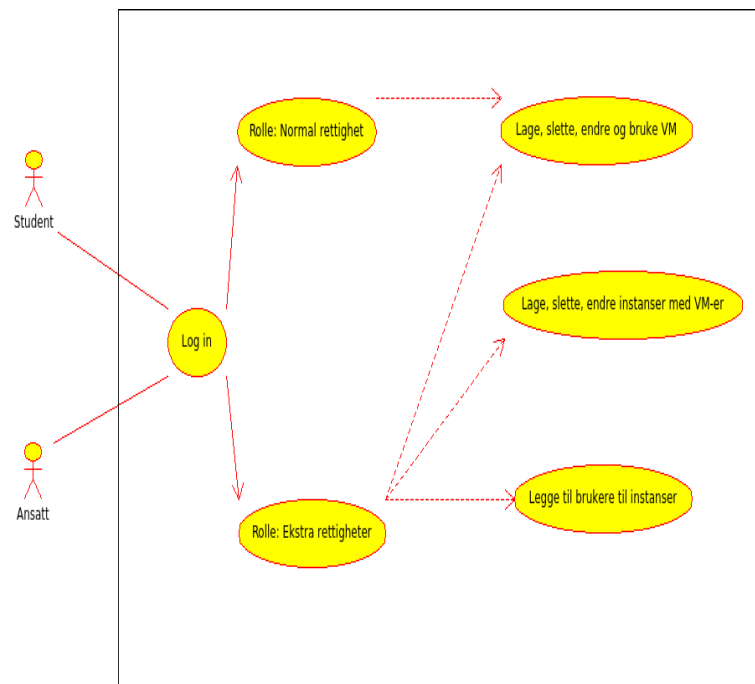
2.2 Detaljert kravspesifikasjon

2.2.1 Funksjonelle krav

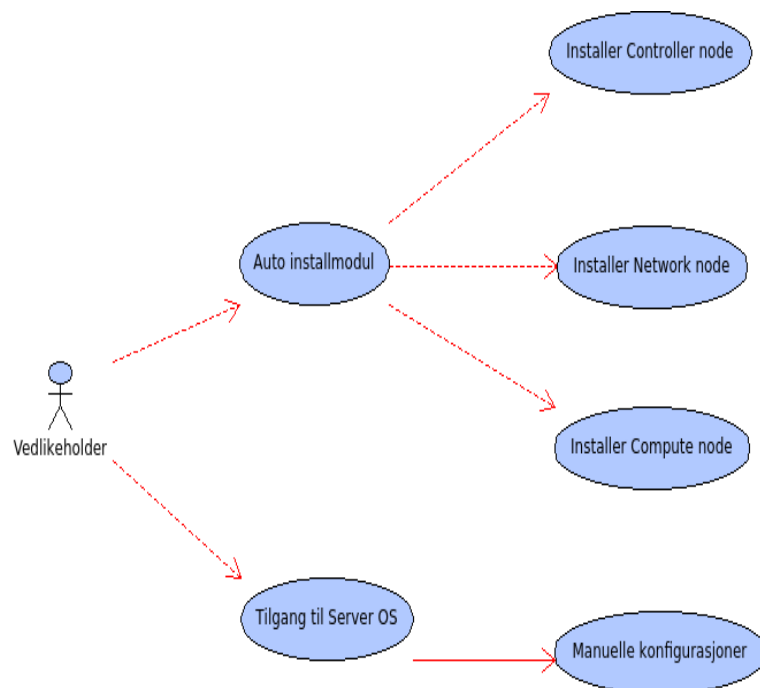
Kravene for funksjonaliteten av tjenesten vil være å få opp modulen som kjører webinterfacet til SkyHiGh. Webinterfacet ligger på Controller node-en i modulen Horizon. For å kunne sette opp Controller node-en er vi nødt til å ha en server å jobbe på. Det er der login-screenet skal være. Login-screenet skal autentiseres mot Feide, det vil også si at vi er nødt til å få opp en testbruker hos Feide. Feide bruker SAML 2.0 som er et xml-basert språk for autentisering.

For at vi skal få autentisert med forskjellige roller må vi legge til noen ekstra metadata til SAML 2.0 dokumentet. Vi må også studere hvordan autentiseringen foregår mellom Horizon- og Keystone modulene for å kunne se hvilke data som sendes mellom de. Disse dataene trengs for å kunne konfigurere SAML 2.0 dokumentet til å ta imot de rette dataene, for dette å kunne autentiseres som forskjellige roller. Så må vi konfigurere på Horizon hvilke oppgaver som skal være tillatt for de forskjellige rollene.

2.2.2 Use case diagram



Figur 1: Use case diagram 1



Figur 2: Use case diagram 2

2.2.3 Høynivå use case

Use case ID	Usecase-navn	aktør	Kompleksitet	Prioritet
1	Log in	Student og ansatt	Høy	1
2	Rolle: Normal rettighet	Student og ansatt	Middels	2
3	Rolle: Ekstra rettighet	Noen ansatte	Middels	2
4	Konfigurere VM-er	Lav	Studenter og ansatte	2
5	Konfigurere VM-instanser	Noen ansatte	Lav	2
6	Administrere VM-instanser	Noen ansatte	Middels	3
7	Auto install-modul	Vedlikeholder	Lav	3
8	Installer Controller node	Vedlikeholder	Lav	3
9	Installer Network node	Vedlikeholder	Lav	3
10	Installer Compute node	Vedlikeholder	Lav	3
11	Tilgang til server-OS	Vedlikeholder	Lav	3
12	Manuelle konfigurasjoner	Vedlikeholder	Lav	3

Use case ID	1
Use case navn	Log in
aktør	Ansatt og student
Beskrivelse	En bruker prøver å logge seg inn på SkyHiGh. Denne tar imot brukernavn og passord, samt informasjon om fylke.

Use case ID	2
Use case navn	Rolle: Normal rettighet
aktør	Ansatt og student
Beskrivelse	Med innloggingsinformasjonen til brukeren vil autentiseringsprosessen avgjøre hvilke rettigheter brukeren har.

Use case ID	3
Use case navn	Rolle: Ekstra rettigheter
aktør	Noen ansatte
Beskrivelse	Med innloggingsinformasjonen til brukeren vil autentiseringsprosessen avgjøre hvilke rettigheter brukeren har.

Use case ID	4
Use case navn	Konfigurere VM-er
aktør	Ansatt og student
Beskrivelse	Her kan de brukeren lage, endre, slette og bruke VM-er. Her er det restriksjoner på ytelse og mengde plass utifra hvilken rettighet brukeren har.

Use case ID	5
Use case navn	Konfigurere instanser med VM-er
aktør	Noen ansatte
Beskrivelse	Brukeren kan lage, endre, slette og bruke instanser med VM-er.

Use case ID	6
Use case navn	Administrere VM-instanser
aktør	Noen ansatte
Beskrivelse	Her har brukeren lov til å administrere de forskjellige instansene med VM-er.

Use case ID	7
Use case navn	Auto installmodul
aktør	Vedlikeholder
Beskrivelse	Denne modulen består enten at installerings-scriptet blir hentet fra en server, eller så er det en usbpinne som har tre forskjellige installeringer. Da er det bare å velge rett installering til rett modul i Openstack man skal installere.

Use case ID	8
Use case navn	Installer Controller node
aktør	Vedlikeholder
Beskrivelse	Script som kjører installasjonen av Controller noden.

Use case ID	9
Use case navn	Installer Network node
aktør	Vedlikeholder
Beskrivelse	Script som kjører installasjonen av Network noden.

Use case ID	10
Use case navn	Installer Compute node
aktør	Vedlikeholder
Beskrivelse	Script som kjører installasjonen av Compute noden.

Use case ID	11
Use case navn	Tilgang til server-OS-et
aktør	Vedlikeholder
Beskrivelse	Dette er direkte tilgang til serverne.

Use case ID	12
Use case navn	Manuell konfigurasjon
aktør	Vedlikeholder
Beskrivelse	Dette er hvis vedlikeholder trenger å installere noe mer på serveren eller konfigurere noe.

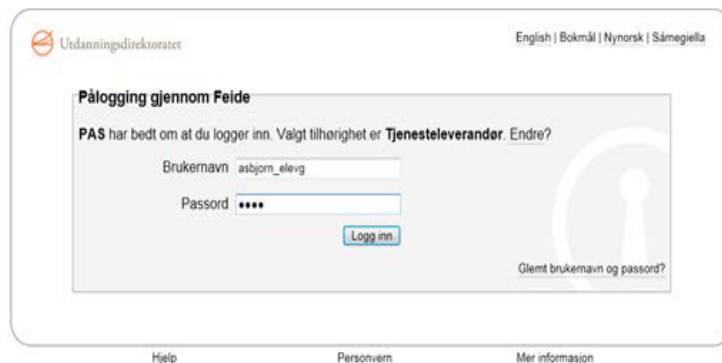
2.2.4 Detaljert use case

ID	3
Name	Rolle: Ekstra rettigheter
Aktør	Noen ansatte
Trigger	Hvis aktør kvalifiserer seg til å ha ekstra rettigheter.
<p style="text-align: center;">Normal hendelsesflyt</p> <ol style="list-style-type: none"> 1. Aktøren skriver inn log in-dataene. 2. Data blir sendt fra web-server til Feide. Dette skjer via simpleSAMLphp, autentiseringsdokument som er laget i SAML 2.0 som inneholder metadata og attributter. 3. Feide slår opp i LDAP-registeret til skolen med de valgte metadataene som brukes i autentiseringsdokumentet. 4. Sender informasjon om aktøren til web-serveren for at aktøren skal kunne se hvilke data som er registrert på han/henne. 5. Sender godkjenning til web-serveren. 6. Web-serveren viser skrivebord for brukeren. 7. Skrivebordet vises med adminrettigheter + at aktør har tilgang til ekstra ressurser. 	
<p style="text-align: center;">Variasjoner (gyldige alternativer og feilsituasjoner)</p> <ol style="list-style-type: none"> 1. Bruker kan taste inn feil innloggingsdata 2. Feil på nettverket så data ikke kommer fram 3. Finner ikke brukeren i LDAP-registeret, evt. kan brukeren være på feil plass i LDAP, noe som gjør at brukeren vil få feil rettigheter ved innlogging. 4. Feil på nettverket så data ikke kommer fram 5. Feil på nettverket så data ikke kommer fram 6. Webserveren funker ikke, eller at brukeren får feil skrivebord. 7. Feil rettigheter vanlig bruker kan få tilgang til adminrettigheter og omvendt. 	

ID	5
Name	Konfigurere VM-instanser
Aktør	Noen ansatte
Trigger	Hvis aktør kvalifiserer seg til å ha ekstra rettigheter.
Normal hendelsesflyt	
<ol style="list-style-type: none">1. Opprette forskjellige instanser med VM-er.2. Aktøren skal kunne Lage grupper med VM-er og sette brukere til gruppene. Hver gruppe med VM-er får et eget nettverk seg imellom.3. Aktøren skal kunne sette opp forskjellige ytelse utifra hva som trengs til de forskjellige instansene.4. Lagring av instanser som han/henne evt. vil bruke om igjen5. Sette opp lagrede instanser6. Endre medlemsgruppen til instansene7. Opprette nye ferdig-instillinger med ytelse som kan tas i bruk.8. Legge til ferdig ytelseinstillinger til instanser	
Variasjoner (gyldige alternativer og feilsituasjoner)	
<ol style="list-style-type: none">1. Kan ikke opprette instanser som vanlig bruker	

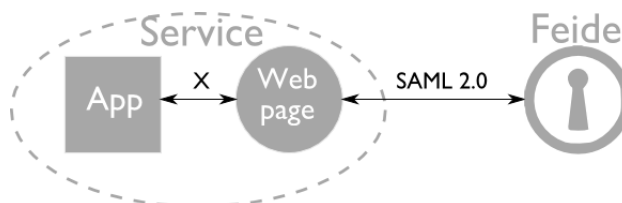
ID	7
Name	Auto-install modul
Aktør	Vedlikeholder
Trigger	Vedlikeholder som har tilgang til serverne
<p style="text-align: center;">Normal hendelsesflyt</p> <ol style="list-style-type: none"> 1. Starter server server har to valg, sette boot på web server eller boot med en USB-pinne. <ol style="list-style-type: none"> 1a. Webserver: velger hvilken type server som skal installeres fra webserver. <ol style="list-style-type: none"> 1a1. Controllernode-installasjon 1a2. Networknode-installasjon 1a3. Computenode-installasjon 2a. USB-pinne: velger hvilken type server som skal installeres fra USB-pinne. <ol style="list-style-type: none"> 1a1. Controllernode-installasjon 1a2. Networknode-installasjon 1a3. Computenode-installasjon 2. Velger hvilken installasjon og trykker «enter». 3. Serveren vil bli installert med Ubuntu server 12.10 med preseed. 4. Preseed-en kjører en installasjon uten interaksjon, det vil si med ferdig valgte konfigurasjoner for Ubuntu server-installasjonen. 5. Når serveren er ferdig installert, vil den kjøre kommandoer som ble sagt i preseed-filen før den blir ferdig installert. Kommandoene den kjører vil være wget av filer som trengs for installasjonen av den spesifikke serveren. 6. Script for å installere serveren som «Controllernode», «Networknode» eller «Computenode» blir kjørt utifra hvilke valg som ble gjort i 1. punkt. <p style="text-align: center;">Variasjoner (gyldige alternativer og feilsituasjoner)</p> <ol style="list-style-type: none"> 1. Klarer ikke å gjøre en boot. 2. Aktøren velger feil installasjon. 3. Finner ikke fil for installasjon av serveren eller finner ikke preseed filen. <ol style="list-style-type: none"> 3a. preseed-filen er feil og det vil kunne oppstå interaksjon ved installasjonen. Dette vil medføre at installasjonen ikke vil være automatisert. 	

2.2.5 Funksjon



Figur 6: Et eksempel på innlogging med feide

På figuren over kan du se hva som møter brukeren. På dette stadiet er det kun to datatyper, det er brukernavn og passord. Hendelsesscenarioet er som figuren under.

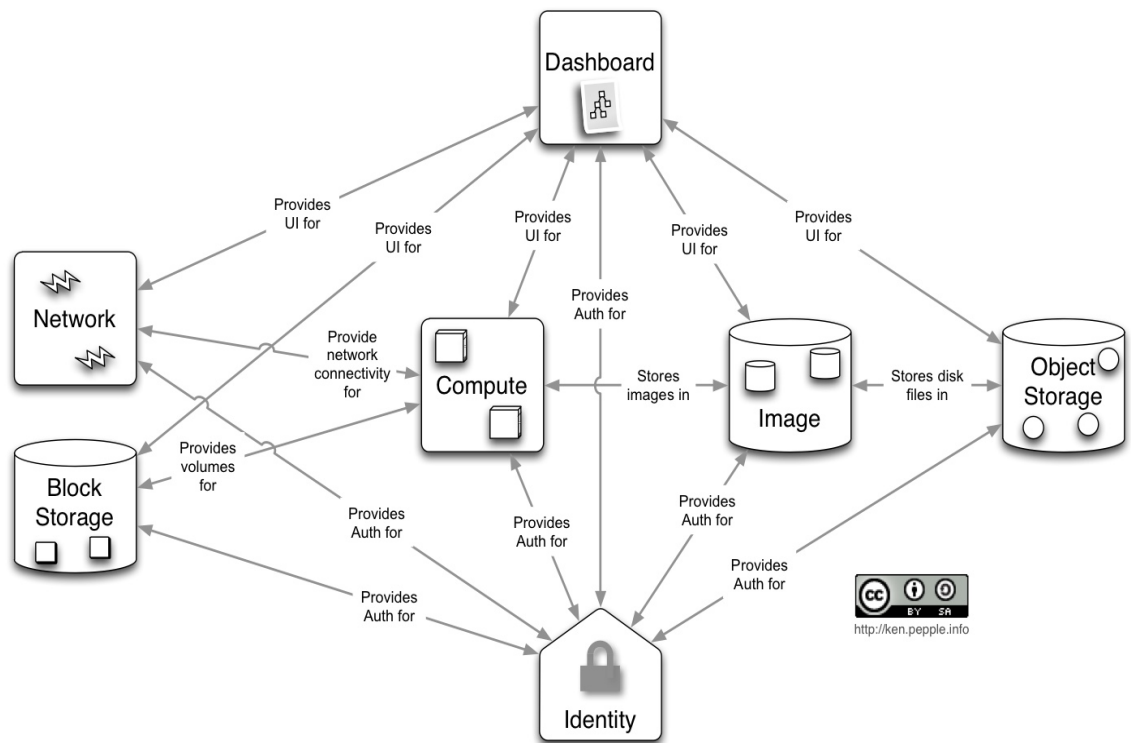


Figur 7: Hvordan autentiseringen foregår

Webserveren er på kontrollernoden, Openstack-systemet er det vi kan referere til som appen på figuren over. Horizon er den som refereres til som “web page” på figuren, det er her vi skal lage innloggingsskjermen som vist på første figur.

- Input - Brukernavn og passord fra brukeren.
Skriver inn info, info-en blir sendt videre til Feide som er autentiseringsdatabase. Feide sjekker om bruker har tilgang og hvilken rolle brukeren har. Sender deretter info tilbake til “web page-en”.
- Output - Enten får brukeren at passord og brukernavn er feil, eller så kommer brukeren seg inn. Da vil brukergrensesnittet på Horizon vise seg for brukeren og brukeren kan lage, endre, slette og bruke VM-er utifra hvilken rolle/autentisering brukeren har.

2.2.6 Struktur og tverr-relasjoner



Figur 8: Hvor går autentiseringstrafikken

Som du kan se på figuren over så går all autentifikasjon mellom dashboard og identity. Dashboard er Horizon og identity er Keystone. Horizon har kun autentisering mot keystone, det vil si at all vesentlig autentiseringsdata som keystone får går til Horizon.

Vi skjønner ut fra figuren, for at å autentisere mot FEIDE, så må vi vite hvilke data som kommer fra keystone. Når vi vet om de, så vet vi også hvilke data vi skal sende videre fra Horizon til FEIDE, utenom de obligatoriske attributtene ().