Auktorisation och grupphantering

FIM vs Grouper

Webadress https://portal.nordu.net/display/Inkubator/Projektrapporter			
Dokumentnamn FIM vs Grouper.pdf			
Dokumentansvarig Jan Rundström			
Dokumentidentitet N/A	**Version** 1.0	**Datum** 2014-19-02	**Status** Publicerad

Innehåll

1 Verktyg för grupphantering

Utredningen fokuserar på två verktyg för grupphantering. Microsoft Forefront Identity Manager (FIM) och open source-verktyget Grouper. Valet beror på att dessa två verktyg har väckt mest intresse hos svenska U/H.

2 Grouper

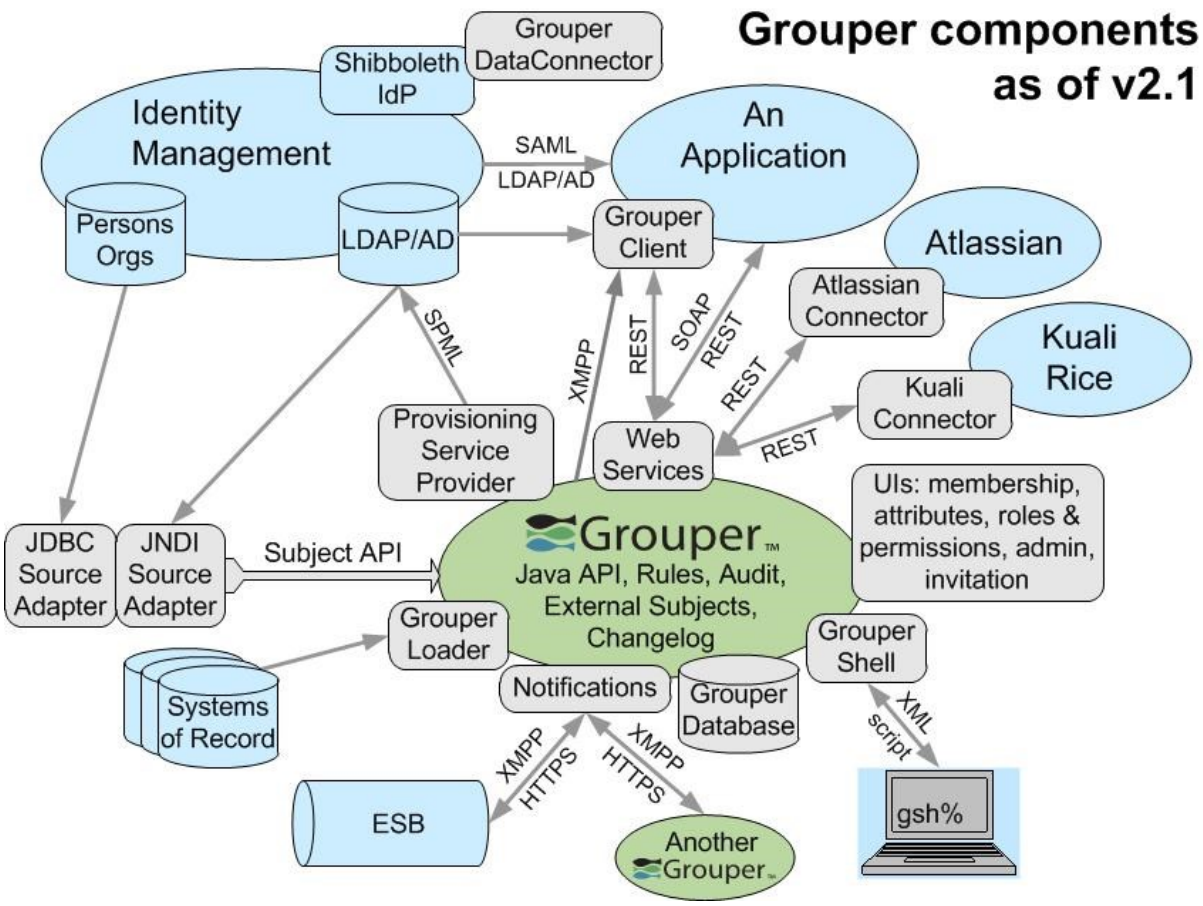
Internet2 är en amerikansk organisation som har till syfte att stödja forskning, utbildning och offentlighet med att kunna producera och samarbeta med hjälp av ny teknik. Internet2s medlemmar är främst universitet. Men även näringsliv, diverse statliga organ och (internationella) utbildningsnätverk finns med som medlemmar och intressenter.

Middleware Architecture Committee for Education (MACE) är en gruppering av IT-arkitekter inom amerikanska universitetsvärlden vars syfte är att främja interoperabilitet och federering inom identitets- och behörighetsinfrastruktur som används och skapas inom universitetsvärlden.
Inom ramen för samarbetet Internet2 Middleware Initiative där MACE finns med skapades grupphanteringssystemet Grouper.

Grouper rubriceras som ett Access Managementsystem specialiserat för universitet. Betoning ligger därför på distribuerad styrning av grupptillhörighet, roller och rättigheter för en identitet. Information som i sin tur ger möjligheter att skapa nya behörigheter. Grouper betonar ad hoc teams, distribuerat/delat ägarskap av forskargrupper mm. Det finns tydliga inslag av universitetsvärldens rörliga organisationsformer inkluderat i grundtankarna. Grouper går under Apatche 2 open source licens.

2.1 Groupers arkitektur

Kärnan i Grouper består av ett Java API, en regelmotor, en audit- och loggmodul, och en modul för interaktion med ett Identity Management system. Naturligtvis måste kärnan kopplas ihop med en databas.



Runt kärnan finns ett stort antal moduler för integration, olika varianter av GUIs och diverse verktyg för att förenkla handhavande och automatiseringar. Tillsammans bildar dessa Grouper toolkit.

2.1.1 Grouper toolkit moduler

Modul/verktyg	Funktion
Installer	Installerar Grouper API, quickstart data, UI, WS, klient och Provisioning Service Provider.
Grouper API	Kärnan av kärnan i Grouper.
Subject API	Hanterar interaktion med Identity Management plattformen.
Grouper DB	Reposatory för Grouper data.
Grouper shell	Shellverktyg för att interagera med API:t. Inkluderar även import/export av xml.
WS services	Verktyg för att jobba med REST/SOAP integrationer.
Grouper client	En javaklient för att hålla reda på Web Services.
Grouper loader	Ett synkroniserings- och integrationsverktyg.
Grouper daemon	Verktyg för att skapa/köra automatiska processer/uppgifter.
Lite UI	En GUI modul. Mest för slutanvändare. Webbaserad.
Admin UI	En GUI modul. För administratörer.
Attribute framework	För koppling av metadata till diverse objekt.
Notification/Changelog	Loggar händelser och kan konfigureras att skicka händelsemeddelanden till externa system.
Access Management	Modul för att skapa attribut, roller, regler och behörigheter. Kopplingsplinten i Grouper.
Rules	En motor för script som applicerar regler på Grouperobjekt.
External users	Stöd för externa och federerade användare.
Diagnostics	Test- och rapporteringsverktyg för Groupers interna status.
Provisioning Service Provider (PSP)	Håller reda på exporter av Grouperobjekt till externa resurser.

Förutom modulerna ovan finns ett antal specialconnectorer att tillgå för att underlätta integrationer. Här är några exempel:

- Enterprise Service Buss
- Kuali
- Atlassian
- Grouper/VOOT
- Grouper to Grouper
- Uportal

2.2 Summering Grouper

Grouper är ett grupphanteringsverktyg för universitet utvecklat av universitet. Det finns en rad moduler som underlättar integration med typiska universitets- och open source-mjukvaror. Verktyget speglar universitetsmentalitet. Det finns stora möjligheter, men det kräver också en del. En intressant och bra detalj är den omfattande dokumentationen och mängden manualer som finns. Välordnat och ofta i form av videoinstruktionsfilmer. Communityn förefaller aktiv och kapabel. Intrycket är att buggar rättas och ny funktionalitet läggs till i hög takt.

Fördelar

- Ingen licens eller investeringskostnad för mjukvara
- Stödjer diverse temporära/föränderliga organisationsformer vanliga i U/H-världen,
- Decentraliserar vissa administratörsuppgifter (potentiellt mindre belastning på IT-avdelningen)
- Förmåga att tilldela roller internt i grupper. Till exempel administratör för gruppen. Som i sin tur kan lämna över sina rättigheter till en ny administratör inom gruppen.
- Fullskaligt grupphanteringsverktyg
- Stor möjlighet att påverka mjukvaran (open source)
- Rikliga integrationsmöjligheter (Alla vedertagna tekniker plus specialconnectorer)
- Erfarenheter finns. Uppsala universitet har Grouper i drift sedan 2012

Nackdelar

- Svårt att hitta kompetens i Sverige. (Extremt få konsulter tillgängliga, om ens någon.)
- Kräver vana att jobba med open source
- Större möjligheter, men kanske också krångligare än FIM, vad gäller grupphantering?

3 FIM

FIM är Microsofts produkt för hantering av digitala identiteter, rättigheter och grupper. Egentligen rubriceras FIM som ett verktyg för Identity Lifecycle Management (ILM). Det vill säga att huvuduppgiften är att hantera identiteter och förändringar av deras status över tid. Identitetshantering och grupphantering hör ihop. Inga identiteter, inga medlemmar att bygga grupper av. Ett väl fungerande identitetshanteringssystem är ett krav för grupphantering oavsett verktygsval.

Kopplingen till Active Directory och Exchange Server med flera MS produkter är naturligtvis stark. FIM möjliggör synkronisering av användaridentiteter, certifikatshantering, lösenordsreset och förmedling/export av rättigheter med mera från en och samma plattform och administratörs GUI.

FIM är idag en sammanslagning av Microsofts tidigare produkter Microsoft Identity Integration Server 2003 (MIIS) och Certificate Lifecycle Manager (CLM).

Utveckling och konfigurering av FIM sker i .Net. Centrala kunskaper för utvecklaren är Windows Communication Framework och Windows Workflow Foundation. FIM körs på Microsoft Server och behöver Microsoft SQL Server, MS Sharepoint för FIM portal samt MS IIS för web services.

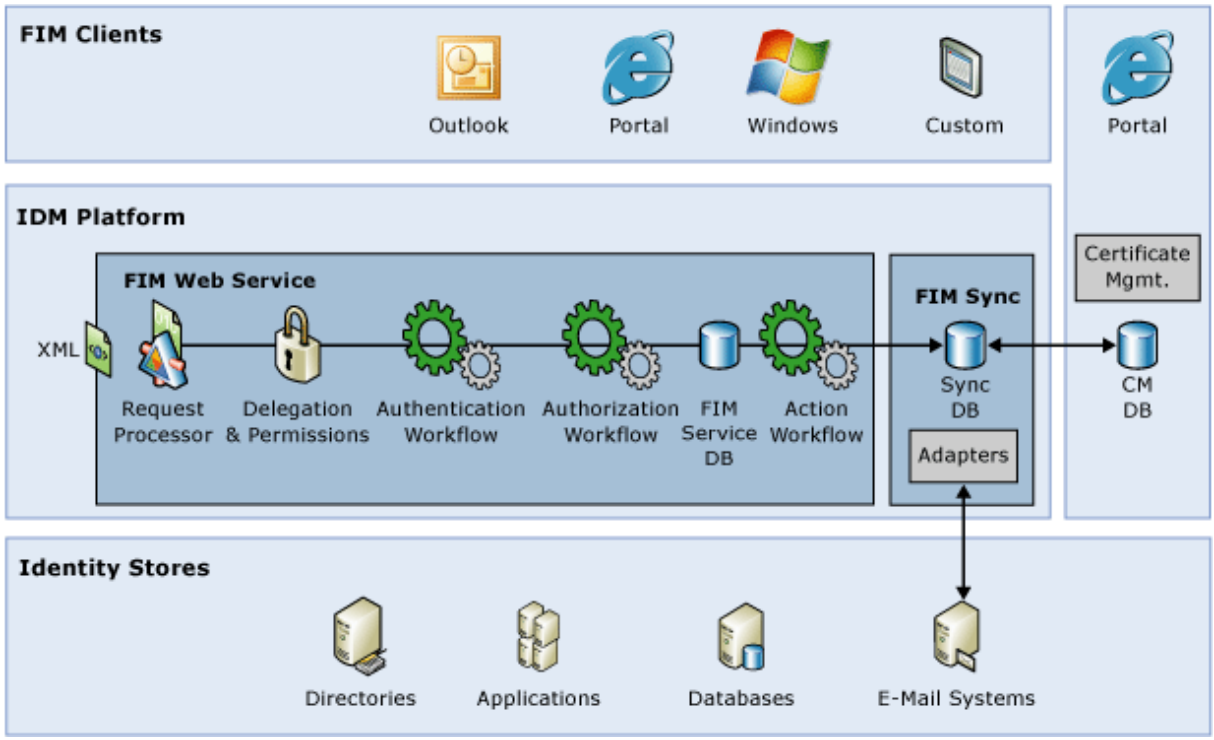
3.1 FIMs arkitektur

Här följer en kort genomgång av FIMs arkitektur.

3.1.1 IDM platform - Web & Synchronization services

FIM Service (heter FIM Web service i bilden) och FIM Synchronization Service utgör tillsammans den så kallade IDM (Identity Management) plattformen. Då det mesta som händer i FIM är workflowbaserat är det

FIM service som gör det logiska jobbet för att sedan vidarebefordra sista delen av uppgiften, import och export av data, till FIM Synchronization Service. Export sker genom så kallade Management Agents (MA) som är connectorer mot diverse mottagare som till exempel AD, LDAP och Web Services.

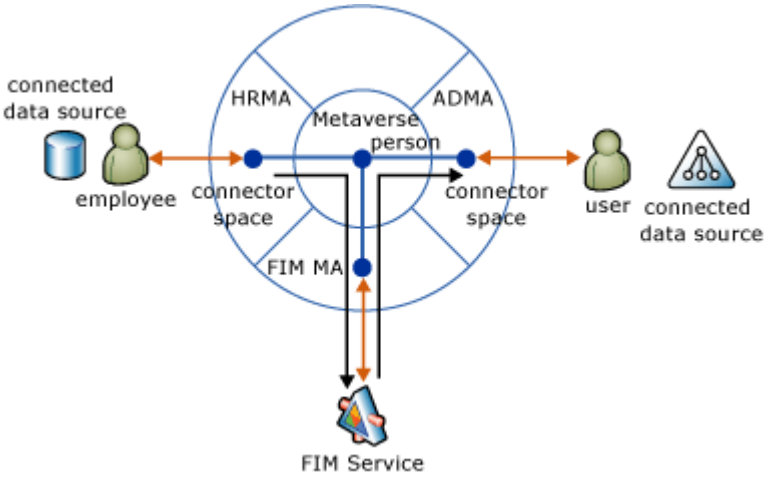


3.1.2 FIMs databas

FIM använder databasen för att lagra data som ett mellansteg mellan olika workflow- och processteg. Databasen lagrar också policys och objekt, till exempel data för sammanställda identiteter. Se Metaverse nedan.

3.1.3 FIM Metaverse

FIM Synchronization Services använder databasen för att lagra en kopia på data från uppkopplade datakällor. Data runt en identitet sammanställs (från flera källor via så kallade connector spaces) i Metaverse. Synchronization Service kan på så sätt tillgå sammanställt data för synkronisering av alla tänkbara konsumenter.



3.1.4 Identity stores & MAs

Identity stores eller connected data sources är externa system som FIM integreras mot genom Management Agents (MAs). Här följer en lista på standard MAs.

- AD av alla former
- IBM Tivoli Directory Server
- Sun ONE and Netscape Directory Servers
- FIM Certificate Management
- MS Exchange
- Lotus Notes
- SQL Server
- IBM DB2
- Oracle DB
- Textfiler av alla former
- Directory Services Markup Language
- LDAP
- SAP R/3 Enterprise

3.1.5 FIM klienter

Den övre bilden visar ett antal FIM klienter. Här följer en förteckning av de vanligaste:

- FIM Synchronization Service
- FIM Portal (MS Sharepoint)
- MS Exchange
- MS Office
- Windows PowerShell
- Custom Windows Communication Foundation (WCF) klienter

3.2 Summering FIM

MS FIM är ett grupphanteringsverktyg där grupphanteringen egentligen bara är en del av Identity Lifecycle processen. FIM integrerar bra i ett sammanhang där det finns många MS produkter och där infrastrukturen bygger på MS plattformen. Vilket torde vara lejonparten av svenska universitet. FIM är en mindre specialiserad produkt vad gäller grupphantering än Grouper. Viss funktionalitet saknas för att de skall vara helt jämförbara. Till exempel förmågan att distribuera administratörskap över gruppen inom gruppen.

Fördelar

- MS plattformen är känd och bekväm för många U/H
- Lättare att hitta konsultkompetens än för Grouper
- Sannolikt finns kompetens för diverse delar av MS infrastruktur som behövs i FIM på plats
- Blir en single point applikation för ILM & grupphantering för den som vill
- Rikliga integrationsmöjligheter mot framför allt MS produkter
- Åtminstone två universitet (LIU & Lunds Universitet) ligger i startgroparna för att använda FIM både som ILM och grupphanterare. På SLU används FIM idag som ILM verktyg.

Nackdelar

- Licenskostnad
- I första hand en ILM applikation (kan även vara en fördel)
- Inget universitet har FIMs grupphantering i drift (vad vi känner till)
- Inte lika samspelt som Grouper med vissa typiska universitetsmjukvaror
- Lite mindre möjligheter, men kanske enklare än Grouper, vad gäller grupphantering?
- Enligt uppgift ett grovt och svårjobbat WS API, som helst skall kompletteras med flera specialskrivna lager för att vara enkla att jobba med och ge snabb affärsnytta.

4 Vilket verktyg skall väljas?

På papperet finns ingen vinnare som passar alla. En framtida inkubatorutredning (2014) kommer sannolikt att belysa valet mer. Men ett antal tankegångar runt valet kan presenteras här:

- Är det dags att ta stora investeringar runt ILM?
  - Gemensam hanteringar av identiteter och grupper i samma verktyg kan vara klokt
  - Fördel FIM
- Är organisationen tung när det gäller en viss teknik?
  - Mycket .Net och Microsoft kompetens. Fördel FIM
  - Mycket kompetens inom Javaplattformen. Fördel Grouper
- Är open source viktigt?
  - Fördel Grouper
- Är det något speciellt typ av integrationer som väger tungt, givet de use case som skall införas?
  - Fördel Grouper i vissa fall. Fördel FIM i andra. Se specialiteter ovan.
- Kommer införandeprojektet att vara konsulttungt?
  - Sannolikt fördel FIM
- Är det aktuellt att pressa ut max ur grupphanteringsfunktionerna?
  - Sannolikt fördel Grouper