

Voordat ik dieper inga op de werking FIM 2010, geef ik eerst een algemeen overzicht over de positionering van dit artikel.

Als de opvolger van Identity Lifecycle Manager 2007 (ILM), maakt FIM onderdeel uit van een groter geheel: het Microsoft Identity & Access management (MS-IDA). Naast FIM maken ook volgende producten deel uit van dat IDA-platform:

- Forefront Unified Access Gateway 2010
- Windows Server 2008 (R2) met Active Directory (AD) en AD Federation Services
- Windows 7

Het Identity and Access Management platform maakt met zijn specifieke producten weer deel uit van een groter geheel: de Microsoft Business Ready Security solutions (BRS).

BRS in een notendop



Figuur 3: **overzicht Microsoft Business Ready Security**

De nieuwe generatie van security producten wordt door Microsoft op de markt gebracht via een allesomvattende set van vijf oplossingen:

- *Secure Messaging Solution en Secure Collaboration Solution*
Deze maken het mogelijk om veiligere bedrijfscommunicatie (messaging) en veiligere samenwerking (collaboration) op te zetten vanaf alle locaties op alle gebruiker devices, waarbij toegang tot vertrouwelijke informatie gereguleerd wordt.
- *Secure Endpoint Solution*
Geeft beveiliging op client- en server besturingssystemen en voorkomt verlies van informatie, zonder dat dit ten koste gaat van de toegangsmogelijkheden.
- *Information Protection Solution*
Registreert, beschermt en beheert vertrouwelijke gegevens in samenwerking met de bedrijfsystemen en bedrijfsapplicaties.
- *Identity and Access Management Solution*

Maakt het mogelijk om een beter beveiligde toegang te op te zetten op basis van identiteiten, zowel binnen eigen infrastructuur als in de cloud.

In dit artikel beperk ik me tot Forefront Identity Manager 2010.

Laten we even verder ingaan op hoe FIM het mogelijk maakt om identiteitsbeheer te vereenvoudigen.

FIM maakt gebruik van degelijke en stabiele synchronisatie- en provisioning-capaciteiten van de 'ILM 2007'-motor, waar ook certificaat- en smartcardbeheer (CLM, certificate lifecycle management) deel van uitmaken. FIM voegt daar een rijke beheersomgeving aan toe, inclusief workflows, integratie met MS Office, self-service functionaliteit voor eindgebruikers, delegatie, beheer van groepen en distributielijsten.

Wat heb je nodig om met FIM te kunnen starten?

Wat betreft componenten, heeft u aan infrastructuur aan de serverkant nodig:

- Windows Server 2008 (of R2) 64-bit Standard, Enterprise or Datacenter Editions
- SQL Server 2008 64-bit Standaard of Enterprise Editie vanaf SP1
- Web Server Internet Information Server 7 (IIS7)
- Windows SharePoint Services 3.0 SP1
- Optioneel Windows SharePoint Services 3.0 Language Pack, omde FIM portal in een andere taal dan het Engels weer te geven
- Microsoft .NET Framework 3.0
- Microsoft .NET Framework 3.5 SP1
- Exchange 2007 SP1 Management Console om Exchange Server 2007 mailboxes aan te maken
- Windows Installer 4.5
- Windows PowerShell 1.0 voor het aanmaken van Exchange Server 2007 mailboxen
- Windows PowerShell 2.0 voor het aanmaken van Exchange Server 2010 mailboxen

Om de client componenten van FIM te ondersteunen, heeft u het volgende nodig:

- Windows XP Professional SP2 of later (32-bit), Windows Vista Enterprise SP1 of later, 32- of 64-bit, Windows 7 Profes-

- sional of Ultimate (zowel 32- als 64-bit)
- Windows Installer 3.1 or later (only needed if running Windows XP SP2)
- Microsoft .NET Framework 3.5 SP1

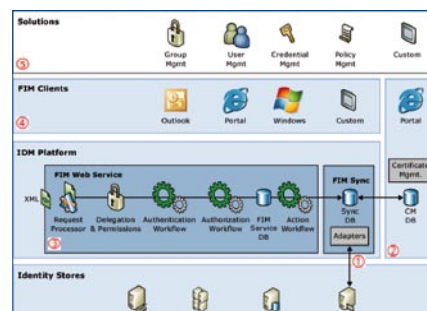
Als u de Forefront Identity Manager add-in voor Office 2007 gebruikt:

- Microsoft Office Outlook 2007 Service Pack 2
- Microsoft Forms .NET 2.0 Programmability Support
- Smart Tag .NET Programmability Support for Microsoft Office 2007
- .Net Programmability Support for Microsoft Office Outlook

Raadpleeg voor meer details de FIM product pagina het onderdeel *System Requirements*.

Hoe zit FIM in elkaar?

Dit schema geeft u een goed overzicht over de opbouw:



Figuur 4: **Overzicht structuur FIM 2010**

Op bovenstaand schema ziet u de vijf hoofdcomponenten:

1. FIM Synchronisation Service: deze zorgt ervoor dat de externe bron-data-systemen en doelsystemen datastromen kunnen leveren en ontvangen. Dit onderdeel kent een aantal verbeteringen ten opzichte van ILM.
2. Certificate Management: dit onderdeel maakt het automatisch beheer van certificaten mogelijk. Zoals u kunt zien, is er nu ook een connector die met de FIM-Sync engine verbonden is. Sinds ILM 2007 Feature Pack 1 maakt Certificate Lifecycle Manager (CLM) deel uit van de oplossing. CLM heeft zijn eigen management in een web-portal.
3. FIM Web Service: dit is een belangrijk, nieuw component bovenop de synchronisatie engine. Ik zal de belangrijkste

Beveiliging

onderdelen nog verder doornemen, maar nu ziet u alvast de volgende onderdelen in het schema:

- a. Request Processor: ontvangt de binnenkomende requests en verzorgt de nodige processen en activiteiten die in de FIM-functionaliteit voorzien
 - b. Delegation & Permissions: FIM biedt de mogelijkheid om beheer te delegeren, dus iemand voor een andere persoon het beheer laten doen. Uiteraard wordt gecontroleerd of hiervoor de juiste rechten zijn.
 - c. Authentication Workflow: verzorgt een workflow achter de procedures om de identiteit van de gebruiker te controleren. Enkele voorbeelden zijn de password reset gate en de *smartcard authenticatie gate*. Ze zorgen ervoor dat u enkele extra vragen moet beantwoorden voordat u uw password kan herstellen, of dat er een smartcard moet worden gepresenteerd om de identiteit te bewijzen.
 - d. Authorization Workflow: verzorgt een workflow om ervoor te zorgen dat een request wordt gevalideerd, nog voor dat de aanvraag naar de FIM-database doorgestuurd wordt, bijvoorbeeld validatie van gegevens en rechten.
 - e. Action Workflow: dit verzorgt een workflow achter een zogenoemde actie binnen FIM, zoals een bevestiging met e-mail versturen of een extra wijziging in de FIM Service database uitvoeren.
4. FIM Clients, er zijn vier typen FIM-clients:
- a. Outlook: deze add-in geeft de mogelijkheid om vanuit Outlook 2007 groepen te beheren en aanvragen voor het deelnemen aan groepen goed te keuren of af te keuren.
 - b. Portal: standaard is er een FIM-management webinterface die met behulp van Sharepoint Portal met de FIM Service communiceert. Naast de management webinterface biedt de FIM-service ook een password-reset portal aan die het mogelijk maakt om in een webinterface een password opnieuw in te stellen.
 - c. Windows: nieuw voor Windows binnen FIM is *FIM-Password en authentication extensions*. Deze is ondermeer zichtbaar in het aanlogscherm van de Windows-client. Onder de

extra knop is het voor een gebruiker mogelijk om - na het beantwoorden van een aantal veiligheidsvragen - het password te wijzigen. Dit is natuurlijk erg handig als de gebruiker zijn password is vergeten en niet meer kan inloggen op het systeem.

- d. Custom: onder uitzonderlijke omstandigheden of omwille van zeer speciale wensen, volstaan de drie standaard clients niet. In dat geval is het mogelijk zelf een client te ontwikkelen. Dat kan door gebruik te maken van de open standaard WS-* (uitgesproken als WS-star) die FIM ondersteunt.
5. Solutions: onderdelen die in het schema beschreven staan, zijn niet zo zeer technische componenten van FIM, maar een aantal out-of-the box scenario's die FIM biedt. Daarmee kunt u makkelijk aan de slag. Een paar voorbeelden zijn dynamisch beheer van security groepen en distributielijsten, geautomatiseerd user management, passwordbeheer en passwordsynchronisatie en de self-service portal.

FIM basis componenten

In dit artikel is er onvoldoende ruimte om elke component tot in detail te bespreken, dus ik beperk me hier tot de belangrijkste.

FIM Synchronisatie service

Deze component verzorgt de verbindingen met de externe bron- en doelsystemen. Ook de doorvoer van data naar de FIM-webservice en de FIM-portal worden door de sync-engine verzorgd. Net zoals ILM 2007, werkt FIM "agentless". Dit betekent dat het niet nodig is om op externe systemen clientsoftware te installeren.

De sync-engine regelt ook de synchronisatie, net zoals de provisioning. Dit behelst het aanmaken van nieuwe objecten en verwijderen van objecten uit de systemen.

Ik heb al eerder users en groepen genoemd. Maar 'objecten' kunt u in deze context zeer breed interpreteren. Ook organisaties, organizational-units, functies, rollen kunnen door FIM worden beheerd. U kunt vrijwel elk type systeem aan FIM koppelen. Standaard ondersteunt FIM 2010 een uitgebreide lijst platformen. De details vindt u in de FIM 2010 FAQ. Kijk

voor de URL in de verwijzingen onder dit artikel. In de lijst van management-agents (connectors) vindt u ook de extensible Management Agent (XMA) terug. Daarmee is het mogelijk om zelf management-agents te bouwen. Er zijn op internet zelfs een aantal open source XMA's vinden.

Certificate management (CLM):

CLM maakt het mogelijk om het certificaat-management en smartcard management te automatiseren. Er zijn daarbij koppelingen mogelijk met 3rd party PKI Certificate Authorities.

CLM wordt met FIM meegeleverd en heeft een eigen webmanagement interface. Met behulp van de CLM-managementagent wordt CLM gekoppeld aan FIM.

FIM Web service:

De FIM webservice is de belangrijkste innovatie in FIM.

Een belangrijke verbetering ten opzichte van de vorige versie is de codeless provisioning. Deze nieuwe functionaliteit maakt dat de ontwikkeling van programmacode overbodig is geworden voor de aanmaak van objecten in externe systemen.

Ook de mogelijkheid om workflows te beheren binnen de FIM-managementinterface is een opvallende nieuwe functie. De workflows in FIM zijn gebaseerd op *Windows Workflow Foundation*. Dit maakt het mogelijk om in FIM workflows te configureren of ze buiten FIM aan te maken en vervolgens te importeren.

Ook bevat de FIM-portal een grote hoeveelheid voorgeconfigureerde componenten, de tijd die u nodig hebt om bedrijfsspecifieke zaken te implementeren is, wordt een stuk korter.

Het is belangrijk te vermelden dat FIM gebruikmaakt "WS-*" API's. API staat voor 'application programming interface'. De API's laten toe dat andere software met FIM kan communiceren. Daarbij is WS-* een open standaard die ondersteund wordt door een groot consortium van bekende bedrijven zoals IBM, RSA en VeriSign. Een andere grote verandering is de management interface. Microsoft heeft de webinterface opnieuw

vormgegeven en vervalt makkelijker in het gebruik gemaakt, zodat u snel er uw weg in kan vinden.

FIM uitrol scenario's

FIM biedt een aantal interessante mogelijkheden om uw infrastructuur redundant op te bouwen.

Er zijn er drie strategieën om FIM te installeren.

1. Alle componenten samen op één systeem
2. Alle componenten apart
3. Iets daar tussenin

Elke strategie heeft zo zijn voor- en nadelen. Bij alles op één systeem heeft FIM een beperkte footprint, maar door in stappen componenten op aparte systemen te installeren, kan FIM flexibel worden opgeschaald. Het is dus technisch mogelijk om alles op één machine te zetten, zowel de FIM-service, als de FIM-portal, de FIM-database en zelfs de CLM componenten. Er is dan wel een single-point-of-failure. Als er iets misgaat met dat ene systeem, stopt alle FIM-functionaliteit. Alles op één systeem is voor productie omgevingen niet aan te bevelen, maar dit kan wel handzaam zijn voor test- en demonstratiedoelinden.

Een compleet andere benadering is om alle componenten apart van elkaar te installeren. Dan zijn er de volgende mogelijkheden:

- De FIM Synchronisatie-service kan losgekoppeld worden van de FIM-service
- De FIM-service kan losgekoppeld worden van de FIM-portal
- De FIM-databases kunnen op een ander toestel worden gehost dan de FIM-service, FIM Sync-service en de optionele CLM
- FIM ondersteunt SQL-clustering, gebruik hiervan verhoogt de beschikbaarheid van de database
- De FIM-service is een Webservice die opschalen ondersteunt
- De FIM-portal maakt gebruik van een Sharepoint-portal die redundant kan worden uitgevoerd

Op deze manier kunt u een hoogredundante en foutbestendige omgeving samenstellen.

Maar het heeft vanzelfsprekend belang-

rijke consequenties voor de aanschaf van ondermeer hardware en besturingssysteemlicenties die nodig zijn om servercomponenten uit te splitsen.

Daarom wordt er in de praktijk een middenweg gekozen. Een goede afweging tussen het aantal servers en de vereiste redundantie maakt het mogelijk om binnen een redelijk budget toch voldoende zekerheid te bieden op de verschillende componenten.

Als u dit verder wil uitspitten, is de FIM 2010 Capacity Planning Guide een handig startpunt ([http://technet.microsoft.com/en-us/library/ff400279\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/ff400279(WS.10).aspx)).

Licentiekosten

Wat betreft licenties, heeft de lancering van FIM 2010 begin maart dit jaar ook goed nieuws gebracht. Voor ILM 2007 was oorspronkelijk één serverlicentie nodig per actieve server, onafhankelijk van de hoeveelheid en type objecten, aantal attributen of datasystemen die u aan ILM koppelde. Met de integratie van CLM, had u ook CALs (Client Access Licenses) nodig voor elk certificaat dat door ILM werd beheerd.

In FIM 2010 is het licentiemodel veranderd. De enkele serverlicentie blijft behouden, maar de wijziging betreft de vereiste CALs. FIM vereist nu ook een CAL voor het gebruik van de nieuwe functionaliteit. Samengevat:

- Serverlicentie: alle instances van *FIM-serversoftware* vereisen een FIM 2010 Serverlicentie
- U heeft een client access licentie nodig voor:
 - o Elke gebruiker van wie de identiteit of het certificaat door FIM 2010 wordt beheerd
 - o Elke gebruiker die de FIM 2010 software gebruikt zoals administrators
 - o Externe gebruikers

Het is belangrijk te weten dat er voor externe gebruikers twee definities zijn. U kunt voor elke gebruiker (dit is een identiteit of certificaat) een CAL aanschaffen of u koopt een 'External Connector' -licentie. Een External Connector-licentie is nodig in specifieke scenario's, bijvoorbeeld als u business-partners,

klanten of externe gebruikers toegang wilt geven tot uw netwerk. Microsoft specificeert een externe gebruiker als een persoon die geen werknemer is of niet gelijkwaardig is aan eigen personeel. Een externe gebruiker kan daarnaast een persoon zijn aan wie u hosted services levert. Een External Connector kan voordeliger zijn dan een CAL per user als u een groot aantal externe gebruikers hebt.

U kunt alles nog eens nalezen op de FAQ op de Microsoft FIM 2010 website: <http://www.microsoft.com/fim>.

Naast technische documentatie is er een interessante lijst van webcasts. En als u met FIM aan de slag gaat, zal u snel merken dat het Forefront Identity Manager 2010 Technet forum een belangrijke hulpbron voor u wordt, waar u makkelijk en snel contact kan maken met het productteam of de community van FIM-gebruikers en FIM-experts.

PETER GEELLEN is MVP voor ILM en Microsoft Certified Trainer. Peter Geelen werkt meer dan 12 jaar in de ICT. Hij heeft vele IT & netwerk projecten begeleid en uitgevoerd, inclusief implementaties van servermanagement. Hij werkt als Senior Consultant bij Traxion in België (<http://www.traxion.com>), in Identity & Access Management, en is verantwoordelijk voor MIIS, ILM, FIM 2010, Omada Identity Manager, IAG, ADFS en andere IDM systemen, single sign-on solutions en security-solutions. Verder is hij oprichter en voorzitter van de Microsoft Security User Group Belgium (<http://www.winsec.be>).