John Reijnders
werkt als Microsoft Architect bij LogicaCMG en is voorzitter van het Technology Cluster Directory Services bij LogicaCMG. http://www.logicacmg.com

Active Directory in Application Mode

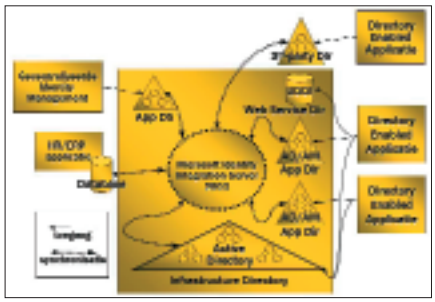
HET ONTBREKENDE STUK VAN DE PUZZEL?

Met de introductie van een 'light versie van Active Directory' die onder andere bedoeld is voor applicatieontwikkeling probeert Microsoft het leven van zowel de ontwikkelaars als de beheerders wat aangenamer te maken. Dit product heet Active Directory in Application Mode. In dit artikel wordt ingegaan op de problematiek voor ontwikkelaars en de positionering en toepassingsmogelijkheden van Active Directory in Application Mode.

Op de komst van Active Directory (AD) in Windows 2000 werd nogal verschillend gereageerd. Veel beheerders waren - vergeleken met de oude SAM van NT4 - na enige gewenning behoorlijk tevreden over de mogelijkheden die AD met zich meebracht. . Veel ontwikkelaars werden daarentegen geconfronteerd met een aantal tekortkomingen die AD in Windows 2000 met zich meedroeg. Discussies over schemawijzigingen, replicatieverkeer als gevolg van extra data en beheer van de data, zal menig ontwikkelaar die een AD-enabled applicatie heeft willen implementeren niet vreemd in de oren klinken.

Positionering

Een noemenswaardige ommezwaai die Microsoft enige tijd geleden heeft ingezet betreft hun visie op Identity Management. Tijdens en kort na de introductie werd Active Directory gepositioneerd als de alles bevattende data-repository voor de hele organisatie. Echter, sinds enige tijd positioneert Microsoft Active Directory meer en meer als een pure Network Operating System (NOS) Directory. Naast de persoonsgegevens die een gecentraliseerde authenticatie mogelijk maken, is AD vooral geschikt voor de opslag van informatie die relatief statisch is en door heel de organisatie beschikbaar moet zijn. De dynamische data, waaronder de data die slechts op een beperkt aantal plaatsen beschikbaar moet zijn, kunnen het beste in een applicatie-directory worden opgeslagen. Applicatie-directory's zijn op zichzelf staande databronnen waarin applicatiespecifieke data wordt opgeslagen. Microsoft heeft hiervoor een nieuw product geïntroduceerd, te weten Active Directory in Application Mode. De implementatie van verscheidene directory's/databronnen in een infrastructuur vraagt in veel gevallen om een bepaalde mate van synchronisatie tussen de databronnen. De synchronisatie kan verzorgd worden door gebruik te maken van een metadirectory. Ook hiervoor heeft Microsoft een nieuwe versie van een bestaand product geïntroduceerd, namelijk Microsoft Identity Integration Server 2003. Met een productenportfolio bestaande uit de AD als NOS-directory (vanaf hier de NOS AD genoemd), Microsoft Identity Integration Server 2003 als 'synchronisatierobot' en Active Directory in Application Mode als applicatie-directory probeert Microsoft een totaaloplossing voor Identity Management aan te bieden; zie afbeelding 1.



Afbeelding 1. Microsoft's visie op Identity Management

De problematiek

Ontwikkelaars kennen in veel gevallen een aantal problemen bij het ontwikkelen van directory-enabled applicaties voor AD. Enkele veel voorkomende problemen zijn:

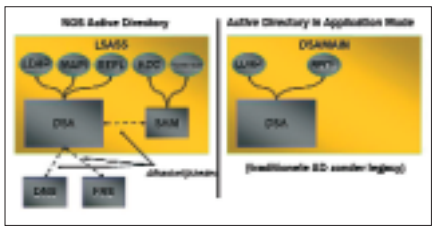
- Ontwikkelaars worden soms geforceerd om hun producten te integreren met een bestaande AD NOS directory-implementatie. Hierdoor kunnen er beperkingen ontstaan op de hoeveelheid data en soorten objecten die opgeslagen kunnen worden. Daarnaast kunnen ontwikkeltrajecten vertraagd worden vanwege langdurige procedures waarmee het change-beleid van de NOS-directory omgeven is.
- Een directory die als enterprise-directory is geïmplementeerd vereist flexibiliteit om de belangen van verschillende afdelingen te ondersteunen. Zaken als

schemawijzigingen die nodig zijn voor verschillende applicaties kunnen op weerstand stuiten. Zo kan de ene afdeling bijvoorbeeld de schoenmaat als verplicht attribuut bij een gebruikersobject willen definiëren, terwijl een andere afdeling dit attribuut als optioneel of misschien wel helemaal niet wil opnemen.

- Applicaties kunnen niet geïmplementeerd worden zolang AD niet geïmplementeerd is. Met name voor grote bedrijven is de implementatie van AD vaak een flink project met een aanzienlijke doorlooptijd.
- Ontwikkelaars willen het liefst een simpele directory waartegen men eenvoudig kan programmeren. De installatie en configuratie van de directory moet ook geen specialistische infrastructuurkennis of speciale hardware vereisen. Dit gaat voor de NOS AD niet op, want hiervoor is enige DNS-kennis vereist, terwijl de NOS AD alleen draait op het Windows Server-platform.

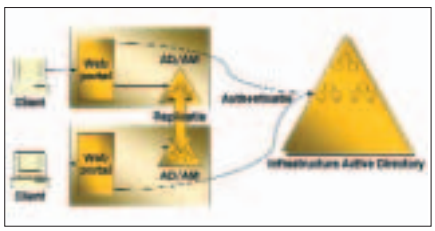
Active Directory 'light'

Active Directory in Application Mode (AD/AM) is een 'light'-versie van AD en vertoont meer overeenkomsten met een standaard LDAP-directory dan de NOS AD zoals we die nu kennen. De verschillend tussen AD en AD/AM zijn schematisch weergegeven in afbeelding 2.



Afbeelding 2. AD versus AD/AM

AD/AM draait als een niet-operating systeemservice en hoeft daarom ook niet persé op een Domain Controller te draaien. De installatie van AD/AM is net zo eenvoudig als het installeren van elke andere service en vereist geen reboot. De ondersteunde platformen waarop AD/AM kan worden geïnstalleerd zijn Windows Server 2003 (Standard, Enterprise en Datacenter) en Windows XP Professional. Een opluchting voor veel ontwikkelaars zal zijn dat AD/AM niet meer afhankelijk is van DNS, dit in tegenstelling tot de NOS AD. Even een testdirectory inrichten in een ontwikkelomgeving wordt hierdoor een stuk eenvoudiger. Bovendien is het mogelijk om verscheidene instanties van AD/AM op een enkele machine te draaien. Hierdoor is het keer op keer herinstalleren van de directory niet meer nodig. Ook is er geen scala aan ontwikkelmachines nodig waarop een directory draait indien men aan verschillende applicaties tegelijk wil werken. Ook kan elk willekeurig schema geïnstalleerd worden op een instantie van AD/AM. Tot slot is het mogelijk om AD/AM in te zetten als directory-server voor applicaties die een X-500 directory tree-structuur verwachten. Bijvoorbeeld een tree die begint met <o=bedrijfsnaam, c=NL>. Dit kan, in combinatie met de standaardondersteuning van het objectclass iNetOrgPerson, de migratie van bestaande applicaties naar een Microsoft-directory (in dit geval AD/AM) sterk vereenvoudigen.



Afbeelding 3. Toepassingsmogelijkheid van AD/AM

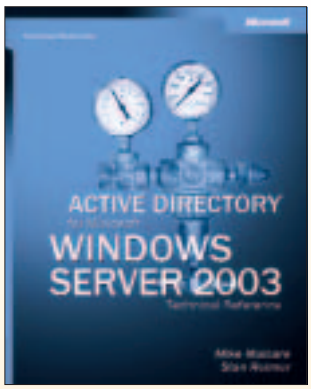
Toepassingsmogelijkheden

Een mogelijke toepassing van AD/AM is de applicatiespecifieke directory. Deze toepassingsmogelijkheid is in afbeelding 3 schematisch weergegeven. In dit voorbeeld slaat een applicatie (bijvoorbeeld een webportal) gegevens op in AD/AM die alleen voor deze applicatie van belang zijn. Het voordeel hiervan is dat deze gegevens niet in de AD staan en dus ook geen onnodig replicatieverkeer veroorzaken. Bovendien kan de applicatie elke willekeurige naamgevingconventie gebruiken die wenselijk is. Eventuele schema-uitbreidingen die voor de applicatie vereist zijn, worden in dit scenario niet doorgevoerd op de NOS AD. Het blijft natuurlijk wel mogelijk om de authenticatie binnen de webportal nog door de NOS AD te laten uitvoeren.
AD/AM kan ook gebruikt worden door ontwikkelaars die een applicatie aan het prototypen zijn voor AD. AD/AM gebruikt hetzelfde programmeermodel en vraagt nagenoeg een zelfde beheerervaring. Hierdoor kan AD/AM prima als lokaal ontwikkelplatform voor applicaties gebruikt worden die later op de NOS AD geïmplementeerd moeten worden.

Eenvoudiger ontwikkelen

AD/AM neemt voor ontwikkelaars een aantal beperkingen en problemen weg die de NOS AD met zich meedraagt. AD/AM vereenvoudigt het ontwerp en de implementatie van de NOS AD omdat minder rekening gehouden hoeft te worden met de eisen die applicaties in uw organisatie aan de directory stellen. Bovendien wordt het ontwikkelen van AD-enabled applicaties minder gehinderd, doordat de rol van applicatie-directory en infrastructuur-directory nu van elkaar los te koppelen zijn.

Microsoft Press



Titel: Active Directory® for Microsoft® Windows® Server 2003 Technical Reference
ISBN: 0-7356-1577-2
Auteur: Mike Mulcare and Stan Reimer

URL's:

Active Directory in Application Mode: http://www.microsoft.com/windowsserver2003/docs/adam.docActive Directory in Windows Server 2003: http://www.microsoft.com/windowsserver2003/evaluation/ overview/technologies/activedirectory.mspx
Microsoft Identity Integration Server 2003: http://www.microsoft.com/windowsserver2003/technologies/ directory/miis/default.mspx