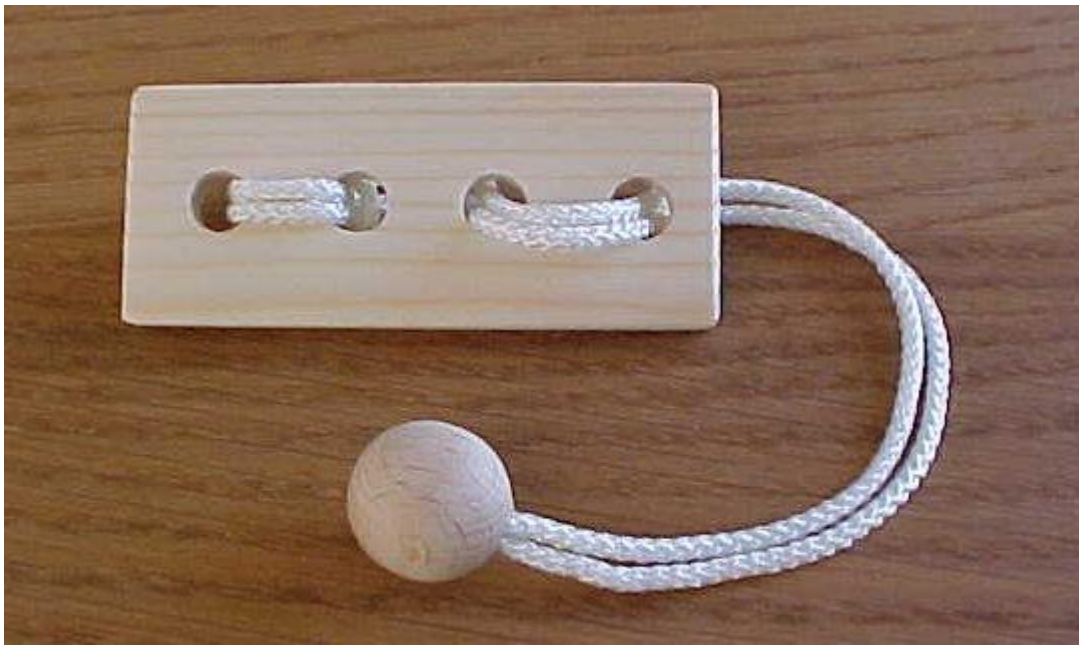


AGDLP

~ maar waarom eigenlijk?

Edward Willemsen, [em'bed], 2011

Algemeen

Wie ooit beheer heeft gedaan binnen een Microsoft omgeving is bekend met de diverse typen groepen. In de loop der jaren zijn hier een aantal smaken bijgekomen waaronder de domein locale en de universele groepen. Bovendien heeft Microsoft een typering aangebracht; beveiliging en distributie. Dit document legt uit waarom het volgen van de Microsoft AGDLP mantra zinvol is in een grotere organisatie.

Voor Microsoft is AGDLP, Account→Global Group→Domain Local Group→Permission, de manier om Role Based Access Control, RBAC, mogelijk te maken binnen de Active Directory Domein Services.

Deze methodiek helpt bij het flexibel inrichten en beheren van complexe omgevingen. Een complexe omgeving is een omgeving met meer dan 500 eindgebruikers, meer dan 10 afdelingen en meer dan 10 resources.

De resource

De resource kan van alles zijn, printers, folders, bestanden, maar ook gedelegeerde autorisaties of toegang tot specifieke views in een database of beheer applicatie. Toegang tot of gebruik maken van een specifieke resource geschiedt door de resource middels een groep te ontsluiten. Door de toegang of het gebruik van de resource te isoleren kan heel scherp getest worden of ook daadwerkelijk het 'minst noodzakelijk recht' verstrekt wordt. Met 'minst noodzakelijke recht' bedoelen we de maximaal verstrekte rechten, vanuit geen recht geredeneerd, om toch de resource te kunnen benutten. Een gewoon gebruikersaccount, lid van maar één groep, deze permissie, geeft veel beter inzicht in de aanwezige rechten dan een gebruikersaccount die lid is van talloze groepen.

Bovendien, door een goede naamconventie is te herleiden wat het doel van de groep is en is dit vanuit beheeroptiek snel te herkennen.

De resource wordt door de materiedeskundige ontsloten. Hierdoor is er een waarborg dat dit correct gebeurt. Eenmaal ontsloten, kan de resource gebruikt worden om als permissie aangeboden te worden aan eindgebruikers. Belangrijker nog, eenmaal ontsloten maakt de inzet van de materiedeskundige niet langer noodzakelijk voor de toegang of gebruik maken van de resource. Dit kan geautomatiseerd of door minder materiedeskundige medewerkers uitgevoerd worden.

Dit concept noemen we resource isolatie.

Microsoft hanteert de volgende best-practice: ontsluit resources met behulp van en Domein Locale groep.

Een permissie

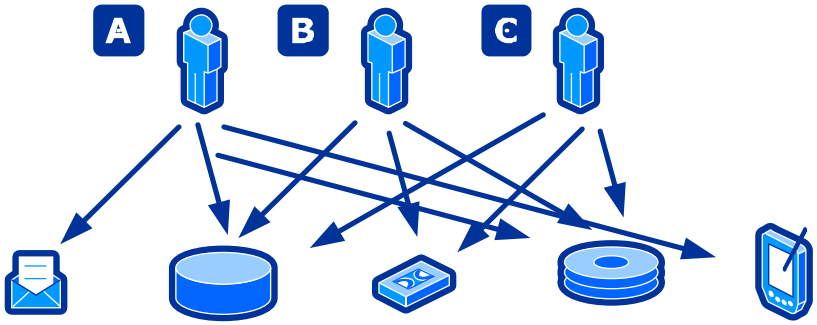
Zodra de ontsluiting getest en productiegereed is kunnen de eindgebruikers er nog geen gebruik van maken. Het gebruik maken van een resource geschiedt door lid te worden van de resource groep. De permissie is dus in feite de lidmaatschap van de groep die de resource ontsluit.

Mocht nu in de praktijk blijken dat het toekennen van een permissie negatieve gevolgen heeft op andere resources, door bijvoorbeeld strijdige instellingen of distributie, dan is een roll-back

eenvoudig te realiseren door dit lidmaatschap te verbreken. Omdat bekend is wie de materiedeskundige is voor dit type resource is een escalatie pad kort en kan de materiedeskundige ingeschakeld worden om het probleem op te lossen.

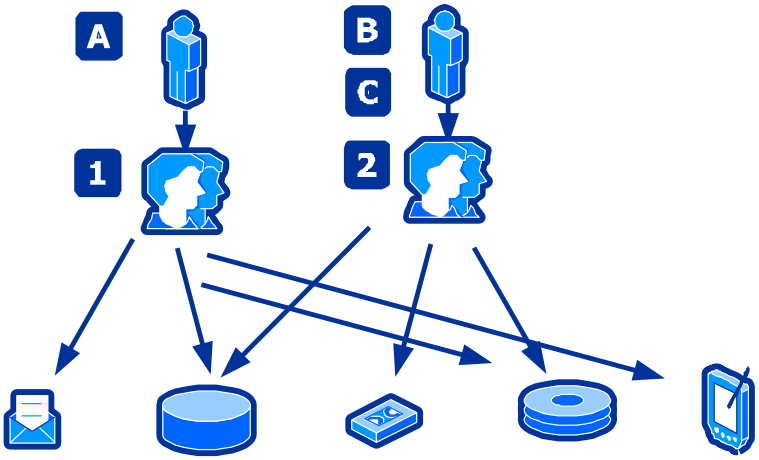
Gebruikersgroep

Niet iedere gebruiker is hetzelfde en heeft dus ook niet dezelfde taken of toegang tot resources nodig. De beschikbare resource daarentegen zijn bekend en dat kunnen er meer of soms minder worden. Met andere woorden; mensen hebben diverse rollen in de organisatie. Neem de volgende afbeelding:



Figuur 1: Toegang tot resources

We zien drie eindgebruikers, vijf resources en 10 permissies. Wat niet direct opvalt, is dat gebruiker B en gebruiker C toegang hebben tot dezelfde resources. Door eindgebruikers te bundelen in een gebruikersgroep wordt het geheel behoorlijk overzichtelijker:



Figuur 2: Toepassen van gebruikersgroepen

De manier om de taken, lees rol, van de eindgebruikers goed te formuleren is door eindgebruikers te bundelen ten aanzien van de taken die ze verrichten.

Microsoft hanteert de volgende best-practice: bundel gebruikers in Globale Groepen.

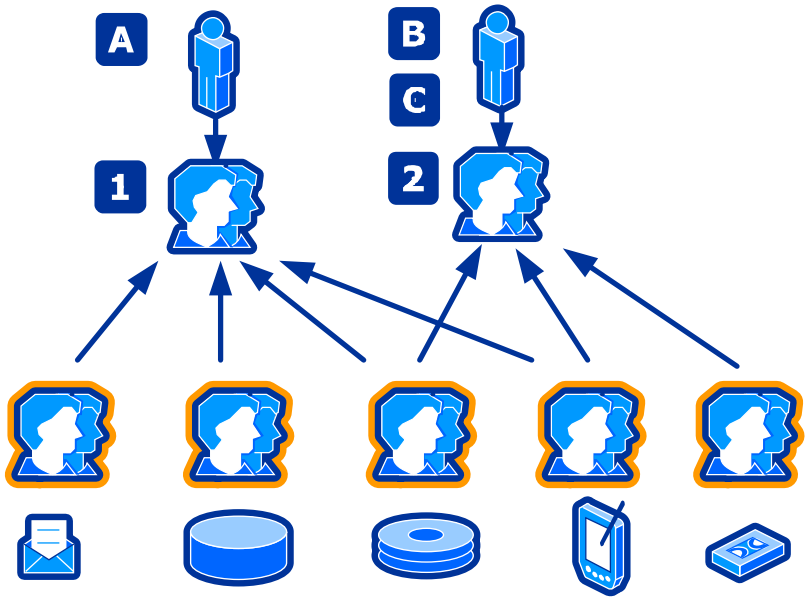
RBAC

Door de diverse groepstypen van Microsoft is het mogelijk verschillende inrichtingsvarianten te kiezen. Varianten als AP, AGP, ADLP, AGGP en nog vele andere zijn allemaal mogelijk. Maar wat is nu verstandig?

De RBAC methode wordt gerealiseerd door de ontsluiting los te zien van de eindgebruikers. Als we kijken naar '**Figuur 2**: Toepassen van gebruikersgroepen', dan zien we dat we meerdere keren en wellicht op verschillende manieren, toegang verleend hebben tot een resource. Wellicht zijn de rechten door een materiedeskundige gezet, maar die heeft hiervoor de groep gebruikt waar de eindgebruikers al inzitten. Dit is een beveiligingsrisico als de materiedeskundige zich vergist en teveel rechten uitdeelt. De materiedeskundige kan dit ook niet goed testen want als de resource ontsloten wordt moet hij/zij lid zijn van de globale groep alwaar de resources nodig zijn. Bovendien moet deze actie herhaalt worden voor iedere rol die de resource nodig heeft. Het is dus aan te bevelen dat de materiedeskundige zich niet ontfermt over de eindgebruikers. Hun verantwoordelijkheid beperkt zich tot de werking en toegankelijkheid van de resource.

In dit geval, hoe voer je een roll-back uit bij complexe permissies? Wordt er iets vergeten, dan is er een potentieel risico geïntroduceerd!

Als we dit nu vertalen in het eerder weergegeven figuur, dan ziet dat er als volgt uit:



Figuur 3: AGDLP implementatie

Iedere resource is via permissies te koppelen aan eindgebruikers met dezelfde rol. Naast de grote controle over permissies en flexibiliteit ten aanzien van rol gebaseerd werken, biedt dit ook veel voordelen bij migraties. Een inventarisatie als; *wie mag wat*?, is te herleiden uit de verstrekte permissies. Dit geldt ook voor de vraag; *wat mag je dan?*, de naam van de resource is nagenoeg zelfverklarend.

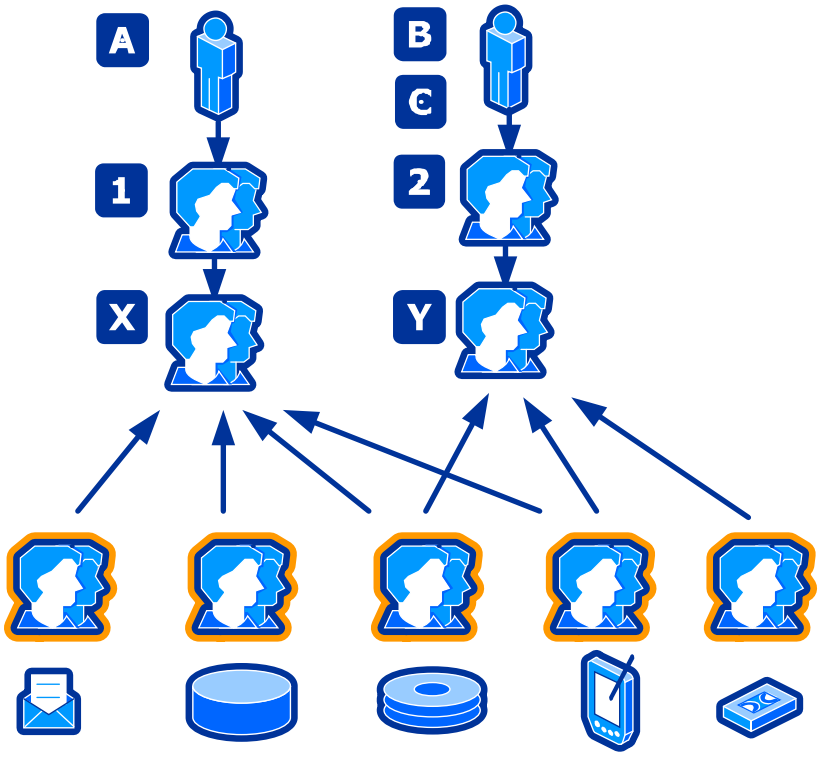
Informatie

Er is een goede uitleg over RBAC via AGDLP op de Engelstalige Wikipedia site: http://en.wikipedia.org/wiki/AGDLP

Universele Groepen

Het gebruik van Universele Groepen is in principe niet nodig. Alleen het gemak van het overal kunnen beschikken van de groep binnen een forest is een beheervoordeel. Dit voordeel is ook weer een nadeel vanuit beveiligingsoptiek, immers, via eventuele permissies kunnen resources benaderd worden.

Microsoft duidt dit aan met AGUDLP. Als we '**Figuur 3**: AGDLP implementatie' zouden projecteren naar dit concept zien we het volgende:



Figuur 4: Implementatie AGUDLP

Uit de figuur valt op te maken dat in een forest met een gering aantal domeinen de doelstelling van het gebruik van een Universele Groep nagenoeg geen toegevoegde waarde heeft.

In de praktijk zien we dat de Universele Groepregelmatig wordt ingezet als vervanging voor DL. Verder is het gebruik van de Universele Groep een handig hulpmiddel tijdens domein migraties. Naar mijn persoonlijke mening; bedrijven die het geheel inrichten volgens '**Figuur 4**: Implementatie AGUDLP' draven een beetje te ver door in het volgen van een mantra.

Technisch

Een eindgebruiker kan lid zijn van maximaal 1015 groepen (1024 – 9 reeds vastgestelde sleutels, de zogenaamde well-known SIDs). Dit lijkt veel, maar door de toekenning van resources en rollen foutief in te richten is dit getal gemakkelijk te bereiken. De RBAC methodiek ziet de Globale Groep dan ook als sleutelhanger met daaraan diverse sleutels. De lidmaatschapen van de diverse resource en permissies worden dus door nestings beperkt. De grens van 1015 is dan ineens weer ver weg.

Negatief aspect is de grootte van het beveiligingstoken. Des te meer groepen er aan een gebruiker 'kleven' des te groter het beveiligingstoken. Dit was met name bij Microsoft Windows 2000 Server een probleem. Het token kan in principe heel groot zijn, maar de 'fabrieksinstellingen' waren nogal zuinig ingesteld. De standaard waarde is bij Microsoft Windows Server 2003 is dit verhoogd en is eenvoudig aan te passen. De grootte van de zogenaamde sleutelhanger is dus niet langer een praktisch probleem.

ACL

Een ACL is een Access Control List. Dit is een lijst met daarin de sleutels van personen en/of groepen, de zogenaamde ACEs, Access Control Entries. De lijst wordt per resource gedefinieerd en wordt geëvalueerd zodra de eindgebruiker de resource al dan niet bewust wil benutten.

Dit evalueren kost tijd en performance aan zowel cliënt als server zijde. Des te langer de ACL, des te meer tijd. Het is dus de kunst deze ACLs zo klein als mogelijk te houden. Door het toepassen van resource isolatie en de beschreven RBAC strategie is er in principe slechts één ACE in de ACL. Alle andere zaken worden op een hoger niveau afgehandeld.

Delegation of Control

Door de split in Globale en Domein Locale groepen kan er op zes plaatsen delegatie van controle ingericht worden:

1. Wie maakt de eindgebruiker aan?
2. Wie maakt de globale groep aan?
3. Wie mag de eindgebruik in de Globale Groep plaatsen?
4. Wie maakt de Domain Locale groep aan?
5. Wie verzorgt de functionaliteit van de permissie?
6. Wie mag de permissie uitdelen, dus de nesting tussen Domein Locale en Globale groep realiseren?

Dit alles gebruikmakend van standaard delegatie van controle functionaliteit binnen AD DS! Tal van deze zaken kunnen natuurlijk eenvoudig gebundeld worden in één of meerdere rollen. Bij gedeelde taken kan de permissie eenvoudig hergebruikt worden en geeft het alle partijen hetzelfde recht tot de resource.

Een ander aspect van het gebruik van delegatie van controle is de opkomst van rol beheer systemen, de zogenaamde ACMS, Access Control Management Systems. Dit zijn niet alleen systemen die permissies regelen op basis van rollen, maar ook op basis van attributen en claims. Zoals, bent u 24 jaar of ouder en van het vrouwelijk geslacht? Deze systemen hebben allen als doel de techniek binnen de inrichting van AD DS te vertalen naar geautomatiseerde processen welke door de business begrepen worden.

Veel van dergelijke systemen zijn geënt op een LDAP directory en verwachten een uniforme inrichting. Omdat AGDLP een Microsoft best-practice is zullen veel producten hier dan ook naadloos op aansluiten. Het afwijken van de best-practice vergt dan ook een afwijking van de inrichting van het ACMS. De inrichting van het ACMS kost dus meer tijd en in het geval van calamiteiten kost het fout zoeken dus ook meer tijd. Bovendien zal bij het overgaan naar een andere leverancier een afwijkende lokale inrichting leiden tot een hogere offerte. Een fenomeen bekend als de vendor-lock.