HelloID Q&A webinar RBAC en Role Mining

1. **Ik heb een vraag over het eigenaarschap. Wij willen in de nabije toekomst het onderzoek hiernaar gaan starten. Bij wie zou volgens jullie ervaring de eigenaar moeten liggen?**

   Het eigenaarschap zit in theorie tussen HR en IT in, bij voorkeur bij een informatiemanager-rol of een security officer. In de praktijk zien we echter dat IT meestal het initiatief neemt en uiteindelijk ook eigenaar wordt, maar wel met regelmatig overleg met de organisatie. Het kan niet enkel door IT worden gedragen.

2. **Ik denk dat voor het maken van scenario's met name de functie van een medewerker een grote rol speelt. Een praktijkvoorbeeld is dat bij ons in het HR-systeem de functies "Stagiaire" en "ZZP niet in loondienst" wordt gebruikt. Dan wordt het volgens mij erg lastig om hier scenario's voor te maken, want dit geeft meer aan welke type/soort medewerker dit is. Wat is jullie ervaring en advies met dergelijke situaties?**

   De functies "Stagiaire" en "ZZP niet in loondienst" zijn inderdaad dermate vloeibaar dat die lastig te vatten zijn in een business rule voor geboorterechten. Je ziet dat dit soort functies veelal taakrechten bevatten en daarom ad-hoc worden aangevraagd en toegekend, bijvoorbeeld via HelloID Service Automation. Wij adviseren om dergelijke functies niet onder te brengen in detailrollen maar globaal te houden met een account, mail en een office licentie. Indien de stagiare apart per functie geadministreerd is zou je deze natuurlijk wel kunnen toevoegen aan de functierol die gedefinieerd is in HelloID Provisioning. Bijvoorbeeld functie: "Stagiaire administratie". Deze functie kan meegenomen worden bij de rol "Administratie".

3. **Kun je als bronsysteem meerdere HR-systemen gebruiken? Wij hebben wel één Active Directory, maar in verschillende landen een ander HR systeem.**

   Dit is mogelijk. Standaard gaan we er echter vanuit dat een identiteit in één bronsysteem voorkomt. Mochten personen in meerdere bronsystemen een identiteit hebben dan dient er persoonsaggregatie te worden toegepast. Hierbij worden een aantal kenmerken gebruikt om de de persoon over meerdere bronsystemen heen te identificeren. Denk hierbij aan de geboortedatum, geboorteplaats, geslacht, geboortenaam etc.

4. **Hoe ver moet je gaan met RBAC als je gaat werken met meerdere HelloID tenants om het beheersbaar te houden?**

   Standaard adviseren wij niet om dit te doen daar je het dan niet "zuiver" houdt. Een RBAC-model is organisatie specifiek, dus zou zich in onze optiek moeten houden aan de bron(nen) van één organisatie en één IT-landschap. Als dat IT-landschap bestaat uit meerdere AD systemen dan is dit wel goed om mee te nemen. Er zijn natuurlijk altijd uitzonderingen op de regel waarbij situaties zich voor doen die wel een goede reden zijn om meerdere tentants gebruiken met HelloID. Dit zal echter altijd eerst besproken moeten worden met de accountmanager/technisch consultant.

5. **Kun je role mining alleen toepassen op AD rechten of ook het autorisatiemodel van/in Nedap ONS?**

   De AD-rechten gebruikten we in de demo puur als voorbeeld, het role mining mechanisme is zeker ook geschikt voor andere systemen. Tot nu toe hebben we het systeem toegepast in combinatie met Active Directory en Azure Active Directory. Voor Google Workspace staat de eerste keer op korte termijn op de planning. Op autorisaties binnen Nedap ONS verwachten wij ook een role mining scan te kunnen uitvoeren. Globaal geldt immers dat wij de autorisaties binnen het doelsysteem moeten kunnen uitlezen, wat binnen Nedap ONS kan. Bij een ECD-systeem kunnen er meerdere accounts per medewerker aanwezig zijn. Dit is een complexere opzet en zullen we daarom eerst moeten onderzoeken voordat we een definitieve "ja" kunnen geven. Via je vaste accountmanager of sales@tools4ever.com kan je dit bij interesse aanvragen.

6. **Hoe kun je vanuit je HR-data de verschillende rollen halen voor je medewekers? Meestal krijgen medewerkers vanuit het HR-pakket één functie naam mee, maar medewerkers kunnen meerdere rollen vervullen binnen een organisatie.**

   Indien er meerdere rollen geadministreerd zijn in het HR-systeem doormiddel van inzet/formatieregels of extra velden, dan is het mogelijk om ook autorisaties uit te delen op basis van deze rollen.

7. **Hoe doen jullie deze analyse? Gebeurt dit met behulp van tooling en zo ja welke tooling? In combinatie met Excel? Op welke manier is rolemodel.html gemaakt? Is dit Excel op de achtergrond of is dit de output van een tool die jullie gebruiken voor role mining?**

   We gebruiken zowel data uit de HelloID Identity Vault als in dit geval een extract van de Active Directory data zoals die in de HelloID User Directory leeft. Voor het analyseren van de data bieden we een tweetal verschillende methoden. De methode die getoond is in de demo is een weergave binnen een webpagina. Dit overzicht is goed te gebruiken voor kleinere organisaties. De andere role mining analysemethode is op basis van een Excel draaitabel. Dit is een minder mooie weergave als de HTML, maar deze geeft een groter overzicht. De combinatie tussen de twee is vaak de meest prettige manier van werken.

8. **Wat betekent deze role mining analyse voor honderden afdelingen?**

   Wat betreft de analysemethode is hierbij ons advies om de HTML rapportage te draaien, maar vooral ook de rapportage via Excel hiervoor te gebruiken. Deze rapportage geeft per afdeling een duidelijk overzicht welke rechten de personen hebben. Het resultaat wat betreft rollen is natuurlijk bij voorbaat lastig te zeggen. Als we echter uit gaan van een reguliere situatie adviseren wij over het algemeen om bij honderden afdelingen te werken met dynamische rollen/business rules, waarbij de afdeling vrijwel 1:1 overeenkomt met het recht wat je wilt uitdelen. Neem bijvoorbeeld een Teams-kanaal of een distributie-lijst, daarvoor hoef je niet per afdeling een business rule aan te maken, dat kan met één dynamische rule.

9. **Als er verschillen zijn van de rol per dienst/afdeling/locatie en team krijg je toch automatisch een exponentieel aantal rollen? Dus Rol-Divisie1-Afdeling1-Locatie1-Afdelingsmedewerker enzovoort.**

   Dat klopt en dat zou je niet moeten willen. De oplossing zit in de stapeling van rollen waarmee je de groei ondervangt. Onze insteek is dat je een combinatie van rollen kunt krijgen, dus een Divisie1 rol, een Locatie1 rol en een Afdelingsmedewerker rol. Vaak zien we dan dat niet alle combinaties nodig zijn, of dat sommige combinaties voor een hele kleine groep zijn en daarom dus beter als optionele rol opgezet kunnen worden. Dat biedt beheersbaarheid voor de grote groepen en flexibiliteit voor kleinere rollen. De juiste vorm van stapeling vereist een goede diepte analyse van de role mining data. Onze businessconsultants kunnen hierbij ondersteunen.

10. **Ziet het role mining systeem zelf wie er binnen een rol ontbreekt?**

    De mining scan herkent per rol (bijvoorbeeld functie of afdeling) wie een recht niet heeft, maar wel bij de rol hoort. De ontbrekende persoon zorgt er dan voor dat er geen 100 procent dekkingsgraad is voor de permissie. Bij het invullen van een business rule kies je dan of het % hoog genoeg is en ga je akkoord met het feit dat de ontbrekende personen alsnog de permissie uitgedeeld gaan krijgen.

11. **Hebben jullie ervaring met de parameter 'gebruikers-context'? Dus bijvoorbeeld: rechten op basis van gebruikerscontext zoals een werkrooster.**

    Jazeker, echter nemen we die op dit moment nog niet mee in een mining scan. De scan gaat uit van een directe relatie tussen persoon en permissie, en gaat nog niet in op context zoals roosterinformatie. De focus van een role mining scan ligt op geboorterechten, rechten die bij instroom/doorstroom toe te kennen zijn op een persoon en langdurig bij de persoon blijven.

12. Deze RBAC inventarisatie lijkt ervan uit te gaan dat je je rollen binnen de Active Directory al perfect gedefinieerd hebt. Helpt de inventarisatie ook wanneer je juist in de AD nog zoekende bent naar een efficiënte indeling van de verschillende rollen?

De role mining scan is juist gemaakt voor de situatie waarbij niet duidelijk is welke rollen er binnen de organisatie zijn. Zo kan er met role mining worden gekeken naar welke AD groepen het meeste voorkomen bij bepaalde rollen vanuit het HR-systeem. Hier is geen gestructureerde opzet in de AD benodigd. Daarnaast is role mining zeer geschikt bij grote mate van vervuiling omdat deze naar de oppervlakte komt. De enige eis met deze vorm van role mining is dat je aan de naam van de permissie kunt afleiden wat de permissie inhoudt.

13. Hoe diep gaat de role mining scanner? Active Directory groepen is één, maar analyseert de role mining scan ook rechten/rollen op eventuele servers binnen een netwerk?

De scan gaat net zo diep als de data die voorhanden is. Het vergaren van AD groepen en de (nested) lidmaatschappen is relatief eenvoudig en is daardoor makkelijk beschikbaar. Als er data voorhanden is met de relatie tussen account en een ander type recht, dan kan deze ook prima worden meegenomen in de scan. De scan staat in principe los van het vergaren van de data zelf.

14. We gebruiken HelloID nu al voor een andere toepassing, maar kan je ook een tweede HelloID naast elkaar laten lopen? We gebruiken momenteel nog UMRA voor ons gebruikers- en autorisatiebeheer. HelloID staat hier los van en wordt enkel gebruikt voor een SSO-koppeling met onze intranet pagina die extern wordt gehost.

Het HelloID platform bestaat uit een drietal modulen die los van elkaar aan en uit kunnen worden gezet. In het geval van de genoemde Single Sign-on functionaliteit betreft dit de module Access Management. De autorisatiematrix en het automatiseren van het in-, door- en uitstroomproces is onderdeel van de module Provisioning. Tot slot kunnen binnen HelloID Service Automation onder andere de optionele rollen worden onderge-bracht. Wij kunnen HelloID naast UMRA opbouwen en naast elkaar laten lopen totdat HelloID de huidige functionaliteit vervangt. In jullie geval is er al een HelloID omgeving beschikbaar en kan de inrichting binnen deze bestaande omgeving worden opgezet. Voor de role mining scan is een basisinrichting binnen HelloID nodig. Een basisinrichting betekent dat HelloID een verbinding moet hebben met het HR-systeem, en ook moet de Active Directory (als in scope) gekoppeld zijn aan HelloID. Er is geen volledige Provisioning of Service Automation inrichting nodig om de scan uit te voeren.

15. Biedt HelloID de mogelijkheid om handmatig rollen toe te kennen? We hebben nu iets gemaakt in Service Automation waardoor leidinggevenden rollen, die niet op functie gebaseerd zijn, kunnen toekennen aan medewerkers.

Dat verloopt inderdaad via Service Automation producten of eventueel (gedelegeerde) formulieren.

16. Hoe beheer je het rollenmodel?

In HelloID Provisioning zit een volledige beheeromgeving voor de business rules. De omgeving is uniek omdat je business rules kunt samenstellen en vervolgens de impact daarvan kunt laten inschatten door HelloID via een evaluatie, voordat je de business rules werkelijk loslaat op je IT-landschap.

17. Hoe diep kijkt de role mining scan als het gaat om nested groups. Dit was volgens mij één laag of is dit inmiddels uitgebreid naar meerdere lagen?

Onze standaard role mining scan kan standaard tot en met één laag diep kijken naar de nested groepen. Nesting kan in de praktijk tot heel diep en er kunnen loops ontstaan die ons hebben doen besluiten om niet meer dan één laag te ondersteunen. De scan staat daarentegen los van het vergaren van de data zelf. Wanneer data van diepere lagen voorhanden is kan deze ook worden meegenomen in de scan. De scan vereist een data levering met relatie tussen account en permissie, dat kan in principe alles zijn en is ook niet gebonden aan enkel Active Directory groepen.

18. **Kan je ook automatisch rechten in applicatie laten toekennen, of blijft dat altijd nog extra handwerk?**

Met HelloID is het mogelijk om businessapplicaties te koppelen om accounts en rechten aan te maken en toe te kennen. Het is vereist dat de leverancier van de applicatie een koppelvlak (API/CSV/XML/OIDC) beschikbaar heeft die deze functionaliteit ondersteunt. Dat ligt daarom dus aan het koppelvlak wat een applicatie levert. Je ziet bij een API van een leverancier nog wel eens dat je “tot de poort” kunt provisionen, dus de basis van een account. Echter de “achter de poort”, dus ook de detailautorisaties of rollen toekennen in een applicatie wil nog wel eens voorbehouden zijn aan de applicatie zelf, en dus niet beschikbaar zijn via een API.

19. **Leveren jullie consultancy diensten om ons hierbij te helpen of moet dit via de partner?**

De mate van inzet van een businessconsultant van Tools4ever en/of partner gebeurt in overleg. Vaak helpen we de klant in een halve tot dag met het draaien van de rapportage, een eerste opzet van de autorisatiematrix of het er uit pakken van een specifieke afdeling, en uitleg en toelichting. We streven er naar dat klanten vervolgens zelf in staat zijn om de role mining scan uit te voeren en te interpreteren.

20. **Hoe kunnen we rollen minen op basis van rechtengroepen in een andere applicatie dan Active Directory?**

De AD-rechten gebruikten we in de demo puur als voorbeeld, het role mining mechanisme is zeker ook geschikt voor andere systemen. Tot nu toe hebben we het systeem toegepast in combinatie met Active Directory en Azure Active Directory. Voor Google Workspace staat de eerste keer op korte termijn op de planning. Globaal geldt dat wij de autorisaties binnen het doelsysteem moeten kunnen uitlezen en koppelen aan een persoon. Wil je weten of we een specifiek doelsysteem kunnen ondersteunen vraag dan bij je accountmanager of via sales@tools4ever.com aan om dit te onderzoeken.

21. **Waarom de keuze voor Role Based Access Control (RBAC) en geen Attribute Based Access Control (ABAC)?**

RBAC is de meer conventionele term die vrijwel iedereen wel kent. HelloID combineert binnen de business rules RBAC en ABAC. Zo is het dus mogelijk business rules te baseren op attributen (waaronder ook de functie en afdeling vallen) uit het HR-systeem.

22. **Kunnen met role mining meer applicaties en systemen worden uitgelezen dan alleen de Active Directory? Zoals applicaties voor middelen als sleutels, een laptop of telefoon.**

De AD-rechten gebruikten we in de demo puur als voorbeeld, het role mining mechanisme is zeker ook geschikt voor andere systemen. Tot nu toe hebben we het systeem toegepast in combinatie met Active Directory en Azure Active Directory. Voor Google Workspace staat de eerste keer op korte termijn op de planning. Globaal geldt dat wij de autorisaties binnen het doelsysteem moeten kunnen uitlezen en koppelen aan een persoon. Wil je weten of we een specifiek doelsysteem kunnen ondersteunen vraag dan bij je accountmanager of via sales@tools4ever.com. aan om dit te onderzoeken.

23. **Wat is jullie ervaring met het schoonhouden van de Active Directory bij een uitgebreid provisioning proces? Als je via HelloID en AD rechten in doelapplicaties gaat zetten krijg je waarschijnlijk enorm lange of heel veel rechten groepen of heel veel rechten groepen, is het bijvoorbeeld mogelijk om deze groepen te nesten?**

Wij adviseren juist om van nesting af te stappen. Met nesting leg je geen directe relatie tussen account en permissie, en sommige applicaties of systemen ondersteunen het ook niet 100 procent. Wij voorzien zelf geen situatie waarin er juist meer rechtengroepen ontstaan. Doordat de toekenning “managed” is wordt de hoeveelheid groepen in AD daarnaast ook minder relevant, er is ten slotte een systeem en proces wat dit overziet.

24. Hoeveel bron systemen kunnen jullie deze dagen koppelen? is het mogelijk om data van 1 persoon uit verschillende systemen te verrijken?

Het limiet voor bronsystemen is momenteel drie systemen per tenant. Indien één natuurlijk persoon in meerdere bronsystemen voorkomt, zal er gekeken moeten worden welke gegeven(s) er te gebruiken zijn voor het herkennen van de personen. Hierop passen wij dan persoonsaggregatie toe zodat alle dienstverbanden van die persoon binnen HelloID beschikbaar zijn onder dezelfde identiteit, zodat op basis hiervan de juiste rollen toegekend kunnen worden. Het verrijken van persoonsattributen (bijvoorbeeld de voornaam uit bronsysteem A en de achternaam uit bronsysteem B) is momenteel nog niet mogelijk. Wij zijn wel plan om ook dit in de toekomst te ondersteunen. Houd hiervoor vooral onze roadmap in de gaten op https://roadmap.helloid.com.

25. Jullie adviseren alleen rollen voor grotere groepen gebruikers. Is het dan nog wel nuttig voor organisaties met kleinere afdelingen

Jazeker, efficiency en compliance gelden ook voor kleinere organisaties. Per organisatie zullen de rollen gedefinieerd moeten worden. Groot is relatief voor elk bedrijf. Het gaat uiteindelijk om grip en regie, niet om de absolute aantallen.

26. Hoe om te gaan met tijdelijke vervanging dus iemand heet tijdelijk twee rollen. vaak niet als dienstverbandregel vastgelegd

Voor deze situaties is HelloID Service Automation goed inzetbaar, waarbij je (tijdelijk) een persoon extra autorisaties kunt geven boven de geboorterechten uitgedeeld via HelloID Provisioning. Deze toebedeling kan via self-service op aanvraag van een medewerker of manager gebeuren, of de servicedesk kent optionele rollen rechten via gedelegeerde formulieren toe. Wanneer deze een tijdelijk karakter hebben kan HelloID de extra rechten na een bepaalde periode weer automatisch intrekken zodat accumulatie van rechten wordt voorkomen.

27. Wij gaan nog overstappen van IAM naar HelloID. Op welk moment past rol mining in de timing. Voor je overstapt, tijdens de migratie of na de implementatie?

Het kan zowel tijdens als na de implementatie. Wij raden zelf aan om het in een relatief vroeg stadium te doen, omdat een scan vaak veel discussie oplevert en ook huiswerk voor het aanpakken van vervuiling. Dit is overigens niet blokkerend voor de implementatie, maar het voortschrijdend inzicht wat je gegarandeerd opdoet met de scan zal bijdragen aan de implementatie.

28. In hoeverre kan ik role mining toepassen in een meer projectmatige omgeving?

De effectiviteit zal bij projecten en/of taken wat minder uitvallen aangezien dat tijdelijke permissies betreft. De mining om puur te gebruiken voor je business rollen in HelloID Provisioning zal in dat opzicht beperkt zijn. Waar je echter veel winst uit haalt is het inzicht in wie er nog “oude” projecten en of taken heeft, en om juist te bepalen wat de “cutoff” is waarbij je juist naar de lage relevante permissies gaat kijken om te valideren of dat inderdaad goed uitgedeelde projecten/taakrechten zijn. Wij zouden juist aanraden om de scan uit te voeren in dit scenario voor het netjes definiëren van optionele rechten en om vervuiling aan te pakken.

29. Hebben jullie ervaring/advies over het vastleggen van rechten in (Azure) Active Directory voor de provisioning binnen een doel applicatie? (bijvoorbeeld het zetten van rechten in Nedap ONS)

Jazeker, dit hebben wij. Tijdens de implementatie zal er een intake/business consultancy moment zijn waarbij de best practices worden besproken. Voel je echter ook altijd vrij om contact op te nemen met je accountmanager of sales@tools4ever.com wanneer je dit gesprek eerder wenst aan te gaan.

30. Dus naast Google Workspace, lezen jullie ook alle rechten van de applicaties die in gebruik zijn?

Jazeker, maar dit ligt wel aan de data die voorhanden is. Per systeem kan verschillen of we dat kunnen/mogen inlezen.

31. Hoe creëer je zo een lijst om te zien wie wat ontbreekt of buiten de rol valt?

De role mining scan kijkt per permissie of iedereen in de rol die permissie ook daadwerkelijk heeft. De ontbrekende personen worden apart getoond zodat je kunt zien wie er “ontbreekt”. Daarnaast kijkt de scan ook naar de personen die wel degelijk de permissie hebben, maar niet in de rol zit waar we op dat moment naar kijken. Je krijgt dus permissie de uitval aan beide kanten te zien, dit puur ter validatie op opschoning.

32. Is het binnen HelloID of de tooling ook mogelijk om een autorisatiematrix te genereren per medewerker om periodiek te laten valideren door bijvoorbeeld de manager?

Op dit moment is dat nog niet mogelijk, we zijn zeker van plan om dat te gaan aanbieden, zie milestones op onze roadmap.

33. Hoe gemakkelijk is het om binnen HelloID zelf de business rules te beheren en zelf eventuele aanpassingen te doen? We werken nu nog met IAM maar zijn hierbij altijd afhankelijk van een consultant van Tools4ever voor aanpassingen.

HelloID biedt een veel betere gebruikersinterface dan IAM en een veel simpelere opzet. Dat is een van de belangrijkste wijzigingen. We streven er naar dat klanten zoveel mogelijk zelf kunnen doen. In HelloID Provisioning zit een volledige beheeromgeving voor de business rules waarin je business rules kunt samenstellen en vervolgens de impact daarvan kunt laten inschatten via een evaluatie, voordat je de business rules werkelijk loslaat op je IT-landschap. In tegenstelling tot IAM is HelloID daarnaast volledig gedocumenteerd (documentatie is beschikbaar op https://docs.helloid.com). Ook bieden we elke maand kosteloze trainingen aan om kennis van HelloID op te doen en zelfs om de verschillende modulen zelf te kunnen implementeren.

34. Kunnen we de role mining afnemen als dienst/consultancy of zit dit in de huidige Tools4ever IAM die wij voeren?

In een halve dag kunnen we helpen met het draaien van de role mining rapportages. Met deze eerste run van de rapportage kan een eerste opzet van het rollenmodel worden gemaakt. Deze dient vervolgens gecontroleerd te worden binnen de organisatie door bijvoorbeeld de afdelingsmanagers. De manager wordt hierbij gevraagd om te controleren of de autorisaties van zijn/haar afdeling kloppen. Mogelijk zijn er in jullie IAM versie ook mogelijkheden, maar vraag dat even na bij je accountmanager.

35. Bestaat de functionaliteit role mining ook voor de ‘legacy’ on premise versie?

De gepresenteerde role mining scan wordt geleverd als dienst bovenop en middels een HelloID IDaaS omgeving. Bepaalde versies van IAM3 bieden echter ook rapportages waar een draaitabel van gemaakt worden die inzicht geeft in de rollen per functie of afdeling.