

Beveiliging op rijniveau (RLS) met Power BI

9-12-2019 • 15 minutes to read • [Edit Online](#)

Beveiliging op rijniveau (RLS) kan in Power BI worden gebruikt om de toegang tot gegevens voor bepaalde gebruikers te beperken. Filters beperken de toegang tot gegevens op rijniveau en u kunt filters definiëren in rollen. Let erop dat in de Power BI-service leden van een werkruimte toegang hebben tot gegevenssets in de werkruimte. Toegang tot deze gegevens wordt niet door Beveiliging op rijniveau beperkt.

U kunt RLS configureren voor gegevensmodellen met Power BI Desktop zijn geïmporteerd in Power BI. U kunt RLS ook configureren voor gegevenssets die gebruikmaken van DirectQuery, zoals SQL Server. Voorheen kon u RLS alleen implementeren binnen on-premises Analysis Services-modellen buiten Power BI. Voor Analysis Services-liveverbindingen configureert u beveiliging op rijniveau voor het on-premises model. De beveiligingsoptie wordt niet weergegeven voor gegevenssets met een liveverbinding.

Rollen en regels definiëren in Power BI Desktop

U kunt rollen en regels definiëren binnen Power BI Desktop. Wanneer u naar Power BI publiceert, worden ook de roldefinities gepubliceerd.

Volg deze stappen om beveiligingsrollen te definiëren.

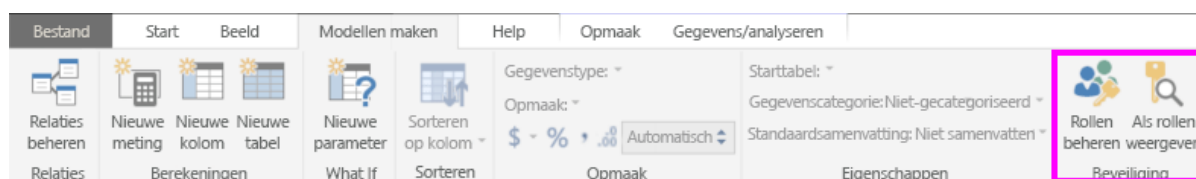
1. Gegevens importeren in uw Power BI Desktop-rapport of een DirectQuery-verbinding configureren.

NOTE

U kunt geen rollen binnen Power BI Desktop definiëren voor live verbindingen met Analysis Services. U moet dat doen binnen het Analysis Services-model.

2. Selecteer het tabblad **Modellering**.

3. Selecteer **Rollen beheren**.



4. Selecteer **Maken**.



5. Geef een naam op voor de rol.
6. Selecteer de tabel waarop u een DAX-regel wilt toepassen.

7. Voer de DAX-expressies in. De expressie moet waar of onwaar retourneren. Bijvoorbeeld: [Entiteit-id] = "Waarde".

NOTE

U kunt `username()` binnen deze expressie gebruiken. Let op: `username()` heeft de indeling `DOMAIN\username` binnen Power BI Desktop. Binnen de Power BI-service en Power BI Report Server heeft deze de indeling van de UPN (User Principal Name) van de gebruiker. U kunt ook `userprincipalname()` gebruiken, waarmee altijd de gebruiker wordt getourneerd in de indeling van zijn/haar naam van de principal van gebruiker, `username@contoso.com`.



8. Nadat u de DAX-expressie hebt gemaakt, kunt u het vakje boven de expressie inschakelen om de expressie te valideren.



NOTE

In dit expressievak gebruikt u komma's om argumenten van DAX-functies te scheiden, zelfs als u een landinstelling gebruikt die gewoonlijk puntkomma's als scheidingstekens gebruikt (bijvoorbeeld Frans of Duits).

9. Selecteer **Opslaan**.

U kunt geen rol toewijzen aan gebruikers binnen Power BI Desktop. U wijst deze toe in de Power BI-service. U kunt dynamische beveiliging inschakelen binnen Power BI Desktop door gebruik te maken van de DAX-functies voor `username()` of `userprincipalname()` en het configureren van de juiste relaties.

Het beveiligingsfilter op rijniveau gebruikt standaard filters in één richting, ongeacht of de relaties zijn ingesteld op één richting of twee richtingen. U kunt handmatig kruisfiltering met beveiliging op rijniveau in twee richtingen inschakelen door de relatie te selecteren en het selectievakje **Beveiligingsfilter toepassen in beide richtingen** te markeren. U moet dit selectievakje inschakelen wanneer u ook dynamische beveiliging op rijniveau op serverniveau hebt geïmplementeerd, waarbij beveiliging op rijniveau is gebaseerd op de gebruikersnaam of aanmeldings-id.

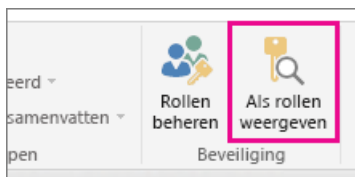
Zie voor meer informatie [Kruisfiltering in twee richtingen met DirectQuery in Power BI Desktop](#) en het technische artikel [Het semantische BI-model in tabelvorm beveiligen](#).



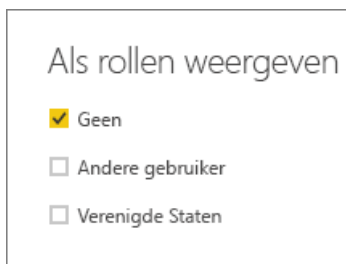
De rollen in Power BI Desktop valideren

Nadat u uw rollen hebt gemaakt, kunt u de resultaten van de rollen testen binnen Power BI Desktop.

1. Selecteer **Als rollen weergeven**.



In **Als rollen weergeven** kunt u de rollen zien die u hebt gemaakt.



2. Selecteer een rol die u hebt gemaakt > **OK** om die rol toe te passen. De rapporten geven de gegevens weer die relevant zijn voor die rol.
3. U kunt ook **Andere gebruiker** selecteren en een bepaalde gebruiker opgeven. U kunt het beste de User Principal Name (UPN) opgeven, omdat die door de Power BI-service Power BI Report Server wordt gebruikt.



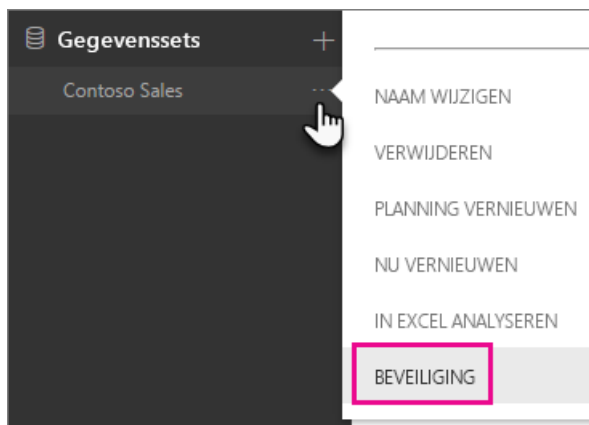
4. Selecteer **OK** en het rapport wordt weergegeven op basis van wat de gebruiker kan zien.

Binnen Power BI Desktop geeft **Andere gebruiker** alleen verschillende resultaten weer wanneer u dynamische beveiliging gebruikt op basis van uw DAX-expressies.

De beveiliging voor uw model beheren

Als u de beveiliging wilt beheren voor uw gegevensmodel, gaat u als volgt te werk:

1. Selecteer het **weglatingssteken (...)** voor een dataset.
2. Selecteer **Beveiliging**.



Zodoende opent u de RLS-pagina, waar u leden kunt toewijzen aan een rol die u hebt gemaakt in Power BI Desktop. De beveiliging is alleen zichtbaar en beschikbaar voor de eigenaren. Als de gegevensset zich in een groep bevindt, zien alleen beheerders van de groep de beveiligingsoptie.

U kunt alleen rollen maken of wijzigen in Power BI Desktop.

Werken met leden

Leden toevoegen

U kunt een lid aan de rol toevoegen door het e-mailadres of de naam van de gebruiker, beveiligingsgroep of distributielijst op te geven die u wilt toevoegen. U kunt geen groepen toevoegen die in Power BI zijn gemaakt. U kunt leden [buiten uw organisatie](#) toevoegen.

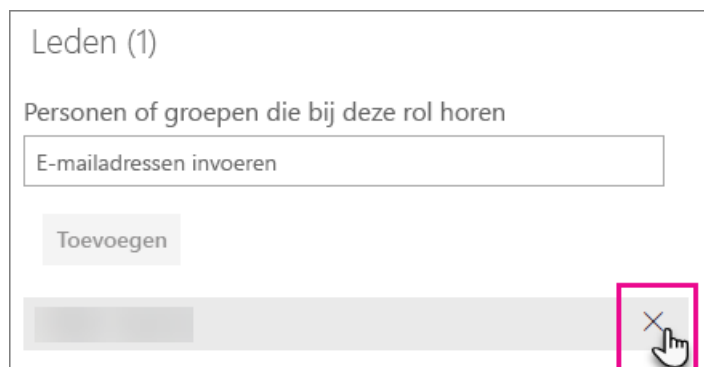


Aan het getal tussen haakjes naast de rolnaam of naast Leden kunt u zien hoeveel leden deel uitmaken van de rol op.



Leden verwijderen

U kunt leden verwijderen door de X naast hun naam te selecteren.



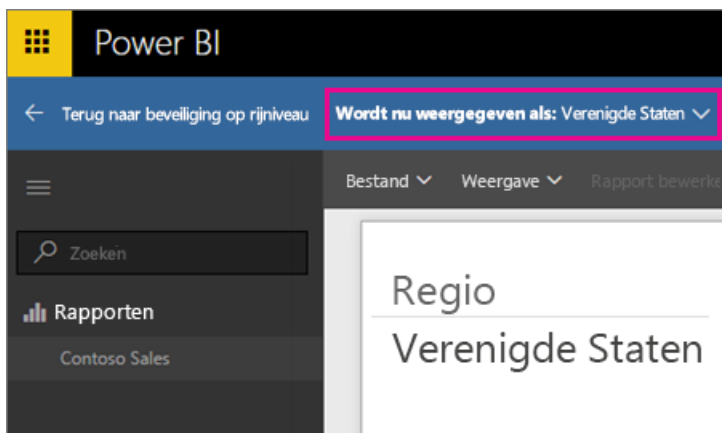
De rol in de Power BI-service valideren

U kunt controleren of de rol die u hebt gedefinieerd, correct werkt door de functie testen.

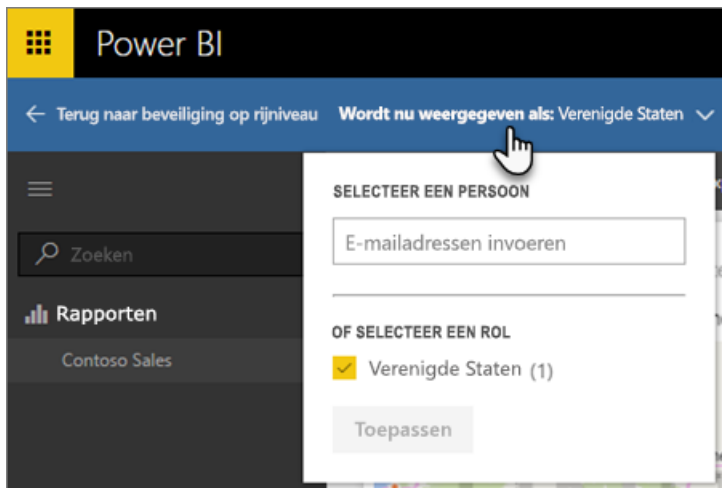
1. Selecteer **Meer opties** (...) naast de rol.
2. Selecteer **Gegevens testen als rol**.



Vervolgens ziet u de rapporten die beschikbaar zijn voor deze rol. Er worden geen dashboards gepresenteerd in deze weergave. In de bovenstaande blauwe balk ziet u wat wordt toegepast.



U kunt andere rollen of een combinatie van rollen testen door te selecteren **Nu weergeven als**.



U kunt ervoor kiezen om de gegevens weer te geven als een specifiek persoon, maar u kunt ook een combinatie van beschikbare rollen selecteren om te valideren of ze werken.

Als u de normale weergave wilt herstellen, selecteert u **Terug naar beveiliging op rijniveau**.

De DAX-functie `username()` of `userprincipalname()` gebruiken

U kunt gebruik maken van de DAX-functies `username()` of `userprincipalname()` binnen uw gegevensset. U kunt deze gebruiken in expressies in Power BI Desktop. Wanneer u uw model publiceert, worden deze functies gebruikt in de Power BI-service.

In Power BI Desktop retourneert de functie `username()` een gebruiker met de indeling `DOMEIN\gebruiker` en retourneert de functie `userprincipalname()` een gebruiker met de indeling `user@contoso.com`.

In de Power BI-service retourneren zowel `username()` als `userprincipalname()` de UPN (User Principal Name) van de gebruiker. Dit lijkt op een e-mailadres.

RLS met werkrumten gebruiken in Power BI

Als u een Power BI Desktop-rapport naar een werkrumte in de Power BI-service publiceert, worden de rollen toegepast op leden met Alleen lezen-toegang. U moet aangeven dat leden de Power BI-inhoud alleen kunnen weergeven binnen de instellingen van de werkrumte.

WARNING

Als u de werkrumte zodanig hebt geconfigureerd dat leden bewerkingsmachtigingen hebben, worden de RLS-rollen niet toegepast op deze leden. Gebruikers kunnen alle de gegevens bekijken.

Privacy

Privé: alleen goedgekeurde leden kunnen de inhoud bekijken

Leden kunnen alleen Power BI-inhoud weergeven ▼

Beperkingen

Hier volgt een lijst van de huidige beperkingen voor beveiliging op rijniveau voor cloudmodellen.

- Als u eerder rollen en regels hebt gedefinieerd in de Power BI-service, moet u deze opnieuw maken in Power BI Desktop.
- U kunt RLS alleen definiëren in gegevenssets die zijn gemaakt met Power BI Desktop. Als u RLS wilt inschakelen voor gegevenssets die zijn gemaakt met Excel, moet u uw bestanden eerst naar PBIX-bestanden (Power BI Desktop) converteren. [Meer informatie](#)
- Alleen Import- en DirectQuery-verbindingen worden ondersteund. Live verbindingen met Analysis Services worden afgehandeld in het on-premises model.

Bekende problemen

Er is een bekend probleem waarbij er een foutmelding optreedt wanneer u een eerder gepubliceerd rapport probeert te publiceren vanuit Power BI Desktop. Het scenario is als volgt.

1. Anna heeft een gegevensset die is gepubliceerd naar de Power BI-service en heeft RLS geconfigureerd.
2. Anna werkt het rapport bij in Power BI Desktop en publiceert het opnieuw.
3. Anna krijgt een foutmelding.

Tijdelijke oplossing: Publiceer het Power BI Desktop-bestand opnieuw vanuit de Power BI-service totdat dit probleem is opgelost. U kunt dat doen door **Gegevensbestanden** > **ophalen** te selecteren.

Veelgestelde vragen

Vraag: Wat als ik eerder rollen en regels hebt gemaakt voor een gegevensset in de Power BI-service? Blijven ze gewoon werken als ik niets doe?

Antwoord: Nee, visuals worden niet goed weergegeven. U moet de rollen en regels opnieuw maken binnen Power BI Desktop en deze publiceren naar de Power BI-service.

Vraag: Kan ik deze rollen voor Analysis Services-gegevensbronnen maken?

Antwoord: Dat kan als u de gegevens hebt geïmporteerd in Power BI Desktop. Als u een live verbinding gebruikt, kunt u RLS niet configureren binnen de Power BI-service. Dit wordt gedefinieerd in het Analysis Services-model on-premises.

Vraag: Kan ik RLS gebruiken om de kolommen of metingen te beperken die toegankelijk zijn voor mijn gebruikers?

Antwoord: Nee. Als een gebruiker toegang heeft tot een bepaalde gegevensrij, kan deze gebruiker alle gegevenskolommen voor die rij zien.

Vraag: Kan ik met RLS gedetailleerde gegevens verbergen maar toegang geven tot samengevatte gegevens in visuele elementen?

Antwoord: Nee, u beveiligt individuele rijen met gegevens maar gebruikers kunnen altijd de details of de samengevatte gegevens zien.

Vraag: Er zijn al beveiligingsrollen gedefinieerd voor mijn gegevensbron (bijvoorbeeld SQL Server-rollen of SAP BW-rollen). Wat is de relatie tussen de beveiligingsrollen en beveiliging op rijniveau?

Antwoord: Het antwoord hangt af van het feit of u gegevens importeert of DirectQuery gebruikt. Als u gegevens importeert in uw Power BI-gegevensset, worden de beveiligingsrollen in uw gegevensbron niet gebruikt. In dat geval moet u beveiliging op rijniveau instellen om beveiligingsregels af te dwingen voor gebruikers die verbinding maken in Power BI. Als u DirectQuery gebruikt, worden de beveiligingsrollen in uw gegevensbron gebruikt. Wanneer een gebruiker een rapport opent, verzendt Power BI een query naar de onderliggende gegevensbron waarmee beveiligingsregels worden toegepast op de gegevens op basis van de inloggegevens van de gebruiker.

Volgende stappen

[Beveiliging op rijniveau \(RLS\) met Power BI](#)

Nog vragen? [Misschien dat de Power BI-community het antwoord weet](#)