# Vanuit onderwijs samenwerken met externen in Office 365

## Kennisdelingsbijeenkomst Office 365

Beat Nideröst - 13 april 2018

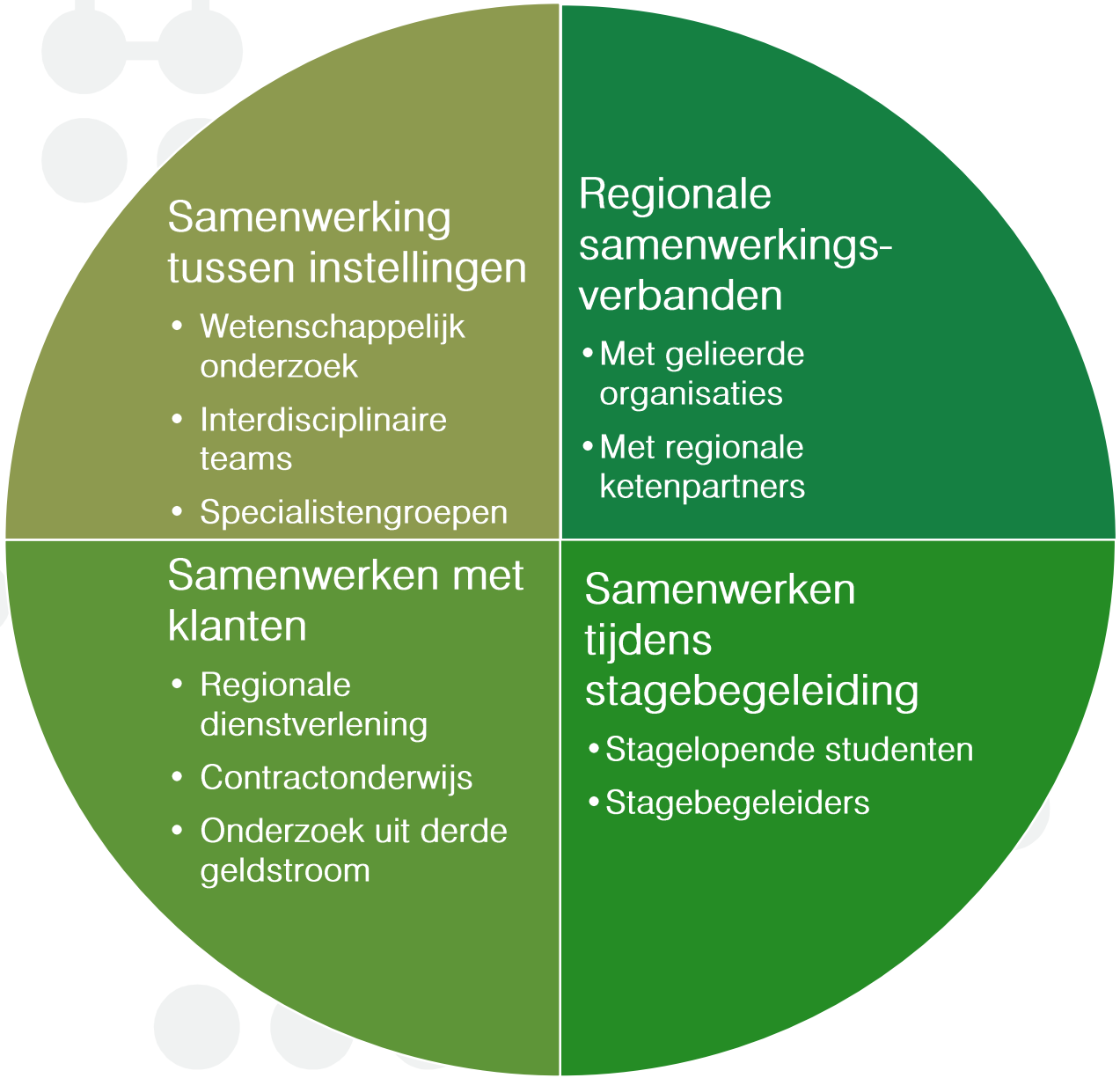
2at.

# Achtergrond

- Office 365 cookbook voor onderwijs en onderzoek in Nederland
  - Regie op Office 365
  - Visie & Strategie, Besluitvorming, Architectuur, Implementatie, Beheer, Off-boarding
  - Onderwijsinstellingen, SURFmarket, 2AT
- Edugroepen en Teamwerk
  - Samenwerken tussen organisaties (onderwijs, UMC's), onderling en met ketenpartners
- Digitale Leer- en Werkomgevingen
  - Samenwerken met externen, bijvoorbeeld stagebegeleiders, gastsprekers, alumni, externe docenten, onderzoekers, internationale samenwerkingsverbanden
  - Bijvoorbeeld HvA, UvA en regionale partijen (VU, Vumc, AMC, …)

2at.

# Wie werken er samen?

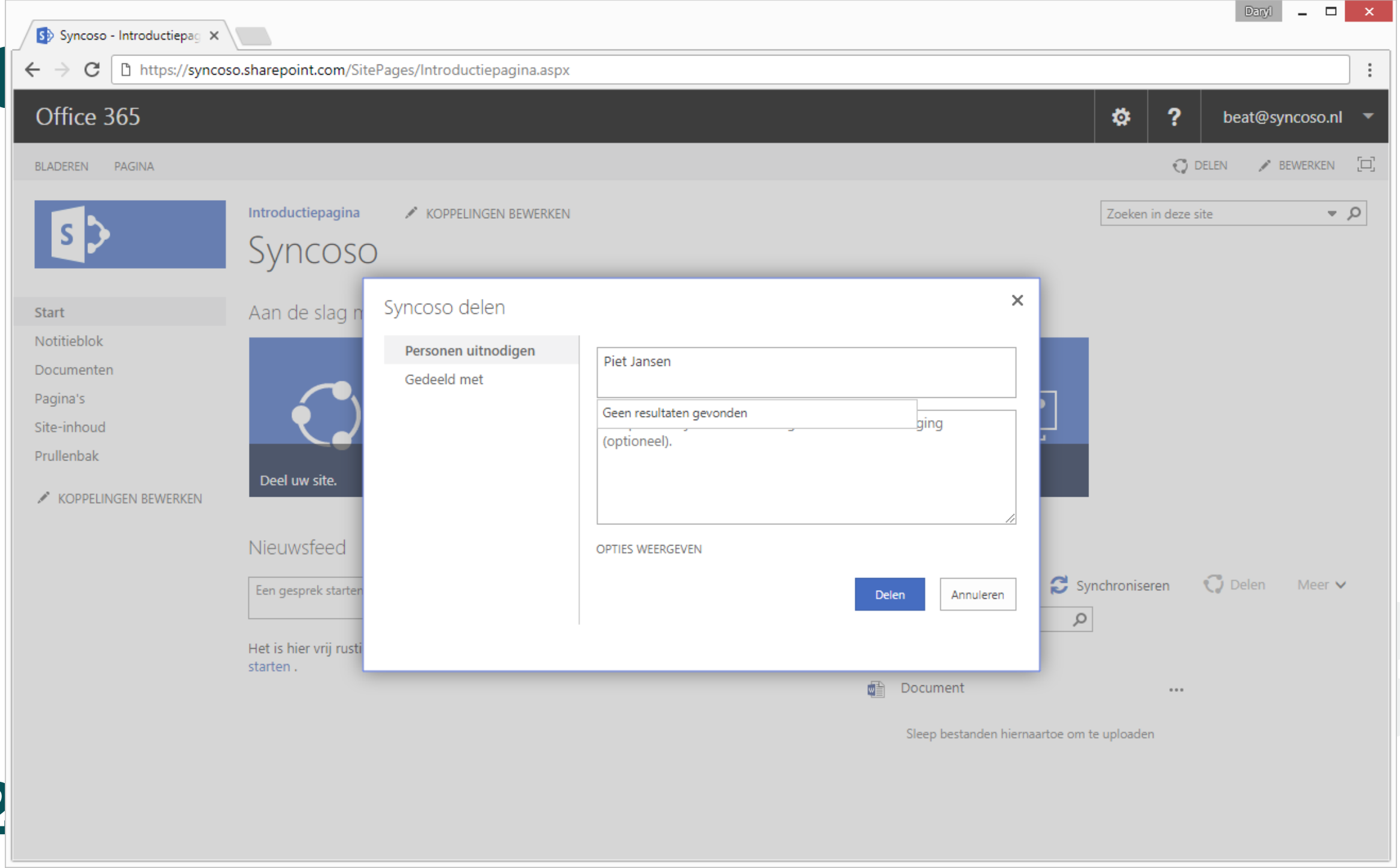


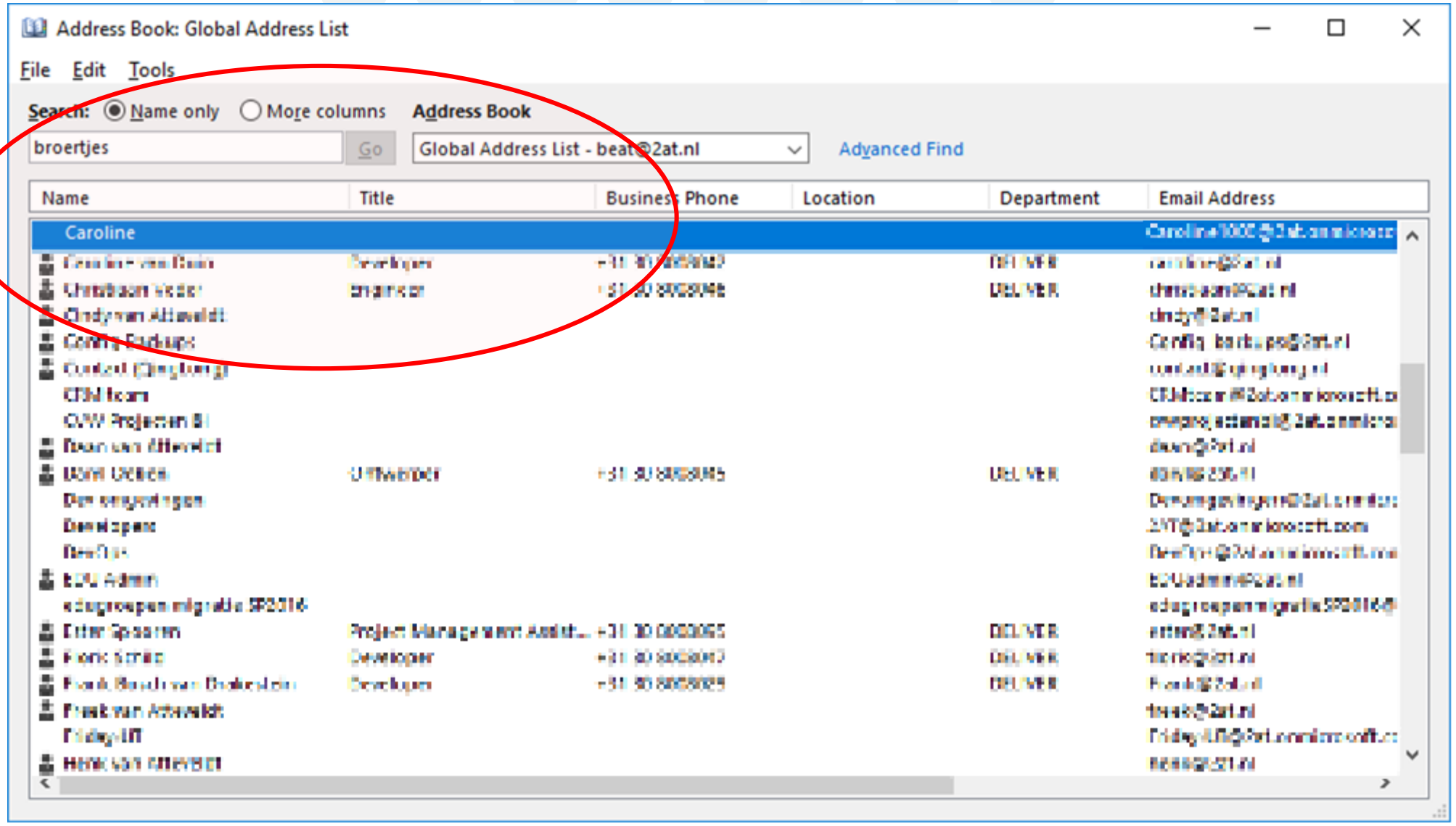

2at.

# Samenwerken in Office 365

- Onderwijsorganisaties werken samen in Office 365
- Ze hebben vaak een aparte Office 365 tenant per organisatie
  - Vanwege juridische aspecten
  - Vanwege autonomie
  - Vanwege beheer(s)baarheid
- Samenwerken in Office 365 is in principe binnen één tenant
  - Binnen één tenant werkt alle functionaliteit van Office 365 zoals bedoeld / samenwerken is goed mogelijk
  - Office 365 workloads gebruiken één gezamenlijke directory:
    - De tenant-specifieke Azure Active Directory (AAD)
- Zonder account in de AAD werken zaken niet of slecht
  - Gebruikers niet vindbaar in adresboek / geen gedeeld adresboek
  - Gebruikers geen toegang of niet de gewenste rechten
  - Verlenen van toegang is omslachtig en foutgevoelig
  - Diverse grote en kleine functionaliteiten werken niet (bijvoorbeeld versturen van e-mails en opslaan van chat history)

2at.


Daryl
Syncoso - Introductiepag
https://syncoso.sharepoint.com/SitePages/Introductiepagina.aspx
Office 365
beat@syncoso.nl
BLADEREN
PAGINA
DELEN
BEWERKEN
Introductiepagina
KOPPELINGEN BEWERKEN
Zoeken in deze site
Syncoso
Start
Notitieblok
Documenten
Pagina's
Site-inhoud
Prullenbak
KOPPELINGEN BEWERKEN
Aan de slag
Deel uw site.
Nieuwsfeed
Een gesprek starten
Het is hier vrij rusti
starten .
Syncoso delen
Personen uitnodigen
Gedeeld met
Piet Jansen
Geen resultaten gevonden
(optioneel).
OPTIES WEERGEVEN
Delen
Annuleren
Synchroniseren
Delen
Meer
Document
Sleep bestanden hiernaartoe om te uploaden


Address Book: Global Address List
File Edit Tools
Search: Name only More columns
Address Book
broertjes
Go
Global Address List - beat@2at.nl
Advanced Find
Name
Title
Business Phone
Location
Department
Email Address
Caroline

# Volwaardig account – een oplossing?

- Uitgangspunt: geef alle gebruikers een volwaardig account in de betreffende tenant
- Vraagstukken:
  - Account-provisioning en deprovisioning
    - Aanvraagprocedures?
    - Welk (bron)systeem is leidend?
    - Wanneer weer opruimen?
    - Wordt ad-hoc samenwerken ondersteund?
  - Vertrouwen (correctheid van attributen, herleidbaar tot natuurlijk persoon?)
  - Licensering / overtekening
  - Welke functionaliteiten zijn echt wenselijk / nodig?
    - Denk aan e-mailadres, mailbox, OneDrive, self-service teamsites, Office Client apps, sip-adres / telefoonnummer
  - Welke informatie moet wel/niet beschikbaar zijn voor externe gebruikers?
    - Beleid en rechten, inrichting en bewaking
    - Aparte gebruikersgroepen? Begrijpen eindgebruikers dit?
  - Hoeveel accounts / toegangsgegevens moet een gebruiker onthouden?

2at.

# Alternatief: gastgebruikers

- Geen volwaardig account? Dan gastgebruik…?
- Gastgebruikers zijn een apart type gebruikers in AAD
  - Afwijkende provisioning, authenticatie, licensering, functionaliteiten en rechten
- Beschikbaar via Office 365 self-service functionaliteiten
  - Self-service voor sites, groepen en teams
  - Self-service voor delen van content met externen
  - Self-service voor uitnodigen gastgebruiker in tenant
- Let op beheer(s)baarheid
  - Wie heeft sites, groepen, teams, gastgebruikers aangemaakt?
  - Hoe lang moeten sites, groepen, teams, gastgebruikers blijven bestaan?
  - Kloppen namen, beschrijvingen, urls en attributen?
    - En zijn deze wenselijk?
  - Wie is verantwoordelijk voor content?

2at.

# Verschillende typen gastgebruikers

| | Gebruikers mét AAD account | Gebruikers zonder AAD account |
|---|---|---|
| Vast samenwerkings-verband | Azure B2B synchronisatie | Pre-provisioned gastgebruik |
| Ad-hoc samenwerken | Azure B2B ad-hoc uitnodigen | Ad-hoc gastgebruik met Microsoft account |

2at.

# Voordelen van de verschillende vormen van gastgebruik

- Voordelen synchronisatie / pre-provisioning
  - Gebruikers van tevoren vindbaar
  - Controle over attributen
  - Beheer(s)baar via controle over containers en attributen
  - Deprovisioning goed mogelijk
- Voordelen ad-hoc samenwerken
  - Light-weight - Ook met partijen mogelijk zonder vast samenwerkingsverband
  - Geen koppeling / synchronisatie noodzakelijk

2at.

# Uitdagingen technische inrichting gastgebruik

- Welke versie van eigen tenant?
- Exacte inrichting van eigen tenant?
- Inrichting van tenant van gast?
- AAD Connect / configuratie
- Authenticatie-infrastructuur
  - SURFconext?
  - Microsoft 2FA, SURF Secure ID en andere multi-factor oplossingen
- Technisch beheer van de wijzigende inrichting
- Probleem schaalt niet
  - Full-mesh versus hub-and-spoke
  - Hoe blijven verschillende typen gastgebruikers herkenbaar en herleidbaar?

2at.

# Het uitnodigingsproces

- Uitnodigen doet meerdere zaken:
  1. Indien noodzakelijk -> aanmaken Microsoft account
  2. Aanmaken gastaccount in AAD van uitnodigende organisatie
  3. Verlenen van toegang tot omgeving (teamsite, groep, …) voor gastgebruik
- Elke stap kan om diverse redenen mislukken
  - Er bestaat al een Microsoft account op het genodigde e-mailadres
  - Gebruiker is op verkeerde / onhandig e-mailadres uitgenodigd
  - Gebruiker is al elders gemachtigd / gastaccount bestaat al
  - Gebruiker wordt niet uitgenodigd maar krijgt rechten toebedeeld
  - Gebruiker is (met verkeerd) account ingelogd bij reageren op uitnodiging
  - Technische inrichting van gast- of doeltenant is niet correct
  - Etc…
- Proces is ingewikkeld
  - Geen eenvoudige handleiding mogelijk
  - (Vertaalde) teksten in uitnodigingsmails, processtappen en foutmeldingen zijn niet helder
  - Niet alle uitzonderingssituaties zijn goed afgedekt

2at.

# Functionele onduidelijkheden

- Uitnodigen van bekende gastgebruikers verloopt anders dan uitnodigen van onbekende gastgebruikers
  - Zowel voor uitnodigende persoon als voor genodigde
- E-mailadres ≠ accountnaam ≠ UPN ≠ SIP adres
- Verschil tussen work- or schoolaccount en Microsoft account niet helder
  - En sommige mensen hebben beide! Met hetzelfde e-mailadres!
- “Welke link moet ik klikken” in uitnodigingsmail groepen
- Verschillen in werkplek
  - Wel/geen Outlook rich client, Office Online / Outlook webtoegang, desktop SSO, 2FA, ondersteunde webbrowser, mobile client apps

2at.

# Lifecycle management

- Wanneer mag / moet een gastgebruiker worden verwijderd?
  - Lifecycle van bronaccount bekend en vertrouwd?
  - Deelname aan meerdere sites/teams/groepen?
  - Wat als uitnodiger niet (meer) bekend of benaderbaar is?
    - Wie is aanspreekbaar op handelingen gastgebruiker?
  - Herleidbaarheid van historische acties?
    - Bijdragen & co-authoring, deelname aan conversaties, audit trail
    - Anonimiseren gewenst, verplicht en technisch mogelijk?
- AVG geeft recht om vergeten te worden
  - Verplichting van verwerkersverantwoordelijke om op te ruimen
    - Wat als informatie is verspreid naar directories van andere instellingen?

2at.

# Waar krijgt een gastgebruiker toegang toe?

- Welke apps en content?
  - Azure AD leestoegang?
  - Adreslijsten?
  - Gebruikersprofielen?
  - Intern gedeelde sites, groepen, teams?
  - Delve?
- Welke (privacygevoelige) attributen?
  - Contactgegevens, (studentenpas)foto, studiegegevens
- Voldoende vertrouwen in authenticatiemiddelen van gastgebruikers?
  - Gastgebruikers herleidbaar tot natuurlijke personen?
  - Registratie van gebruikte e-mailadressen en/of ip-adressen?
  - Voldoende beveiliging tegen identity theft?
  - Wel / geen tweede factor verplicht?
    - Extra factor vanuit doeltenant beschikbaar stellen?
- Risico is omvangrijker bij “normale” accounts
  - Worden studenten in dezelfde mate vertrouwd als medewerkers?
  - Is de noodzaak voor een instellingsbreed adresboek met medewerkers én studenten wel voldoende onderbouwd?

2at.

## Uw team maken

Nauw samenwerken met een groep mensen binnen uw bedrijf op basis van organisatie, project, initiatief of gemeenschappelijk belang. Een kort overzicht bekijken

Teamnaam

Beschrijving

Privacy

Openbaar - iedereen in uw organisatie kan deelnemen

Een team maken met een bestaande Office 365-groep

Annuleren Volgende

2at.

# Case: Teamwerk naar Office 365

- Teamwerk
  - Samenwerken tussen 8 UMC's
    - In totaal 65'000 FTE, > 100'000 interne gebruikers
  - Gasttoegang voor regionale zorginstellingen, internationale onderzoekers en deelnemers, etc., etc.
  - Migratie van één On-Premises SharePoint omgeving naar 7 aparte Office 365 tenants
    - (AMC en Vumc gaan samen naar één tenant)
- Probleemstelling vergelijkbaar met in onderwijsland
  - Vergelijkbare omvang van samenwerking tussen instellingen
  - Ook studenten aanwezig (van universiteiten en hbo instellingen)

2at.

# Scenario's


2at.

# Doel en randvoorwaarden

- Eenvoudige documentuitwisseling
- Laagdrempelige toegang tot contactgegevens
- Optimale samenwerking faciliteren

- Randvoorwaarden
  - Betrouwbare omgeving, direct begrijpelijk
  - Vanuit diversiteit van werkplekken bruikbaar met beperkte functionele support
  - Functionarissen gegevensbescherming besluiten: niet in control van (privacy)gevoelige gegevens = niet naar cloud!

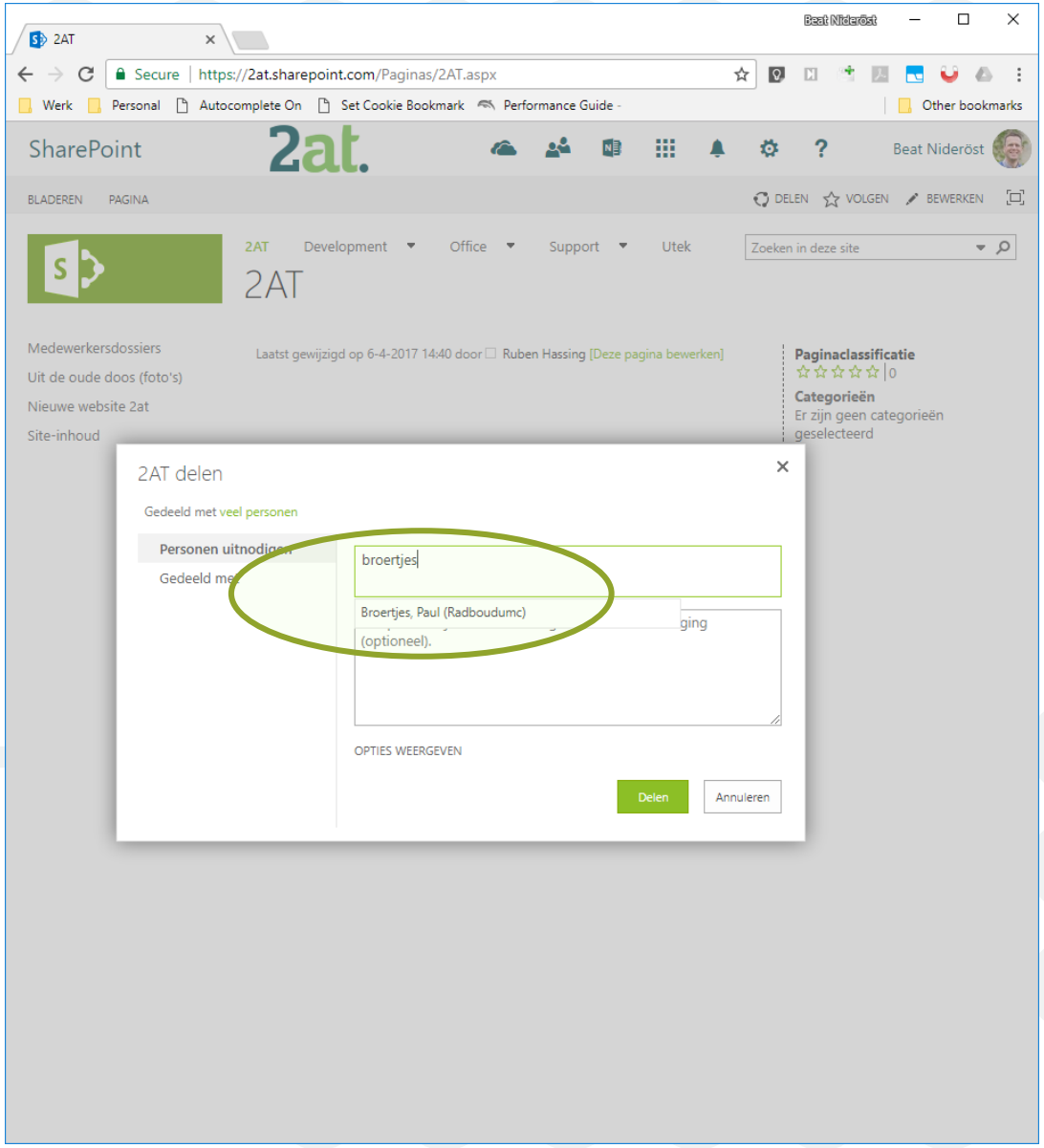
2at.

# Identity Hub for Healthcare

## Optimale samenwerking

- Door laagdrempelige toegang tot correcte contactgegevens
- Door eenvoudig beschikbare contactpersonen bij:
  - Versturen van e-mails
  - Delen van documenten
  - Samenwerken in groepen, teams, sites
  - Gedeelde mailboxen, agenda's, etc.

2at.


2AT
Secure https://2at.sharepoint.com/Paginas/2AT.aspx
Werk
Personal
Autocomplete On
Set Cookie Bookmark
Performance Guide -
Other bookmarks
SharePoint
2at.
Beat Nideröst
BLADEREN
PAGINA
DELEN
VOLGEN
BEWERKEN
2AT
Development
Office
Support
Utek
Zoeken in deze site
2AT
Medewerkersdossiers
Uit de oude doos (foto's)
Nieuwe website 2at
Site-inhoud
Laatst gewijzigd op 6-4-2017 14:40 door Ruben Hassing [Deze pagina bewerken]
Paginaclassificatie
Categorieën
Er zijn geen categorieën geselecteerd
2AT delen
Gedeeld met veel personen
Personen uitnodigen
Gedeeld met
broertjes
Broertjes, Paul (Radboudumc)
(optioneel).
OPTIES WEERGEVEN
Delen
Annuleren

2at.

# Oplossingsrichting

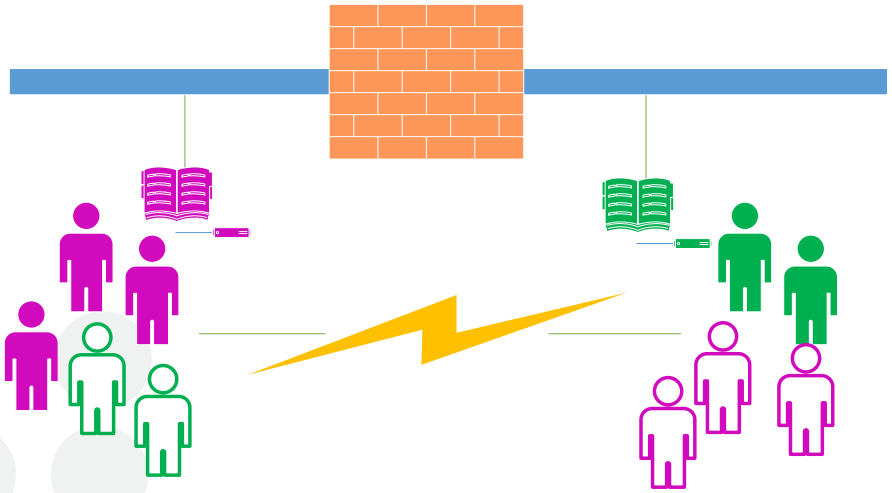
- Gebruikers en groepen synchroniseren tussen adresboeken van deelnemende instellingen
- Identity management as a trusted-third-party service
- Hub-en-spoke model voor schaalbaarheid
- Gestandaardiseerde processen voor ad-hoc gastgebruik (validatie van identiteit, provisioning  & deprovisioning)
- Aansluitvoorwaarden en compliance monitoring en rapportage voor trust (op tenantinrichting, identity management en contentbeheer)

2at.

# Details gebruikerssynchronisatie

Volwaardige gebruikers uit adresboek van bronorganisatie worden beheerde gastgebruikers in adresboek van doelorganisatie

- Voor gastgebruikers zijn geen Office 365 licenties nodig
- Ook groepen en lidmaatschap kunnen worden gesynchroniseerd



Samenwerking met gasten wordt evenwaardig aan samenwerken met collega's van eigen organisatie

- Gedeeld adresboek
- Toegang verlenen
- Content delen

2at.

# Portaal voor beheerders

- Selecteren van gebruikers en groepen om te delen (export)
- Delen met externe instellingen (export)
- Accepteren inkomende synchronisatiebronnen (import)
- Controle van synchronisatiestatus
- Inzage in gesynchroniseerde gegevens (details)
- Onderhouden business regels en attribuuttransformaties
- Rapportage over compliance en lifecycle management

2at.

# Functionaliteiten in beheerportaal 1/2

- Configuratie van bron
  - Query, filters, projectie
- Configuratie van exports
  - Welke zorginstellingen
  - Per zorginstelling: welke subset van objecten en attributen
  - Per zorginstelling: attribuuttransformaties
- Configuratie van import
  - Welke zorginstellingen
  - Per zorginstelling: resource voor locatie, rechten en beheer
  - Per zorginstelling: welke subset van objecten en attributen
  - Per zorginstelling: attribuuttransformaties

2at.

# Functionaliteiten in beheerportaal – 2/2

- Zoekfunctionaliteiten
  - Van eigen gebruikers en externe gebruikers
    - Attributen
      - Uit bron / import
      - Naar verschillende exports / eigen Azure AD
      - Desired vs actual
    - Status
      - Van imports en verschillende exports
- Logging en rapportage
  - Syncmomenten en resultaten (gelukt / log van fouten)
  - Statistieken
    - Aantallen objecten, creates, updates, deletes, etc.
  - Lifecycle managementrapportage, ook voor eigen objecten in vreemde AAD's
  - Licentiebeheer / uitnutting

2at.

# Identity Hub for Healthcare “as a Service”

- Identitymanagementoplossing ontwikkeld en onderhouden door 2AT
  - Support en onderhoud bij wijzigingen in technologie
  - Helpdesk, functioneel en applicatiebeheer met SLA
- Synchronisatie op basis van Microsoft technologie
  - Azure AD B2B API
  - Ontwikkeld en gehost als Azure Services
  - Gebruikt Microsoft Identity Management synchronisatietechnologie

2at.

# Support met gegarandeerde servicelevel

- Supportverzoeken aanmelden:
  - Per e-mail via support@2at.nl, óf
  - Telefonisch via 030 800 8080
- Gegarandeerde responstijd van 1 werkdag
  - Hoge prioriteit verstoringen aan de dienst worden gegarandeerd binnen 1 uur na telefonisch melden opgepakt
- Servicedesk telefonisch 24 x 7 beschikbaar bij calamiteiten

2at.

# Voordelen 1/2

- Organisatie blijft eigenaar van persoonsgegevens eigen gebruikers
  - Inzage in en controle over gesynchroniseerde objecten en attributen in externe tenants
  - Data privacy rapportage - Zijn objecten écht aangemaakt, gewijzigd of verwijderd in adresboek van doelorganisatie?
- Organisatie houdt volledige controle over eigen tenant
  - Duidelijk herkenbare externe gebruikers
  - Minimale rechten benodigd voor sync (leesrechten op brongegevens, beperkte schrijfrechten voor doelgegevens, hub & spokes model zorgt voor minimale complexiteit)
  - Volledige controle over welke gegevens worden geëxporteerd en geïmporteerd
- Integrale lifecycle management & rapportage
  - Op geëxporteerde eigen objecten
  - Op geïmporteerde objecten van andere organisaties

2at.

# Voordelen 2/2

- Gegarandeerde beschikbaarheid 99,9% met stateful recovery
- Technisch beheer en applicatiebeheer volledig uitbesteed
- Geen onderhoud aan dienst en codebase noodzakelijk
- Snelle uitrol en lage beheerlast dankzij gestandaardiseerde interfaces en loosely coupled architectuur
  - Laagdrempelig te configureren via beheerportaal
  - Standaard https verkeer (TLS) / geen firewall changes nodig

2at.

# Security & Privacy

- Technische beveiliging
  - Data @ rest encryption
  - Transport layer encryption
  - Message encryption
  - Managed Firewall (Microsoft Azure)
  - Afgeschermde backup & recovery
- Privacy
  - Gestandaardiseerde verwerkersovereenkomst
  - Conform Algemene Verordening Gegevensbescherming (AVG) / General Data Protection Regulation (GDPR)
- 2AT levert Identity Hub for Healthcare conform de richtlijnen en uitgangspunten van NEN 7510

2at.

Beat Nideröst / Carl Reitsma
beat@2at.nl / carl@2at.nl
www.2at.nl

2at.