nordic summit

Connecting to Dataverse:
do's, don'ts and how not to make all your data public by accident

DIAMOND SPONSOR

The Digital Neighborhood

PLATINUM SPONSOR

Microsoft

GOLD SPONSORS

mscrm-**addons**.com
Your company for MS-CRM ADD-ONS!

CRMK

link mobility

dox42
automate your documents
integrate your data

SILVER SPONSORS

ClickDimensions
It's your lead now™

resco.net

exflow

Evidi

BRONZE SPONSORS

PROXIMO3

abakion

QUBIX

knk

amanzia

sturx oü

sopra steria

Mats Necker

Likes all cloud stuff

- CTO @ knk Customer Engagement GmbH
- Business Applications MVP
- nckr.de
- @matzzt

Yannick Reekmans

Jack of all Trades

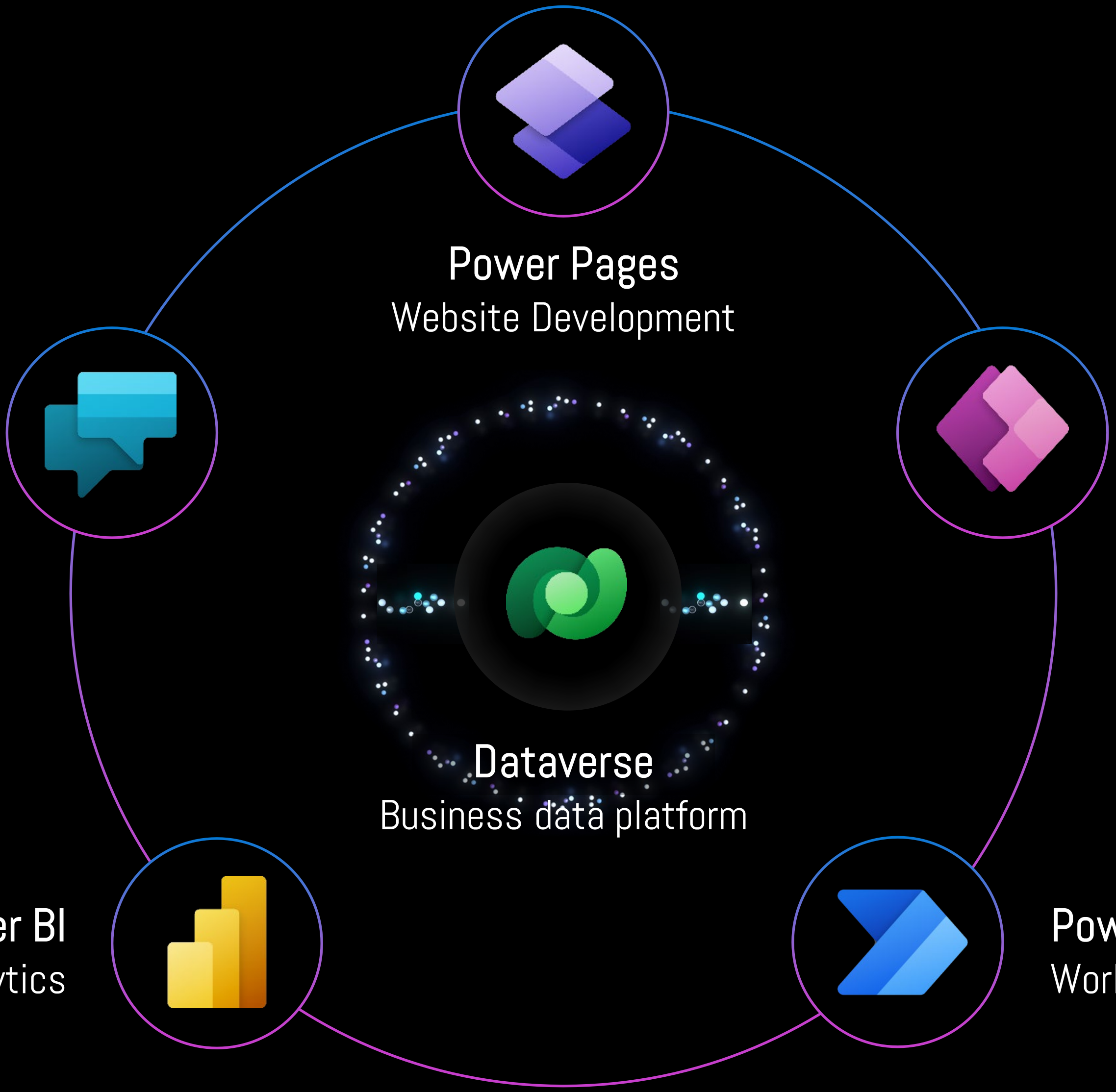
- Cloud Solution Architect @ Qubix
- Business Applications & M365 Development MVP
- blog.yannickreekmans.be
- @YannickReekmans

Agenda Session Goals

- Overview Dataverse
- Low Code Connectivity
- Authentication / Authorization
- Pro-Code Connectivity

+ Demos 🔥

Power Platform



Microsoft Dataverse – what´s in the box?

API

Security

- Authentication
- Authorization
- Role-based security
- Auditing

Logic

- Calculated & Rollup fields
- Jobs
- Plugins
- Business Rules
- Duplicate Detection
- Workflows

Data

- Modelling
- Catalog and discovery
- Reporting
- Data validation
- Common Data Model
- Multi-language Multi-currency

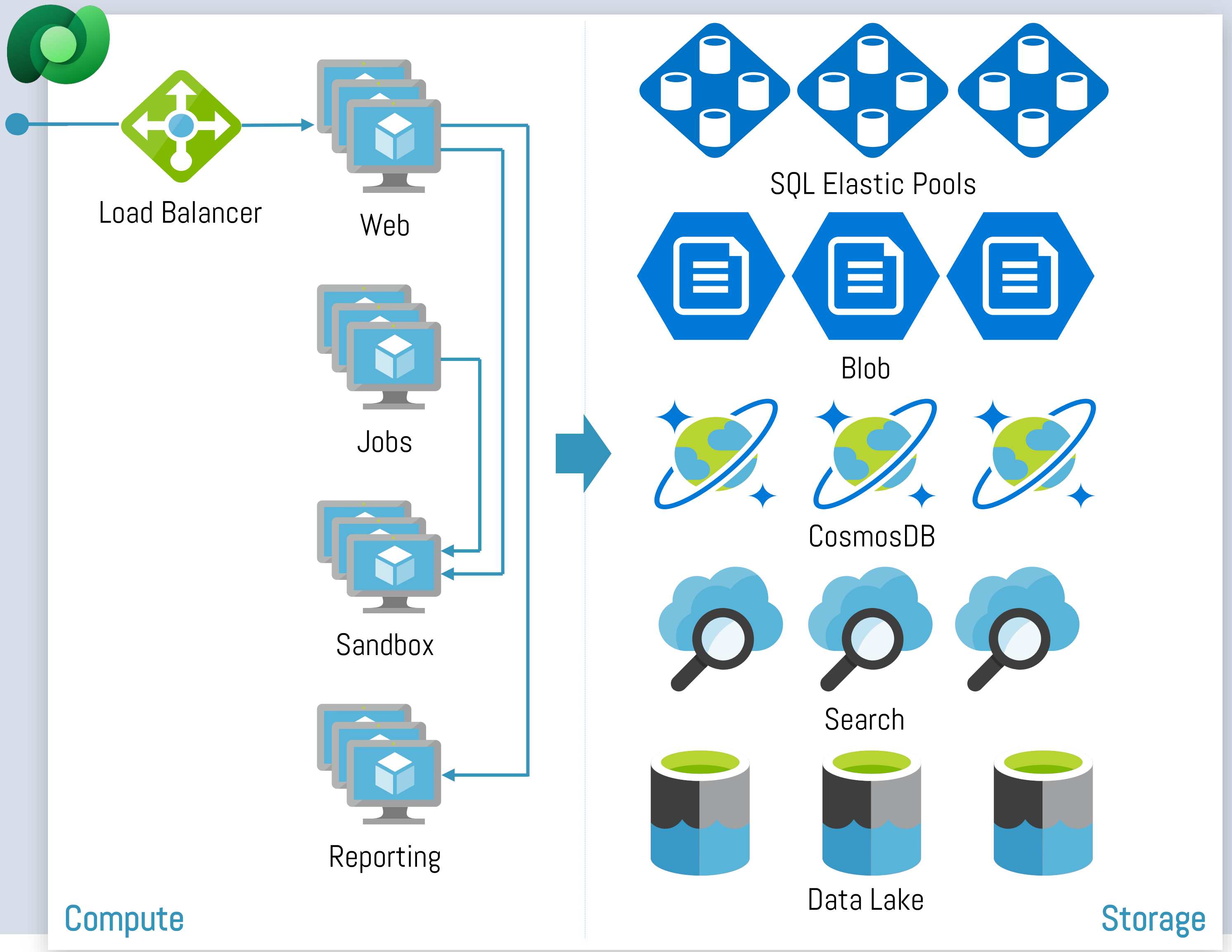
Storage

- Files and blobs
- Relational databases
- Semi-structured data
- Log files
- Relevance Search & Find data

Integration

- Webhooks
- ALM
- Azure DevOps
- Azure Synapse Analytics
- GitHub
- Data export

Dataverse on Azure



low-code Dataverse connectivity

SHOWTIME

authentication & authorization

It's a story of multiple layers

Authentication & Authorization

Authentication
Who are you?

Authorization
Do you have access?

Permissions
What are you allowed to do?

Authentication basics

Authentication

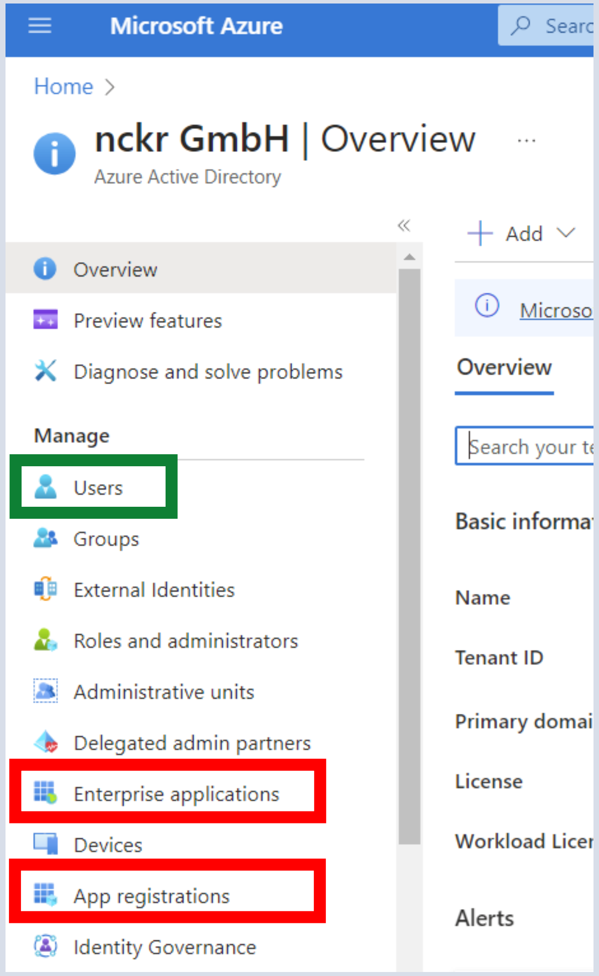
is the process of proving that you are who you say you are

Authorization

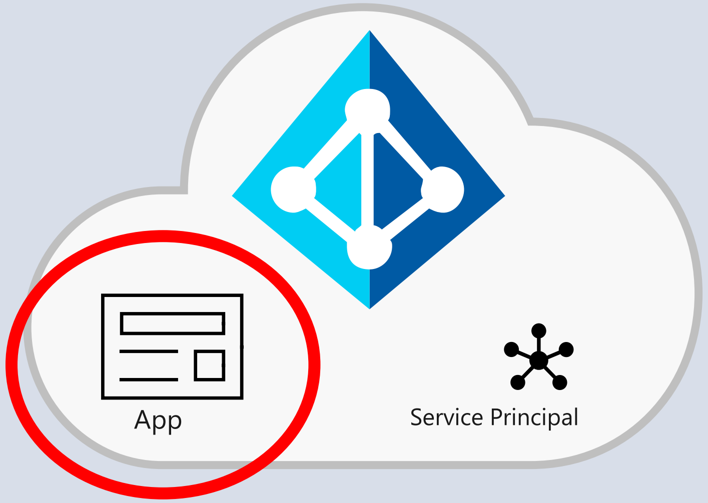
is the act of granting an authenticated party permission to do something. It specifies what data you're allowed to access and what you can do with that data.

Authentication basics

Microsoft Entra (The artist formerly known as "Azure Active Directory")



Everything needs an app



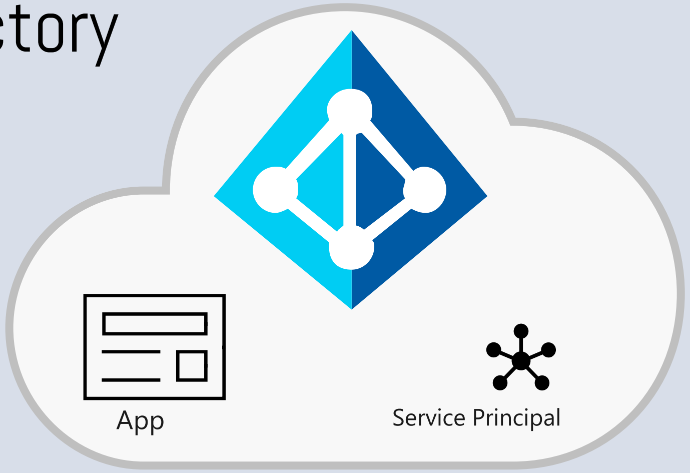
Authentication basics

Single Organization App

- App registered for a specific Azure AD directory

Single-tenant

- Only accessible by users from that Azure AD directory



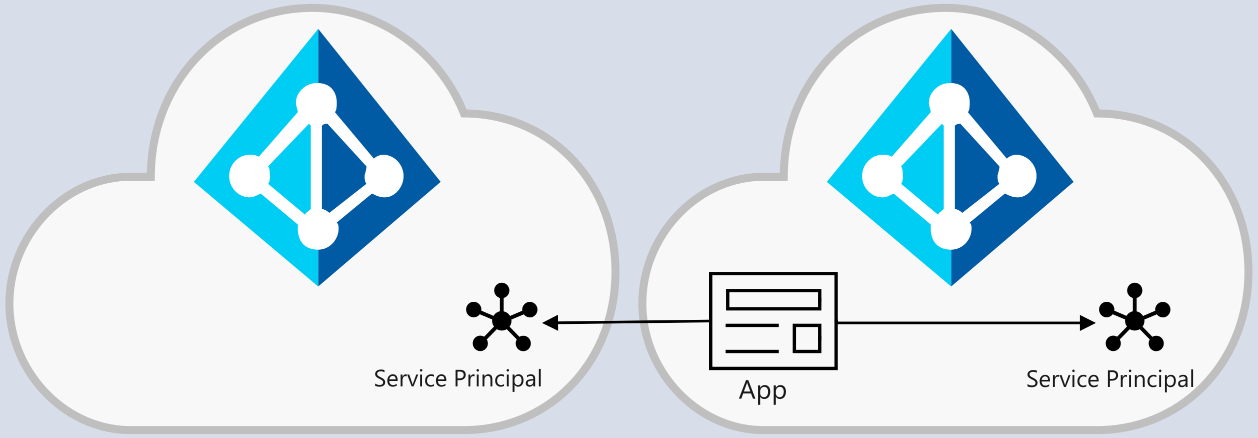
Authentication basics

Multi Organization App

- App registered for use in any Azure Directory or any Azure AD and personal Microsoft accounts (e.g. Skype, Xbox, Outlook.com)

Multi-tenant

- Registered in its "Home" directory (same process as single-tenant)
- Admins decide who can consent to apps in their tenant
- Developers are responsible for limiting to specific tenants!!



Permissions and consent

Delegated permissions

- Used by apps with a signed-in user present
- Either the user or an administrator consents to the permissions the app requests
- App is then enabled to act on behalf of the signed-in user
- **Important to note:** users do not grant apps permission; they grant the app ability to act on their behalf

Application permissions

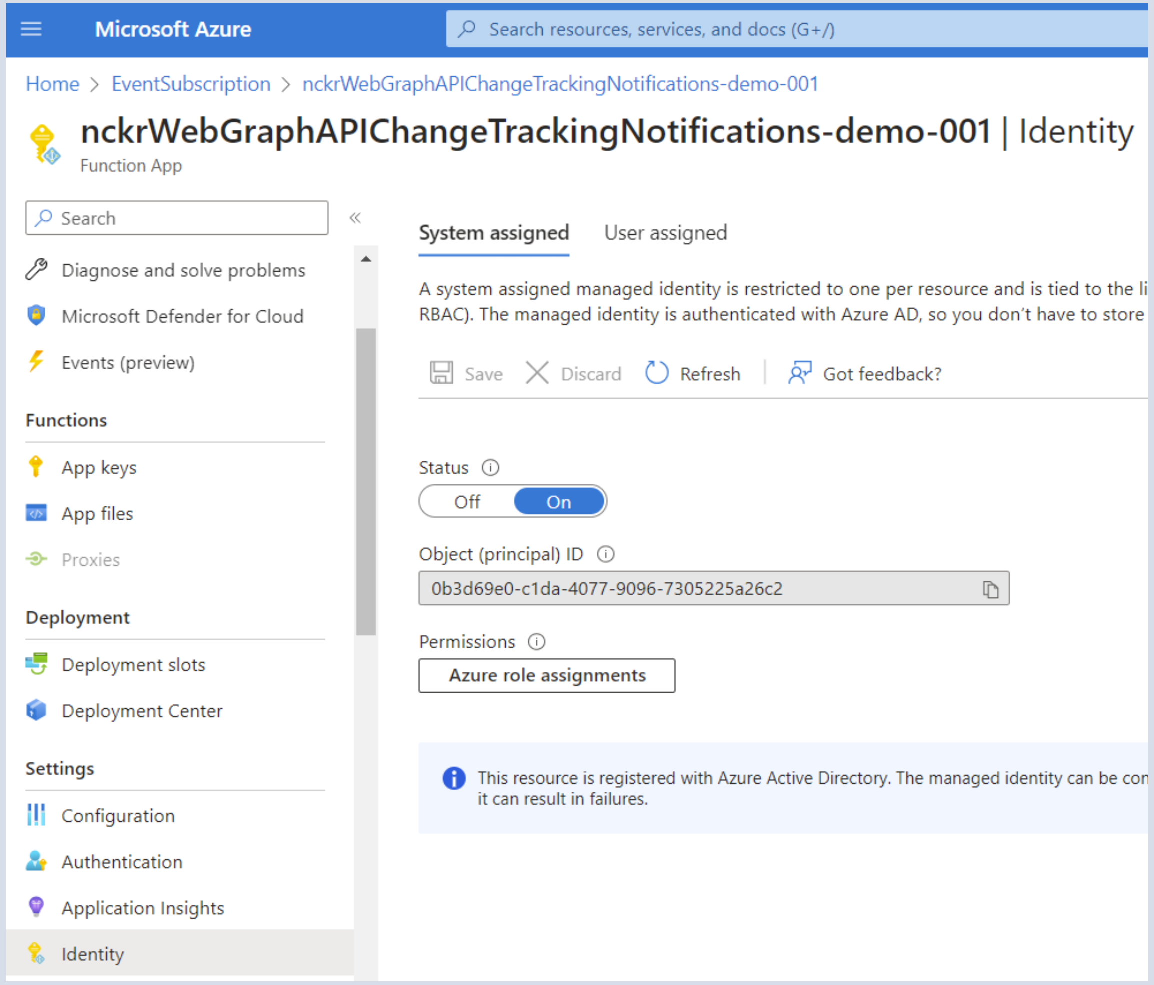
- Used by apps that run without a signed-in user present
- When the administrator grants application permissions, unlike delegated permissions, the grant isn't done on behalf of any specific user
- Client application is directly granted the application permission
- **Important to note:** requires the creation of an Application User in the Dataverse environment

Connection Credentials

User or Service Accounts	Service Principals aka. Application Users
Named account	System account
Requires username & password	Uses client id & client secret
Conditional Access & MFA impact flows	Secret lifetime to be monitored
Account lifecycle can impact flows	Managed separately
Requires licenses	Don't require licenses
Supported in many connectors	Limited connector support
Separation of concerns == more licenses	Separation of concerns == more SPN's
Lower API limits	Higher API limits

Managed Identities

Not a generic application – but one specific


Microsoft Azure

Search resources, services, and docs (G+/)

Home > EventSubscription > nckrWebGraphAPIChangeTrackingNotifications-demo-001

nckrWebGraphAPIChangeTrackingNotifications-demo-001 | Identity

Function App

Search

Diagnose and solve problems
Microsoft Defender for Cloud
Events (preview)

Functions
App keys
App files
Proxies

Deployment
Deployment slots
Deployment Center

Settings
Configuration
Authentication
Application Insights
Identity

System assigned | User assigned

A system assigned managed identity is restricted to one per resource and is tied to the li
RBAC). The managed identity is authenticated with Azure AD, so you don't have to store

Save | Discard | Refresh | Got feedback?

Status: Off [✓ On]

Object (principal) ID: 0b3d69e0-c1da-4077-9096-7305225a26c2

Permissions: Azure role assignments

This resource is registered with Azure Active Directory. The managed identity can be con
it can result in failures.

- Register "something" as an Application
- Make that application know to other systems
- Backend: An Application Registration
- BUT: Fully managed
- Assign specific permissions to Managed Identity
- Secret lifetime managed by Azure
- No secrets need to be know in code

Managed Identities

are better than

Service Principals or Application Users

are better than

Service Accounts

are better than

User (or named) Accounts

Security Roles

Authorization

- Users & Application Users need a security role
- Without a Security Role, no access!
- Security Roles define what a user can and cannot do

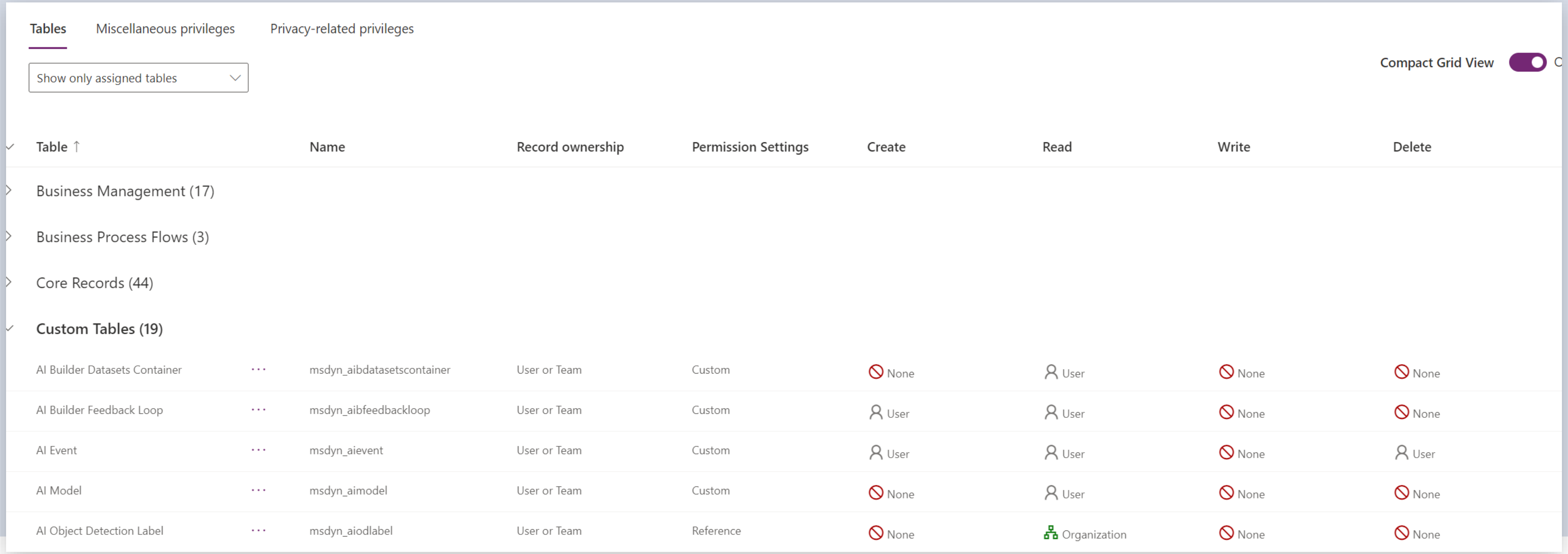


Table ↑	Name	Record ownership	Permission Settings	Create	Read	Write	Delete
Business Management (17)							
Business Process Flows (3)							
Core Records (44)							
Custom Tables (19)							
AI Builder Datasets Container	msdyn_aibdatasetscontainer	User or Team	Custom	None	User	None	None
AI Builder Feedback Loop	msdyn_aibfeedbackloop	User or Team	Custom	User	User	None	None
AI Event	msdyn_aievent	User or Team	Custom	User	User	None	User
AI Model	msdyn_aimodel	User or Team	Custom	None	User	None	None
AI Object Detection Label	msdyn_aiodlabel	User or Team	Reference	None	Organization	None	None

authentication & authorization

SHOWTIME

pro-code Dataverse connectivity

Work with data in Dataverse, using code

The options are plentiful, and mostly confusing...

- `/XRMServices/2011/OrganizationData.svc` aka. OrganizationDataService, using OData v2.0 ==> DEPRECATED!

- `/api/data/v9.2` aka. Web API, using OData v4.0
  - The future 😉

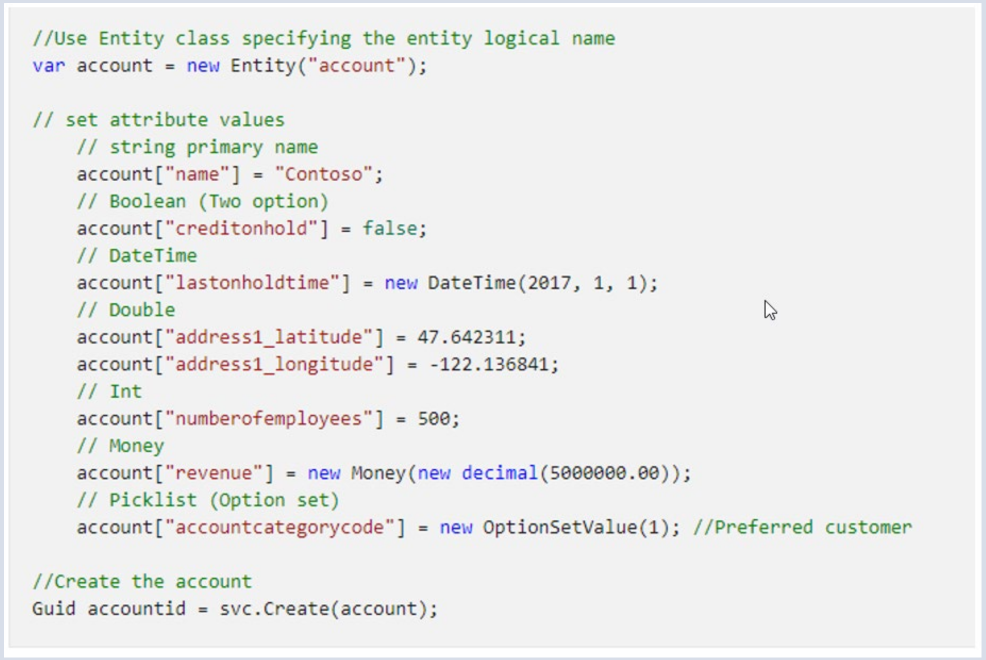
- `CrmServiceClient` aka. OrganizationService, using SOAP ==> SUPERSEDED!
  - The SDK, but only for .NET Framework
  - Still used in the sandbox

- `DataverseServiceClient` aka. OrganizationService
  - The SDK, for .NET Core and .NET 6+
  - The future 😉

ServiceClient SDK's

Late-bound Code

- No generated classes
- Runtime validation
- Limited Intellisense



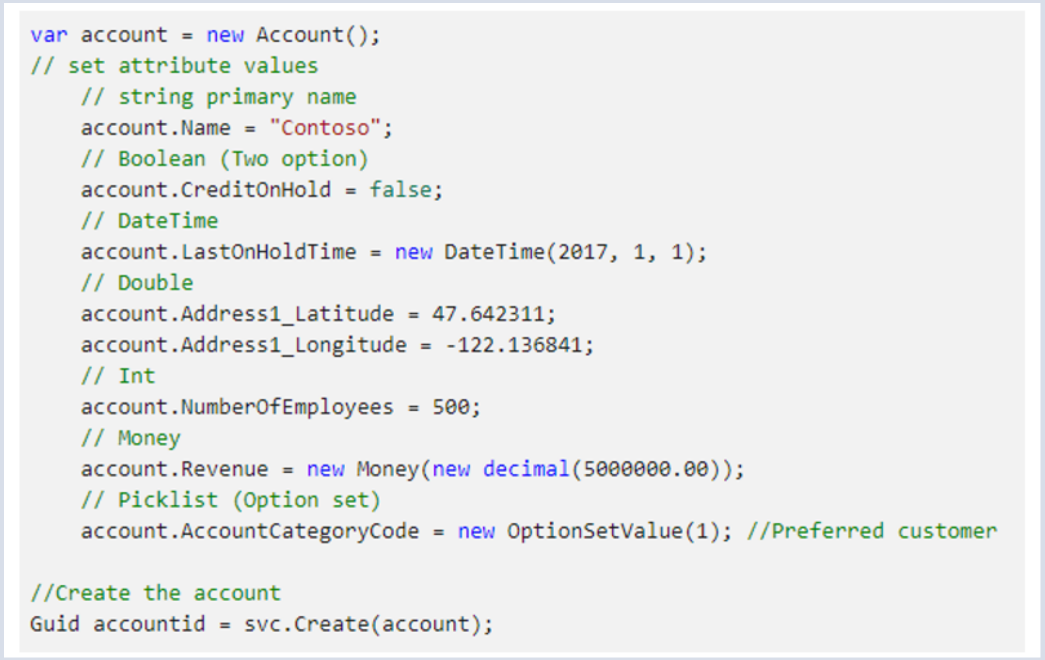
```
//Use Entity class specifying the entity logical name
var account = new Entity("account");

// set attribute values
    // string primary name
    account["name"] = "Contoso";
    // Boolean (Two option)
    account["creditonhold"] = false;
    // DateTime
    account["lastonholdtime"] = new DateTime(2017, 1, 1);
    // Double
    account["address1_latitude"] = 47.642311;
    account["address1_longitude"] = -122.136841;
    // Int
    account["numberofemployees"] = 500;
    // Money
    account["revenue"] = new Money(new decimal(5000000.00));
    // Picklist (Option set)
    account["accountcategorycode"] = new OptionSetValue(1); //Preferred customer

//Create the account
Guid accountid = svc.Create(account);
```

Early-bound Code

- Generated classes using tool
- Compile-time validation
- Supports Intellisense



```
var account = new Account();
// set attribute values
    // string primary name
    account.Name = "Contoso";
    // Boolean (Two option)
    account.CreditOnHold = false;
    // DateTime
    account.LastOnHoldTime = new DateTime(2017, 1, 1);
    // Double
    account.Address1_Latitude = 47.642311;
    account.Address1_Longitude = -122.136841;
    // Int
    account.NumberOfEmployees = 500;
    // Money
    account.Revenue = new Money(new decimal(5000000.00));
    // Picklist (Option set)
    account.AccountCategoryCode = new OptionSetValue(1); //Preferred customer

//Create the account
Guid accountid = svc.Create(account);
```

Helpful Tooling

For early-bound

- CrmSvcUtil.exe
- Early Bound Generator in XrmToolBox

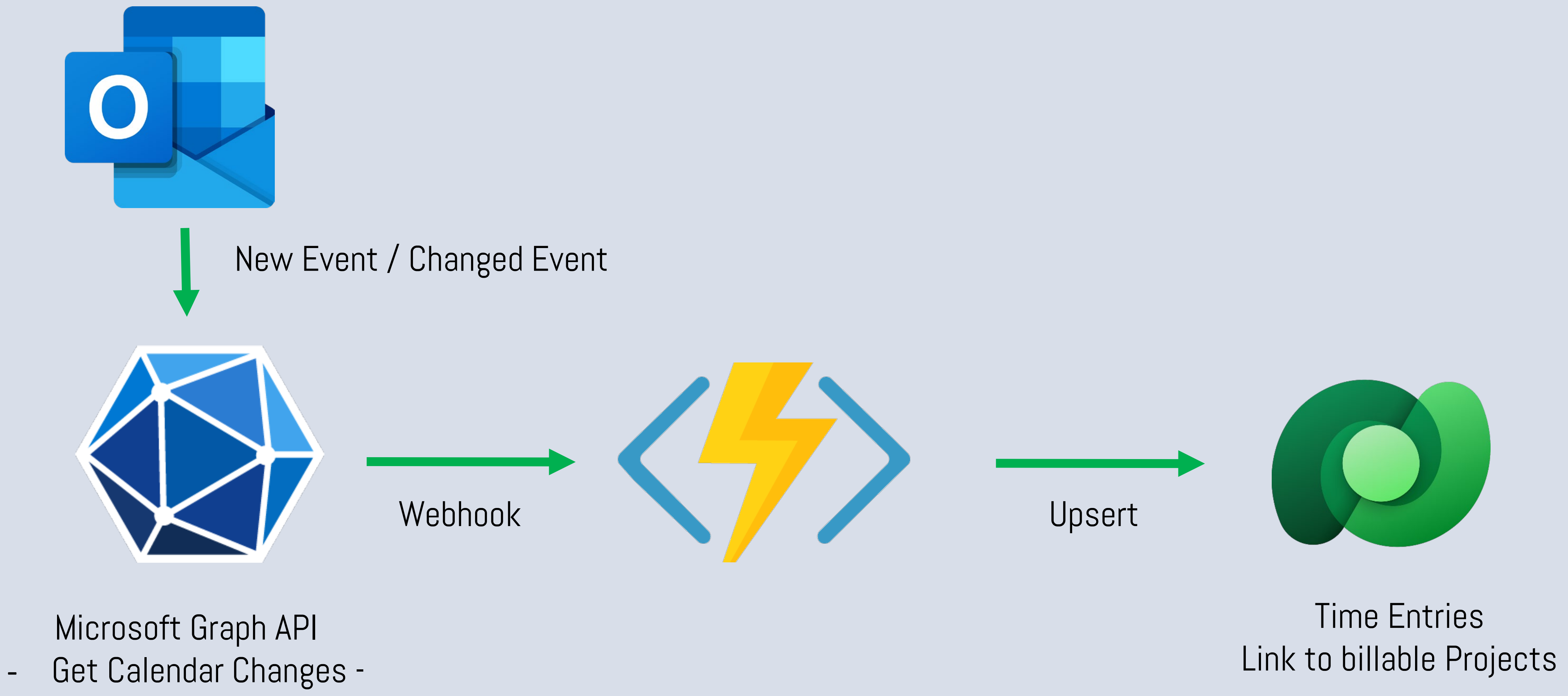
- pac modelbuilder
- Early Bound Generator v2 in XrmToolBox

For Dataverse queries

- FetchXML Builder
- Dataverse REST Builder

XrmToolBox
The ultimate set of tools for Microsoft Dataverse and Microsoft Dynamics 365
Empowering Business analysts, Developers, Administrators and Users since 2012

Use Case: "Everybody hates Time-Sheets"



pro-code Dataverse connectivity

authentication & authorization

SHOWTIME

Do the Do's!

- Delegated authentication for Users
- App-only: Managed Identity > Service Principals > Service Account
- Scoped privileges / Least privilege / Permission Concept
- Web API for OData access to Dataverse
- ServiceClient for .NET Core with Early-Bound code
- Use helper tools 👉 XrmToolBox

Use Dataverse & Power Platform ☺

nordic summit

Q&A

nordic summit

THANK YOU!