scieneers
DRIVEN BY DATA

Advanced security of PaaS based Azure data applications – from setup to ALM

Marco Fischer @ New Stars of Data

Hamburg, 14.08.2020

Marco Fischer

- Driven by data over 10 years

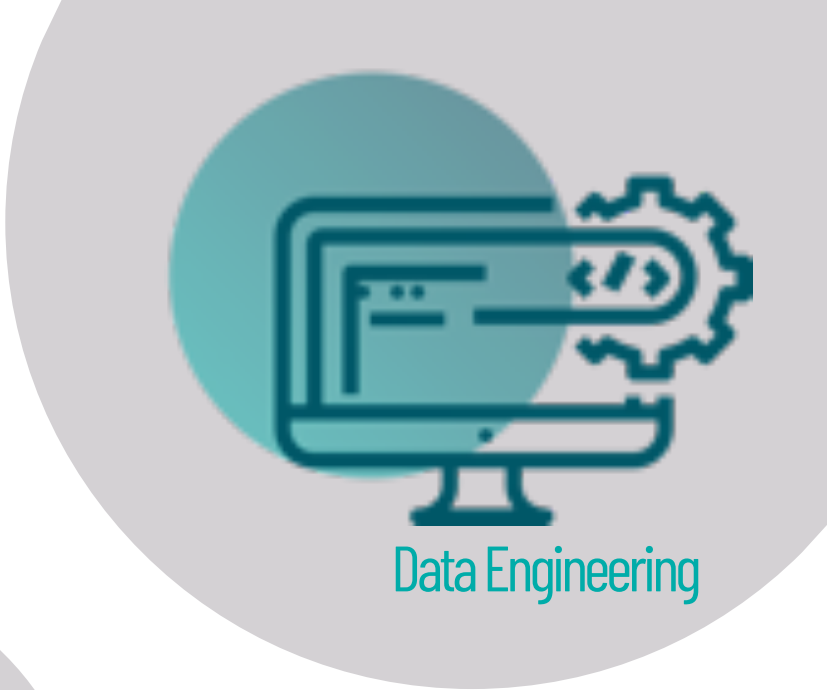
- Data Engineer
  - Microsoft BI stack
  - Databricks
  - SQL Server
- Azure Analytics with PaaS
- Azure Infrastructure

- Living in Hamburg, Germany
- Son of 3 years

scieneers – DRIVEN BY DATA

We gain insights into data & generate value out of it.
For our customers, in society and ourselves.

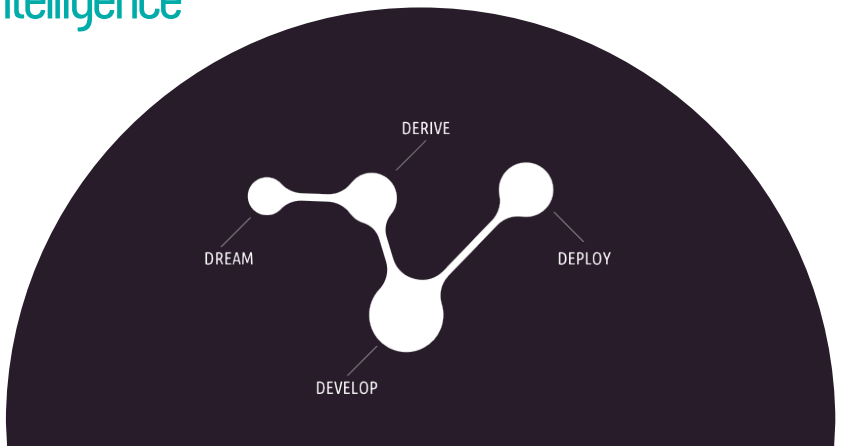
Business Intelligence



Data Engineering

Big Data

Artificial Intelligence



Data Science

Our locations

Karlsruhe

Cologne

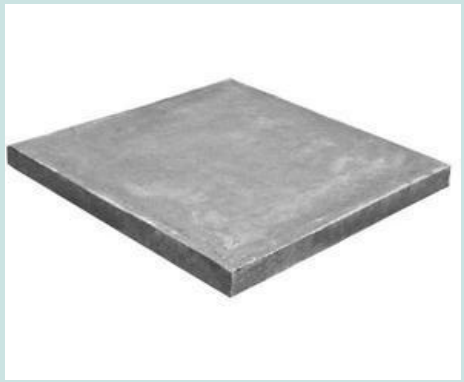
Hamburg

Cloud Service Models

IaaS

PaaS

SaaS



Cloud Service Models

IaaS

most flexible

intense in
- operation
- development

manage
- OS
- processes (e.g. DB)
- interfaces

PaaS

flexible

bunch of "black boxes"
- some parameters
- less components than IaaS

manage
- interfaces

SaaS

take it or leave it

one big „black box“ with an URL endpoint
- customizing if possible
- sometimes REST API available

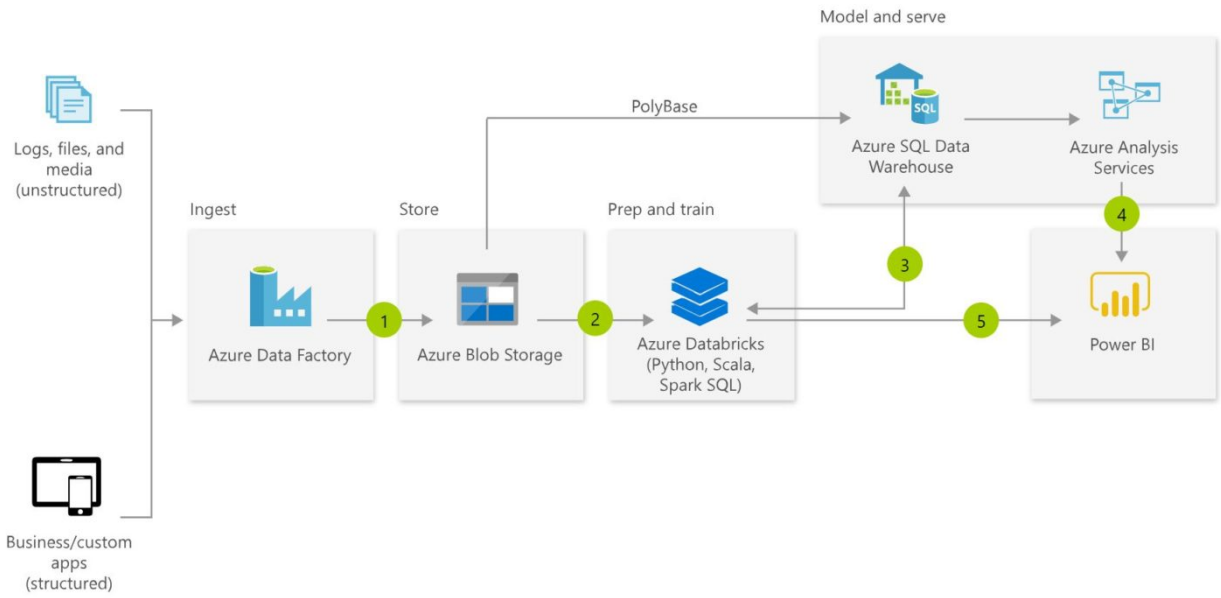
manage
- nothing

Benefits of PaaS Architecture

- „Puzzle pieces“ for every data requirement
- Short ramp up time for infrastructure
- Only connect services

→Faster creation of business value

Example



scieneers
DRIVEN BY DATA

WHY security?

Security Grade – lax attitude

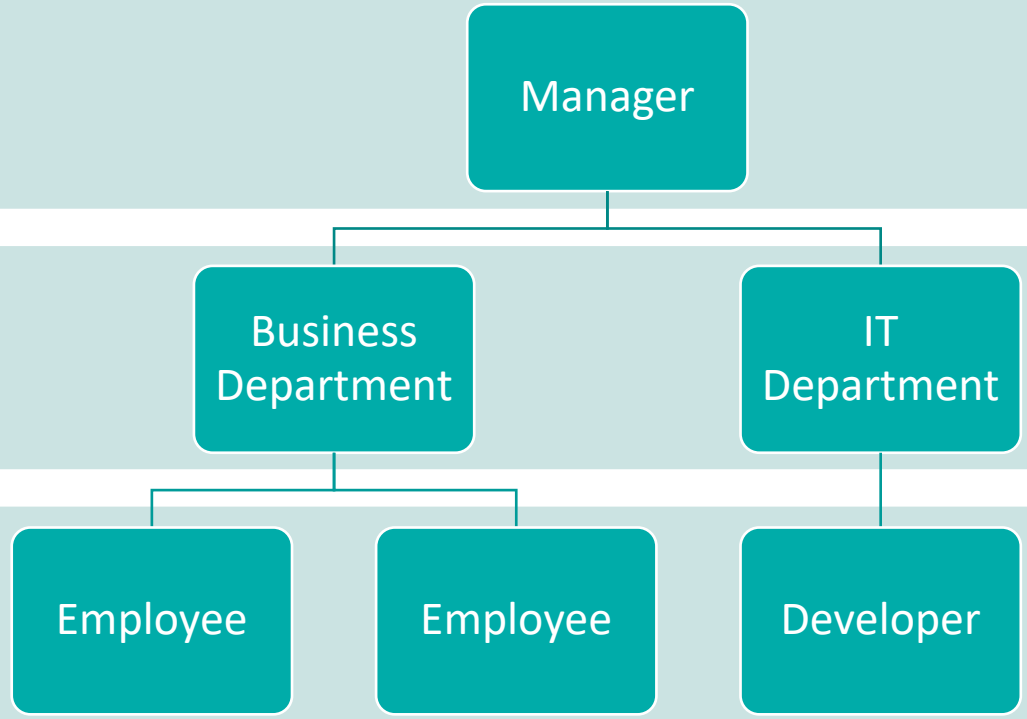
Fast results

+ no costs

Just deliver value

Business people don‘t ask for security.

→ IT guys „thank god they don‘t require security“



→ Vulnerable in any point in time

Security Grade – strict attitude

200 % secured

No time preassure

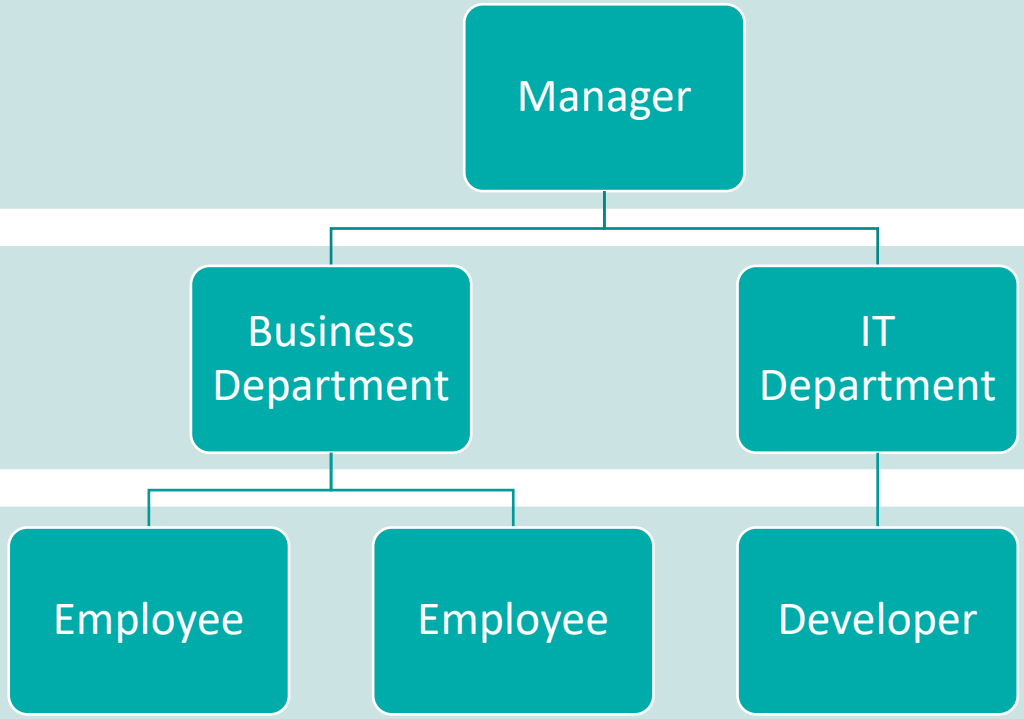
Thousands of policies e.g. long passwords

Rights splitt of 10 accounts per developer

Big corporation – responsibility splitting by departments – just create service requests

Developer implements security in Architecture

During development he makes his life as easy as possible



→ Vulnerable as people use workarounds

Security – Know the people

Role	Task	Compromise
Developer	passwords for data sources	Azure KeyVault entry (by IT)
Developer	Password for development access	One Person -> One digital identity (prefer 2FA
IT	Creation of tech. User/new environments	Simple and fast process No blockers for developers

Just a few examples

- People over processes (see SCRUM guide)
- Know the needs
  - Developers
  - IT Security Department
- Teams should speak
- Avoid “we” and “you”

→ be close by and available

Role of security for your business

- Self protection of your venture
  - Avoid legal dispute
  - Protect business secrets
- good reputation
  - Trust of
    - clients
    - business partners – whole supply chain
    - employees

→ your business don‘t want to be vulnerable at all

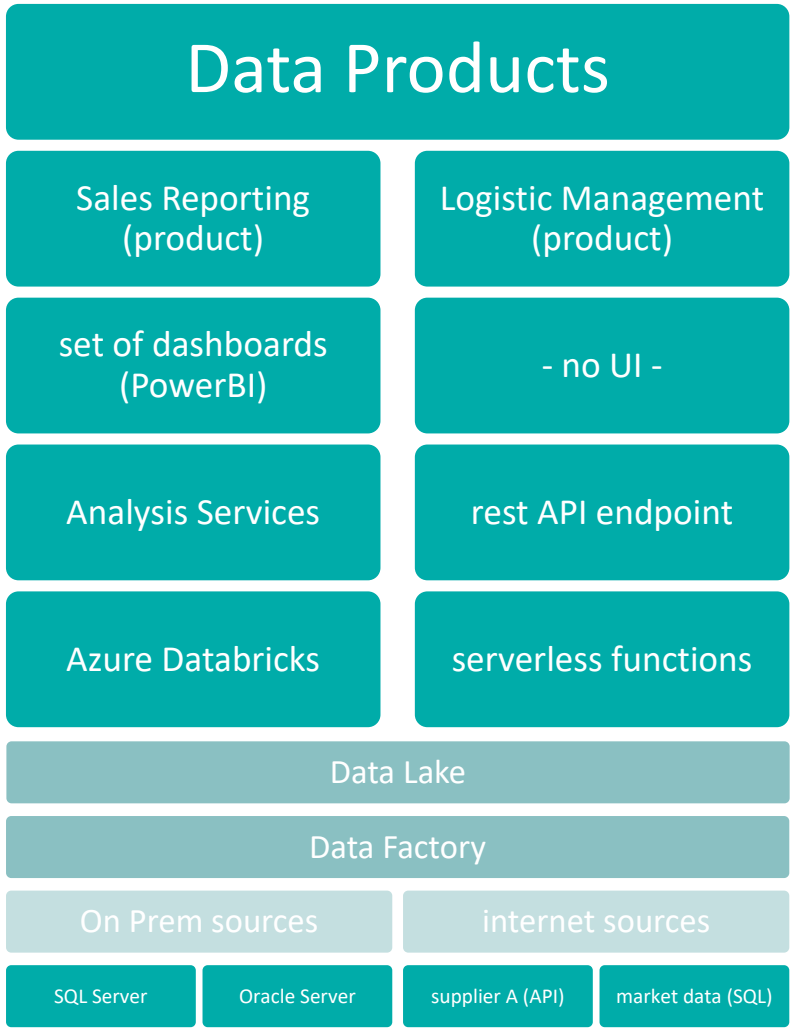
scieneers
DRIVEN BY DATA

Data Products

clear objective

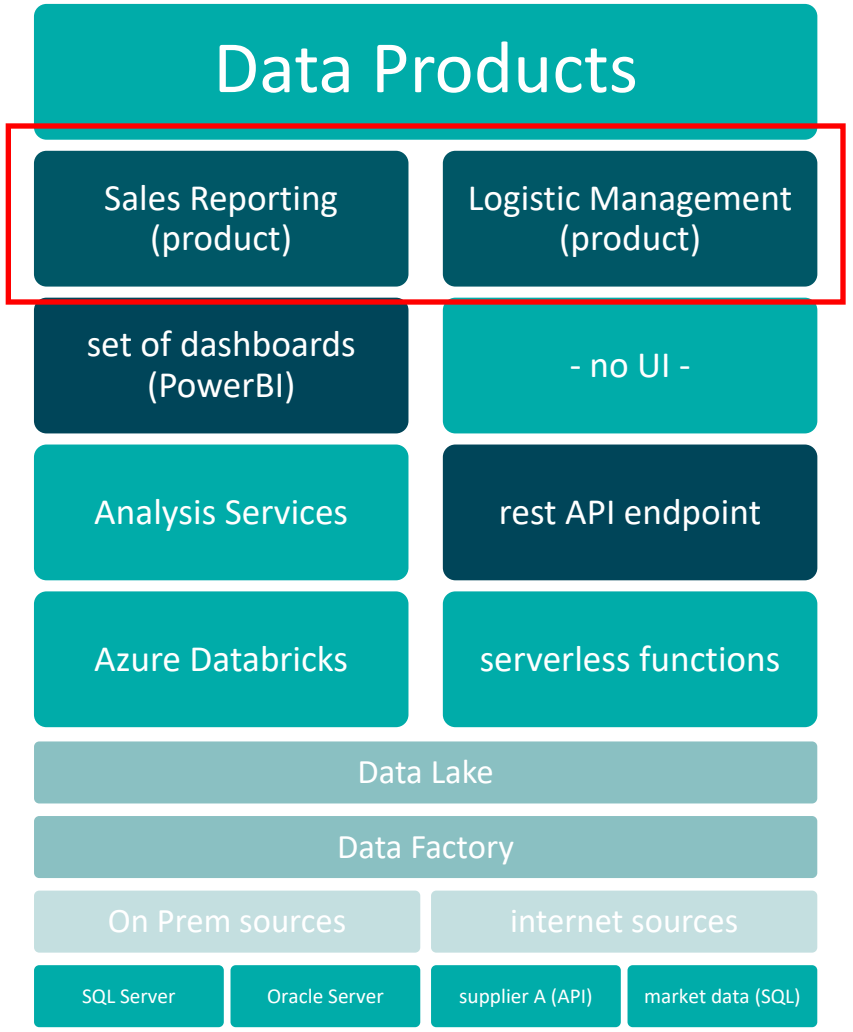
Data Product view

- Clear “big picture” for all stakeholders
- Makes large architectures understandable
- Improves risk assessment
- Enforce proper planning



Data Product - example

- Clear “big picture” for all stakeholders
- Makes large architectures understandable
- Improves risk assessment
- Enforce proper planning



Data Product - Lifecycle

- ✓ Life time? → adjust effort for security level and extendability
- ✓ how it should operated ?
  - ✓ skills available for operations team
  - ✓ time available for operations team
- ✓ Which network my consumers / suppliers use?
  - ✓Public internet?
  - ✓Corporate network?
- ✓ Disaster recovery time?

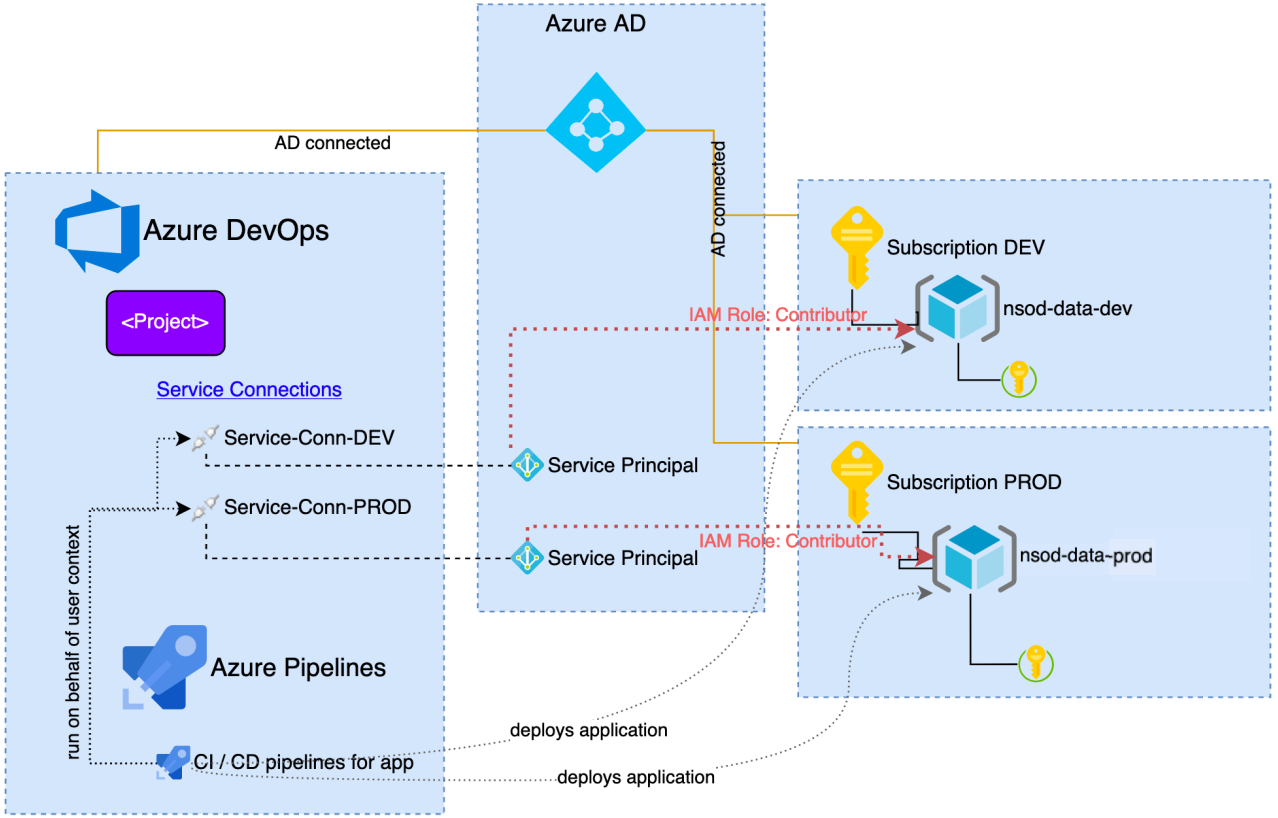
→This creates clarity about grade of security and automation

scieneers
DRIVEN BY DATA

Security Components in Azure

what's available

Azure Overview



- Azure AD [only one]
  - Subscription [1..n]
    - Resource Group [1..n]
      - Azure Resources itself - e.g. "Azure SQL Database"
        - Identity and Access Management (UI)
          - Role assignments (UI shows the ones for this resource)

Azure Active Directory – the one and only

- The “heart” of Azure Cloud
- A single Azure AD (AAD) per venture/cooperation
  - Provides access control of everything which is managed with it

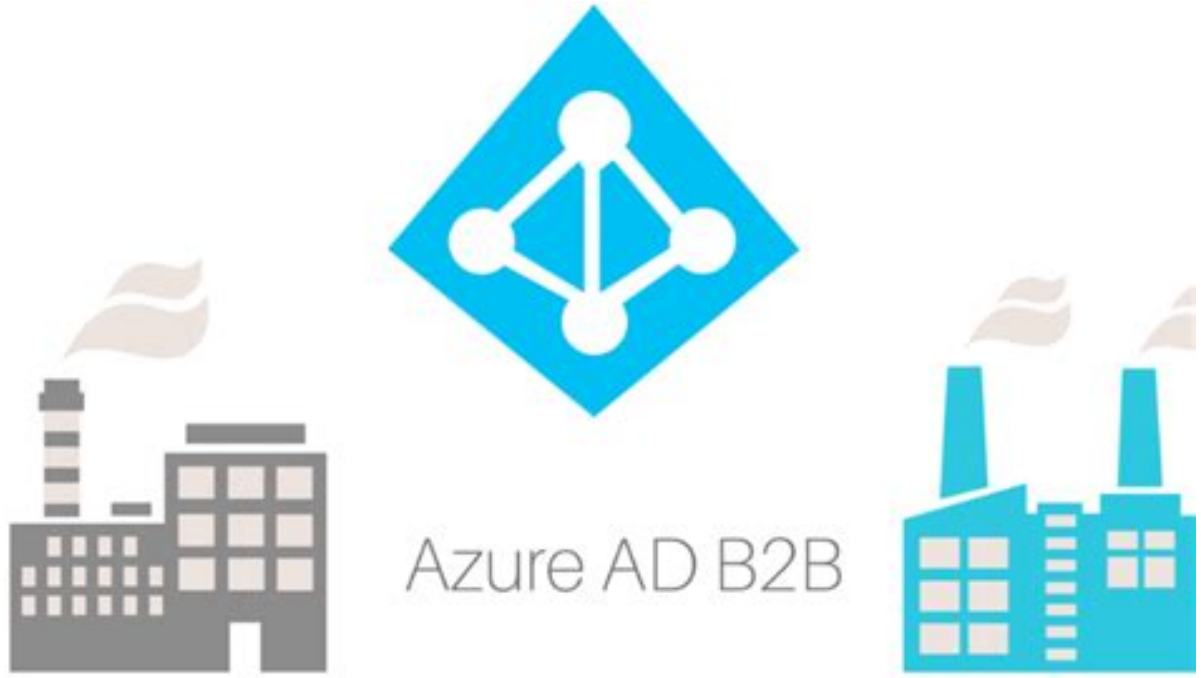
- Services
  - Store for
    - Roles (standard and user roles)
    - Identities
      - Groups (can be synced)
      - Users
      - Service Principals
        - Standalone
        - Application
        - Managed Identity

    - Role Memberships
      - Identity + Role + Scope

→ Unique service across the world (not located in special data center)

Azure Active Directory – Collaboration enablement

- Azure AD B2B
  - Invite guest users from other domains
  - People can
    - use their own identity
    - Authenticate against own authentication server



Guest authenticate against his / her Own AAD,
but selects our AAD
to browse for resources

Guest user gets new objectId in our AAD
→ We grant access

Azure Active Directory – Technical View

#	Identity Type	User Type	Technical Role assignment to	Azure Portal (UI) Displayed
1	User	Member	objectId	displayName
2	User	Guest	objectId (of our AAD)	displayName
3	Group	-	objectId	displayName
4	Service Principal	Techn.	objectId	AppId
5	Managed Identity	Techn.	objectId	AppId
6	Application	Techn.	objectId	AppId

Technical users – The glue of your data application

- Mandatory for service connections of our interfaces
- All types are "Service Principals" in the background
- Avoid passwords if possible
  - Take "Managed Identities" if available → they have no passwords
  - 2nd choice Service Principal with "certificate"
  - 3rd choice Service Principal with Password, but put it in KeyVault

Services for Security

- Azure KeyVault
  - Stores all your credentials, certificates in one save place
  - Use it by day one in development
  - Use it for deployment automation
  - Use it in all connections if possible → simlify your CI/CD setup

  → No passwords in code!

- Firewall
  - Each PaaS Services has it's firewall settings
    - → make use of them as you have public endpoints!

scieneers
DRIVEN BY DATA

Demo

let's check it out

scieneers
DRIVEN BY DATA

Thanks for your attention

Marco Fischer @ New Stars of Data