



FusionDev

How to securely work with Azure Functions, Managed Identity and Microsoft Graph

Luise Freese

About me

 Microsoft 365 Consultant and Developer

 Power Platform

 ProvisionGenie.com

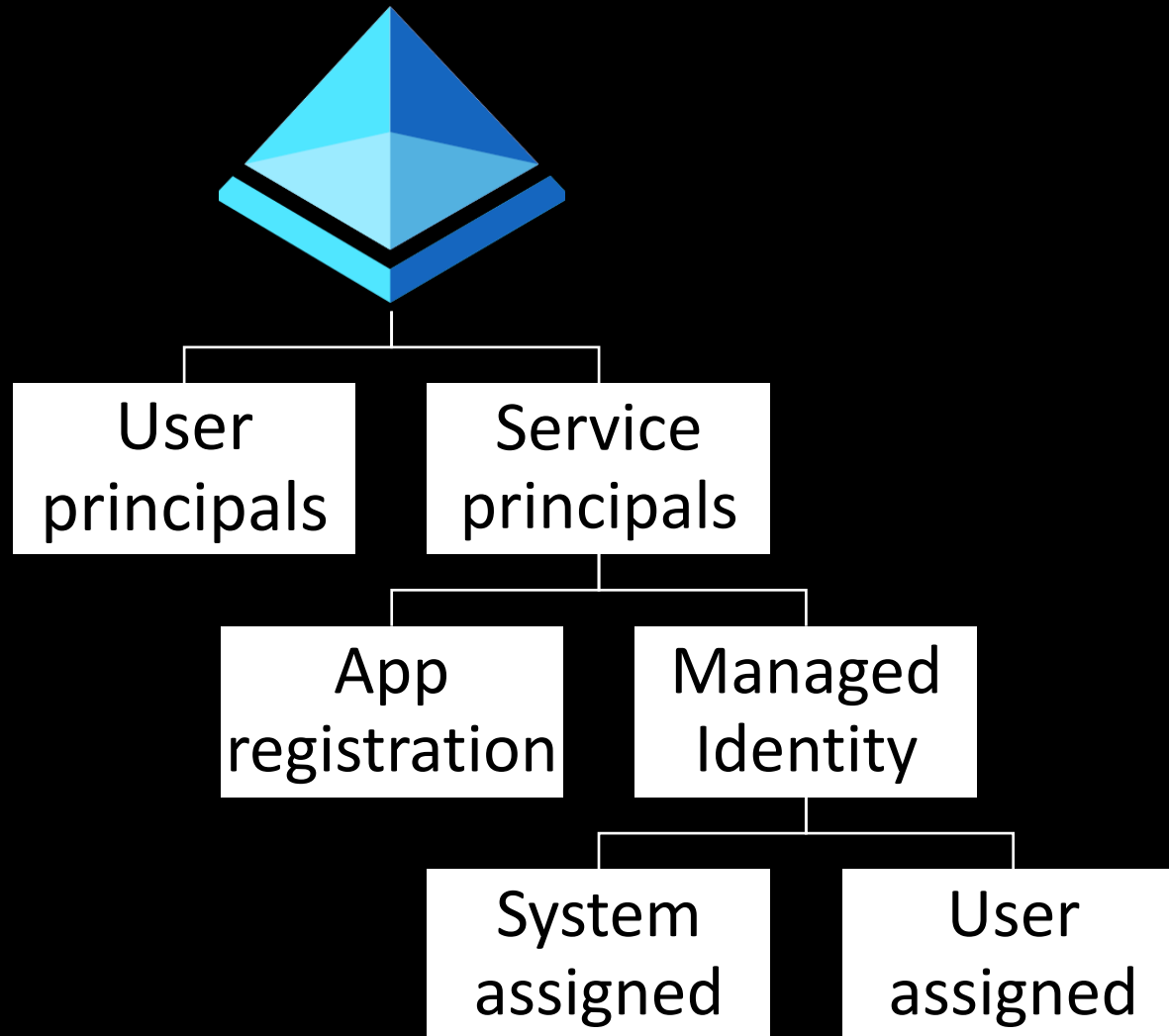
 PimpYourOwnDevice.com

 m365princess.com

Find me on twitter: @LuiseFreese



Service Principals and Managed Identity



Stop using service accounts aka fake-users

Administration

- Storing passwords is a challenge
- changing passwords in AAD and in every service/app that uses a service account is a tedious task
- Can lead to cascading system or process failures

Security

- Service accounts are used by several apps and then over-privileged
- Violates the rule of least privilege

Accountability

- Sharing credentials is never a good practice
- Only poor overview

Lifecycle

- Service accounts don't get deleted after installation/maintenance job

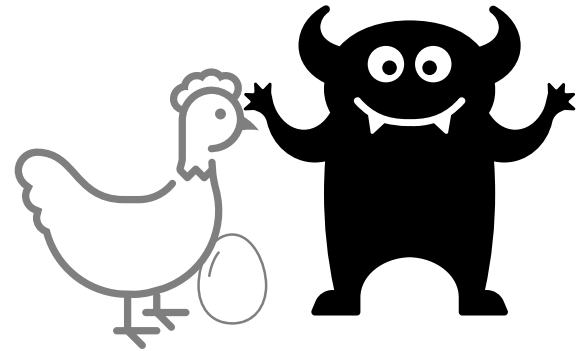
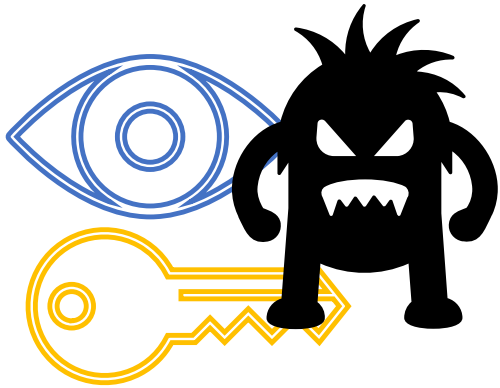


Azure Managed Identity Overview

- Managed identities give your apps an identity without an app registration in Azure AD
- No need to manage secrets or store credentials in your code
- No extra costs



Why Managed Identities are superior to secrets in a Key Vault



Managed identities

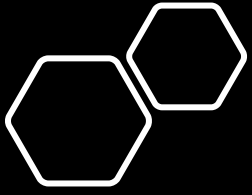


System assigned

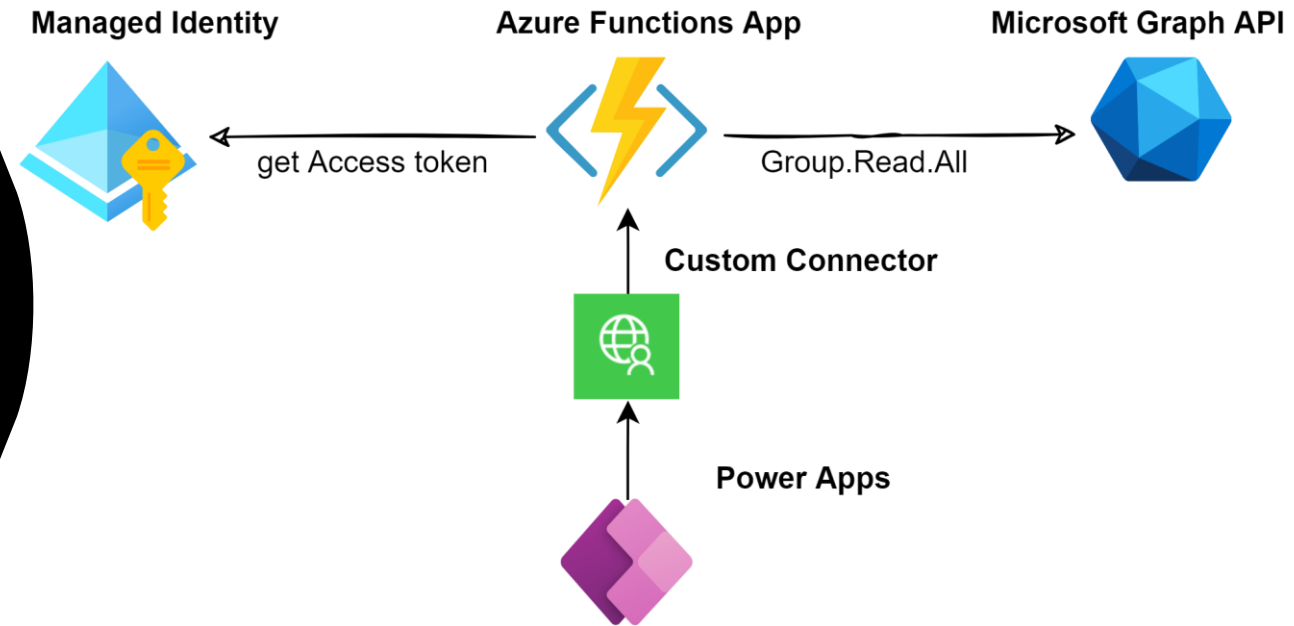
- Created as part of an Azure resource - like an Azure Function
- Life cycle equals the parent resource life cycle
- Can't be shared, but be associated with a single Azure resource.

User assigned

- Created as a stand-alone Azure resource
- Independent life cycle.
- Can be shared: The same user-assigned managed identity can be associated with more than one Azure resource.



Solution Overview



Microsoft Graph Explorer

The screenshot displays the Microsoft Graph Explorer web application. The interface includes a left sidebar with navigation options like 'Sample queries' and 'History', a main query editor, and a right panel showing the response preview.

Query Details:

- Method:** GET
- Version:** v1.0
- URL:** https://graph.microsoft.com/v1.0/groups
- Run query button:** Run query

Response Status: OK - 200 - 128ms

Response Preview (JSON):

```
{
  "@odata.context": "https://graph.microsoft.com/v1.0/$metadata#groups",
  "value": [
    {
      "id": "205b19e8-80df-4e8b-ba82-7d403aa2e658",
      "deletedDateTime": null,
      "classification": null,
      "createdDateTime": "2021-09-08T09:02:59Z",
      "creationOptions": [
        "ProvisionGroupHomepage",
        "HubSiteId:00000000-0000-0000-0000-000000000000"
      ],
      "description": "DreamTeam",
      "displayName": "DreamTeam",
      "expirationDateTime": null,
      "groupTypes": [
        "Unified"
      ],
      "isAssignableToRole": null,
      "mail": "DreamTeam@hsluise.onmicrosoft.com",
      "mailEnabled": true,
      "mailNickname": "DreamTeam",
      "membershipRule": null,
      "membershipRuleProcessingState": null,
      "onPremisesDomainName": null,
      "onPremisesLastSyncDateTime": null,
      "onPremisesNetBiosName": null,
      "onPremisesSamAccountName": null,
      "onPremisesSecurityIdentifier": null,
      "onPremisesSyncEnabled": null,
      "preferredDataLocation": null,
      "preferredLanguage": null,
      "proxyAddresses": [
        "SPO:SPO_c5787dca-45d6-47d7-992d-fdc6ee446a8d@SPO_b469e370-d6a6-45b5-928e-856ae0307a6d",
        "SMTP:DreamTeam@hsluise.onmicrosoft.com"
      ],
      "renewedDateTime": "2021-09-08T09:02:59Z",
      "resourceBehaviorOptions": [],
      "resourceProvisioningOptions": [],
      "securityEnabled": false,
      "securityIdentifier": "S-1-12-1-542841320-1317765343-1081934522-1357292090",
      "theme": null,
      "visibility": "Public",
      "onPremisesProvisioningErrors": []
    }
  ]
}
```



Demo time

- Create the Function locally
- Create Azure resources
- Assign permissions to MI
- Deploy to Azure



Developers

CAN YOU JUST
LET ME CODE?



ENDLESS EDITS
FOR MINOR UI
CHANGES 🤯

EVERYTHING
THEY DO WE CAN
DO BETTER 🧐

YET ANOTHER
MEETING 🙄


Makers

I NEED A SAFE
SPACE TO TRY
OUT THINGS

I NEED HELP TO
GET THIS APP
OUT!

I WISH
SOMEONE
COULD SHOW ME
SOME TRICKS

THERE SEEM TO BE NO
RULES AT ALL - DON'T
KNOW IF THIS IS GOOD
OR BAD?!



FusionDev – what is it & why would I want it?

Pro Devs

- Environment strategy
- Application Lifecycle Management
- Integrations like Custom connectors

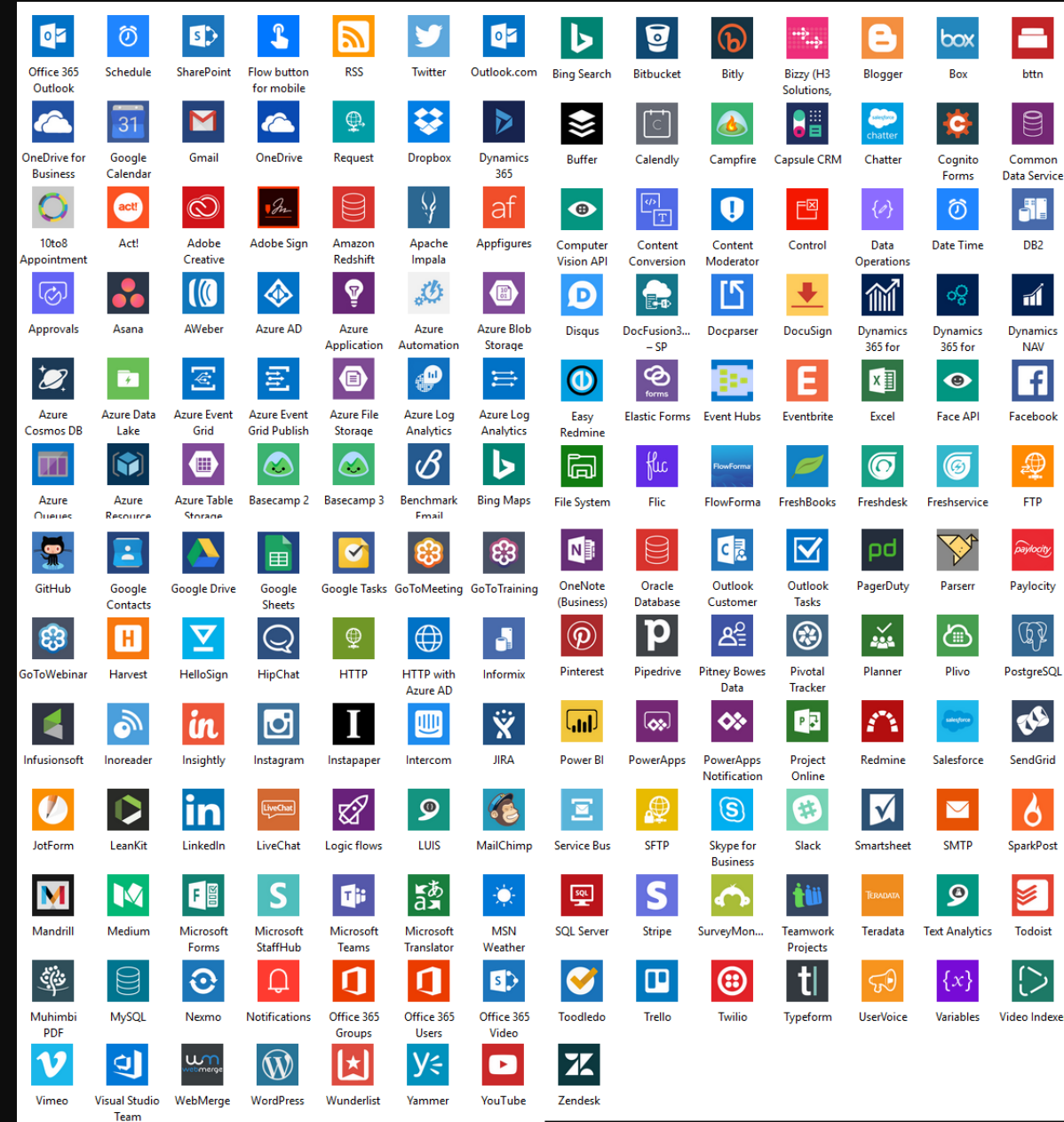
Makers

- Know business requirements
- Outline their processes
- Create UI/UX



Custom Connector

- A wrapper around a REST API that allows
 - Logic Apps
 - Power Automate
 - Power Appsto communicate with that REST API
- Can be secured via also
 - OAuth 2.0 for specific services incl. Azure Active Directory
 - API key
- Needs to be described in
 - an OpenAPI definition
 - a Postman collection
 - or created via make.powerapps.com



Power Platform Custom Connector

demo



Custom Connector

Connector Name: GraphGetGroups

1. General > 2. Security > 3. Definition > 4. Code (Preview) > 5. Test

Swagger Editor Update connector Close

Actions (1)
Actions determine the operations that users can perform. Actions can be used to read, create, update or delete resources in the underlying connector.
GetGroups
New action

References (0)
References are reusable parameters used by both actions and triggers.

Policies (0)
Policies are used to change the behavior of actions and triggers through configuration. You can use one or more policies from a set of predefined templates.
New policy

General
Summary Learn more
GetGroups
Description Learn more
GetGroups
Operation ID *
This is the unique string used to identify the operation.
GetGroups
Visibility Learn more
none advanced internal important

Request
Web *
Method *
GET
URL *
This is the request URL.
https://huseidemo-functionsapp489.azurewebsites.net/api/GetGroups

define

Connector Name: GraphGetGroups

1. General > 2. Security > 3. Definition > 4. Code (Preview) > 5. Test

Swagger Editor Update connector Close

Security
Choose the authentication type and fill in the required fields to set the security for your custom connector. Learn more

Authentication type
Choose what authentication is implemented by your API *
API Key
Edit

API Key
Users will be required to provide the API Key when creating a connection
Parameter label *
API Key
Parameter name *
code
Parameter location *
Query
Edit

General secure Definition

Connector Name: GraphGetGroups

Details Share

Share with
Adding another people allows them to edit, update, delete, and access the details of this custom connector.

Add people
Enter names, emails, or user groups

hscluse Share with org

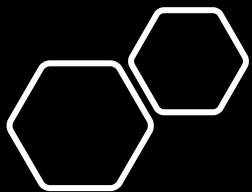
Currently shared with ...

Adele Vance
AdeleV@hscuse.onmicrosoft.com Can view

Luisa Freese
luisa@hscuse.onmicrosoft.com Can view Can view share Can edit

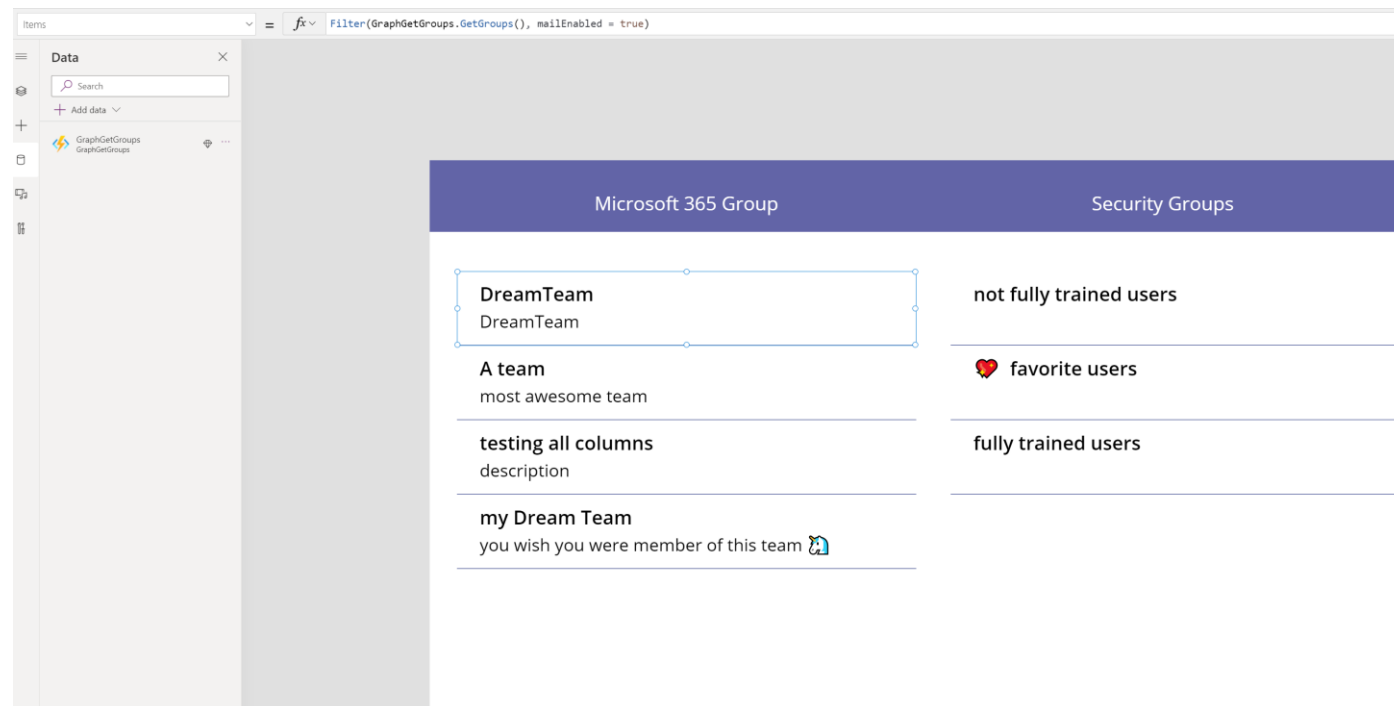
Save Discard

share



Maker experience in Power Apps

- Add connector
- Create UI as you wish





thank you



questions?



TWITTER HANDLE



BLOG URL