



CLOUD IDENTITY SUMMIT '22

Identity Management Track

**Using Logic Apps to automate tasks in
your AAD - and secure your Logic Apps**
Christopher Brumm glueckkanja-gab

Community Event by



BONN



Hi I'm Chris!

Living in Hamburg, Germany
Consultant & Architect
Identity & Security enthusiast

Follow me on Twitter



@cbrhh



Agenda

- Why Logic Apps and some Use Cases?
- Some good practices
- Connections from a Logic App
- Connection to a Logic App

Some use cases from the last months

Scheduled

Config and Asset Management

- Set Password Policies for Service Accounts
- Maintain dynamic groups based on Authentication methods

Reporting and Alerting

- Write Authentication Methods for specific groups to a custom Log Analytics table.
- Fetch 3rd Party app data from MDCA

Triggered

Security

- Block a specific user.

Deployment

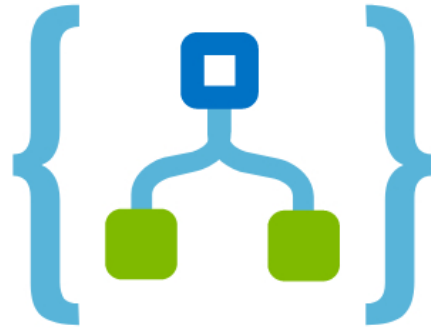
- Create and configure Enterprise Apps to integrate AWS Accounts via SAML

APIs

MS Graph

MDCA API

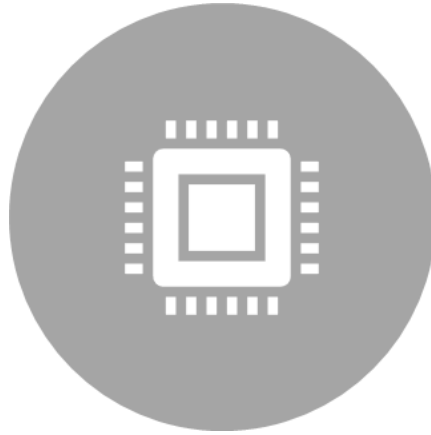
Choosing a platform



Logic App concept



TRIGGER



LOGIC



API



DEMO

A simple Logic App

If you work with MS Graph...

Determine needed permissions

- with the Permission Reference in MS Docs and Graph Explorer
- document the reasoning for the needed permissions

Only one Managed Identity can be bound to a Logic App.

- Note that the tokens are cached for up to 24hours
- For dev/testing you can work with User Assigned
- For prod you should use System Assigned (portability, transparency)

! Enabling system assigned managed identity

ManagedIdentityLimitPerFlowExceeded: The workflow 'LogicApp05' can only have one managed identity. Remove the user-assigned managed identity before enabling the system-assigned managed identity.

Use PowerShell to manage the permission of the Managed Identities

If you work with credentials...

Use Case:
Fetch 3rd Party app
data from MDCA



**HIDE INPUTS AND
OUTPUTS**



USE A KEY VAULT



**USE MANAGED
IDENTITIES**



**RESTRICT READ
ACCESS TO THE
LOGIC APP**

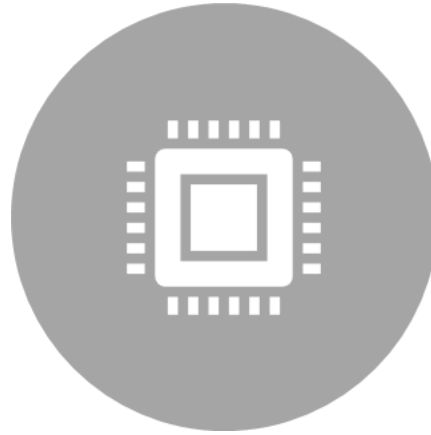
Next Level...



Logic App concept



TRIGGER



LOGIC



API



DEMO

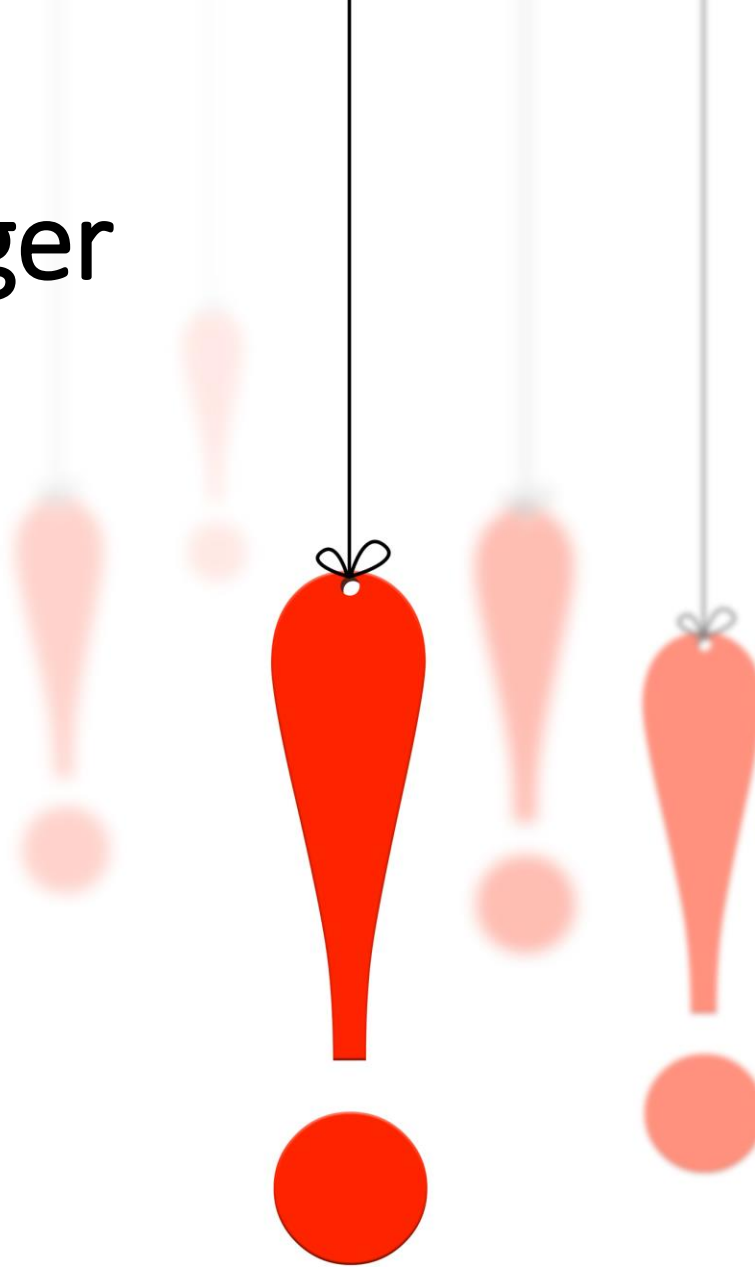
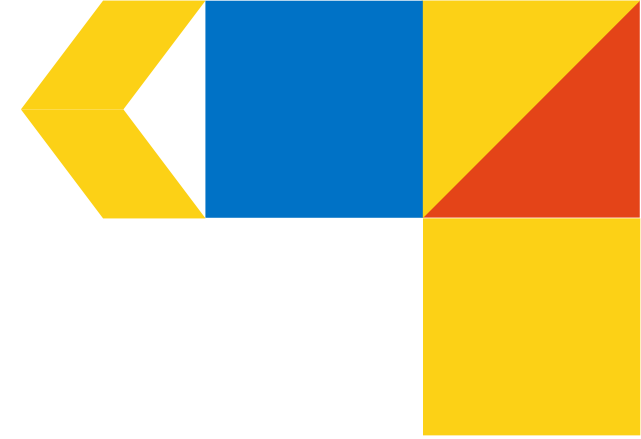
Triggering a Logic
App

Securing the trigger

Input validation

Firewalling

Authentication
and authorization
of clients



Next Level...



To Do List


1. Create Apps for the HTTP Trigger and the Client
2. Create and assign permissions for the trigger
3. Enable Oauth and check Permissions at the Logic App
4. Enhance the security with Conditional Access and the Packet Filter of the Logic App





If you work with App Registrations...


- Use the integration assistant!
- Know the difference between
 - API permissions and app roles
 - a redirect URI and an app ID URI
 - V1 and V2 endpoints


Manage

 Branding & properties

 Authentication


 Certificates & secrets


 Token configuration


 API permissions

 Expose an API

 App roles

 Owners

 Roles and administrators | Preview

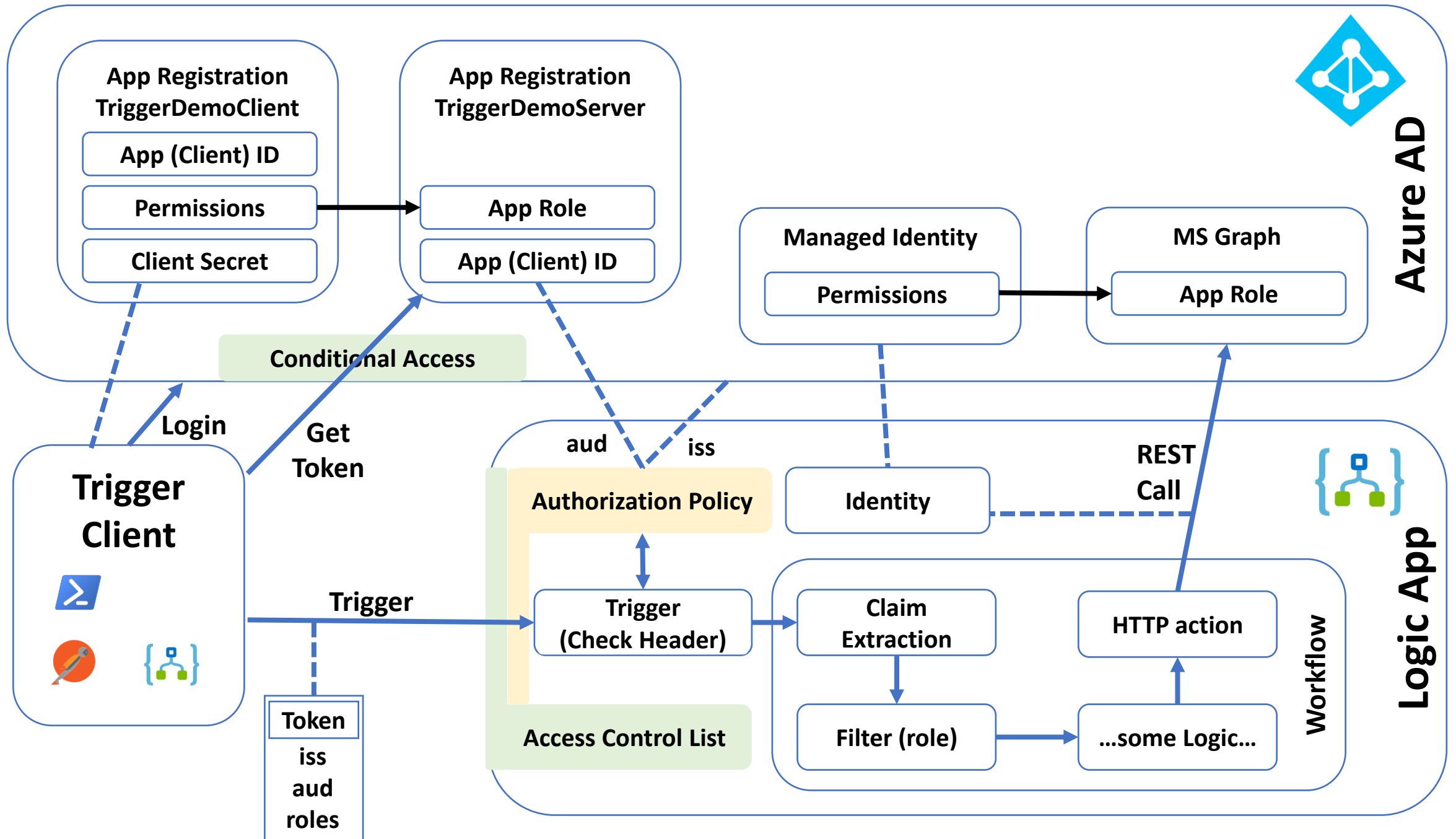
 Manifest





DEMO

Securing the trigger



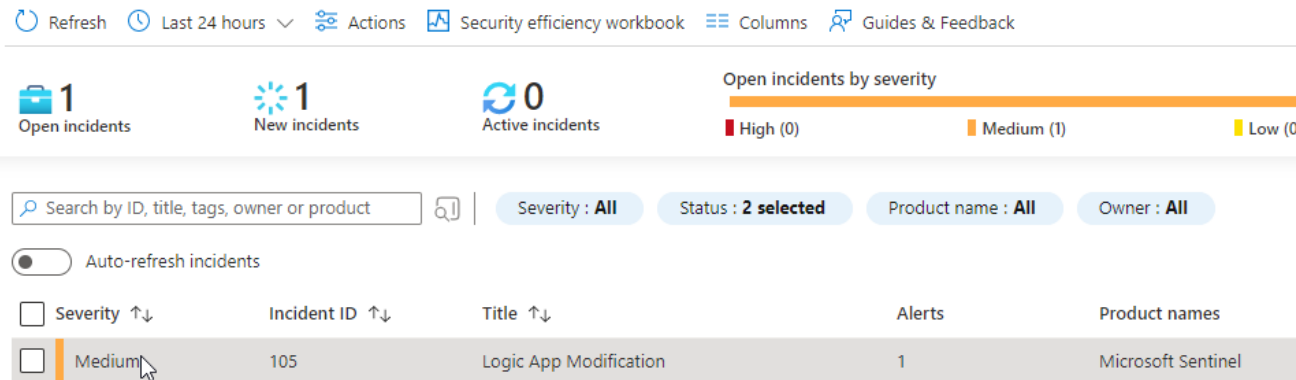
Date :

To Do List

1. Start with using Consumption Based Logic Apps
2. Use least privilege for your Logic App
3. Restrict the Access to your Logic Apps
4. Monitor your Logic Apps



One last thing...



If you're automating stuff in AAD you might have high permissions...

- Send your Activity Logs to Microsoft Sentinel and monitor modifications.



If you're automating stuff in AAD you want to rely on success...

- Send your Diagnostic Logs to Azure Monitor and monitor failed runs



CLOUD IDENTITY SUMMIT '22

Thanks to our sponsors!



glueckkanja  gab

yubico



CLOUD IDENTITY SUMMIT '22

Thu, September 22nd, 2022

Ask Me Anything (AMA)

Roundtable discussion and Q&A
on experiences from the field and current trends!

Meet the speakers and exchange with members of the community!

Community Event by



BONN

Follow us on Twitter



@identitysummit



CLOUD IDENTITY SUMMIT '22

Your Feedback is Important!

<https://www.identitysummit.cloud/feedback/>

Community Event by



Follow us on Twitter



@identitysummit