



EntraOps: Deploying and Managing Conditional Access at Scale

Thomas Naunheim



resco



PROMISE
GRUPA APN PROMISE

502nm

ANW



EUROPEAN CLOUD SUMMIT

cloudtechtallinn.com

GOLD



Sparkle



NORDIC KOOLITUS



FORCEWORKS



GLOBAL



QUBIX



Digital



CRM

netspore

DYNAMICS
MINDS



ColorCloud
HAMBURG

#CTTT24

CTTT



Thomas Naunheim

Cyber Security Architect @glueckkanja AG

Focus on Identity + Security in Microsoft Azure and Microsoft Entra
Community Speaker, Blogger and Podcast (Cloud Inspires)
Co-Organizer Azure Meetup Bonn and Cloud Identity Summit
Live in Lahnstein/Koblenz, Germany



thomas@naunheim.net



cloud-architekt.net



[@Thomas_Live](https://twitter.com/Thomas_Live)



[/in/ThomasNaunheim](https://www.linkedin.com/in/ThomasNaunheim)

Agenda

- Conditional Access and Microsoft Graph
- Introduction of “EntraOps” PoC Project
- Coding and CI/CD of CA Templates
- Management of Deployed CA Policies



Conditional Access and Microsoft Graph

Conditional Access and Microsoft Graph

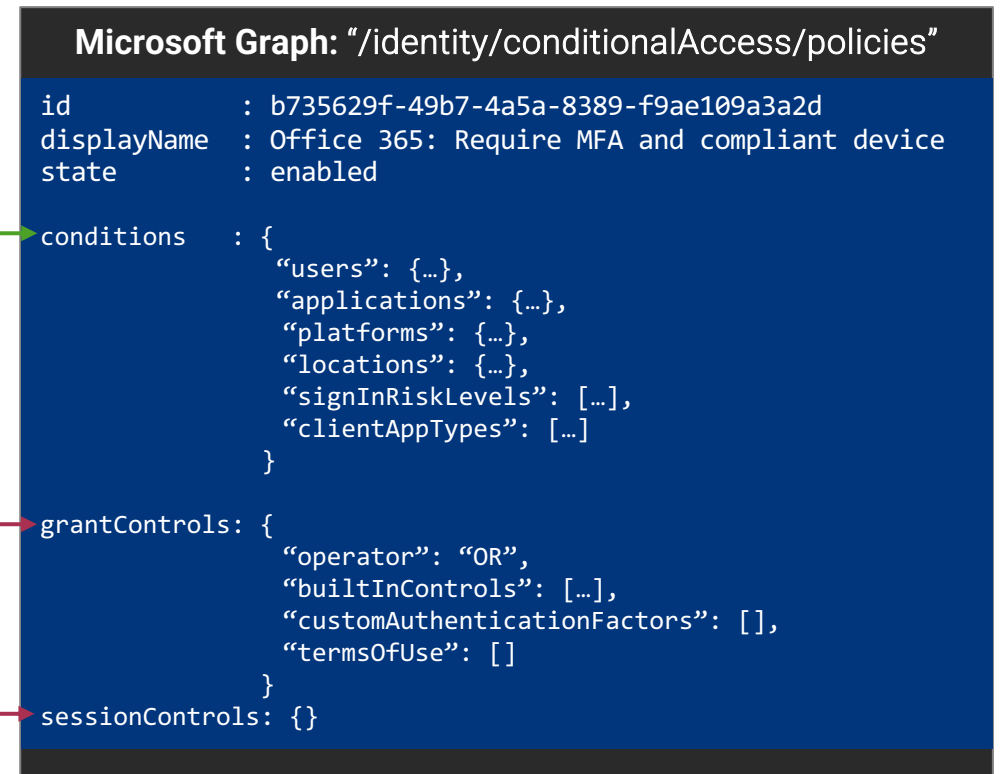
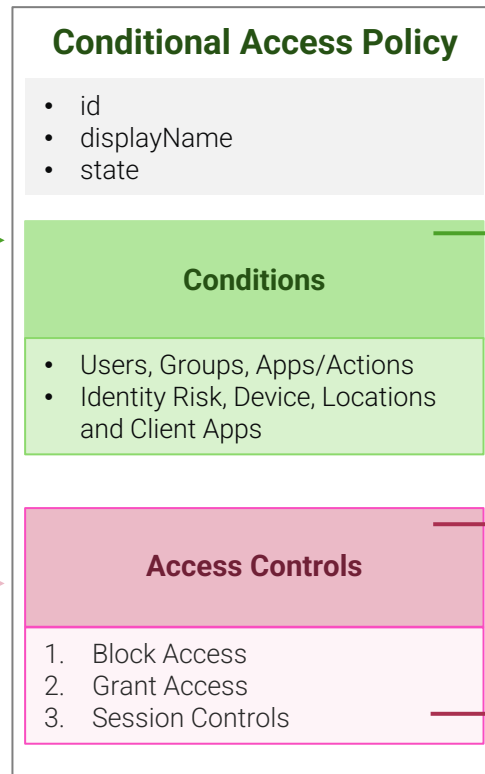
Overview of Conditional Access Policies

When this happens...

A user from (group) “Marketing employees” is accessing “Office 365” from a browser on a Windows device from any location and no sign-in risk was detected.

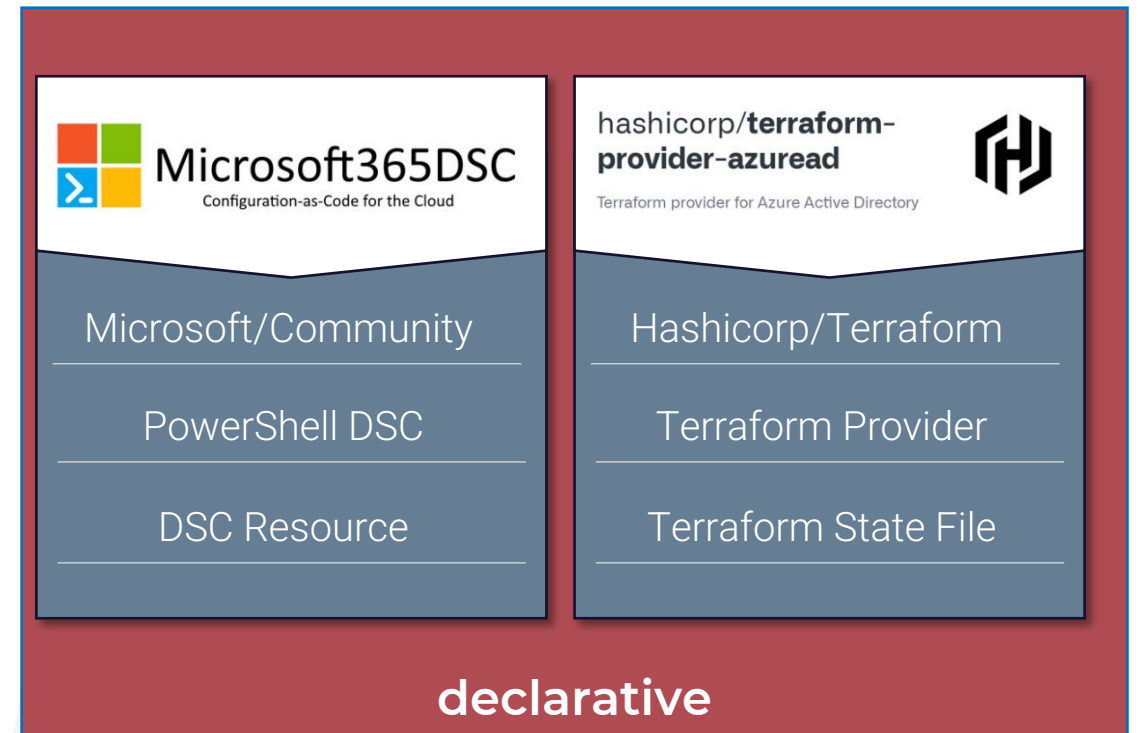
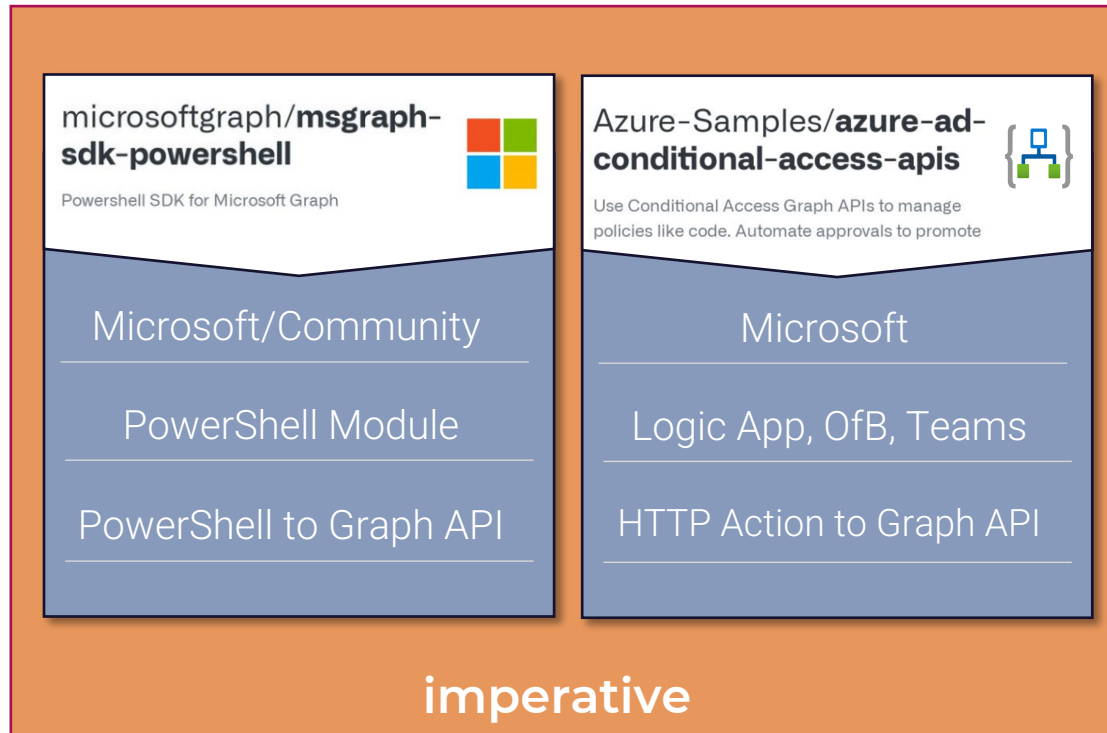
...then do this!

Require a user with strong (multi-factor) authentication and device to be marked as compliant. No session control (CA App Control policies or limited sign-in frequency).



Conditional Access and Microsoft Graph

Configuration As Code



DEMO

Microsoft Graph and Conditional Access Management

Conditional Access and Microsoft Graph

Scripts and Templates

DanielChronlund/
DCToolbox




Tools for Microsoft cloud fans

Daniel Chronlund

Templates, Report

PowerShell

AlexFilipin/
ConditionalAccess




Alex Filipin

Scripts, Templates

PowerShell

Fortigi/
ConditionalAccess



Fortigi

Scripts, GUID Convert

PowerShell



Introduction of “EntraOps” Project

Introduction of “EntraOps” Project

Benefits of DevOps Lifecycle for Microsoft Entra Conditional Access



Change Management

- Documentation of policy requirements and changes
- Planning, **versioning** (incl. backup/restore) and tracking policy changes
- Integration of “Quality Gates” and “Approval Workflows”



Ring- / Multi-Tenant (Staged) Deploy

- Deploy policy configuration across various target groups or tenants
- Using templates for **standardized policy sets**
- **Reduced roll-out risks** by automated and staged deployment
- Reduced costs by automated deployment (**Managed Service Provider**)

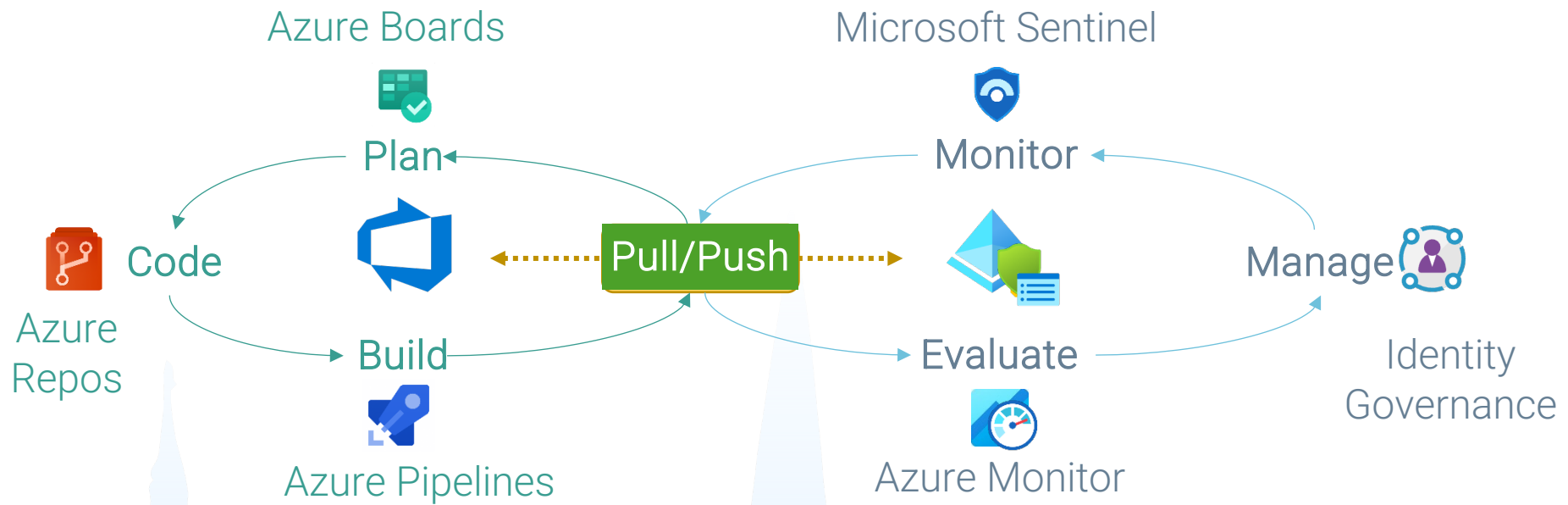


Policy-As-Code and Governance

- **Reduced role assignments** to “Conditional Access Administrator”
- **Comparison and “full visibility”** of deployed policies (incl. Device Compliance)
- Roll-out of **contingency plan** and **resilient access controls** (in case of MFA disruption or emergency access)

Introduction of “EntraOps” Project

DevOps Lifecycle for Microsoft Entra Conditional Access

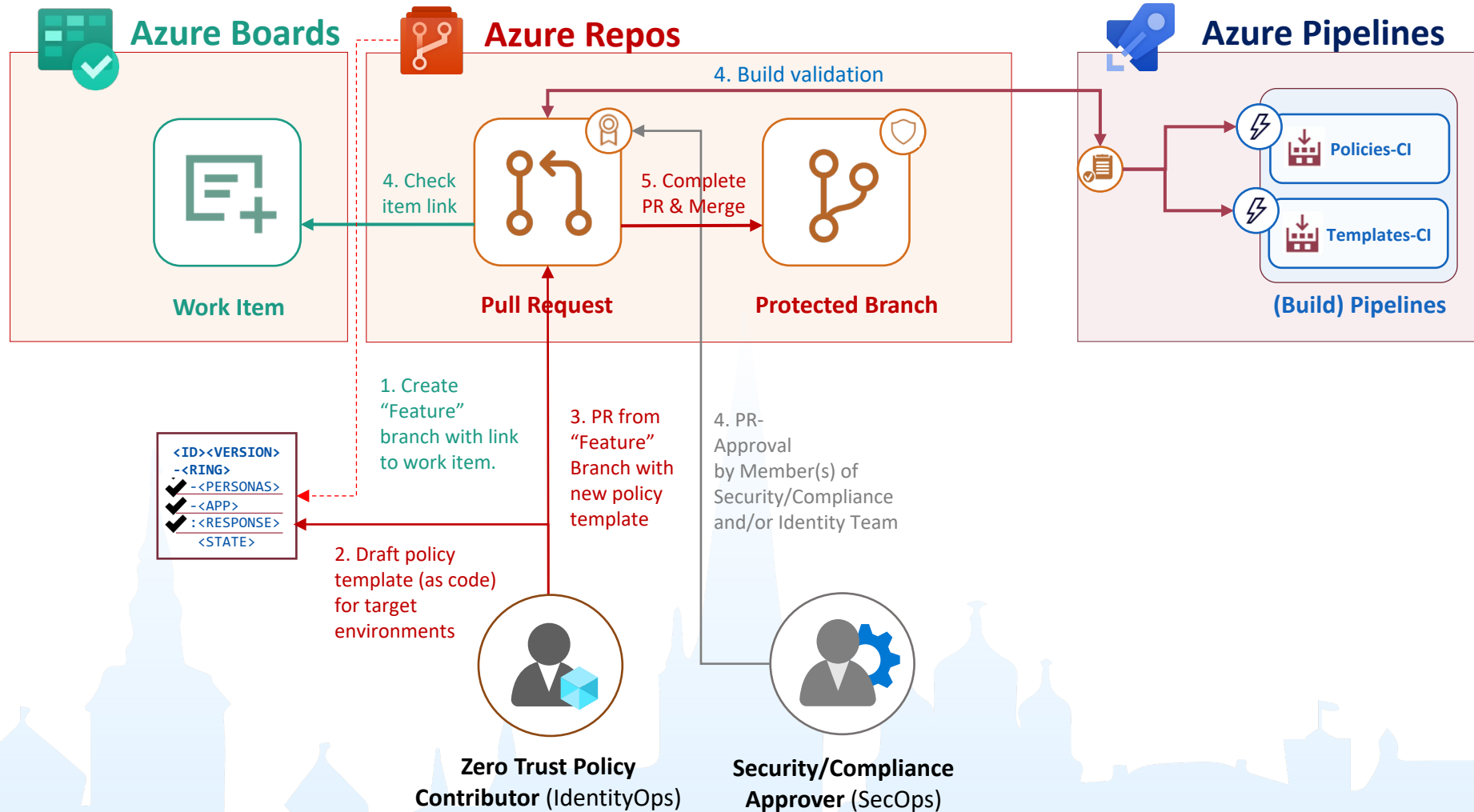




Coding and CI/CD of CA templates

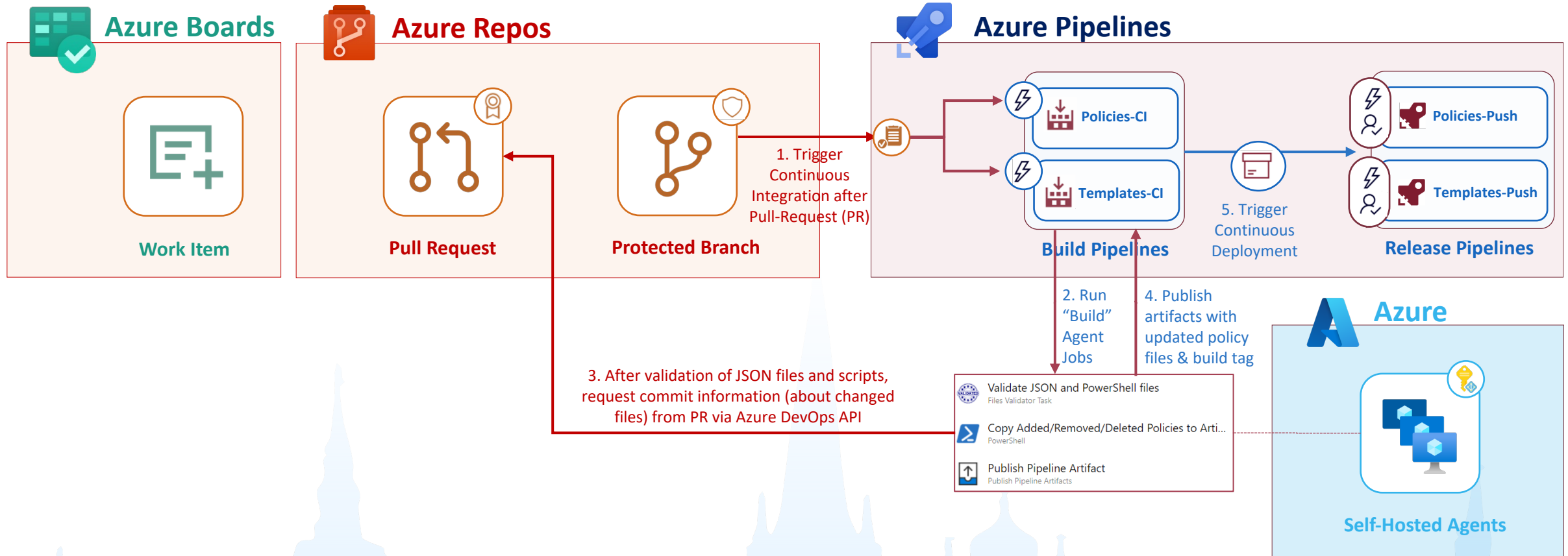
Introduction of “EntraOps” Project

Planning & Coding



Introduction of “EntraOps” Project

Build Process

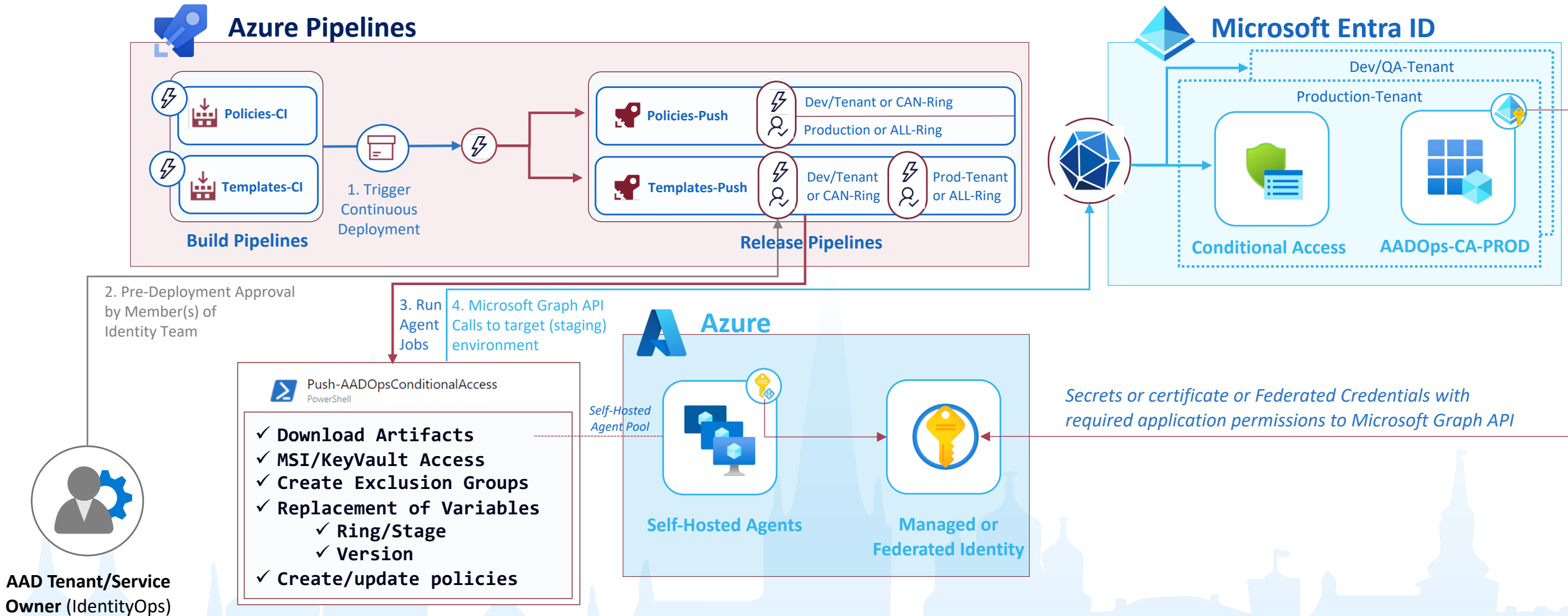


DEMO

Pull and Templating of Conditional Access Policies

Introduction of “EntraOps” Project

Deployment and Release



DEMO

Continuous Integration/Deployment and Staging of CA Templates



Management of deployed CA Policies

Management of deployed CA Policies

Exclusion Management of Conditional Access Policies

General approach:

- Exclusion by (Cloud-only) Security Group
- Review of Excluded Groups (Entra ID Governance access reviews)
- Protection of Exclusion Group (e.g. modified by Group or Intune Admins)

Include **Exclude**

Select the users and groups to exempt from the policy

☐ All guest and external users ⓘ

☐ Directory roles ⓘ

☒ Users and groups

Select excluded users

3 groups

- SU** sug_AAD.CA.Exclusion.304.CAN ...
- SU** sug_AAD.CA.Exclusion.Emerge...
- SU** sug_AAD.CA.Exclusion.Synchr...

Use Case A: Individual or wide scoped

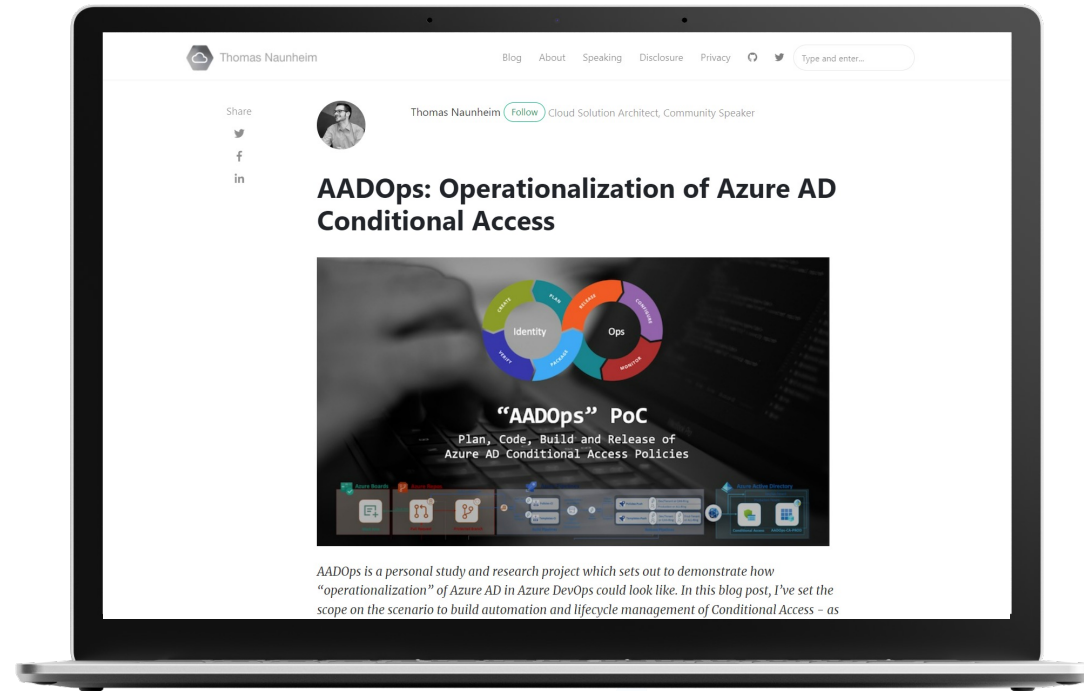
- Temporary or limited Exclusion
- Exclusion for each policy (or group of policies)
- Exclusion after approval process, assignment as Access Package

Use Case B: Break Glass or Sync Account

- Permanent Exclusion
- Assignment to certain account type, strictly monitored

DEMO

Management and Monitoring of changes outside of EntraOps Deployments



AADOps: Operationalization of Azure AD Conditional Access Cloud-Architekt.net



Please rate this session!

Your feedback will help with

- speaker evaluation
- content relevance
- decision making for future events
- quality improvement

Thank you!

Q&A

