# OPERATIONALIZATION OF AZURE AD CONDITIONAL ACCESS

PROJECT “AADOPS”

**Microsoft 365 Security & Compliance User Group**

November 30th, 2022

# **THOMAS** NAUNHEIM

Cloud Security Architect
@glueckkanja-gab AG

Koblenz, Germany

@Thomas_Live

cloud-architekt.net

Microsoft® MVP Most Valuable Professional

Azure Meetup BONN

CLOUD IDENTITY SUMMIT '22

# AGENDA

- CONDITIONAL ACCESS AND MICROSOFT GRAPH
- INTRODUCTION OF "AADOPS" PROJECT
- CODING AND CI/CD OF CONDITIONAL ACCESS TEMPLATES
- MANAGEMENT OF DEPLOYED CONDITIONAL ACCESS POLICIES

# CONDITIONAL ACCESS & MICROSOFT GRAPH

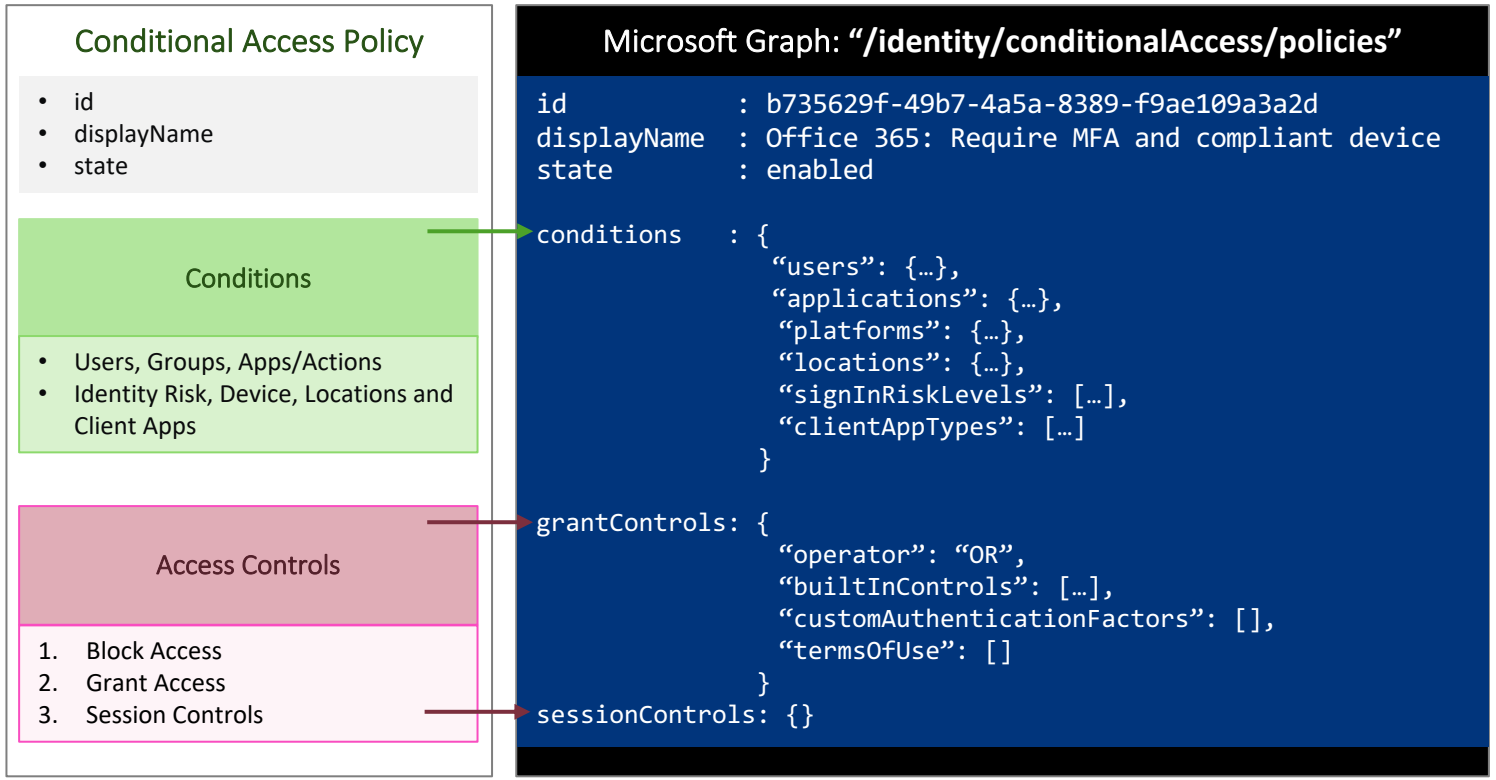
# Overview of Conditional Access Policies

**When this happens…**

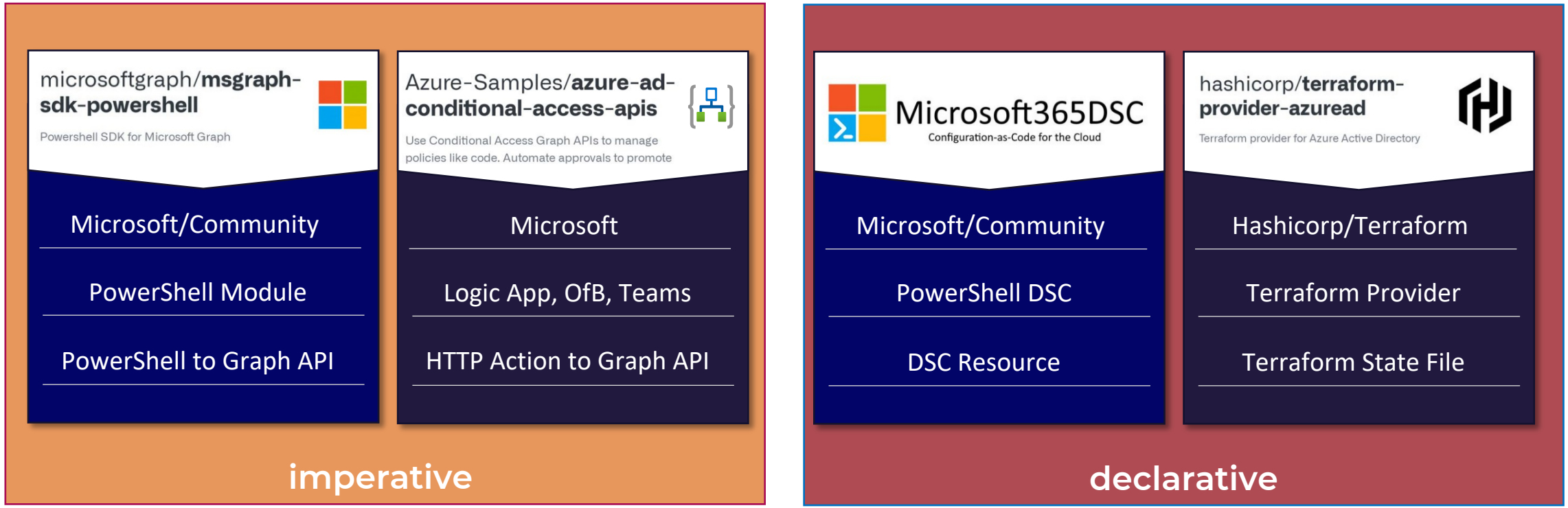
A **user** from **(group) "Marketing employees"** is accessing **"Office 365"** from **a browser** on a **Windows** device from **any location** and **no sign-in risk** was detected.

**…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).



# Configuration-As-Code



# Scripts and Templates

Fortigi/
**ConditionalAccess**

Fortigi

Scripts, GUID Convert

**PowerShell**

DanielChronlund/
**DCToolbox**

Tools for Microsoft cloud fans

Daniel Chronlund

**Templates, Report**

**PowerShell**

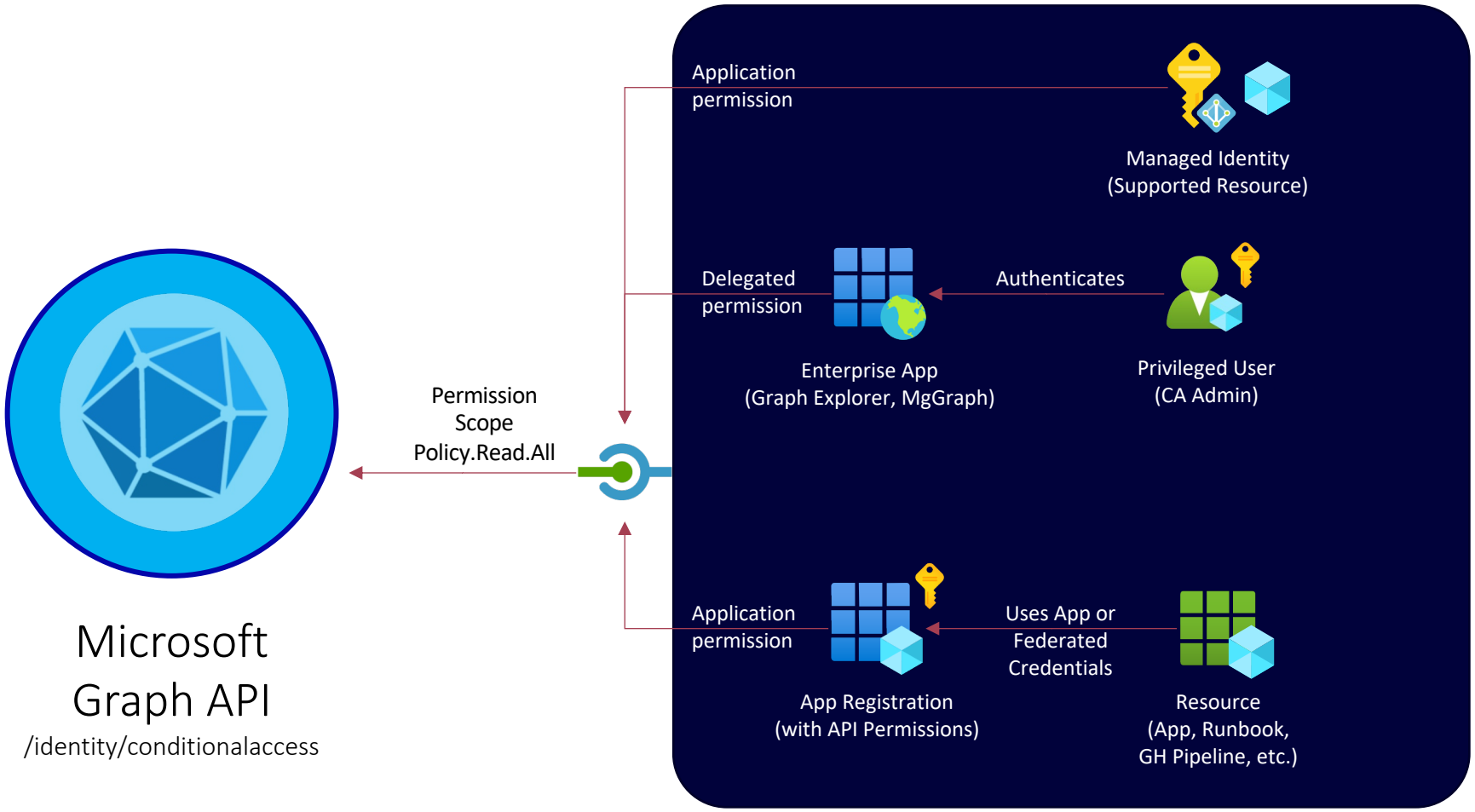
AlexFilipin/
**ConditionalAccess**

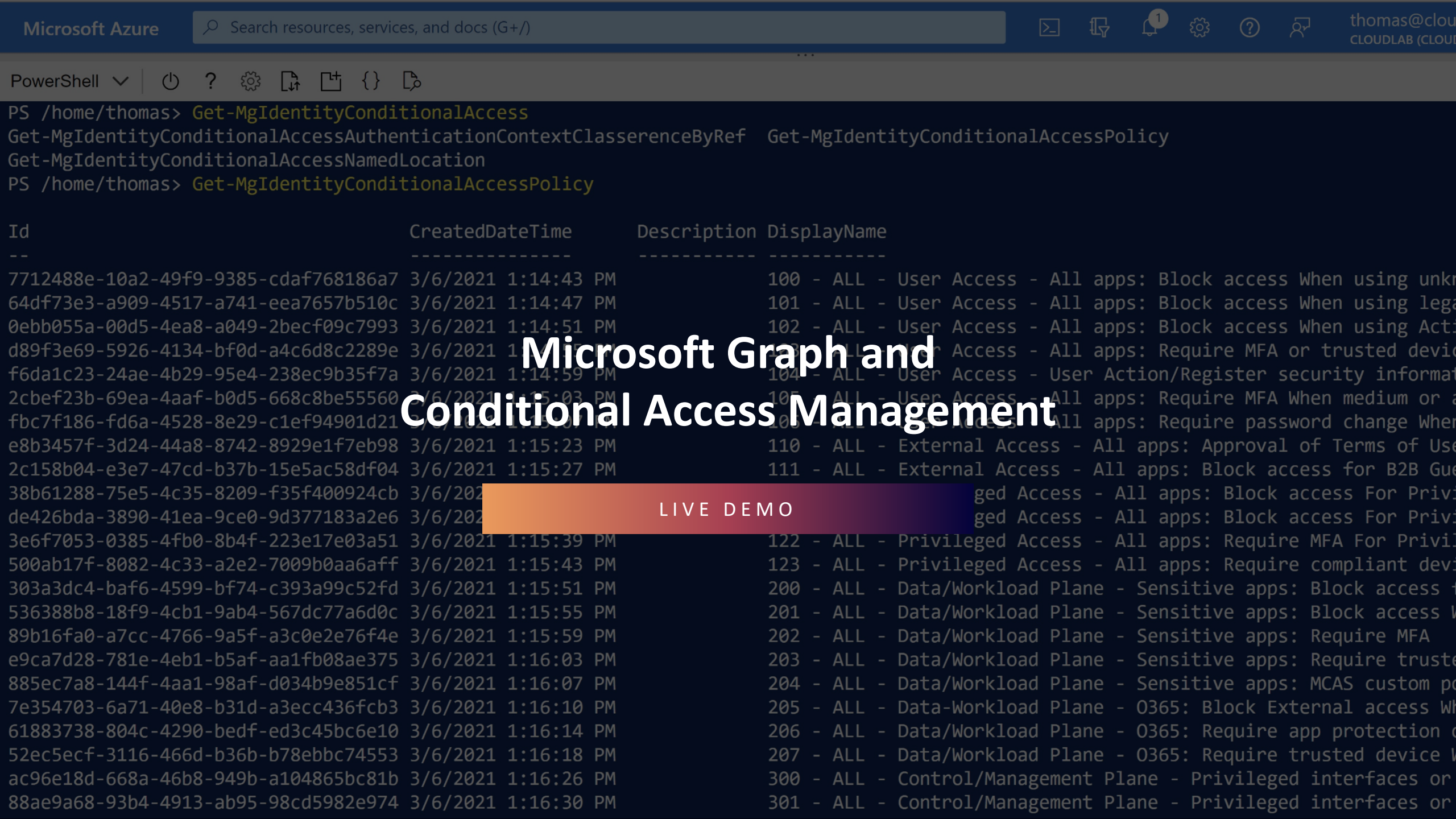
Alex Filipin

**Scripts, Templates**

**PowerShell**

# Access to Microsoft Graph






# Microsoft Graph and Conditional Access Management

LIVE DEMO

# INTRODUCTION OF "AADOPS" PROJECT

# DevOps Lifecycle for Azure AD 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"**

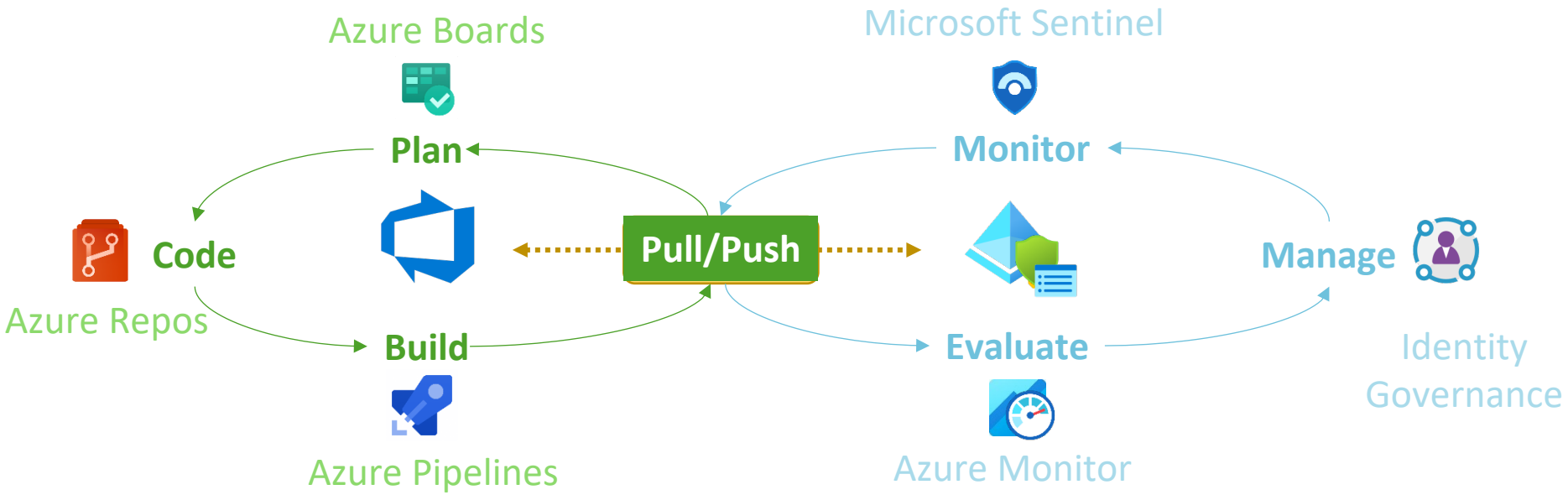
Ring- / Multi-Tenant (Staged) Deploy

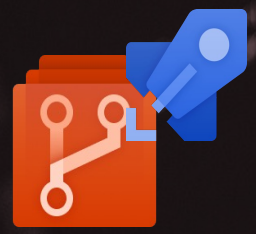
- Deploy policy configuration across various target groups or tenants
- Using templates for **standardized policy sets**
- **Reduced roll-out risks** by automated and staged deployment
- Reduced costs by automated deployment (**Managed Service Provider**)

Policy-As-Code and Governance

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

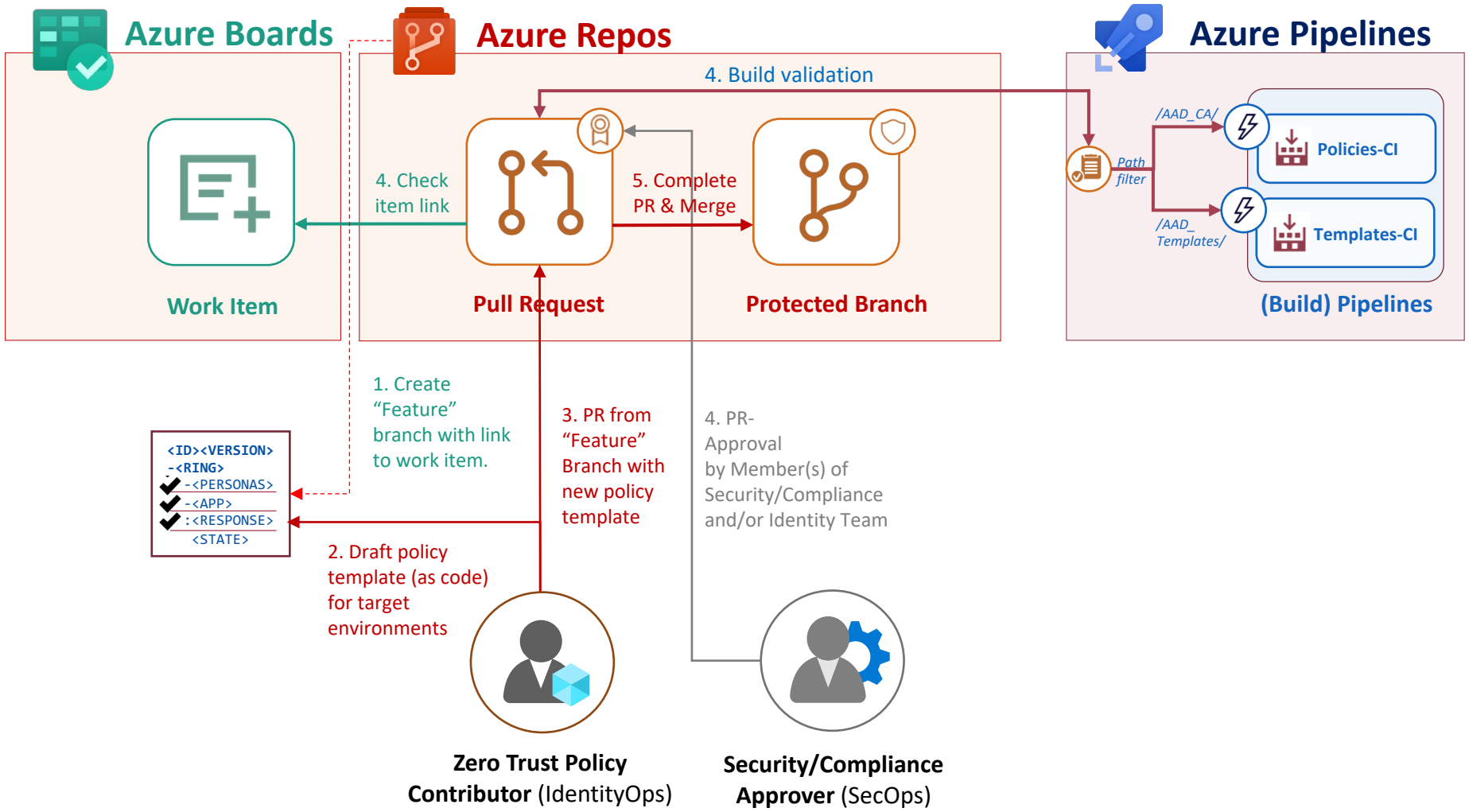
# DevOps Lifecycle for Azure AD Conditional Access



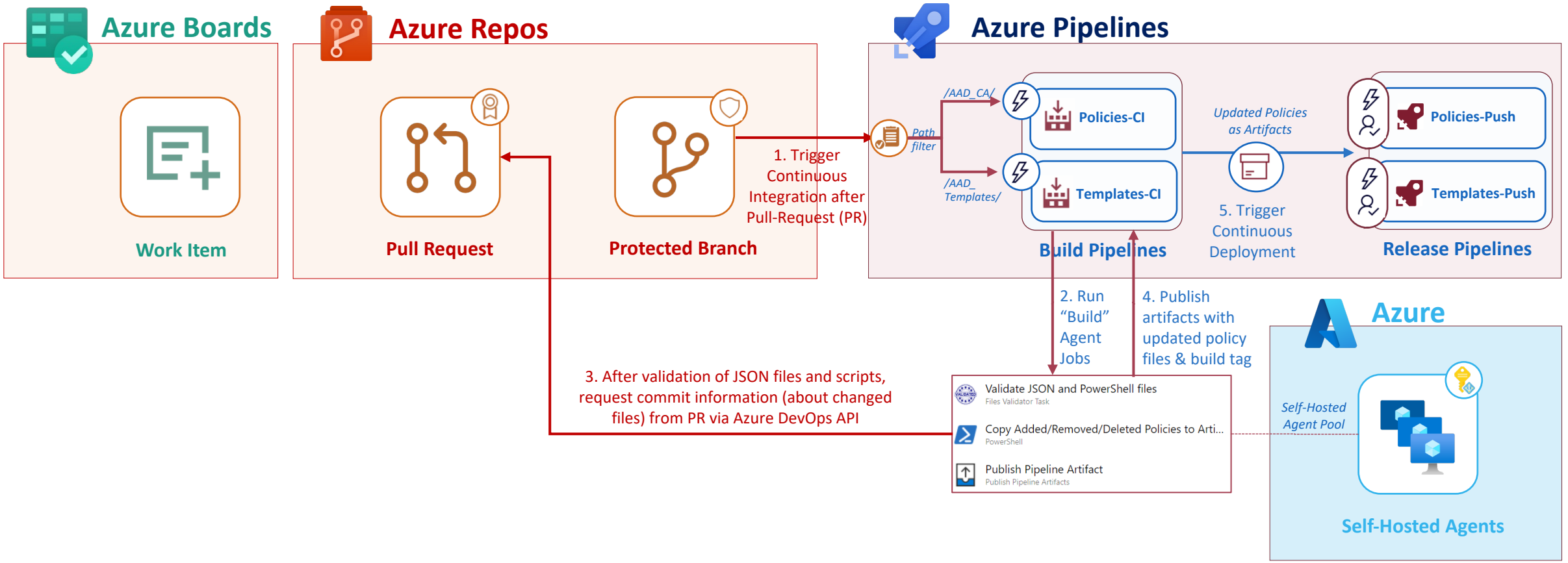


# CODING AND CI/CD OF CA TEMPLATES

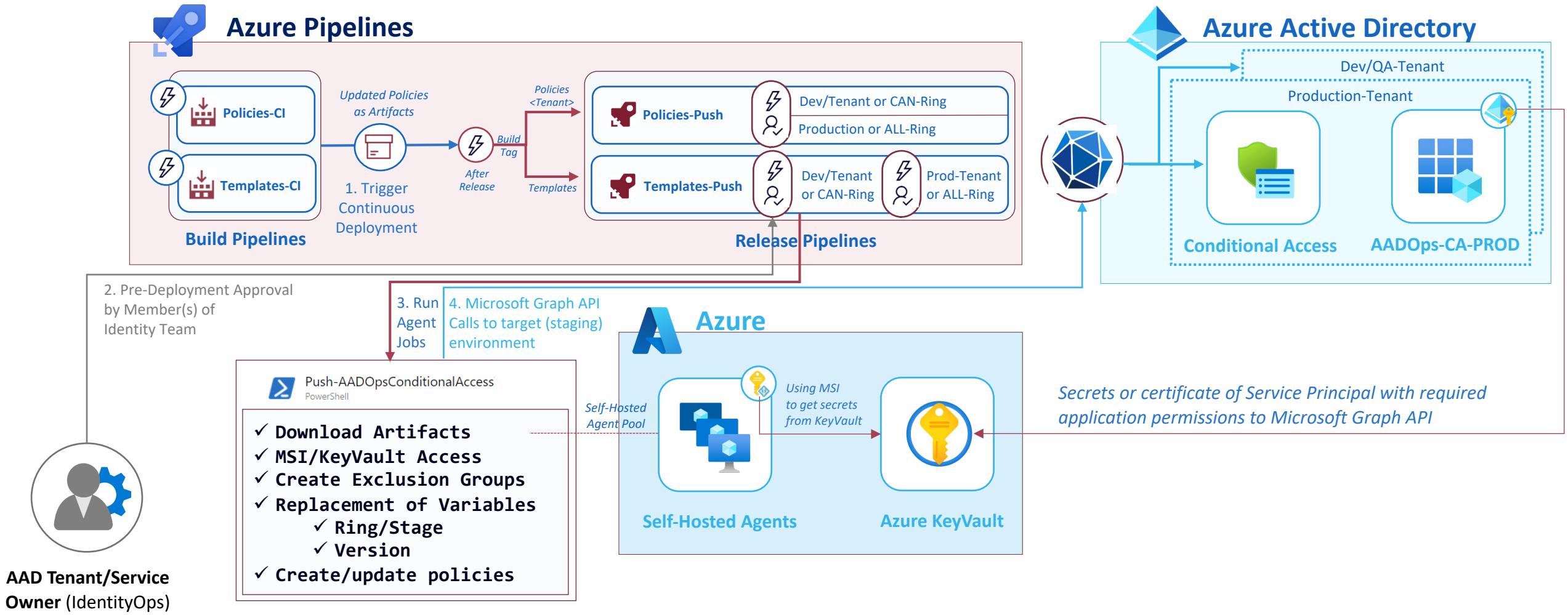
# AADOps Planning & Coding

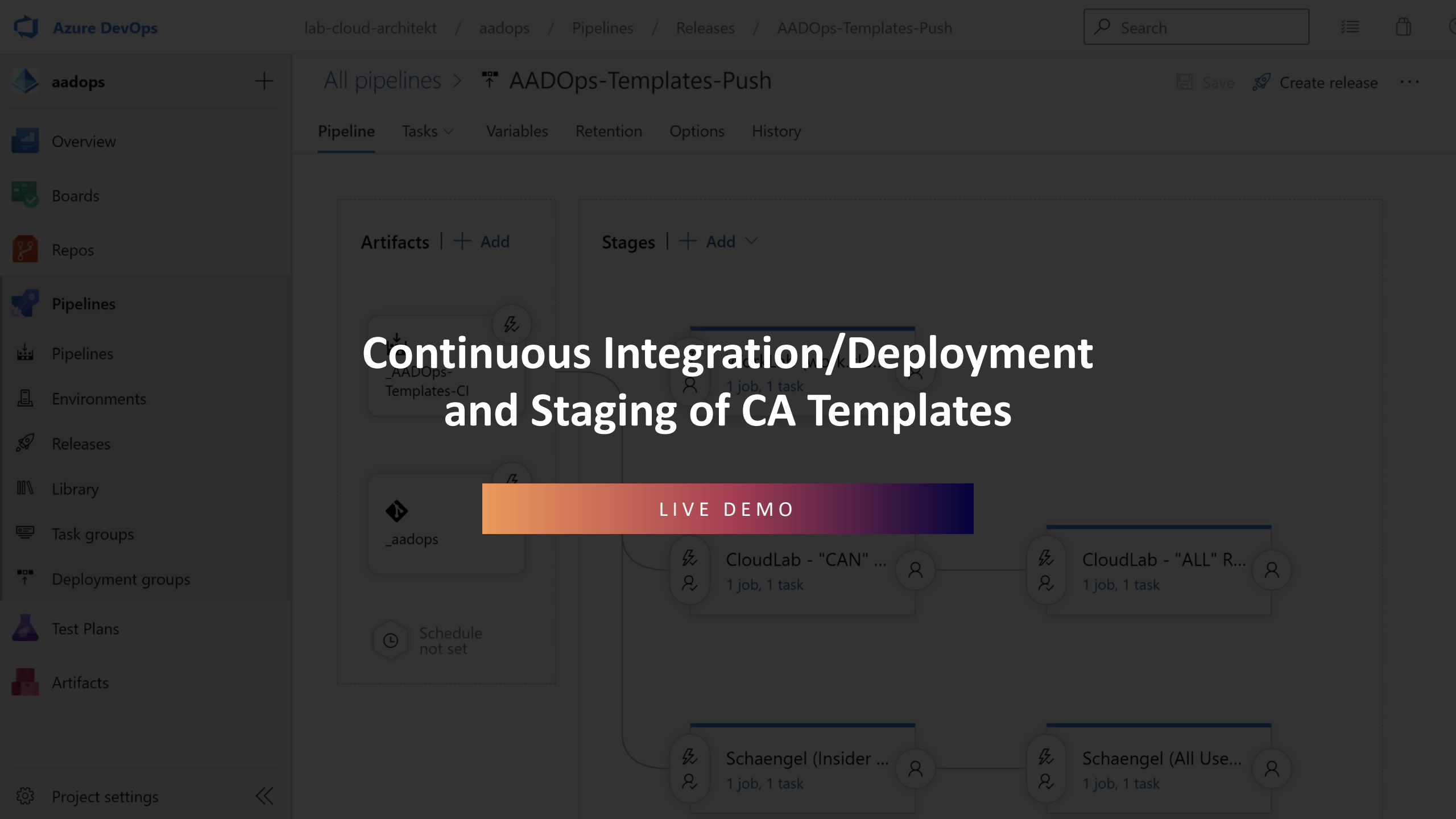


# AADOps Building Process



# AADOps Deployment Process



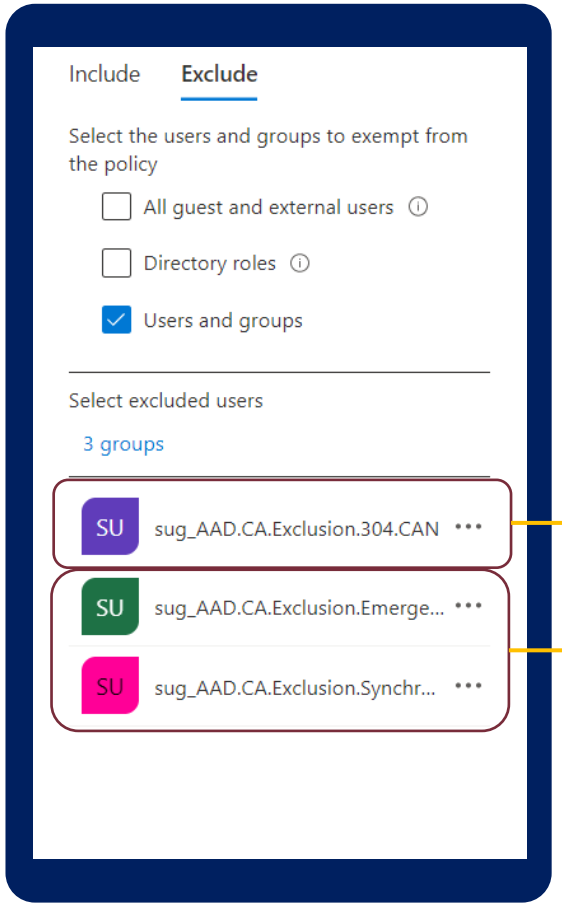



# Continuous Integration/Deployment and Staging of CA Templates

LIVE DEMO

# MANAGEMENT OF DEPLOYED CA POLICIES

# Conditional Access Exclusions




**General approach:**

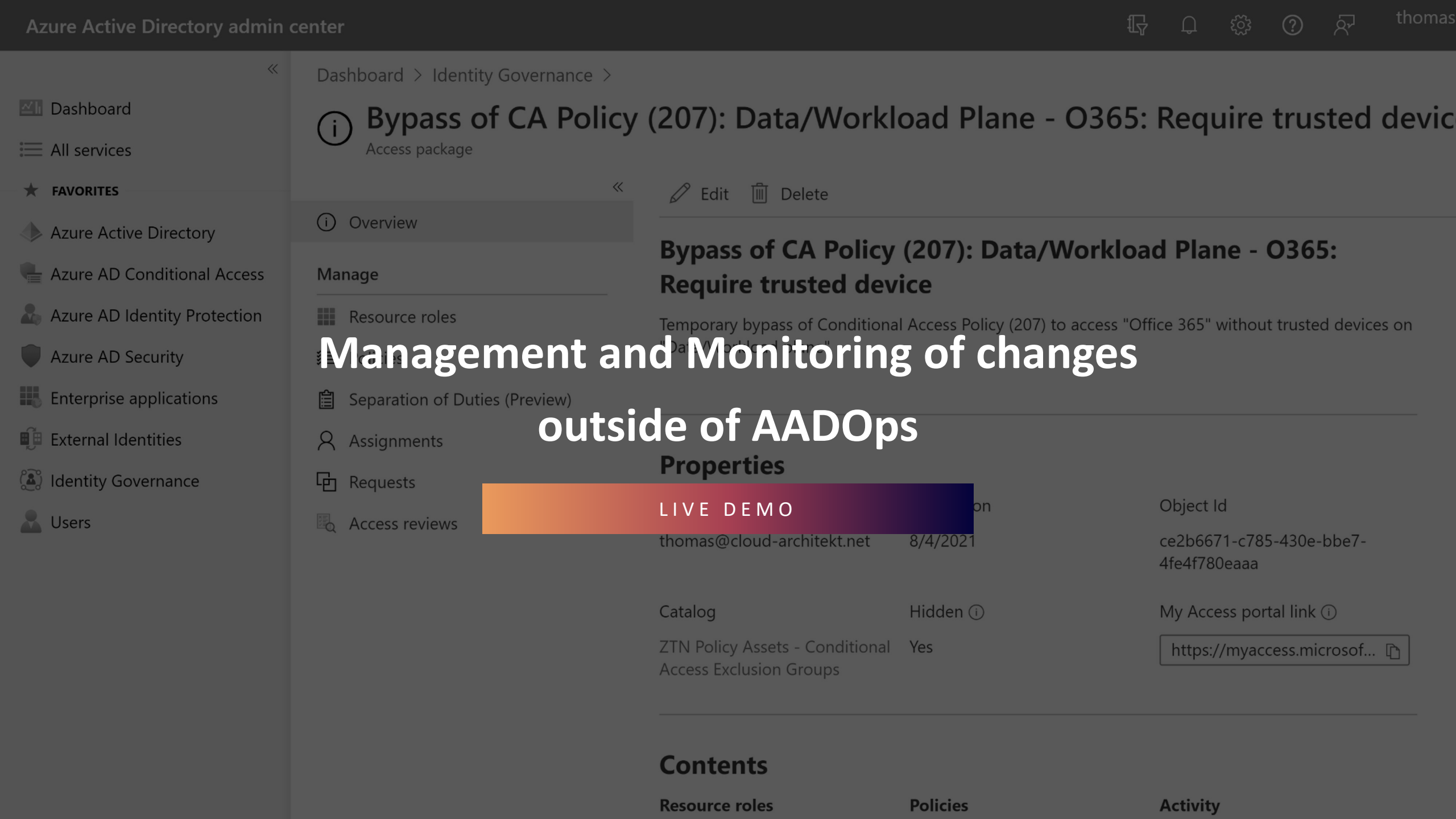
- Exclusion by (Cloud-only) Security Group
- Review of Excluded Groups (Azure AD access reviews)
- Monitoring of Exclusion Group (e.g. modified by Group or Intune Admins)

**Use Case A: Individual or wide scoped**

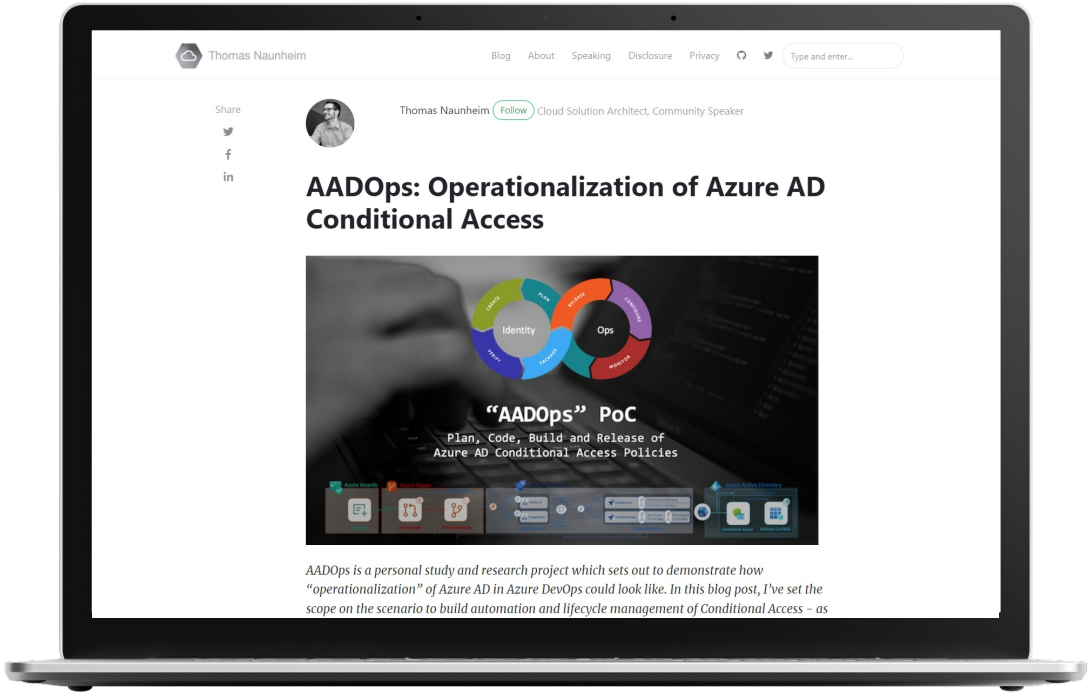
- Temporary or limited Exclusion
- Exclusion for each policy (or group of policies)
- Exclusion after approval process, assignment as Access Package

**Use Case B: Break Glass or Sync Account**

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


Azure Active Directory admin center
thomas
Dashboard
All services
FAVORITES
Azure Active Directory
Azure AD Conditional Access
Azure AD Identity Protection
Azure AD Security
Enterprise applications
External Identities
Identity Governance
Users
Dashboard > Identity Governance >
Bypass of CA Policy (207): Data/Workload Plane - O365: Require trusted devic
Access package
Overview
Manage
Resource roles
Separation of Duties (Preview)
Assignments
Requests
Access reviews
Edit
Delete
Bypass of CA Policy (207): Data/Workload Plane - O365: Require trusted device
Temporary bypass of Conditional Access Policy (207) to access "Office 365" without trusted devices on
Management and Monitoring of changes
outside of AADOps
LIVE DEMO
Properties
Object Id
thomas@cloud-architekt.net
8/4/2021
ce2b6671-c785-430e-bbe7-4fe4f780eaaa
Catalog
Hidden
My Access portal link
ZTN Policy Assets - Conditional Access Exclusion Groups
Yes
https://myaccess.microsof...
Contents
Resource roles
Policies
Activity

# Blog post about AADOps




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

# THANK YOU

@Thomas_Live

Thomas@Naunheim.net

www.cloud-architekt.net