



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





AGENDA



CONDITIONAL ACCESS
AND MICROSOFT GRAPH



INTRODUCTION OF
"AADOPS" PROJECT



CODING AND CI/CD OF
CONDITIONAL ACCESS TEMPLATES

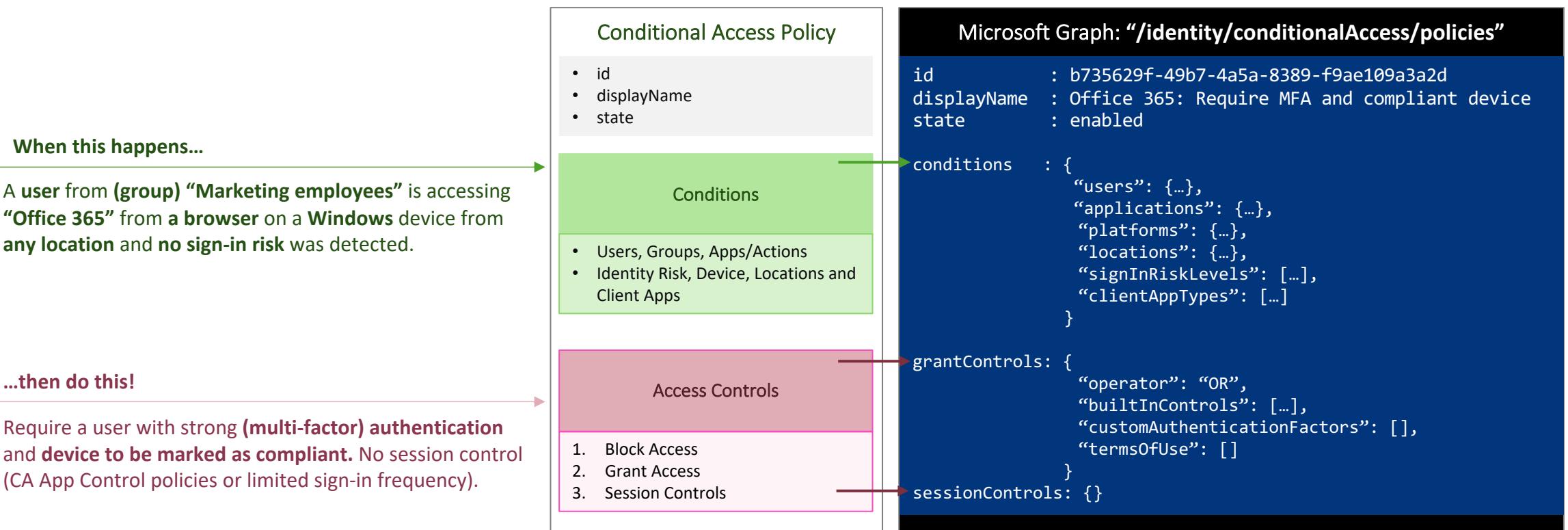


MANAGEMENT OF DEPLOYED
CONDITIONAL ACCESS POLICIES



CONDITIONAL ACCESS & MICROSOFT GRAPH

Overview of Conditional Access Policies



Configuration-As-Code

[microsoftgraph/msgraph-sdk-powershell](#)  Powershell SDK for Microsoft Graph

Microsoft/Community

PowerShell Module

PowerShell to Graph API

[Azure-Samples/azure-ad-conditional-access-apis](#)  Use Conditional Access Graph APIs to manage policies like code. Automate approvals to promote

Microsoft

Logic App, OfB, Teams

HTTP Action to Graph API

imperative

[Microsoft365DSC](#) Configuration-as-Code for the Cloud 

Microsoft/Community

PowerShell DSC

DSC Resource

[hashicorp/terraform-provider-azuread](#)  Terraform provider for Azure Active Directory

Hashicorp/Terraform

Terraform Provider

Terraform State File

declarative

Scripts and Templates

**Fortigi/
ConditionalAccess** 

Fortigi

Scripts, GUID Convert

PowerShell

**DanielChronlund/
DCToolbox** 
Tools for Microsoft cloud fans

Daniel Chronlund

Templates, Report

PowerShell

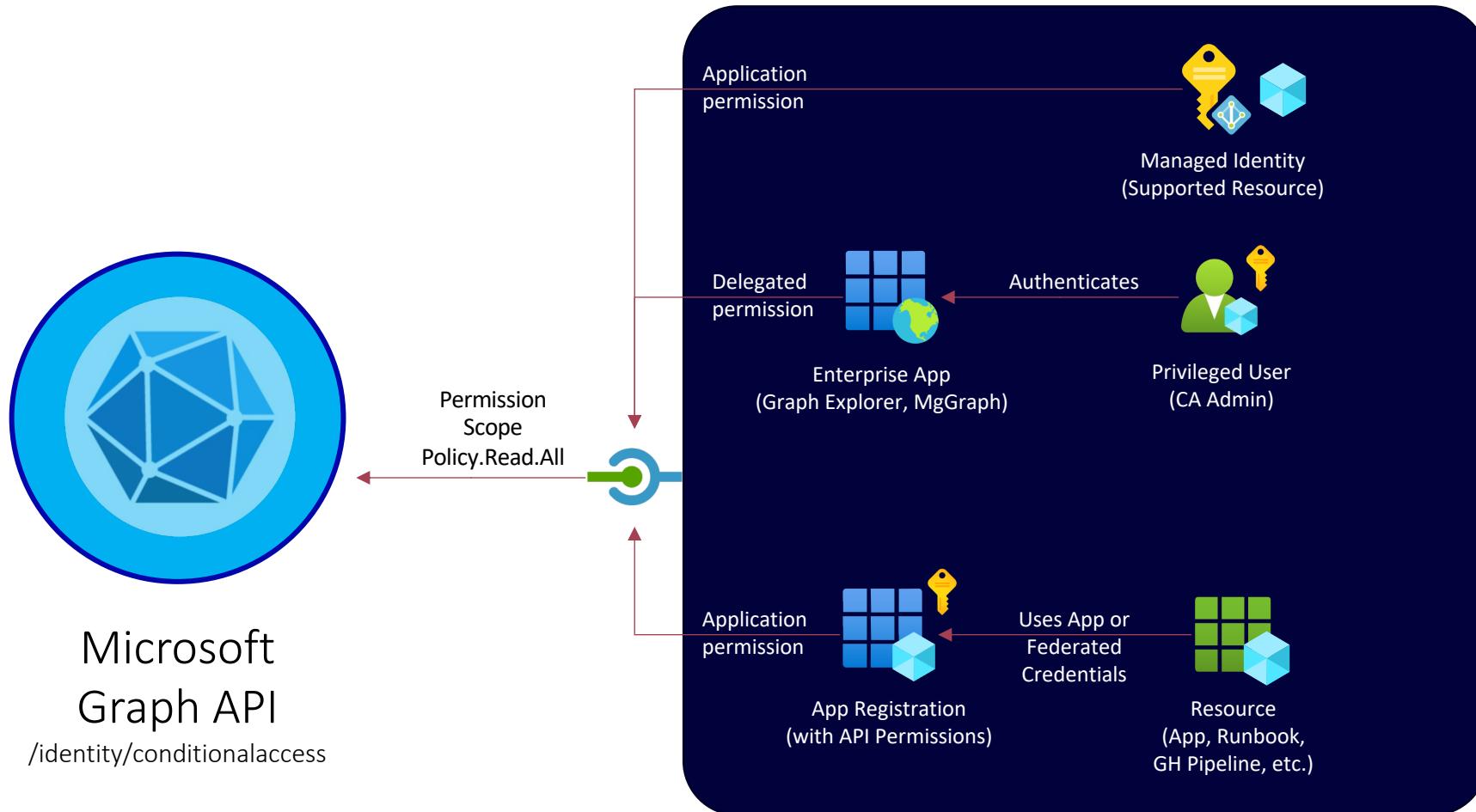
**AlexFilipin/
ConditionalAccess** 

Alex Filipin

Scripts, Templates

PowerShell

Access to Microsoft Graph



PowerShell | ⚡ ? 🛡 { } 🔍

```
PS /home/thomas> Get-MgIdentityConditionalAccess
Get-MgIdentityConditionalAccessAuthenticationContextClasserenceByRef  Get-MgIdentityConditionalAccessPolicy
Get-MgIdentityConditionalAccessNamedLocation
PS /home/thomas> Get-MgIdentityConditionalAccessPolicy
```

Id	CreatedDateTime	Description	DisplayName
7712488e-10a2-49f9-9385-cdaf768186a7	3/6/2021 1:14:43 PM	100 - ALL - User Access - All apps: Block access When using unknown device	All apps: Block access When using unknown device
64df73e3-a909-4517-a741-eea7657b510c	3/6/2021 1:14:47 PM	101 - ALL - User Access - All apps: Block access When using legacy device	All apps: Block access When using legacy device
0ebb055a-00d5-4ea8-a049-2becf09c7993	3/6/2021 1:14:51 PM	102 - ALL - User Access - All apps: Block access When using ActiveSync device	All apps: Block access When using ActiveSync device
d89f3e69-5926-4134-bf0d-a4c6d8c2289e	3/6/2021 1:14:55 PM	103 - ALL - User Access - All apps: Require MFA or trusted device	All apps: Require MFA or trusted device
f6da1c23-24ae-4b29-95e4-238ec9b35f7a	3/6/2021 1:14:59 PM	104 - ALL - User Access - User Action/Register security information	User Action/Register security information
2cbef23b-69ea-4aaf-b0d5-668c8be55560	3/6/2021 1:15:03 PM	105 - ALL - User Access - All apps: Require MFA When medium or large device	All apps: Require MFA When medium or large device
fbef186-fd6a-4528-8e29-c1ef94901d21	3/6/2021 1:15:07 PM	106 - ALL - User Access - All apps: Require password change When device changes	All apps: Require password change When device changes
e8b3457f-3d24-44a8-8742-8929e1f7eb98	3/6/2021 1:15:23 PM	110 - ALL - External Access - All apps: Approval of Terms of Use	Approval of Terms of Use
2c158b04-e3e7-47cd-b37b-15e5ac58df04	3/6/2021 1:15:27 PM	111 - ALL - External Access - All apps: Block access for B2B Guest	Block access for B2B Guest
38b61288-75e5-4c35-8209-f35f400924cb	3/6/2021 1:15:31 PM	112 - ALL - External Access - All apps: Block access For Privileged users	Block access For Privileged users
de426bda-3890-41ea-9ce0-9d377183a2e6	3/6/2021 1:15:35 PM	113 - ALL - External Access - All apps: Block access For Privileged users	Block access For Privileged users
3e6f7053-0385-4fb0-8b4f-223e17e03a51	3/6/2021 1:15:39 PM	122 - ALL - Privileged Access - All apps: Require MFA For Privileged users	Require MFA For Privileged users
500ab17f-8082-4c33-a2e2-7009b0aa6aff	3/6/2021 1:15:43 PM	123 - ALL - Privileged Access - All apps: Require compliant device	Require compliant device
303a3dc4-baf6-4599-bf74-c393a99c52fd	3/6/2021 1:15:51 PM	200 - ALL - Data/Workload Plane - Sensitive apps: Block access	Sensitive apps: Block access
536388b8-18f9-4cb1-9ab4-567dc77a6d0c	3/6/2021 1:15:55 PM	201 - ALL - Data/Workload Plane - Sensitive apps: Block access When device changes	Sensitive apps: Block access When device changes
89b16fa0-a7cc-4766-9a5f-a3c0e2e76f4e	3/6/2021 1:15:59 PM	202 - ALL - Data/Workload Plane - Sensitive apps: Require MFA	Sensitive apps: Require MFA
e9ca7d28-781e-4eb1-b5af-aa1fb08ae375	3/6/2021 1:16:03 PM	203 - ALL - Data/Workload Plane - Sensitive apps: Require trusted device	Sensitive apps: Require trusted device
885ec7a8-144f-4aa1-98af-d034b9e851cf	3/6/2021 1:16:07 PM	204 - ALL - Data/Workload Plane - Sensitive apps: MCAS custom policy	MCAS custom policy
7e354703-6a71-40e8-b31d-a3ecc436fcbb	3/6/2021 1:16:10 PM	205 - ALL - Data/Workload Plane - O365: Block External access	Block External access
61883738-804c-4290-bedf-ed3c45bc6e10	3/6/2021 1:16:14 PM	206 - ALL - Data/Workload Plane - O365: Require app protection	Require app protection
52ec5ecf-3116-466d-b36b-b78ebbc74553	3/6/2021 1:16:18 PM	207 - ALL - Data/Workload Plane - O365: Require trusted device	Require trusted device
ac96e18d-668a-46b8-949b-a104865bc81b	3/6/2021 1:16:26 PM	300 - ALL - Control/Management Plane - Privileged interfaces or services	Privileged interfaces or services
88ae9a68-93b4-4913-ab95-98cd5982e974	3/6/2021 1:16:30 PM	301 - ALL - Control/Management Plane - Privileged interfaces or services	Privileged interfaces or services

LIVE DEMO



INTRODUCTION OF "AADOPS" PROJECT

DevOps Lifecycle for Azure AD Conditional Access



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

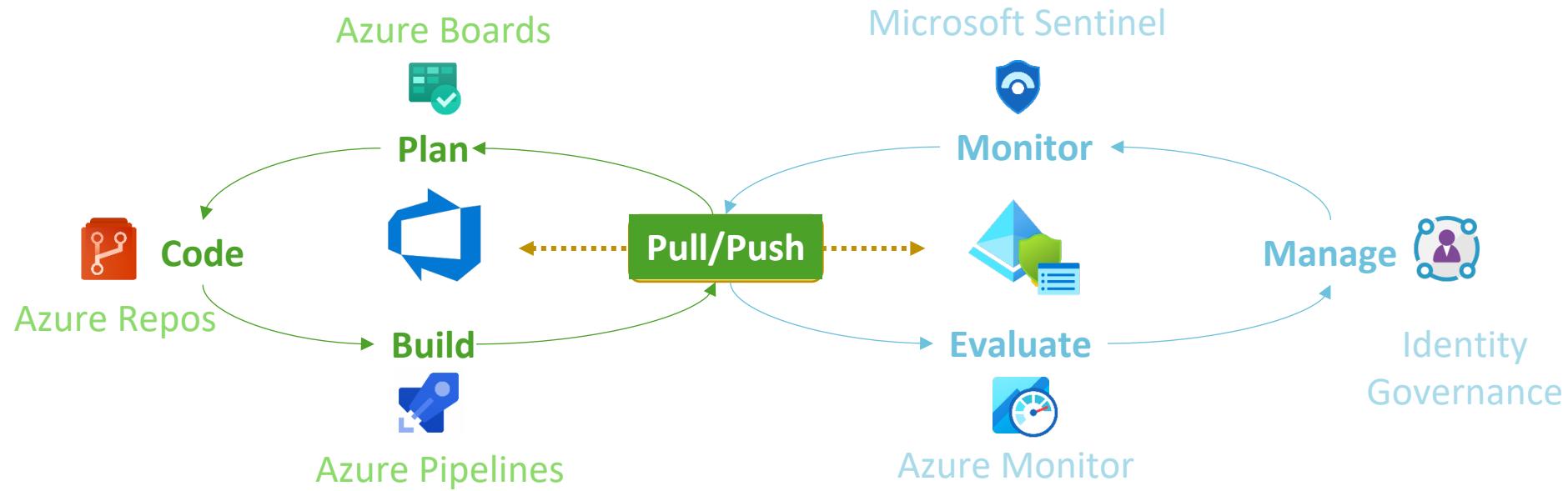


- Deploy policy configuration across various target groups or tenants
- Using templates for **standardized policy sets**
- **Reduced roll-out risks** by automated and staged deployment
- Reduced costs by automated deployment (**Managed Service Provider**)



- **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





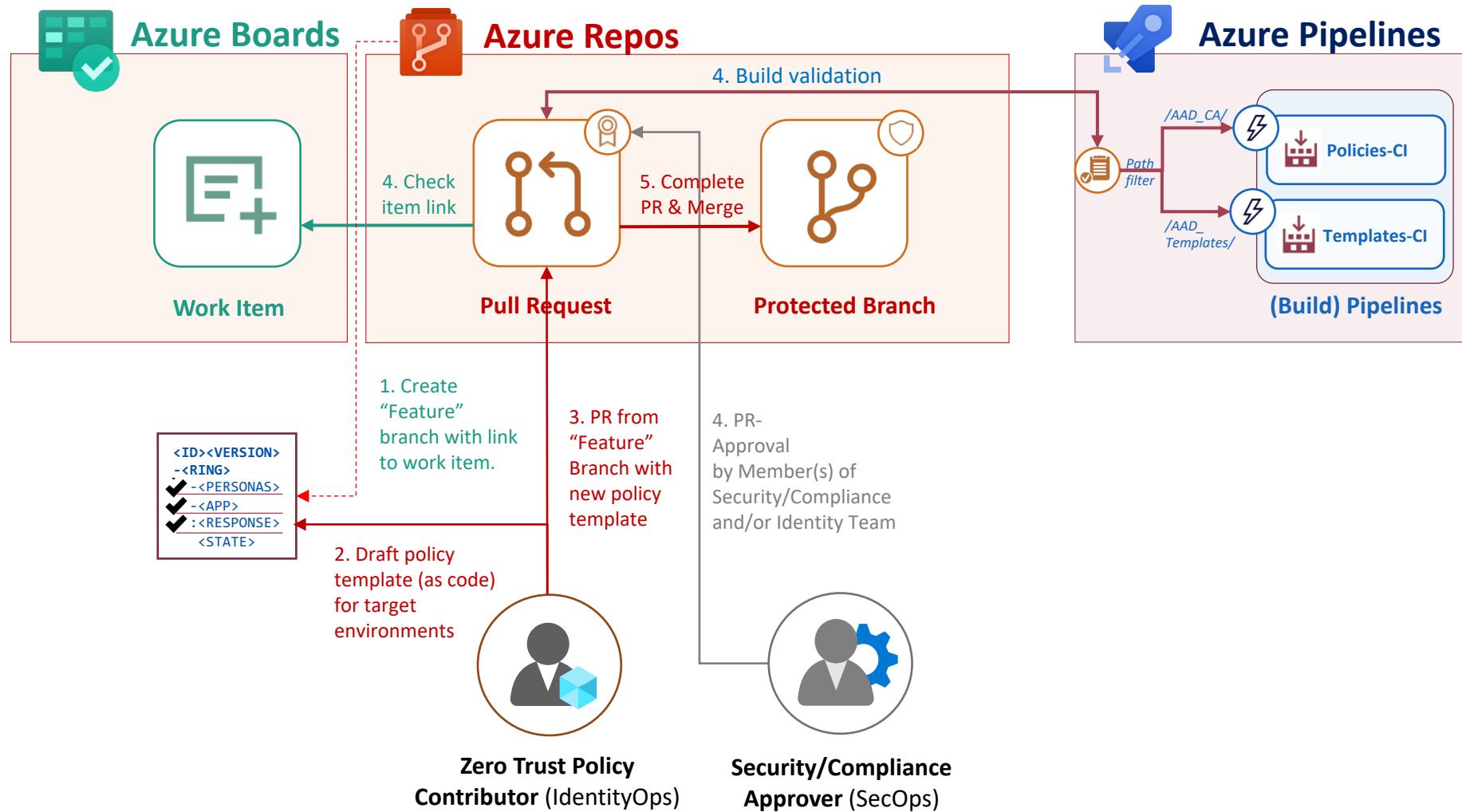
CODING AND CI/CD OF CA TEMPLATES

```
        class = 'zoom' );
    elseif( $loop % $columns == 0 )
        $column[] = 'first';
    elseif( ($loop + 1) % $columns == 0 )
        $column[] = 'last';
    $image_url = wp_get_attachment_url( $attachment->guid );
    if( ! $image_link )
        continue;
    $image = wp_get_attachment_image( $attachment->ID, 'large' );
    $image_class = esc_attr( $attachment->post_thumbnail_class );
    $image_title = esc_attr( $attachment->post_thumbnail_title );
    $image_html = '

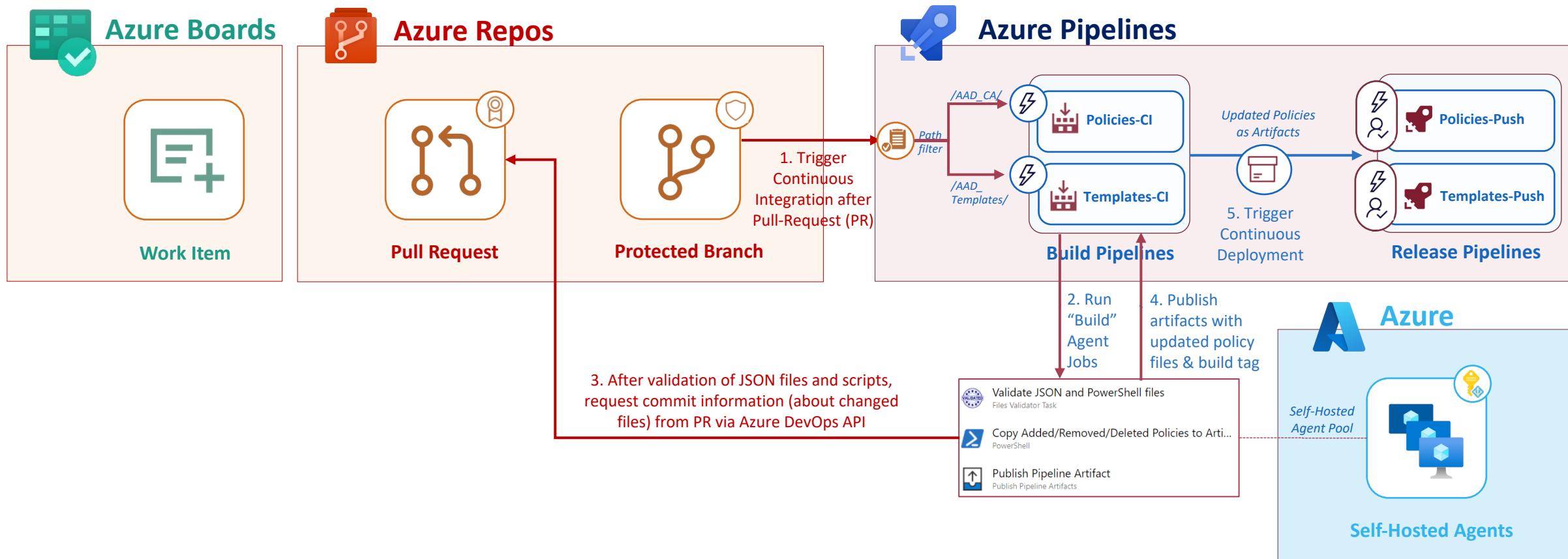
' . $image . '

' . $attachment->post_content;
    $image_html = str_replace( '<div>', '<div><div>', $image_html );
    $image_html = str_replace( '</div>', '</div></div>', $image_html );
    $image_html = str_replace( 'wp_get_attachment_image', 'get_post_thumbnail', $image_html );
    $image_html = str_replace( 'large_thumbnail_size', 'large', $image_html );
    echo $image_html;
}
```

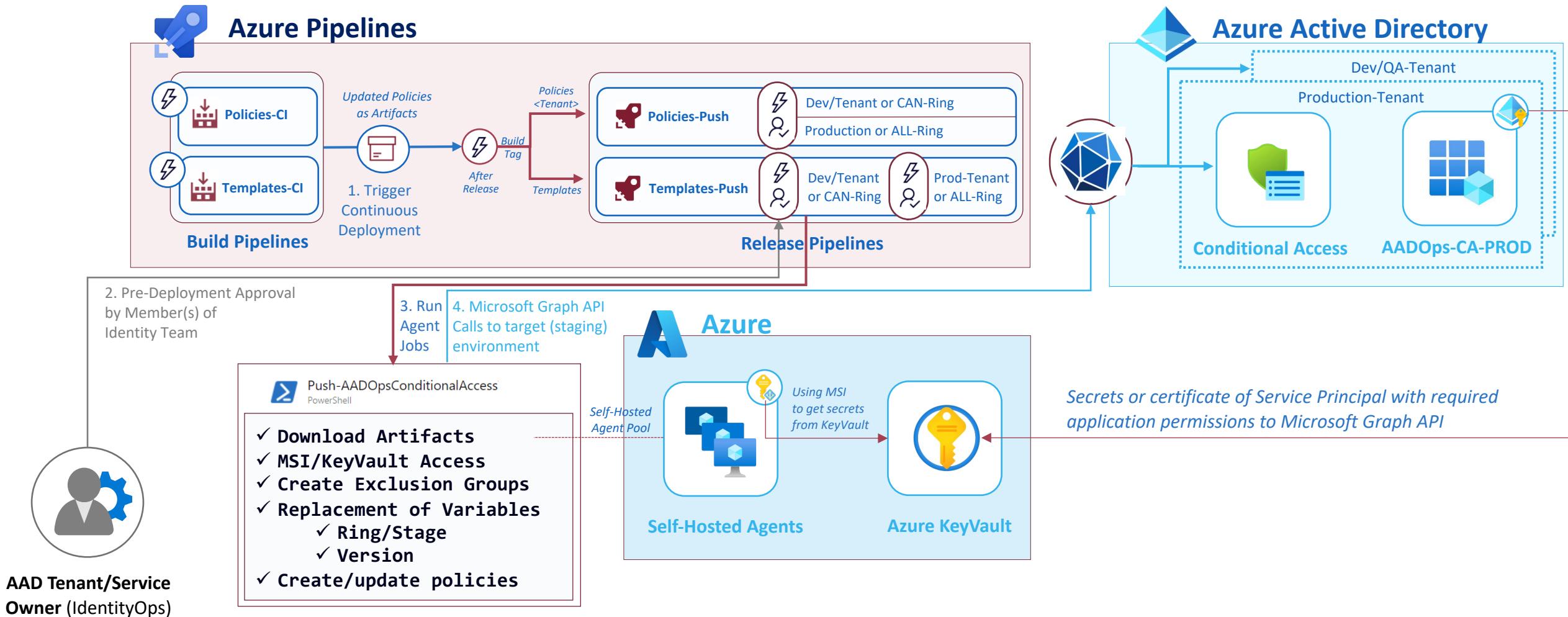
AADOps Planning & Coding



AADOps Building Process



AADOps Deployment Process





aadops



All pipelines > AADOps-Templates-Push

Save

Create release

...

Pipeline

Tasks ▾

Variables

Retention

Options

History

Artifacts | + Add

Stages | + Add ▾

Continuous Integration/Deployment and Staging of CA Templates

LIVE DEMO



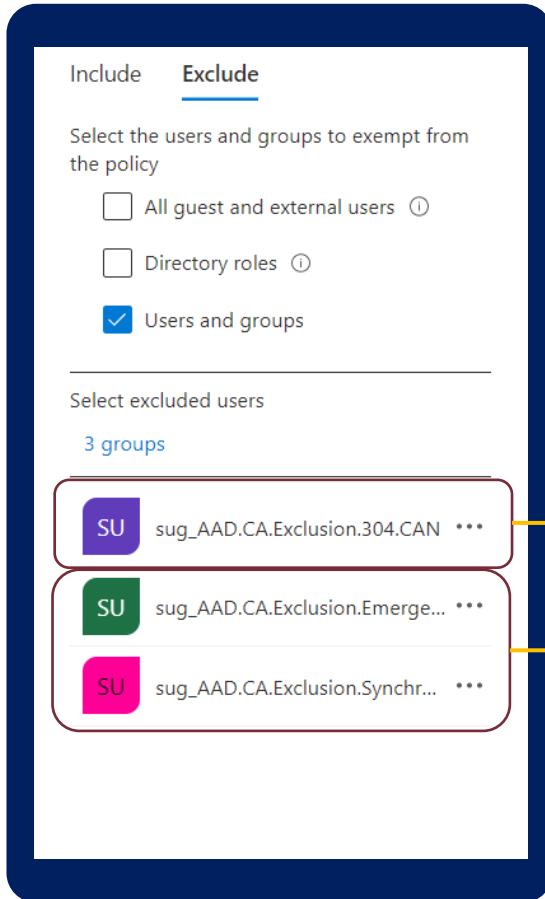
_aadops

Schedule
not setCloudLab - "CAN" ...
1 job, 1 taskCloudLab - "ALL" R...
1 job, 1 taskSchaengel (Insider ...
1 job, 1 taskSchaengel (All Use...
1 job, 1 task



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

<<

Dashboard > Identity Governance >

Bypass of CA Policy (207): Data/Workload Plane - O365: Require trusted device

Access package

Edit Delete

Overview

Manage

Resource roles

Separation of Duties (Preview)

Assignments

Requests

Access reviews

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 "Data/Workload Plane".

Management and Monitoring of changes outside of AADOps

Properties

LIVE DEMO

thomas@cloud-architekt.net 8/4/2021

Object Id

ce2b6671-c785-430e-bbe7-
4fe4f780eaaa

Catalog

Hidden

My Access portal link

ZTN Policy Assets - Conditional
Access Exclusion Groups Yes[https://myaccess.microsoft...](https://myaccess.microsoft.com)

Contents

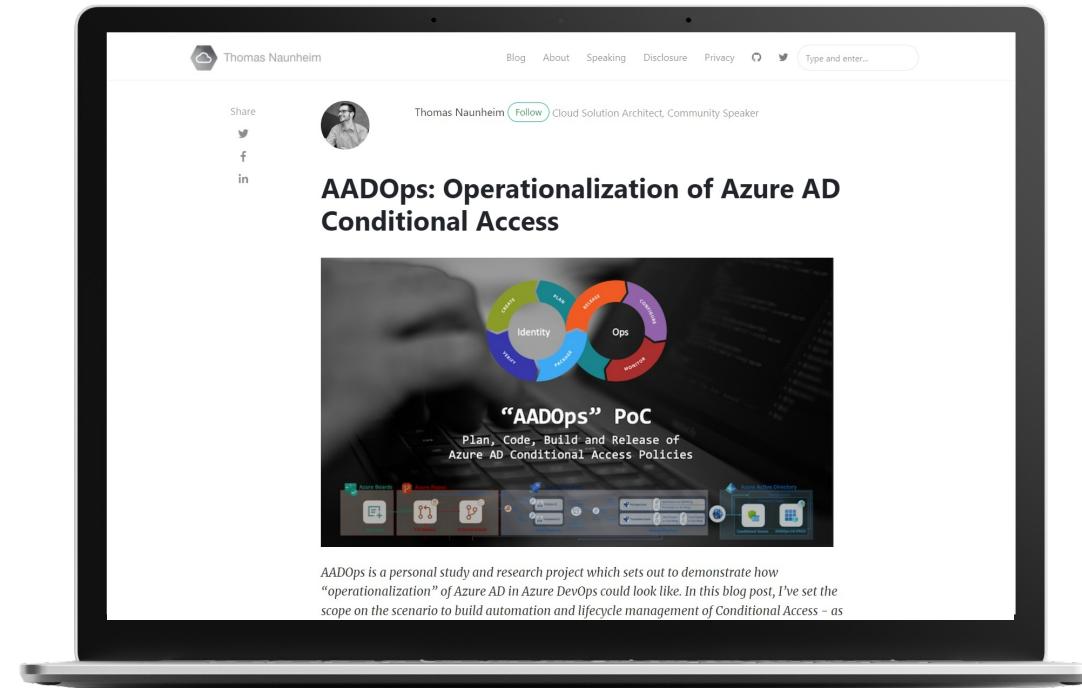
Resource roles

Policies

Activity

DO YOU LIKE TO LEARN MORE?

Blog post about AADOps



AADOps: Operationalization
of Azure AD Conditional Access
[Cloud-Architekt.net](#)

THANK YOU



@Thomas_Live



Thomas@Naunheim.net

www.cloud-architekt.net