

Azure Governance with Enterprise Azure Policy As Code

Haflidi Fridthjofsson

Sopra Steria | azureviking.com

MVP
Dagen

Haflidi Fridthjofsson

Principal Cloud Architect at Sopra Steria

- IT specialist since 2011.
- Microsoft Certified Professional (MCP) since 2014.
- Microsoft MVP within Security since 2023.
- Co-founder of the [Microsoft Security User Group](#).
 - Specialist within.
 - Azure Infrastructure.
 - Infrastructure as code.
 - Security.
 - Free Time
 - Spending time with my family.
 - Check out and learn new technology
 - Bit of gaming, primarily FPS here and there when I got time.



Follow me on:



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



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

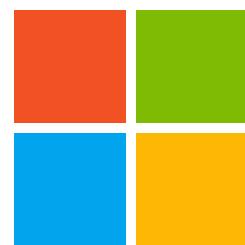


azureviking.com



MVP-Dagen





Microsoft

Evidi



INNOFACTOR®



POINT : TAKEN

iver The iver logo consists of the word "iver" in a black, sans-serif font followed by a black, right-pointing arrow icon.

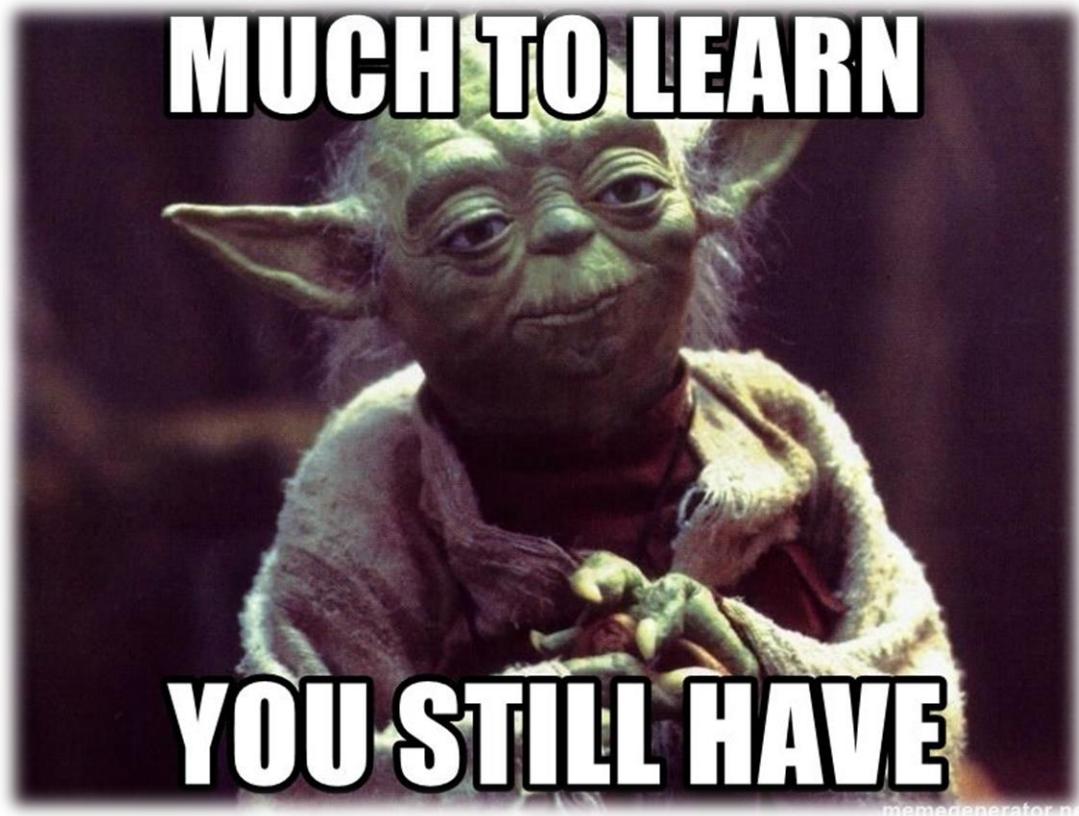
MVP-Dagen

Session Goal

What we want to achieve.

Your takeaways from this session.

- What Enterprise Azure Policy as Code (EPAC) is.
- What some of the key advantages of using Azure Policy as code are.
- Who should use the Enterprise Azure Policy as code. (EPAC)
- **DEMO TIME!** 😎 - Deep dive into EPAC Scenarios and learn how to get started with EPAC.
- Q&A if we got time 🍻



Slides & code used in the demos will be shared afterwards

[presentations/mvp-dagen-2023 · haflidif/presentations \(github.com\)](https://github.com/haflidif/presentations)

MVP-Dagen

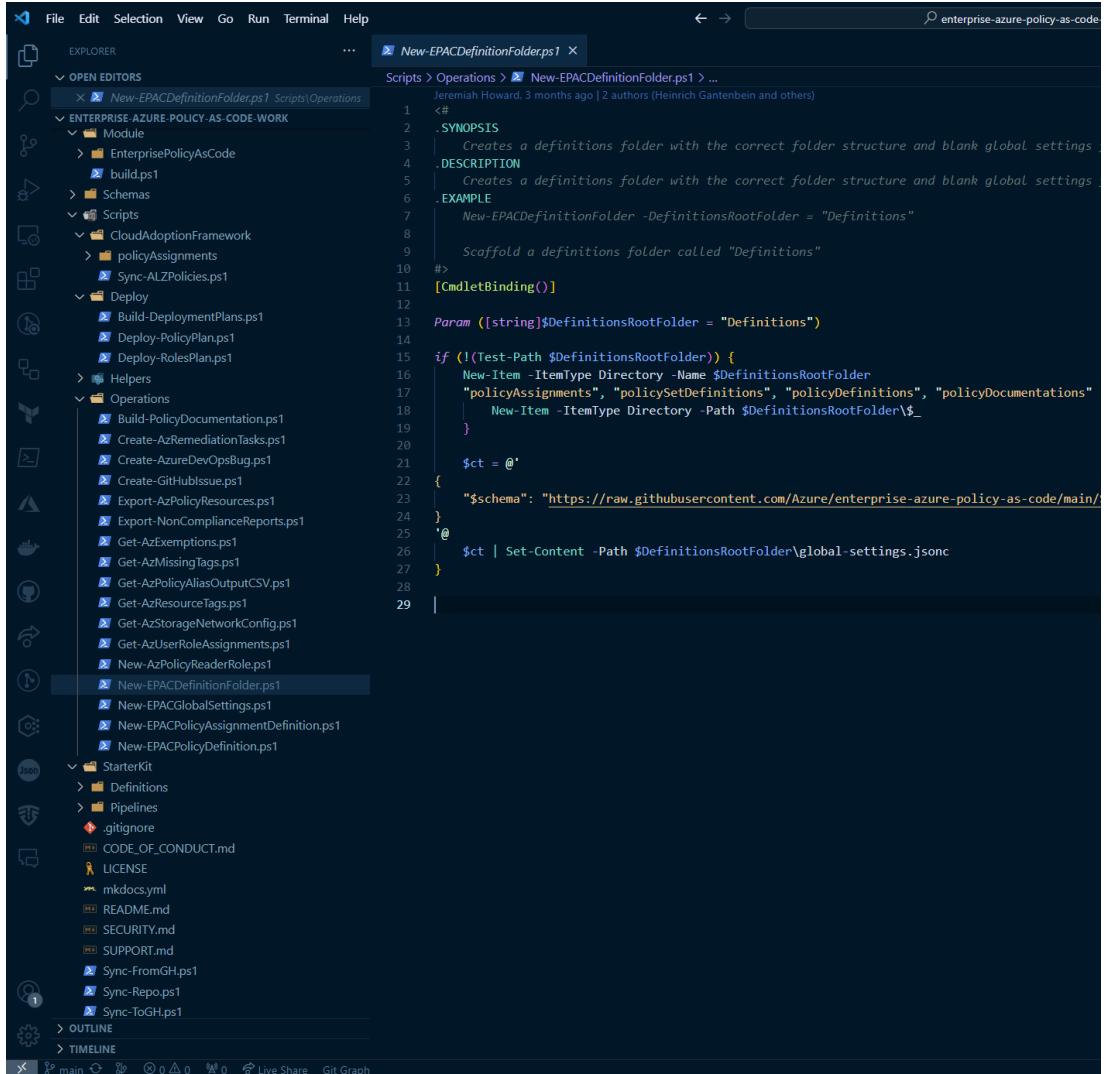
The background of the slide features a dense, futuristic cityscape with towering skyscrapers and intricate, glowing blue circuitry or data streams weaving between them. In the foreground, there is a large, semi-transparent silhouette of a diverse crowd of people, appearing as dark blue shapes against the lighter blue of the background.

Enterprise Azure Policy as code ?

Enterprise Azure Policy as Code

What is it ?

- Set of PowerShell Scripts and modules.
- Can manage Azure policies, policy sets, assignments, exemptions and role assignments.
- Supported in CI/CD based systems or in a semi-automated way.
- Integrates well with Cloud Adoption Framework and Azure Landing Zone.
- Supports multi-tenant/environments policy deployment.
- Recognized as an alternative deployment method and management for policies within the Azure Architecture Center.



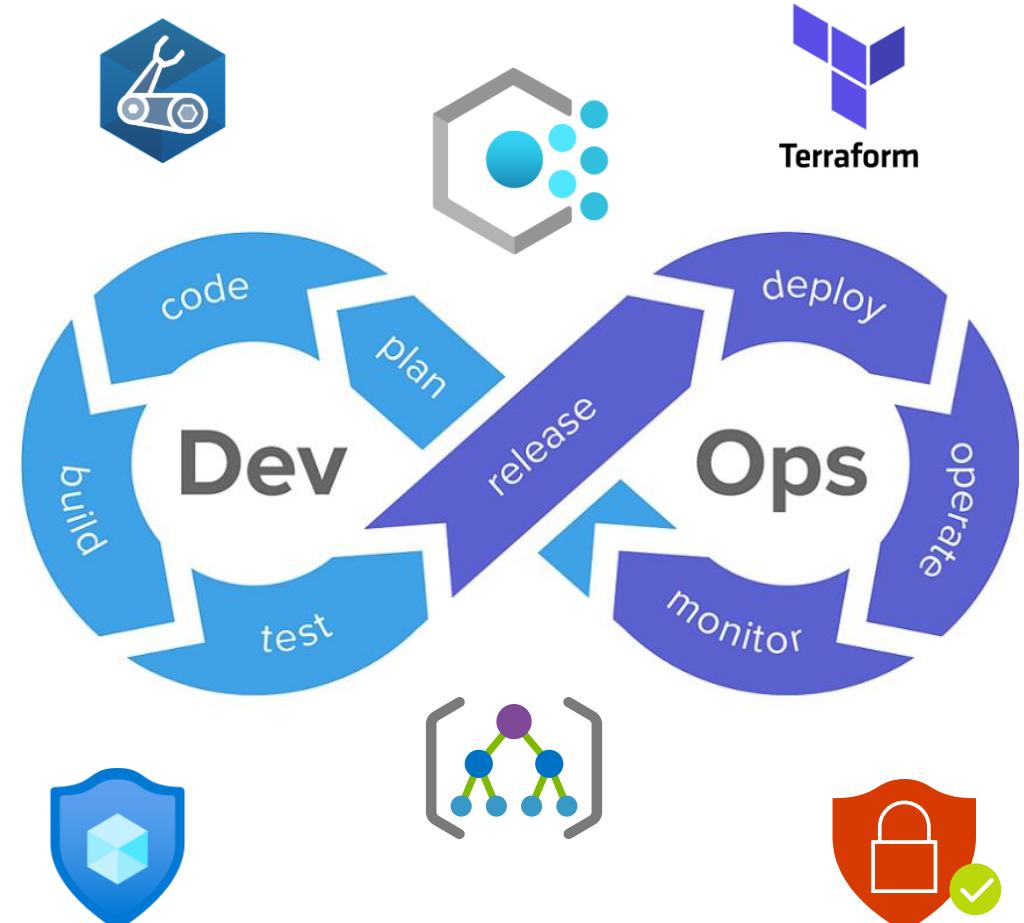
The screenshot shows a code editor interface with a dark theme. On the left is the Explorer sidebar, which lists several PowerShell scripts and modules under the 'ENTERPRISE-AZURE-POLICY-AS-CODE-WORK' folder. The main pane displays the content of the 'New-EPACDefinitionFolder.ps1' script. The script is a PowerShell function that creates a definitions folder with the correct folder structure and blank global settings. It includes synopsis, description, example, cmdlet binding, and parameters sections. The code uses New-Item cmdlets to create directory structures and files like 'policyAssignments', 'policySetDefinitions', 'policyDefinitions', and 'policyDocumentations'. It also handles cases where the root folder might not exist. The script ends with a schema URL and a command to set content to a global settings file.

```
<#
.SYNOPSIS
Creates a definitions folder with the correct folder structure and blank global settings
.DESCRIPTION
Creates a definitions folder with the correct folder structure and blank global settings
.EXAMPLE
New-EPACDefinitionFolder -DefinitionsRootFolder = "Definitions"
    Scaffold a definitions folder called "Definitions"
#>
[CmdletBinding()]
Param ([string]$DefinitionsRootFolder = "Definitions")
if (!(Test-Path $DefinitionsRootFolder)) {
    New-Item -ItemType Directory -Name $DefinitionsRootFolder
    "policyAssignments", "policySetDefinitions", "policyDefinitions", "policyDocumentations"
        New-Item -ItemType Directory -Path $DefinitionsRootFolder\$_
}
$ct = @'
{
    "$schema": "https://raw.githubusercontent.com/Azure/enterprise-azure-policy-as-code/main/
'@
$ct | Set-Content -Path $DefinitionsRootFolder\global-settings.jsonc
```

Enterprise Azure Policy as Code

Key advantages of using Azure Policy as code.

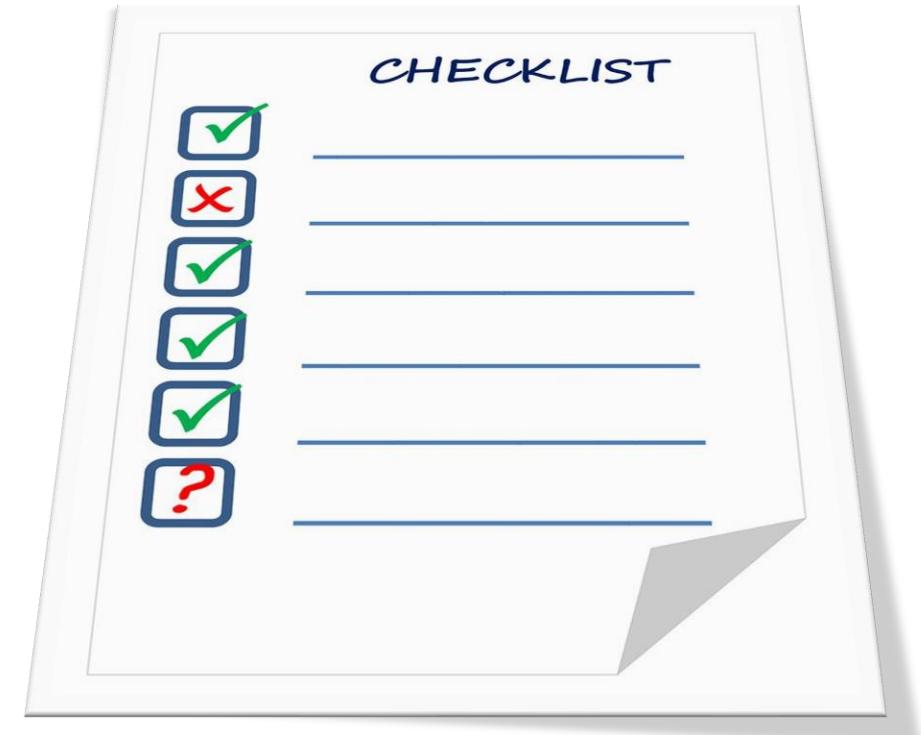
- Shifting from manually managing each policy definition in the Azure Portal or through the various SDKs to something more manageable and repeatable at scale.
- Integrates with current Infrastructure as code frameworks like Bicep, Terraform and ARM Templates.
- Integrates with DevOps where Azure Policy as Code is essentially the combination of IaC and DevOps, where you keep your Policy definitions in source control and whenever a change is made, it's tested and validated.
- Validation in CI/CD workflows, where you can validate deployments and changes on the policies, assignments etc, before they are applied.
- Desired state and source of truth for Azure Policy deployments.



Enterprise Azure Policy as Code

Who should use Enterprise Azure Policy as code

- Mainly designed for organizations with large number of policies, policy sets and assignments.
- Can be used in a multi-tenant/environment setup.
- Can be combined with Azure Landing Zone Policy implementations.
- Smaller environments can benefit from using EPAC, but it depends on their maturity of DevSecOps.
- Direct Implementation through Azure Lading Zones Bicep or Terraform might be a better choice for smaller environments.



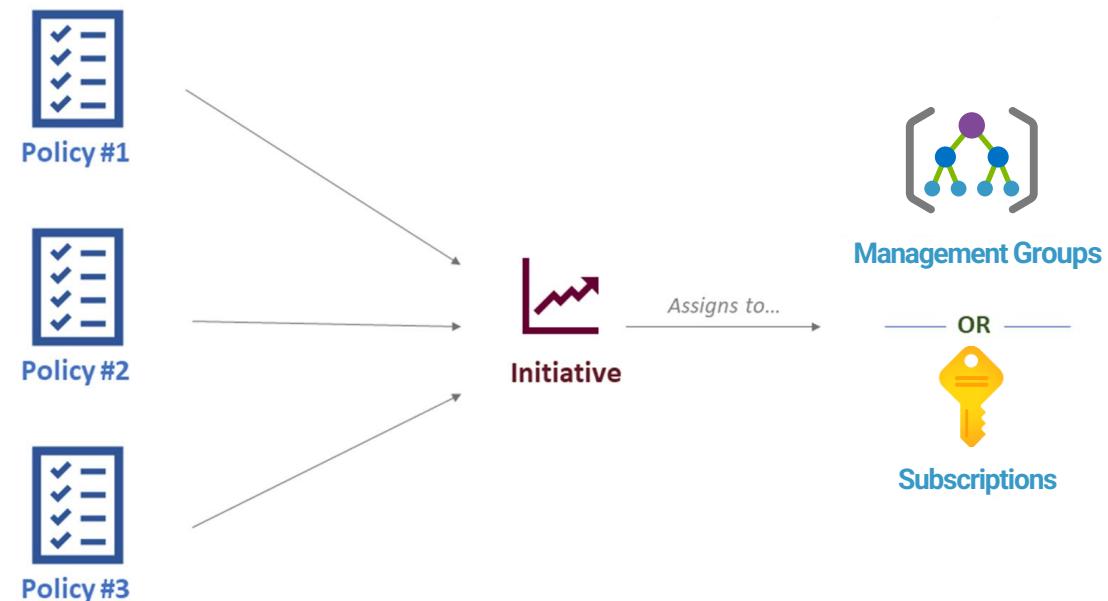


Getting started with Enterprise Azure Policy as Code

Getting started with Enterprise Azure Policy as Code

Desired state strategy and use cases

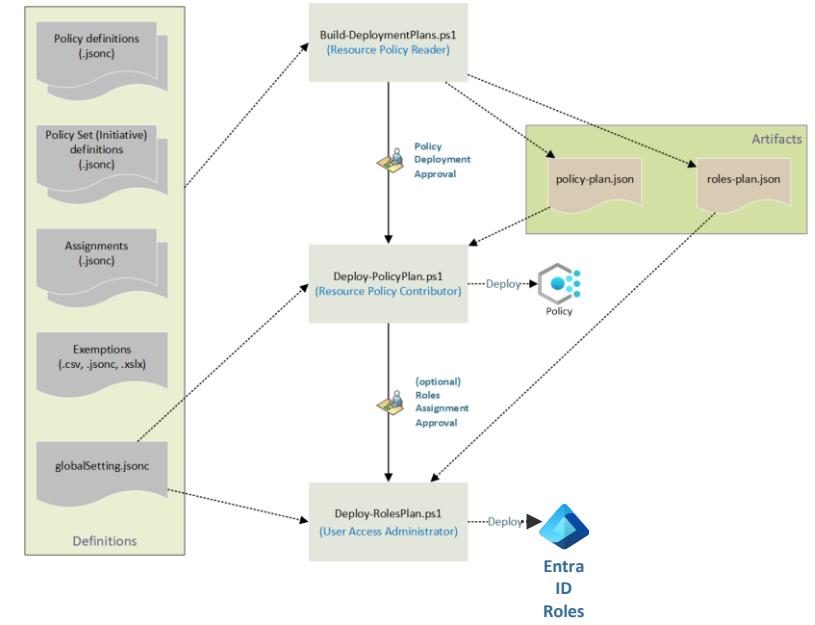
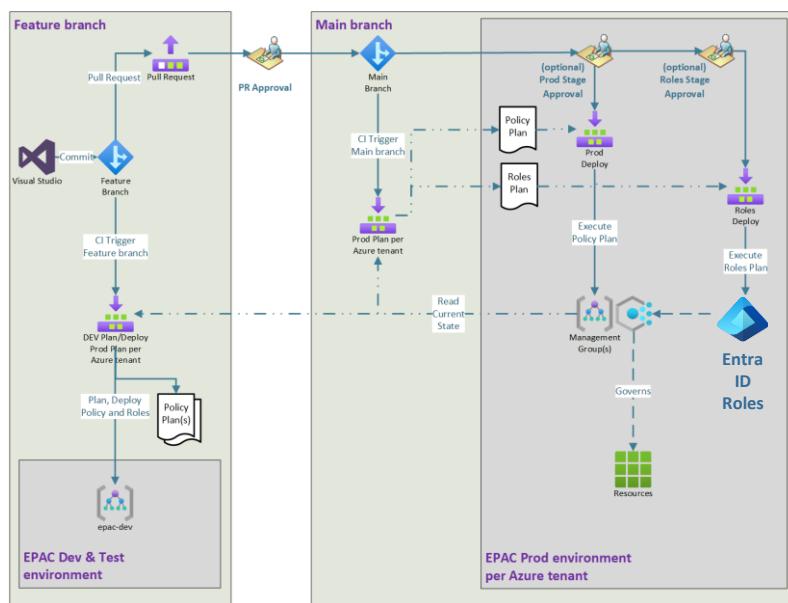
- Different ways of adopting and start using EPAC, whether you are planning to use it in the beginning or transition your already deployed policies into the EPAC framework.
- Primary use cases
 - One centralized team manages all policies in one or more tenants where desired state is set to full deployment and EPAC is the source of all policy resources.
 - A team is transitioning to EPAC while preserving existing policy resources, where desired state is set to "ownedOnly" to only remove or manages the policies that already has been transitioned to the EPAC environment.
- Other use cases
 - Multiple teams manage policies at the same scope in tenant, where the metadata "pacOwnerId" is used to identify who the owner of each policy resource



Getting started with Enterprise Azure Policy as Code

Understanding the Deployment workflow.

- The deployment workflow is intended to be used with CI/CD Pipelines, with proper flow and approval stages.
- Can be run manually by using the EnterprisePolicyAsCode PowerShell Module to create a semi-automated EPAC Solution this is useful when CI/CD environment is not yet available.



Azure DevOps Pipeline details:

- Triggered by:** Repository and version: epac-development, Branch: main, Commit ID: 7c3c11c.
- Stages:**
 - DEV Plan, Deploy Pol... (1 job completed, 1 artifact)
 - Tenant1 Plan - Feature... (1 job completed, 1 artifact)
 - Tenant1 Plan - Main ... (Skipped)
 - Tenant1 Deploy Policy (Skipped)
 - Tenant1 Deploy Role ... (Skipped)

Azure DevOps Pipeline details:

- Triggered by:** Repository and version: epac-development, Branch: main, Commit ID: cee50fe.
- Stages:**
 - DEV Plan, Deploy Pol... (Skipped)
 - Tenant1 Plan - Feature... (Skipped)
 - Tenant1 Plan - Main ... (1 job completed, 1 artifact)
 - Tenant1 Deploy Policy (Waiting)
 - Tenant1 Deploy Role ... (Not started)

Azure DevOps Pipeline details:

- Triggered by:** Repository and version: epac-development, Branch: main, Commit ID: cee50fe.
- Stages:**
 - DEV Plan, Deploy Pol... (Skipped)
 - Tenant1 Plan - Feature... (Skipped)
 - Tenant1 Plan - Main ... (1 job completed, 1 artifact)
 - Tenant1 Deploy Policy (1 job completed, 1 check passed)
 - Tenant1 Deploy Role ... (1 job completed, 1 check passed)

DEMO

Getting Started

Start using, testing and deploying the first policy with EPAC

DEMO

ALZ Policy Integration

Transitioning from Terraform CAF to EPAC Managed Policies
Strategy: Full deployment

Slides & code used in the demos will be shared afterwards
[presentations/mvp-dagen-2023 · haflidif/presentations \(github.com\)](https://github.com/haflidif/presentations)

What did we learn from this session.

To refresh your memory

- What Enterprise Azure Policy as Code (EPAC) is.
- What some of the key advantages of using Azure Policy as code are.
- Who should use the Enterprise Azure Policy as code. (EPAC)
- **DEMO TIME!** 😎
 - Getting started with EPAC
 - Full transitioning from ALZ Policies within the Terraform CAF Module to EPAC Managed Policies.



Slides & code used in the demos will be shared afterwards
[presentations/mvp-dagen-2023 · haflidif/presentations \(github.com\)](https://github.com/haflidif/presentations)

?



Useful links to Start exploring Enterprise Azure Policy as Code

- [Deploy Azure landing zones - Alternative platform deployment for policies - Azure Architecture Center | Microsoft Learn](#)
- [Overview - Enterprise Policy As Code \(EPAC\) \(azure.github.io\)](#)
- [Desired State Strategy - Enterprise Policy As Code \(EPAC\) \(azure.github.io\)](#)
- [ALZ Policy Integration - Enterprise Policy As Code \(EPAC\) \(azure.github.io\)](#)
- [Azure Enterprise Policy as Code – A New Approach - Microsoft Community Hub](#)
- [Azure Enterprise Policy as Code – Azure Landing Zones Integration - Microsoft Community Hub](#)



Follow me on:

X [@haflidif](#) | in [in/haflidif](#) | [www.azureviking.com](#) | [haflidif](#) | MVP-Dagen



MVP-Dagen 2023





Tusen takk! MVP-Dagen

Slides & code used in the demos will be shared afterwards
[presentations/mvp-dagen-2023 · haflidif/presentations \(github.com\)](https://github.com/haflidif/presentations)