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.

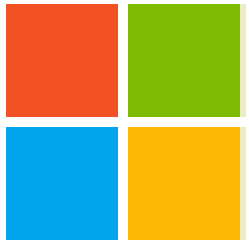
AZURE VIKING
Cloud Security
EST 2022

Microsoft Security
USER GROUP

Follow me on:

@haflidif | in/haflidif | azureviking.com | haflidif

MVP-Dagen



Microsoft

Evidi


blinQ


CloudWay


amesto
Fortytwo


INNOFACTOR®


03C


POINT : TAKEN

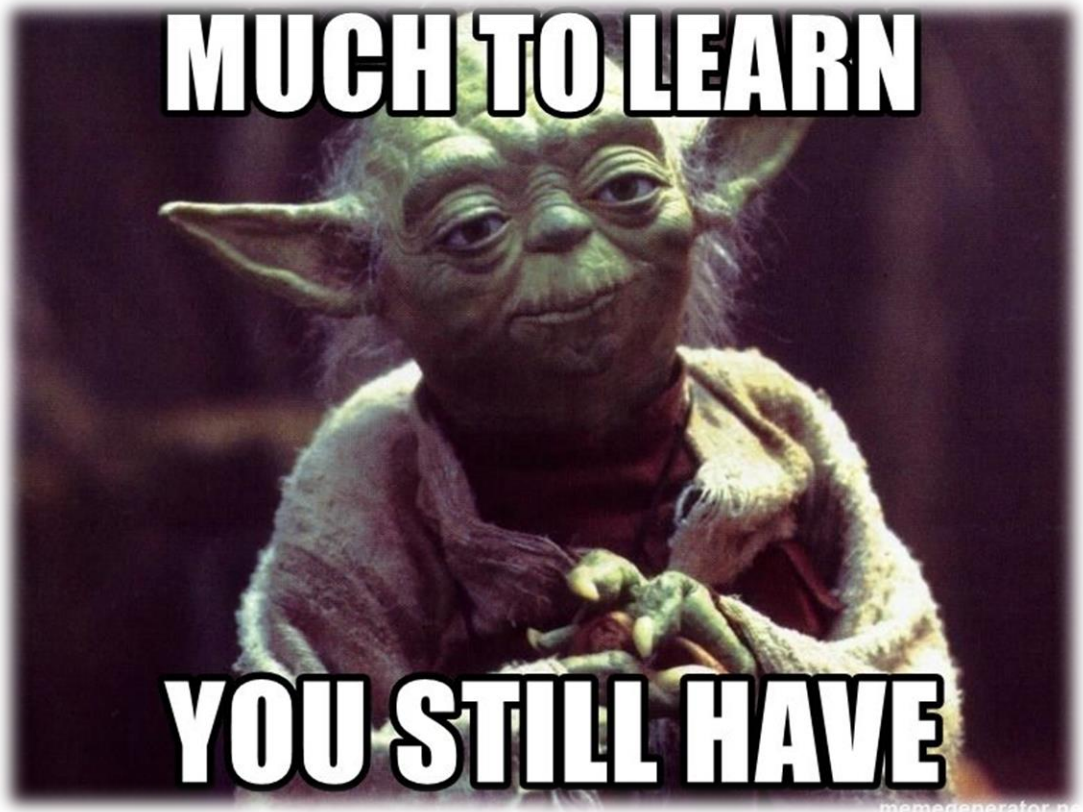

iver

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)]

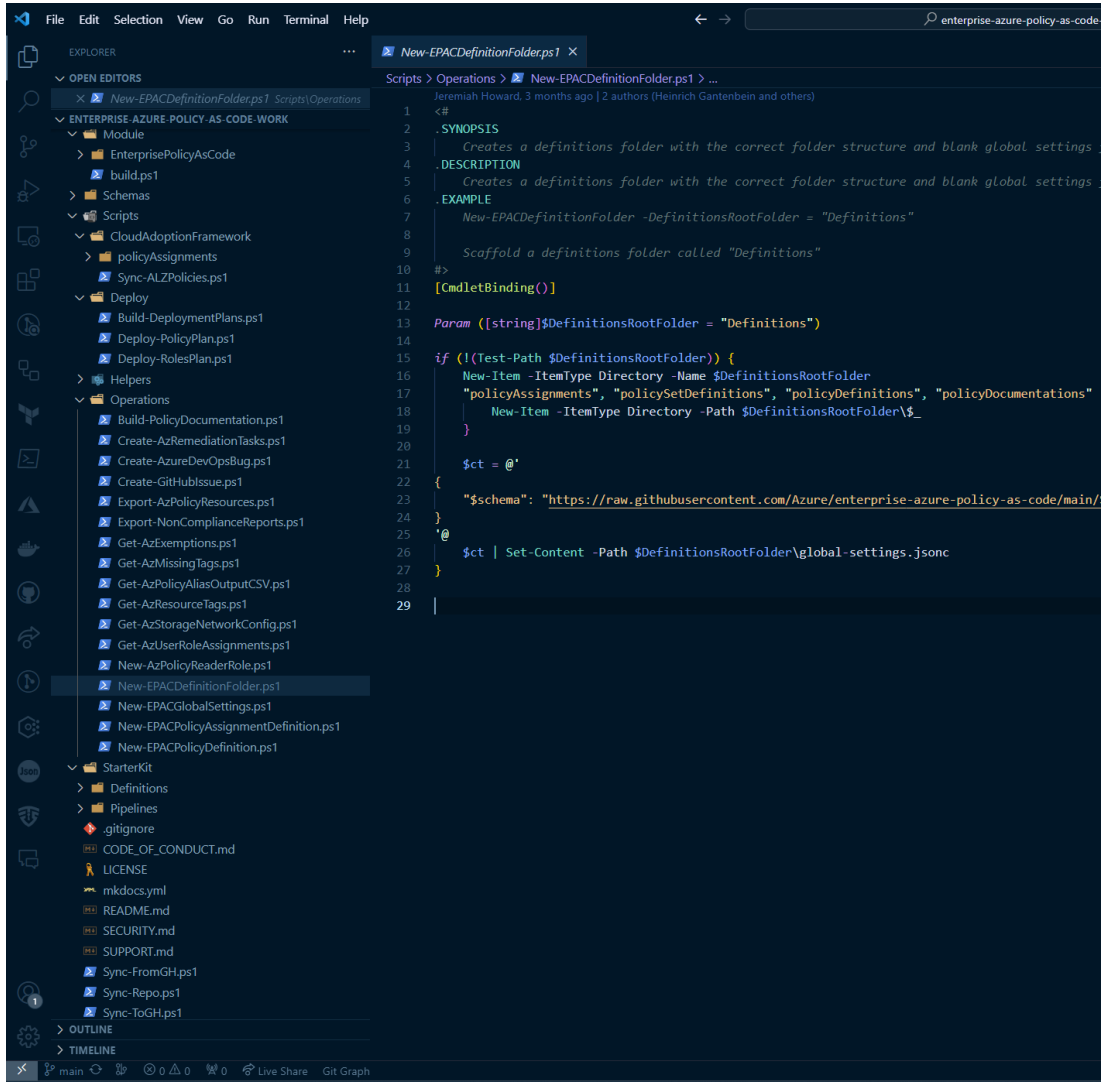
MVP-Dagen


Enterprise
Azure Policy as code ?

Enterprise Azure Policy as Code

What is it ?

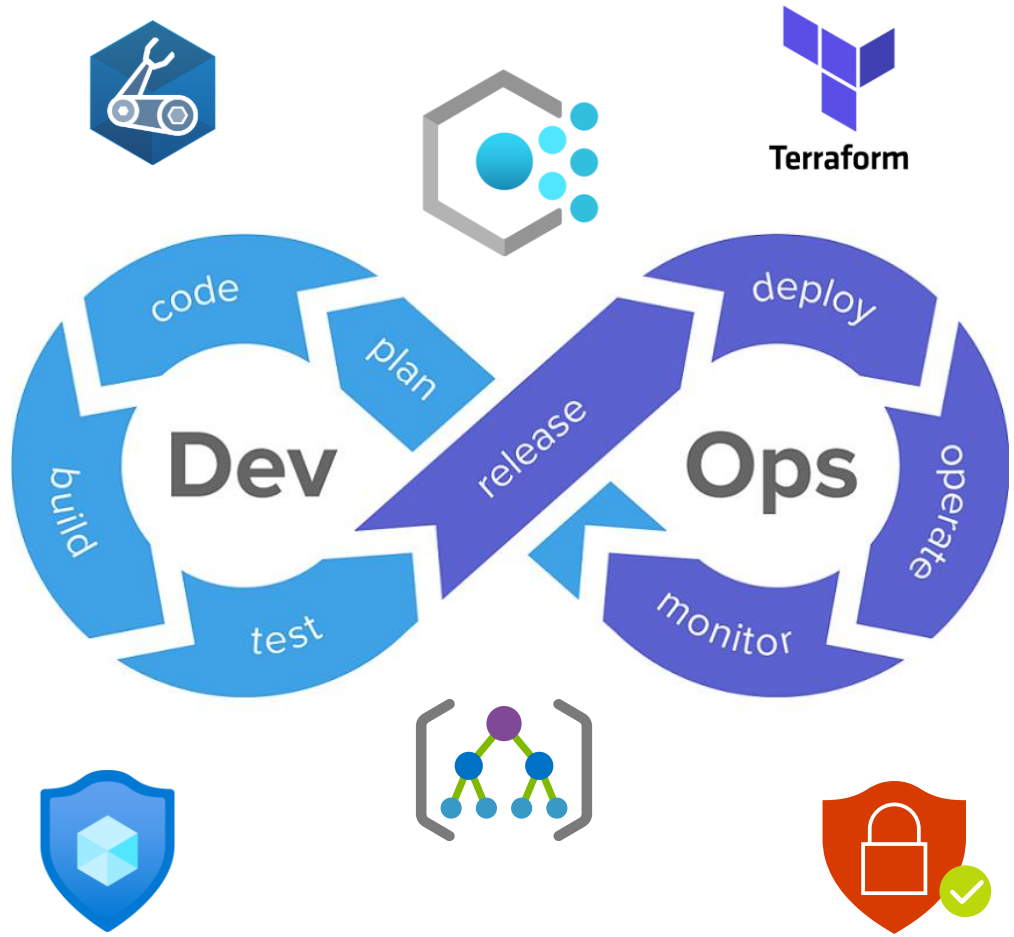
- Set of PowerShell Scripts and modules.
- Can manage Azure policies, policy sets, assignments, exemptions and role assignments.
- Supported in CI/CD based systems or in a semi-automated way.
- Integrates well with Cloud Adoption Framework and Azure Landing Zone.
- Supports multi-tenant/environments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



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

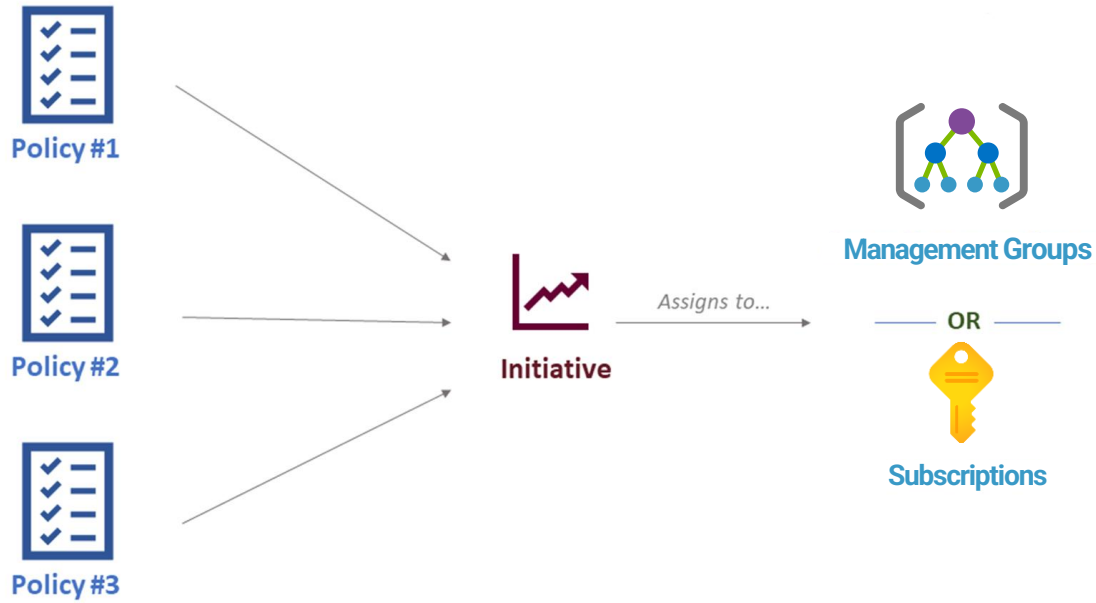
- Mainly designed for organizations with large number of polices, policy sets and assignments.
- Can be used in a multi-tenant/environment setup.
- Can be combined with Azure Landing Zone Policy implementations.
- Smaller environments can benefit from using EPAC, but it depends on their maturity of DevSecOps.
- 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

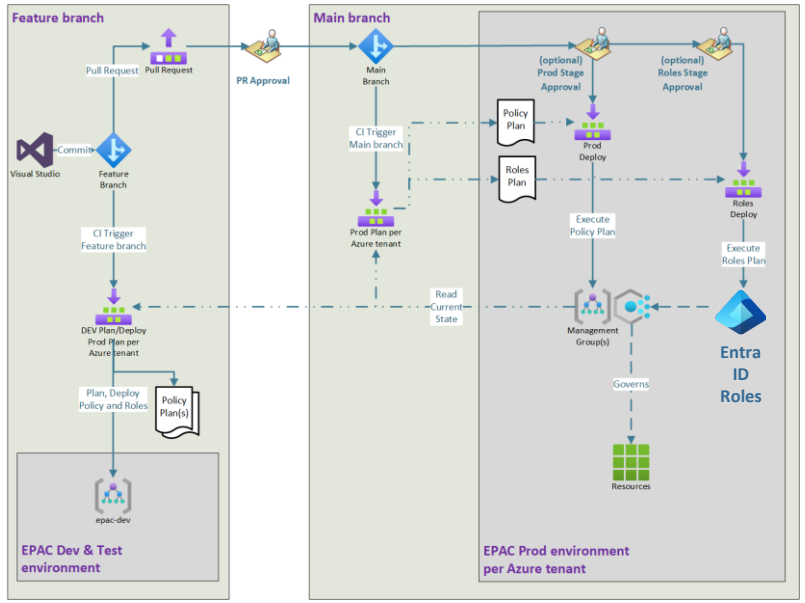
- Different ways of adopting and start using EPAC, whether you are planning to use it in the beginning or transition your already deployed policies into the EPAC framework.
- Primary use cases
  - One centralized team manages all policies in one or more tenants where desired state is set to full deployment 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

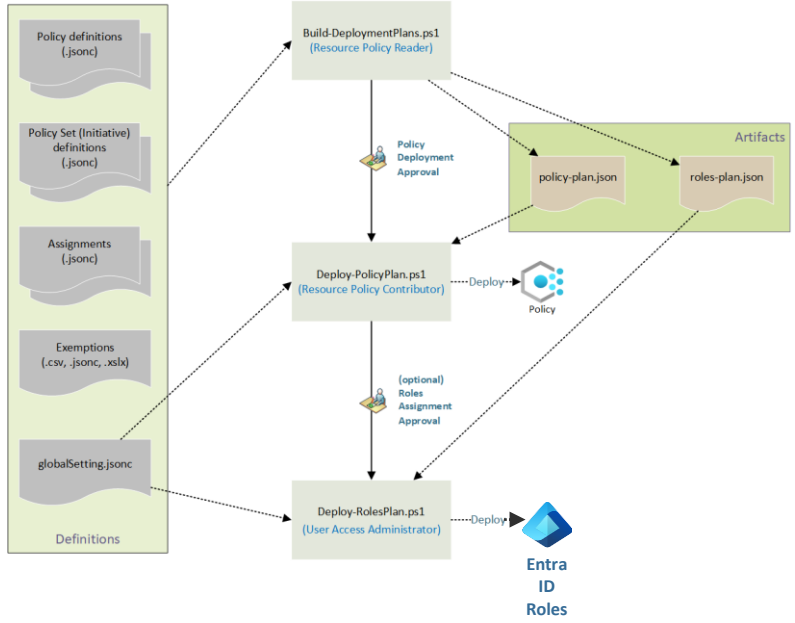


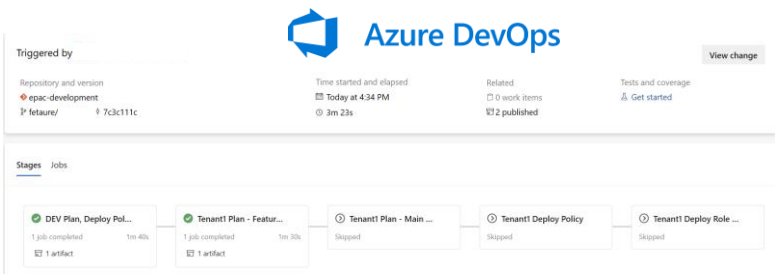
Getting started with Enterprise Azure Policy as Code

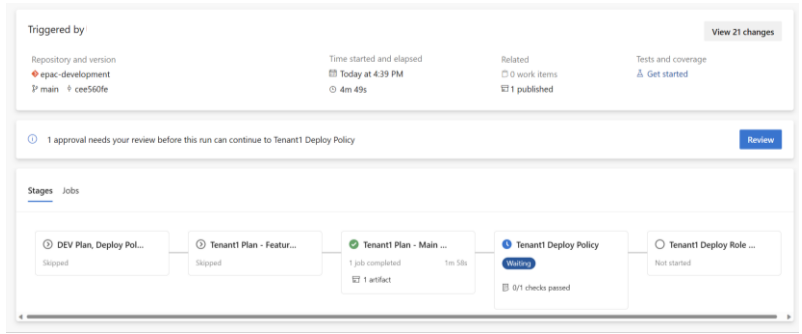
Understanding the Deployment workflow.

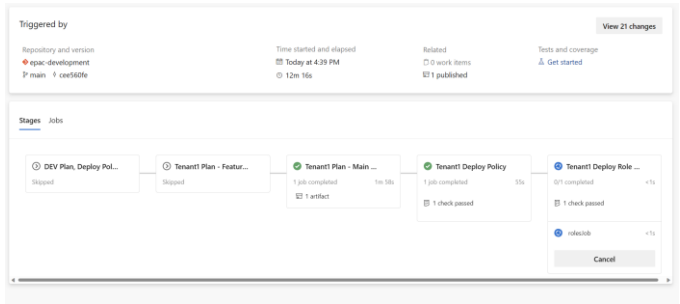
- The deployment workflow is intended to be used with CI/CD Pipelines, with proper flow and approval stages.
- Can be run manually by using the EnterprisePolicyAsCode PowerShell Module to create a semi-automated EPAC Solution this is useful when CI/CD environment is not yet available.











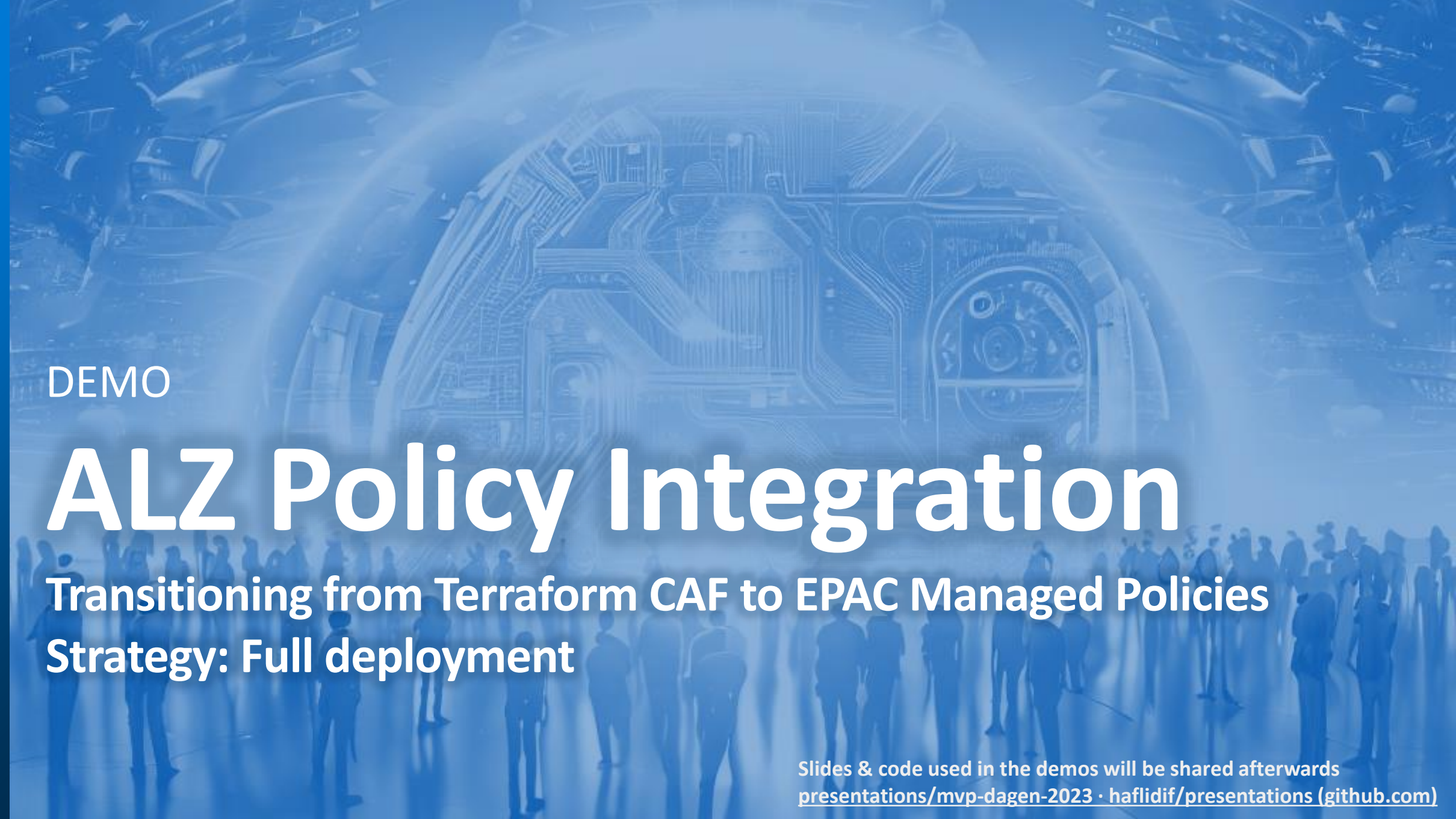
MVP-Dagen

DEMO

Getting Started

Start using, testing and deploying the first policy with EPAC

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



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)

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)

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

Cloud Security AZURE VIKING EST 2022

Microsoft Security USER GROUP

Follow me on:

@haflidif | in/haflidif | azureviking.com | haflidif

MVP-Dagen


MVP-Dagen 2023

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