Microsoft Azure

Azure Governance saai, maar absoluut nodig!

Daniël Etten

Daniël Etten

Premier Field Engineer bij Microsoft

🐦 @danieletten

www heyazureguy.com

Disclaimer

Deze presentatie is gebaseerd ***persoonlijke*** verhalen, ervaringen, demo’s en adviezen van de spreker en is geen visie van Microsoft.

Nieuwe on premises omgeving

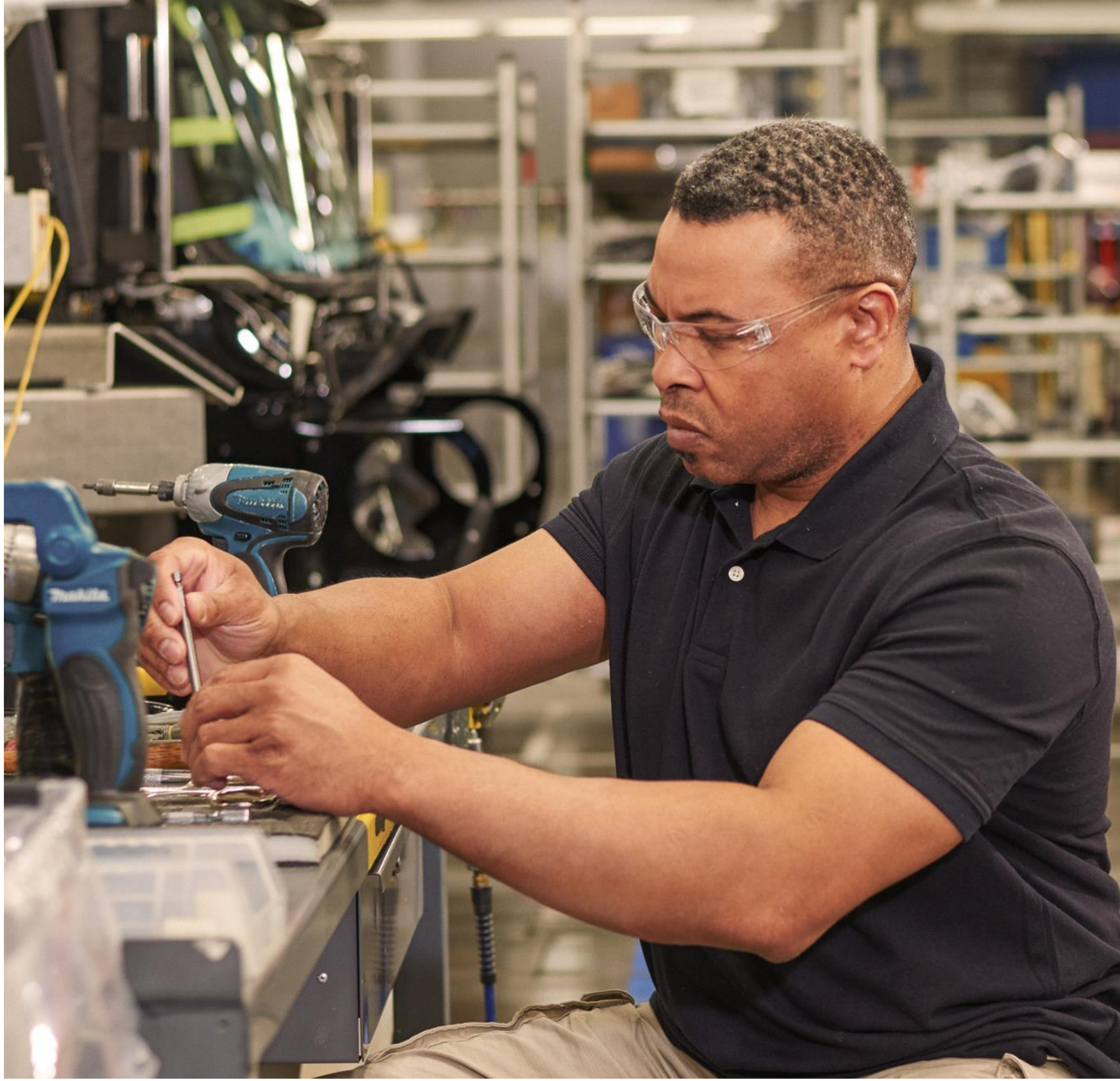
- Locatie
- Kosten
- Management
- Beveiliging

Nieuwe Azure omgeving

- Locatie
- Kosten
- Management
- Beveiliging

“Governance is niet om mensen te belemmeren in hun werkzaamheden.

Het is net als het plaatsen van een vangnet in de bouw om veilig te werken.”



Governance

- Oorsprong in Latijn (Guberno)
- Betekenis: Sturen

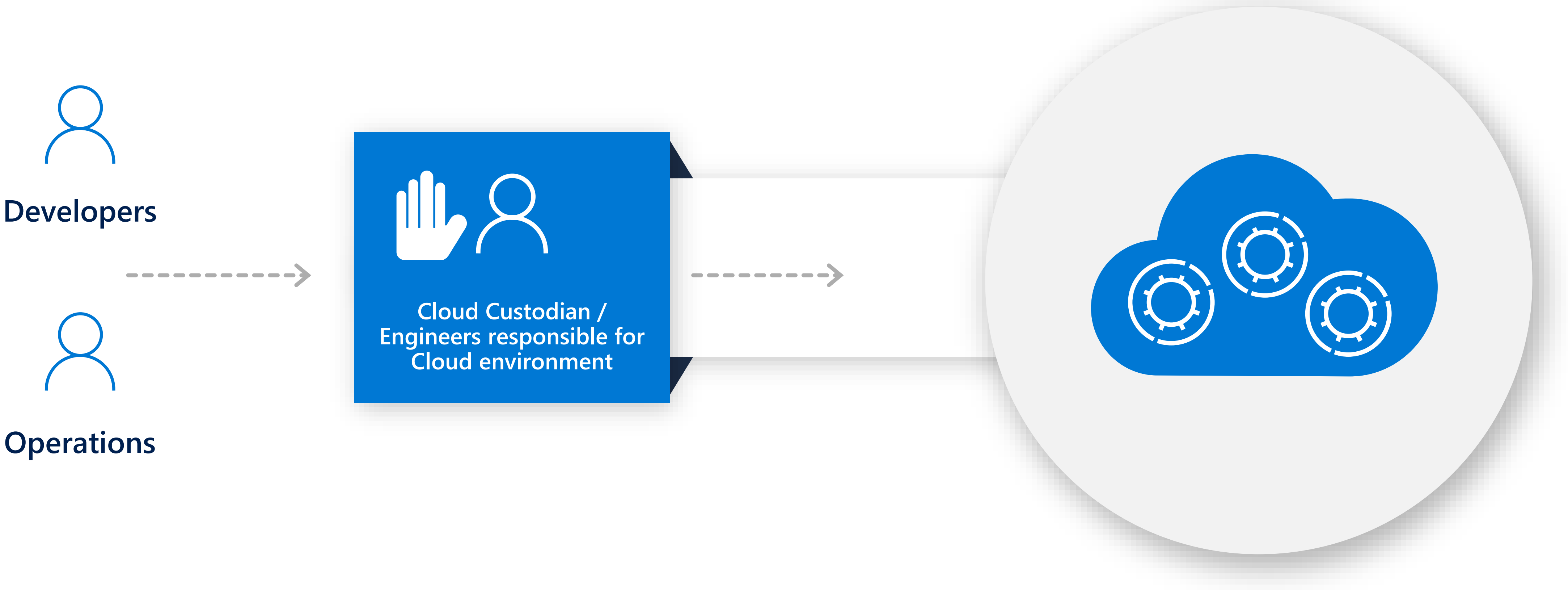
- Wijze van besturen

Governance

Data honderdduizenden patiënten in stilte naar Google verhuisd

Traditional approach

- Block Dev/Ops from directly accessing the cloud (portal/api/cli) to attain control



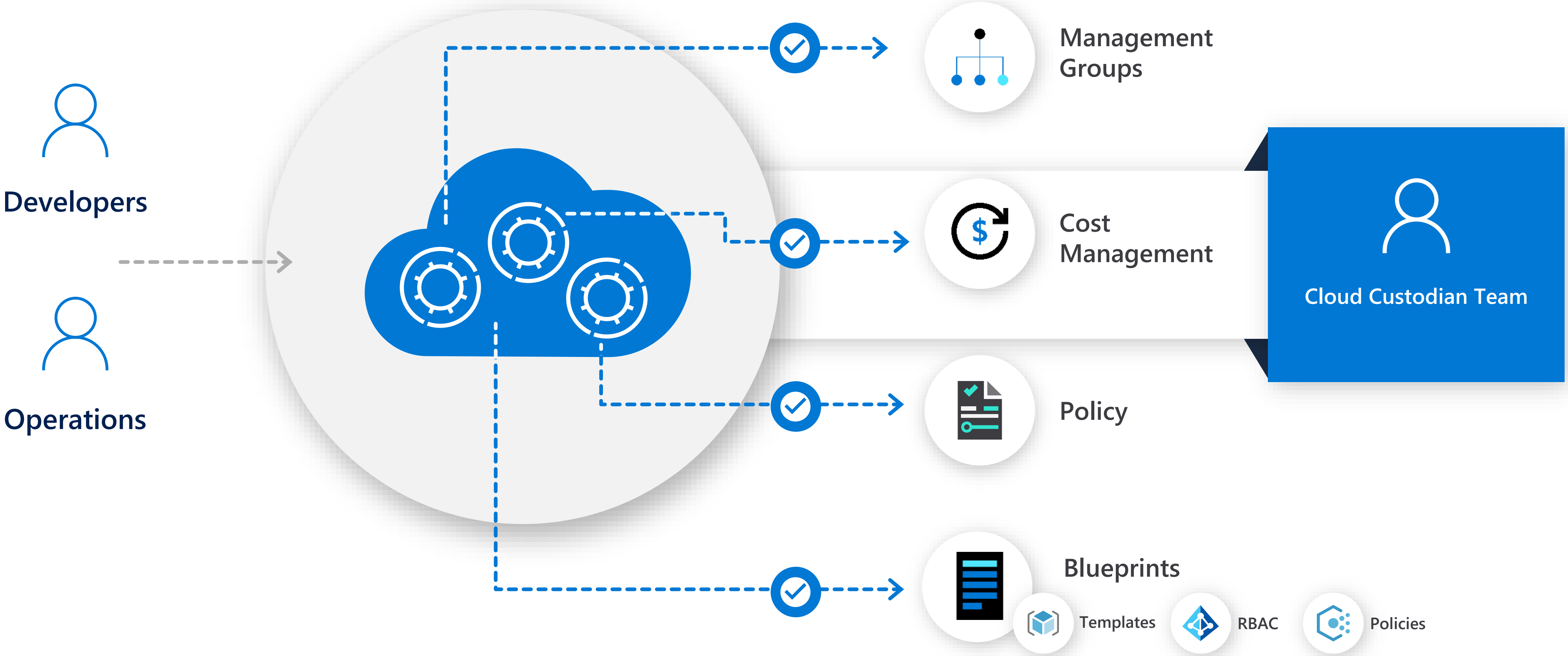
Developers

Operations

Cloud Custodian / Engineers responsible for Cloud environment

SPEED + CONTROL

- Cloud-native governance -> removing barriers to compliance and enabling velocity



What does it mean to govern in the cloud?

Right people

Right resources

Right configurations

Governance for the cloud

Native platform capabilities to ensure compliant use of cloud resources

Management Group	**Policy**	**Blueprints**	**Resource Graph**	**Cost Management**
Define organizational hierarchy	Real-time enforcement, compliance assessment and remediation	Deploy and update cloud environments in a repeatable manner using composable artifacts	Query, explore & analyze cloud resources at scale	Monitor cloud spend and optimize resources
Hierarchy	Control	Environment	Visibility	Consumption

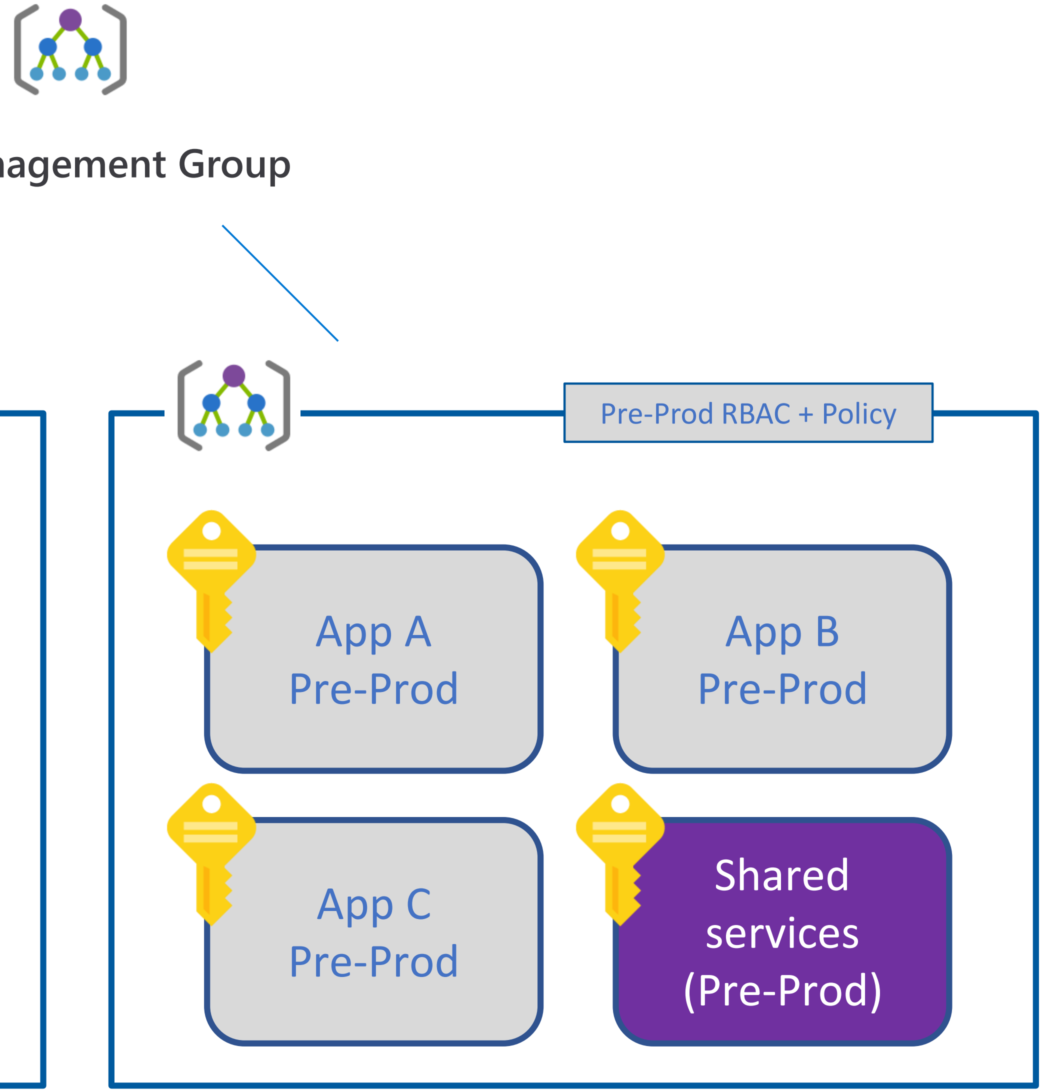
Subscription modeling strategy

What defines an app in your organization?

Subscription

Management Group

Microsoft Recommended



Org Management Group

Prod RBAC + Policy

App A Prod

App B Prod

App C Prod

Shared services (Prod)

Pre-Prod RBAC + Policy

App A Pre-Prod

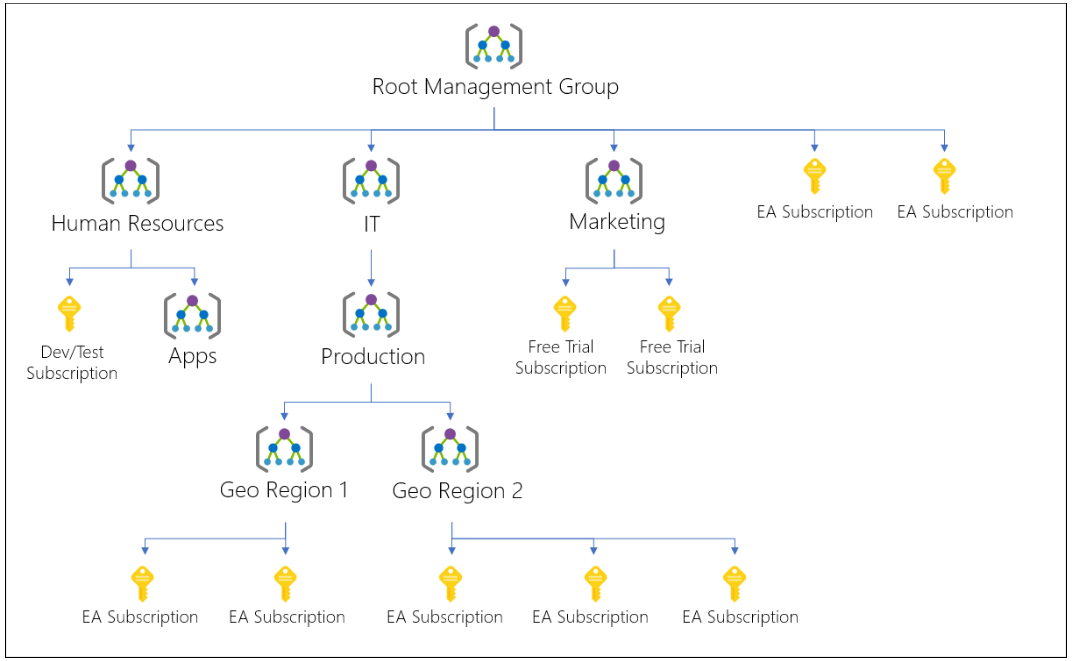
App B Pre-Prod

App C Pre-Prod

Shared services (Pre-Prod)

Management Group best practices

- Define your hierarchy based on organization and environment type (prod, pre-prod, etc. / internal, external or departments)
- The root MG is for global configuration
  - Be careful with MG level assignments as they will cascade through large chunks of your hierarchy
- Try not to repeat yourself. Assign common policies and rbac higher up in your hierarchy
- Built-in RBAC roles for MGs (MG contributor, MG reader)
  - Need subscription owner access to move to another MG



RBAC best practices

- Follow the principle of granting the least privilege required to do the expected work
- Inherited to all children of the assigned scope
  - Use Management Groups to assign roles across multiple subscriptions
- Learn and use Managed Identities where possible

Demo Management Groups & RBAC

Governance for the cloud

Native platform capabilities to ensure compliant use of cloud resources

Management Group	Policy	Blueprints	Resource Graph	Cost Management
Define organizational hierarchy	Real-time enforcement, compliance assessment and remediation	Deploy and update cloud environments in a repeatable manner using composable artifacts	Query, explore & analyze cloud resources at scale	Monitor cloud spend and optimize resources
Hierarchy	Control	Environment	Visibility	Consumption

Policies

- Beleidsregels
  - Resources voldoen aan beleid
  - Bestaande en nieuwe resources
- Bijvoorbeeld
  - Locatie – SKU’s verbieden
  - Naamgeving - Tags

Policy rule

- **Logical operators**
- "not": {condition or operator}
- "allOf": [{condition or operator},
- {condition or operator}]
- "anyOf": [{condition or operator},
- {condition or operator}]

Conditions

"equals": "value"

"like": "value"

"match": "value"

"contains": "value"

"in": ["value1","value2"]

"containsKey": "keyName"

"exists": "bool"

- **Fields**
- name
- kind
- type
- location
- tags
- tags.*
- property aliases

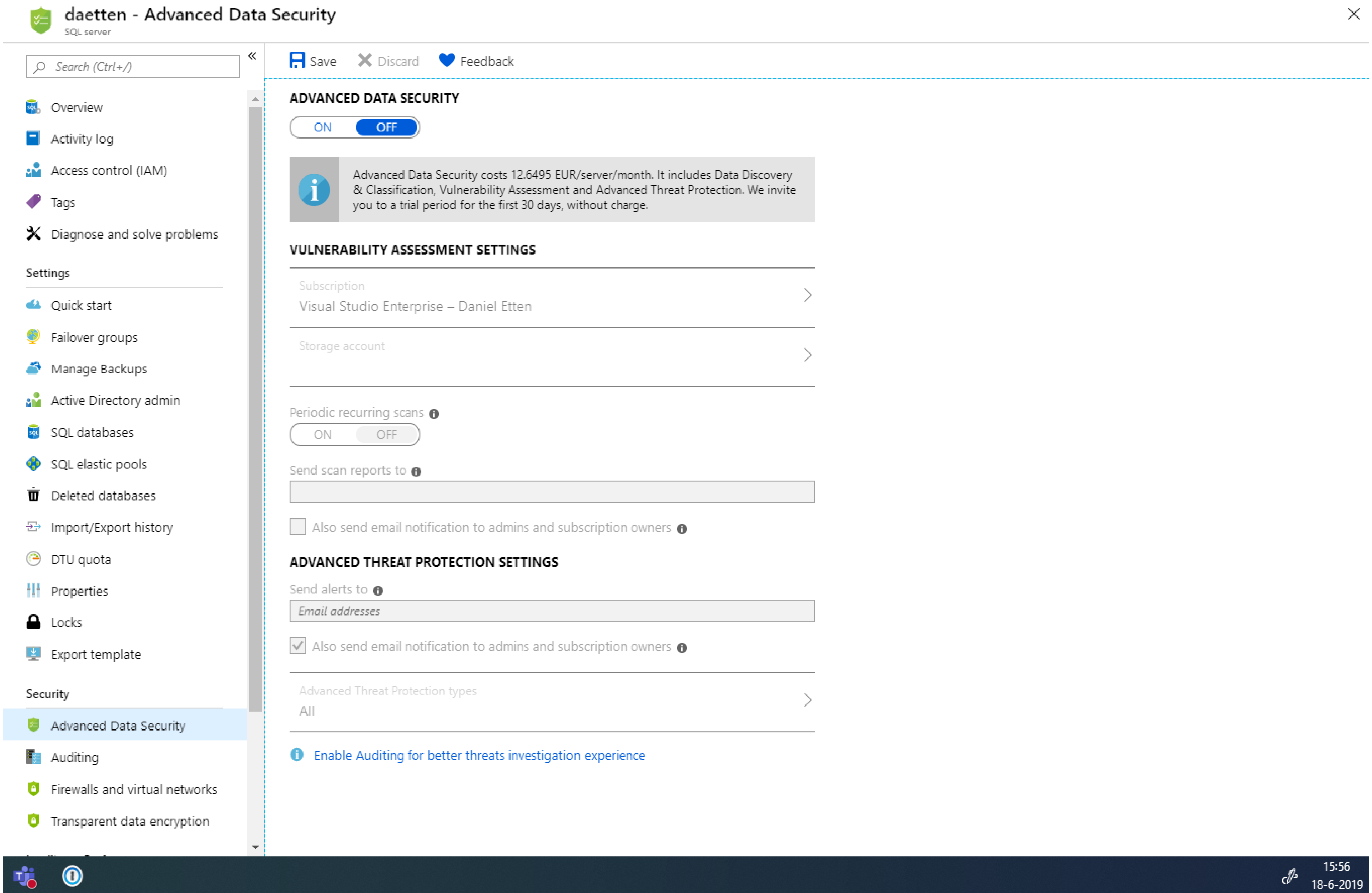
Effects

Deny,
Audit,
Append,
AuditIfNotExists,
DeployIfNotExists

Policy rule

```
$policy = New-AzureRmPolicyDefinition -Name
costCenterTagPolicyDefinition -Description "Policy to deny
resource creation if no costCenter tag is provided" -Policy '{
  "if": {
    "not" : {
      "field" : "tags",
      "containsKey" : "costCenter"
    }
  },
  "then" : {
    "effect" : "deny"
  }
}'
```

Demo Policies



daetten - Advanced Data Security

SQL server

ADVANCED DATA SECURITY

ON [✓ OFF]

Advanced Data Security costs 12.6495 EUR/server/month. It includes Data Discovery & Classification, Vulnerability Assessment and Advanced Threat Protection. We invite you to a trial period for the first 30 days, without charge.

VULNERABILITY ASSESSMENT SETTINGS

Subscription
Visual Studio Enterprise – Daniel Etten

Storage account

Periodic recurring scans
ON [✓ OFF]

Send scan reports to

□ Also send email notification to admins and subscription owners

ADVANCED THREAT PROTECTION SETTINGS

Send alerts to
Email addresses

☑ Also send email notification to admins and subscription owners

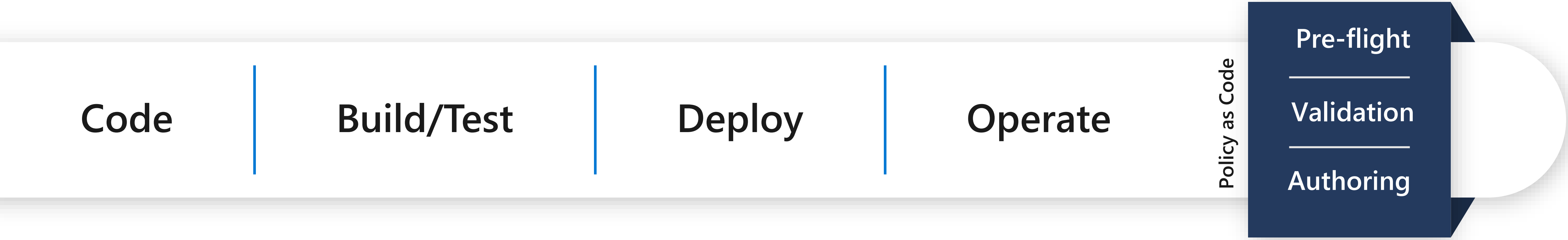
Advanced Threat Protection types
All

Enable Auditing for better threats investigation experience

Policies integration into Azure DevOps

Enforce policies as part of the development process

Shift left to deliver compliant code faster



Policy

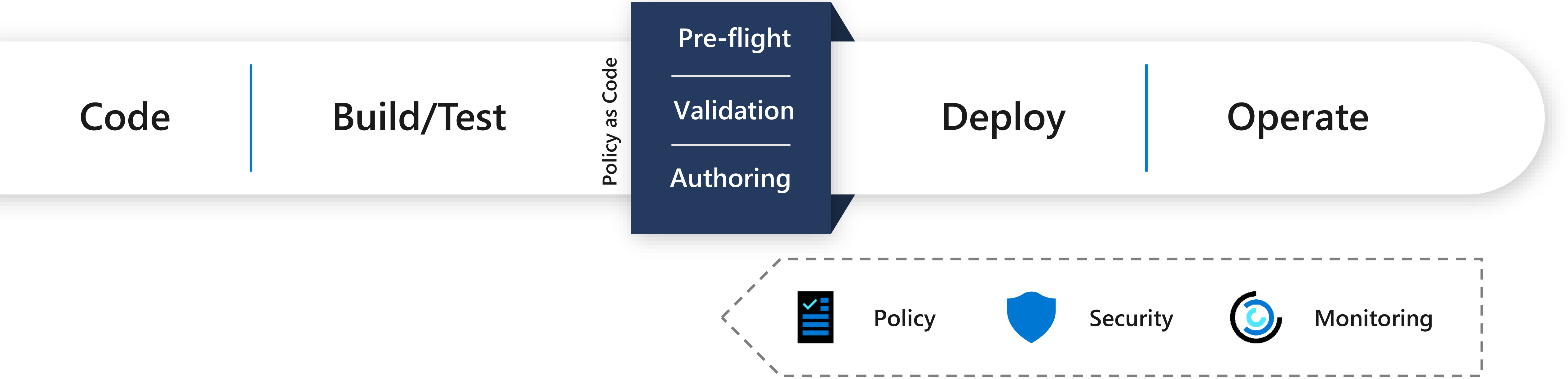
Security

Monitoring

Azure DevOps

Enforce policies as part of the development process

Shift left to deliver compliant code faster



Code

Build/Test

Policy as Code

Pre-flight

Validation

Authoring

Deploy

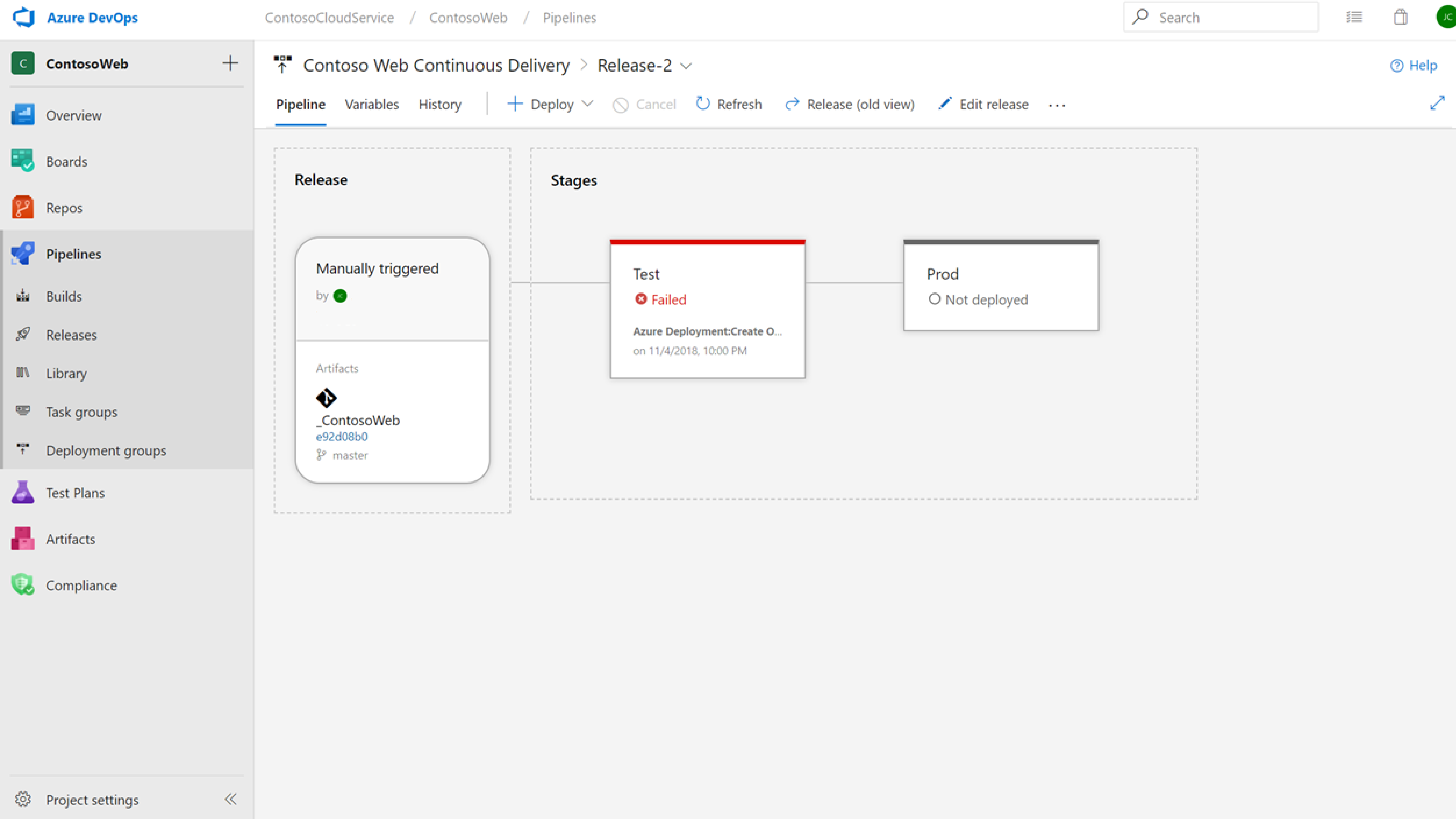
Operate

Policy

Security

Monitoring

Azure DevOps + Azure Policy



Contoso Web Continuous Delivery > Release-2

Manually triggered

by

Artifacts

_ContosoWeb

e92d08b0

master

Test

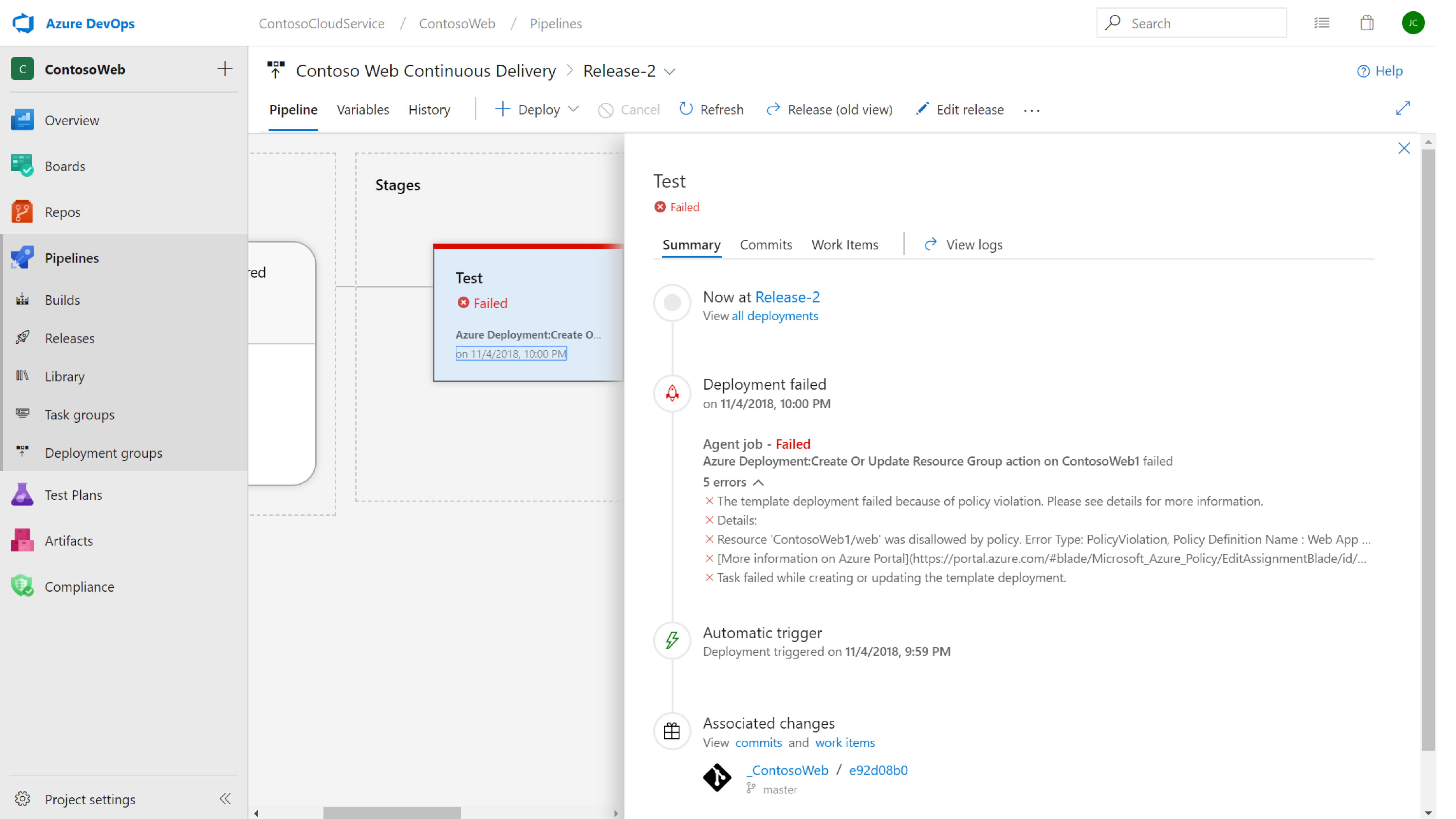
Failed

Azure Deployment:Create O...

on 11/4/2018, 10:00 PM

Prod

○ Not deployed



Test

Failed

Now at Release-2
View all deployments

Deployment failed
on **11/4/2018, 10:00 PM**

Agent job - Failed
Azure Deployment:Create Or Update Resource Group action on ContosoWeb1 failed

5 errors

- The template deployment failed because of policy violation. Please see details for more information.
- Details:
- Resource 'ContosoWeb1/web' was disallowed by policy. Error Type: PolicyViolation, Policy Definition Name : Web App ...
- [More information on Azure Portal](https://portal.azure.com/#blade/Microsoft_Azure_Policy/EditAssignmentBlade/id/...
- Task failed while creating or updating the template deployment.

Automatic trigger
Deployment triggered on **11/4/2018, 9:59 PM**

Associated changes
View commits and work items

_ContosoWeb / e92d08b0
master

Governance for the cloud

Native platform capabilities to ensure compliant use of cloud resources

Management Group

Define organizational hierarchy

Hierarchy

Policy

Real-time enforcement, compliance assessment and remediation

Control

Blueprints

Deploy and update cloud environments in a repeatable manner using composable artifacts

Environment

Resource Graph

Query, explore & analyze cloud resources at scale

Visibility

Cost Management

Monitor cloud spend and optimize resources

Consumption

Blueprints

Enabling quick, repeatable creation of fully governed environments

Streamline environment creation

Centralize environment creation through templates

Add resources, policies and role access controls

Track blueprint updates through versioning

Enable compliant development

Empower developers to create fully governed environments through self-service

Create multiple dev-ready environments and subscriptions from a centralize location

Leverage the integration with Azure Policy on the DevOps lifecycle

Lock foundational resources

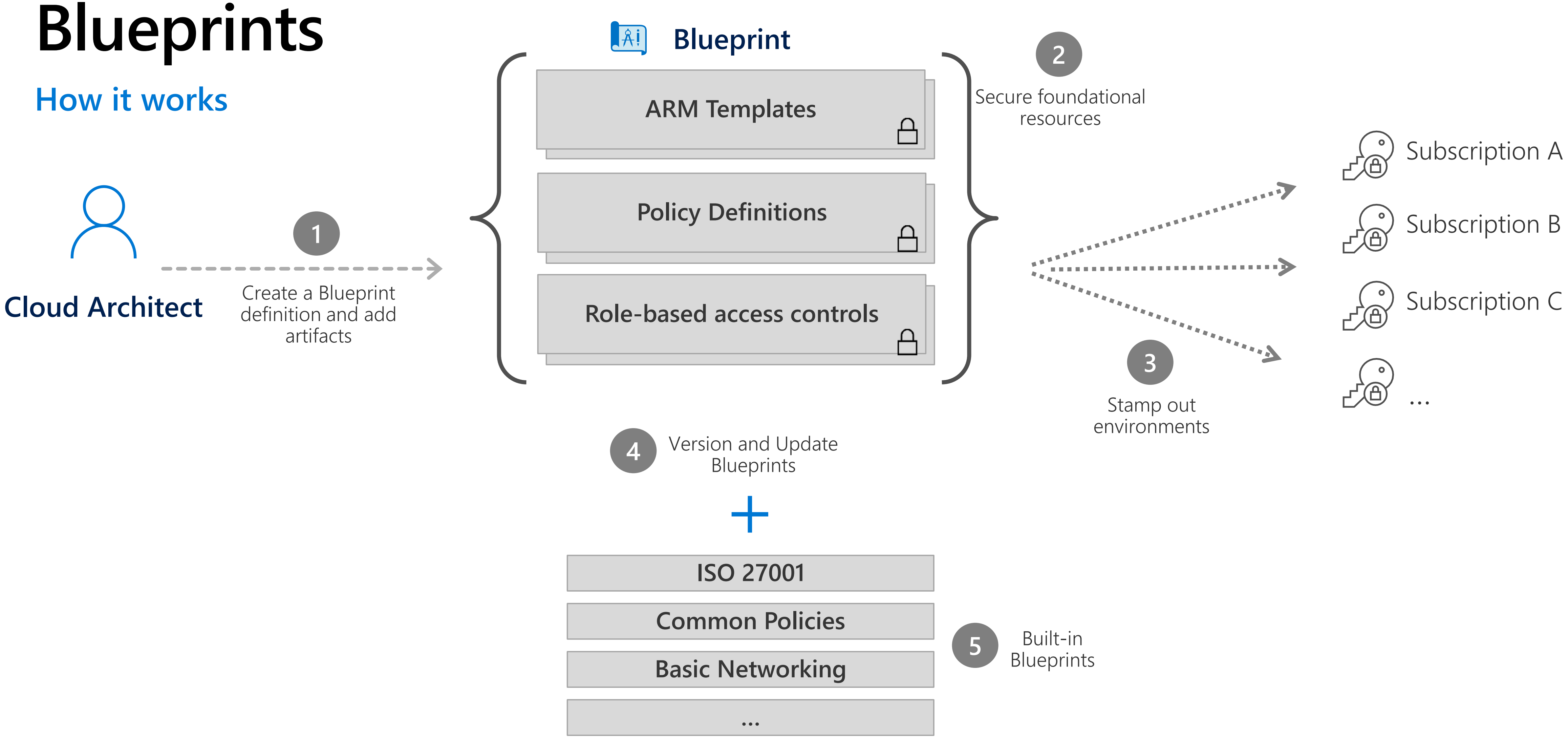
Ensure foundational resources cannot be changed by subscription owners

Manage locks through a centralize location

Update locked resource through blueprint definition updates

Blueprints

How it works



Cloud Architect

1 Create a Blueprint definition and add artifacts

Blueprint

ARM Templates

Policy Definitions

Role-based access controls

2 Secure foundational resources

3 Stamp out environments

Subscription A

Subscription B

Subscription C

…

4 Version and Update Blueprints

+

ISO 27001

Common Policies

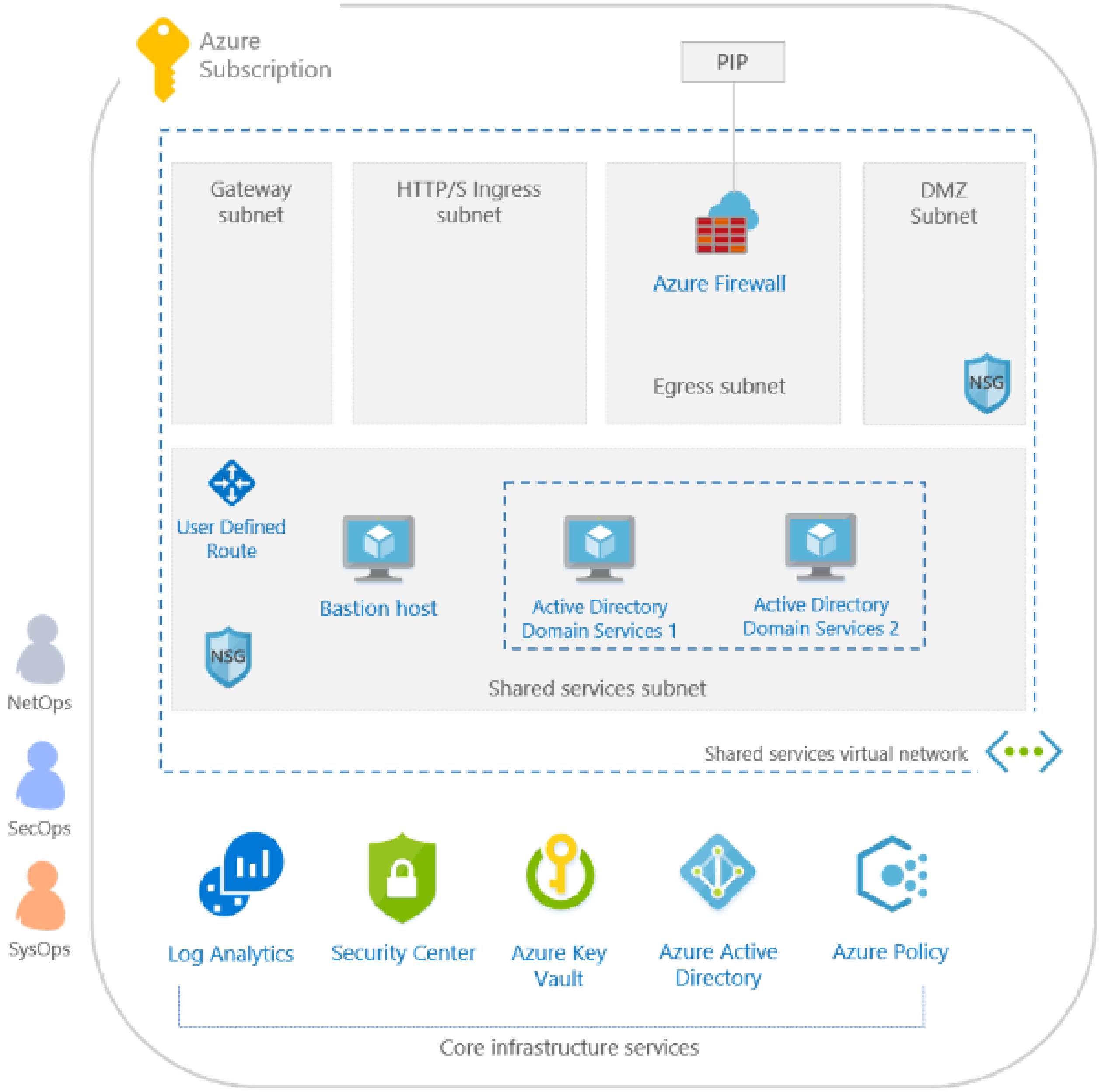
Basic Networking

…

5 Built-in Blueprints

Blueprints best pratices

- Use those built-in blueprints!
    - ISO27001: Shared Services is a great place to start for setting up a new hub subscription
- Build out blueprints incrementally
- Test by deploying to resource groups, which are easy to clean up
- Use the MG hierarchy to limit which blueprints are applicable for which sections of an organization
- Have blueprints ready to go for new engagements



Blueprints

And ARM

- ARM is the key building block
- Scaling up ARM is a challenge
    - How do you use ARM templates across 50, 100, 1,000 app teams?
    - How do you keep your templates modular for maximum re-use?
    - How do you make sure those environments stay up to date?
- Blueprints are ideal for stamping out standardized environments
    - Build out a library of different environment types

Demo Blueprints

Governance for the cloud

Native platform capabilities to ensure compliant use of cloud resources

Management Group

Define organizational hierarchy

Hierarchy

Policy

Real-time enforcement, compliance assessment and remediation

Control

Blueprints

Deploy and update cloud environments in a repeatable manner using composable artifacts

Environment

Resource Graph

Query, explore & analyze cloud resources at scale

Visibility

Cost Management

Monitor cloud spend and optimize resources

Consumption

Azure Resource Graph

Query, **explore** & **analyze** cloud resources at scale

Explore

Perform fast ad hoc **exploration** in large cloud environment

Query & Analyze

Query & analyze across all of your cloud resources at scale in seconds

Impact Assessment

Ability to **assess the impact** of applying policies in vast cloud environment

Recap Azure Governance

Native platform capabilities to ensure compliant use of cloud resources

Management Group

Define organizational hierarchy

Hierarchy

Policy

Real-time enforcement, compliance assessment and remediation

Control

Blueprints

Deploy and update cloud environments in a repeatable manner using composable artifacts

Environment

Resource Graph

Query, explore & analyze cloud resources at scale

Visibility

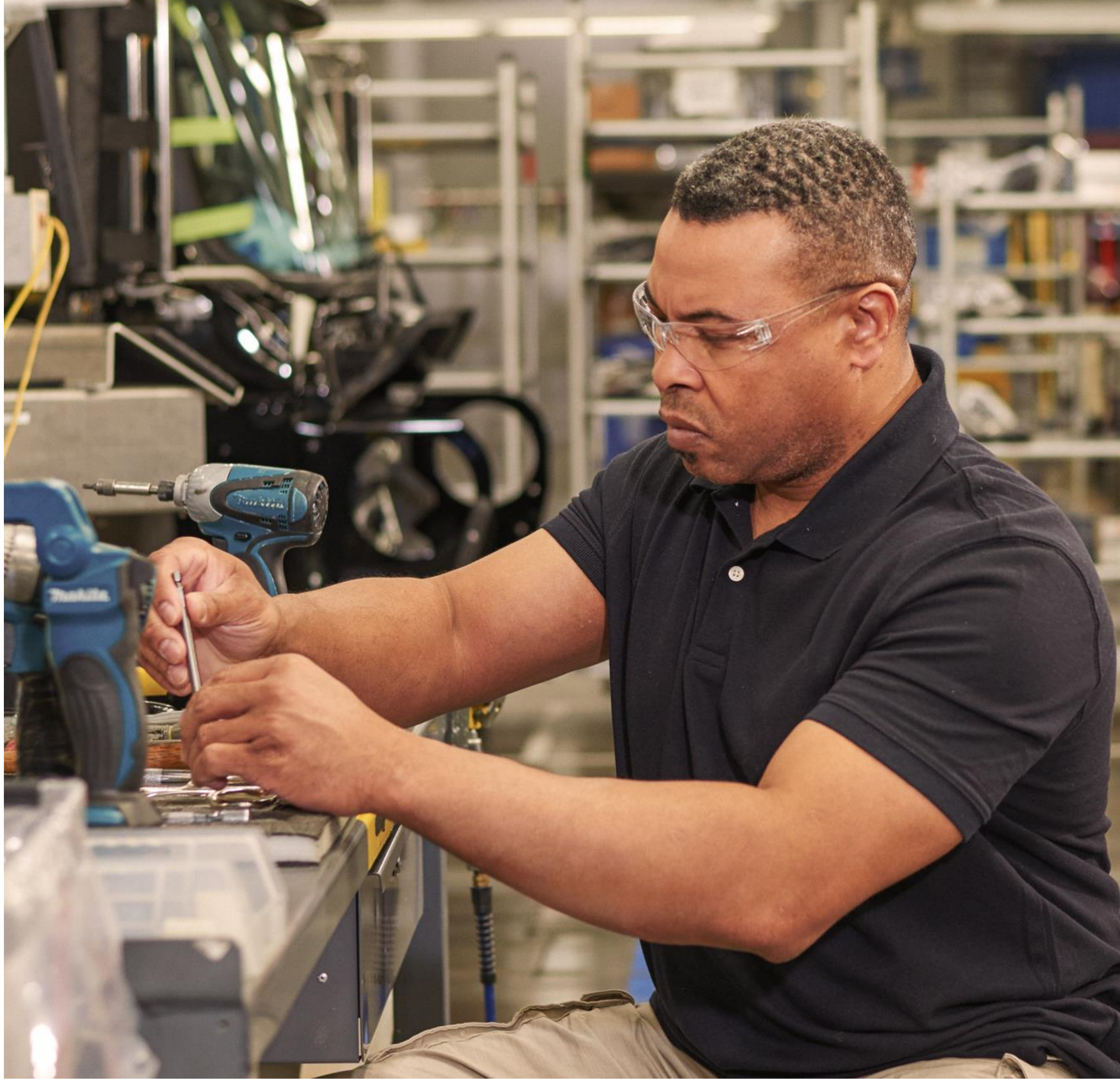
Cost Management

Monitor cloud spend and optimize resources

Consumption

“Governance is niet om mensen te belemmeren in hun werkzaamheden.

Het is net als het plaatsen van een vangnet in de bouw om veilig te werken.”



Meer weten?

- RBAC: https://aka.ms/RBACLab
- Governance: https://aka.ms/AZGovernance
- Blueprints: http://aka.ms/WhatAreBlueprints
- Policies: https://aka.ms/AzurePolicies
    - Repo: https://github.com/Azure/azure-policy/

Vind mij online:

@danieletten

heyazureguy.com

Microsoft