Azure Governance einfach gemacht mit Azure Blueprints

Gregor Reimling | Azure MVP

Orga and Main Sponsors

Hochschule
Bonn-Rhein-Sieg
University of Applied Sciences

SOLISYON

You Rock!
Sponsor

PASS Microsoft Data Platform Community
DEUTSCHLAND e.V.

Many thanks to our sponsors, without whom such an event would not be possible.

@GregorReimling

Sponsors (Gold)

ORAYLIS Business Intelligence

melissa GLOBAL INTELLIGENCE

oh22data

Quest

adesso business. people. technology.

redgate

Many thanks to our sponsors, without whom such an event would not be possible.

Sponsors continued

Silver:

GDS BUSINESS INTELLIGENCE GmbH

SentryOne.

Bronze:

inovex

dbWatch DATABASE CONTROL

Global:

PASS

Microsoft Azure

This event is climate neutral:

nachdenken • klimabewusst reisen
atmosfair
KLIMAFREUNDLICHER EVENTPARTNER

Many thanks to our sponsors, without whom such an event would not be possible.

About me

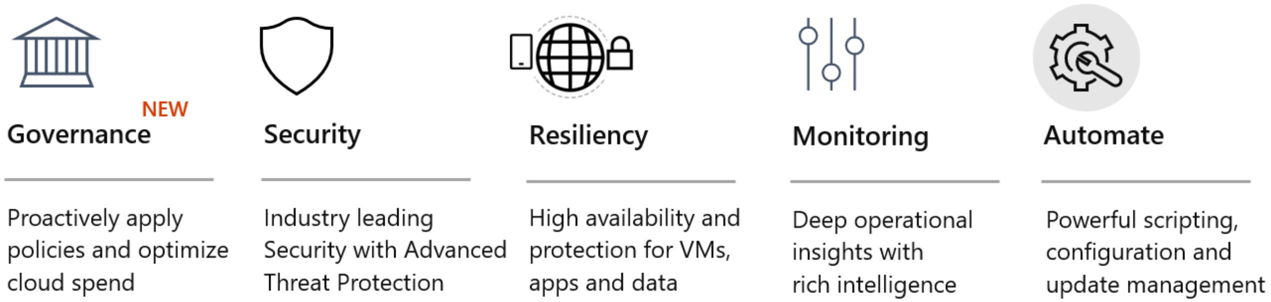
- Gregor Reimling
  - Cloud Architekt – Fokus Azure
  - Orga AzureBonn Meetup (www.azurebonn.de)
  - Microsoft MVP for Azure
  - Tätig bei sepago® GmbH Köln
- Kontakt:
  - Mail: Gregor.Reimling@sepago.de
  - Twitter: @GregorReimling
  - Blog: https://www.reimling.eu

Azure Meetup BONN

Microsoft® MVP Most Valuable Professional

Agenda

- Azure Governance
- Azure Management Groups
- Azure Policys
- Azure Blueprints



NEW
Governance
Proactively apply policies and optimize cloud spend

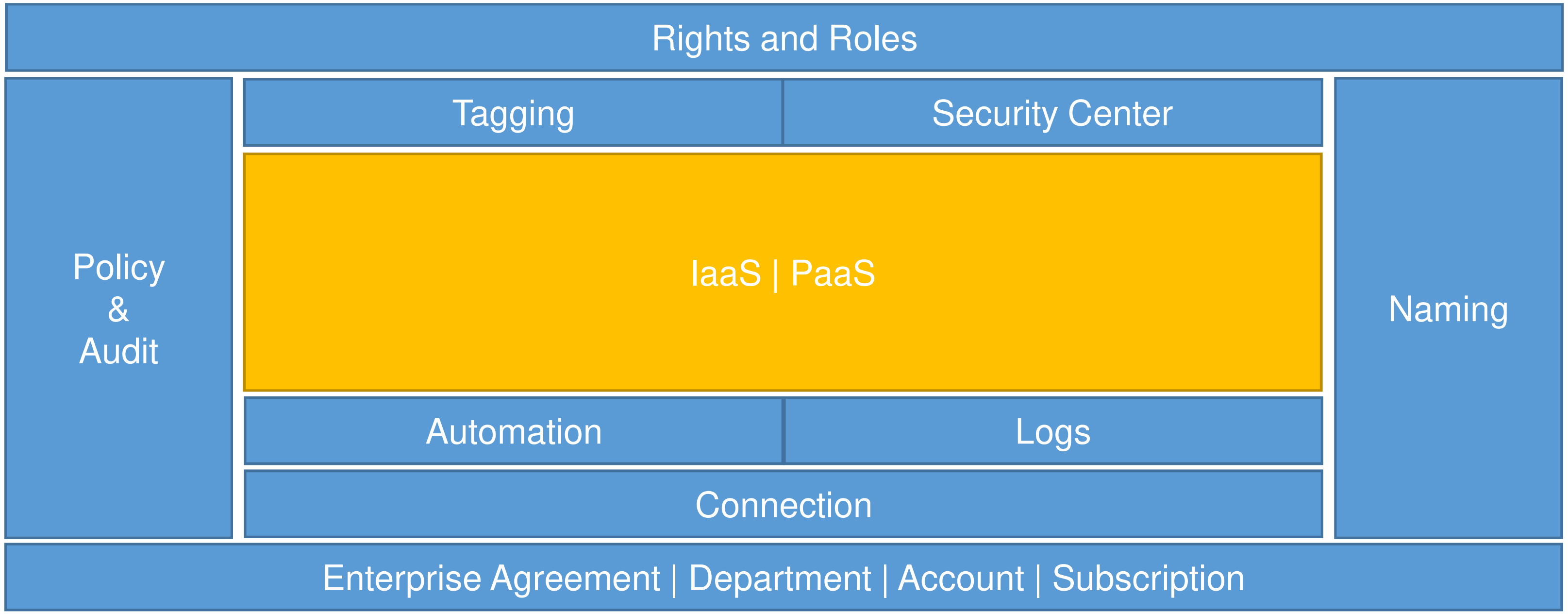
Security
Industry leading Security with Advanced Threat Protection

Resiliency
High availability and protection for VMs, apps and data

Monitoring
Deep operational insights with rich intelligence

Automate
Powerful scripting, configuration and update management

Azure Governance



Rights and Roles

Policy & Audit

Tagging

Security Center

IaaS | PaaS

Automation

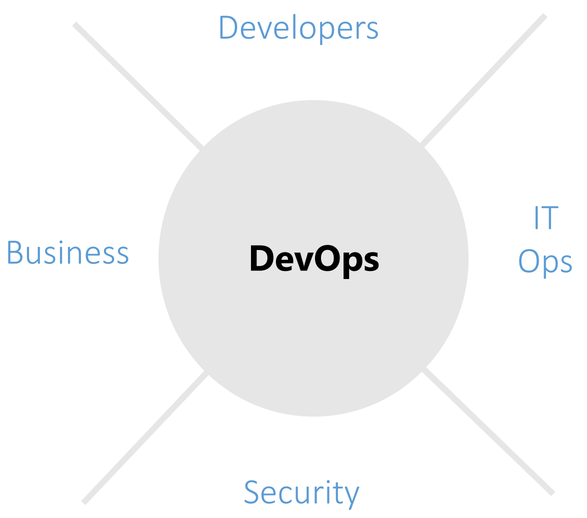
Logs

Connection

Naming

Enterprise Agreement | Department | Account | Subscription

IT is transforming



Adopting new cloud technologies

- API ARM
- Templates
- Scripting
- Functions
- Event Grid

Changing operating model

- **Developer Collaboration**
- **Business value**
- **Time to market**

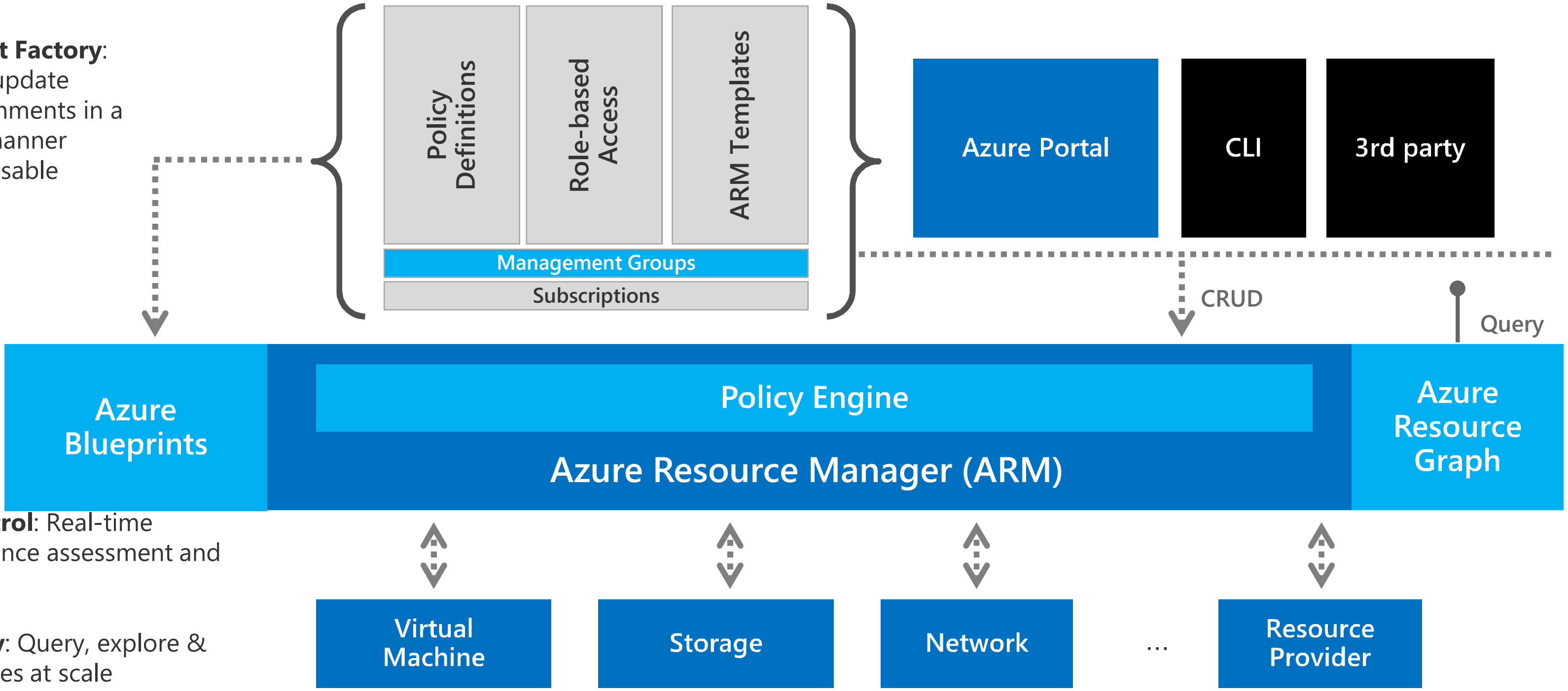
Azure Governance Architecture

providing control over the cloud environment, without sacrificing developer agility

1. **Environment Factory**: Deploy and update cloud environments in a repeatable manner using composable artifacts

2. **Policy-based Control**: Real-time enforcement, compliance assessment and remediation at scale

3. **Resource Visibility**: Query, explore & analyze cloud resources at scale



Azure Security & Management

Built-in Azure services options to keep your Azure and hybrid resources secure and well-managed

Governance

Proactively apply policies and optimize cloud spend

Security

Industry leading Security with Advanced Threat Protection

Resiliency

High availability and protection for VMs, apps and data

Monitoring

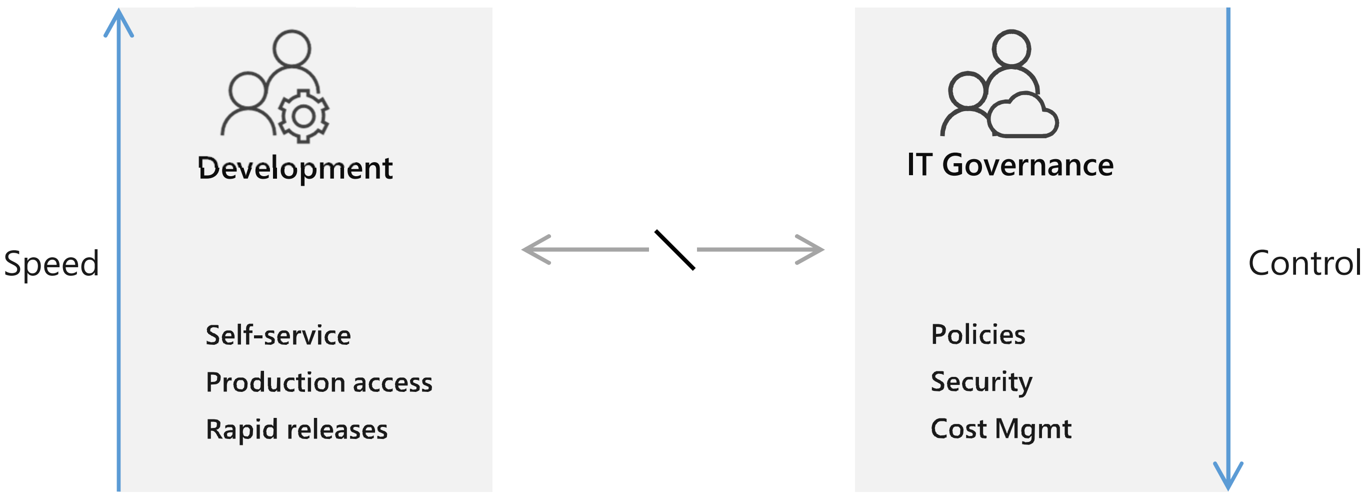
Deep operational insights with rich intelligence

Automate

Powerful scripting, configuration and update management

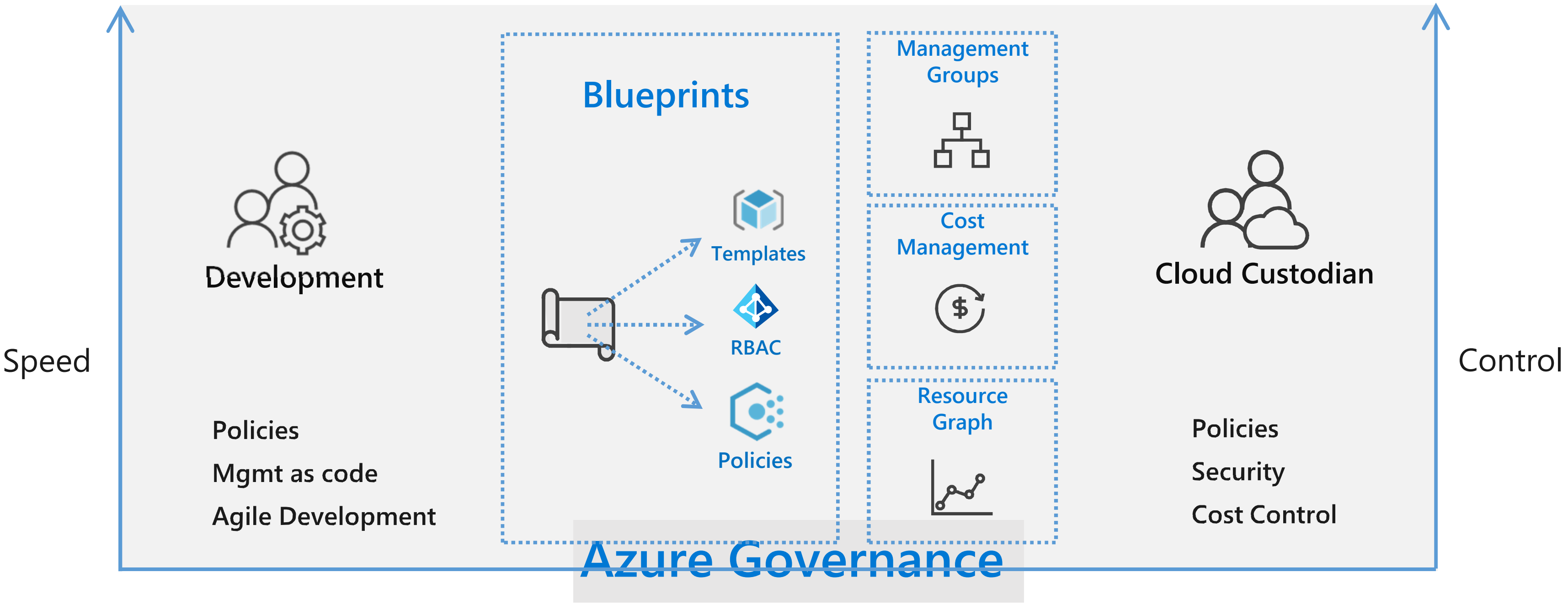
Traditional approach needs rethinking

Speed versus control



Built-in modern governance

Speed *and* control

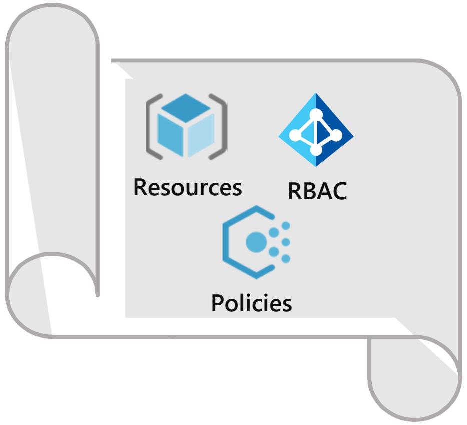


Key Azure governance technologies

```
"policyRule": {
"if": {
"not": {
"field": "location",
"in":
"[parameters('listOfAllowedLocation
s')]"
       }
    },
"then": {
"effect": "Deny"
        }
}
```

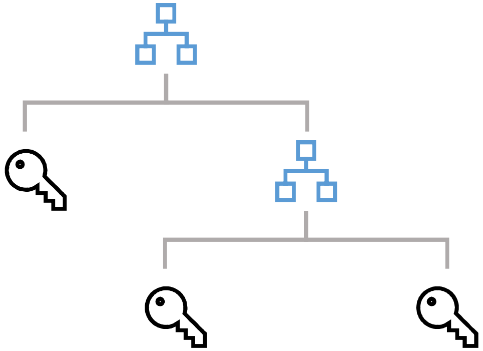
Policy

Enforce or audit rules to ensure compliance.



Blueprints

Quickly create multiple subscriptions with resources, policies and users already setup.



Management groups

Map your organizational structure into Azure to enable governance in multi-tenant and cross-regional scenarios

Azure Resource Manager + Azure Resource Graph

Azure Management Groups

Introducing Azure Management Groups

Make environment management easier by grouping subscriptions together

- Grouping subscriptions into logical groups allow for new organization models
- Inheritance allows for single assignment of controls that apply to all subscriptions
- Aggregated views above the subscription level

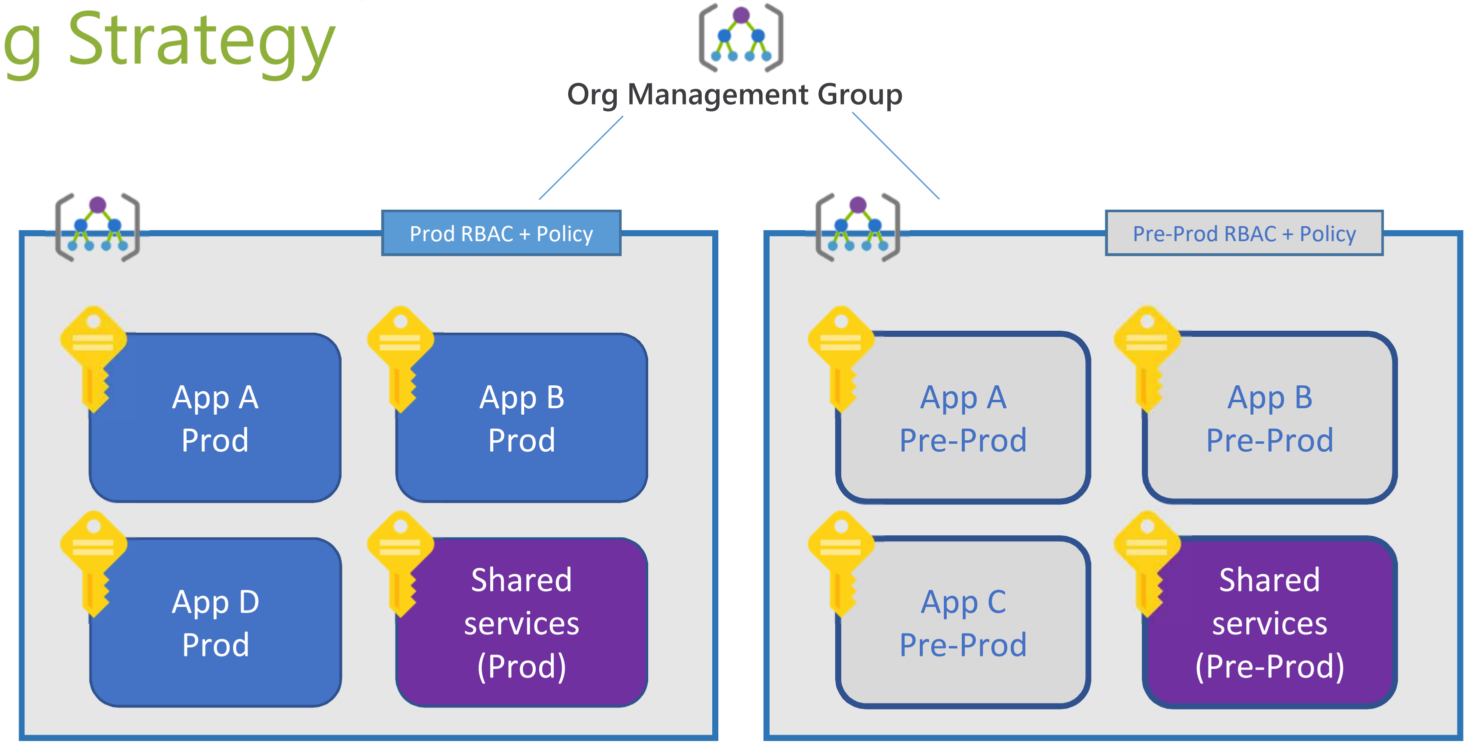
Create a hierarchy of management groups that fit your organization

- Create a flexible hierarchy that can be updated quickly
- Hierarchy doesn't need to model the organizations billing hierarchy
- Can easily scale up or down depending on the organizational needs

Apply governance controls with policies and access controls along with other Azure services

- Azure Resource Manager (ARM) objects that allow integrations with other Azure services
- Azure services:
  - Azure Policy
  - RBAC
  - Azure Cost Management
  - Azure Blueprints
  - Azure Security Center

Management Group & Subscription Modeling Strategy



Azure Management Groups

DEMO

Azure Policys

Azure Policy Journey

09/2017

Limited public preview

Introduced the new compliance engine (scans every 24 hours), UX and initiative

12/2017

Public preview

Introduced Management Group support

Compliance scan on resource change (delta scan)

Built-in definition support for remediation

05/2018

GA

Pricing details announcement (FREE!)

National clouds support

Introduced policy events view (count by user)

09/2018

Compliance percentage

Full fidelity of resources (store compliant resources)

'Last evaluated' timestamp

Trigger scan (on-demand scan) API

Custom definition support for remediation

Remediation on existing resources

'Denied due to policy' UX improvement

Progressive compliance results

In-guest Policy public preview

Default parameters

Azure DevOps integration

Azure Security Center integration

09/2017 12/2017 05/2018 09/2018

Azure Policy

- Turn on built-in policies or build custom ones for all resource types
- Real-time policy evaluation and enforcement
- Periodic & on-demand compliance evaluation
- VM In-Guest Policy (NEW)

Enforcement & Compliance

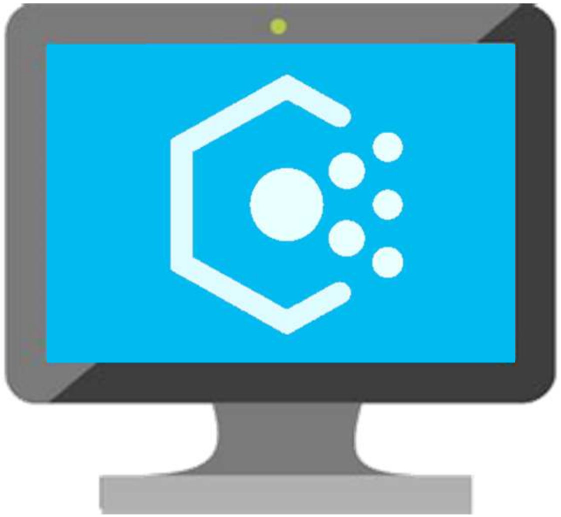
- Apply policies to a Management Group with control across your entire organization
- Apply multiple policies and & aggregate policy states with policy initiative
- Exclusion Scope

Apply policies at scale

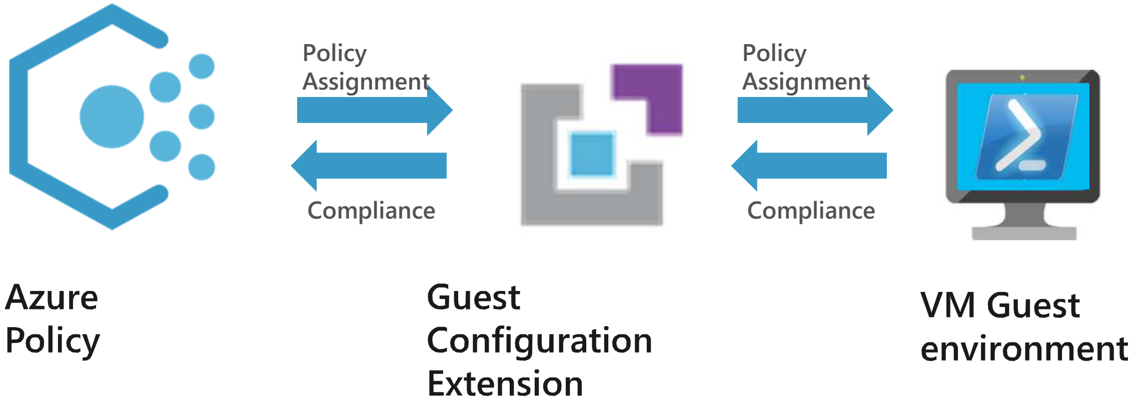
- Real time remediation
- Remediation on existing resources (NEW)

Remediation

Introducing VM guest policy



How VM guest policy works



How does it work?

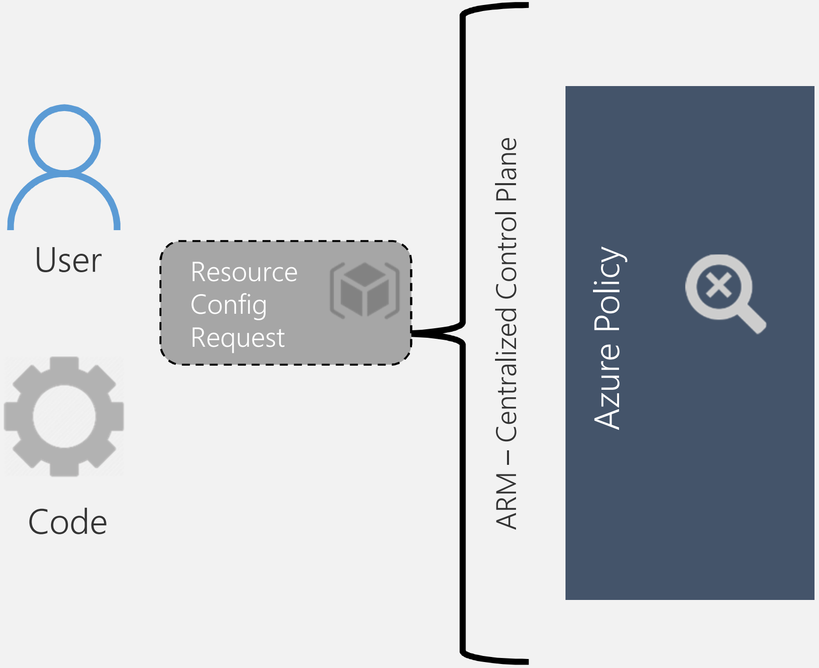
Enforcement

Real-time (on change & on creation):
Audit, Audit if not exists
Deny
Append
Deploy if not exists (NEW)

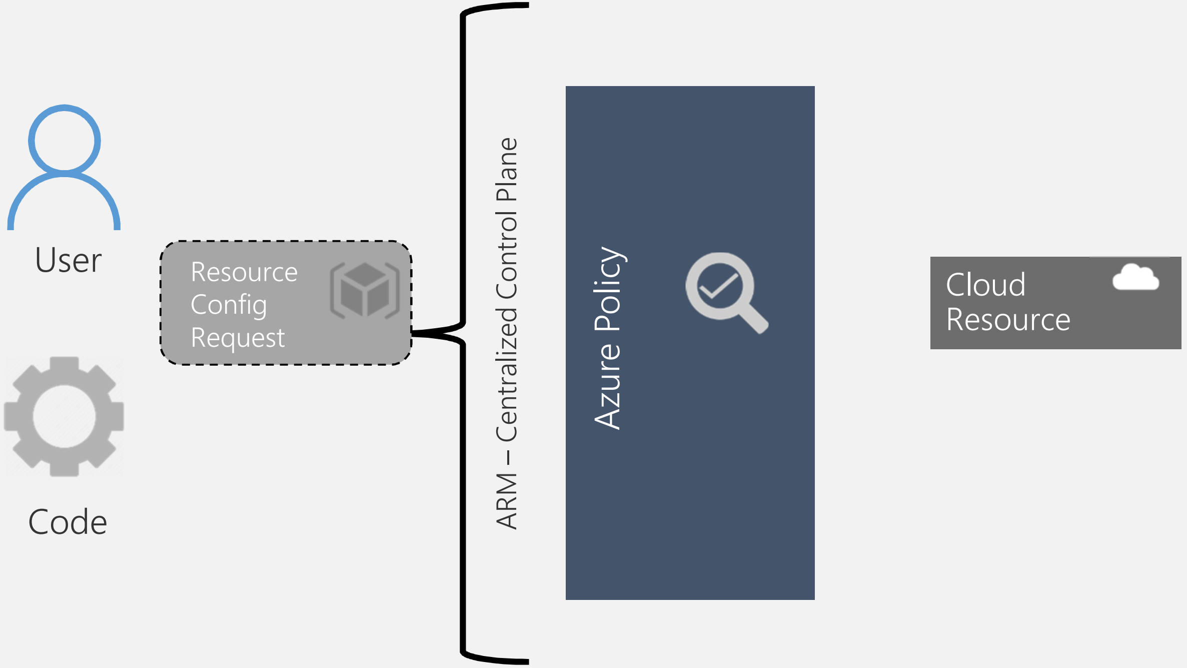
Compliance

Always On:
On Change
On Periodic Cadence
On Demand (PREVIEW)

How does it work?



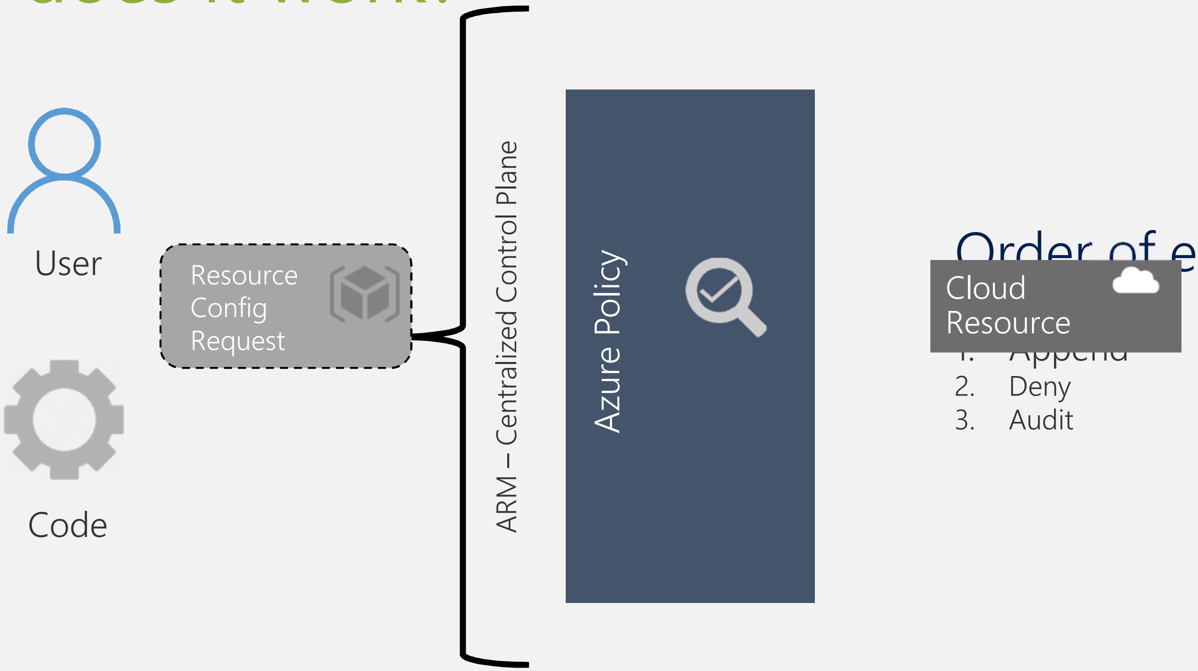
How does it work?



Order of evaluation

- Append
- Deny
- Audit
- DeployIfNotExists
- AuditIfNotExists

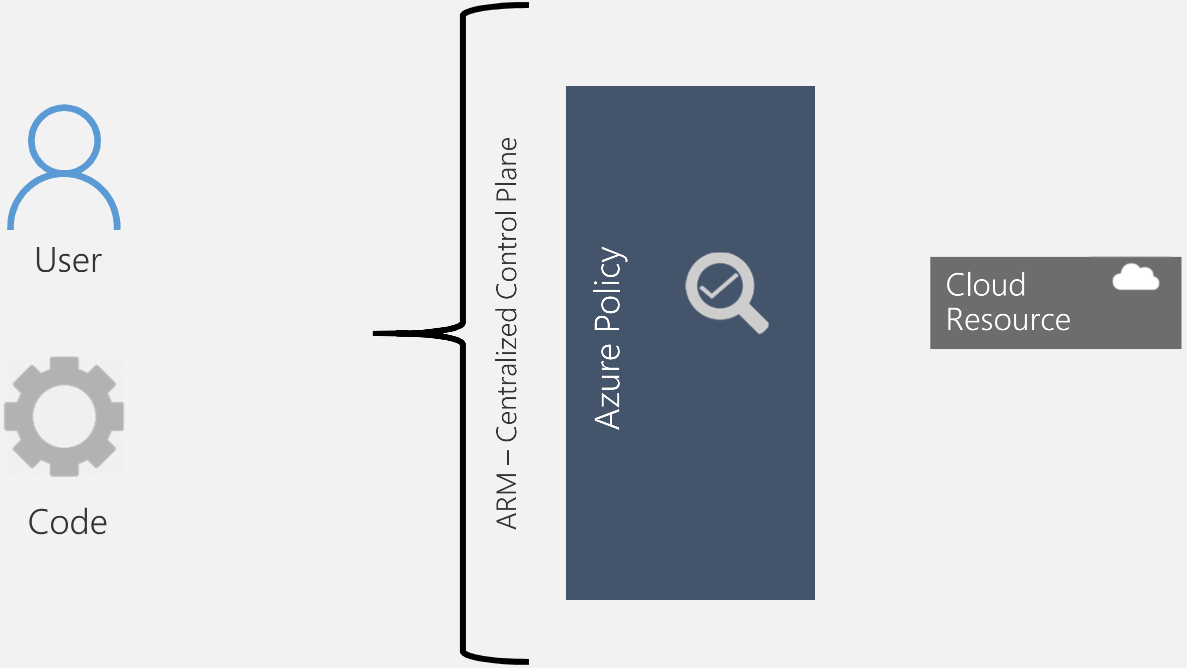
How does it work?



Order of evaluation

1. Append
2. Deny
3. Audit

How does it work?



4. DeployIfNotExists
5. AuditIfNotExists

Policy

- 250 policy definitions per scope
- 100 policy set definitions per scope
- 1000 policy set definitions per tenant
- 100 policyDefinition references per policySetDefinition
- 100 policy assignments per scope
- 250 notScopes per policyAssignment

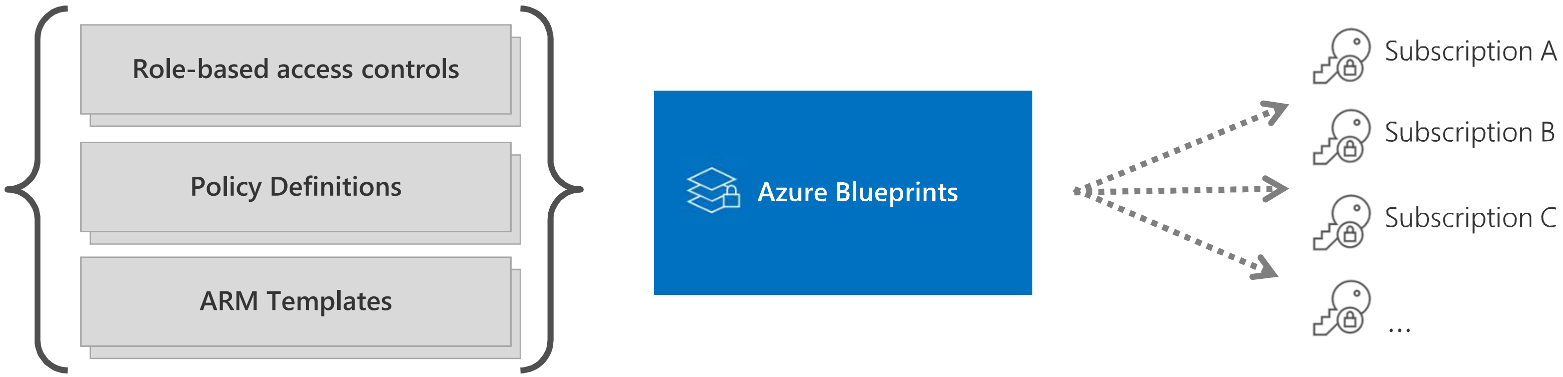
Azure Policys

DEMO

Azure Blueprints

Azure Blueprints

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



Role-based access controls

Policy Definitions

ARM Templates

Azure Blueprints

Subscription A

Subscription B

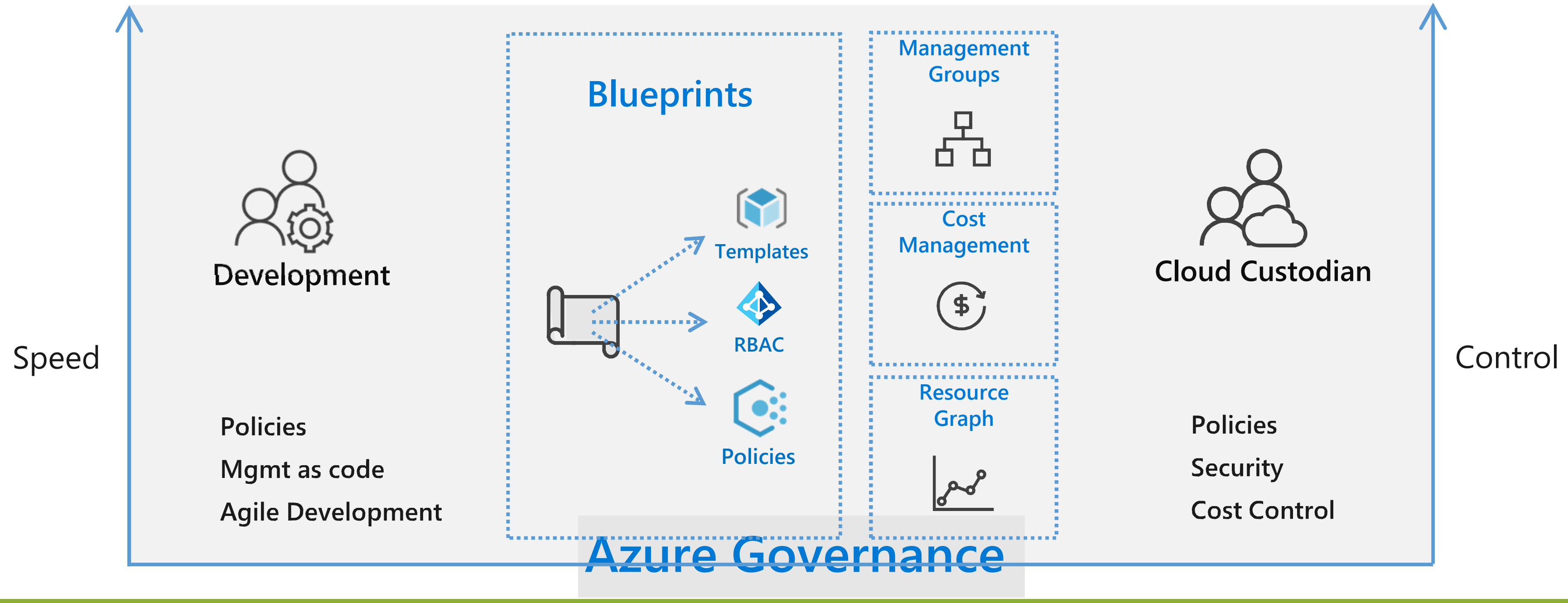
Subscription C

…

compose | manage | scale

Built-in modern governance

Speed *and* control



Azure Blueprints

DEMO

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

Links

- Microsoft Docs – Azure Blueprints
- Microsoft GitHub Repo – Managing Blueprints as Code
- Microsoft Docs – Azure Policies
- Microsoft Docs – Azure Management Groups
- Buchatech – Azure Blueprints
- Gregor Suttie – Azure Policy
- Azure Management Groups and Blueprints – Einrichtung und Konfiguration – www.reimling.eu

SQLSaturday #880 - Munich

19.10.2019

http://www.sqlsaturday.com/880

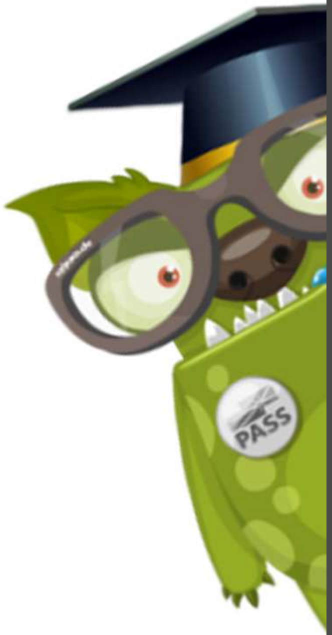
SQLSATURDAY
PASS

PASS Microsoft Data Platform Community
DEUTSCHLAND e.V.

PASS Deutschland e.V.

For further information about future events, visit our PASS Deutschland e.V. booth in the exhibitor area.

PASS SQLSATURDAY
RHEINLAND | 25 MAI 2019



Q&A

Thank you!

PASS DEUTSCHLAND e.V. Microsoft Data Platform Community

Thank you

- Mail: Gregor.Reimling@sepago.de
- Twitter: @GregorReimling
- Blog: https://www.reimling.eu

https://www.reimling.eu

Azure Meetup
BONN

www.azurebonn.de