Authoring Custom Azure Policy Definitions

Jesse Loudon

Principal - LAB[3], Azure MVP

Microsoft Reactor Sydney

Speaker Bio

Background: Infra, SysAdmin, PreSales, Consulting

Pre 2018 Tech: AD, Exchange, VMware, Citrix

Post 2018 Tech: Microsoft Azure, IaC, DevOps, Git

Microsoft Reactor Sydney

Session Abstract

Quick refresher on Azure Policy

Authoring examples and gotchas

Authoring tips and tricks

# AzPolicy - Ecosystem

Official Docs	aka.ms/azurepolicy bicep, arm templates, api references
Official Code	github/azure-policy github/community-policy
Official Tooling	GitHub, Azure DevOps, Azure Policy extension (VS Code)
Deployment	Terraform, Azure CLI, ARM Templates, Bicep
Community	azadvertizer.net github/awesome-azure-policy

- **902** GA policy definitions

  - **71** categories

- **54403** aliases

  - **110** namespaces

  - **944** resource types

  - **17690** network aliases

Microsoft Reactor Sydney

AzPolicy – Resource Aliases
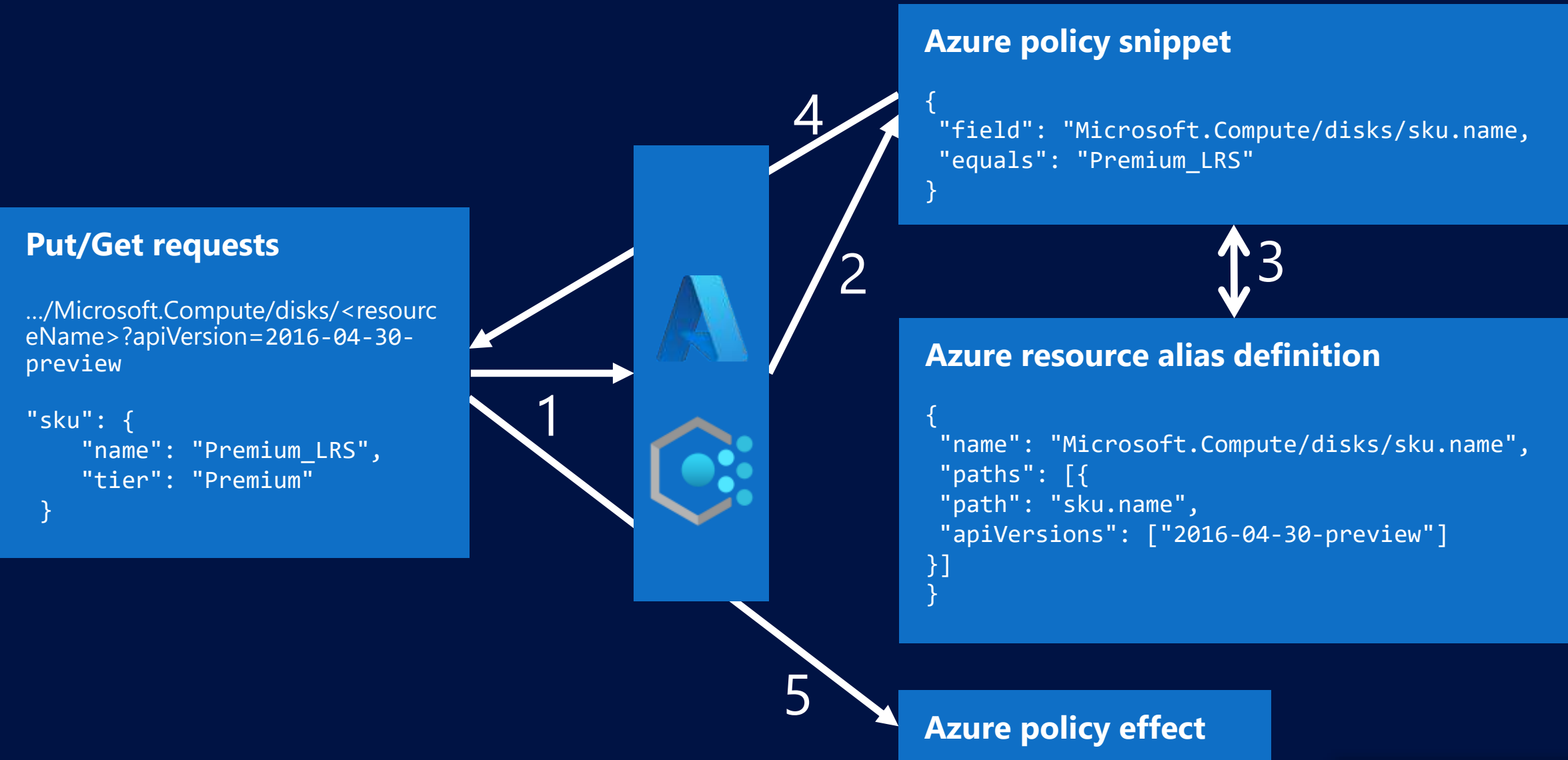
Put/Get requests

.../Microsoft.Compute/disks/<resourc
eName>?apiVersion=2016-04-30-
preview

```
"sku": {
    "name": "Premium_LRS",
    "tier": "Premium"
}
```

Azure policy snippet

```
{
  "field": "Microsoft.Compute/disks/sku.name,
  "equals": "Premium_LRS"
}
```
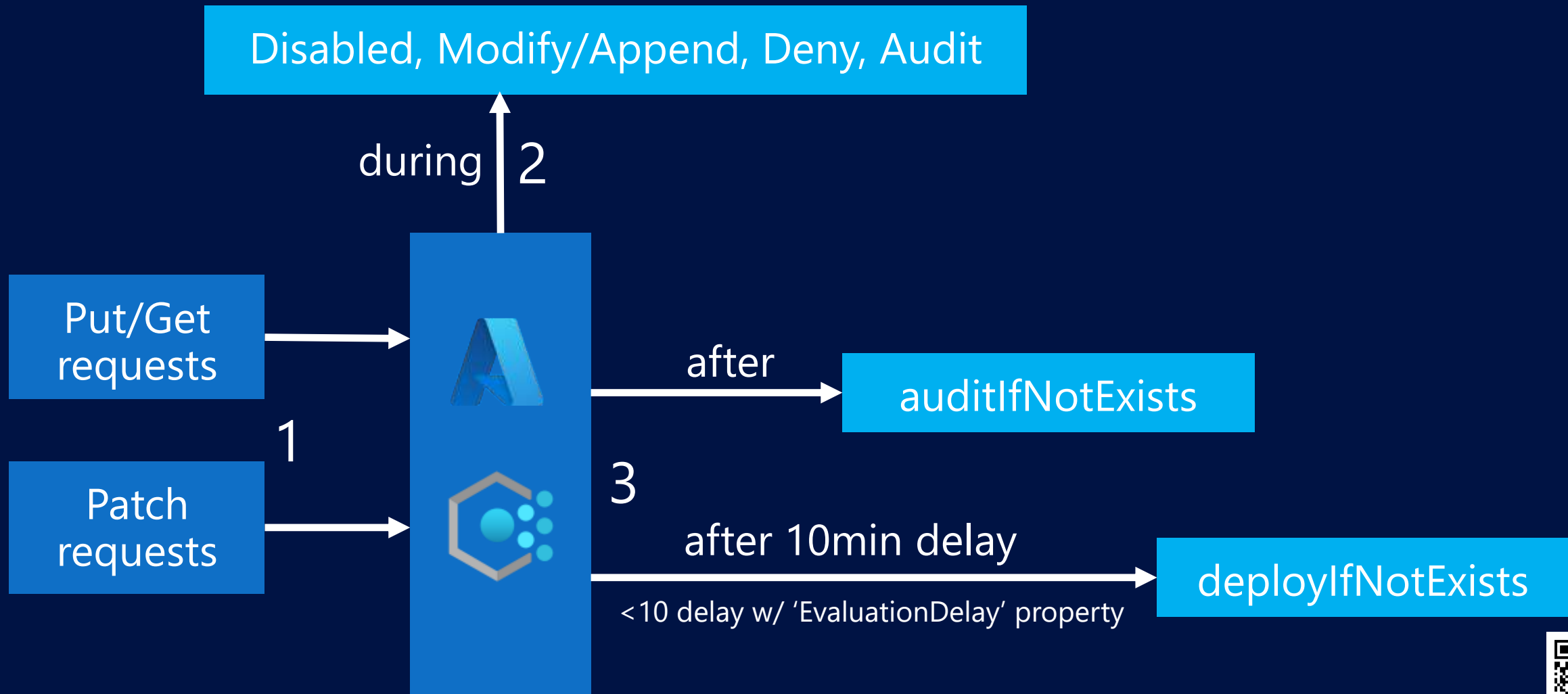
Azure resource alias definition

```
{
  "name": "Microsoft.Compute/disks/sku.name",
  "paths": [{
  "path": "sku.name",
  "apiVersions": ["2016-04-30-preview"]
}]
}
```
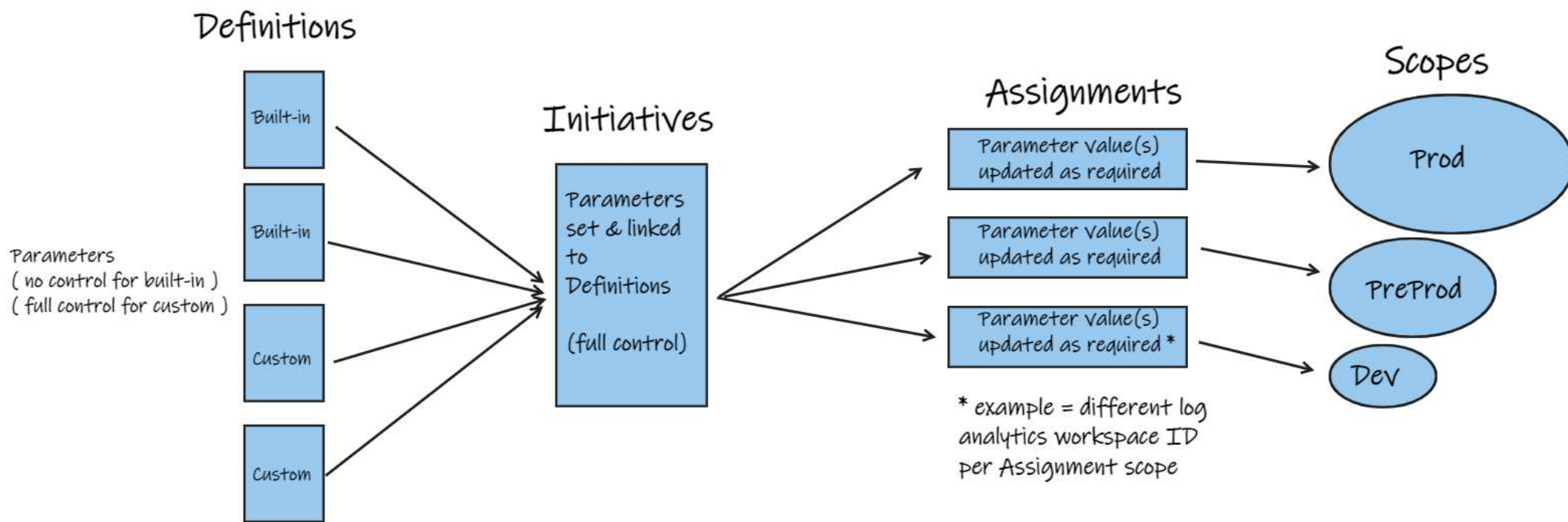
Azure policy effect

AzPolicy – Parameters

Definitions

Built-in

Built-in

Parameters
(no control for built-in)
(full control for custom)

Custom

Custom

Initiatives

Parameters
set & linked
to
Definitions

(full control)

Assignments

Parameter value(s)
updated as required

Parameter value(s)
updated as required

Parameter value(s)
updated as required *

* example = different log
analytics workspace ID
per Assignment scope

Scopes

Prod

PreProd

Dev

8 Step Authoring Process

1. Establish business case / requirements
2. Check for any existing built-in policies
3. Create a baseline custom policy definition
4. Test and validate compliance evaluation works
5. Test and validate remediation works (if modify/deployIfNotExists)
6. Parameterize for maximum reusability
7. Final validation
8. Ship to production

Thanks For Watching!

Connect w/ Jesse

[

🐦 @coder_au,

  jloudon.com,

🐙 @jesseloudon

]

Microsoft Reactor Sydney