Flexing your Security Governance w/ Azure Policy as Code

Jesse Loudon

Azure MVP | Principal Consultant

Melbourne Azure Security Meetup

Demo

https://youtu.be/-KSLh2I9e1U

Flexing Your Security Governance with Azure Policy As Code

Ecosystem

Docs	azure policy arm templates / api references
Code	github/azure-policy github/community-policy
Tools	azure cli, github, azure devops, azure policy vscode extension
Languages	json, arm templates, powershell, terraform, bicep
Community	azadvertizer.net youtube/azure deployments & governance

- **1498** GA policy definitions
  - **56** categories
- **41755** aliases
  - **105** namespaces
  - **867** resource types
  - **17362** network aliases

Use Cases

Tagging

- Mandatory tags
- RG tag inheritance

Monitoring

- Metric alerts
- Diagnostic settings
- Monitor Agents
- Data Collection Rules

Data Protection

- Configure VM backups
- Configure ASR
- Storage/Disk/DB Encryption

Network

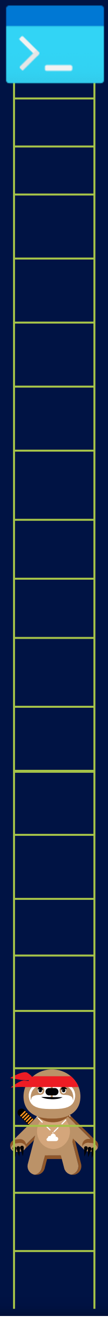
- PIPs, NICs
- NSG rules
- VNET Peering
- SA/KV Firewalls
- Gateways

Regulatory Compliance

- CIS
- HIPAA
- ISO 27001
- NIST

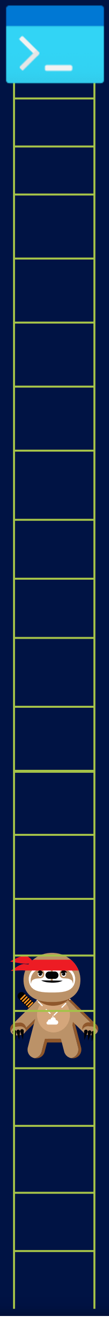
General

- Allowed locations
- Allowed SKUs
- Naming convention

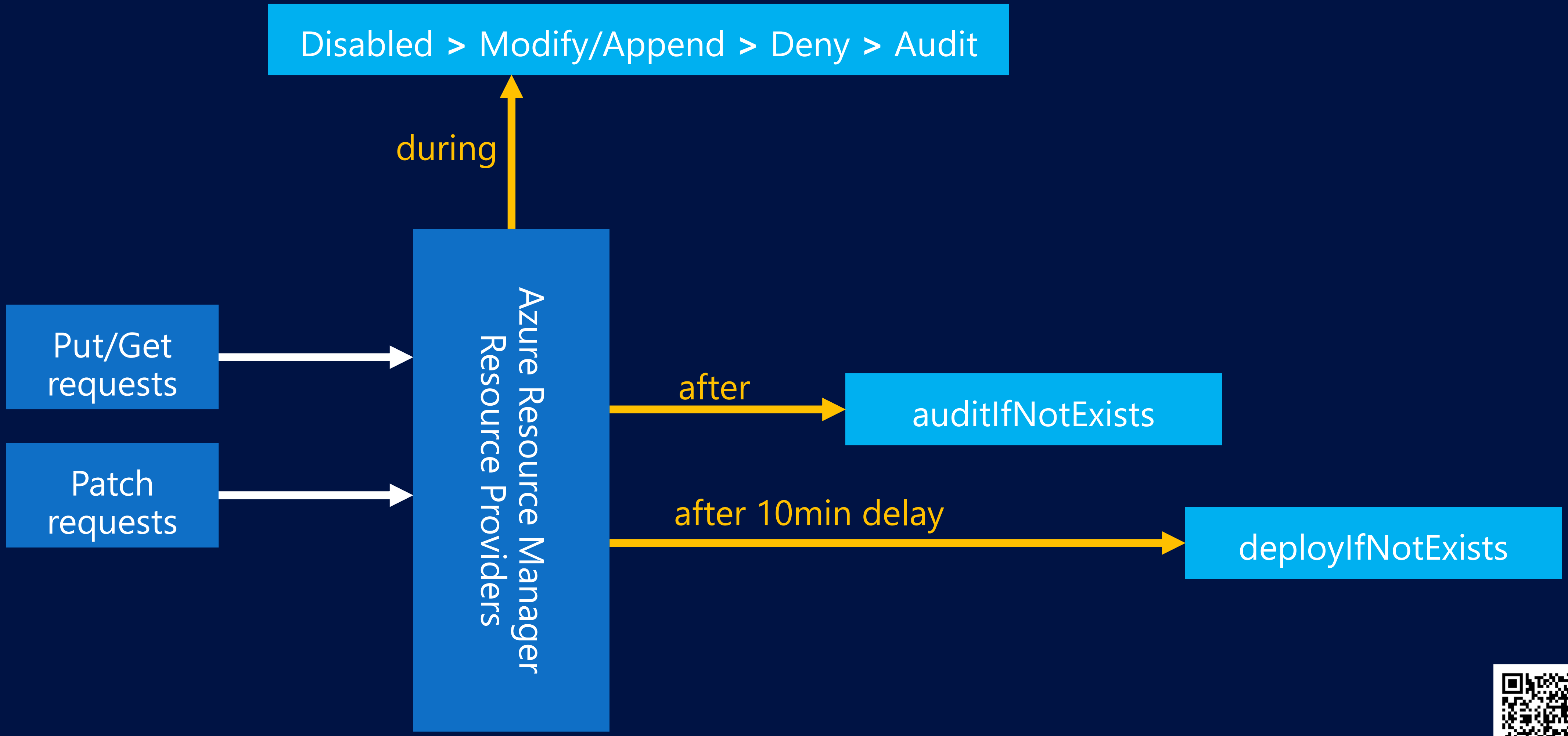


RBAC

Identity/AAD Group	Built-in Roles	Role Assignment Scope
Service-Principals	Resource Policy Contributor User Access Administrator Contributor (bicep deployments)	Tenant, Management Group
Policy-Developers	Resource Policy Contributor Contributor	Management Group, Subscription
Policy-Users	Resource Policy Contributor	Subscription, Resource Group
Policy-Readers	Reader	Tenant or Management Group



Effects



Disabled > Modify/Append > Deny > Audit

during

Put/Get requests

Patch requests

Azure Resource Manager
Resource Providers

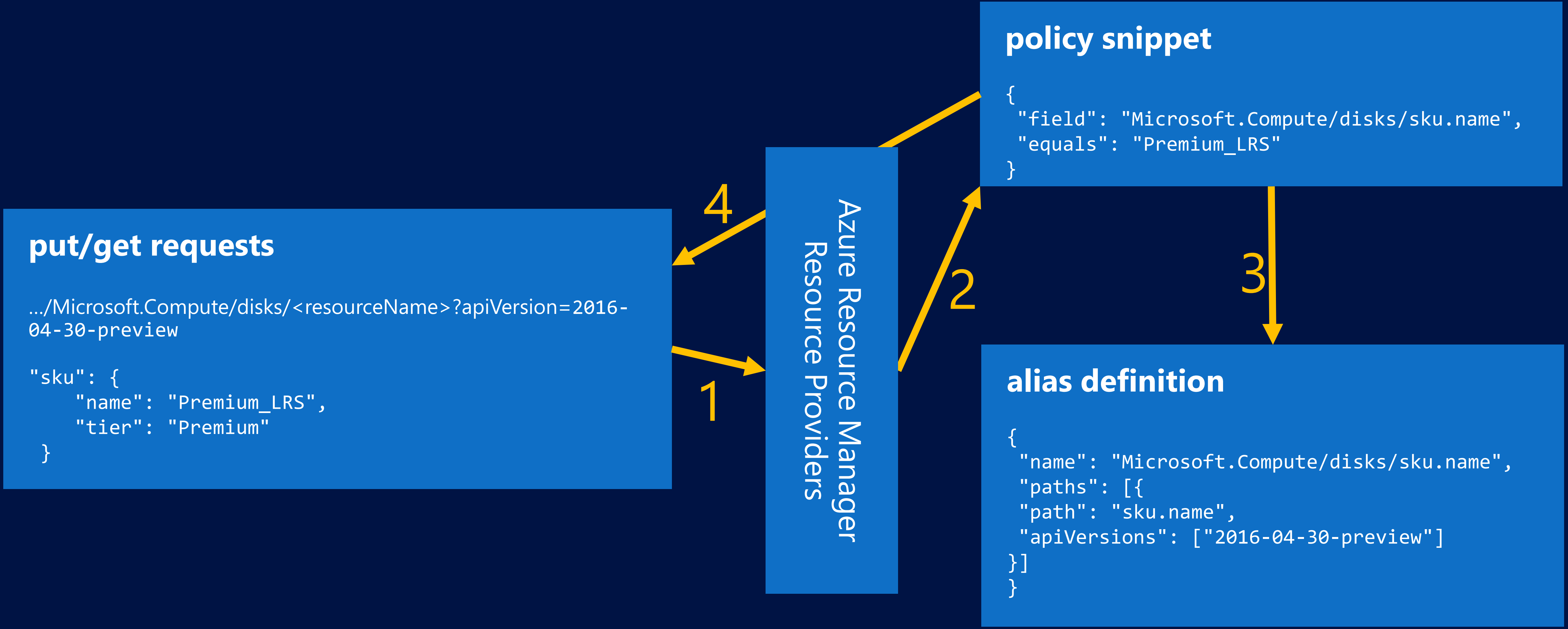
after

auditIfNotExists

after 10min delay

deployIfNotExists

Aliases



put/get requests

```
.../Microsoft.Compute/disks/<resourceName>?apiVersion=2016-04-30-preview

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

policy snippet

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

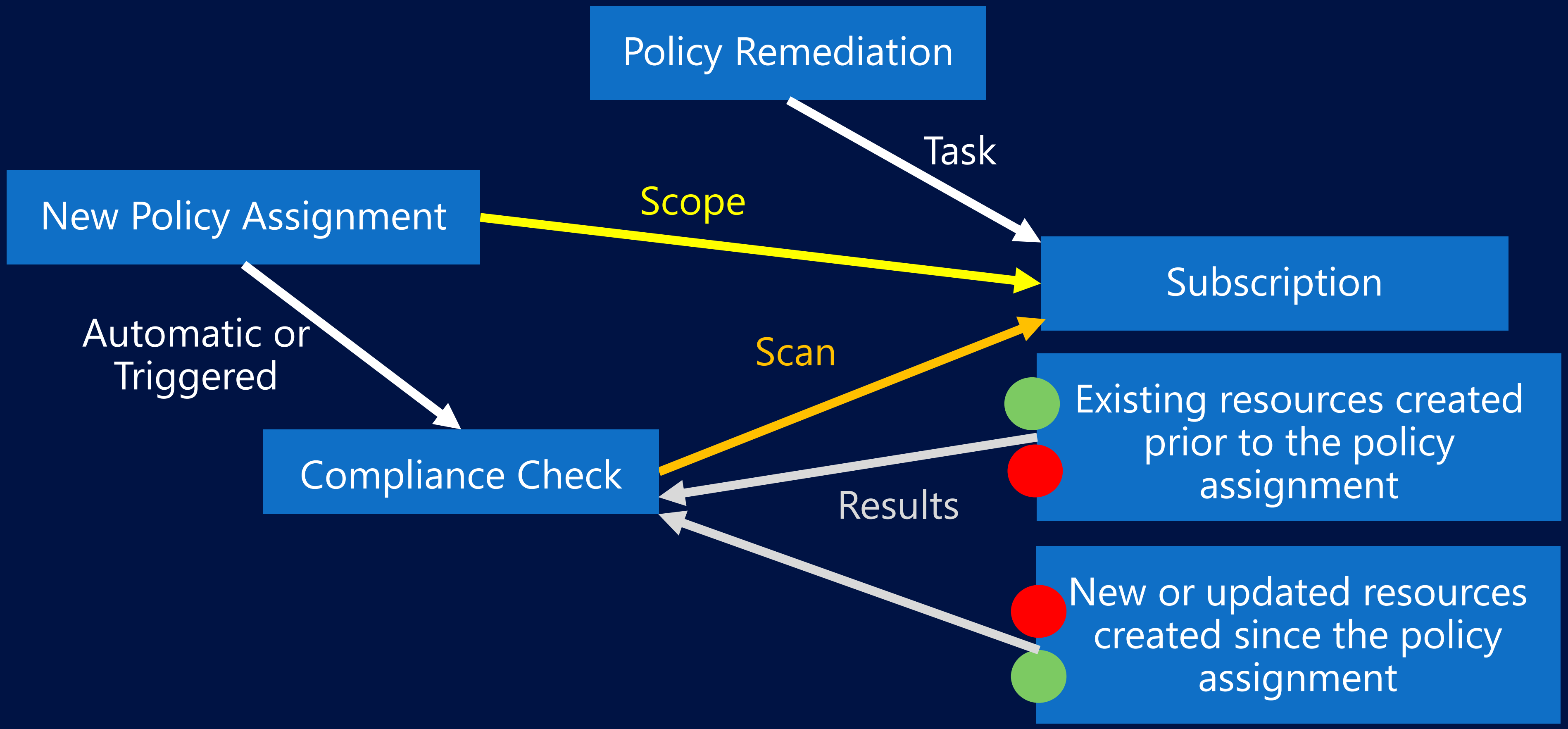
alias definition

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

Compliance & Remediation

Complaint ●

Non-Complaint ●



Policy Remediation

Task

New Policy Assignment

Scope

Subscription

Automatic or Triggered

Scan

Compliance Check

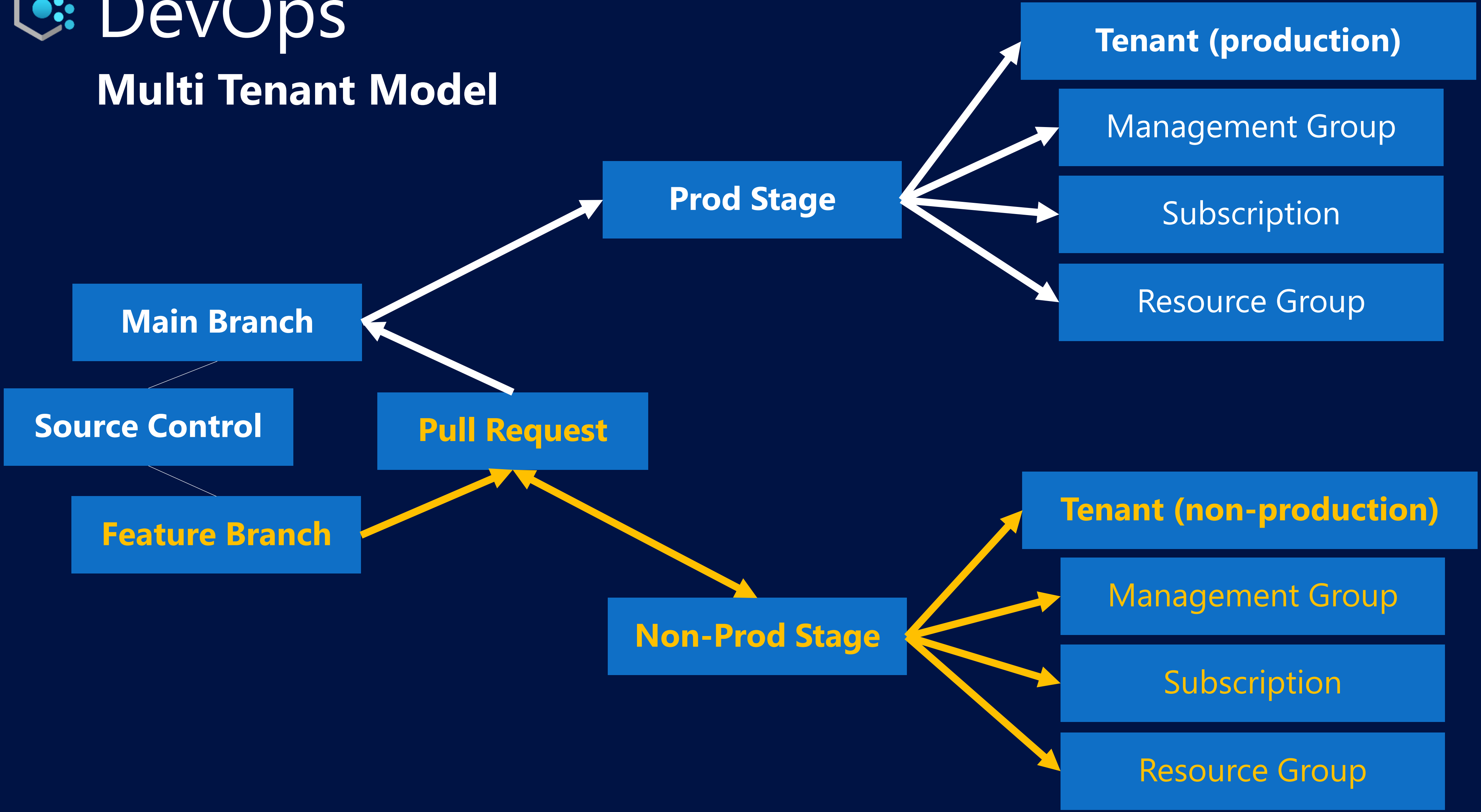
Results

Existing resources created prior to the policy assignment

New or updated resources created since the policy assignment

DevOps

Multi Tenant Model



Source Control

Main Branch

Feature Branch

Pull Request

Prod Stage

Non-Prod Stage

Tenant (production)

Management Group

Subscription

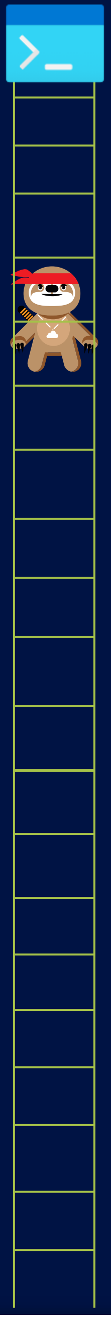
Resource Group

Tenant (non-production)

Management Group

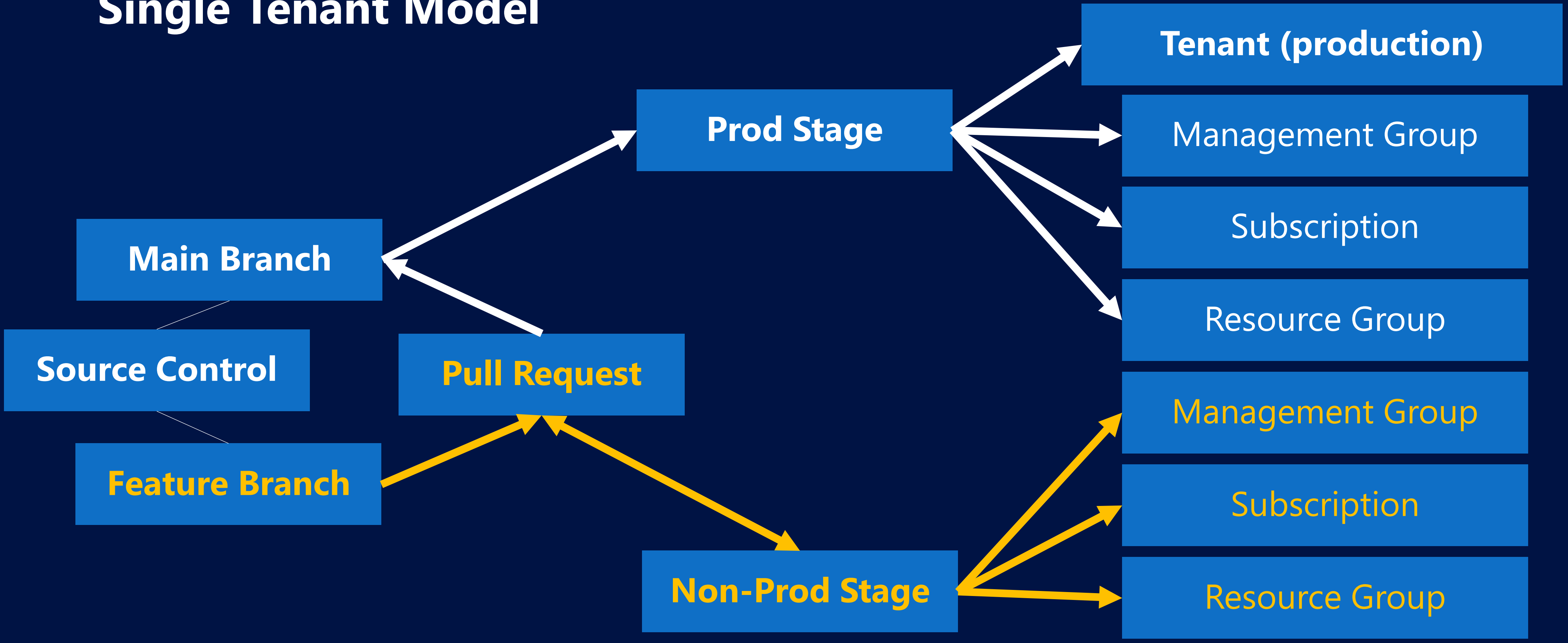
Subscription

Resource Group



DevOps

Single Tenant Model



Next Steps

{ Use Bicep snippets to build new policy resources }

{ Review existing policy repo code/pipeline for improvements }

{ Setup policy non-compliance alerting and remediation workflows }

{ Group common policies into initiatives for assignment }

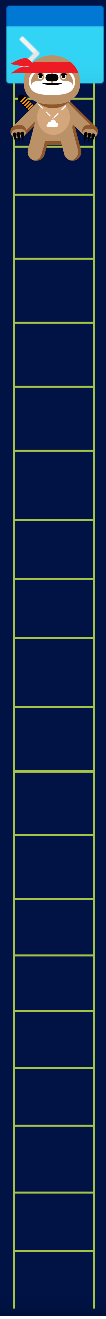
{ Enhance your code deployment with CI/CD tasks }

{ Implement policy assignment custom deny messages }

{ Find an existing built-in policy to customise or BYO }

{ Setup your policy development environment }

{ Create, deploy, and test your 1st custom policy }



“Blogs + Code”:
[
“Stefan Stranger”,
“Tao Yang”,
“Adin Ermie”,
“Jack Tracey”,
“Matt Felton”,
]
// & many more!

Thanks For Watching!

“Socials”:
[
“coder_au”,
“jloudon.com”,
“jesseloudon”
]

Melbourne Azure Security Meetup