Automating Infrastructure Governance with Azure Policy

Jesse Loudon

Principal Consultant - Azure and DevOps

"Socials":

[

"coder_au",

"jloudon.com",

"jesseloudon"

]

DevOps Sydney

Ecosystem

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

- **1353** GA policy definitions
- **89** preview policy definitions
- **38704** policy aliases
  - for **98** namespaces
  - **17362** Microsoft.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

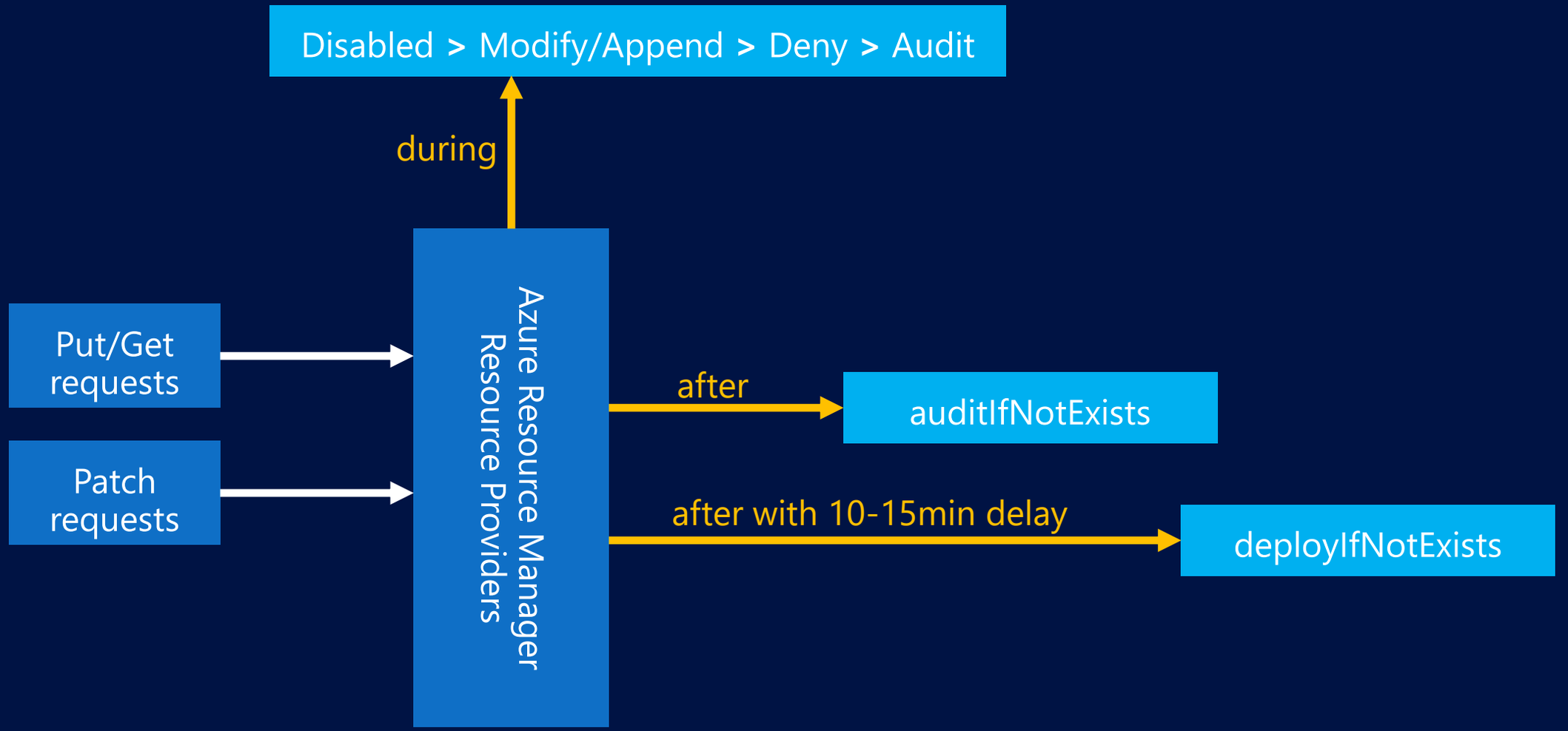
Regulatory Compliance

- CIS
- HIPAA
- ISO 27001
- NIST

General

- Allowed locations
- Allowed SKUs
- Naming convention

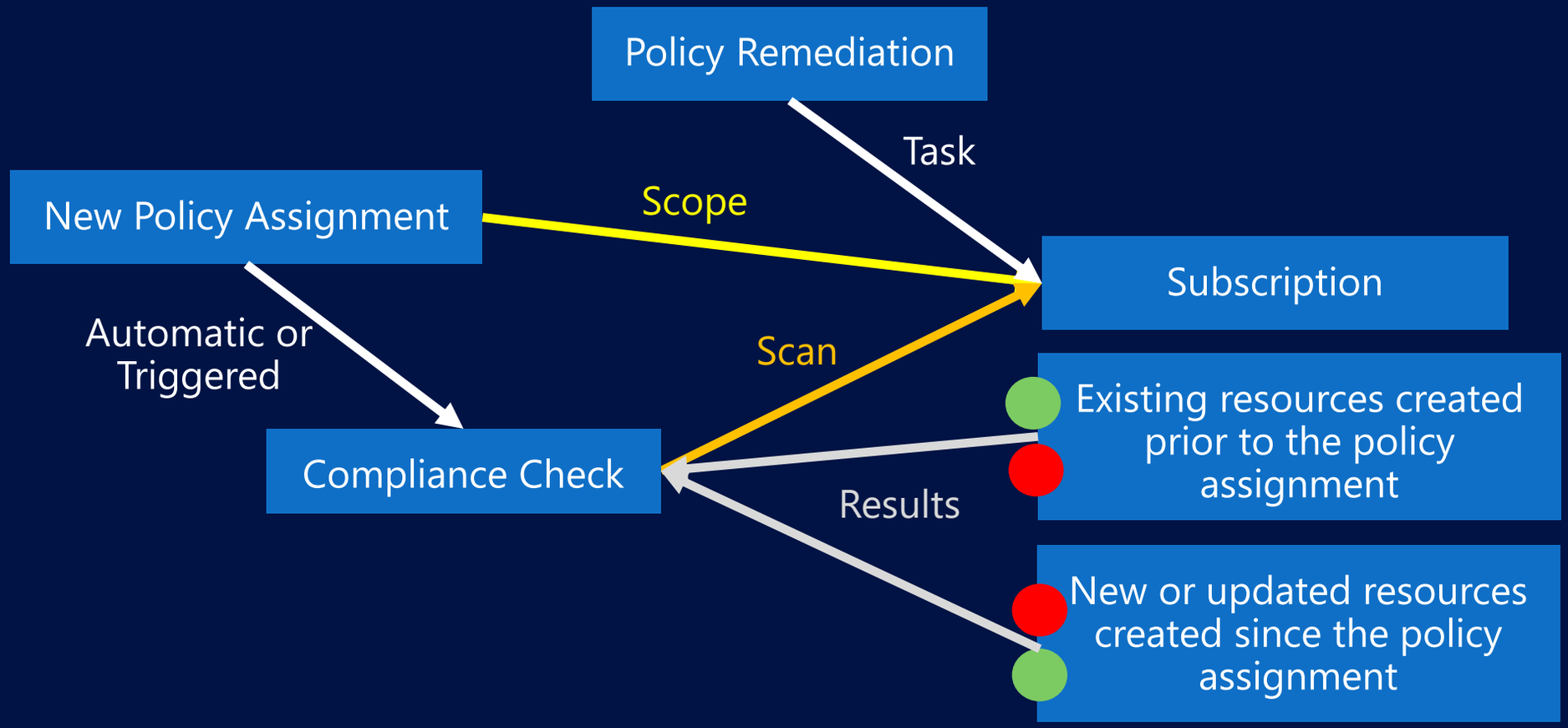
Effects & Order of Evaluation



https://docs.microsoft.com/en-gb/azure/governance/policy/concepts/effects

Compliance & Remediation

Complaint
Non-Complaint



https://docs.microsoft.com/en-gb/azure/governance/policy/how-to/determine-non-compliance

DevOps Sydney

Tip - Custom Policies

Name : Deploy new Azure Monitor Agent to Windows VMs and tie to DCR

Description : Deploy new Azure Monitor Agent to Windows VMs and tie to DCR

Available Effects : DeployIfNotExists

Category : Custom

Definition Assignments (0)

```
{
  "properties": {
    "displayName": "Deploy new Azure Monitor Agent to Windows VMs and tie to DCR",
    "policyType": "Custom",
    "mode": "All",
    "description": "Deploy new Azure Monitor Agent to Windows VMs and tie to DCR",
    "metadata": {
      "category": "Custom",
      "source": "globalbao/azure-policy-as-code",
      "version": "0.1.0",
      "createdBy": "a579205b-7856-4680-a131-24b965441e4c",
      "createdOn": "2021-06-19T22:27:16.7403998Z",
      "updatedBy": null,
      "updatedOn": null
    },
```

Custom Policies

- Check ‘mode’ is correct
- Leverage ‘metadata’

DevOps Sydney

Tip - Custom Policies

```bicep
resource policy 'Microsoft.Authorization/policyDefinitions@2020-09-01' = {
  name: 'deployAzureMonitorAgentWindowsDCR'
  properties: {
    displayName: 'Deploy new Azure Monitor Agent to Windows VMs and tie to DCR'
    policyType: 'Custom'
    mode: 'All'
    description: 'Deploy new Azure Monitor Agent to Windows VMs and tie to DCR'
    metadata: {
      category: policyCategory
      source: policySource
      version: '0.1.0'
    }
```

Custom Policies

- Check ‘mode’ is correct
- Leverage ‘metadata’

Tip – Managed Identity Permissions

Managed Identity

Policies with the deployIfNotExists and modify effect types need the ability to deploy resources and edit tags on existing resources respectively. To do this, a managed identity will be created for you. Learn more about Managed Identity.

Managed identity location

Australia East

Principal ID

97eb48d1-b995-4d2d-8638-7ff330f5661c

Permissions

This identity currently has the following permissions:

This identity will also be given the following permissions:

Contributor

Managed Identity

Policies with the deployIfNotExists and modify effect types need the ability to deploy resources and edit tags on existing resources respectively. To do this, a managed identity will be created for you. Learn more about Managed Identity.

Managed identity location

Australia East

Principal ID

97eb48d1-b995-4d2d-8638-7ff330f5661c

Permissions

This identity currently has the following permissions:

Contributor

Policy Assignments

- Check ‘role assignment’ creation for ‘managed identity’

Tip – Managed Identity Permissions

Policy Assignments

- Create a **'role assignment'** resource for each policy assignment's system '**managed identity**'

```
resource monitoringGovernanceRoleAssignment 'Microsoft.Authorization/
roleAssignments@2020-04-01-preview' = {
  name: guid(monitoringGovernanceAssignment.name,
   monitoringGovernanceAssignment.type, subscription().subscriptionId)
  properties: {
    principalId: monitoringGovernanceAssignment.identity.principalId
    roleDefinitionId: '/providers/microsoft.authorization/roleDefinitions/
     b24988ac-6180-42a0-ab88-20f7382dd24c'
  }
}
```

Tip – Custom Deny Messages

Add deny msgs to your policy assignments

- **Minimum apiVersion = "2020-09-01"**

```
nonComplianceMessages: [
  {
    message: '***DENIED*** Missing Mandatory
    tag. ***DENIED***'
  }
  {
    message: '***DENIED*** Missing $
    {mandatoryTag2Key} tag. Please update your
    resource to include the $
    {mandatoryTag2Key} tag. ***DENIED***'
    policyDefinitionReferenceId:
    'requireTagToRG_${mandatoryTag2Key}'
  }
]
```

Summary Raw Error

ERROR DETAILS

Resource 'BicepExampleRG' was disallowed by policy. (Code: RequestDisallowedByPolicy)

Initiative: Tag Governance Assignment
Policy: Add tag Owner to resource group
Reason: ***DENIED*** Missing Owner tag. Please update your resource to include the Owner tag. ***DENIED***

DevOps Sydney

Tip – DeployIfNotExists Effect

```
resource bicepExampleDINEpolicy 'Microsoft.Authorization/policyDefinitions@2020-09-01' = {
    name: 'bicepExampleDINEpolicy'
    properties: {
        displayName: ''
        description: ''
        policyType: 'Custom'
        mode: 'All'
        metadata: {}
        parameters: {}
        policyRule: {
            if: {
                allOf: []   <-- define condition(s) for Policy evaluation
            }
            then: {
                effect: 'deployIfNotExists'   <-- use DINE effect
                details: {
                    roleDefinitionIds: []
                    type: 'Microsoft.Insights/metricAlerts'   <-- ARM resource type to evaluate
                    existenceCondition: {
                        allOf: []   <-- define condition(s) for DINE evaluation
                    }
                    deployment: {
                        properties: {
                            mode: 'incremental'
                            template: {
                                '$schema': 'https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#'
                                contentVersion: '1.0.0.0'
                                parameters: {}
                                variables: {}
                                resources: []   <-- define resource(s) to create w/ ARM template
                            }
                            parameters: {}
                        }
                    }
                }
            }
        }
    }
}
```

Policy definition

ARM template

#inception :-)

Policy Definitions

- Leverage ARM template capabilities via ‘deployIfNotExists’ effect

DevOps Sydney

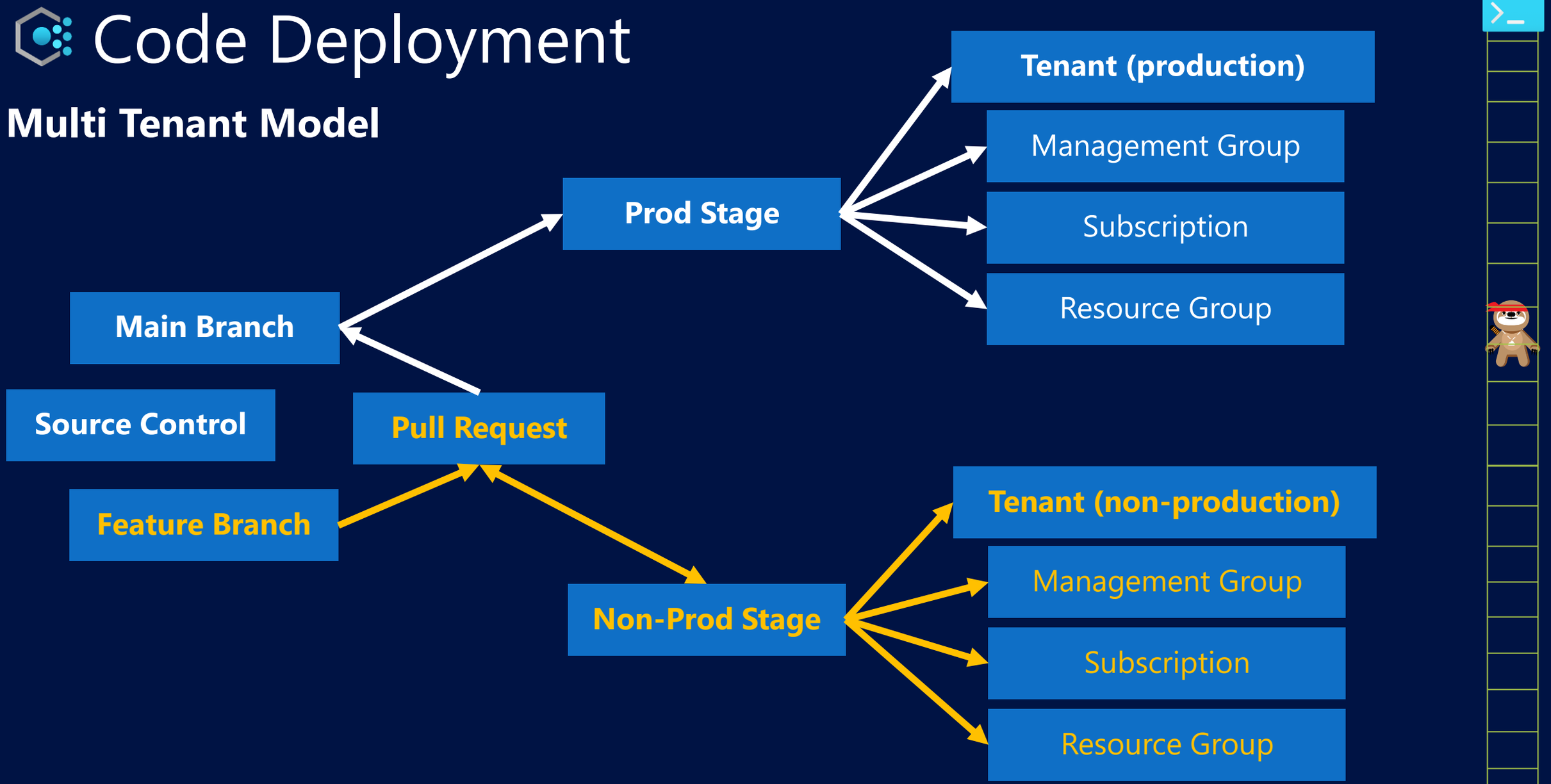
Tip – AAD RBAC Permissions

Design your RBAC permissions and scope carefully

Identity/AAD Group	Built-in Role Assignments	Scope
Service Principals	• Resource Policy Contributor • User Access Administrator	Tenant or MG level
Policy Developers	• Resource Policy Contributor • Contributor	MG or Subscription level
Policy Users	Resource Policy Contributor	Subscription or RG level
Policy Readers	Reader	Tenant or MG level

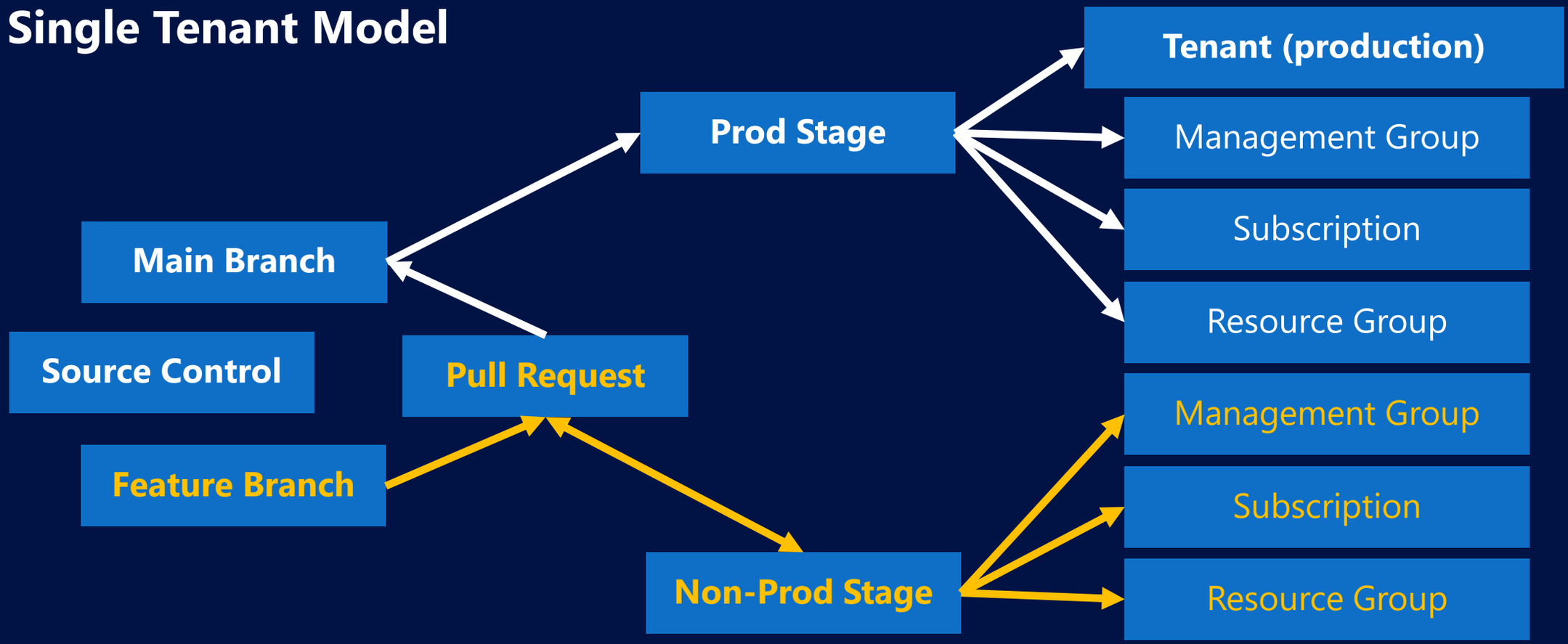
Code Deployment

Multi Tenant Model



Code Deployment

Single Tenant Model



DevOps Sydney

Choose Your Path

- 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"
]

DevOps Sydney