Managing governance and implementing Guard Rails with Azure Blueprints

Dutch
Microsoft
& Security
meetup

Wesley Haakman

Lead Azure Architect @ Intercept

@whaakman

www.linkedin.com/in/wesleyhaakman

whaakman@intercept.nl

Governance

Governance

- Organizing resources
- Control Costs
- Role Based Access Control
- Consistency in code & infrastructure
- Regulatory requirements & Compliance
- Life cycle management

Governance & Compliance

"I'm concerned about data sovereignty; how can I ensure that my data and systems meet our regulatory requirements?"

"How do I know what each resource is supporting so I can account for it and bill it back accurately?"

"I want to make sure that everything we deploy or do in the public cloud starts with the mindset of security first, how do I help facilitate that?"

The challenges with governance

- Nobody wants to do it
- Governance can slow down a company’s ability to release new innovations
- Bad or no governance results in non-compliance, unforeseen costs and unmanageable environments

But… We do want consistency, predictable outcome and happy customers

This is an automation problem

Automation of Governance on Azure

- Implement governance early in the process (shift left)
- Enforce internal standards and guardrails
- Meet regulatory compliance requirements
- Consistent security management
- Setup environments faster
- Release compliant code faster
- Control costs

What do we need?

- Management Groups
- Azure Policy
- Azure Blueprints
- Azure DevOps

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

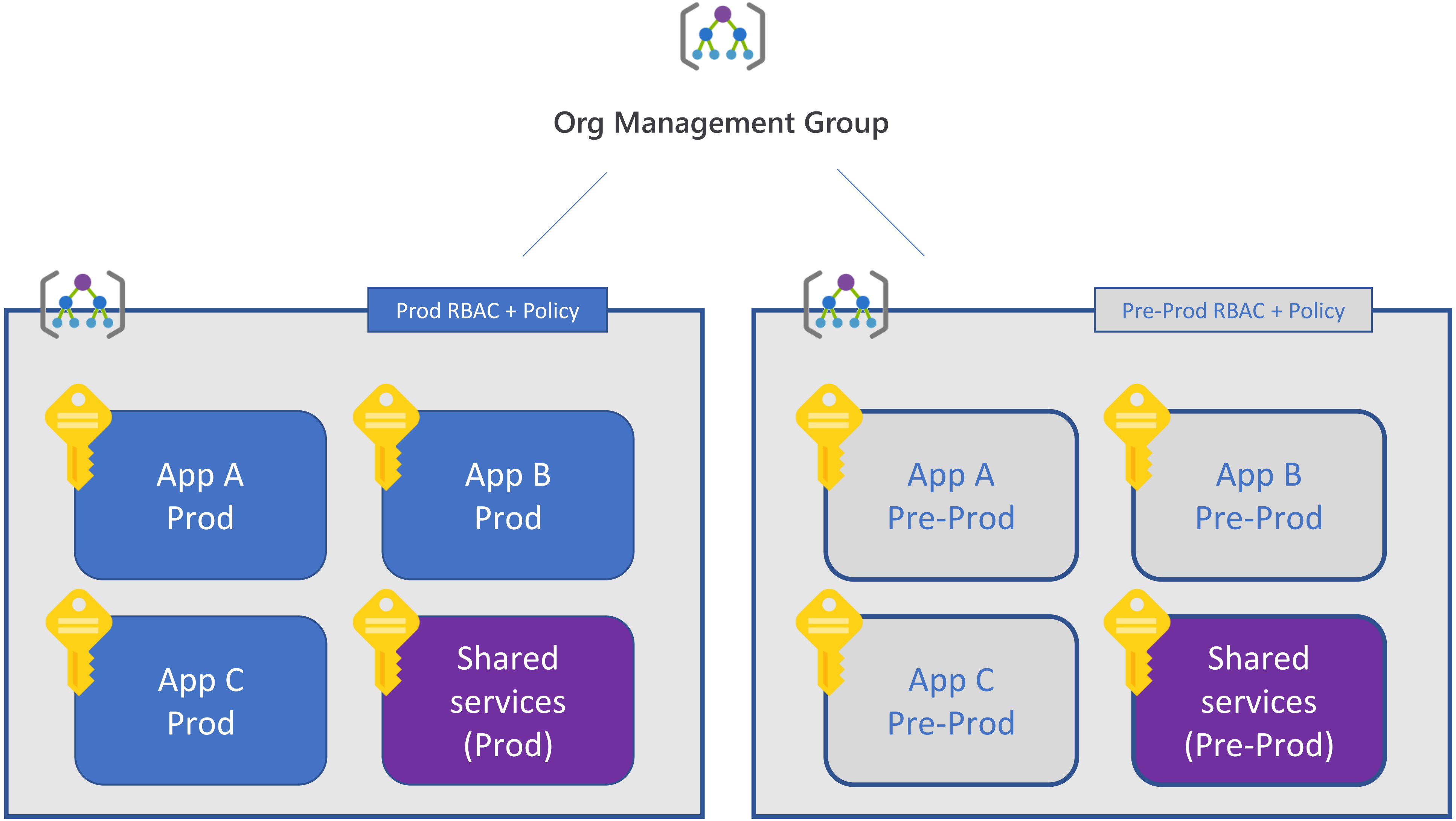
- Create a flexible hierarchy that can be updated quickly
- Hierarchy doesn’t need to model the organizations billing hierarchy
- Can easily scale up or down depending on the organizational needs

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

Modeling Strategy

Microsoft
Recommended



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

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

Remediation

Azure Policy

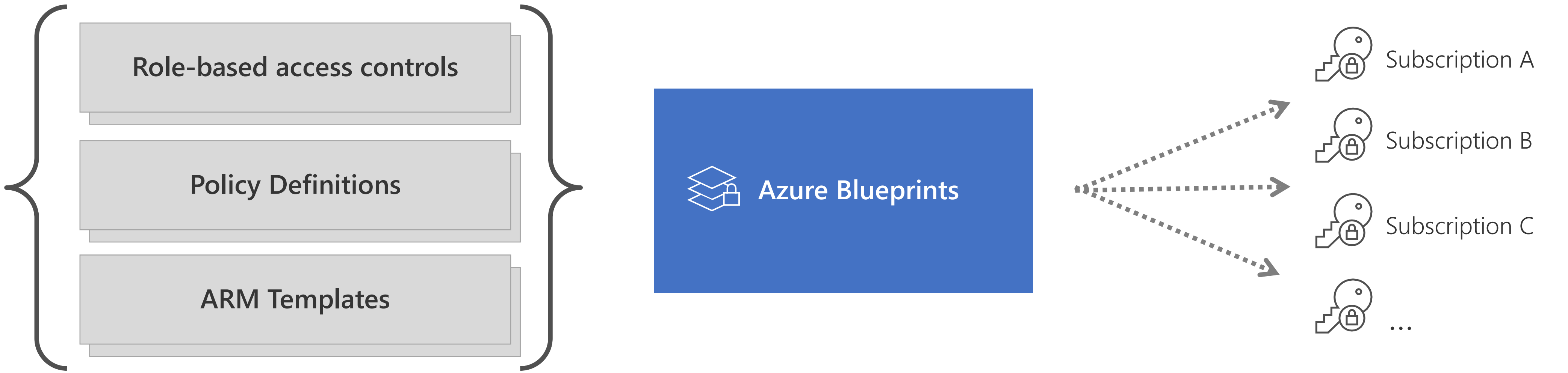
Enforcement

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

Compliance

Always On:
On Change
On Periodic Cadence
On Demand

Azure Blueprints



Role-based access controls

Policy Definitions

ARM Templates

Azure Blueprints

Subscription A

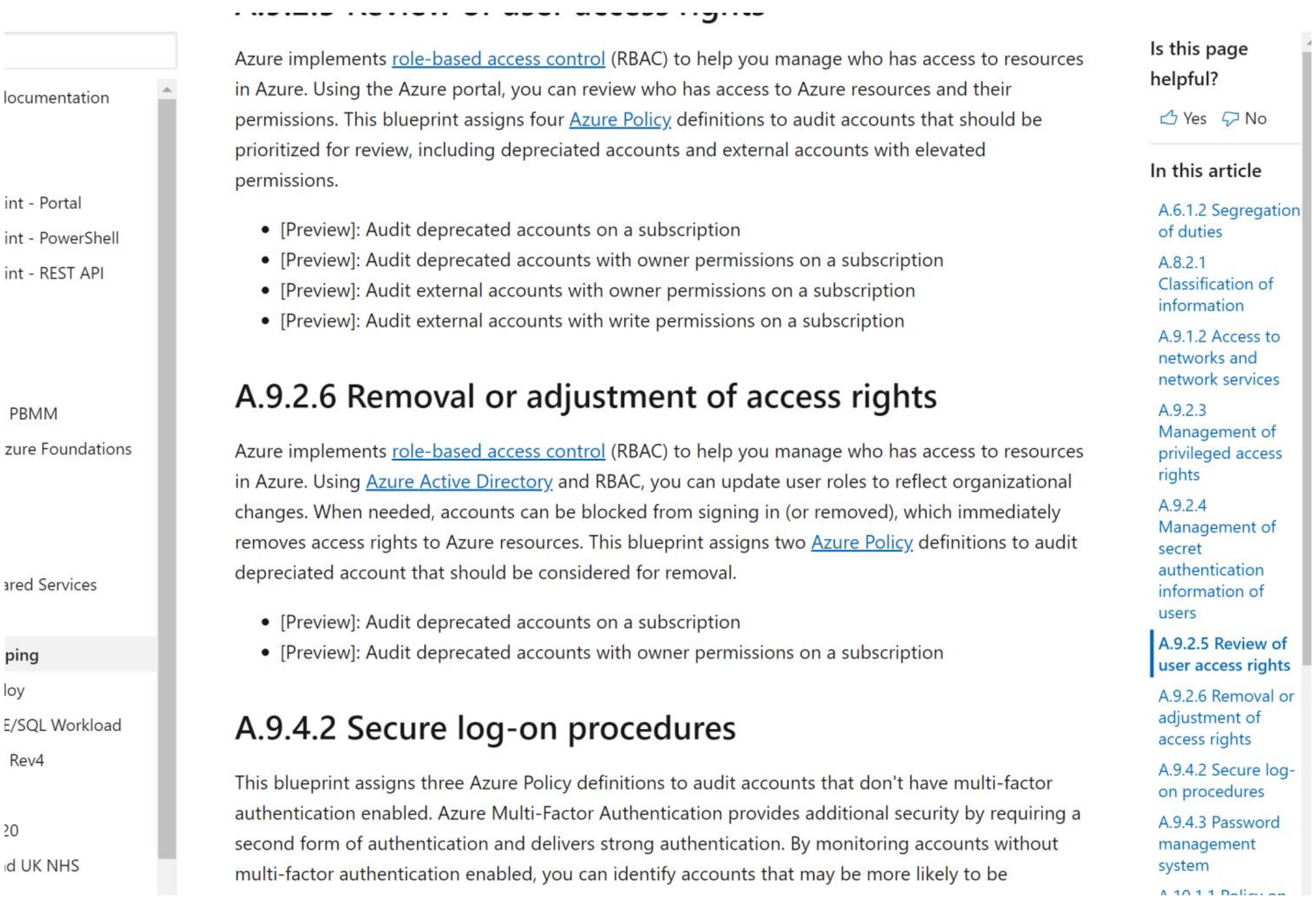
Subscription B

Subscription C

…

compose | manage | scale

ISO 27001 Control mapping


locumentation
int - Portal
int - PowerShell
int - REST API
PBMM
zure Foundations
ared Services
ping
loy
E/SQL Workload
Rev4
20
d UK NHS
Is this page helpful?
Yes
No
In this article
A.6.1.2 Segregation of duties
A.8.2.1 Classification of information
A.9.1.2 Access to networks and network services
A.9.2.3 Management of privileged access rights
A.9.2.4 Management of secret authentication information of users
A.9.2.5 Review of user access rights
A.9.2.6 Removal or adjustment of access rights
A.9.4.2 Secure log-on procedures
A.9.4.3 Password management system
A.10.1.1 Policy on

A.9.2.5 Review of user access rights

Azure implements role-based access control (RBAC) to help you manage who has access to resources in Azure. Using the Azure portal, you can review who has access to Azure resources and their permissions. This blueprint assigns four Azure Policy definitions to audit accounts that should be prioritized for review, including depreciated accounts and external accounts with elevated permissions.

- [Preview]: Audit deprecated accounts on a subscription
- [Preview]: Audit deprecated accounts with owner permissions on a subscription
- [Preview]: Audit external accounts with owner permissions on a subscription
- [Preview]: Audit external accounts with write permissions on a subscription

A.9.2.6 Removal or adjustment of access rights

Azure implements role-based access control (RBAC) to help you manage who has access to resources in Azure. Using Azure Active Directory and RBAC, you can update user roles to reflect organizational changes. When needed, accounts can be blocked from signing in (or removed), which immediately removes access rights to Azure resources. This blueprint assigns two Azure Policy definitions to audit depreciated account that should be considered for removal.

- [Preview]: Audit deprecated accounts on a subscription
- [Preview]: Audit deprecated accounts with owner permissions on a subscription

A.9.4.2 Secure log-on procedures

This blueprint assigns three Azure Policy definitions to audit accounts that don't have multi-factor authentication enabled. Azure Multi-Factor Authentication provides additional security by requiring a second form of authentication and delivers strong authentication. By monitoring accounts without multi-factor authentication enabled, you can identify accounts that may be more likely to be

The Blueprint process

1. Create Blueprint Draft
2. Publish Blueprint Definition
3. Assign Blueprint Definition
4. Repeat

Building Guard rails by example

Use Case

JJ Binks – CEO of Cloud Adventures, just landed a contract with 3 large manufacturers: *Incom-FreiTek*, *Sienar Fleet Systems* and *Astromech*.

The contract includes hosting their solutions on Microsoft Azure and implement guard rails to ensure the environments are conforming with applicable laws and regulations. Even though the industries these manufacturers operate in are largely similar – there some nuances in the required guard rails. Each company also requires a landing zone to deploy their solutions in. All environments must be separated from each other.

To simplify management for Cloud Adventures, all solutions should be managed from a single tenant with a single source of truth.

- Incom-Freitek operates out of Europe and requires their data to remain within Europe
- Sienar Fleet Systems operates out of the United States, data needs to remain within the US
- Astromech requires their data to remain in France or the West Europe Region

Use Case

JJ Binks – CEO of Cloud Adventures, just landed a contract with **3 large manufacturers**: *Incom-FreiTek*, *Sienar Fleet Systems* and *Astromech*.

The contract includes hosting their solutions on Microsoft Azure and **implement guard rails** to ensure the environments are conforming with applicable laws and regulations. Even though the industries these manufacturers operate in are largely similar – there some **nuances in the required guard rails**. Each company also requires a landing zone to deploy their solutions in. All environments must be separated from each other.

To simplify management for Cloud Adventures, all solutions should be managed from a **single tenant** with a **single source of truth**.

- **Incom-Freitek** operates out of Europe and **requires their data to remain within Europe**
- **Sienar Fleet Systems** operates out of the United States, **data needs to remain within the US**
- **Astromech** operates globally but requires **their data to remain in France or West Europe**

Use Case

- 3 large manufacturers
- Implement guard rails
- Nuances in the required guard rails
- Managed from a single tenant
- Single source of truth.

- Incom-Freitek operates out of Europe and requires their data to remain within Europe
- Sienar Fleet Systems operates out of the United States and requires their data to remain within the US
- Astromech operates globally but requires their data to remain in France or West Europe

What just happened?

- ~~3 large manufacturers~~
- ~~Implement guard rails~~
- ~~Nuances in the required guard rails~~
- ~~Managed from a single tenant~~
- Single source of truth.

Drawbacks

- Managing through the portal is quite the “Point and click adventure”
- Managing parameters for each customer can be time-consuming
- Blueprints on a Management Group level is not suited for cross-tenant management
- Blueprints are incremental
- Manual versioning

Managing your Blueprints through Azure DevOps

Blueprints as Code

- Build based on existing samples
- Leverage the Az.Blueprints PowerShell module

Use Case (continued)

JJ Binks just provisioned two new customers and leveraged Azure Blueprints to comply with industry standards and regulatory compliance.

This proved to be quite time consuming and there are signs that more companies will request services from Cloud Adventures. He is thinking of managing the Azure Blueprints as code and possibly use Azure DevOps to manage the process to overcome the repetitive actions and eliminate the chances of human error. Additionally, Astromech requested Cloud Adventures to deploy a Web App and Database for them to deploy their solution on top of.

Because Astromech is in the business of developing droids and their latest model "R2D2" seems to have a mind of it's own. JJ Binks is also looking into deploying one of his Sentinels to keep them in check.

Use Case (continued)

JJ Binks just provisioned two new customers and leveraged Azure Blueprints to comply with industry standards and regulatory compliance.

This proved to be quite **time consuming** and there are signs that more companies will request services from Cloud Adventures. He is thinking of managing the **Azure Blueprints as code** and possibly use **Azure DevOps** to manage the process to overcome the repetitive actions and eliminate the chances of human error. Additionally, Astromech requested Cloud Adventures to deploy a **Web App and Database** for them to deploy their solution on top of.

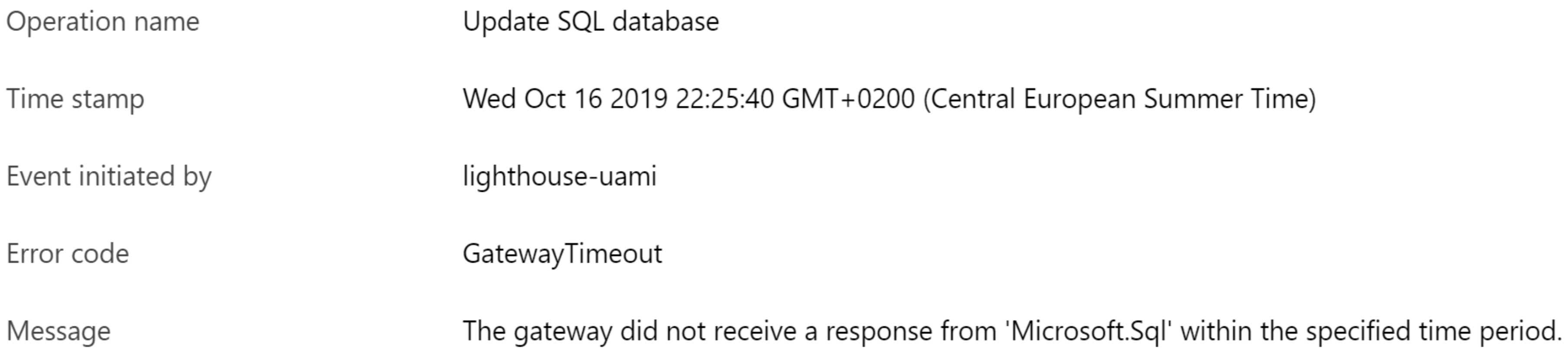
Because Astromech is in the business of developing droids and their latest model "R2D2" seems to have a mind of its own. JJ Binks is also looking into deploying one of his **Sentinels** to keep them in check.

What just happened?

- Single source of truth
- Source Control
- Versioning through Azure DevOps

Drawbacks

- Learning Curve
- Prone to Azure Resource Manager time outs
- Blueprints are always incremental



Operation name	Update SQL database
Time stamp	Wed Oct 16 2019 22:25:40 GMT+0200 (Central European Summer Time)
Event initiated by	lighthouse-uami
Error code	GatewayTimeout
Message	The gateway did not receive a response from 'Microsoft.Sql' within the specified time period.

But it’s still pretty awesome..

Thank You

@whaakman

www.linkedin.com/in/wesleyhaakman

whaakman@intercept.nl