Ce qu'il faut comprendre à la gouvernance Azure quand on est Dev

FLORENT APPOINTAIRE
DAVID FRAPPART
DAVID FRAPPART

Agenda

- Présentations
- Pourquoi la gouvernance?
- Azure RBAC
- Management Groups
- Azure Blueprint
- Azure Cost Management

Florent Appointaire

- Microsoft MVP Azure (4 times)
- Azure Solution Architect certified
- Membre aOS/SCUGBE
- Freelance Cloud Architect
  - florent@falaconsulting.be
- CSP Tier 2
- +7 ans d'expérience
- Speaker (MMSMOA, ELEU, ELNL, aOS, etc.)
- Blog: https://cloudyjourney.fr
- Twitter: @florent_app

David Frappart

- Cloud Architect @devoteam
- Agile IT core team Cloud
- ~ 15 years of experiences in IT
- A few cloud certifications:
  - Azure
  - AWS
  - GCP
- Recently nominated MVP, because I speak a lot
- Fonds of Terraform as a IaC tool
- Currently decrypting the complexity of the K8S for my clients, thus the talk tonight

Pourquoi la gouvernance?

- Donner les bons droits aux bonnes personnes (Azure RBAC)
- Appliquer des polices pour un meilleur contrôle (Azure Policy)
- Séparations des ressources pour une meilleure visibilitée (Management Groups)
- Application d'un template de base sur les souscriptions (Azure Blueprint)
- Gestion des coûts (Azure Cost Management)

Azure RBAC

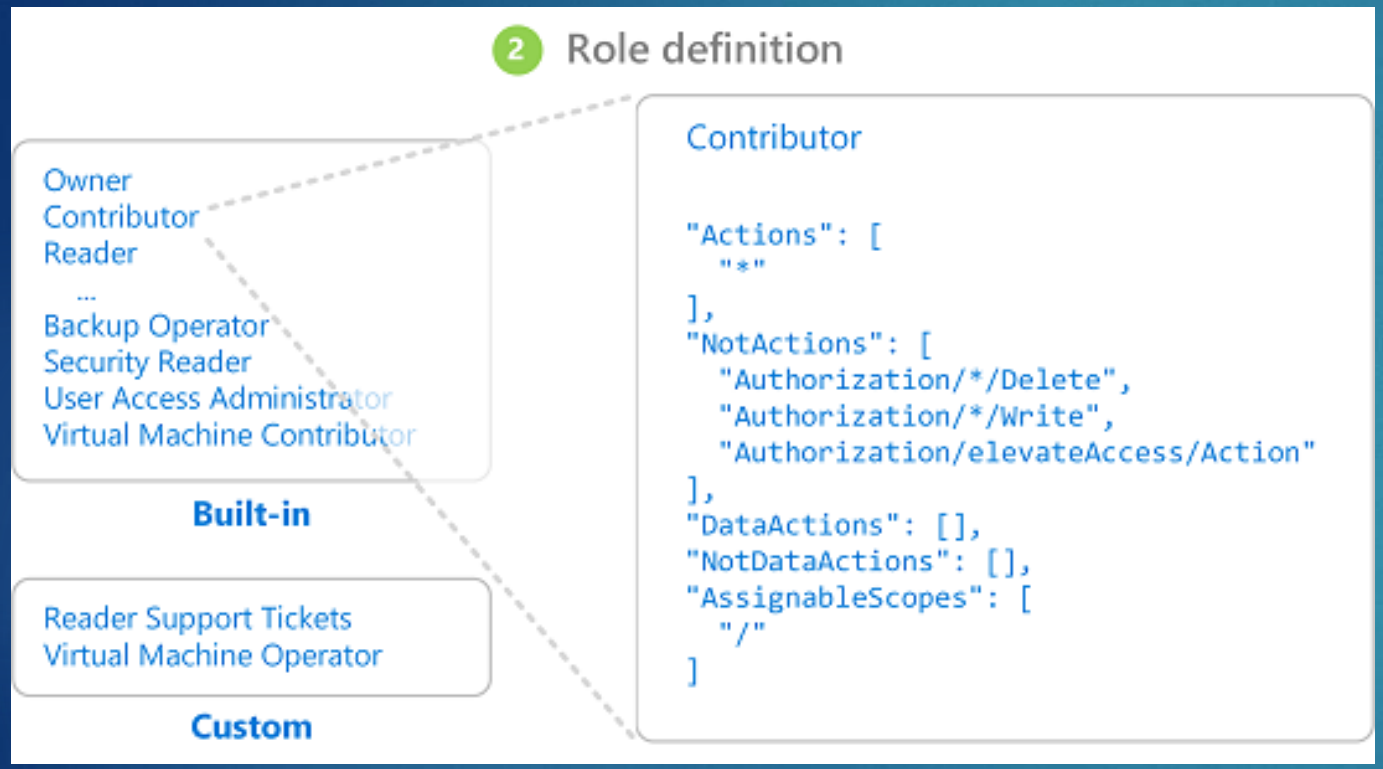
- RBAC = Role Based Access Control
- RBAC dans le portail Azure: IAM (Access Control)
- ROLE est la clé, il définit le niveau d'accès à une ressource / groupe de ressources:
  - utilisateur (ex. Votre admin système)
  - groupe (ex. SQL DBA's)
  - service principal (ex. votre SQL VM)
  - managed identity (ex. votre SQL service account)
- La création de rôles personnalisés possible (JSON)

Azure RBAC

- Toujours ce poser les 3 questions suivantes:
  - 1) QUI a besoin d'avoir accès? – Un utilisateur, un groupe, un service principal ou une managed identity
  - 2) QUELLES permissions a-t-il besoin? – Les permissions sont groupées à des rôles. Vous pouvez sélectionner des rôles built-in ou créer les votres
  - 3) OÙ doit-il avoir accès? – Où les permissions doivent être appliquées? Sur une ressource, un groupe de ressource ou une souscription. On appelle ceci le scope.

- https://docs.microsoft.com/en-us/azure/role-based-access-control/overview

Azure RBAC




```
{
 "Name": "Virtual Machine Operator",
 "Id": "42da8e3e-d841-4764-84d6-4429b524ba42",
 "IsCustom": true,
 "Description": "Can start/stop/restart virtual machines.",
 "Actions": [
  "Microsoft.Storage/*/read",
  "Microsoft.Network/*/read",
  "Microsoft.Compute/*/read",
  "Microsoft.Compute/virtualMachines/start/action",
  "Microsoft.Compute/virtualMachines/powerOff/action",
  "Microsoft.Compute/virtualMachines/restart/action",
  "Microsoft.Compute/virtualMachines/deallocate/action",
  "Microsoft.Authorization/*/read",
  "Microsoft.Resources/subscriptions/resourceGroups/read",
  "Microsoft.Support/*"
 ],
 "NotActions": [
 ],
 "AssignableScopes": [
  "/subscriptions/34ff03e8-f173-47d4-879c-ba30a0683e0b"
 ]
}
```


LIVE DEMO

Azure Policy

- Azure Policies donne la possibilité d'auditer/refuser la création/configure les ressources sur Azure
- Ceci peut être appliqué sur un Management Group, une souscription,un Resource Group, ou une Resource
- **Azure Policy est gratuit, utilisez le!**

- https://docs.microsoft.com/en-us/azure/governance/policy/overview

Azure Policy


```
{
  "properties": {
    "displayName": "Restrict Public IP",
    "policyType": "Custom",
    "mode": "All",
    "description": "Restrict Public IP resource from being associated to a NIC",
    "policyRule": {
      "if": {
        "allOf": [
          {
            "field": "type",
            "equals": "Microsoft.Network/networkInterfaces"
          },
          {
            "field": "Microsoft.Network/networkInterfaces/ipconfigurations[*].publicIpAddress.id",
            "exists": true
          }
        ]
      },
      "then": {
        "effect": "deny"
      }
    }
  },
  "id": "/subscriptions/af77b8c1-97e3-4145-94b6-bba6e4dd5972/
providers/Microsoft.Authorization/policyDefinitions/restrict-public-ip",
  "type": "Microsoft.Authorization/policyDefinitions",
  "name": "restrict-public-ip"
}
```

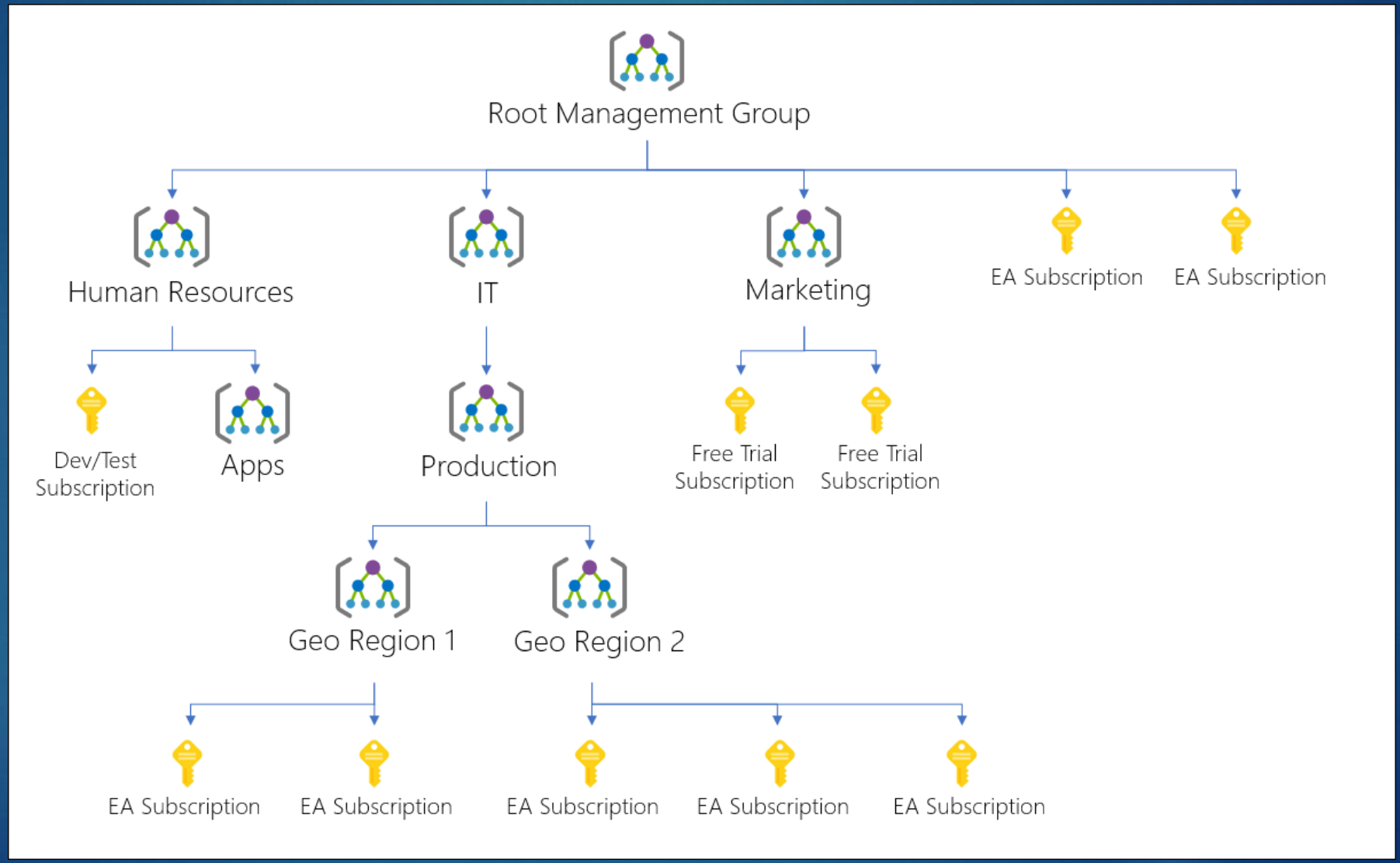

LIVE DEMO

Management Groups

- Organisation: Groupez vos souscriptions en fonction du business et de l'environnement
- Scale Management: les rôles RBAC et les Policy inhéritent d'en bas
- Exceptions: les Policy peuvent être controllées par "exception"
- Flexibilité: Peut être mis à jour/bougé entre les souscriptions Azure si vous décidez de changer dont les choses doivent s'organizer plus tard
- NOTE: Maximum 6 niveaux

- https://docs.microsoft.com/en-us/azure/governance/management-groups/overview

Management Groups




LIVE DEMO

Azure Blueprint (Preview)

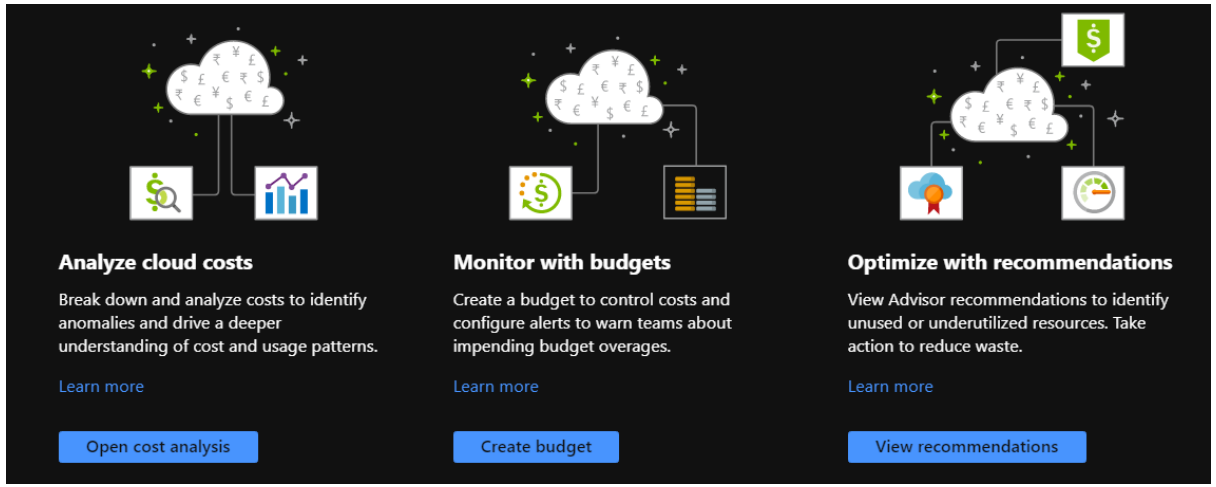
- Automatisation du déploiement de vos ressources de base
  - Groupe de ressources
  - Polices
  - Permissions
  - Templates ARM
- Sécurisation des options de déploiement de base avec Azure Policy

- https://docs.microsoft.com/en-us/azure/governance/blueprints/overview


LIVE DEMO

Azure Cost Management

- Support de tout type de souscription (même le CSP depuis le 19/11) sauf les souscriptions Sponsorship
- Gestion du coût et des alertes
- Recommandations Microsoft pour économiser de l'argent



- https://docs.microsoft.com/en-us/azure/cost-management/overview-cost-mgt


LIVE DEMO

THANKS TO

ONIRYX

Make IT happen

CORILUS

Connecting Care

digital wallonia .be

GENESIS CONSULT

IT Consultancy Services

Microsoft

Références

Satellit

DEDICATED EXPERTS DELIVER

ingenico

ePayments