

Azure Policy

w akcji, po co to komu?



@RogalaPiotr



justcloud



Microsoft Azure
User Group Poland



About me: Piotr Rogala

Currently working in  **Nordcloud**

Azure Cloud Architect Lead

Blog  

MVP Azure

Group leader  Microsoft Azure
User Group Poland



 @RogalaPiotr

 linkedin.com/in/rogalapiotr

Questions?

JustCloud.pl

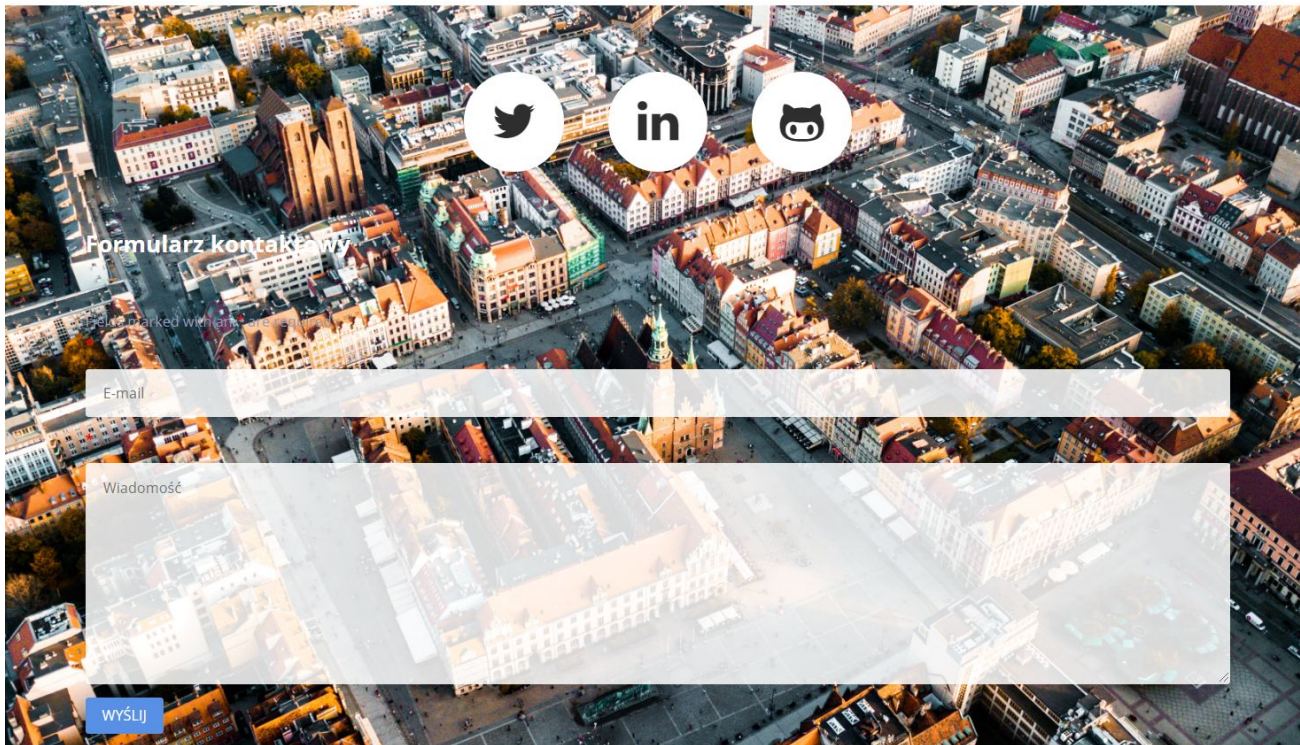
[O MNIE](#)

[BLOG](#)

[AKTUALNOŚCI](#)

[MEETUP'Y](#)

[KONTAKT](#)



Formularz kontaktowy

Fields marked with an asterisk are required

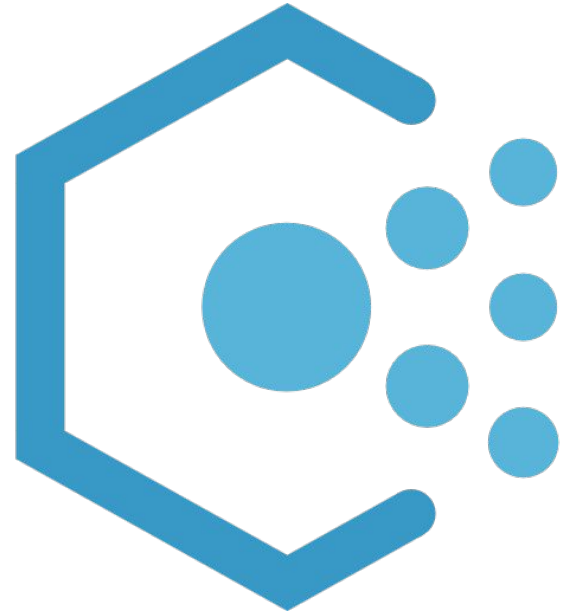
E-mail *

Wiadomość *

WYŚLIJ

Agenda

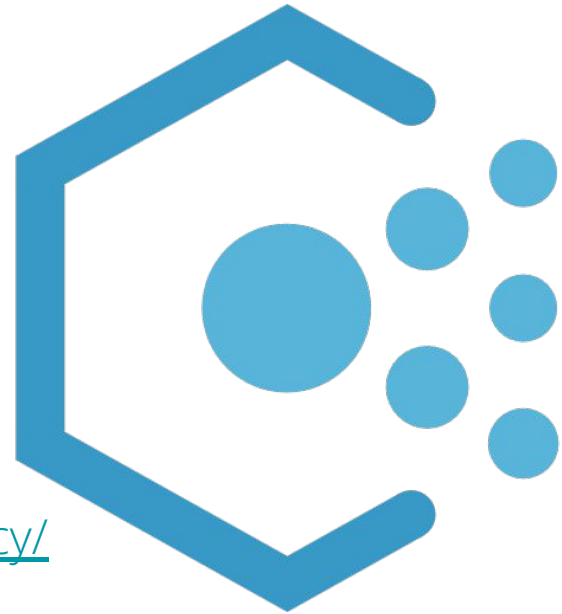
1. Co to jest Azure Policy?
2. Po co komu Azure Policy?
3. Przypadki użycia Azure Policy



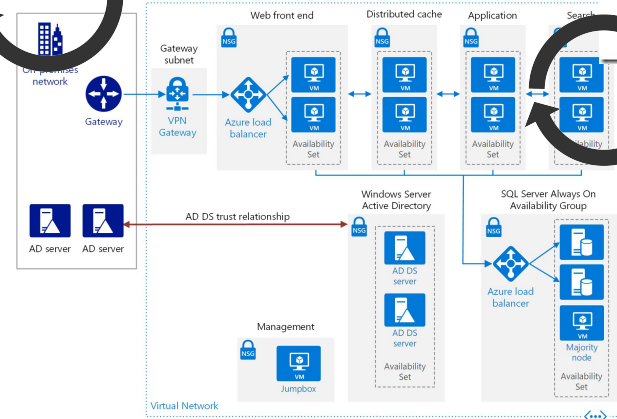
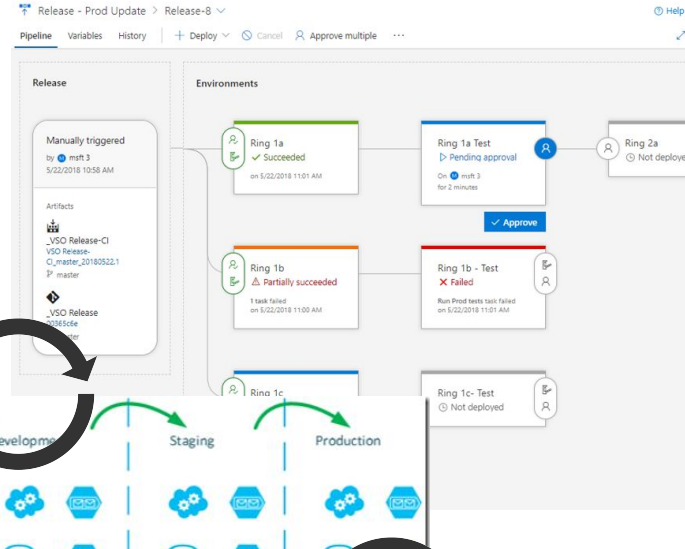
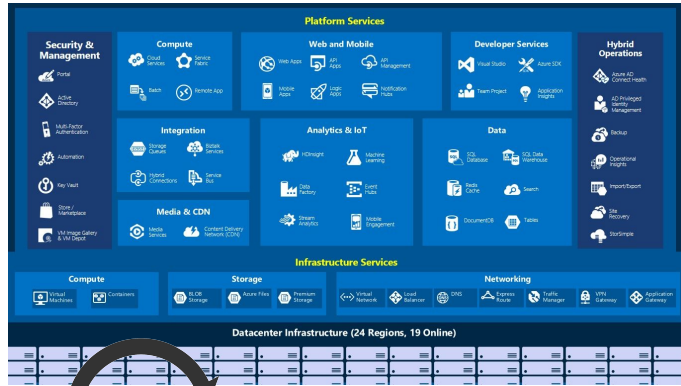
Azure Policy

1. Enforcing organizational standards
2. Remediation for existing resources and automatic remediation for new resources
3. Remediating non-compliant resources
4. Compliance dashboard
5. Policy Definitions (JSON format)
6. Policy Initiative (Group)

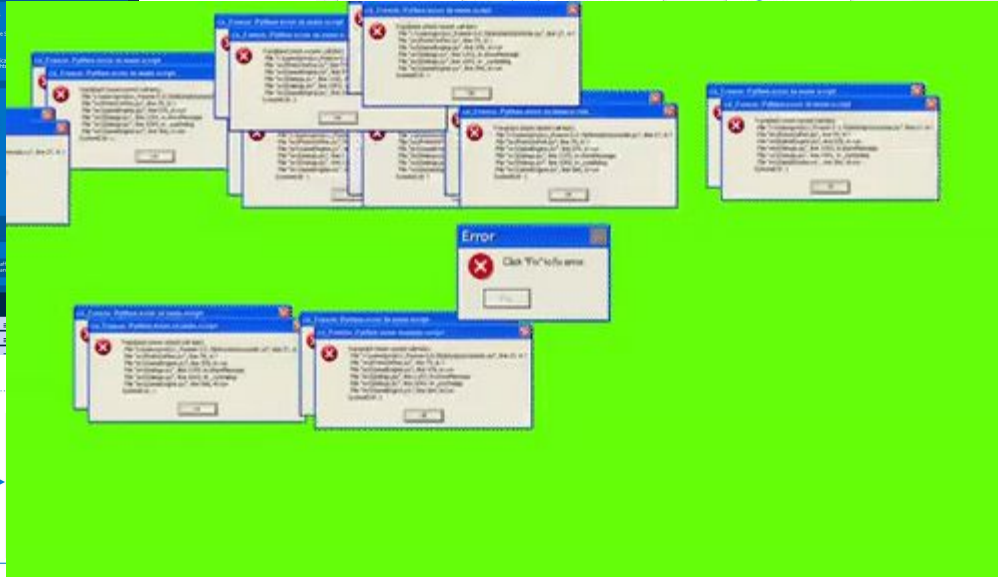
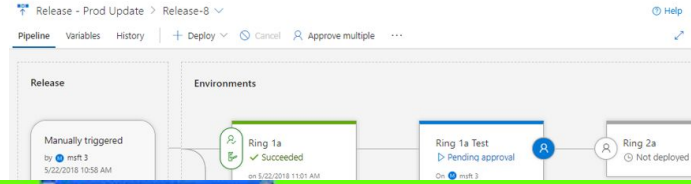
<https://docs.microsoft.com/en-us/azure/governance/policy/>



Cloud - Microsoft Azure

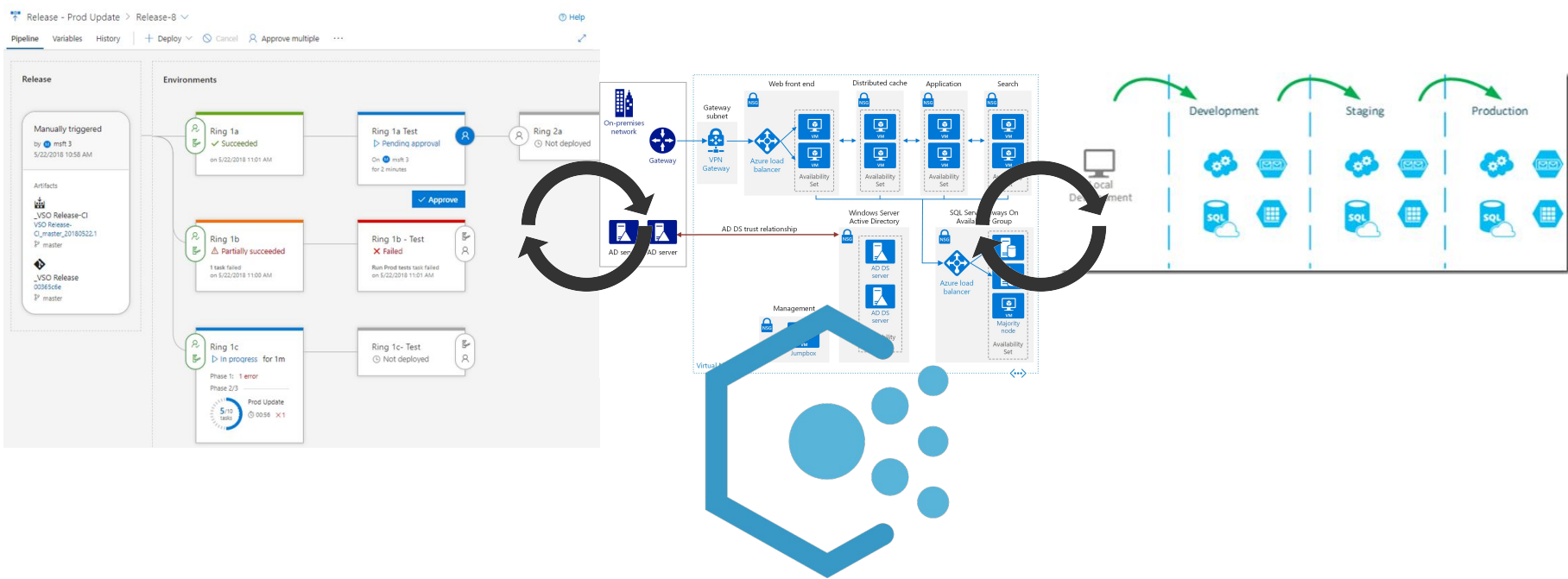


Cloud - Microsoft Azure



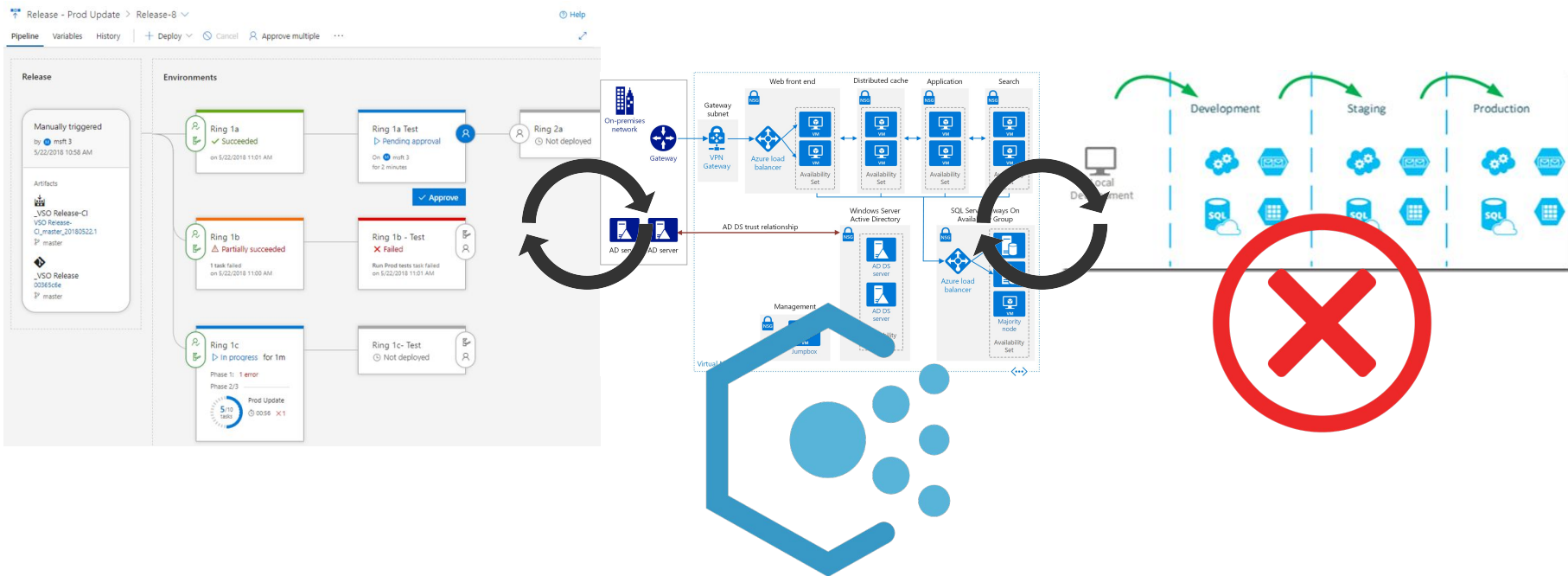
Azure Policy

- Regions
- Resources

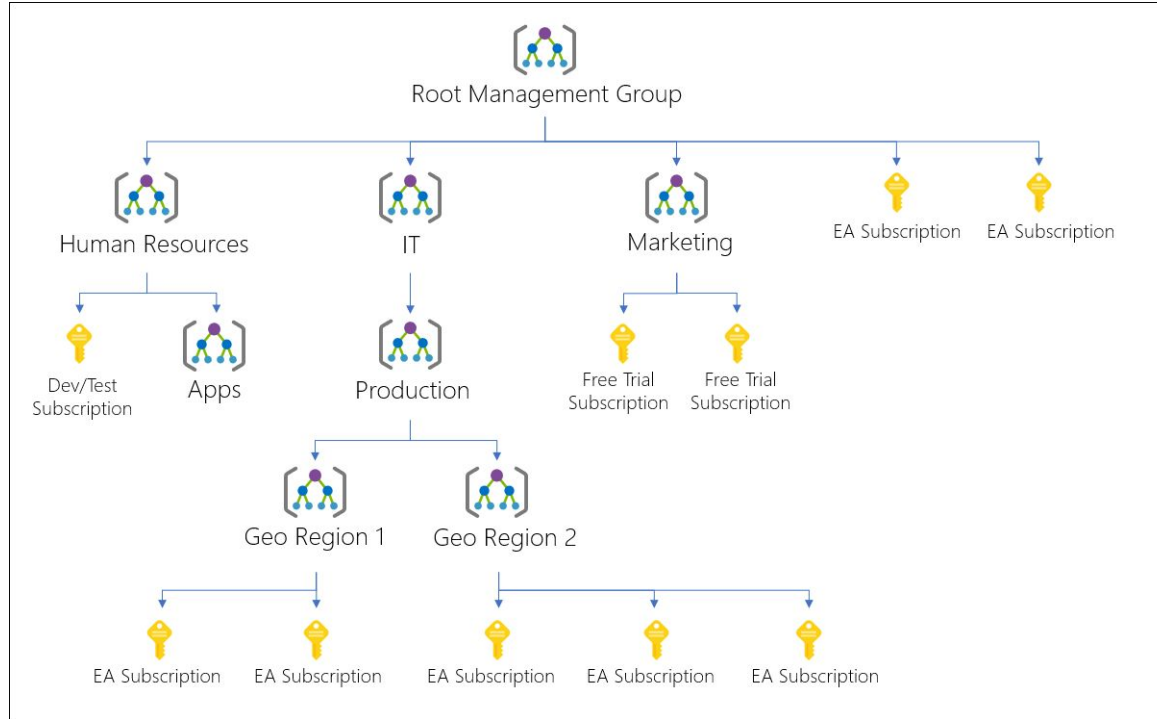


Azure Policy

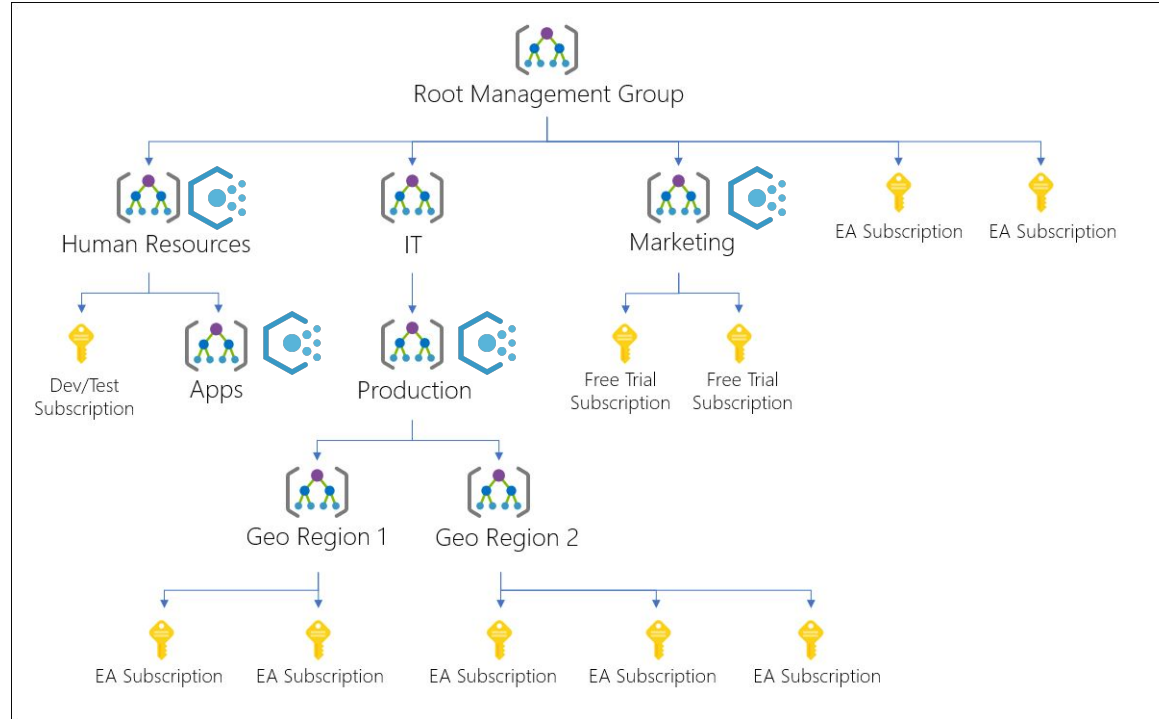
- Regions
- Resources



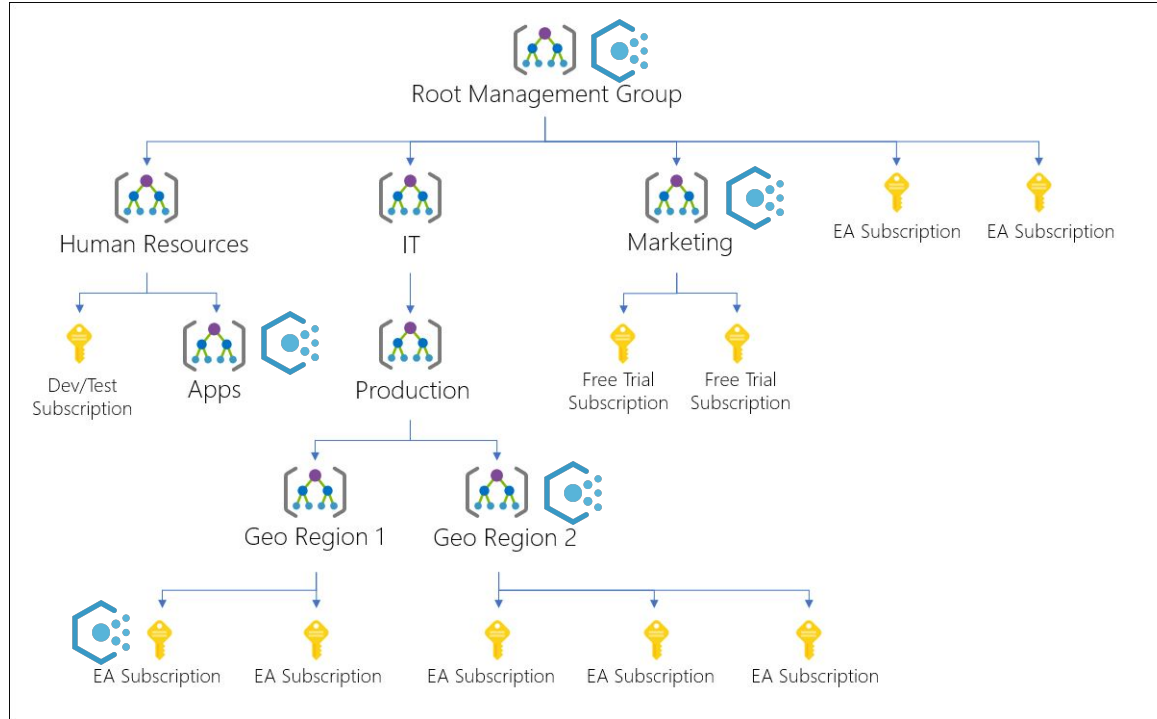
Management Groups



Management Groups

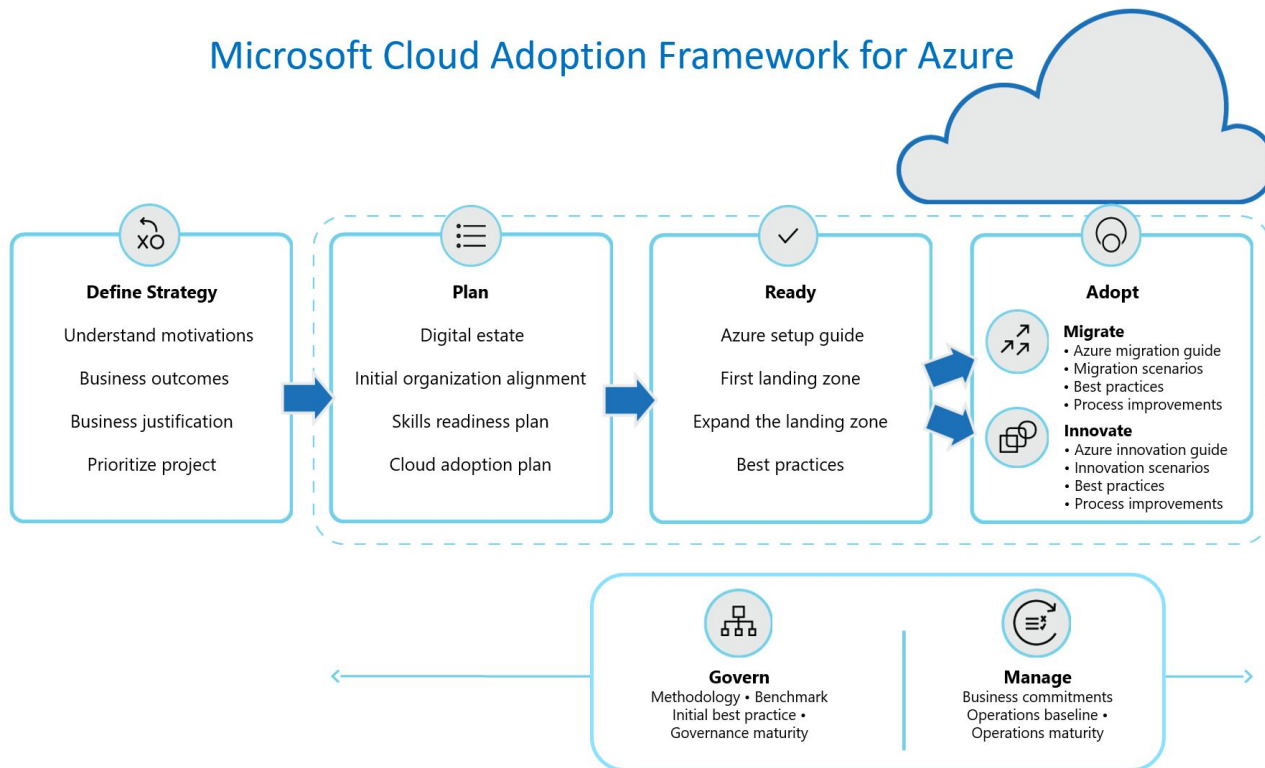


Management Groups



Cloud Adoption Framework

Microsoft Cloud Adoption Framework for Azure



Policy types

- **Audit: generates a warning event in activity log but doesn't fail the request**
- AuditIfNotExists: generates a warning event in activity log if a related resource doesn't exist
- **Allow/Deny: generates an event in the activity log and fails the request**
- **DeployIfNotExists: deploys a related resource if it doesn't already exist**
- Modify: adds, updates, or removes the defined tags from a resource
- EnforceOPAConstraint (preview): configures the Open Policy Agent admissions controller with Gatekeeper v3 for self-managed Kubernetes clusters on Azure (preview)
- EnforceRegoPolicy (preview): configures the Open Policy Agent admissions controller with Gatekeeper v2 in Azure Kubernetes Service

<https://docs.microsoft.com/pl-pl/azure/governance/policy/concepts/definition-structure>

Policy examples


- Set up Diagnostics on resources:
 - <https://github.com/Azure/Community-Policy/tree/master/Policies/Monitoring>
- Set up Tags or allow only defined
 - <https://github.com/Azure/Community-Policy/tree/master/Policies/General/enforce-tag%2Bvalue-to-select-types>
- Deploy geo-redundant storage accounts
 - <https://github.com/Azure/Community-Policy/tree/master/Policies/Storage/deploy-geo-redundant-replication>

ASC - Azure Security Center

[Dashboard](#) > [Security Center](#) | [Security policy](#) > Security policy



Security policy

Microsoft Azure Sponsorship

 New content is available for the Azure CIS standard. Update your view by clicking on 'Add more standards' below and selecting Azure CIS 1.1.0 (new), or click [here](#).

Security policy on: Microsoft Azure Sponsorship



Policies assigned in this subscription

 **Security center default policy**

ASC default (1 assignments)

This is the default policy for Azure Security Center recommendations which is enabled by default on your subscription.

[View effective policy](#)

 **Industry & regulatory standards**

Compliance policies that you can view in the compliance dashboard. To add more compliance standards, click **Add more standards**.

Azure CIS 1.1.0	Track Azure CIS 1.1.0 controls in the Compliance Dashboard, based on a recommended set of policies and assessments.	Out of the box
PCI DSS 3.2.1	Track PCI-DSS v3.2.1:2018 controls in the Compliance Dashboard, based on a recommended set of policies and assessments.	Out of the box
ISO 27001	Track ISO 27001:2013 controls in the Compliance Dashboard, based on a recommended set of policies and assessments.	Out of the box
SOC TSP	Track SOC TSP controls in the Compliance Dashboard, based on a recommended set of policies and assessments.	Out of the box

[Add more standards](#)

Policy initiative - ASC

Compliance state ⓘ



Non-compliant

Overall resource compliance ⓘ

88%

187 out of 212

Non-compliant policies ⓘ

26

out of 99

Non-compliant resources ⓘ

25

out of 212

Events (last 7 days) ⓘ

Audit 8

Append 0

Modify 0

Deny 0

Deploy 0

Policies Non-compliant resources Events

Filter by policy name or definition id...

All compliance states

Name	↑↓ Effect Type	↑↓ Compliance state	↑↓ Non-Compliant Resources	↑↓ Total resources
Just-In-Time network access control should be applied on virtual mac...	AuditIfNotExists	✖ Non-compliant	8	8
Adaptive Application Controls should be enabled on virtual machines	AuditIfNotExists	✖ Non-compliant	8	8
Vulnerabilities in security configuration on your machines should be r...	AuditIfNotExists	✖ Non-compliant	8	8
Monitor missing Endpoint Protection in Azure Security Center	AuditIfNotExists	✖ Non-compliant	8	8
Disk encryption should be applied on virtual machines	AuditIfNotExists	✖ Non-compliant	8	8
Vulnerabilities should be remediated by a Vulnerability Assessment s...	AuditIfNotExists	✖ Non-compliant	8	8
[Preview] Vulnerability Assessment should be enabled on Virtual Mac...	AuditIfNotExists	✖ Non-compliant	8	8
Vulnerabilities in container security configurations should be remedia...	AuditIfNotExists	✖ Non-compliant	8	8
Automation account variables should be encrypted	Audit	✖ Non-compliant	7	7
System updates should be installed on your machines	AuditIfNotExists	✖ Non-compliant	7	8
Adaptive Network Hardening recommendations should be applied o...	AuditIfNotExists	✖ Non-compliant	7	8
DDoS Protection Standard should be enabled	AuditIfNotExists	✖ Non-compliant	6	6
Internet-facing virtual machines should be protected with Network S...	AuditIfNotExists	✖ Non-compliant	5	8

Policy limitation

Where	What	Maximum count
Scope	Policy definitions	500
Scope	Initiative definitions	100
Tenant	Initiative definitions	1,000
Scope	Policy or initiative assignments	100
Policy definition	Parameters	20
Initiative definition	Policies	100
Initiative definition	Parameters	100
Policy or initiative assignments	Exclusions (notScopes)	400
Policy rule	Nested conditionals	512
Remediation task	Resources	500

Policy costs

Azure Policy — cennik

✓ Żadnych kosztów ponoszonych z góry ✓ Żadnych opłat za rezygnację

Wypróbuj bezpłatnie >

Informacje: [Azure Policy — omówienie](#) [Dokumentacja](#) [Kalkulator](#)



Azure Policy

Za korzystanie z usługi Azure Policy nie są naliczane żadne opłaty.

Azure Policy - Strategy

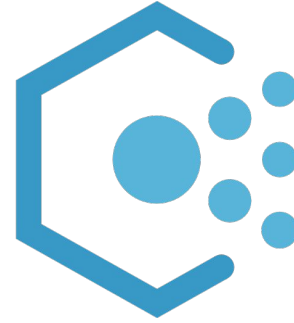
- IaC
 - Should I use Azure Policy?
- Hidden automation - Azure Policy
 - Less code in DevOps
- Security compliance
 - SOC requirements
- Corporate reasons
 - Company standards
- Banks market
 - Zero trust

Azure Policy - How to start?

- Examples: Powershell / Portal / CLI
 - <https://docs.microsoft.com/en-us/azure/governance/policy/assign-policy-powershell>
- Examples: Azure DevOps
 - <https://docs.microsoft.com/en-us/azure/devops/pipelines/policies/azure-policy?view=azure-devops>
- Basic support (docs)
 - No tools for management
- GitHub
 - <https://github.com/Azure/azure-policy/tree/master/samples/ResourceGroup>
 - <https://github.com/Azure/Community-Policy/tree/master/Policies/General/enforce-tag%2Bvalue-to-select-types>





Demo


- 3 resource groups
 - Remediation on RG1
 - Deployment VM without extension - RG2
 - Assigned policy
 - Deployment VM with extension - RG3
 - Assigned policy



Log Analytics Policy - Diagnostics Settings

- <https://github.com/DeanCefola/Azure-Policy/tree/master/Log%20Analytics>

 .vs	reload with corrections	11 months ago
 LogAnalytics.json	Merge branch 'master' of https://github.com/DeanCefola/Azure-Policy	11 months ago
 LogAnalytics-Diag-Settings.ps1	reload with corrections	11 months ago
 readme.md	reload with corrections	11 months ago

 readme.md

Create Azure Policy & Initiative for 47 resource types to be protected by Log Analytics Workspace

Azure Policy to add Log Analytics on Azure Resources Diagnostics settings: 47 Resource Types covered...so far

To deploy the ARM template with the policy and initiatives do the following:

```
New-azurermdployment -name 'policies' -templatefile 'C:\temp\LogAnalytics.json' -location 'eastus2' -verbose
```

Azure Policy - Recommendations

1. Start with an audit
2. Consider organizational hierarchies
3. Start from one assigned policy
4. Use the standard policies in the portal
5. Find a compromise between standards/automation



Questions?

JustCloud.pl

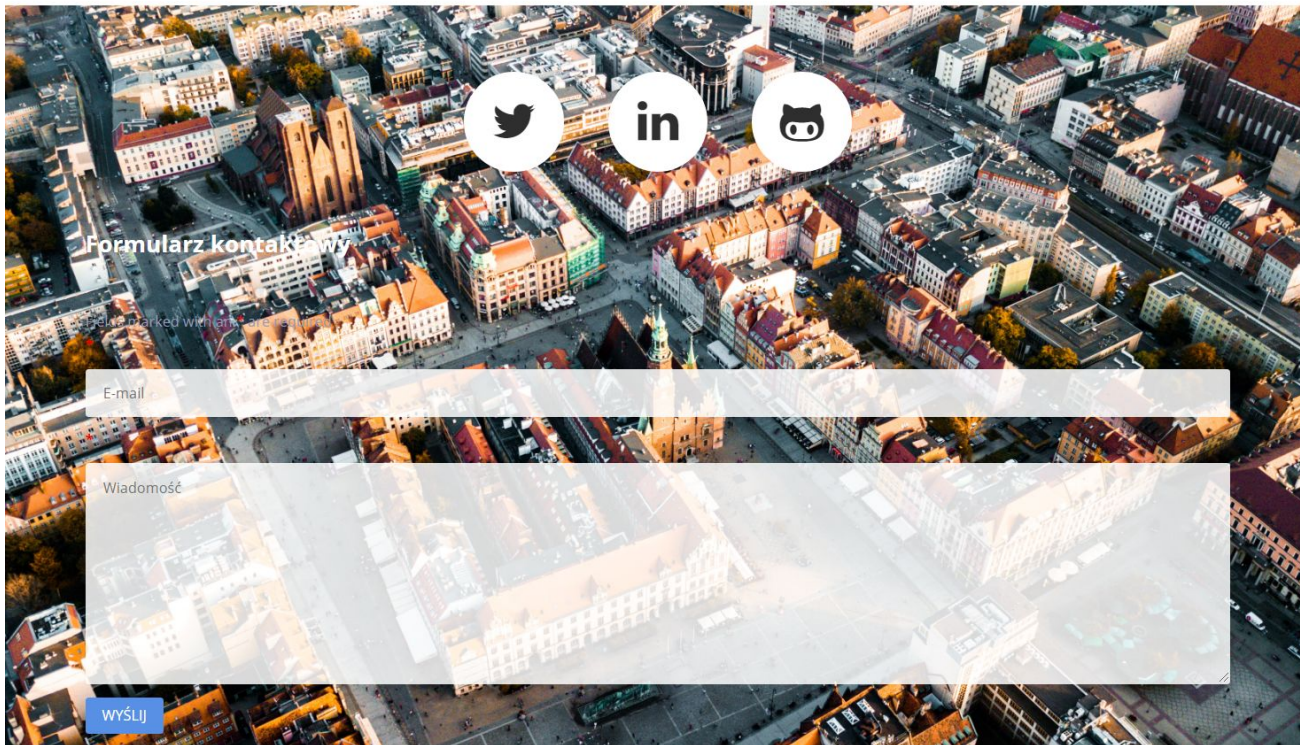
[O MNIE](#)

[BLOG](#)

[AKTUALNOŚCI](#)

[MEETUP'Y](#)

[KONTAKT](#)



Formularz kontaktowy

E-mail

Wiadomość

WYŚLIJ