Streamlining Azure Policy Exemptions with Azure Functions

Jason Rappaport
DevOps Engineer, Princeton University
The situation

- Many languages
- Many DevOps Projects within an ORG
- Many ORGs
The Project

• Provide a shared mechanism for creating Azure Policy exemptions.
Project Toolbox

- Azure DevOps
- Azure Resources
- Programming Languages
- Code Editor
Resource deployment scopes

1. Sub: Creating the resource group
2. Group: Function Resources within a resource group
3. Group: Centrally stored KeyVault Secret (shared services resource group)
4. MG: Role assignment
Release Deployment Methodology

1. Plan
2. Review
3. Do
4. Test
5. Eat your own dog food
Exemption Function API Resources
Shared Services Resource Group

- keyVault
  - secrets

- KVdiagn
  - settings
diagnosticSettings

- logAnal
  - rkspace
workspaces

- ringURL
  - secrets
IAM Management Group Role
Use Case: Kion Cost Management Exports

Grant the Container Permissions

To manage your billing data, your storage container must be enabled for blob storage. This part of the process is done in the Azure Portal.

1. In the Azure Portal, navigate to Cost Management > Exports.
2. Click the name of your export.
3. Click the link next to Storage account.
4. In the left menu, click Containers.
5. Click the Role Assignments tab.
6. Click Add.
7. In the Role dropdown, select Storage Blob Data Reader.
8. In the Assign access to dropdown, select User, group, or service principal.
9. In the Select dropdown, select your Kion app registration.
Demo: Kion Cost Management Exports (~3 minutes)

- Release pipeline inclusion of exemption function
- Actual code to invoke
- Results from release pipeline for an exemption
- Policy exemption in Azure
Creating Azure Policy Exemptions using the Azure Exemptions tool

KB0013843
12 views

To ensure the security of your resources, we use Azure Policies to define and enforce policies to meet compliance requirements. However, you may need to create exemptions for certain policies. In this article, we will discuss the exemption features for the Azure policy and the Security Implications of creating policy exemptions.

Security Implications

Creating policy exemptions can have security implications. Exemptions should only be created after careful consideration and require CAB review (see KB0013947). You should ensure that the exemption is necessary, any mitigations in place, and that it does not compromise your compliance requirements. You should also consider the potential impact on the security of your resources.
Lessons Learned

Azure Resources
• Daily cost is < $0.01
• Redeployment was a pain

DevOps
• Deployment sometimes fails, then works
• AZ deployment what-if is noisy
• Task variables (inline vs script)
• Bicep variables and token replacement
• Classic interface vs pipeline as code
Future Work

Exemption Governance
- Exemption request documentation
- Exemption attestation process
- Allowable exemptions

DevOps/ Code
- Create exemptions on RGs
QUESTIONS?