
WELKOM BIJ
dotnet
friday
Vrijdag 1 december 2023

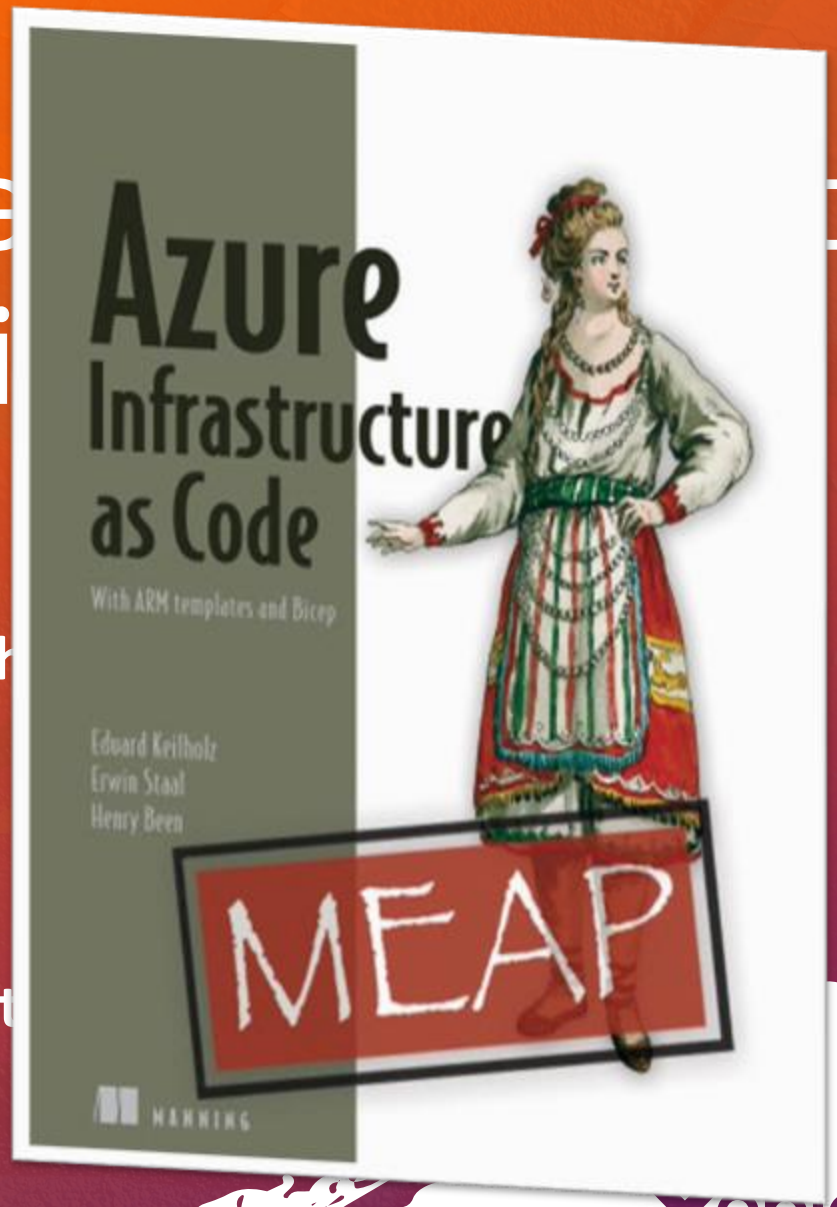
Govern your Azure
through Azure Poli

Patrick de Kruijf - Azure Arch

https://www.linkedin.com/in/patrickdk
https://www.azurefreakconfessions.com

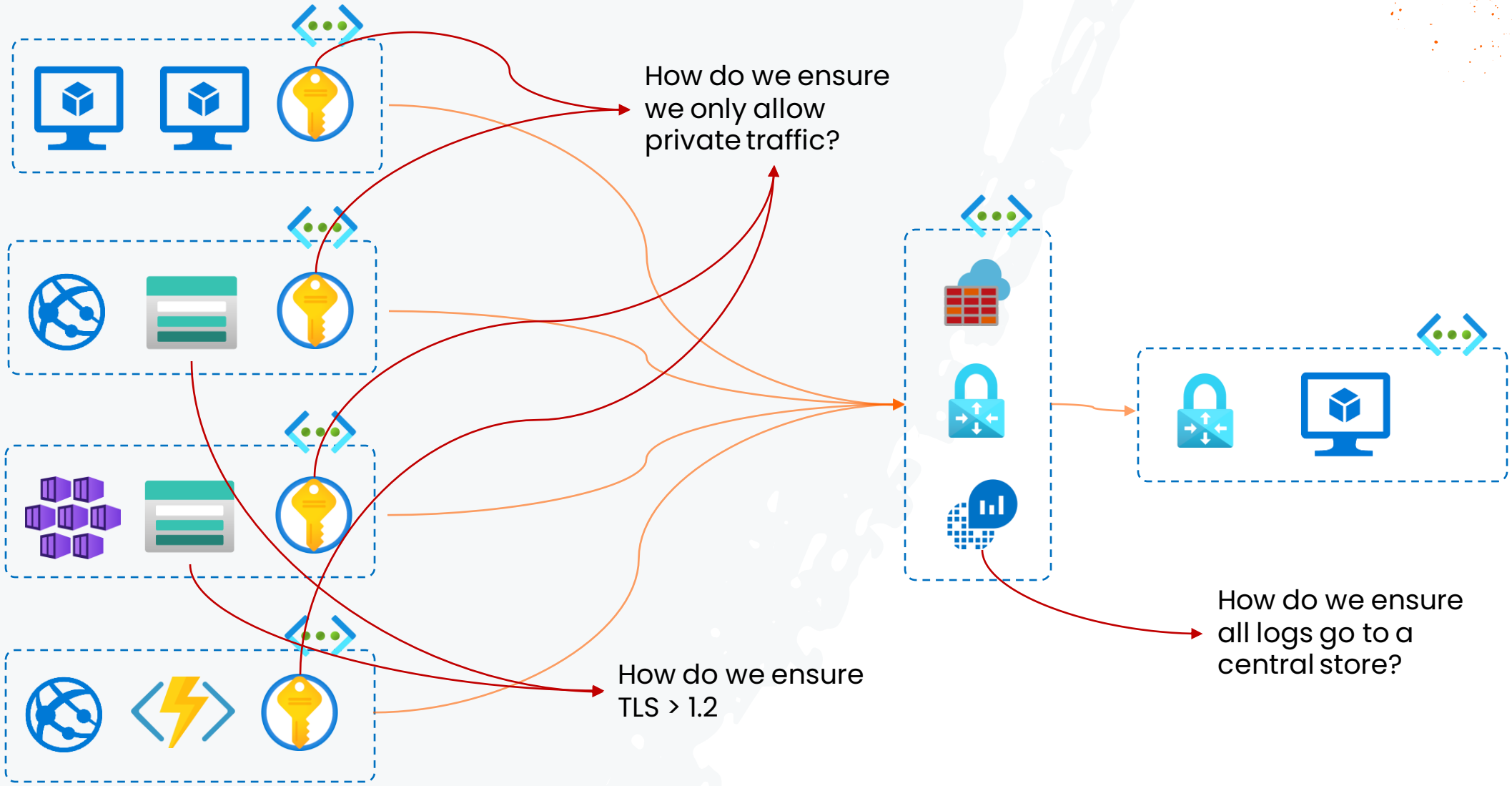
Erwin Staal - Azure Architect

@erwin_staal
https://www.linkedin.com/in/erwinstaal
https://www.erwinstaal.nl



Xebia | Xpirit

Why use Azure Policy?



Azure Policy

It helps organizations establish and maintain governance standards by defining and enforcing rules and best practices for resource configurations.

Governance Framework

Azure Policy operates on a rule-based system, where policies are authored using JSON and consist of conditions and effects.

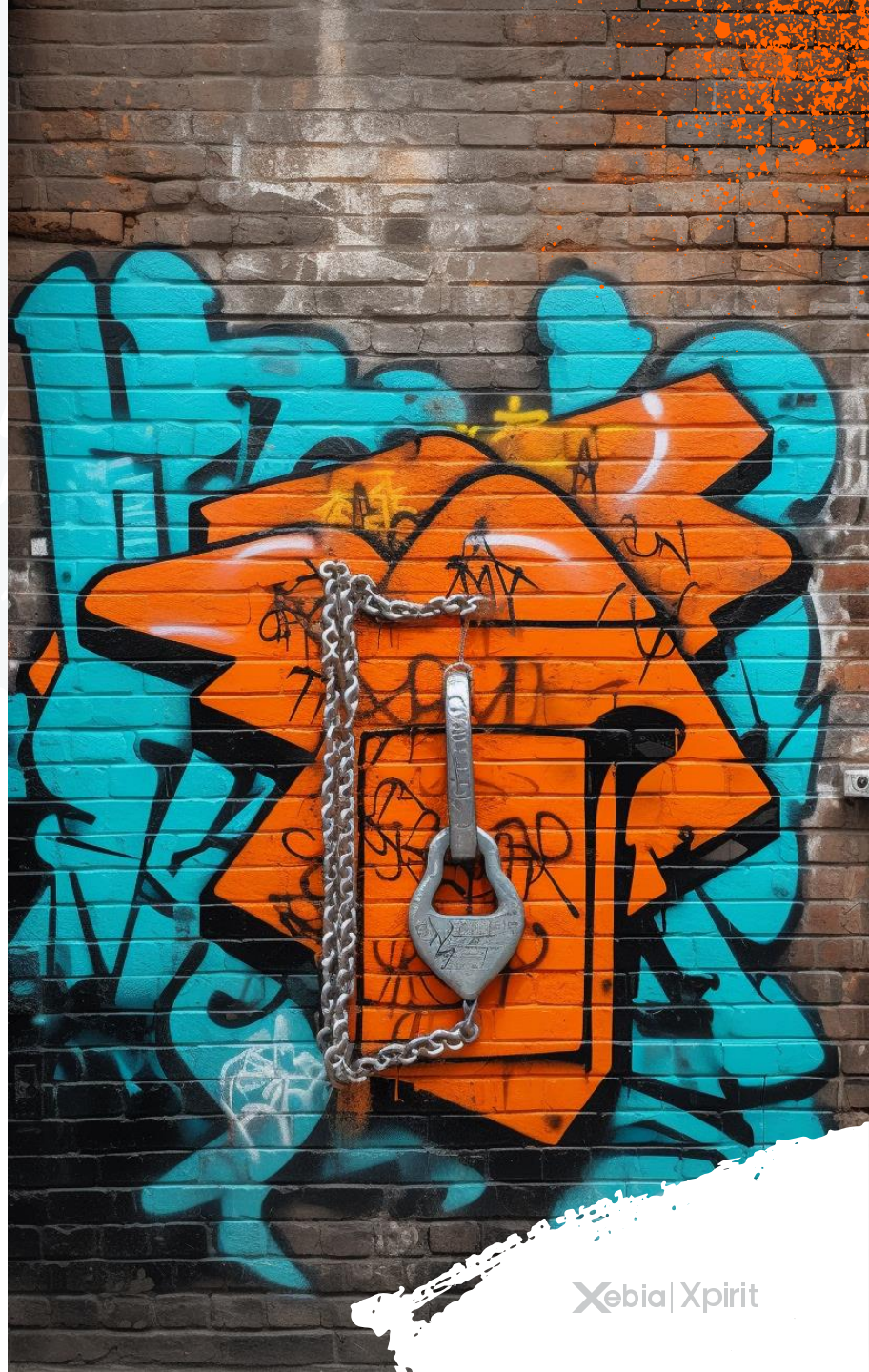
Rule-Based Enforcement

Azure Policy provides monitoring and reporting capabilities to track compliance status across the Azure resources.

Compliance and Reporting

Azure Policy is designed to scale across large and complex Azure environments, offering centralized policy management.

Scalable and Centralized



Policy Definition Sample

Azure Key Vault should have firewall enabled

Policy definition

Assign | Edit definition | Duplicate definition | Delete definition

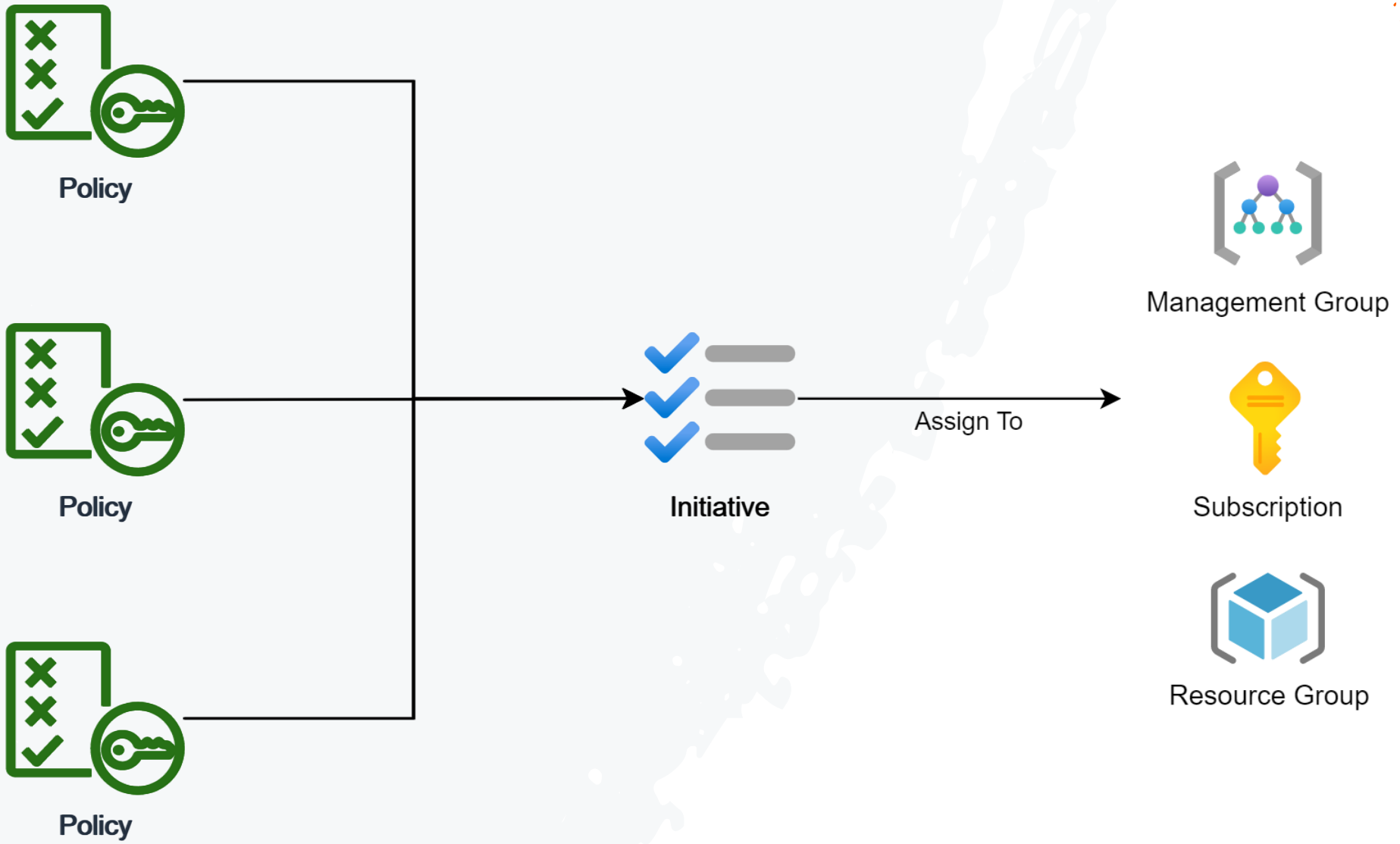
Essentials

Name	: Azure Key Vault should have firewall enabled	Definition location	: --
Description	: Enable the key vault firewall so that the key vault is not accessible by default to any ...	Definition ID	: /providers/Microsoft.Authorization/policyDefinitions/55615ac9-af46-4a59-874e-3...
Available Effects	: Audit	Type	: Built-in
Category	: Key Vault	Mode	: Indexed

Definition | Assignments (0) | Parameters

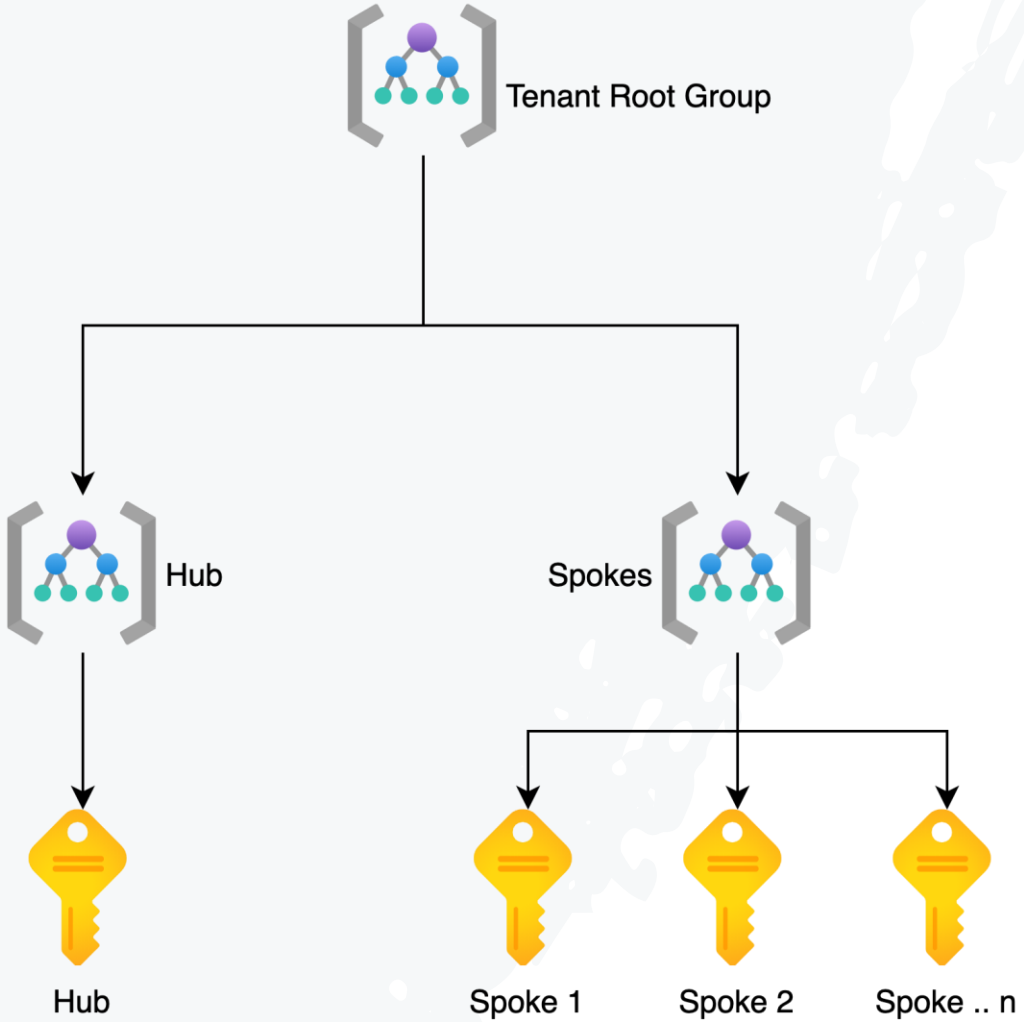
```
{
  "properties": {
    "displayName": "Azure Key Vault should have firewall enabled",
    "policyType": "BuiltIn",
    "mode": "Indexed",
    "description": "Enable the key vault firewall so that the key vault is not accessible by default to any public IPs. Optionally, you can configure specific IP ranges t
    "metadata": {
      "version": "3.2.1",
      "category": "Key Vault"
    },
    "parameters": {
      "effect": {
        "type": "String",
        "metadata": {
          "displayName": "Effect",
          "description": "Enable or disable the execution of the policy"
        },
        "allowedValues": [
          "Audit",
          "Deny",
          "Disabled"
        ],
        "defaultValue": "Audit"
      },
      "restrictIPAddresses": {
```

What are policies?

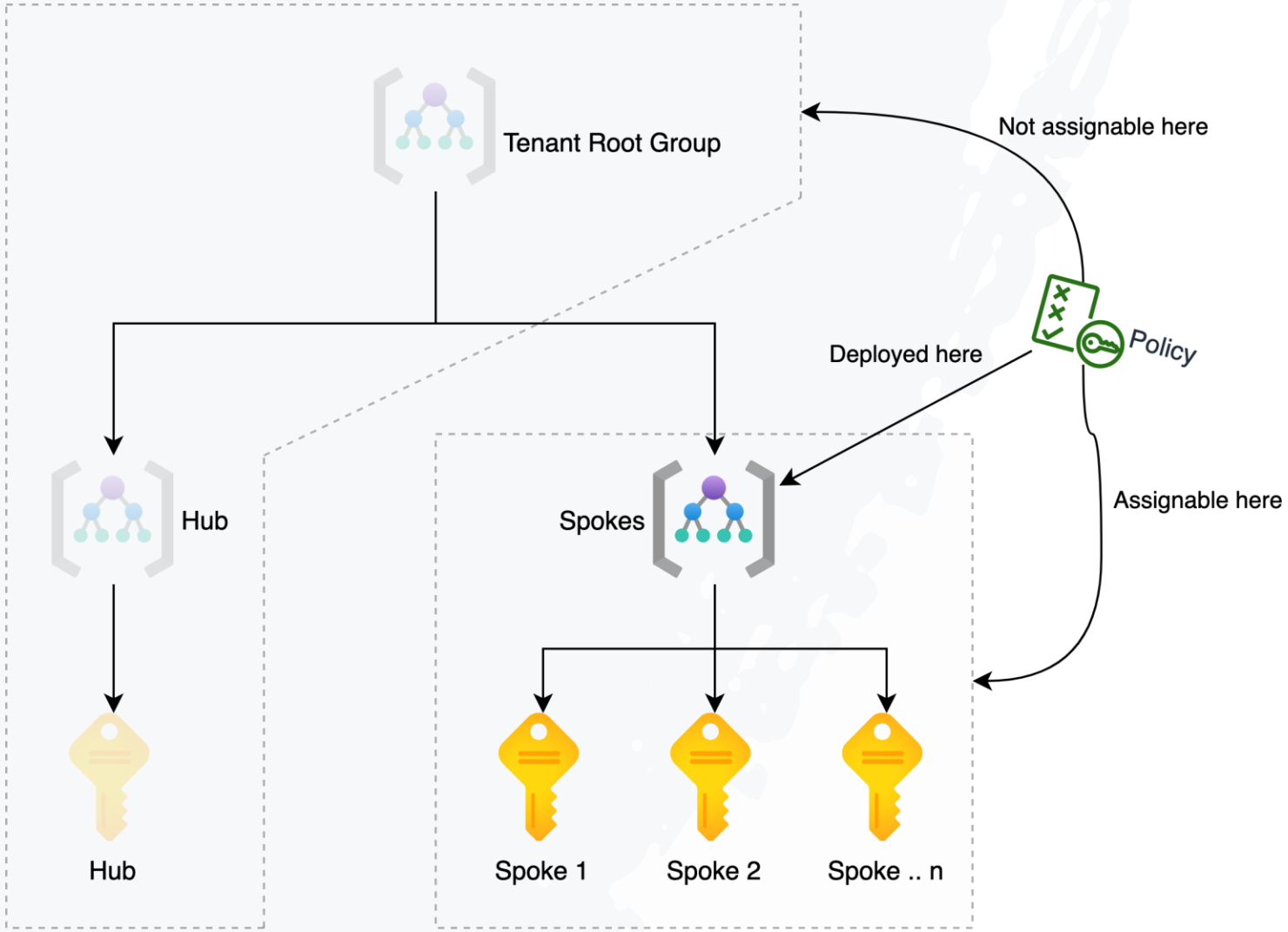


DEMO

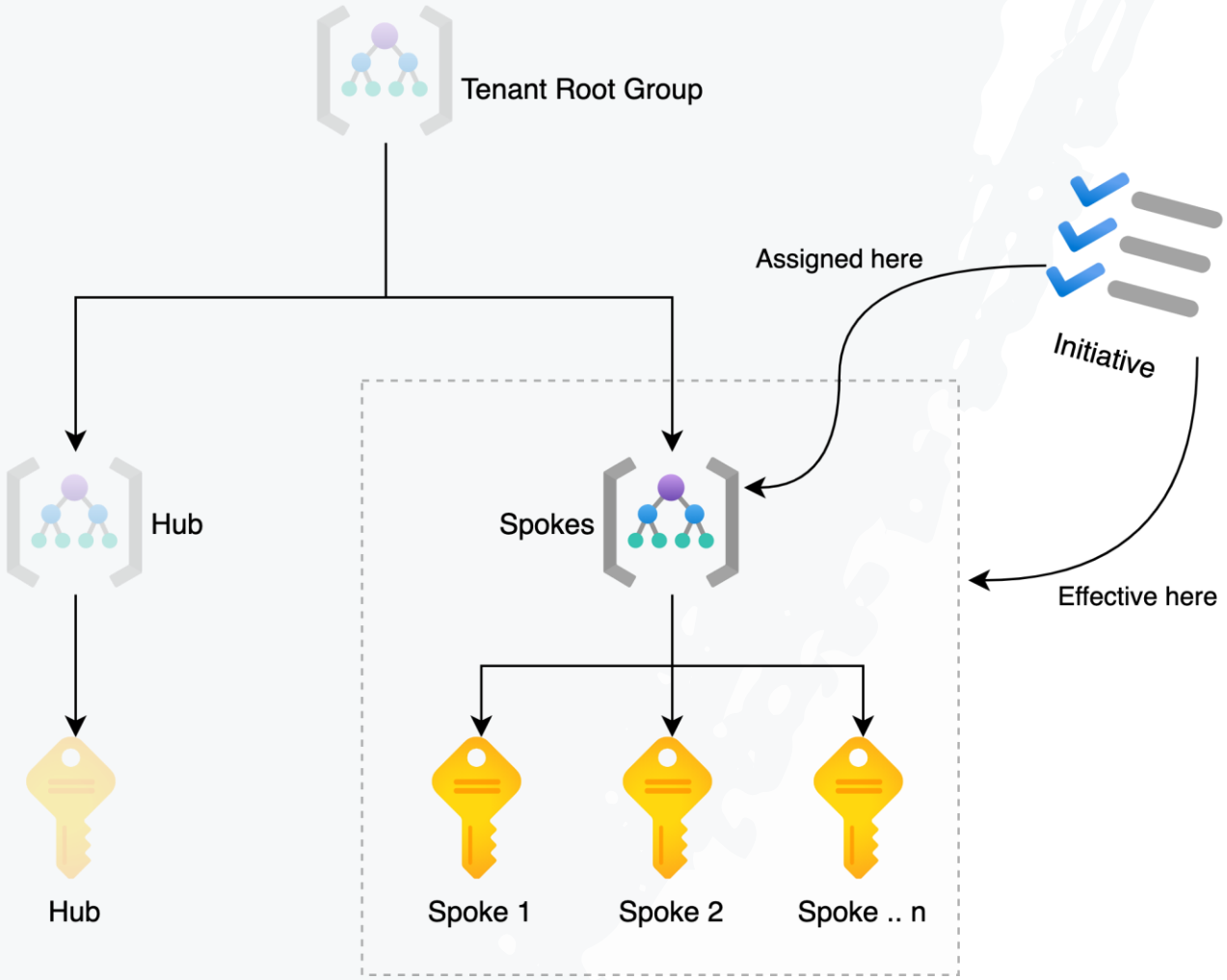
Definition location and Assignable scope



Definition location



Assignment scope



DEMO

Policy Effects

The policy rule is defined but not enforced, allowing be created or modified without compliance c

Resources that violate the policy rule are not allowed to be created or modified.

Disabled

Audit

AuditIfNotExists

Deny

DenyAction

Append

DeployIfNotExists

Modify

Used to block requests based on intended action to resources. The only supported action today is DELETE.

source violates the policy rule, the existing properties or elements are modified to bring it into compliance.

DEMO

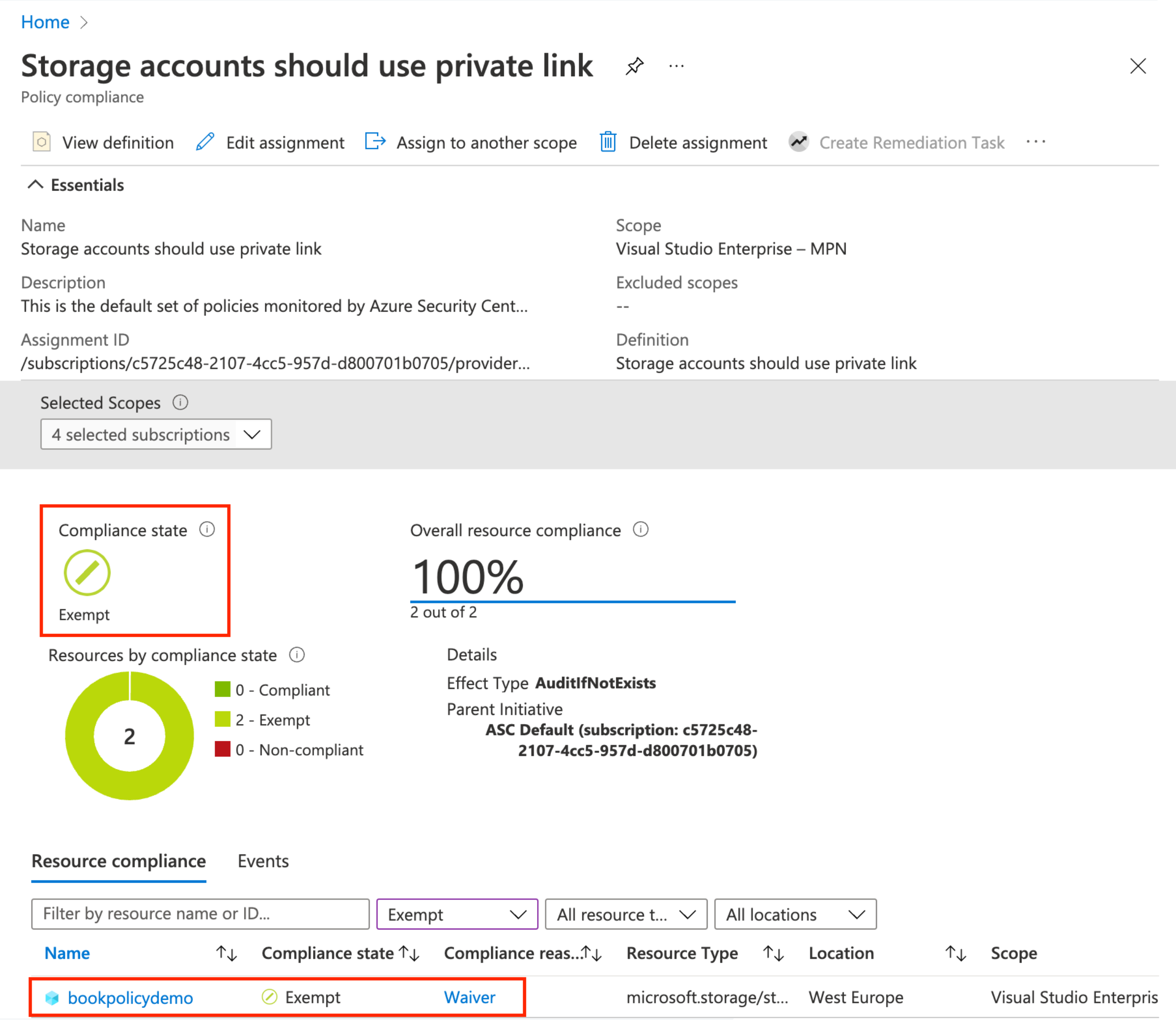
Remediation

DeployIfNotExists or **Modify**

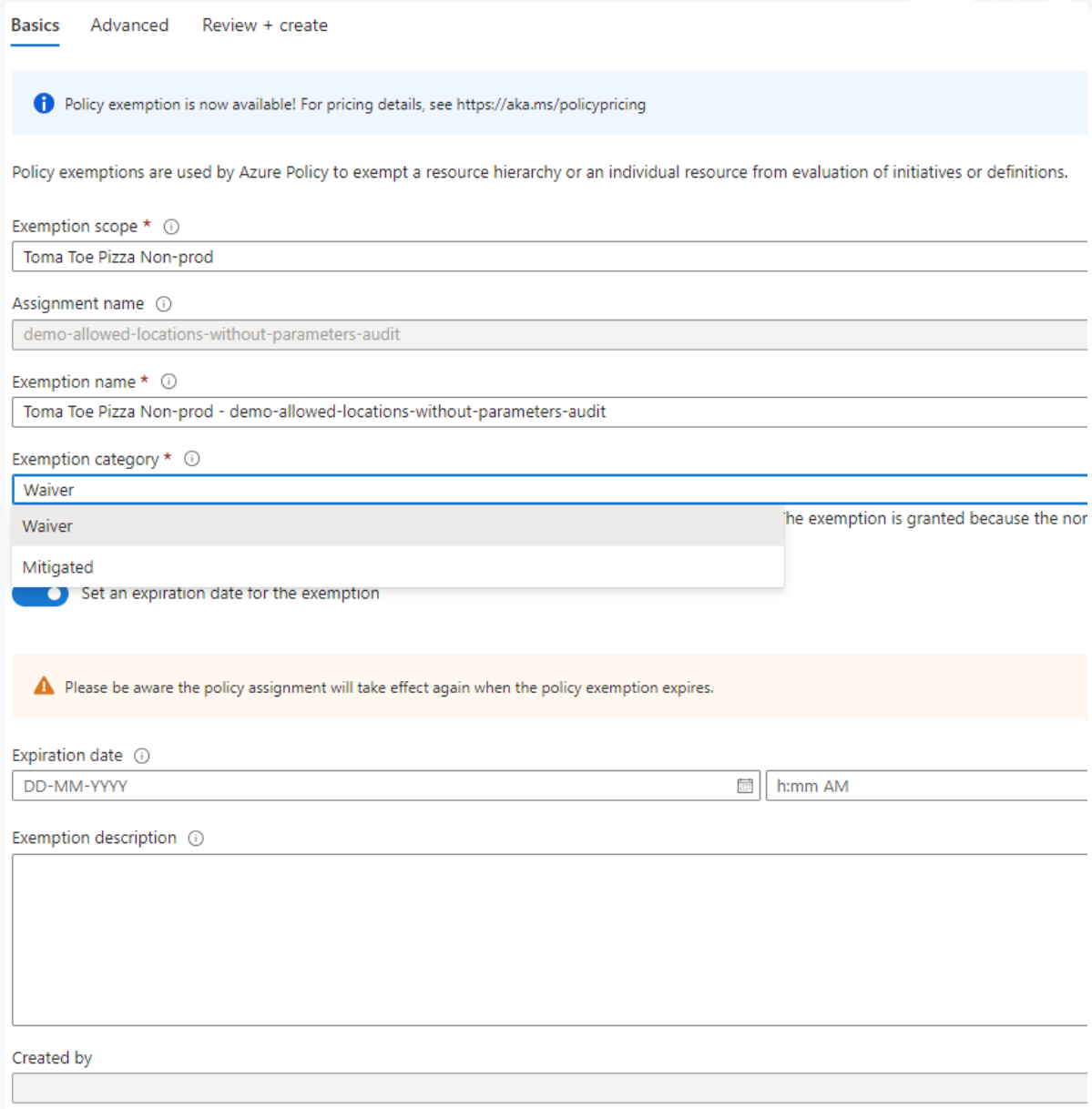
Uses a managed identity

DEMO

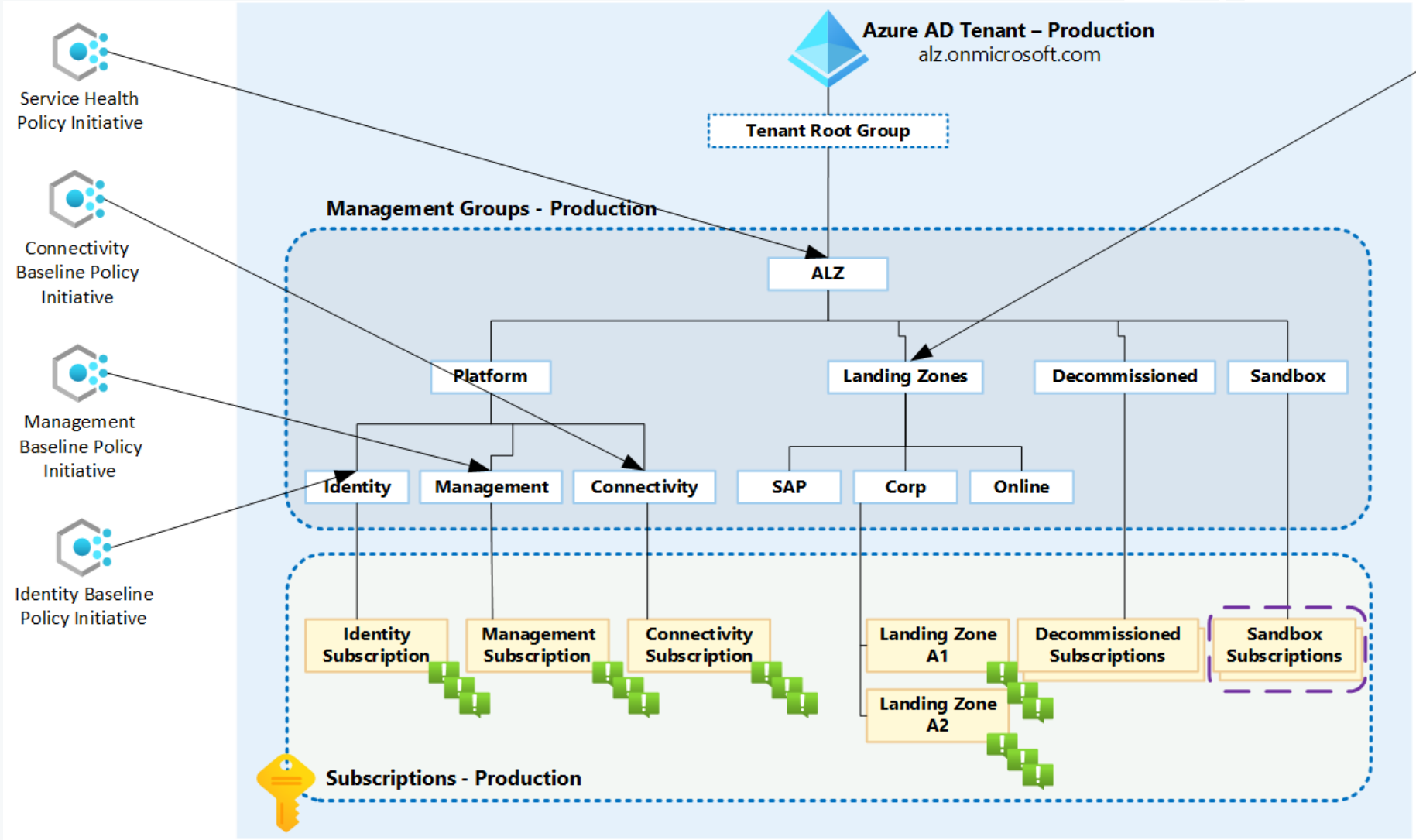
Exemptions


Home >
Storage accounts should use private link
Policy compliance
View definition
Edit assignment
Assign to another scope
Delete assignment
Create Remediation Task
Essentials
Name
Storage accounts should use private link
Description
This is the default set of policies monitored by Azure Security Cent...
Assignment ID
/subscriptions/c5725c48-2107-4cc5-957d-d800701b0705/provider...
Scope
Visual Studio Enterprise – MPN
Excluded scopes
--
Definition
Storage accounts should use private link
Selected Scopes
4 selected subscriptions
Compliance state
Exempt
Overall resource compliance
100%
2 out of 2
Resources by compliance state
2
0 - Compliant
2 - Exempt
0 - Non-compliant
Details
Effect Type AuditIfNotExists
Parent Initiative
ASC Default (subscription: c5725c48-2107-4cc5-957d-d800701b0705)
Resource compliance
Events
Filter by resource name or ID...
Exempt
All resource t...
All locations
Name
Compliance state
Compliance reas...
Resource Type
Location
Scope
bookpolicydemo
Exempt
Waiver
microsoft.storage/st...
West Europe
Visual Studio Enterpris

Exemptions


Basics
Advanced
Review + create
Policy exemption is now available! For pricing details, see https://aka.ms/policypricing
Policy exemptions are used by Azure Policy to exempt a resource hierarchy or an individual resource from evaluation of initiatives or definitions.
Exemption scope *
Toma Toe Pizza Non-prod
Assignment name
demo-allowed-locations-without-parameters-audit
Exemption name *
Toma Toe Pizza Non-prod - demo-allowed-locations-without-parameters-audit
Exemption category *
Waiver
Waiver
Mitigated
he exemption is granted because the nor
Set an expiration date for the exemption
Please be aware the policy assignment will take effect again when the policy exemption expires.
Expiration date
DD-MM-YYYY
h:mm AM
Exemption description
Created by

Real-life examples



References

- https://github.com/XpiritBV/azure-policy-session
- https://xpirit.com/azure-policy-unveiled-ignite-your-cloud-management-passion/
- https://www.manning.com/books/azure-infrastructure-as-code
- https://www.azadvertizer.net/azpolicyadvertizer_all.html

Thanks!

Patrick de Kruijf - Azure Architect

https://www.linkedin.com/in/patrickdk
https://www.azurefreakconfessions.com

Erwin Staal - Azure Architect

@erwin_staal
https://www.linkedin.com/in/erwinstaal
https://www.erwinstaal.nl

Xebia | Xpirit