NIC

EMPOWER

November 13-15, Oslo Spektrum

Patrick de Kruijf – Erwin Staal

Azure Architect

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

Azure Architect

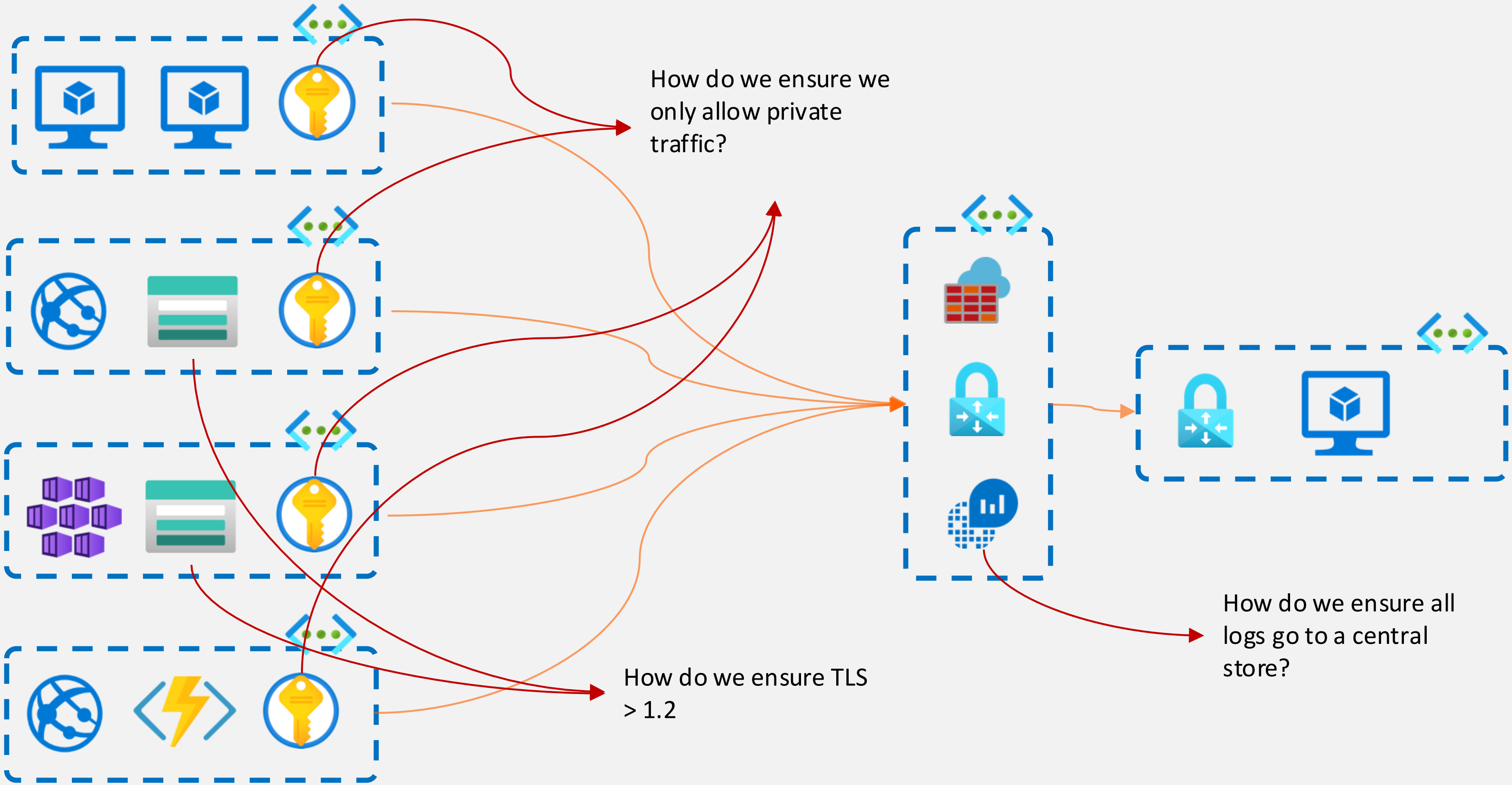
@erwin_staal
https://www.linkedin.com/in/erwinstaal
https://www.erwinstaal.nl

Govern your Azure environment through Azure Policy

Xebia

NIC
EMPOWER

Why use Azure Policy?



How do we ensure we only allow private traffic?

How do we ensure TLS > 1.2

How do we ensure all logs go to a central store?

What is 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

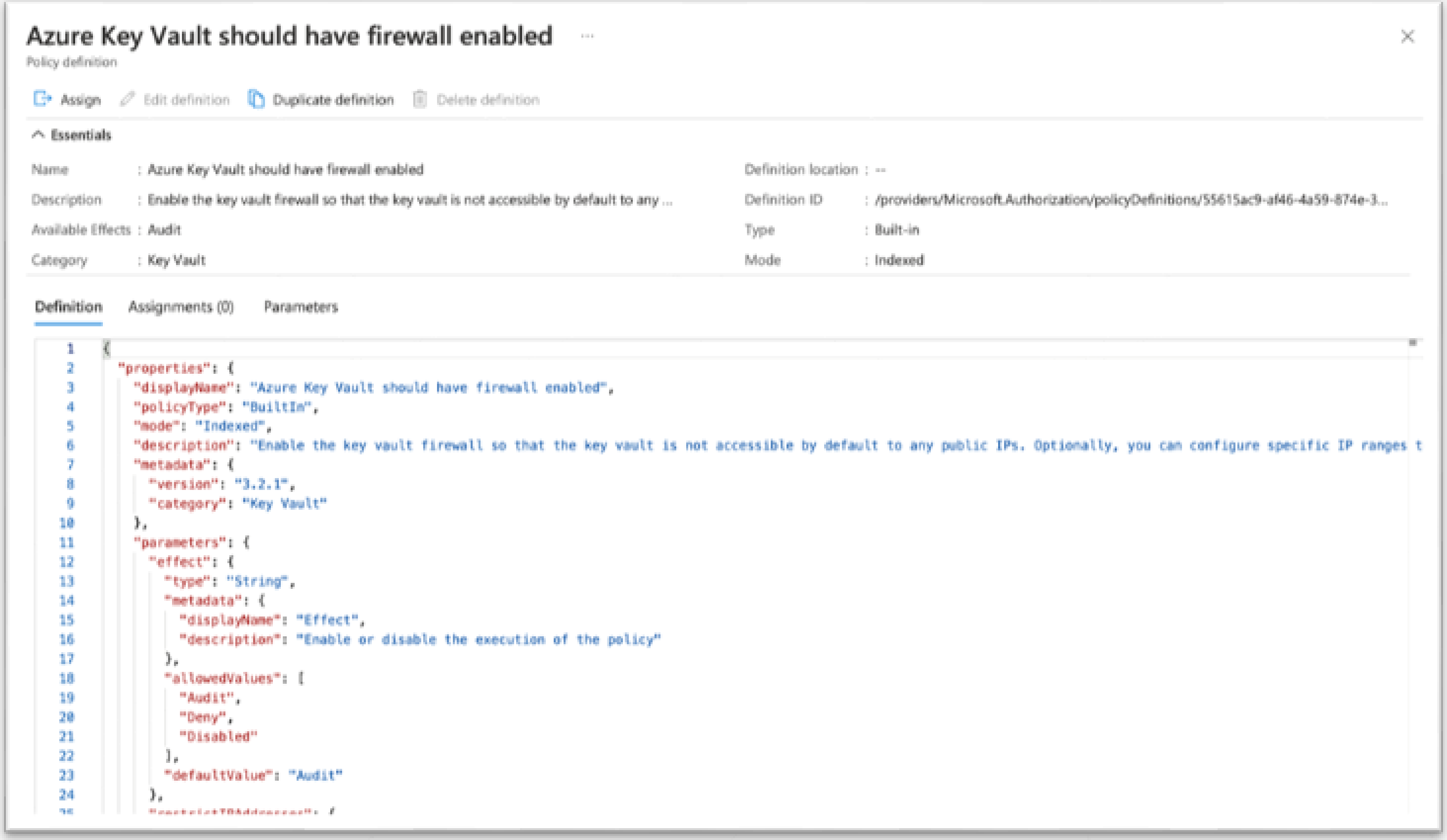
Azure Policy provides monitoring and reporting capabilities to track compliance status across the Azure resources.

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

Name : Azure Key Vault should have firewall enabled

Description : Enable the key vault firewall so that the key vault is not accessible by default to any ...

Available Effects : Audit

Category : Key Vault

Definition location : --

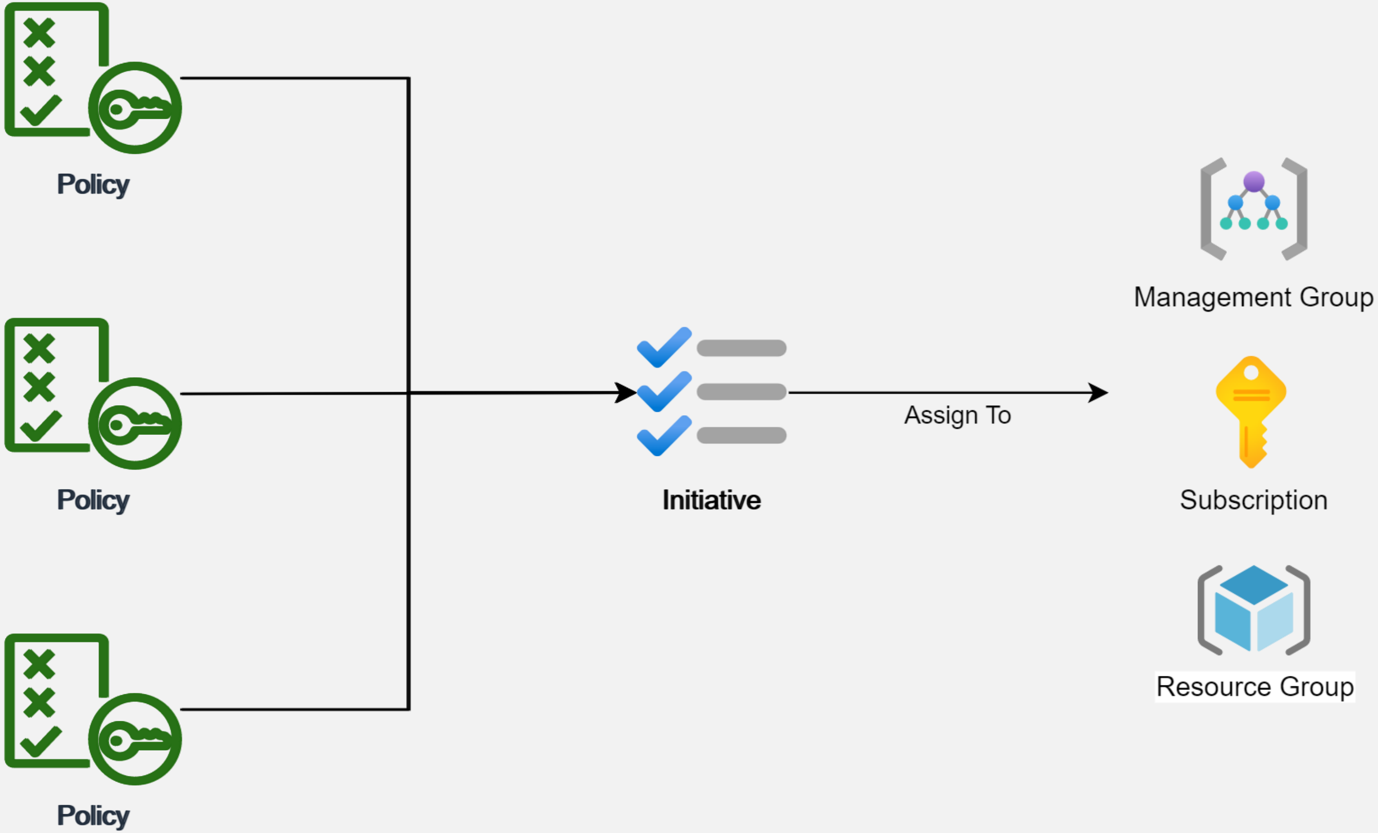
Definition ID : /providers/Microsoft.Authorization/policyDefinitions/55615ac9-af46-4a59-874e-3...

Type : Built-in

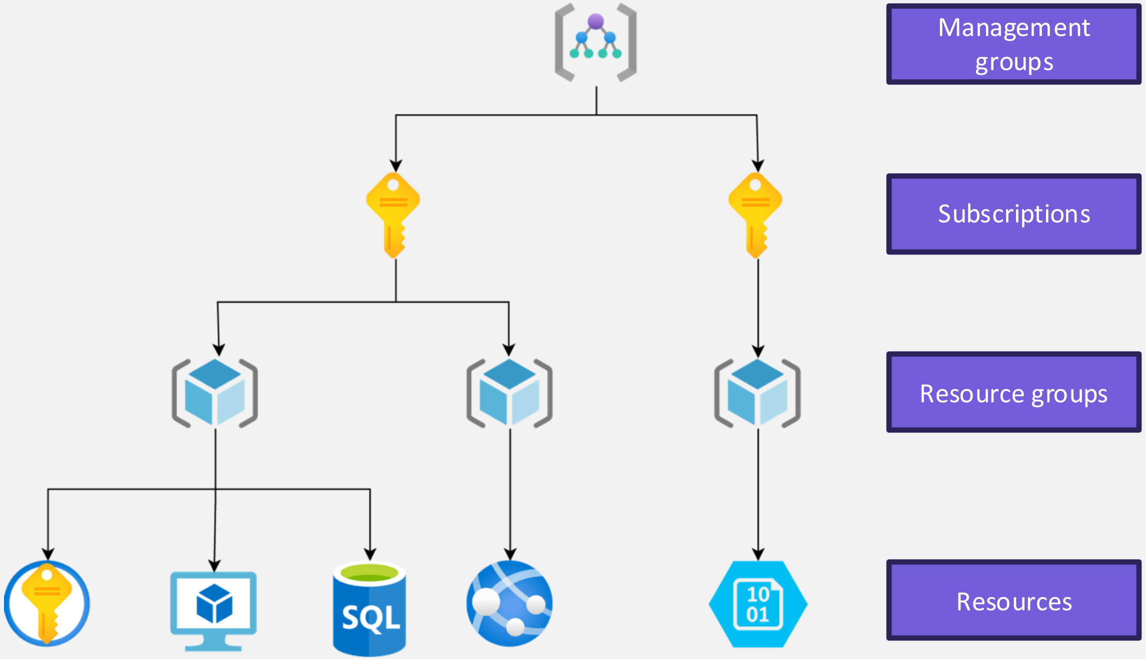
Mode : Indexed

```
{
  "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": {
```

Policy Assignment



Azure Deployment Scope



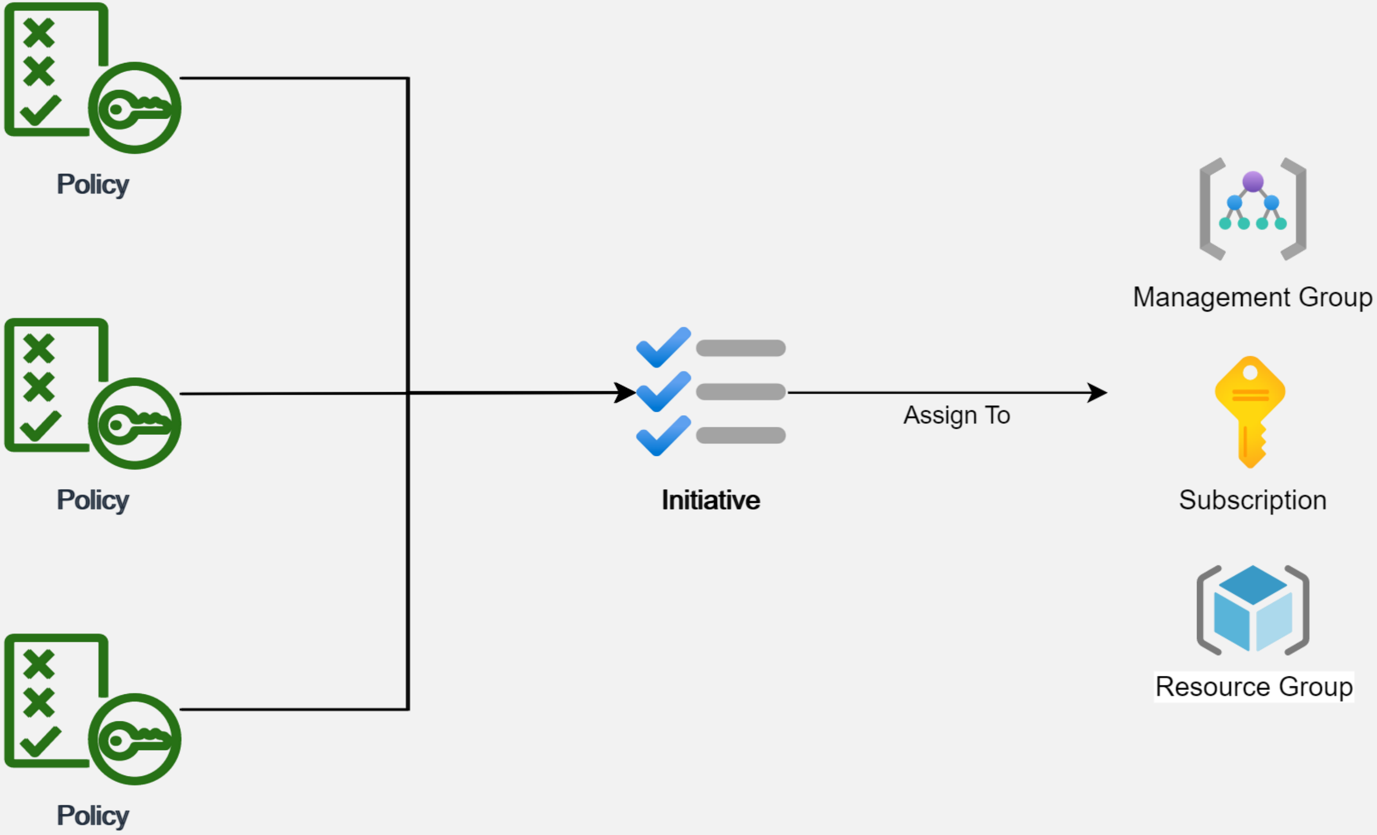
Management groups

Subscriptions

Resource groups

Resources

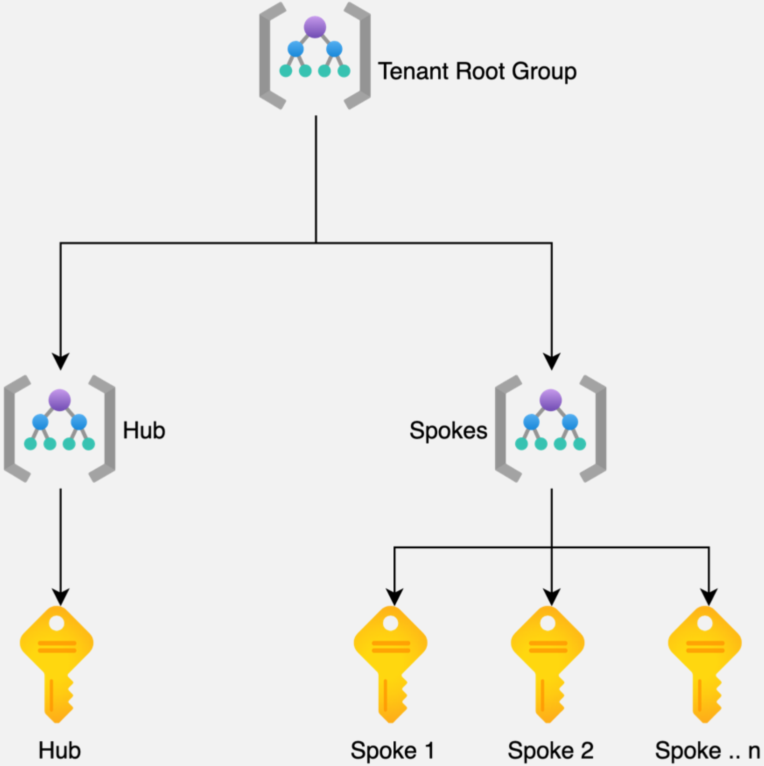
Policy Assignment



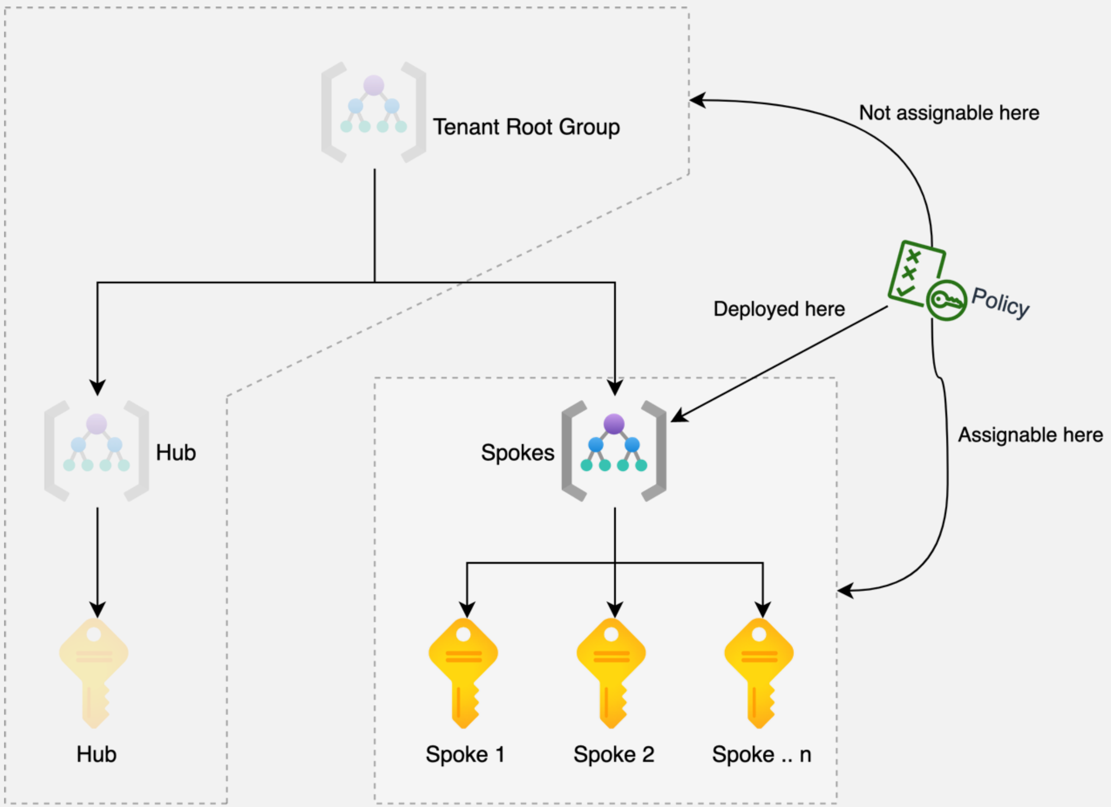
DEMO

NIC
EMPOWER

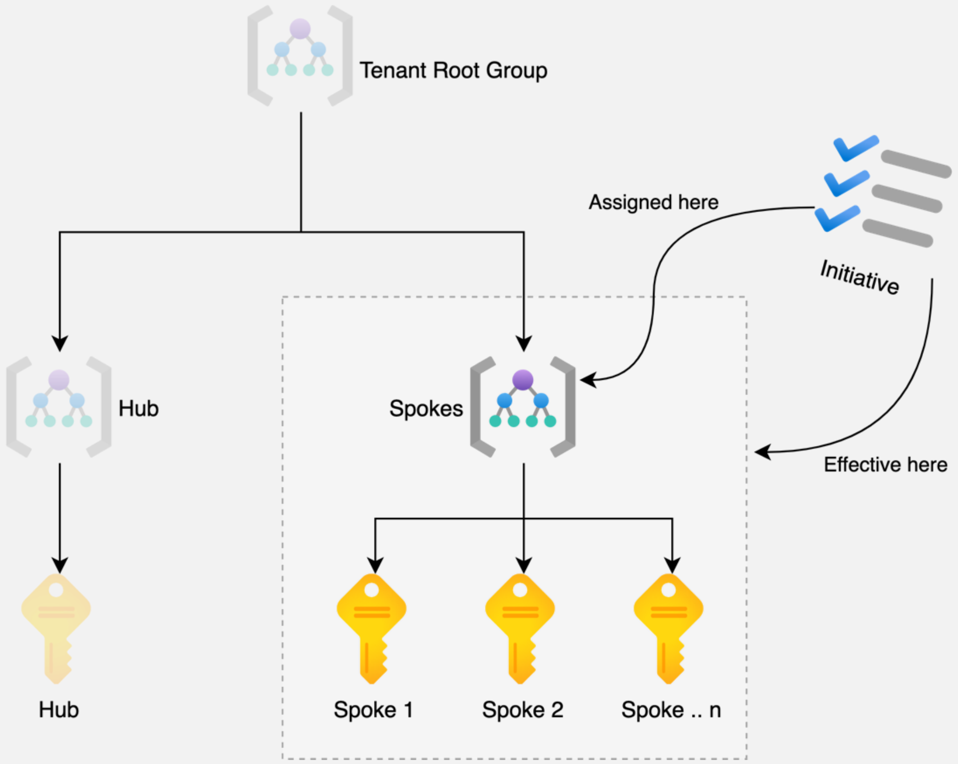
Definition location and Assignable scope



Definition location



Assignment scope



NIC
EMPOWER

DEMO

Policy Effects

The policy rule is defined but not enforced, allowing resources t
modified without compliance checks.

The auditIfNotExists effect enables auditing of resources related to the resource.

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.

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

DEMO

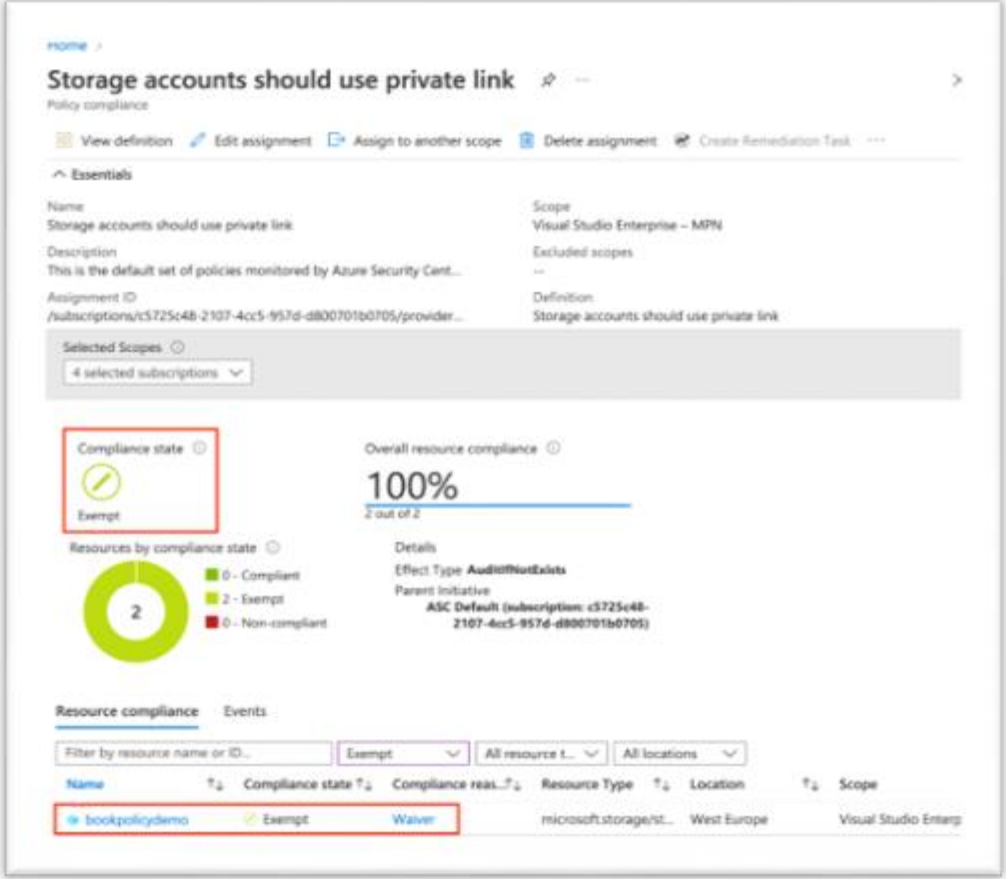
Remediation

DeployIfNotExists or **Modify**

Uses a managed identity

DEMO

Exemptions



Storage accounts should use private link

Policy compliance

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

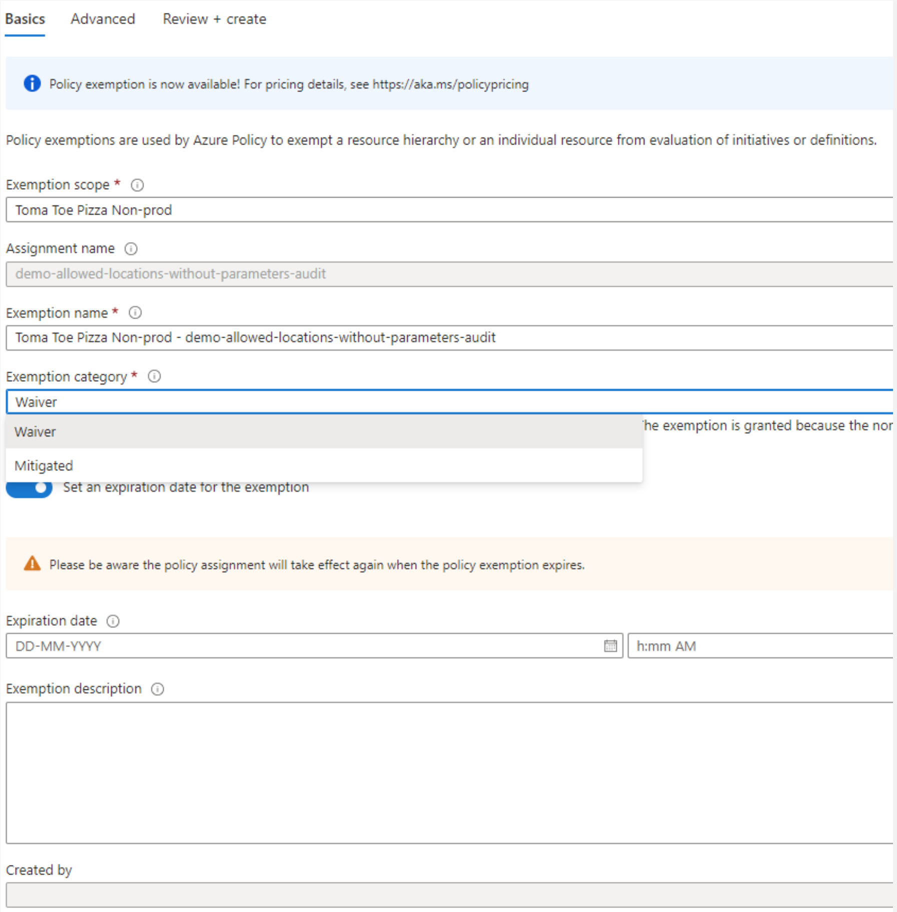
Details
Effect Type **AuditIfNotExists**
Parent Initiative
ASC Default (subscription: c5725c48-2107-4cc5-957d-d800701b0705)

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 Enterp

NIC
EMPOWER

Exemptions



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

he exemption is granted because the nor

Set an expiration date for the exemption

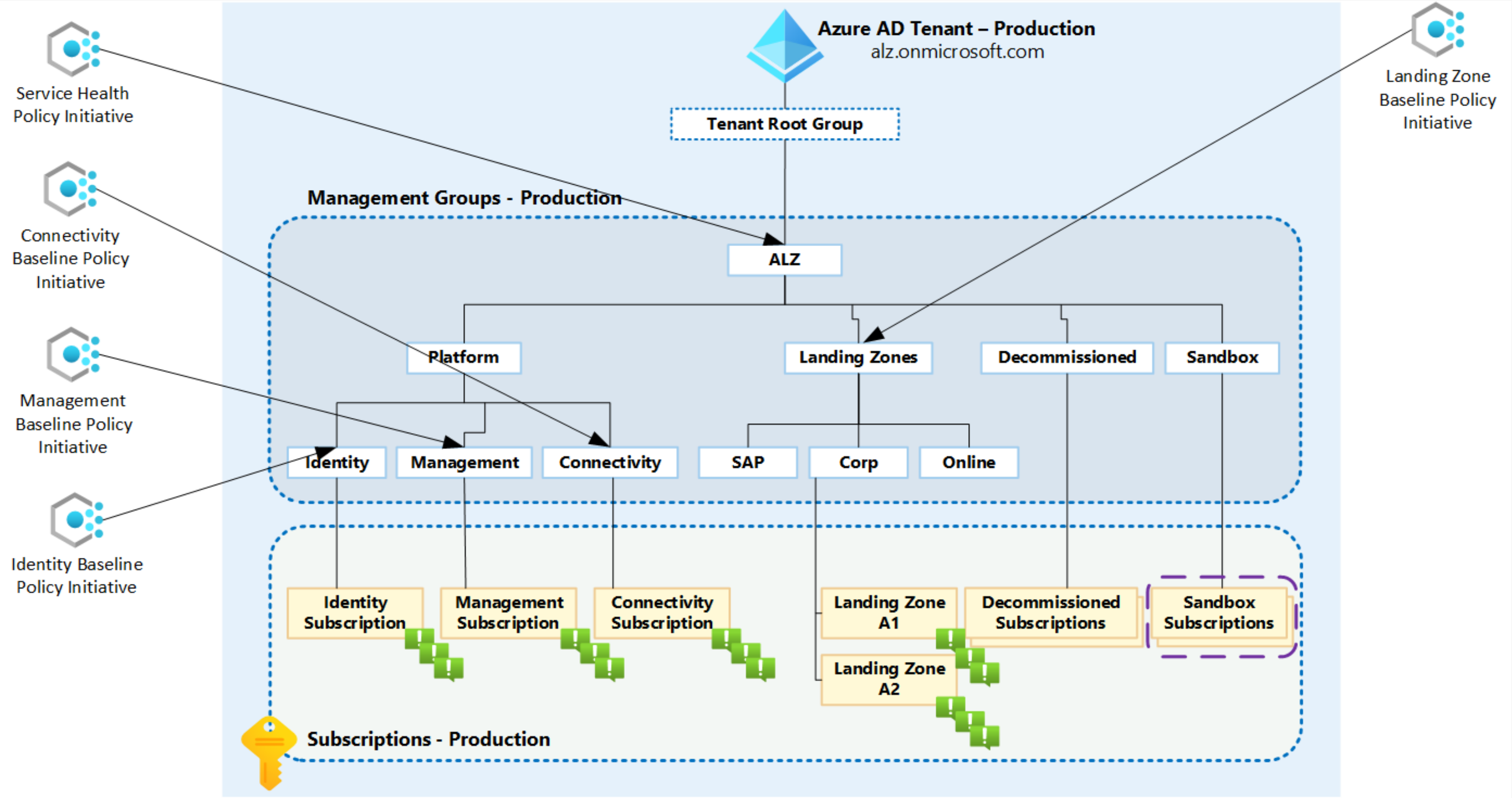
Please be aware the policy assignment will take effect again when the policy exemption expires.

Expiration date: DD-MM-YYYY h:mm AM

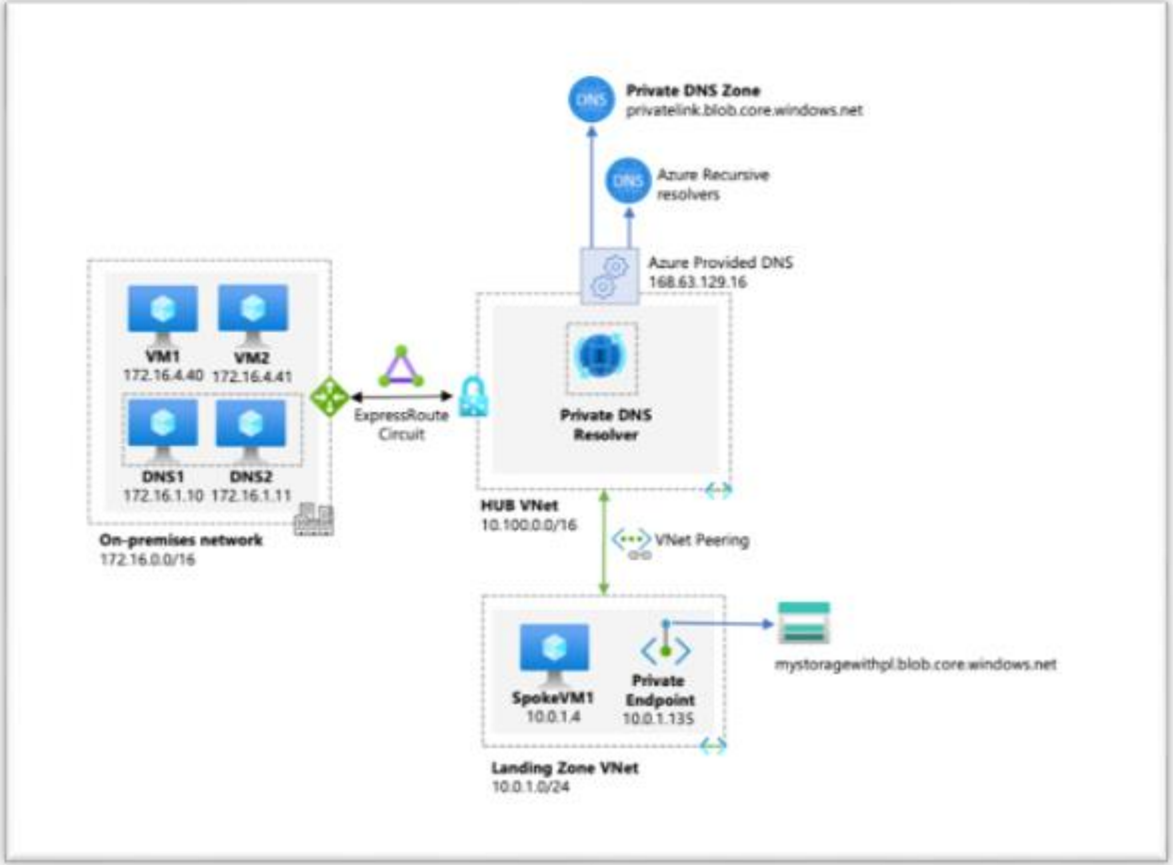
Exemption description

Created by

Real-life examples


Azure AD Tenant – Production
alz.onmicrosoft.com
Tenant Root Group
Management Groups - Production
ALZ
Platform
Landing Zones
Decommissioned
Sandbox
Identity
Management
Connectivity
SAP
Corp
Online
Identity Subscription
Management Subscription
Connectivity Subscription
Landing Zone A1
Landing Zone A2
Decommissioned Subscriptions
Sandbox Subscriptions
Subscriptions - Production
Service Health Policy Initiative
Connectivity Baseline Policy Initiative
Management Baseline Policy Initiative
Identity Baseline Policy Initiative
Landing Zone Baseline Policy Initiative

Real-life examples



References

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

Shameless plugs

Understanding Azure Virtual WAN and lessons learned

8.30 | Room 5

Smooth Sailing to Azure: Streamlining Datacenter Workload Migration

11.10 | Room 5

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