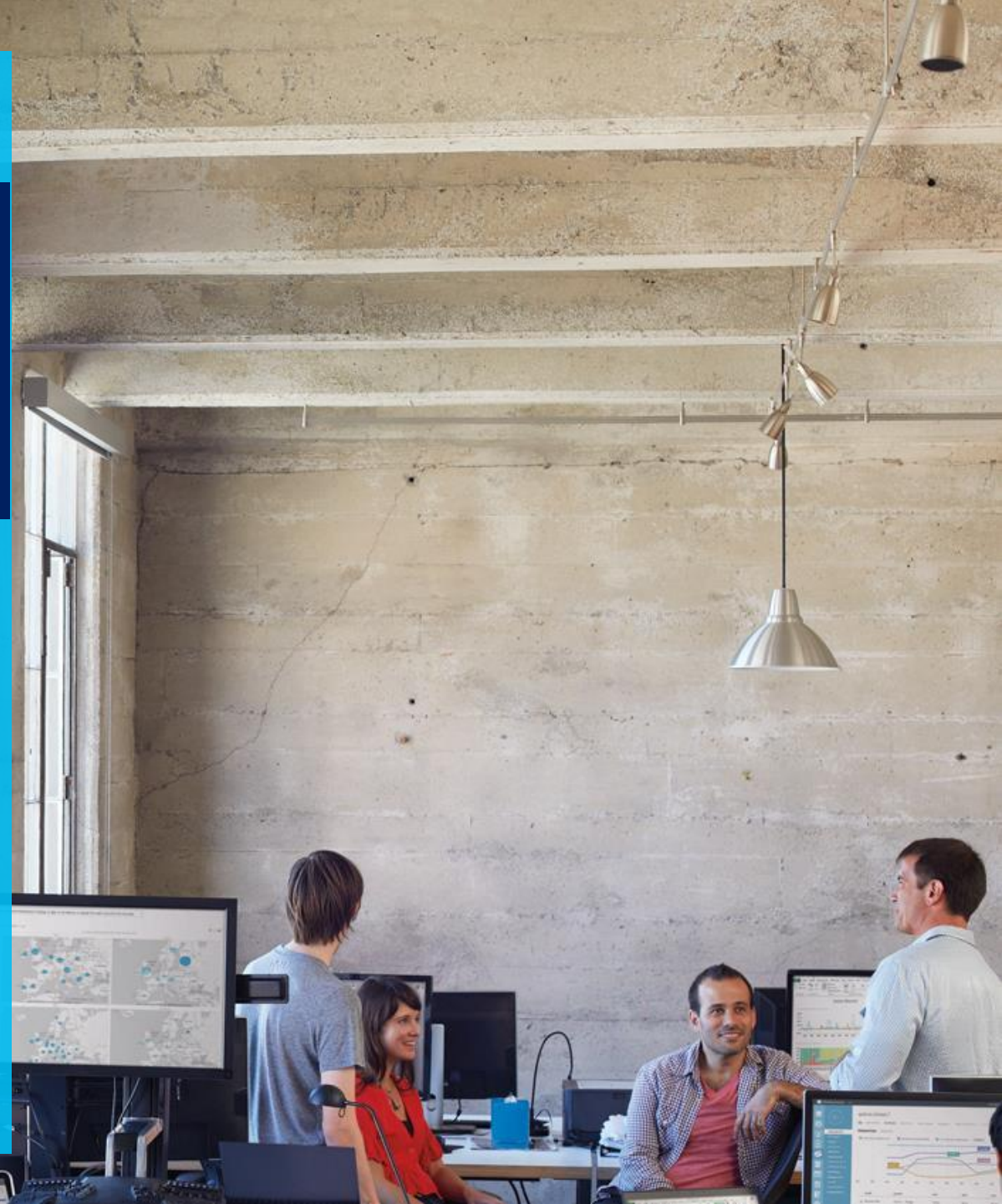




Microsoft Azure Power Lunch

Today's Topic:
AzGovViz
Azure Governance Visualizer

Date: 14-AUG-2020



Julian Hayward – Customer Engineer



- Germany based
- Been with Microsoft for 2,5 years
- Technical focus on Azure Infrastructure, Automation and Governance

Problem statement

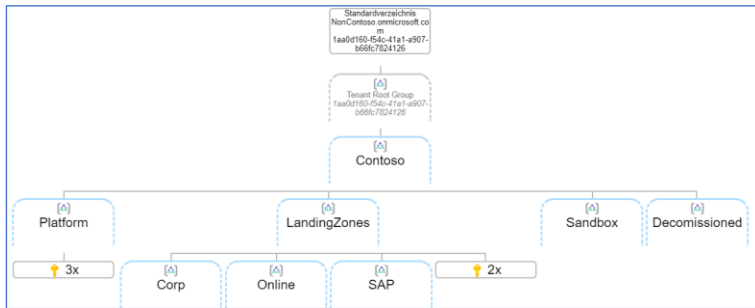
- Governance can be a complex topic
- Holistic overview on governance implementation
- Connecting the dots

What is it?

AzGovViz is a PowerShell based script that iterates your Azure Tenants Management Group hierarchy down to Subscription level. It captures most relevant Azure governance capabilities such as Azure Policy, RBAC and Blueprints and more. From the collected data AzGovViz provides visibility on your **Hierarchy Map**, creates a **Tenant Summary** and builds granular **Scope Insights** on Management Groups and Subscriptions.

Scope Insights

Hierarchy Map



Tenant Summary

- ✓ 24 Custom Policies (8 from superior Management Groups) (MG 'Contoso' and descendants wide)
- ✓ 5 Custom PolicySets (2 from superior Management Groups) (MG 'Contoso' and descendants wide) (Limit: 5/2500)
- ✓ 6 Custom Roles (MG 'Contoso' and descendants wide) (Limit: 6/5000)
- ✓ 13 Orphaned Custom Policies (MG 'Contoso' and descendants wide)
- ✓ 1 Orphaned Custom PolicySets (MG 'Contoso' and descendants wide)
- ✓ 2 Orphaned Custom Roles (MG 'Contoso' and descendants wide)
- ✓ 1 Orphaned Role Assignments (MG 'Contoso' and descendants wide)
- ✓ 1 Custom Roles Owner permissions (MG 'Contoso' and descendants wide)
- ✓ 1 Owner permission assignments to ServicePrincipal (MG 'Contoso' and descendants wide)
- ✓ 9 ResourceTypes (29 Resources) in 2 Locations (MG 'Contoso' and descendants wide)
- ✓ 9 Management Groups (3 levels of depth)
- ✓ 0 Management Groups approaching Limit for PolicyAssignment
- ✓ 0 Management Groups approaching Limit for Policy Scope
- ✓ 0 Management Groups approaching Limit for PolicySets Scope
- ✓ 5 Subscriptions
- ✓ 0 Subscriptions approaching Limit for ResourceGroups
- ✓ 0 Subscriptions approaching Limit for Tags
- ✓ 1 Subscriptions approaching Limit for PolicyAssignment
- ✓ 0 Subscriptions approaching Limit for Policy Scope
- ✓ 0 Subscriptions approaching Limit for PolicySet Scope

Contoso

Decommissioned

LandingZones

Highlight Management Group in hierarchy tree

Management Group Name: **LandingZones**

Management Group Id: **LandingZones**

Management Group Path: '1aa0d160-f54c-41a1-a907-b66fc7824126'/Contoso/LandingZones'

3 Policy Assignments (1 at scope, 2 inherited) (BuiltIn: 3 | Custom: 0)

0 PolicySet Assignments (0 at scope, 0 inherited) (BuiltIn: 0 | Custom: 0)

Policy Assignment Limit: 1/100

0 Custom Policies scoped

0 Custom PolicySets scoped

0 Blueprints scoped

17 Role Assignments (16 inherited) (User: 8 | Group: 0 | ServicePrincipal: 9 | Orphaned: 0) (CustomRoleOwner: 0, OwnerAssignmentSP: 0) (Policy related: 2) | Limit: (1/500)

2 Subscriptions linked

LandingZoneA1 (214003f-a60d-4bcd-be9a-204937acb1d4)

Highlight Subscription in hierarchy tree

Subscription Name: **LandingZoneA1**

Subscription Id: **214003f-a60d-4bcd-be9a-204937acb1d4**

Subscription Path: '1aa0d160-f54c-41a1-a907-b66fc7824126'/Contoso/LandingZones/'214003f-a60d-4bcd-be9a-204937acb1d4'

State: Enabled

QuotaId: PayAsYouGo_2014-09-01

ASC Secure Score: n/a

3 Resource Groups | Limit: (3/980)

2 Subscription Tags | Limit: (2/50)

2 ResourceTypes (2 Resources) in 1 Locations

4 Policy Assignments (1 at scope, 3 inherited) (BuiltIn: 3 | Custom: 1)

0 PolicySet Assignments (0 at scope, 0 inherited) (BuiltIn: 0 | Custom: 0)

Policy Assignment Limit: 1/100

1 Custom Policies scoped | Limit: (1/500)

0 Custom PolicySets scoped

0 Blueprints assigned

0 Blueprints scoped

17 Role Assignments (17 inherited) (User: 8 | Group: 0 | ServicePrincipal: 9 | Orphaned: 0) (CustomRoleOwner: 0, OwnerAssignmentSP: 0) (Policy related: 2) | Limit: (0/2000)

- Management Groups
- Subscriptions
- Policy Definitions, Assignments, Compliance
- RBAC Definitions, Assignments
- Blueprints Definitions, Assignments
- Limits
- Resource Groups
- Resource Types
- Resource Providers
- Diagnostics capable
- Security

CSV file

- All collected data available in CSV file

HTML file

- Connects the dots by providing insights on hierarchy tree, tenant summary and granular reporting on Management Groups and Subscriptions

Azure DevOps Wiki 'Mermaid plugin' ready markdown file

- Limited to hierarchy and list of Management Groups / Subscriptions

Scenarios / Prerequisites

Requirements for all scenarios

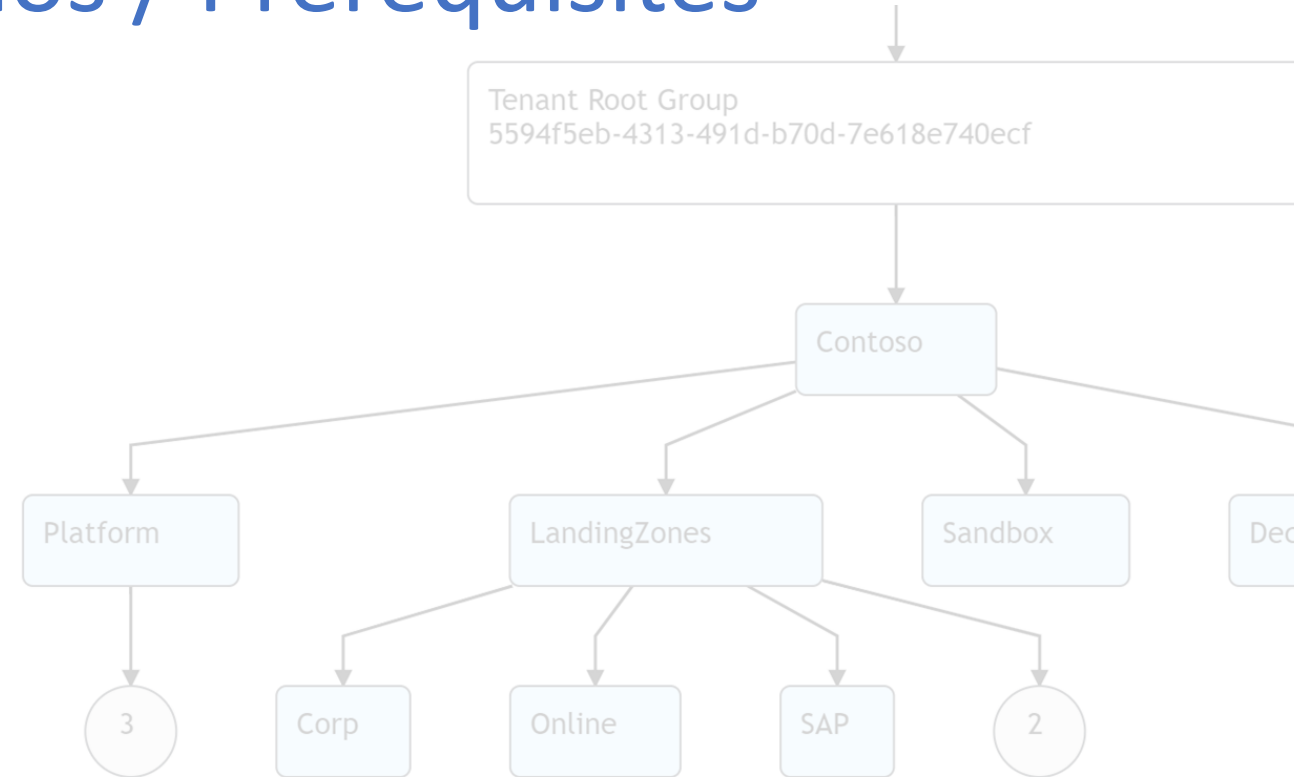
- PowerShell Az Modules
 - Az.Accounts
 - Az.Resources
 - Az.ResourceGraph
- RBAC Role 'Reader' on Management Group

Scenario: Local (any PS console)

Scenario: Azure DevOps Pipeline

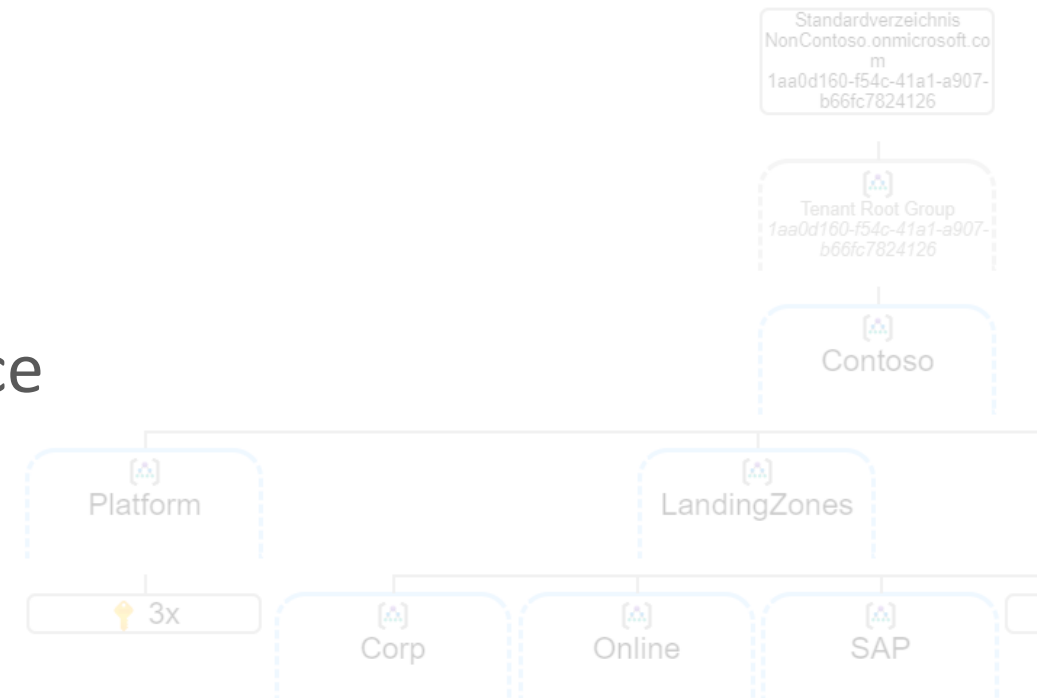
Requirements: Service Connection (Service Principal) requires API permissions (Azure Active Directory API | Application | Directory | Read.All)

Environments: AzGovViz is designed to support all Azure Clouds (AzureCloud, AzureUSGovernment, AzureChinaCloud, AzureGermanCloud), however it is only verified working on AzureCloud by today



Features

- User friendly visualization of entire governance implementation [DEMO](#)
- Create Hierarchy map ONLY - parameter
- Define limit warning percentage - parameter
- Data protection / scrub user information - parameter
- Whitelist Subscriptions by QuotaId - parameter
- Target Management Group - parameter
- HTML file embedded version check
- HTML filterable tables
- Azure Pipeline YAML example provided / Azure DevOps Wiki As Code



- Orphaned Roles/Policies Definitions & Assignment
- Indicate use of deprecated policies
- Filter Policy Assignments Excludes Scopes
- Filter Policy Assignments Inheritance
- Relation of Role Assignments and Policy Assignments
- Approaching Limits information – e.g. Scope limits, ARM limits
- Resource Types count per region
- Resource Types Diagnostics capable
- Resource Provider states
- Security recommendations (custom owner roles, owner assignment on SP, owner/UserAccessAdmin assignment on identity rather than group)



AzGovViz creates very detailed information about your Azure Governance setup. In your organizations best interest the **Outputs** should be protected from not authorized access!

Your contribution welcome!

AzGovViz GitHub Repositories

- <https://github.com/JulianHayward/Azure-MG-Sub-Governance-Reporting>
(latest version in 'dev' branch)
- <https://github.com/microsoft/CloudAdoptionFramework/tree/master/govern/AzureGovernanceVisualizer>

Also checkout AzAdvertizer <https://www.azadvertizer.net/>

..to keep up with the pace on Azure Governance capabilities such as Azure Policies, Policy Initiatives, Policy Aliases, RBAC Roles and Resource Provider Operations