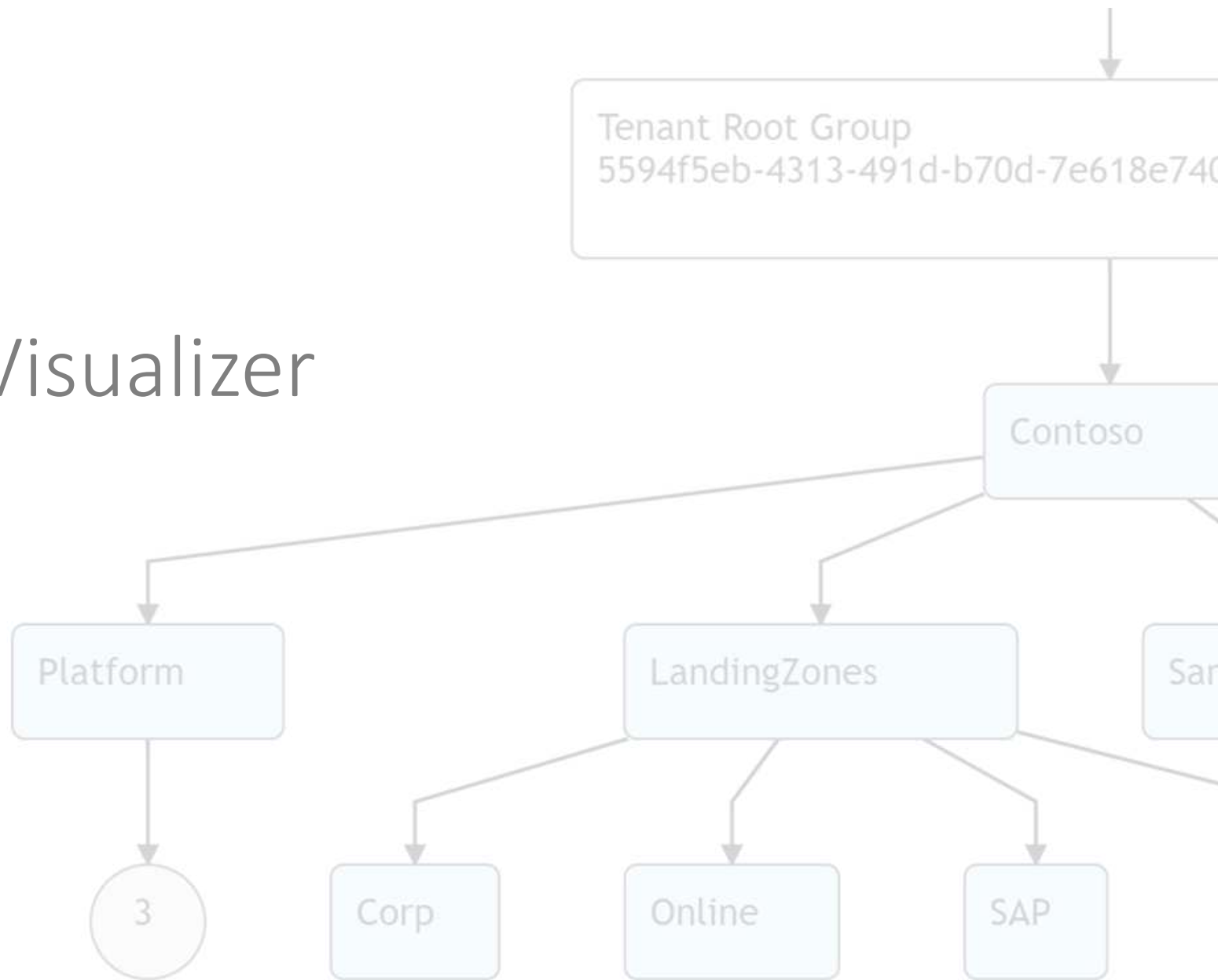


# AzGovViz

## Azure Governance Visualizer



[aka.ms/AzGovViz](https://aka.ms/AzGovViz)

# AzGovViz

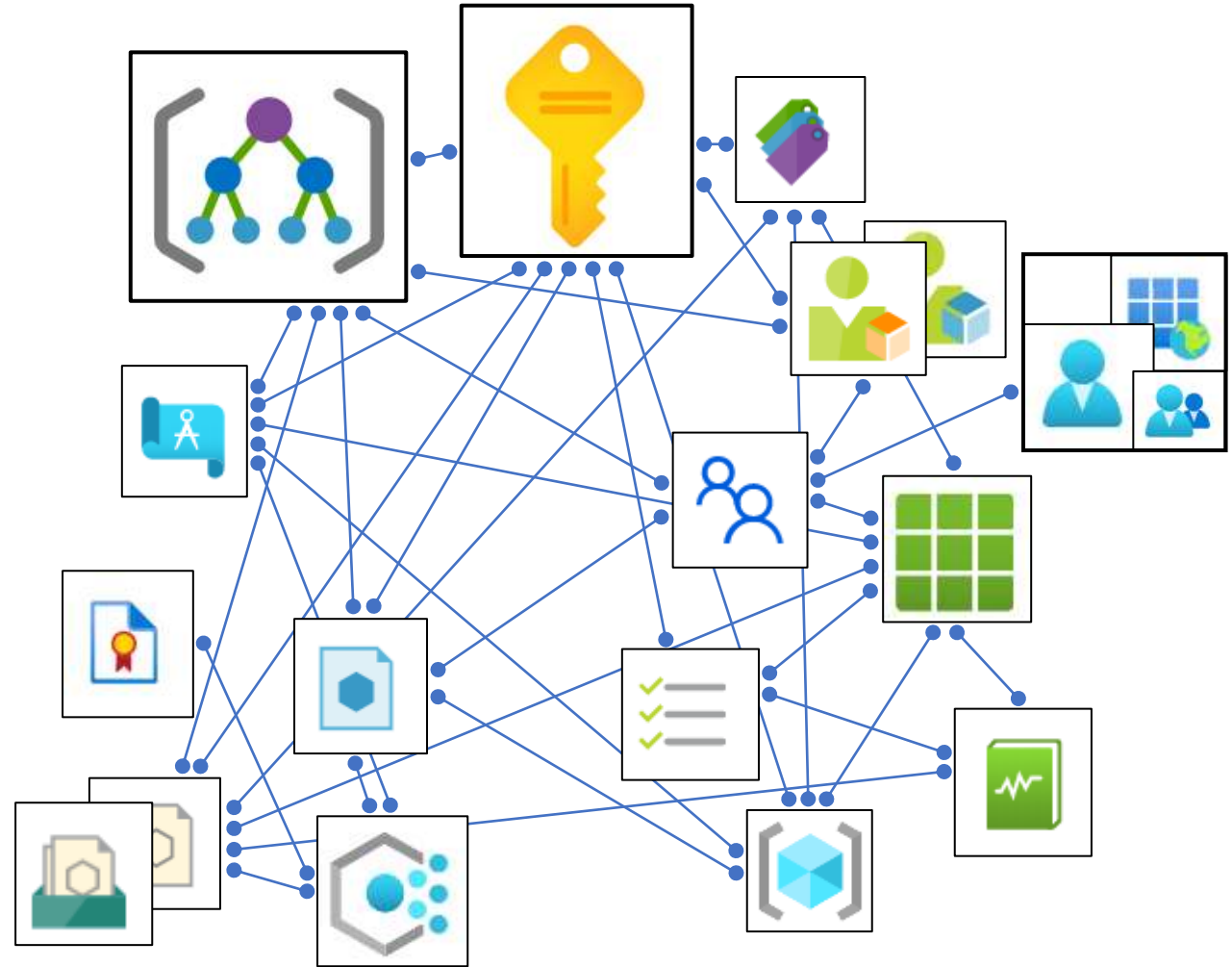
## Azure Governance Visualizer

*'Azure Governance can be a complex thing.'*

### Challenging

- Holistic overview on technical Azure Governance implementation
- Connecting the dots

AzGovViz is intended to help you to get a holistic overview on your technical Azure Governance implementation by connecting the dots.



# AzGovViz

## Azure Governance Visualizer

AzGovViz is a PowerShell script that captures Azure Governance related information such as Azure Policy, RBAC (a lot more) by polling Azure ARM and Microsoft Graph APIs.

AzGovViz leverages from the PowerShell Core parallelization feature.

The technical requirements as well as the required permissions are minimal.

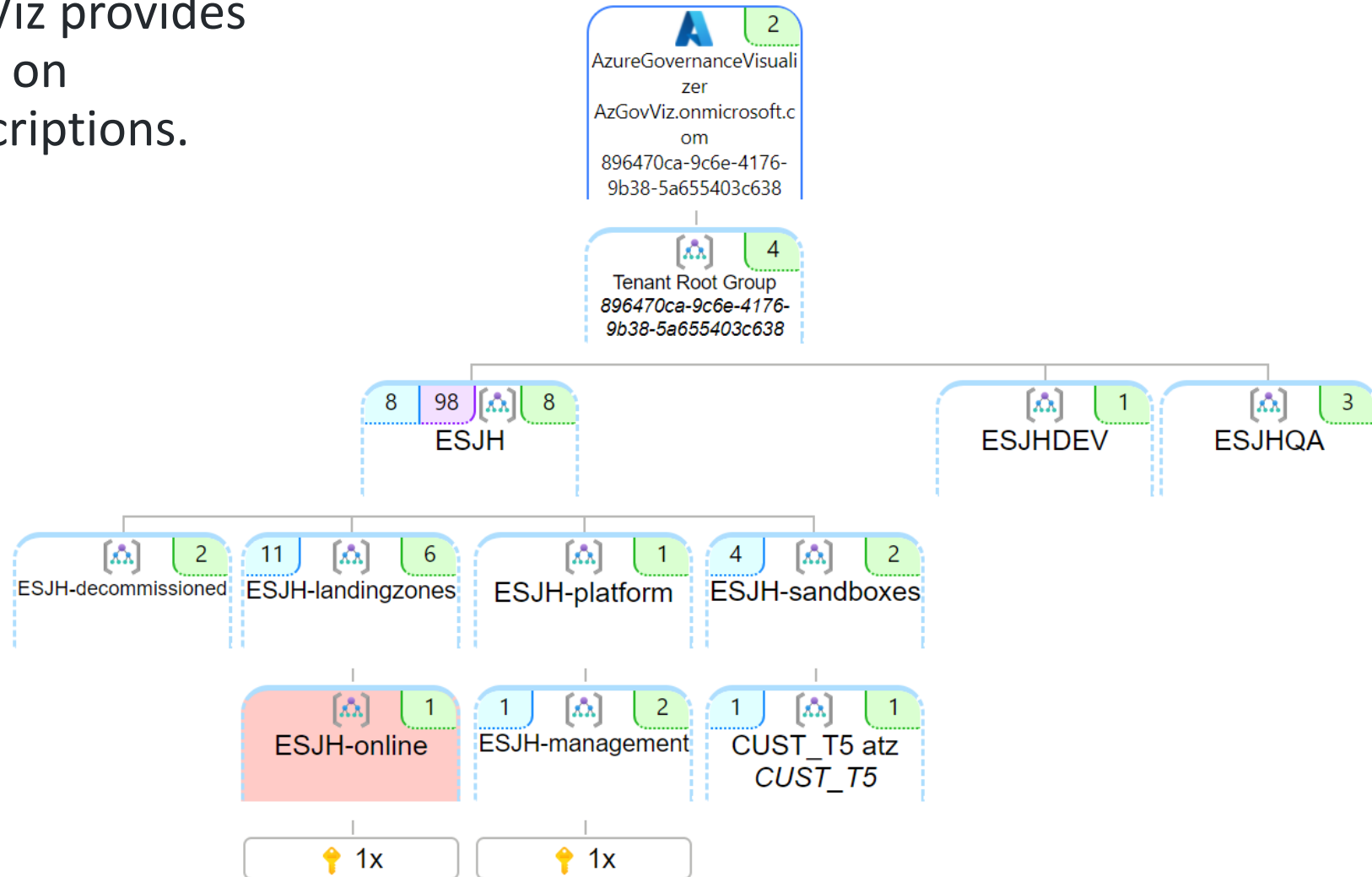
```
PowerShell 7 (x64)
Getting all Subscriptions
Getting all Subscriptions duration: 0.7313769 seconds
Getting Consumption data for scope: '8' for period 1 days (2021-04-11 - 2021-04-11)
7 consumption data entries
Getting Consumption data duration: 8.9268303 seconds
Caching built-in Policy and RBAC Role definitions
  Caching built-in Policy definitions
  Caching built-in PolicySet definitions
  Caching built-in Role definitions
Caching built-in definitions duration: 23.6690131 seconds
Collecting custom data
CustomDataCollection ManagementGroups
  1/12 ManagementGroups processed
  2/12 ManagementGroups processed
  3/12 ManagementGroups processed
  4/12 ManagementGroups processed
  5/12 ManagementGroups processed
  6/12 ManagementGroups processed
  7/12 ManagementGroups processed
  8/12 ManagementGroups processed
  9/12 ManagementGroups processed
  10/12 ManagementGroups processed
  11/12 ManagementGroups processed
  12/12 ManagementGroups processed
CustomDataCollection ManagementGroups processing duration: 1.2565152583333 minutes (75.39091 minutes)
CustomDataCollection Subscriptions
CustomDataCollection Subscriptions will process 6 of 6
processing Batch #1/1 (6 Subscriptions)
  1/6 Subscriptions processed
  2/6 Subscriptions processed
  3/6 Subscriptions processed
  4/6 Subscriptions processed
  5/6 Subscriptions processed
  6/6 Subscriptions processed
Batch #1 processing duration: 1.153349395 minutes (69.2009637 seconds)
CustomDataCollection Subscriptions processing duration: 1.1537639733333 minutes (69.2258384 minutes)
Collecting custom data duration: 2.41118401 minutes (144.6710406 seconds)
Collecting custom data for 12 ManagementGroups Avg/Max/Min duration in seconds: Average: 26.13
: 23.2589
Collecting custom data for 6 Subscriptions Avg/Max/Min duration in seconds: Average: 37.5827,
.5441
Collecting custom data total duration writing the subResourcesArray: 0.0109504 seconds
Collecting custom data API Calls (Management) total count: 176 (0 retries; 0 nextLinkReset)
Getting AAD Guest Users
  Found 5 AAD Guest Users
Getting AAD Guest Users duration: 0.0062080416666667 minutes (0.3724825 seconds)
Resolving AAD Groups
  processing 3 AAD Groups with Role assignments (indicating progress in steps of 1)
  1 AAD Groups processed
  2 AAD Groups processed
  3 AAD Groups processed
Resolving AAD Groups duration: 0.018606438333333 minutes (1.1163863 seconds)
Getting ServicePrincipals
  40 ServicePrincipals with Role assignment on MG/Sub
  1 ServicePrincipals with Role assignment on RG/Resource
  1 ServicePrincipals with Role Assignment inherited through AAD Group membership
```

PS C:\>.\AzGovViz.ps1 -ManagementGroupId <your-Management-Group-Id>

# AzGovViz

## Azure Governance Visualizer

From the collected data AzGovViz provides visibility on your **HierarchyMap** on Management Groups and Subscriptions.



# AzGovViz

## Azure Governance Visualizer

From the collected data AzGovViz provides visibility on your **HierarchyMap**, creates a **TenantSummary** on Management Groups and Subscriptions.

- Policy
- RBAC
- Blueprints
- Management Groups
- Subscriptions & Resources
- Diagnostics
- Limits
- Azure Active Directory
- Consumption
- Change tracking





# AzGovViz

## Azure Governance Visualizer

From the collected data AzGovViz provides visibility on your **HierarchyMap**, creates a **TenantSummary** on Management Groups and Subscriptions and creates **DefinitionInsights** for Policy and RBAC.

- Policy
  - Policy definitions
  - PolicySet definitions
- RBAC Role definitions

The screenshot displays the 'DefinitionInsights' tool interface. At the top, the 'Policy' section shows 1189 Policy definitions and 68 PolicySet definitions. The 'RBAC' section shows 329 Role definitions. A search bar contains the text 'Contributor'. Below the search bar, there are filters for 'Builtin/Custom', 'Data', 'canDoRoleAssignments', and 'hasAssi'. The results section shows 'results: 1-1 / 1'. The JSON definition for the 'Contributor' role is displayed, with a 'Copy definition' button. The JSON structure is as follows:

```
{
  "roleName": "Contributor",
  "type": "BuiltInRole",
  "description": "Grants full access to manage all resources, but",
  "assignableScopes": [
    "/"
  ],
  "permissions": [
    {
      "actions": [
        ""
      ],
      "notActions": [
        "Microsoft.Authorization/*/Delete",
        "Microsoft.Authorization/*/Write",
        "Microsoft.Authorization/elevateAccess/Action",
        "Microsoft.Blueprint/blueprintAssignments/write",
        "Microsoft.Blueprint/blueprintAssignments/delete",
        "Microsoft.Compute/galleries/share/action"
      ],
      "dataActions": [],
      "notDataActions": []
    }
  ],
  "createdOn": "2015-02-02T21:55:09.8806423Z",
  "updatedOn": "2021-11-11T20:13:28.6061853Z",
  "createdBy": null,
  "updatedBy": null
}
```

# AzGovViz

## Azure Governance Visualizer

From the collected data AzGovViz provides visibility on your **HierarchyMap**, creates a **TenantSummary** on Management Groups and Subscriptions, creates **DefinitionInsights** for Policy and RBAC and builds granular **ScopeInsights** on Management Groups and Subscriptions.

- Management Groups
- Subscriptions

The screenshot displays the AzGovViz interface. At the top, a 'Tenant Root Group' is listed with several sub-items: ESJH, ESJH-decommissioned, ESJH-landingzones, ESJH-online (1), ESJH-platform, and ESJH-management (1). Below this, a section titled 'Highlight Management Group in HierarchyMap' provides details for the 'ESJH-management' group. This includes its ID, path, and a summary of its contents: 0 ManagementGroups below, 1 Subscription below, no consumption data, 3 ResourceTypes (12 Resources) in 1 Location, 2/3 ResourceTypes with Diagnostics, 5 Policy Assignments, 4 PolicySet Assignments, and a Policy Assignment Limit of 1/200. It also lists 15 Role Assignments and 1 linked Subscription. A yellow bar highlights the 'management' subscription. Below this, a section titled 'Highlight Subscription in HierarchyMap' provides details for the 'management' subscription. This includes its ID, path, state (Enabled), QuotaID (PayAsYouGo\_2014-09-01), and an ASC Secure Score of 0 of 14 points. It also lists 1 Subscription Tag, 1 Tag Name Usage, no consumption data, 1 Resource Group, 3 ResourceTypes (12 Resources) in 1 Location, 2/3 ResourceTypes with Diagnostics, 5 Policy Assignments, 5 PolicySet Assignments, and a Policy Assignment Limit of 1/200. It also lists 15 Role Assignments. At the bottom, a partial view of the 'ESJH-sandboxes' group is visible.

Tenant Root Group (7b97aaae-e49f-4c81-81b3-1446d85cdc22) ↑

- ESJH ↑
- ESJH-decommissioned ↑
- ESJH-landingzones ↑
- ESJH-online 1
- ESJH-platform ↑
- ESJH-management 1

**Highlight Management Group in HierarchyMap**  
Management Group Name: ESJH-management  
Management Group Id: ESJH-management  
Management Group Path: 7b97aaae-e49f-4c81-81b3-1446d85cdc22/ESJH/ESJH-platform/ESJH-management  
0 ManagementGroups below this scope  
1 Subscriptions below this scope  
No Consumption data available for Subscriptions under this ManagementGroup  
3 ResourceTypes (12 Resources) in 1 Locations (all Subscriptions below this scope)  
2/3 ResourceTypes Diagnostics capable (2 Metrics, 2 Logs) (all Subscriptions below this scope)  
5 Policy Assignments (1 at scope, 4 inherited) (Built-in: 2 | Custom: 3)  
4 PolicySet Assignments (0 at scope, 4 inherited) (Built-in: 3 | Custom: 1)  
Policy Assignment Limit: 1/200  
0 Custom Policy definitions scoped  
0 Custom PolicySet definitions scoped  
0 Blueprints scoped  
15 Role Assignments (13 inherited) (User: 0 | Group: 0 | ServicePrincipal: 0 | Orphaned: 0) (CustomRoleOwn  
1 Subscriptions linked  
management (f1145e47-d746-40cc-ab37-d392b0cdb666)

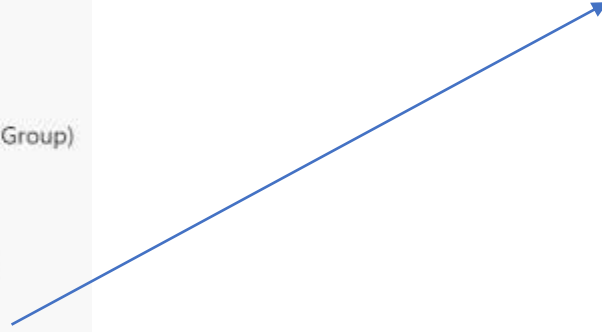
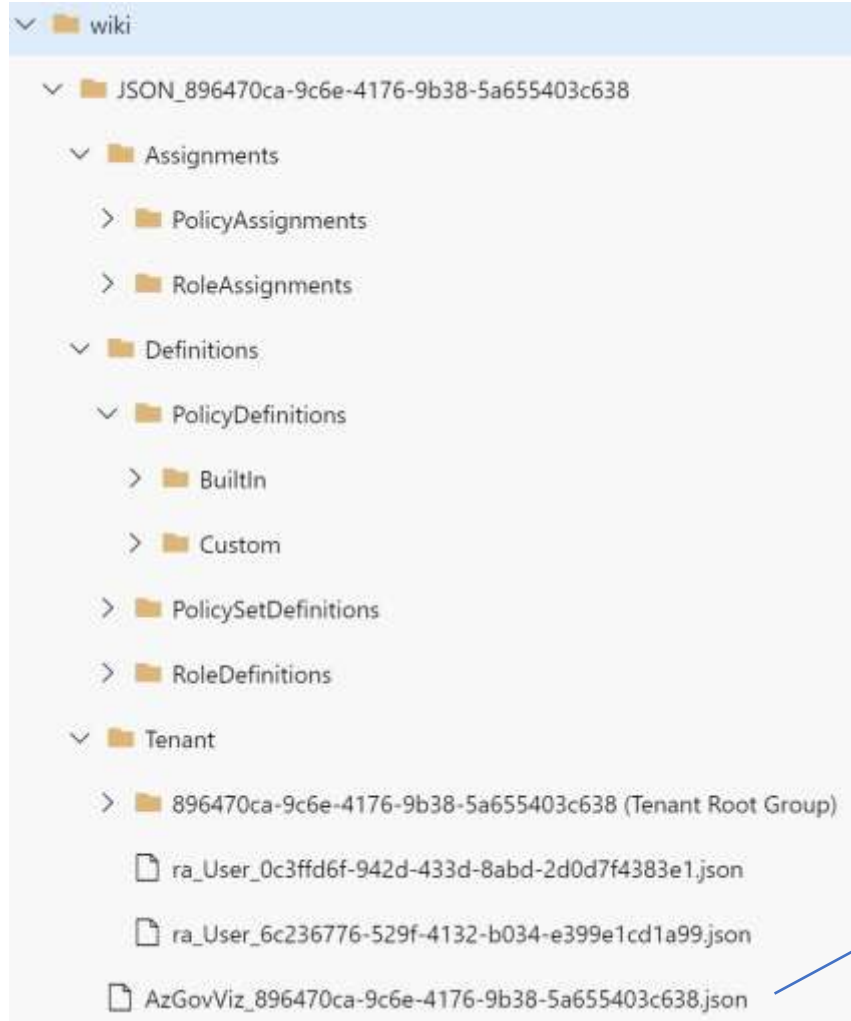
**Highlight Subscription in HierarchyMap**  
Subscription Name: management  
Subscription Id: f1145e47-d746-40cc-ab37-d392b0cdb666  
Subscription Path: 7b97aaae-e49f-4c81-81b3-1446d85cdc22/ESJH/ESJH-platform/ESJH-management/f11  
State: Enabled  
QuotaId: PayAsYouGo\_2014-09-01  
ASC Secure Score: 0 of 14 points [Video](#) [Blog](#)  
1 Subscription Tags | Limit: (1/50)  
Tag Name Usage (1 unique Tag Names applied at Subscription)  
No Consumption data available  
1 Resource Groups | Limit: (1/980)  
Resource Providers Detailed  
Resource Locks  
3 ResourceTypes (12 Resources) in 1 Locations  
2/3 ResourceTypes Diagnostics capable (2 Metrics, 2 Logs)  
5 Policy Assignments (0 at scope, 5 inherited) (Built-in: 2 | Custom: 3)  
5 PolicySet Assignments (1 at scope, 4 inherited) (Built-in: 4 | Custom: 1)  
Policy Assignment Limit: 1/200  
0 Custom Policy definitions scoped  
0 Custom PolicySet definitions scoped  
0 Blueprints assigned  
0 Blueprints scoped  
15 Role Assignments (15 inherited) (User: 0 | Group: 0 | ServicePrincipal: 0 | Orphaned: 0) (CustomRoleOwn

ESJH-sandboxes ↑

# AzGovViz

## Azure Governance Visualizer

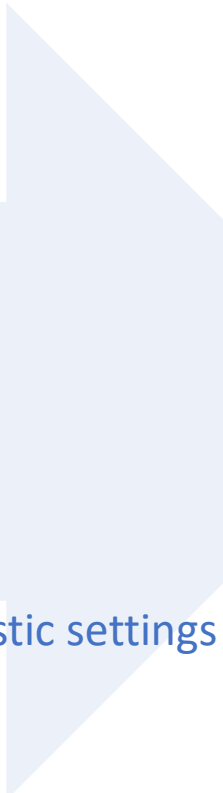
### Your Tenant in JSON



```
1 {
2   "Tenant": {
3     "TenantId": "896470ca-9c6e-4176-9b38-5a655403c638",
4     "RoleAssignments": {
5       "/providers/Microsoft.Authorization/roleAssignments/0c3ffd6f-942d-433d-8abd-2d0d7f4383e1": {
18       },
19       "/providers/Microsoft.Authorization/roleAssignments/6c236776-529f-4132-b034-e399e1cd1a99": {
32       }
33     },
34     "ManagementGroups": {
35       "896470ca-9c6e-4176-9b38-5a655403c638": {
36         "MgId": "896470ca-9c6e-4176-9b38-5a655403c638",
37         "MgName": "Tenant Root Group",
38         "mgParentId": "TenantRoot",
39         "mgParentName": "TenantRoot",
40         "level": "0",
41         "PolicyDefinitionsCustom": {},
42         "PolicySetDefinitionsCustom": {},
43         "BlueprintDefinitions": {},
44         "PolicyAssignments": {},
45         "RoleAssignments": { ...
102       },
103       "DiagnosticSettings": {},
104       "Subscriptions": {},
105       "ManagementGroups": {
106         "ESJH": {
107           "MgId": "ESJH",
108           "MgName": "ESJH",
109           "mgParentId": "896470ca-9c6e-4176-9b38-5a655403c638",
110           "mgParentName": "Tenant Root Group",
111           "level": "1",
112           "PolicyDefinitionsCustom": { ...
16156         },
16157           "PolicySetDefinitionsCustom": { ...
18005         },
18006         "BlueprintDefinitions": {},
18007         "PolicyAssignments": { ...
18262         },
18263         "RoleAssignments": { ...
18376         },
18377         "DiagnosticSettings": {},
18378         "Subscriptions": {},
18379         "ManagementGroups": { ...
19587       }
19588     },
19589     "ESJHDEV": { ...
19618     },
19619     "ESJHQA": { ...
19676     }
19677   }
19678 }
19679 },
19680 "CustomRoleDefinitions": {
19681   "08a2d627-a94e-461e-8350-432b457d00a3": {
```



### data → output

- 
- Hierarchy Settings
  - Policy Definitions, Assignments, Compliance
  - RBAC Definitions, Assignments
  - Blueprints Definitions, Assignments
  - Resource Groups
  - Resource Providers
  - Resource Types
  - Resources
  - Resources leveraging UAMI / vice versa
  - Microsoft Defender for Cloud plan insights
  - Locks usage
  - Tags usage
  - Approaching ARM Limits
  - Management Group & Subscription diagnostic settings
  - Resource diagnostics capability
  - ServicePrincipal/Application insights
  - Consumption information
  - Security
  - Change Tracking (RBAC, Policy, Resources)

#### CSV file(s)

- Collected data available in CSV file

#### HTML file

- Connects the dots by providing insights on **HierarchyMap**, **TenantSummary**, **DefinitionInsights** and **ScopeInsights** on Management Groups and Subscriptions
- Single HTML file **ScopeInsights** per Subscription

#### Azure DevOps Wiki 'Mermaid plugin' ready markdown file

- Limited to hierarchy and list of Management Groups / Subscriptions plus a short summary

#### JSON file(s)

- Export of Management Group Hierarchy including all MG/Sub Policy/RBAC definitions, Policy/RBAC assignments and some more relevant information to JSON
- All Policy and RBAC definitions

### Parameters

#### -DoManagementGroupsOnly

Collect data only for Management Groups

Subscription data such as e.g. Policy assignments etc. will not be collected

#### -HierarchyMapOnly

Only create the Hierarchy Map

#### -DoNotShowRoleAssignmentsUserData

Scrub pii data such as user names and E-Mail address information

#### -ChangeTrackingDays

Define the period for change tracking on RBAC, Policy and Resources

#### -DoAzureConsumption

Collect consumption information (aggregation for Management Group scopes; by ResourceType)

```
.\pwsh\AzGovVizParallel.ps1 -DoAzureConsumption
```

.. and a lot more parameters are available to adjust AzGovViz data return to your needs.

*aka.ms/AzGovViz#Parameters*

# AzGovViz

## Azure Governance Visualizer

### Scenarios / requirements

#### Requirements for all scenarios

- PowerShell Core (7.0.3)
- PowerShell Az Modules
  - Az.Accounts
  - ~~Az.Resources~~
  - ~~Az.ResourceGraph~~
- RBAC: **Reader** on Management Group

Scenario **A**: Console - User (userType=member) \*

Scenario **B**: Console - User (userType=guest) \*\*

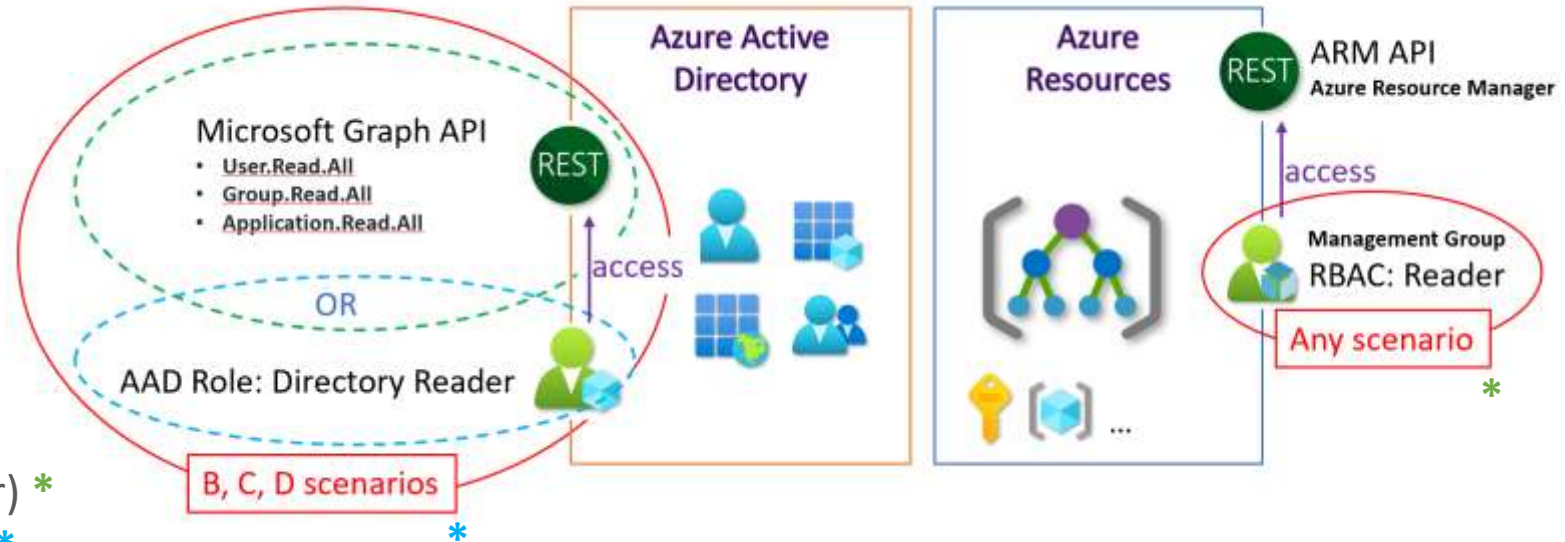
Scenario **C**: Console - ServicePrincipal \*\*

Scenario **D**: Azure DevOps, GitHub Actions - ServicePrincipal \*\*

\*API permissions: <http://aka.ms/AzGovViz#azgovviz-technical-documentation>

**Azure Environments:** AzGovViz is designed to support all Azure Clouds. By today it is verified working on AzureCloud, AzureUSGovernment and AzureChinaCloud (China Billing not supported)

**Run AzGovViz in** Azure DevOps | Azure CloudShell | GitHub Actions | GitHub Codespaces | Any PowerShell console



## AzGovViz DEMO

Enterprise-Scale Landing Zones ([WingTip](#))



## RoadMap

- Option to ingest data to Log Analytics
- Option to publish HTML output to Azure Static Web App

## Confidentiality of information

AzGovViz creates very detailed information on your Azure Governance setup.

In your organizations best interest, the **outputs should be protected from non-authorized access!**

### Your contribution welcome!

#### AzGovViz GitHub repositories

- Project Repository  
<https://github.com/JulianHayward/Azure-MG-Sub-Governance-Reporting> (aka.ms/AzGovViz)
- Microsoft CAF (Cloud Adoption Framework) Repository  
<https://github.com/microsoft/CloudAdoptionFramework/tree/master/govern/AzureGovernanceVisualizer>

#### Also checkout **AzAdvertizer**

.. helps you to keep up with the pace by providing overview and insights on new releases and changes/updates for Azure Governance capabilities such as Azure Policy's policy definitions, initiatives (set definitions), aliases and Azure RBAC's role definitions and resource provider operations. [aka.ms/AzAdvertizer](https://aka.ms/AzAdvertizer)