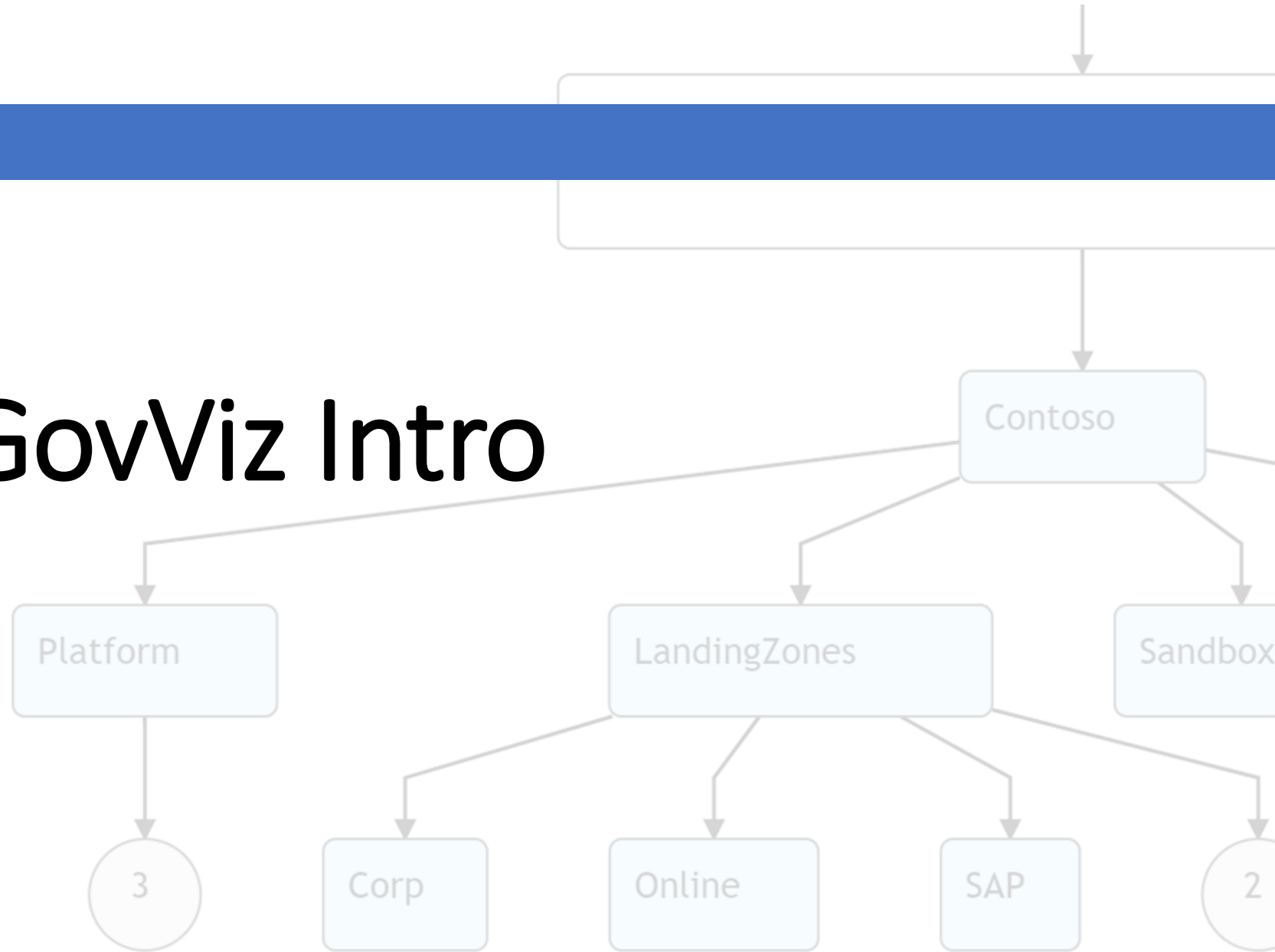


AzGovViz Intro

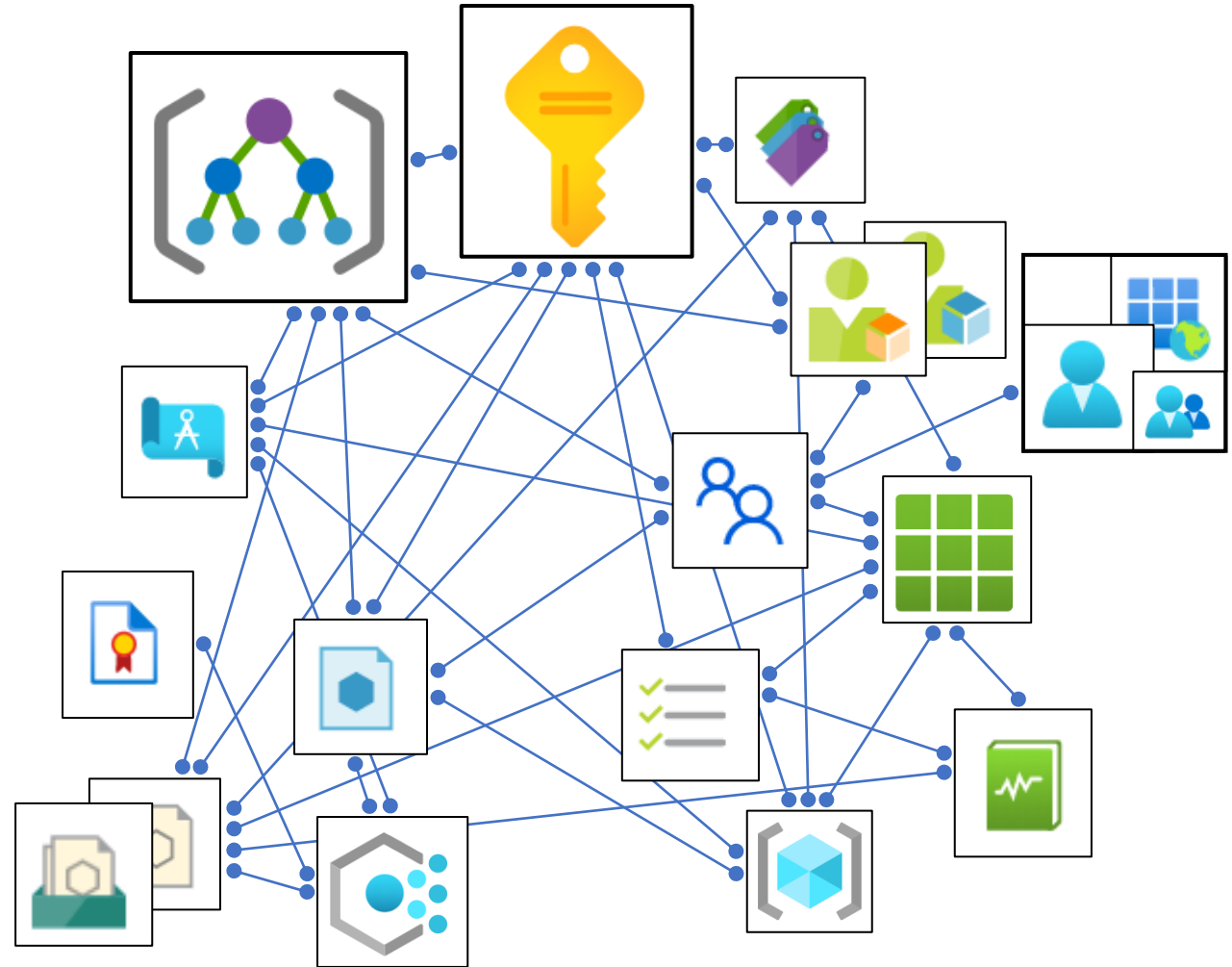


'Azure Governance can be a complex thing.'

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.



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.

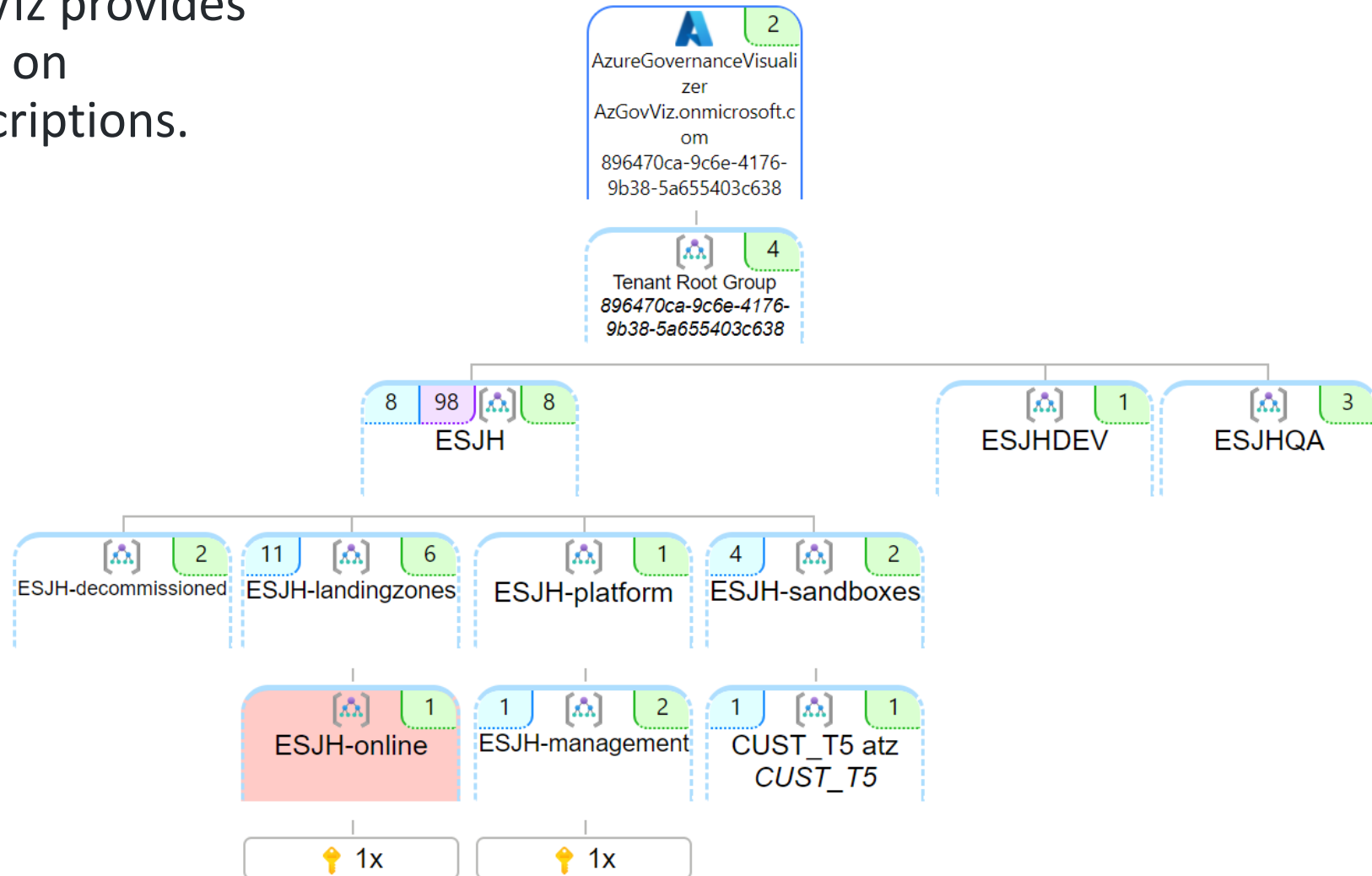
The technical requirements as well as the required permissions are minimal.

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

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: 1.25651525833333 minutes (75.3909155 seconds)  
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: 1.15376397333333 minutes (69.2258384 seconds)  
Collecting custom data duration: 2.41118401 minutes (144.6710406 seconds)  
Collecting custom data for 12 ManagementGroups Avg/Max/Min duration in seconds: Average: 26.1304; Maximum:  
: 23.2589  
Collecting custom data for 6 Subscriptions Avg/Max/Min duration in seconds: Average: 37.5827; Maximum: 41.2  
.5441  
Collecting custom data total duration writing the subResourcesArray: 0.0109504 seconds  
Collecting custom data APICalls (Management) total count: 176 (0 retries; 0 nextLinkReset)  
Getting AAD Guest Users  
Found 5 AAD Guest Users  
Getting AAD Guest Users duration: 0.00620804166666667 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: 0.0186064383333333 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  
processing 41 unique ServicePrincipals (indicating progress in steps of 5)  
5 ServicePrincipals processed  
10 ServicePrincipals processed
```

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



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

The screenshot displays the AzGovViz Tenant Summary dashboard, which provides a comprehensive overview of Azure governance metrics for a specific tenant. The dashboard is organized into several sections, each with a distinct icon and color-coded header.

- Policy:** This section shows 96 Custom Policy definitions (Tenant wide), 24 Orphaned Custom Policy definitions (Tenant wide), 3 Custom PolicySet definitions (Tenant wide) (Limit: 3/2500), 2 Orphaned Custom PolicySet definitions (Tenant wide), 0 PolicySets / deprecated Built-in Policy, 0 Policy Assignments / deprecated Built-in Policy, 2 Policy Exemptions | Expired: 2, and 120 Policy Assignments (24 unique).
- RBAC:** This section shows 3 Custom Role definitions (Tenant wide) (Limit: 3/5000), 3 Orphaned Custom Role definitions (Tenant wide), 0 Orphaned Role Assignments (Tenant wide), 190 Role Assignments (31 unique), 2 Classic Role Assignments (Tenant wide), 0 Custom Role definitions Owner permissions (Tenant wide), 12 Owner permission assignments to ServicePrincipal (Tenant wide), 23 Owner permission assignments to notGroup (Tenant wide), 1 UserAccessAdministrator permission assignments to notGroup (Tenant wide), and 0 Guest Users with high permissions (Tenant wide).
- Blueprints:** This section shows 0 Blueprint definitions, 0 Blueprint Assignments, and 0 Orphaned Blueprint definitions.
- Management Groups:** This section shows 9 Management Groups, Hierarchy Settings | Default Management Group ID: 'ESJH-online' docs, and Hierarchy Settings | Require authorization for Management Group creation: 'False' docs.
- Subscriptions & Resources:** This section shows 2 Subscriptions (state: enabled), 0 Subscriptions out-of-scope, Tag Name Usage (2 unique Tag Names applied at Resource, ResourceGroup, Subscription), Resources (9 ResourceTypes) (21 Resources) (Tenant wide), Resources byLocation (9 ResourceTypes) (21 Resources) in 2 Locations (Tenant wide), Resource Providers Total: 214 Registered/Registering: 211 NotRegistered/Unregistering: 3, Resource Providers Detailed, and Resource Locks.
- Diagnostics:** This section shows Management Groups (1 Management Groups configured for Diagnostic settings (1 settings), 8 Management Groups NOT configured for Diagnostic settings), Subscriptions (2 Subscriptions configured for Diagnostic settings (2 settings), All Subscriptions are configured for Diagnostic settings docs), and Resources (Resources Diagnostics capable 5/9 ResourceTypes (4 Metrics, 4 Logs), ResourceDiagnostics for Logs - Policy Lifecycle recommendations).
- Limits:** This section shows a summary of 80% limits.
- Tenant:** This section shows PolicySet definitions: 3/2500 docs and Custom Role definitions: 3/5000 docs.
- Management Groups:** This section shows 0 Management Groups approaching Limit (200) for PolicyAssignment docs, 0 Management Groups approaching Limit (500) for Policy Scope docs, 0 Management Groups approaching Limit (200) for PolicySet Scope docs, and 0 Management Groups approaching Limit (500) for RoleAssignment docs.
- Subscriptions:** This section shows 1 Subscriptions approaching Limit (980) for ResourceGroups, 0 Subscriptions approaching Limit (50) for Tags docs, 0 Subscriptions approaching Limit (200) for PolicyAssignment docs, 0 Subscriptions approaching Limit (500) for Policy Scope docs, 0 Subscriptions approaching Limit (200) for PolicySet Scope docs, and 0 Subscriptions approaching Limit (2000) for RoleAssignment docs.
- Azure Active Directory:** This section shows Demystifying Service Principals - Managed Identities devBlogs, No ServicePrincipals where the API returned 'Request_ResourceNotFound', No Applications where the API returned 'Request_ResourceNotFound', 12 AAD ServicePrincipals type=ManagedIdentity, 3 AAD ServicePrincipals type=Application | 0 Secrets expire < 14d | 0 Certificates expire < 14d, and 0 External (appOwnerOrganizationId) AAD ServicePrincipals type=Application.
- Consumption:** This section shows Customize your Azure environment optimizations (Cost, Reliability & more) with Azure Optimization Engine (AOE), Total cost 0.00001838376 EUR generated by 1 Resources (1 ResourceTypes) in 1 Subscriptions last 1 days (2021-06-15 - 2021-06-15), and Preview: Change tracking | last 14 days; after 02-Jun-2021 16:10:16.

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

- Policy definitions
- PolicySet definitions
- RBAC Role definitions

— Policy

✓ 916 Policy definitions

✓ 59 PolicySet definitions

— RBAC

✓ 252 Role definitions

Search JSON BuiltIn/Custom Data hasAssignment

Clear Clear Clear

results: 1-10 / 252 Page 1 of 26

JSON

```
{
  "Name": "AcrDelete",
  "Id": "c2f4ef07-c644-48eb-af81-4b1b4947fb11",
  "IsCustom": false,
  "Description": "acr delete",
  "Actions": [
    "Microsoft.ContainerRegistry/registries/artifacts/delete"
  ],
  "NotActions": [],
  "DataActions": [],
  "NotDataActions": [],
  "AssignableScopes": [
    "/"
  ]
}
```

```
{
  "Name": "AcrImageSigner",
  "Id": "6cef56e8-d556-48e5-a04f-b8e64114680f",
  "IsCustom": false,
  "Description": "acr image signer",
  "Actions": [
    "Microsoft.ContainerRegistry/registries/sign/write"
  ],
  "NotActions": [],
  "DataActions": [],
  "NotDataActions": [],
  "AssignableScopes": [
    "/"
  ]
}
```

```
{
  "Name": "AcrPull",
  "Id": "7f951dda-4ed3-4680-a7ca-43fe172d538d",
  "IsCustom": false,
  "Description": "acr pull",
  "Actions": [
    "Microsoft.ContainerRegistry/registries/pull/read"
  ],
  "NotActions": [],
  "DataActions": [],
  "NotDataActions": [],
  "AssignableScopes": [
    "/"
  ]
}
```

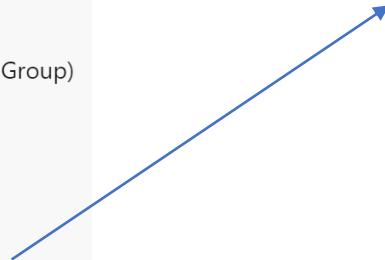
From the collected data AzGovViz provides visibility on your **HierarchyMap**, creates a **TenantSummary**, creates **DefinitionInsights** and builds granular **ScopeInsights** on Management Groups and Subscriptions.

- Management Groups
- Subscriptions

The screenshot displays the AzGovViz interface. At the top, a 'Tenant Root Group' is expanded to show a hierarchy of Management Groups: ESJH, ESJH-decommissioned, ESJH-landingzones, ESJH-online (1), ESJH-platform, and ESJH-management (1). The 'ESJH-management' group is selected, and its 'ScopeInsights' are shown. The insights include: 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) (Builtin: 2 | Custom: 3), 4 PolicySet Assignments (0 at scope, 4 inherited) (Builtin: 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) (CustomRoleOwner: 0, OwnerAssignmentSP: 8) (Policy related: 8) | Limit: (2/500), 1 Subscriptions linked, and management (f1145e47-d746-40cc-ab37-d392b0cdb666). The 'management' subscription is selected, and its 'ScopeInsights' are shown. The insights include: Subscription Name: management, Subscription Id: f1145e47-d746-40cc-ab37-d392b0cdb666, Subscription Path: 7b97aaae-e49f-4c81-81b3-1446d85cdc22/ESJH/ESJH-platform/ESJH-management/f1145e47-d746-40cc-ab37-d392b0cdb666, 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) (Builtin: 2 | Custom: 3), 5 PolicySet Assignments (1 at scope, 4 inherited) (Builtin: 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) (CustomRoleOwner: 0, OwnerAssignmentSP: 8) (Policy related: 8) | Limit: (0/2000), and ESJH-sandboxes.

Your Tenant in JSON

- ▼ wiki
 - ▼ JSON_896470ca-9c6e-4176-9b38-5a655403c638
 - ▼ Assignments
 - > PolicyAssignments
 - > RoleAssignments
 - ▼ Definitions
 - ▼ PolicyDefinitions
 - > BuiltIn
 - > Custom
 - > PolicySetDefinitions
 - > RoleDefinitions
 - ▼ Tenant
 - > 896470ca-9c6e-4176-9b38-5a655403c638 (Tenant Root Group)
 - ra_User_0c3ffd6f-942d-433d-8abd-2d0d7f4383e1.json
 - ra_User_6c236776-529f-4132-b034-e399e1cd1a99.json
 - AzGovViz_896470ca-9c6e-4176-9b38-5a655403c638.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
- Locks usage
- Tags usage
- Approaching ARM Limits
- Management Group & Subscription diagnostic settings
- Resource diagnostics capability
- ServicePrincipal/Application insights
- Consumption information
- Security

CSV file(s)

- Collected data available in CSV file
- PolicyAssignments, RoleAssignments, AllResource

HTML file

- Connects the dots by providing insights on **HierarchyMap**, **TenantSummary**, **DefinitionInsights** and **ScopeInsights** on Management Groups and Subscriptions

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

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

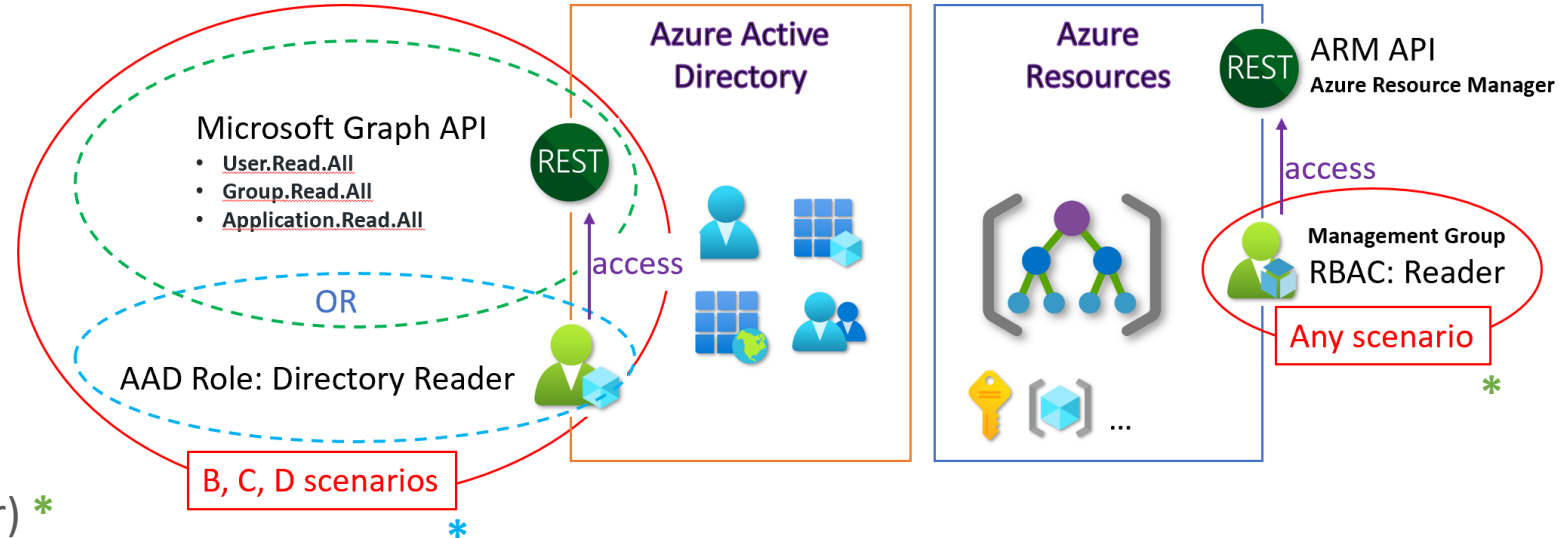
Scenario **A**: Console - User (userType=member) *

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

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

Scenario **D**: Azure DevOps Pipeline - ServiceConnection/ServicePrincipal **

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



Environments: AzGovViz is designed to support all Azure Clouds (AzureCloud, AzureUSGovernment, AzureChinaCloud, AzureGermanCloud), however by today it is only verified working on AzureCloud and AzureChinaCloud (China Billing not supported)

AzGovViz DEMO version 5

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

RoadMap

- Ingest findings to Log Analytics



Confidentiality of information



AzGovViz creates very detailed information about your Azure Governance setup. In your organizations best interest, the **outputs should be protected from non-authorized access!**

Your contribution welcome!

AzGovViz GitHub Repositories

- Main 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

