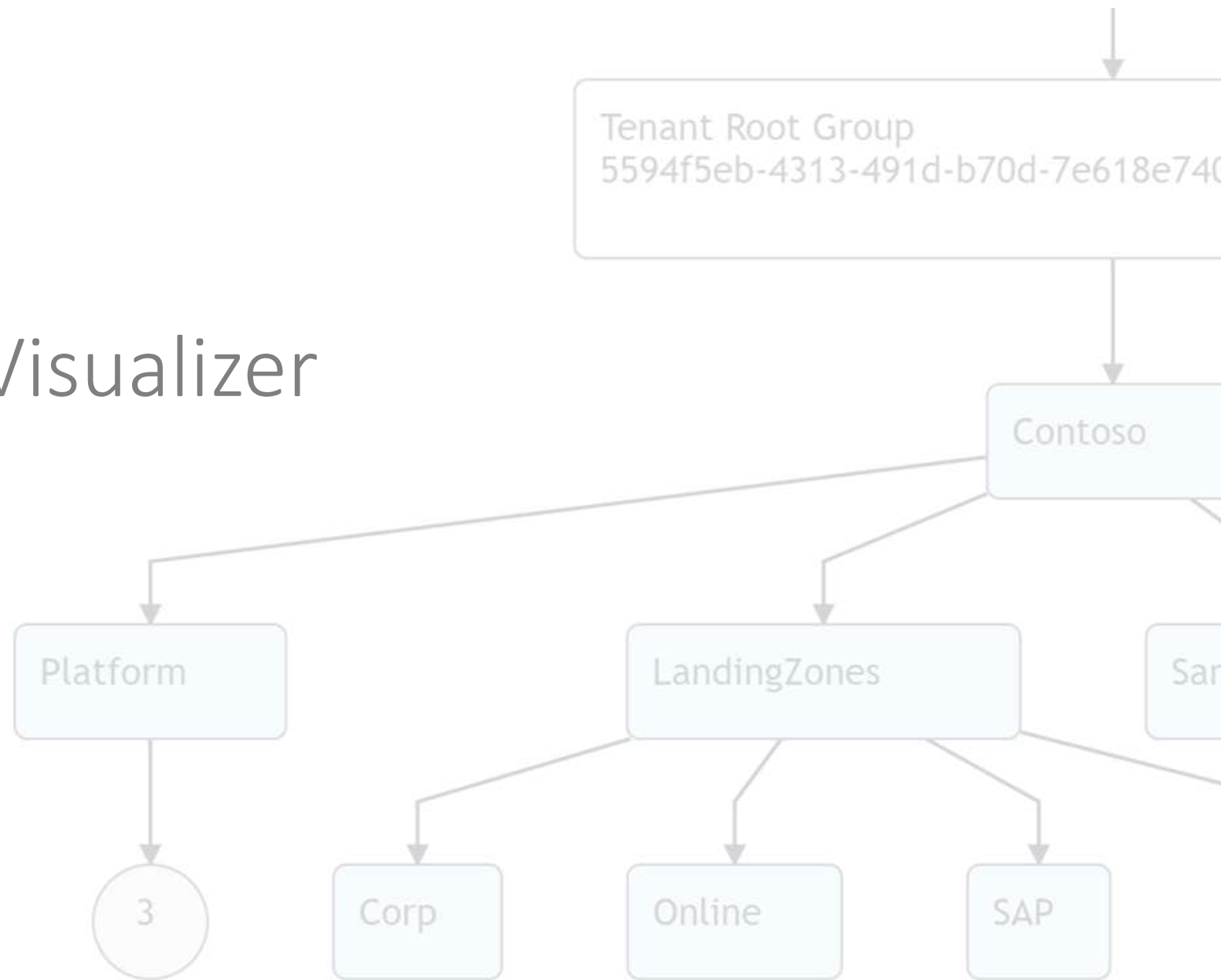


# AzGovViz

## Azure Governance Visualizer



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



# 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.

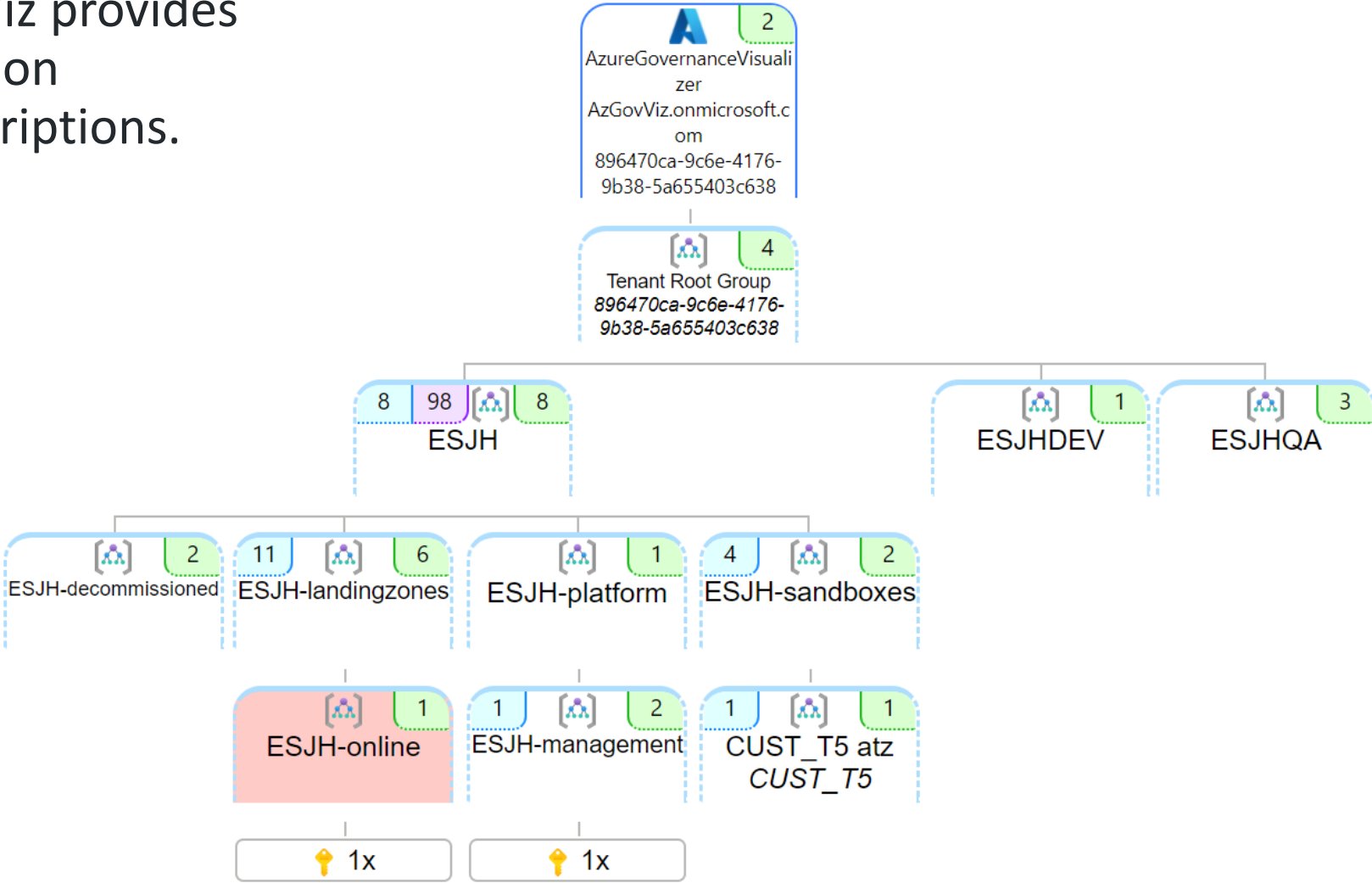
```
PowerShell 7 (x64)
Getting all Subscriptions
Getting all Subscriptions duration: 0.7313769 seconds
Getting Consumption data for scope: '8' for period 1 days (2021-04-11 - 2021-04-11)
  7 consumption data entries
Getting Consumption data duration: 8.9268303 seconds
Caching built-in Policy and RBAC 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: 1.25651525833333 minutes (75.39091
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
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 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
```

```
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

The screenshot displays a comprehensive overview of a tenant's Azure governance state. Key sections include:

- Policy:** 96 Custom Policy definitions (Tenant wide), 24 Orphaned Custom Policy definitions (Tenant wide), 1 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, 120 Policy Assignments (24 unique).
- RBAC:** 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), 0 Guest Users with high permissions (Tenant wide).
- Blueprints:** 0 Blueprint definitions, 0 Blueprint Assignments, 0 Orphaned Blueprint definitions.
- Management Groups:** 9 Management Groups, Hierarchy Settings | Default Management Group Id: 'ES/4-online' docs, Hierarchy Settings | Require authorization for Management Group creation: 'False' docs.
- Subscriptions & Resources:** 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 (1 ResourceTypes) (21 Resources) in 2 Locations (Tenant wide), Resource Providers Total: 214 Registered/Registering, 211 NotRegistered/Unregistering, 3 Resource Providers Detailed, Resource Locks.
- Diagnostics:** 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; Resources: Resources Diagnostics capable: 5/9 ResourceTypes (4 Metrics, 4 Logs), ResourceDiagnostics for Logs - Policy lifecycle recommendations.
- Limits:** 00%
- Tenant:** PolicySet definitions: 3/2500 docs, Custom Role definitions: 3/5000 docs.
- Management Groups:** 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, 0 Management Groups approaching Limit (500) for RoleAssignment docs.
- Subscriptions:** 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, 0 Subscriptions approaching Limit (2000) for RoleAssignment docs.
- Azure Active Directory:** Demythifying Service Principals - Managed Identities settings, 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, 0 External (appOwnerOrganizationId) AAD ServicePrincipals type=Application.
- Consumption:** 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), Preview: Change tracking | last 14 days; after 02-Jun-2021 16:10:16.

# 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 AzGovViz interface. At the top, the 'DefinitionInsights' section is active, showing a summary of 1189 Policy definitions and 68 PolicySet definitions. Below this, the 'RBAC' section is selected, showing 329 Role definitions. A search bar contains the text 'Contributor', and several filter buttons (Builtin/Custom, Data, canDoRoleAssignments, hasAssi) are visible. The main content area shows a JSON definition for the 'Contributor' role, with the role name highlighted in yellow. The JSON includes details such as the role type, description, assignable scopes, permissions, and creation/update timestamps.

```
JSON
Copy definition
{
  "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 HierarchyMap shows a tree structure of Management Groups under a Tenant Root Group. The selected group is 'ESJH-management'. Below the HierarchyMap, the 'Highlight Management Group in HierarchyMap' section provides details for the 'ESJH-management' group, including its ID, path, and various insights such as 3 ResourceTypes, 5 Policy Assignments, and 4 PolicySet Assignments. The 'management' subscription is highlighted in yellow. Below this, the 'Highlight Subscription in HierarchyMap' section provides details for the 'management' subscription, including its ID, path, state, and various insights such as 1 Subscription Tags, 1 Resource Groups, and 3 ResourceTypes.



### 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) \*\*

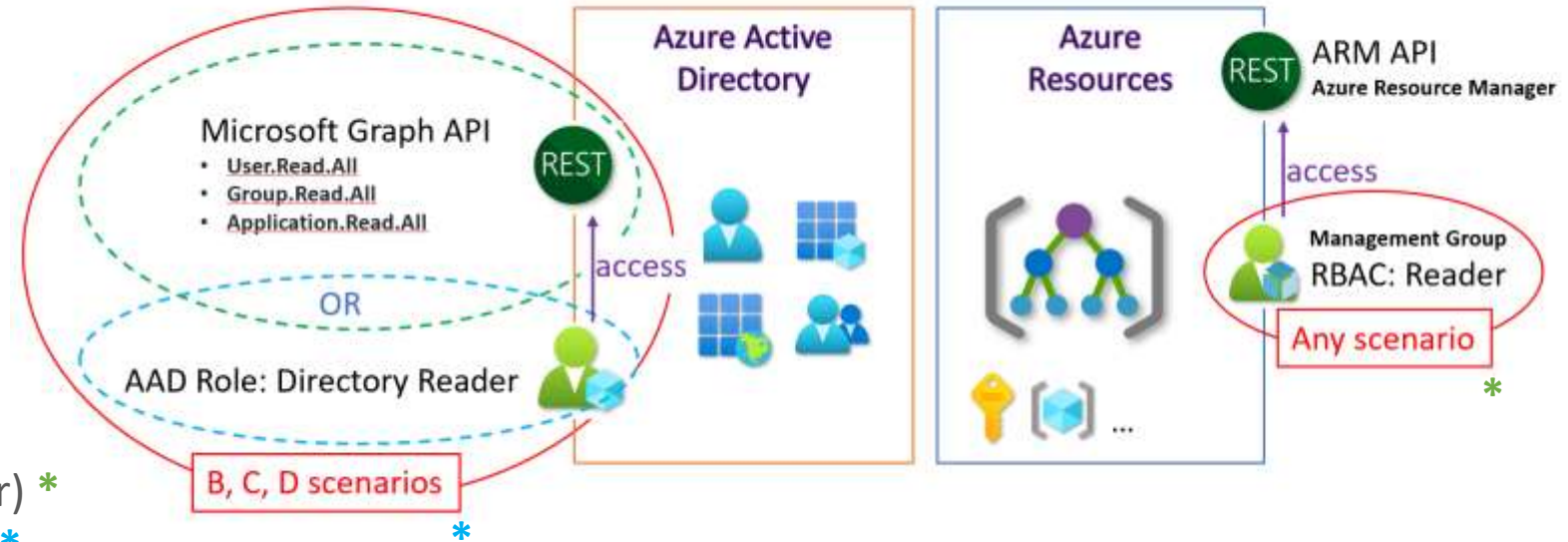
Scenario **C**: Console - ServicePrincipal \*\*

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 **AzAdvertiser**

.. 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/AzAdvertiser](https://aka.ms/AzAdvertiser)