

Azure RBAC, Access policies and other Azure Myths

Eric Berg
Microsoft MVP



Eric Berg



Vice President Expert @ CGI



Cloud, Datacenter and Management



Azure, AWS, GCP



info@ericberg.de



[@ericberg_de](https://twitter.com/ericberg_de) | [@GeekZeugs](https://twitter.com/GeekZeugs)



www.ericberg.de | www.geekzeugs.de



Azure Account

RBAC

Access Policies

Global Admin

Owner

Roles

Assignment

Control Plane



Service Principal

Contributor



Scopes

Custom Roles

Data Plane

...

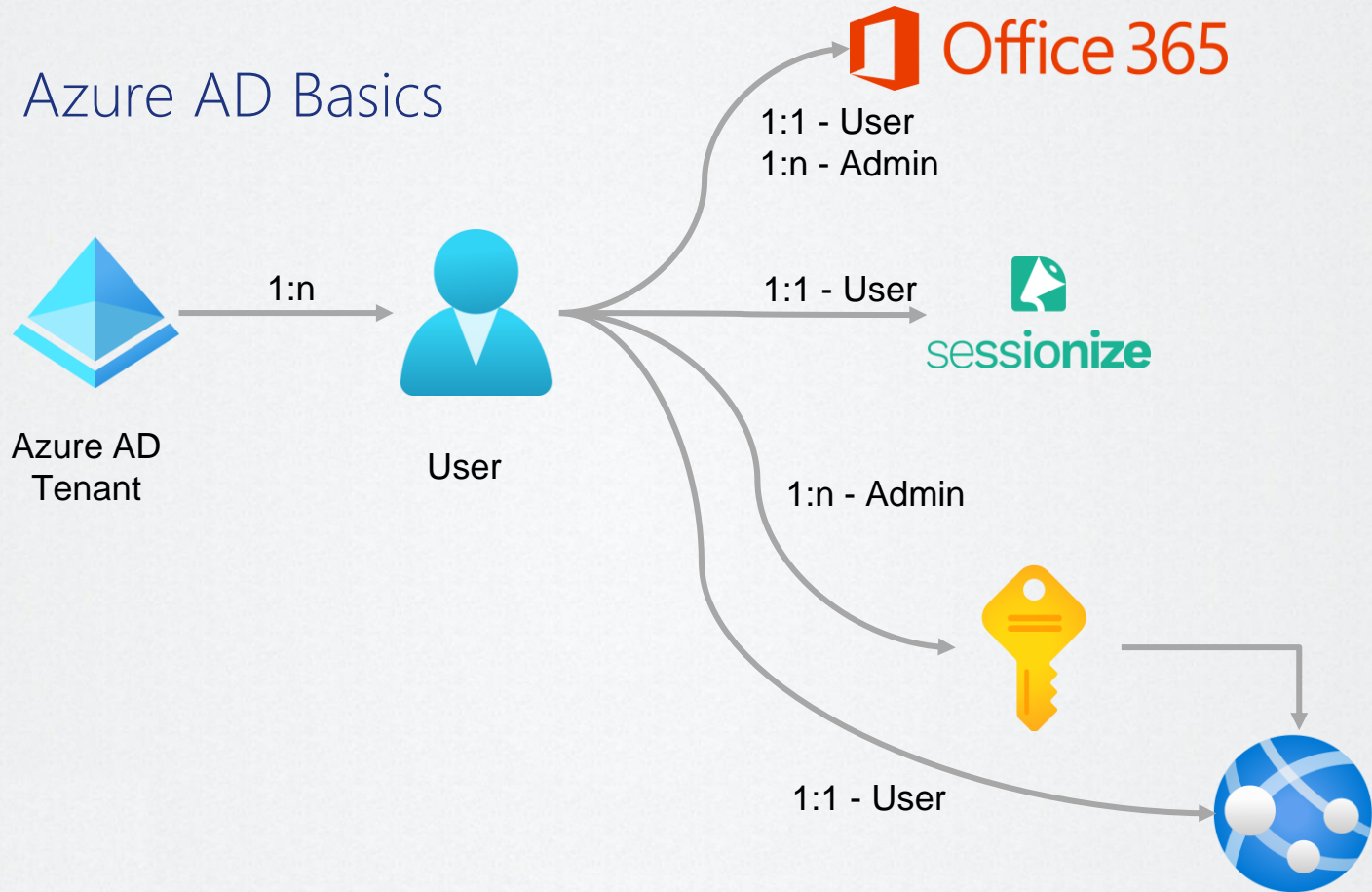




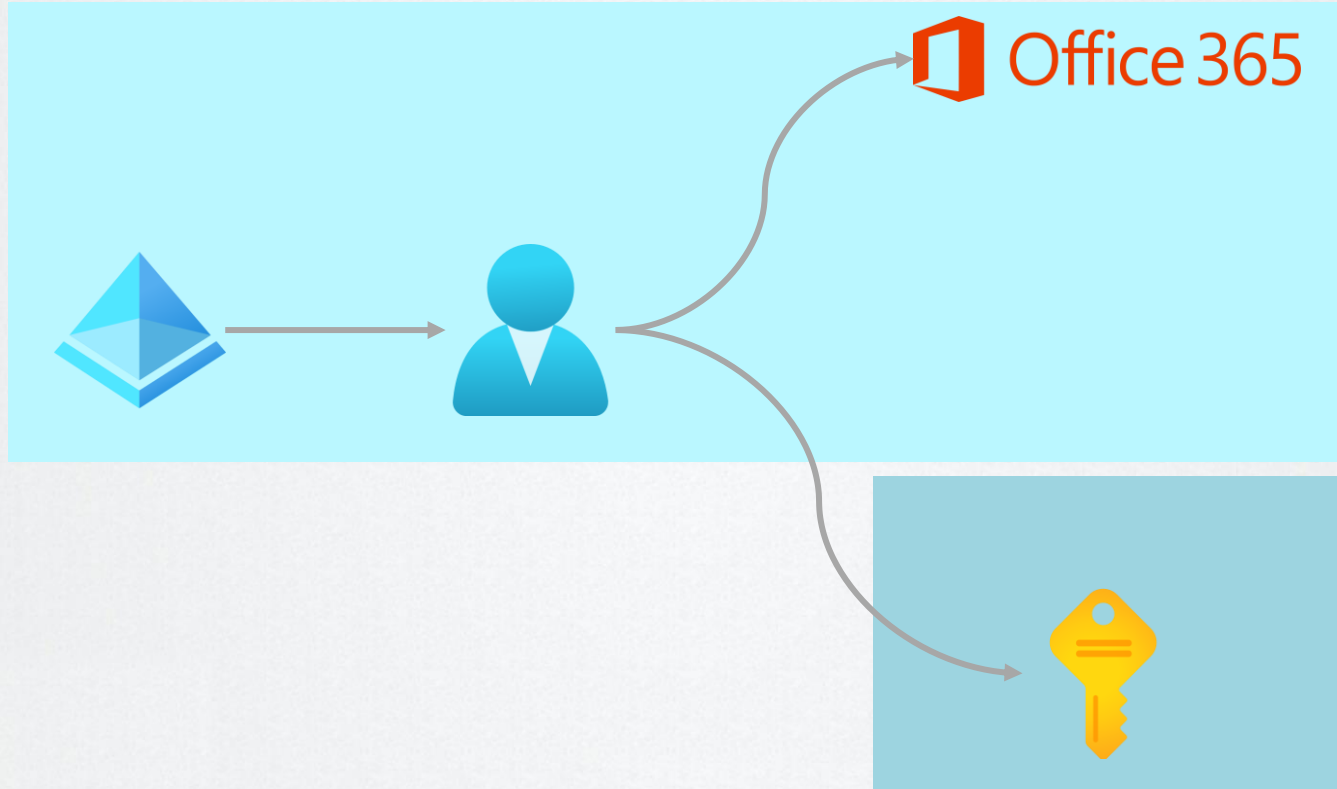
How Azure AD works ...



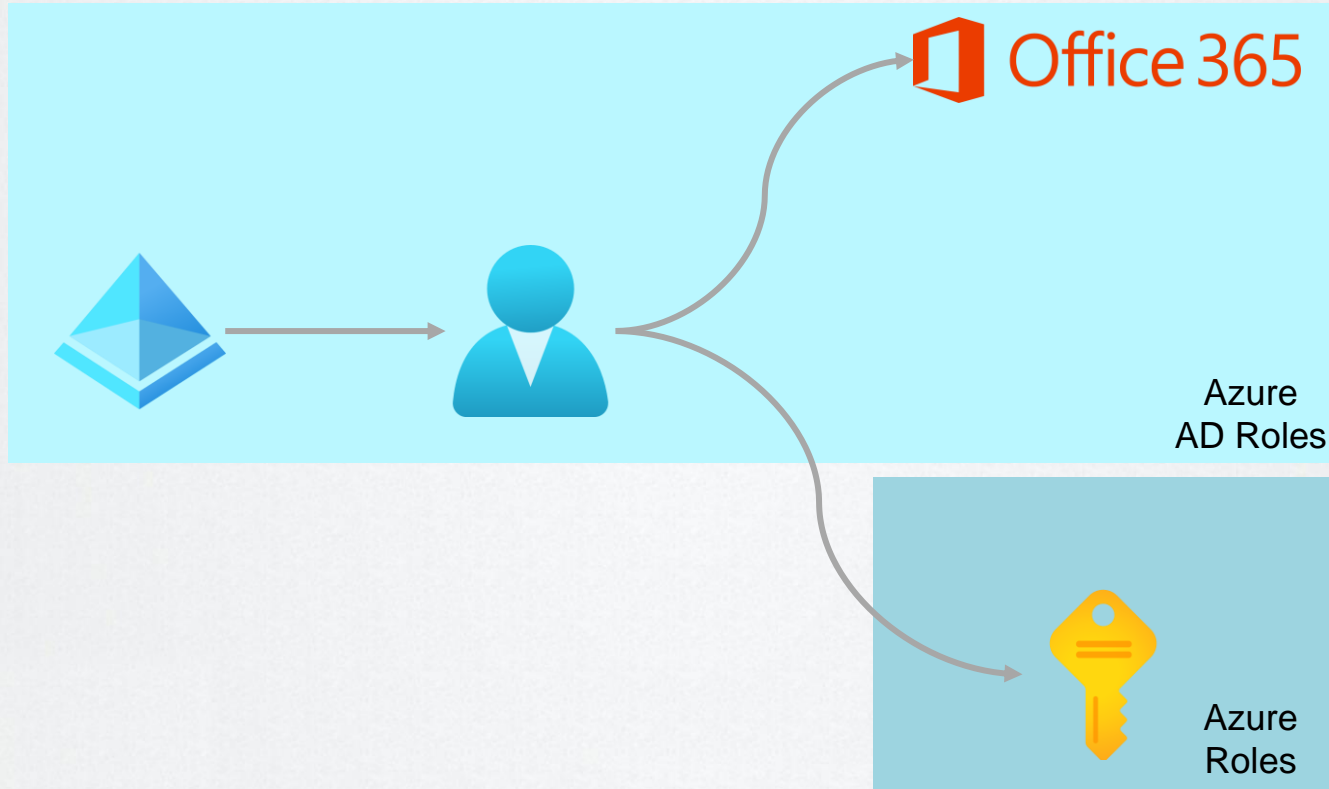
Azure AD Basics



Azure AD Basics



Azure AD Basics





How Roles work ...



Azure - 3 Layers of Access

Tenant



Control Plane



Data Plane



Role Definitions

roleName

name

type

description

actions []

notActions []

dataActions []

notDataActions []

assignableScopes []

Management
Operations
=
Control Plane



Data
Operations
=
Data Plane



Role Definition - Contributor

```
"id": "/providers/Microsoft.Authorization/roleDefinitions/b24988ac-6180-  
"properties": {  
  "roleName": "Contributor",  
  "description": "Grants full access to manage all resources, but does  
  "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": []
```



Let's repeat – Data or Control Plane?!

"Microsoft.Storage/storageAccounts/blobServices/containers/read"

CONTROL PLANE → Actions

"Microsoft.Storage/storageAccounts/blobServices/containers/blobs/read"

DATA PLANE → dataActions

"Microsoft.CognitiveServices/accounts/CustomVoice/evaluations/*"

DATA PLANE → dataActions

"Microsoft.Compute/disks/write"

CONTROL PLANE → Actions

"Microsoft.RecoveryServices/Vaults/backupOperations/read"

CONTROL PLANE → Actions

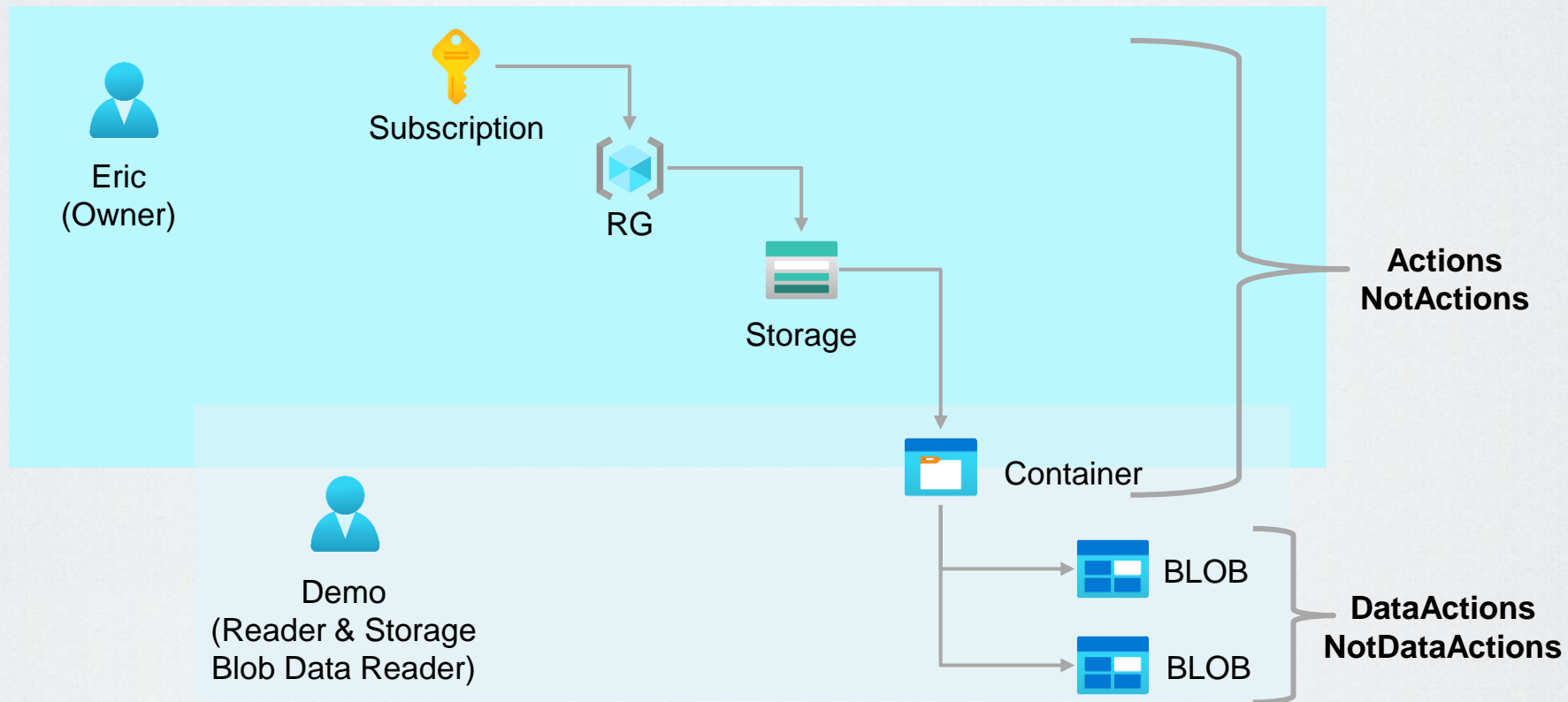




Example – Storage Accounts



Scenario





DEMO



How Roles really work ...



Azure AD Roles, Azure Roles, Classic Roles



Global Admin Role

Global Admins can gain “User Access Admin” role with a click:

Access management for Azure resources


Eric Berg (info@ericberg.de) can manage access to all Azure subscriptions and management groups in this tenant.

[Learn more](#)

Yes

No

Permissions are set at “Root”

<input type="checkbox"/>	Name	Type	Role	Scope
✓	User Access Administrator			
<input type="checkbox"/>	 Eric Berg info@ericberg.de	User	User Access Administrator ⓘ	Root (Inherited)



DEMO

Global Admin Role

“User Access Admin”:

```
"permissions": [  
  {  
    "actions": [  
      "*/read",  
      "Microsoft.Authorization/*",  
      "Microsoft.Support/*"  
    ],  
    "notActions": [],  
    "dataActions": [],  
    "notDataActions": []  
  }  
]
```

Reverse in Portal to “No” or use PS or CLI

Azure AD Roles, Azure Roles, Classic Roles





Roles

Built-In Roles

- General Roles
 - Owner
 - Contributor
 - ...
- Resource specific roles
 - VM Contributor
 - Network Admin
 - Blob Reader

Custom Roles

- Created by Enterprise
- Custom combination of permissions
- Often seen for Network Resource Access, Delegation of Sub-Tasks, etc.
- Require continuous management



Azure AD Roles, Azure Roles, Classic Roles





Classic Admins

Account Administrator (1)

- Subscription creator, billing owner, changes Service Admin

Service Administrator (1)

- Manages Services, can assign Co-Admins, can change Tenant

Co-Administrator (up to 200)

- Can assign Co-Admins, cannot change service admin or tenant

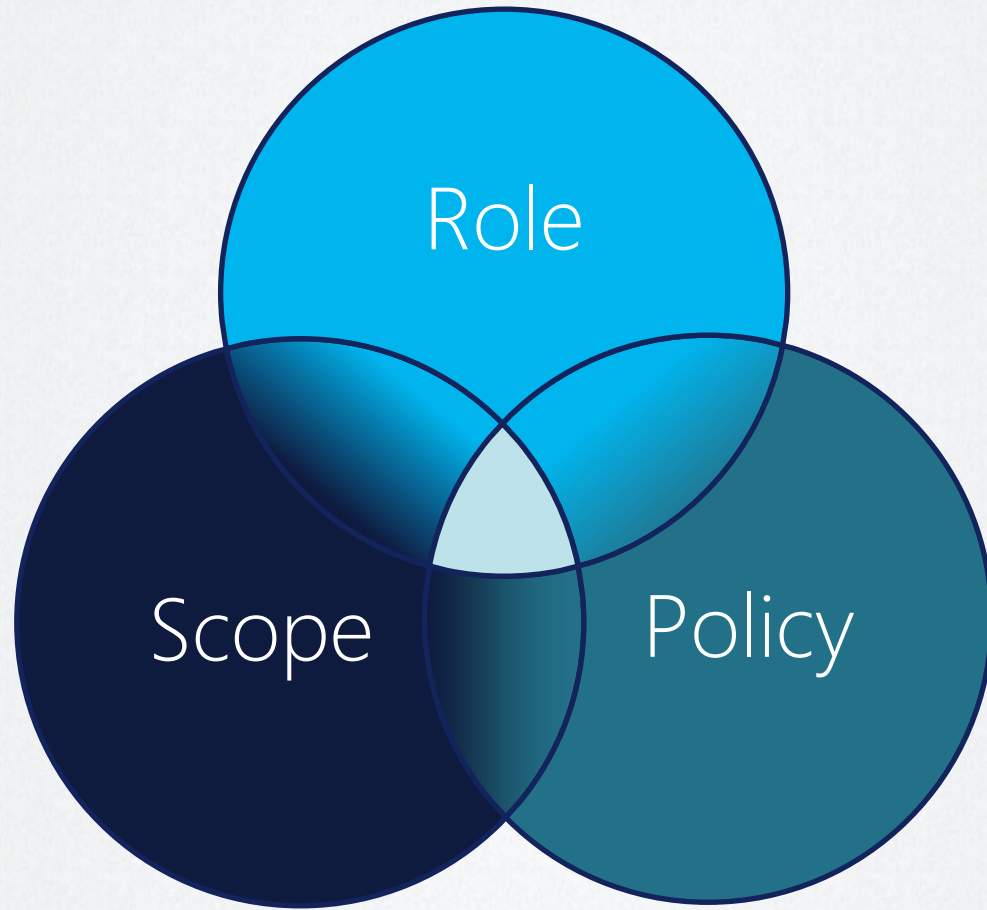
→ Always full access → Move to RBAC → check Accounts

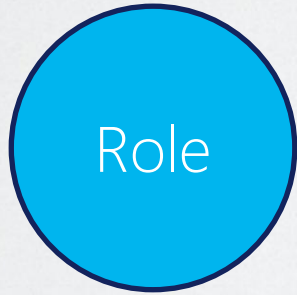




How RBAC works ...







- Collection of permissions
- Built-In Roles
- Custom Roles

VM CONTRIBUTOR



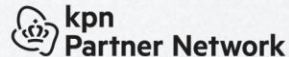
- Set of resources
- Defines range of access
- MG->Sub->RG->Res

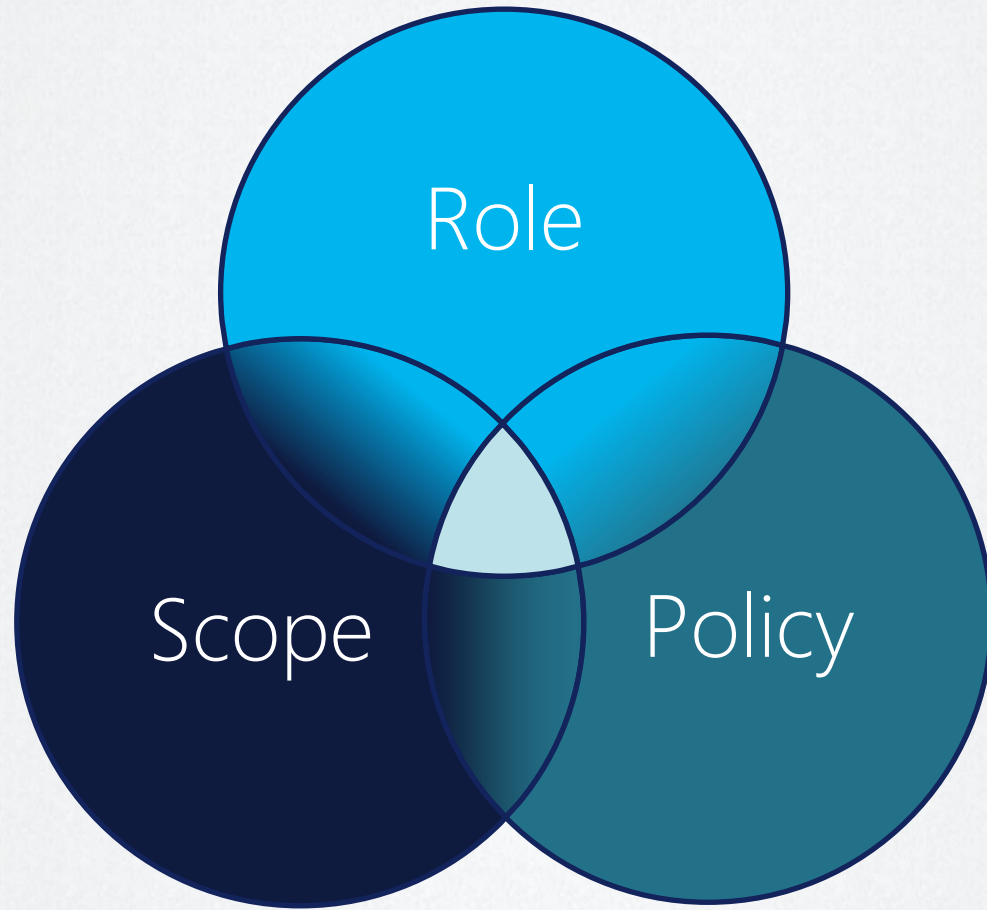
ONLY in RG1



- Works with if-then principle
- Allows refinement of permissions

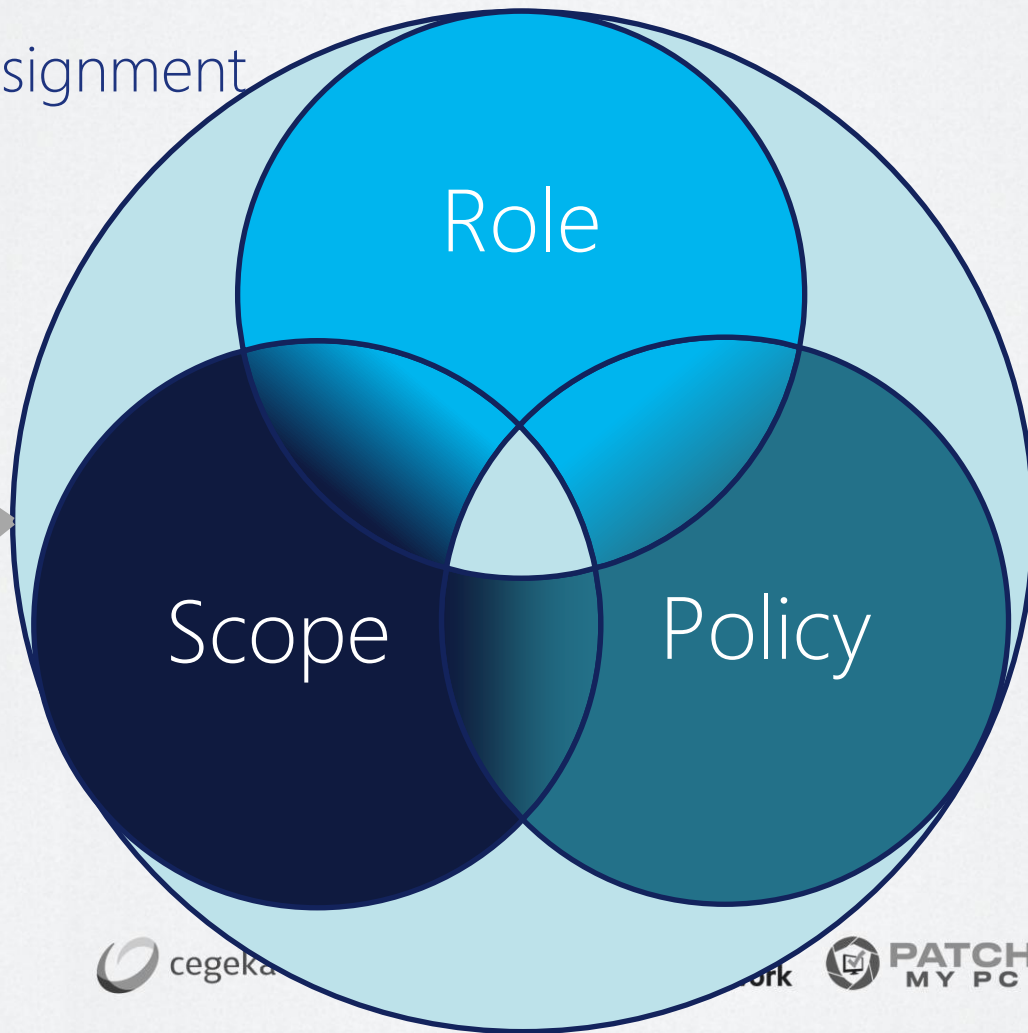
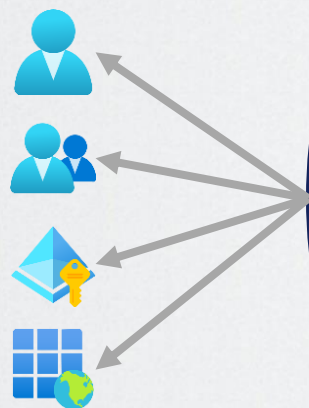
ONLY D-SERIES VMs



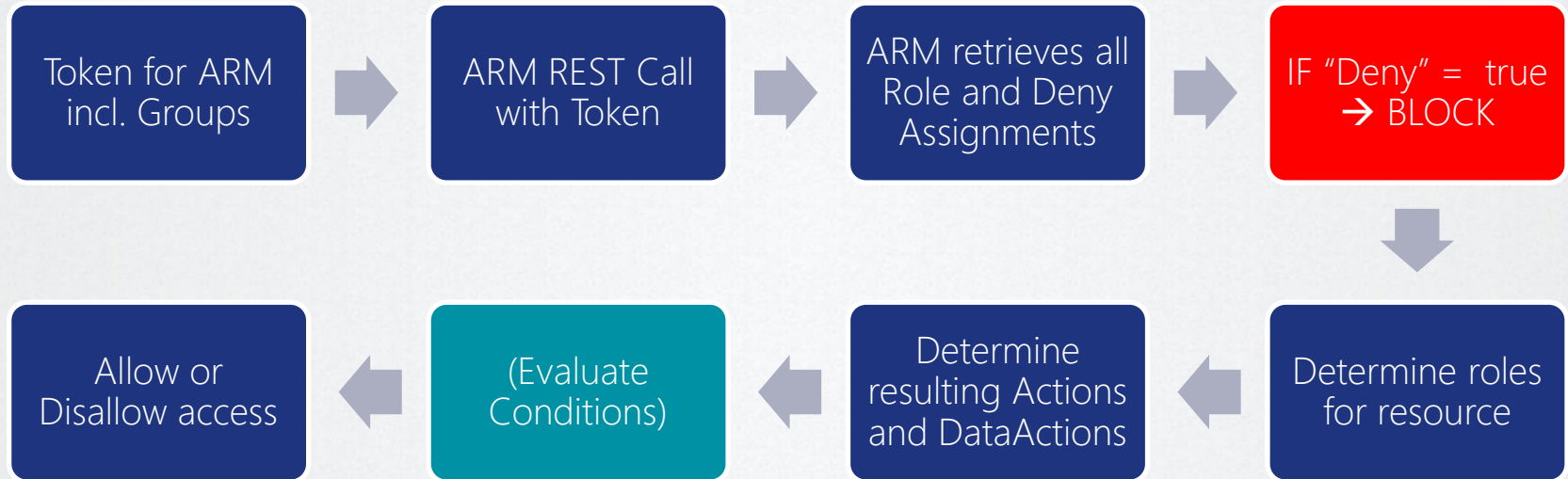


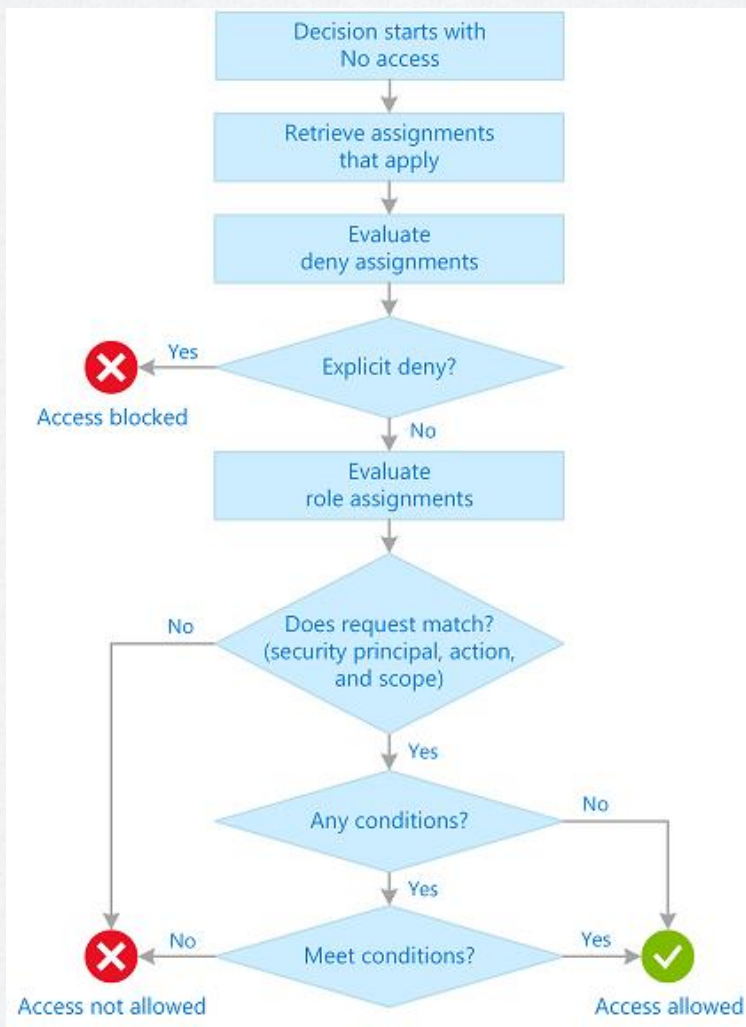


Assignment



RBAC Evaluation







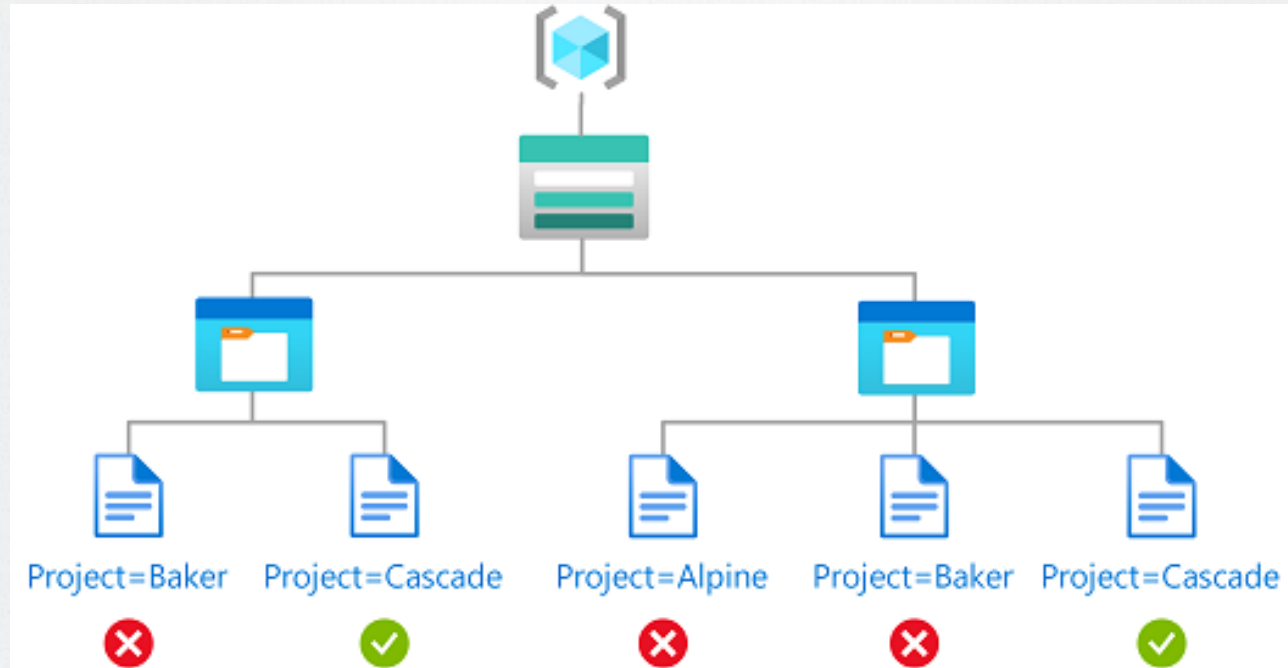
DEMO



How life works ...



RBAC vs. ABAC (preview)



DEMO - Attributes

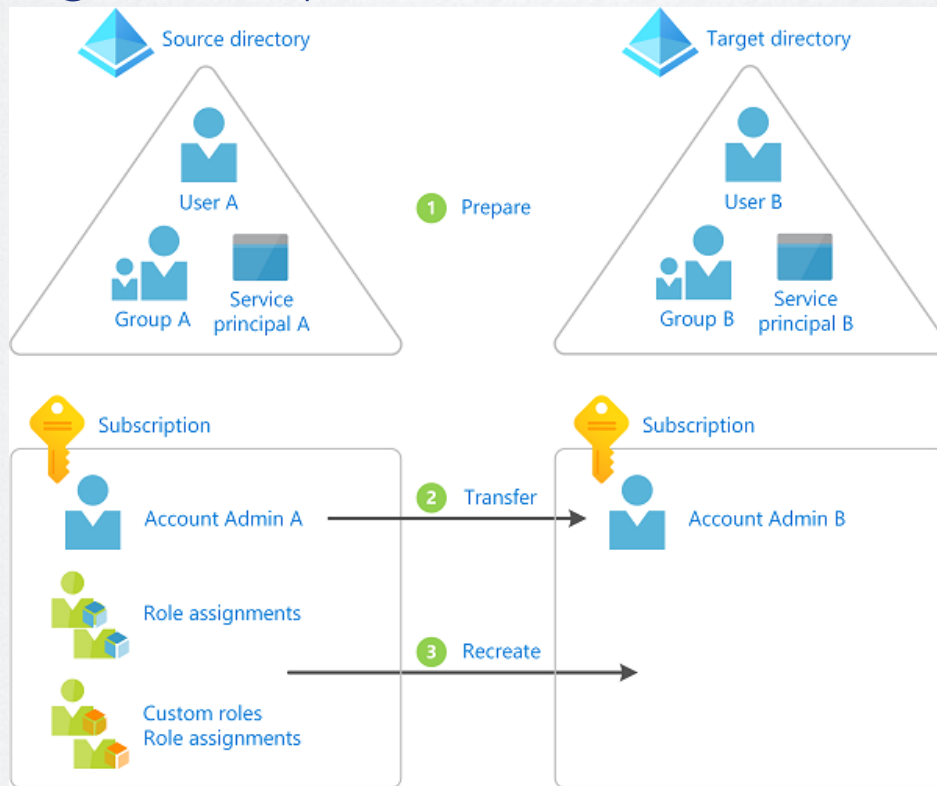




Moving Subscriptions between Tenants

- Only account Admin of new Tenant remains access
- All role assignments are deleted
- All custom roles are deleted
- Huge impacts
 - Managed identities → re-enable and reassign roles
 - KeyVault → update TenantID and recreate access policies
 - Azure SQL DB with AAD Auth → not supported
 - AKS → not supported
 - ...

Moving Subscriptions between Tenants





Best Practices

Follow Least Privilege

Maximum of 3 owners per subscription

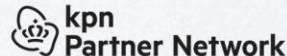
Assign roles to groups, not users

Use Privileged Identity Management (PIM)

Use Role IDs instead of names

Avoid wildcards (*) in custom roles / or avoid custom roles ;-)

Be careful with “Read-Only” ResourceLocks





Next Session: 15:30 - 16:20

Resurrecting Active Directory After a Ransomware Attack





Please give us feedback in
the Yellenge App!!!

Thank you :-)