Manage Azure Subscriptions and RBAC

- Understanding Azure Subscriptions
- Configuring Role Based Access Control
- RBAC using Portal
- RBAC using PowerShell and CLI
- Custom Roles for RBAC

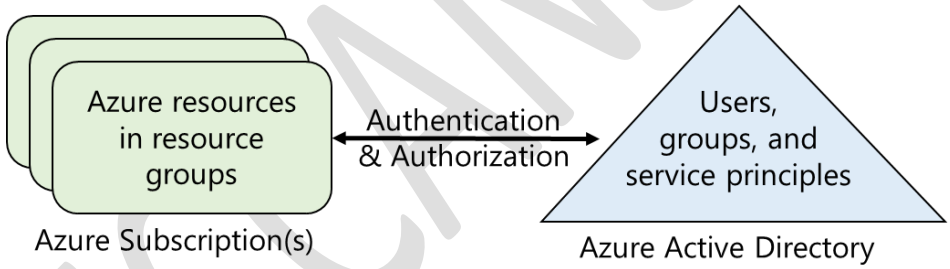
Understanding Azure Subscriptions

An Azure subscription is a logical unit of Azure services that is linked to an Azure account. Billing for Azure services is done on a per-subscription basis.

AZURE ACTIVE DIRECTORY IS NOT A SERVICE IN AZURE SUBSCRIPTION.

ITS USED FOR AUTHENTICATING USERS TO MANAGE RESOURCES IN AZURE SUBSCRIPTION.

ACTIVE DIRECTORY IS INDEPENDENT OF SUBSCRIPTION BUT SUBSCRIPTION MUST AN TRUSTED AZURE AD.



Azure Accounts

- Any user with Microsoft ID (Outlook / Hotmail / MSN / Skype / etc…) can create an Azure Subscription.
- An Azure account determines how Azure usage is reported and who the **Account Administrator** is.
- The person who creates the account, is the Account Administrator for all subscriptions created in that account. That person is also the **default Service Administrator** for the subscription.

Access control in Azure starts from a billing perspective.

- The actual owner of an Azure account is the Account Administrator (AA).
- **Subscriptions are a container for billing**, but they also act as a security boundary.

Deccansoft Software Services H.No: 153, A/4, Balamrai, Rasoolpura, Secunderabad-500003 TELANGANA, NDIA.
http://www.deccansoft.com | http://www.bestdotnettraining.com
Phone: +91 40 2784 1517 OR +91 8008327000 (INDIA)

- **Your Azure subscription has a trust relationship with Azure AD**, which means that it trusts the directory to authenticate users, services, and devices.
- Multiple subscriptions can trust the same directory, but each subscription trusts only one directory.

For a user to access to your Azure resources, you would add them to the Azure AD directory associated with your subscription.

Azure Account Administration = sandeepsonideccansoft.onmicrosoft.com (sandeepsoni@deccansoft.com)

Every Subscription has a trusted Azure AD tenant. Users in Azure AD Tenant are assigned Role either Subscription / RG / Resource.

Hierarchy:

- Subscription -> Resource Group -> Resource

Tenant (Azure AD) -> Domain -> User, Group and Service Principal

- Azure AD Tenant (sandeepsonideccansoft.onmicrosoft.com)
    - Domains
        - sandeepsonideccansoft.onmicrosoft.com (Primary)
        - bestazuretraining.com (verified)
    - Organization Users / **Members** (only verified domains are allowed)
        - abc@sandeepsonideccansoft.onmicrosoft.com
        - xyz@sandeepsonideccansoft.onmicrosoft.com
        - abc@bestazuretraining.com
    - Guest Users (External Azure AD Account & Microsoft Account)
        - abc@hotmail.com
        - zyx@microsoft.com
        - test@contoso.com
- Azure Subscription is binding to an Azure AD.
    - FREE Trail
    - Pay-As-You-Go
    - Pay-As-You-Go (Dev/Test)
    - Enterprise Aggrement

Deccansoft Software Services H.No: 153, A/4, Balamrai, Rasoolpura, Secunderabad-500003 TELANGANA, NDIA.
http://www.deccansoft.com | http://www.bestdotnettraining.com
Phone: +91 40 2784 1517 OR +91 8008327000 (INDIA)

  - Enterprise Aggrement (Dev/Test)
  - Visual Studio Subscription
  - Azure Sponsorship
  - Azure Pass Sponsorship
- Permissions to AD Users
  - Permission Scopes (Users can be given access to)
    - Management Group
    - Subscription
    - ResourceGroup
    - Resource

Azure AD Roles

Global Administrator (Azure AD Role)

- Manage access to all administrative features in Azure Active Directory, as well as services that federate to Azure Active Directory.
- Assign administrator roles to others.
- Reset the password for any user and all other administrators.

User Administrator (Azure AD Role)

- Create and manage all aspects of users and groups.
- Manage support tickets.
- Monitor service health.
- Change passwords for users, Helpdesk administrators, and other User Administrators.

Billing Administrator (Azure AD Role)

- Manage subscriptions
- Manage support tickets
- Monitors service health

Many more…

Resource Group and Management Group

About Resource Group:

- A resource groups is a fundamental concept of the Azure platform.
  - Serves as a logical grouping of resources

Deccansoft Software Services H.No: 153, A/4, Balamrai, Rasoolpura, Secunderabad-500003 TELANGANA, NDIA.
http://www.deccansoft.com | http://www.bestdotnettraining.com

Phone: +91 40 2784 1517 OR +91 8008327000 (INDIA)

  - Ties to resource life cycle
  - Can't be nested
- Each resource must belong to a resource group.
- Most resources can be moved between resource groups.
- Organization of Resource Group
  - Organizing for authorization
  - Organizing for life cycle
  - Organizing for billing

Using Resource Mover, you can currently move the following resources across regions:

- Azure VMs and associated disks
- NICs
- Availability sets
- Azure virtual networks
- Public IP addresses
- Network security groups (NSGs)
- Internal and public load balancers
- Azure SQL databases and elastic pools

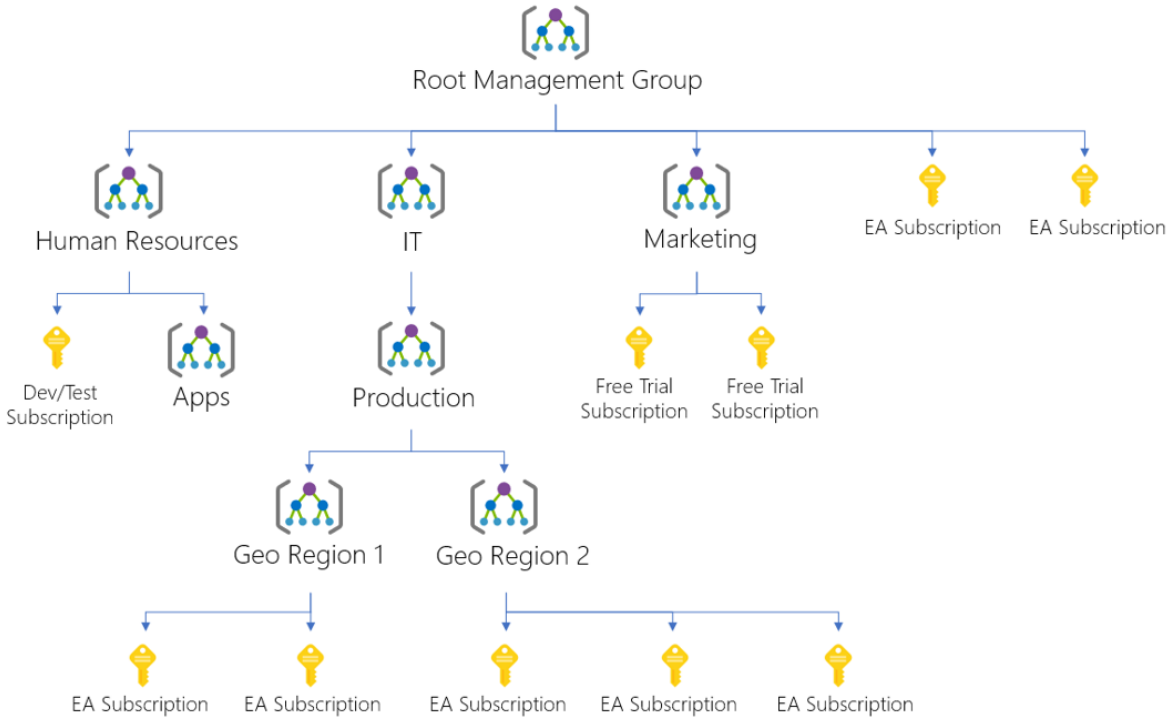
About Management Group

- Provides a level of scope above subscriptions.
- Targeting of policies and spend budgets across subscriptions and inheritance down the hierarchies.
- Compliance and cost reporting by organization (business/teams).

Deccansoft Software Services H.No: 153, A/4, Balamrai, Rasoolpura, Secunderabad-500003 TELANGANA, NDIA.
http://www.deccansoft.com | http://www.bestdotnettraining.com

Phone: +91 40 2784 1517 OR +91 8008327000 (INDIA)

- We can have upto 6 levels of management group.

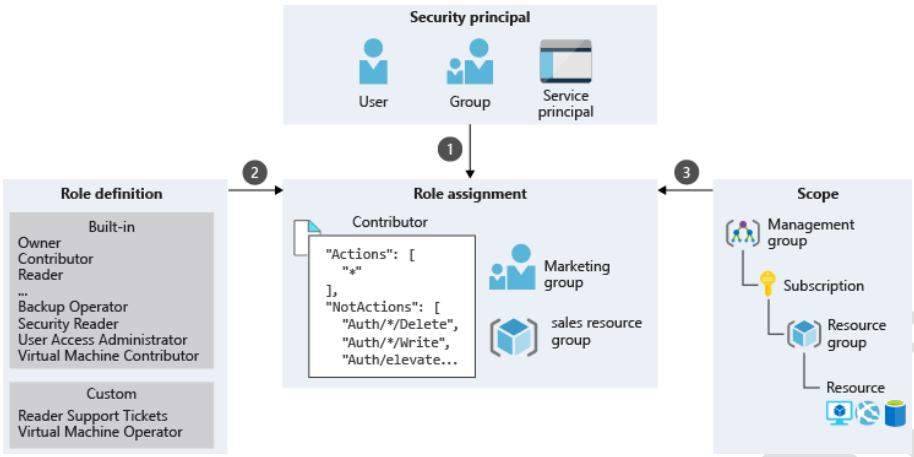


Configuring Role Based Access Control (RBAC)

- Managing access to resources in Azure is a critical part of an organization's security and compliance requirements. Role-based access control (RBAC) is the capability for you to grant appropriate access to Azure AD users, groups, and services.
- RBAC is configured by selecting a role (the definition of what actions are allowed and/or denied), then associating the role with a user, group or service principal.
- **Finally, this combination of role and user/group/service principal is scoped to either the entire subscription, a resource group, or specific resources within a resource group.**

Role Assignment:

Deccansoft Software Services H.No: 153, A/4, Balamrai, Rasoolpura, Secunderabad-500003 TELANGANA, NDIA.
http://www.deccansoft.com | http://www.bestdotnettraining.com
Phone: +91 40 2784 1517 OR +91 8008327000 (INDIA)



Role Definition (What you can do):

Each role is a set of properties defined in a **JSON** file. This role definition includes **Name**, **Id**, and **Description**. It also includes the allowable permissions (**Actions**), denied permissions (**NotActions**), and **scope** (read access, etc.) for the role.

Name: Owner

ID: 8e3af657-a8ff-443c-a75c-2fe8c4bcb65

IsCustom: False

Description: Manage everything, including access to resources

Actions: {*}

NotActions: {}

AssignableScopes: {/}

In this example the Owner role means all (*) actions, no denied actions, and all (/) scopes.

Actions:

It specifies the Azure operations to which the role grants access. It is a collection of operation strings that identify securable operations of Azure resource providers.

Operation strings follow the format of **Microsoft.<ProviderName>/<ChildResourceType>/<action>**.

Examples:

- */read grants access to read operations for all resource types of all Azure resource providers.

Deccansoft Software Services H.No: 153, A/4, Balamrai, Rasoolpura, Secunderabad-500003 TELANGANA, NDIA.
http://www.deccansoft.com | http://www.bestdotnettraining.com
Phone: +91 40 2784 1517 OR +91 8008327000 (INDIA)

- `Microsoft.Compute/*` grants access to all operations for all resource types in the Microsoft.Compute resource provider.
- `Microsoft.Network/*/read` grants access to read operations for all resource types in the Microsoft.Network resource provider of Azure.
- `Microsoft.Compute/virtualMachines/*` grants access to all operations of virtual machines and its child resource types.
- `Microsoft.Web/sites/restart` grants access to restart websites.

NotActions:

Use the **NotActions** property if the set of operations that you wish to allow is more easily defined by **excluding restricted operations**. The access granted by a custom role is computed by subtracting the **NotActions** operations from the **Actions** operations.

AssignableScopes:

This property of the role specifies the scopes (subscriptions, resource groups, or resources) within which the custom role is available for assignment.

- /
- /subscriptions/[subscription id]
- /subscriptions/[subscription id]/resourceGroups/[resource group name]
- **/subscriptions/[subscription id]/resourceGroups/[resource group name]/[resource]**

Example 1: Make a role available for assignment in **two** subscriptions.

```
"/subscriptions/c276fc76-9cd4-44c9-99a7-4fd71546436e", "/subscriptions/e91d47c4-76f3-4271-a796-21b4ecfe3624"
```

Example 2: Makes a role available for assignment only in the Network resource group.

```
"/subscriptions/c276fc76-9cd4-44c9-99a7-4fd71546436e/resourceGroups/NetworkRG"
```

Built-in Roles and their Action and NotActions

Role	Action	NotActions	Description

Deccansoft Software Services H.No: 153, A/4, Balamrai, Rasoolpura, Secunderabad-500003 TELANGANA, NDIA.
http://www.deccansoft.com | http://www.bestdotnettraining.com
Phone: +91 40 2784 1517 OR +91 8008327000 (INDIA)

Owner	*	-	This role has full access to all the resources and can **delegate** access to others.
Contributor	*	Microsoft.Authorization/*/Delete, Microsoft.Authorization/*/Write,	This role can **create and manage** all types of resources, but **can't grant access** to other users and groups.
Reader	*/read		This role can **view** existing Azure resources

Walkthrough: To manage RBAC by using the Azure portal, perform the following steps:

1. In the Azure portal, locate the Users blade for the resource for which you plan to manage RBAC.
   Eg: App Services → Select the App → Settings → **Access Control (IAM)**.
   OR
   Azure Portal → Subscriptions → Select **Subscription** → Settings → **Access Control (IAM)**.
2. Click the Add icon on the Users blade.
   a. Select the role that you want to assign. Eg: **Reader** / Contributor / Owner
   b. Search for and select the user, group, or application to which you want to grant access. You can search the directory for users, groups, and applications by using display names, email addresses, and object identifiers. (User should have been created using Classic Portal in the Azure AD Directory)
   c. Click OK to confirm the selection.
3. In new instance of the browser, Login using the identity of the user who has been given permissions and verify (that the user is added as a reader to your Azure subscription)

On a given Subscription/ResourceGroup/Resource a User/Group/ServicePrincipal is assigned role which be either Owner/Contributor/Reader/... so that based on permissions in that role, operations can be performed.

RBAC supports *deny assignments*:

- Attaches a set of deny actions to a user, group, service principal, or managed identity at a particular scope for the purpose of denying access.
- Deny assignments block users from performing specified actions even if a role assignment grants them access.
- Deny assignments take precedence over role assignments.
- At this time, the only way you can add your own deny assignments is by using **Azure Blueprints**.

Custom Roles for RBAC

Create custom roles for Azure Role-Based Access Control

The following template shows a custom role for **monitoring and restarting virtual machines**:

d:\VMOperator.json

```
{
 "Name": "Virtual Machine Operator",
 "Id": "97e15602-5e9d-4f79-b737-ae959719b65d",
 "IsCustom": true,
 "Description": "Can monitor and restart virtual machines.",
 "Actions": [
  "Microsoft.Storage/*/read",
  "Microsoft.Network/*/read",
  "Microsoft.Compute/*/read",
  "Microsoft.Compute/virtualMachines/start/action",
  "Microsoft.Compute/virtualMachines/restart/action",
  "Microsoft.Authorization/*/read",
  "Microsoft.Resources/subscriptions/resourceGroups/read",
  "Microsoft.Insights/alertRules/*",
  "Microsoft.Insights/diagnosticSettings/*",
  "Microsoft.Support/*"
 ],
 "NotActions": [
 ],
 "AssignableScopes": [
  "/subscriptions/c276fc76-9cd4-44c9-99a7-4fd71546436e",
 ]
}
```

Then you use the New-AzRoleDefinition or az role definition create commands to create the custom role.

```
New-AzRoleDefinition -InputFile VMOperator.json
```

Service Principal

Create an Azure Active Directory application

Deccansoft Software Services H.No: 153, A/4, Balamrai, Rasoolpura, Secunderabad-500003 TELANGANA, NDIA.
http://www.deccansoft.com | http://www.bestdotnettraining.com

Phone: +91 40 2784 1517 OR +91 8008327000 (INDIA)

1. Azure Portal → Azure Active Directory → App registrations → New application registration
2. Provide a name and URL for the application. Select **Web app / API** for the type of application you want to create. **You cannot create credentials for a Native application; therefore, that type does not work for an automated application**.
3. Get application ID and authentication key
4. Get tenant id: Azure AD → Properties → Directory ID

Assign Application to role (for a given subscription)

- To access resources in your subscription, you must assign the application to a role.
- You can set the scope at the level of the subscription, resource group, or resource. Permissions are inherited to lower levels of scope. For example, adding an application to the Reader role for a resource group means it can read the resource group and any resources it contains.

1. More Services → Subscription → Select the Subscription → Access Control (IAM)
2. Select + Add → Role = Reader, Select = **<The application created above>** → Save

Deccansoft Software Services H.No: 153, A/4, Balamrai, Rasoolpura, Secunderabad-500003 TELANGANA, NDIA.
http://www.deccansoft.com | http://www.bestdotnettraining.com

Phone: +91 40 2784 1517 OR +91 8008327000 (INDIA)