Contents

[Azure management groups 1](#_Toc49818263)

[Important facts about management groups 1](#_Toc49818264)

[Root management group for each directory 2](#_Toc49818265)

[Important facts about the Root management group 2](#_Toc49818266)

[Management group access 3](#_Toc49818267)

[Issues with breaking the role definition and assignment hierarchy path 3](#_Toc49818268)

[Resource groups 5](#_Toc49818269)

[Azure Resource Manager 5](#_Toc49818270)

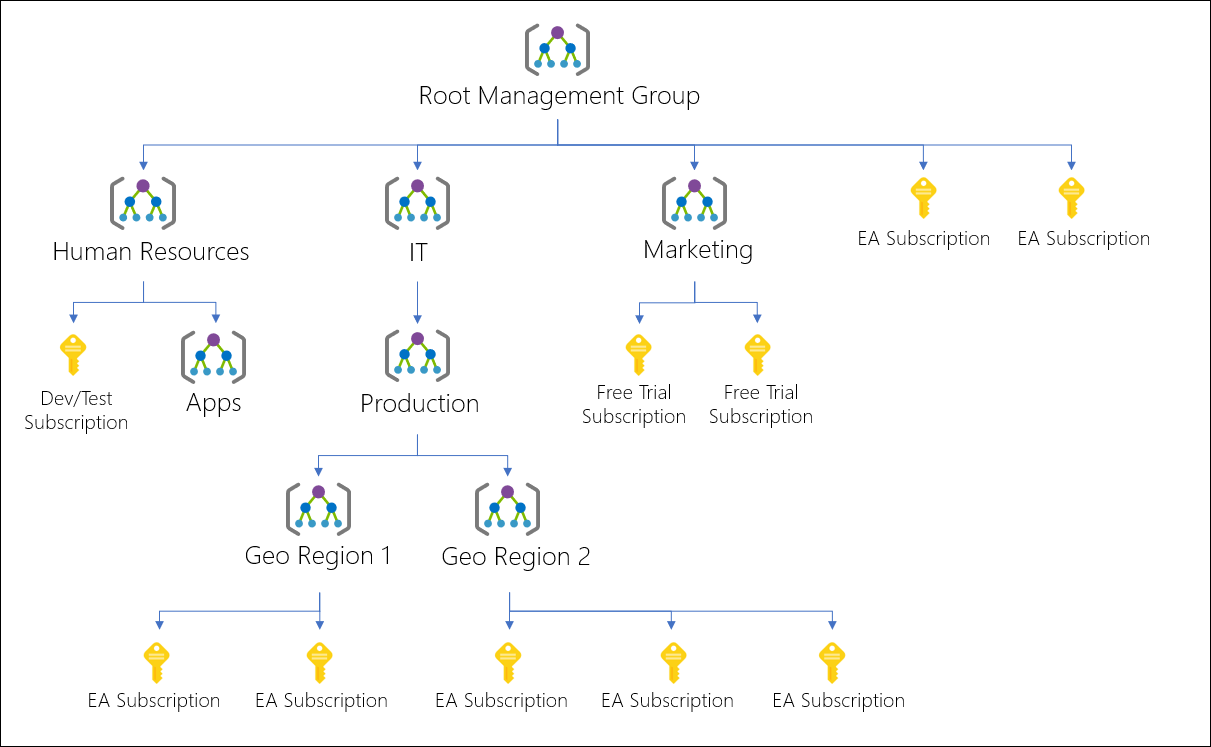
[Terminology 6](#_Toc49818271)

[Understand scope 7](#_Toc49818272)

# Azure management groups

## Important facts about management groups

* 10,000 management groups can be supported in a single directory.
* A management group tree can support up to six levels of depth.
  + This limit doesn't include the Root level or the subscription level.
* Each management group and subscription can only support one parent.
* Each management group can have many children.
* All subscriptions and management groups are within a single hierarchy in each directory.



## Root management group for each directory

Each directory is given a single top-level management group called the "Root" management group. This root management group is built into the hierarchy to have all management groups and subscriptions fold up to it. This root management group allows for global policies and Azure role assignments to be applied at the directory level.

### Important facts about the Root management group

* By default, the root management group's display name is **Tenant root group**. The ID is the Azure Active Directory ID.
* To change the display name, your account must be assigned the Owner or Contributor role on the root management group. See [Change the name of a management group](https://docs.microsoft.com/en-us/azure/governance/management-groups/manage#change-the-name-of-a-management-group) to update the name of a management group.
* **The root management group can't be moved or deleted, unlike other management groups**.
* **All subscriptions and management groups fold up to the one root management group** within the directory.
  + All resources in the directory fold up to the root management group for global management.
  + New subscriptions are automatically defaulted to the root management group when created.
* **All Azure customers can see the root management group**, but not all customers have access to manage that root management group.
  + Everyone who has access to a subscription can see the context of where that subscription is in the hierarchy.
  + No one is given default access to the root management group. Azure AD Global Administrators are the only users that can elevate themselves to gain access. Once they have access to the root management group, the global administrators can assign any Azure role to other users to manage  
    it.
* In SDK, the root management group, or 'Tenant Root', operates as a management group.

<https://www.youtube.com/watch?v=jOprhCxnEAg>

## Management group access

Azure management groups support [Azure role-based access control (Azure RBAC)](https://docs.microsoft.com/en-us/azure/role-based-access-control/overview) for all resource accesses and role definitions. These permissions are inherited to child resources that exist in the hierarchy. Any Azure role can be assigned to a management group that will inherit down the hierarchy to the resources.

The following chart shows the list of roles and the supported actions on management groups.

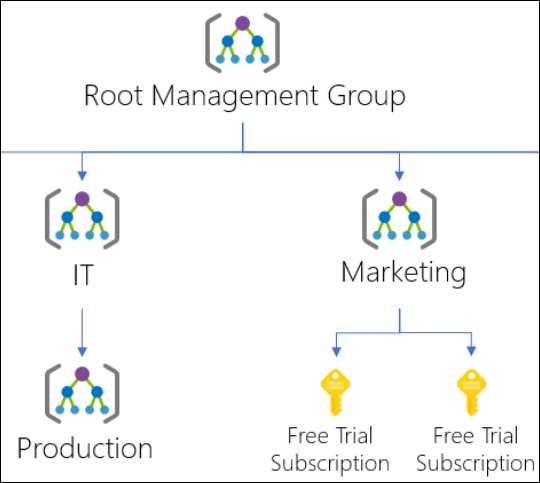
| Management group access | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Azure Role Name** | **Create** | **Rename** | **Move\*\*** | **Delete** | **Assign Access** | **Assign Policy** | **Read** |
| Owner | X | X | X | X | X | X | X |
| Contributor | X | X | X | X |  |  | X |
| MG Contributor\* | X | X | X | X |  |  | X |
| Reader |  |  |  |  |  |  | X |
| MG Reader\* |  |  |  |  |  |  | X |
| Resource Policy Contributor |  |  |  |  |  | X |  |
| User Access Administrator |  |  |  |  | X | X |  |

\*: MG Contributor and MG Reader only allow users to do those actions on the management group scope.  
\*\*: Role Assignments on the Root management group aren't required to move a subscription or management group to and from it. See [Manage your resources with management groups](https://docs.microsoft.com/en-us/azure/governance/management-groups/manage) for details on moving items within the hierarchy.

### Issues with breaking the role definition and assignment hierarchy path

Role definitions are assignable scope anywhere within the management group hierarchy. A role definition can be defined on a parent management group while the actual role assignment exists on the child subscription. Since there's a relationship between the two items, you'll receive an error when trying to separate the assignment from its definition.

For example, let's look at a small section of a hierarchy for a visual.



Let's say there's a custom role defined on the Marketing management group. That custom role is then assigned on the two free trial subscriptions.

If we try to move one of those subscriptions to be a child of the Production management group, this move would break the path from subscription role assignment to the Marketing management group role definition. In this scenario, you'll receive an error saying the move isn't allowed since it will break this relationship.

There are a couple different options to fix this scenario:

* Remove the role assignment from the subscription before moving the subscription to a new parent MG.
* Add the subscription to the Role Definition's assignable scope.
* Change the assignable scope within the role definition. In the above example, you can update the assignable scopes from Marketing to Root Management Group so that the definition can be reached by both branches of the hierarchy.
* Create an additional Custom Role that will be defined in the other branch. This new role will require the role assignment to be changed on the subscription also.

**Task :**

<https://docs.microsoft.com/en-us/azure/governance/management-groups/overview#moving-management-groups-and-subscriptions>

# Resource groups

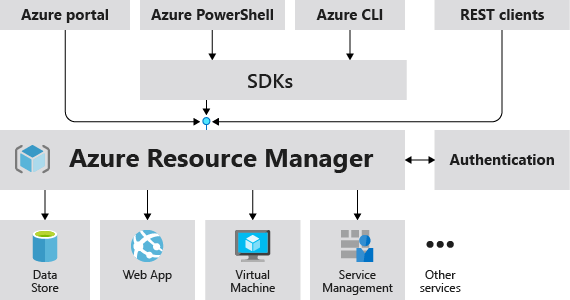
There are some important factors to consider when defining your resource group:

* All the resources in your group should share the same lifecycle. You deploy, update, and delete them together. If one resource, such as a server, needs to exist on a different deployment cycle it should be in another resource group.
* Each resource can only exist in one resource group.
* Some resources can exist outside of a resource group. These resources are deployed to the [subscription](https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/deploy-to-subscription), [management group](https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/deploy-to-management-group), or [tenant](https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/deploy-to-tenant). Only specific resource types are supported at these scopes.
* You can add or remove a resource to a resource group at any time.
* You can move a resource from one resource group to another group. For more information, see [Move resources to new resource group or subscription](https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/move-resource-group-and-subscription).
* A resource group can contain resources that are located in different regions.
* A resource group can be used to scope access control for administrative actions.
* A resource can interact with resources in other resource groups. This interaction is common when the two resources are related but don't share the same lifecycle (for example, web apps connecting to a database).

# Azure Resource Manager

Azure Resource Manager is the deployment and management service for Azure. It provides a management layer that enables you to create, update, and delete resources in your Azure account.

When a user sends a request from any of the Azure tools, APIs, or SDKs, Resource Manager receives the request. It authenticates and authorizes the request. Resource Manager sends the request to the Azure service, which takes the requested action. Because all requests are handled through the same API, you see consistent results and capabilities in all the different tools.



## Terminology

**resource** - A manageable item that is available through Azure. Virtual machines, storage accounts, web apps, databases, and virtual networks are examples of resources. Resource groups, subscriptions, management groups, and tags are also examples of resources.

**resource group** - A container that holds related resources for an Azure solution. The resource group includes those resources that you want to manage as a group. You decide which resources belong in a resource group based on what makes the most sense for your organization.

**resource provider** - A service that supplies Azure resources. For example, a common resource provider is **Microsoft.Compute**, which supplies the virtual machine resource. **Microsoft.Storage** is another common resource provider. See [Resource providers and types](https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/resource-providers-and-types).

**Resource Manager template** - A JavaScript Object Notation (JSON) file that defines one or more resources to deploy to a resource group, subscription, management group, or tenant.

**declarative syntax** - Syntax that lets you state "Here is what I intend to create" without having to write the sequence of programming commands to create it. The Resource Manager template is an example of declarative syntax.

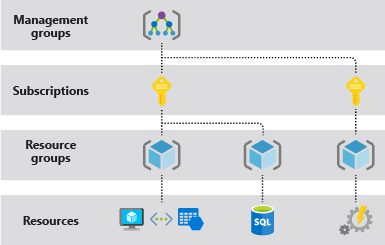
**tenant** - A Tenant, as it relates to Azure, refers to a single instance of [Azure Active Directory](https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis), or, as it is often called “Azure AD”. Azure AD is a key piece of Microsoft’s cloud platform as it provides a single place to manage users, groups and the permissions they hold in relation to applications published in Azure AD.

Azure AD Tenants are globally unique and are scoped using a domain that ends with ‘onmicrosoft.com’ (i.e. myazuread.onmicrosoft.com) and each has a ‘Tenant ID’ in the form of an [UUID/GUID](https://en.wikipedia.org/wiki/Universally_unique_identifier). Some customers choose to connect their internal Active Directory environment to Azure AD to allow single or same sign-on for their staff and will also use a custom domain instead of the default ‘onmicrosoft.com’.

Finally, **Azure AD Tenants can be associated with multiple Subscriptions (typically in larger organisations), but a Subscription can only ever be associated with a single Azure AD Tenant at any time.**

## Understand scope

Azure provides four levels of scope: [management groups](https://docs.microsoft.com/en-us/azure/governance/management-groups/overview), subscriptions, [resource groups](https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/overview#resource-groups), and resources. The following image shows an example of these layers.



You apply management settings at any of these levels of scope. The level you select determines how widely the setting is applied. Lower levels inherit settings from higher levels. For example, when you apply a [policy](https://docs.microsoft.com/en-us/azure/governance/policy/overview) to the subscription, the policy is applied to all resource groups and resources in your subscription.