✓ 100 XP

Create management groups

3 minutes

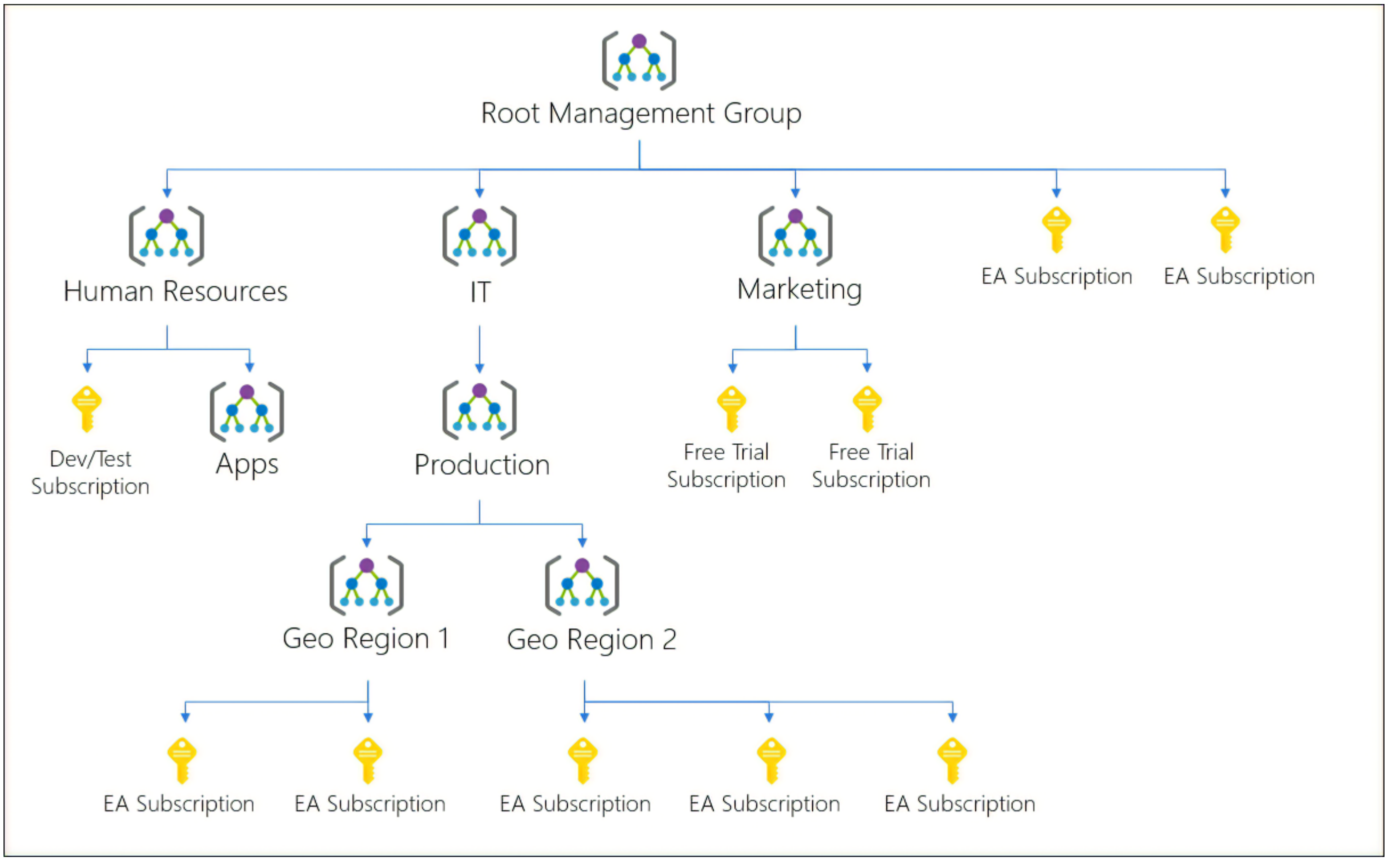
Organizations that use multiple subscriptions need a way to efficiently manage access, policies, and compliance. Azure management groups provide a level of scope and control above your subscriptions. You can use management groups as containers to manage access, policy, and compliance across your subscriptions.

Things to know about management groups

Consider the following characteristics of Azure management groups:

- By default, all new subscriptions are placed under the top-level management group, or *root group*.
- All subscriptions within a management group automatically inherit the conditions applied to that management group.
- A management group tree can support up to six levels of depth.
- Azure role-based access control authorization for management group operations isn't enabled by default.

The following diagram shows how Azure management groups can be used to organize subscriptions in a hierarchy of unified policy and access management. In this scenario, the organization has a single top-level management group. Every directory under the root group is folded into the top-level group.



Things to consider when using management groups

Review the following ways you can use management groups in Azure Policy to manage your subscriptions:

- **Consider custom hierarchies and groups**. Align your Azure subscriptions by using custom hierarchies and grouping that meet your company's organizational structure and business scenarios. You can use management groups to target policies and spending budgets across subscriptions.

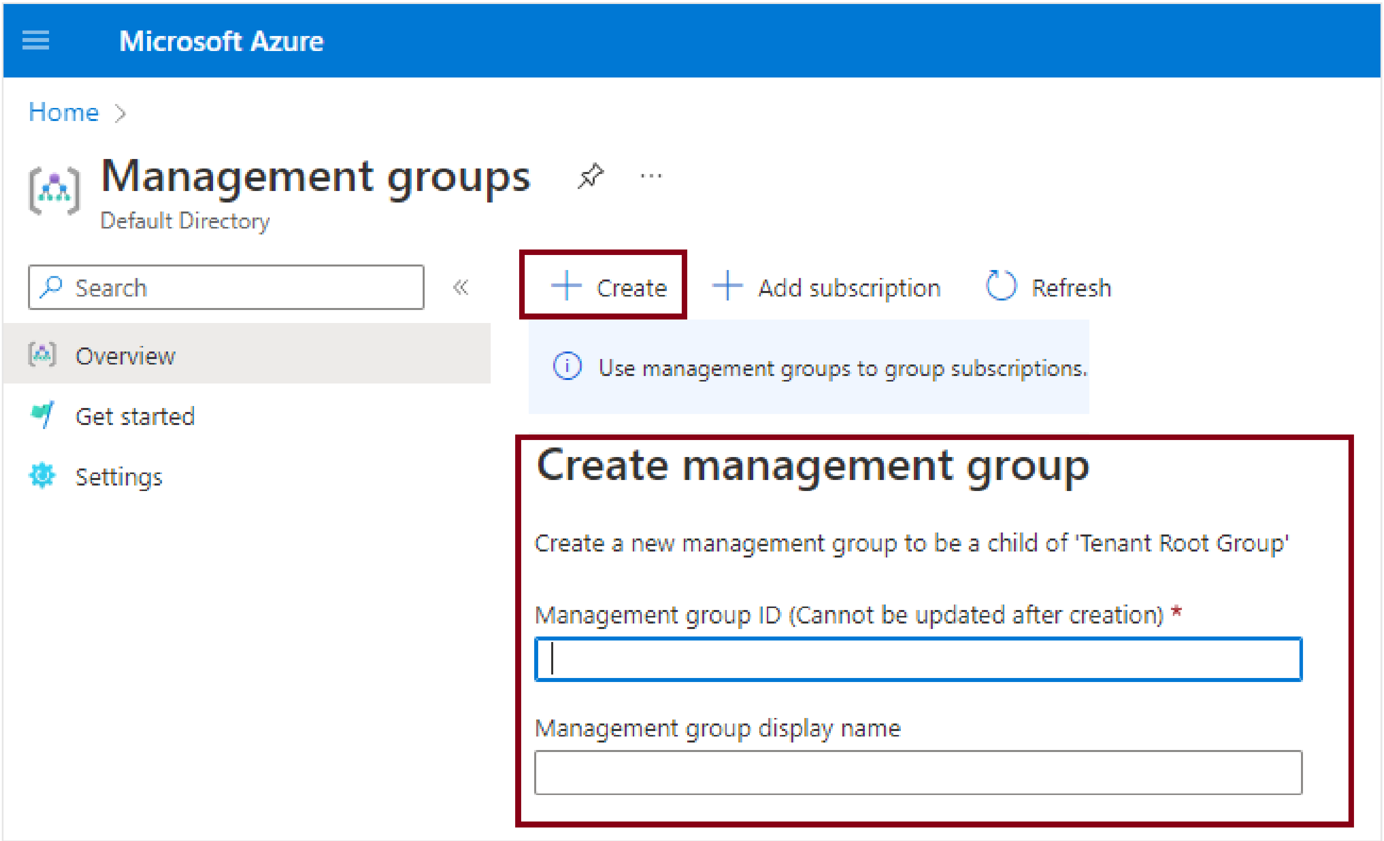
- **Consider policy inheritance**. Control the hierarchical inheritance of access and privileges in policy definitions. All subscriptions within a management group inherit the conditions applied to the management group. You can apply policies to a management group to limit the regions available for creating virtual machines (VMs). The policy can be applied to all management groups, subscriptions, and resources under the initial management group, to ensure VMs are created only in the specified regions.

- **Consider compliance rules**. Organize your subscriptions into management groups to help meet compliance rules for individual departments and teams.

- **Consider cost reporting**. Use management groups to do cost reporting by department or for specific business scenarios. You can use management groups to report on budget details across subscriptions.

Create management groups

You can create a management group with Azure Policy by using the Azure portal, PowerShell, or the Azure CLI. Here's an example of what you see in the Azure portal:



Use management groups to group subscriptions.

Create management group

Create a new management group to be a child of 'Tenant Root Group'

Management group ID (Cannot be updated after creation) *

Management group display name

A management group has a directory unique identifier (ID) and a display name. The ID is used to submit commands on the management group. The ID value can't be changed after it's created because it's used throughout the Azure system to identify the management group. The display name for the management group is optional and can be changed at any time.

Next unit: Implement Azure policies

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆