**Introduction**

Completed100 XP

* 1 minute

[Azure Policy](https://azure.microsoft.com/services/azure-policy/) is a service in Azure that enables you to create, assign, and manage policies to control or audit your resources. These policies enforce different rules over your resource configurations so the configurations stay compliant with corporate standards. You apply the policies to your resources by using management groups.

In this module, your business is subject to many regulations and compliance rules. Your company wants to ensure each department implements and deploys resources correctly. You're responsible for investigating how to use Azure Policy and management groups to implement compliance measures.

**Learning objectives**

In this module, you learn how to:

* Create management groups to target policies and spending budgets.
* Implement Azure Policy with policy and initiative definitions.
* Scope Azure policies and determine compliance.

**Skills measured**

The content in the module helps you prepare for [Exam AZ-104: Microsoft Azure Administrator](https://learn.microsoft.com/en-us/certifications/exams/az-104). The module concepts are covered in:

Manage identities and governance in Azure (15-20%)

* Manage subscriptions and governance
  + Configure Azure policies
  + Configure management groups

**Prerequisites**

None.

**Next unit: Create management groups**

# Create management groups

Completed100 XP

* 3 minutes

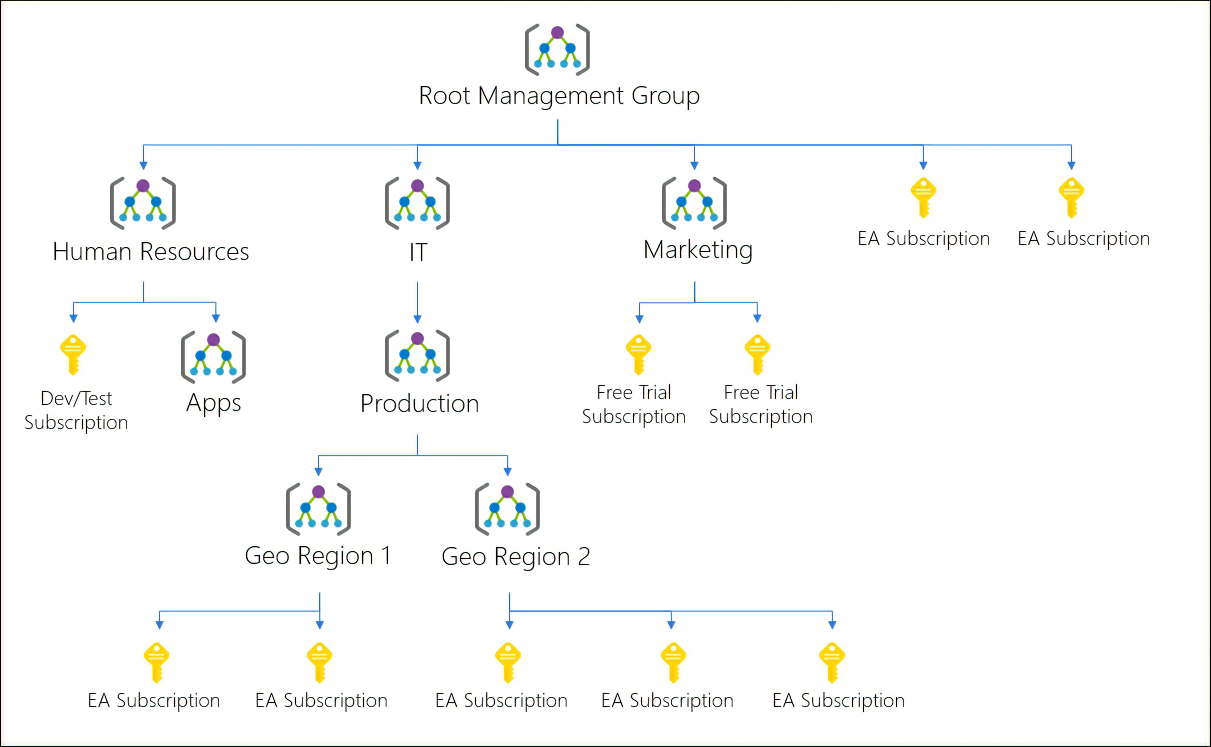
Organizations that use multiple subscriptions need a way to efficiently manage access, policies, and compliance. [Azure management groups](https://learn.microsoft.com/en-us/azure/governance/management-groups/overview) provide a level of scope and control above your subscriptions. You can use management 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.



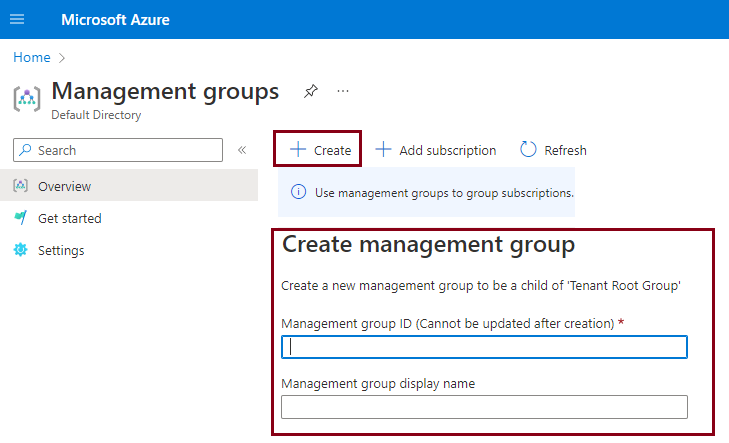
### Things to consider when using management groups

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:



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

# Implement Azure policies

Completed100 XP

* 2 minutes

Azure Policy is a service in Azure that you can use to create, assign, and manage policies. You can use policies to enforce rules on your resources to meet corporate compliance standards and service level agreements. Azure Policy runs evaluations and scans on your resources to make sure they're compliant.

### Things to know about Azure Policy

The main advantages of Azure Policy are in the areas of enforcement and compliance, scaling, and remediation. Azure Policy is also important for teams that run an environment that requires different forms of governance.

| **Advantage** | **Description** |
| --- | --- |
| **Enforce rules and compliance** | Enable built-in policies, or build custom policies for all resource types. Support real-time policy evaluation and enforcement, and periodic or on-demand compliance evaluation. |
| **Apply policies at scale** | Apply policies to a management group with control across your entire organization. Apply multiple policies and aggregate policy states with policy initiative. Define an exclusion scope. |
| **Perform remediation** | Conduct real-time remediation, and remediation on your existing resources. |
| **Exercise governance** | Implement governance tasks for your environment: - Support multiple engineering teams (deploying to and operating in the environment) - Manage multiple subscriptions - Standardize and enforce how cloud resources are configured - Manage regulatory compliance, cost control, security, and design consistency |

### Things to consider when using Azure Policy

Review the following scenarios for using Azure Policy. Consider how you can implement the service in your organization.

* **Consider deployable resources**. Specify the resource types that your organization can deploy by using Azure Policy. You can specify the set of virtual machine SKUs that your organization can deploy.
* **Consider location restrictions**. Restrict the locations your users can specify when deploying resources. You can choose the geographic locations or regions that are available to your organization.
* **Consider rules enforcement**. Enforce compliance rules and configuration options to help manage your resources and user options. You can enforce a required tag on resources and define the allowed values.
* **Consider inventory audits**. Use Azure Policy with Azure Backup service on your VMs and run inventory audits.

## Next unit: Create Azure policies