


Organize your Azure resources

04/09/2019 • 5 minutes to read • Contributors 

In this article

[Scope of management settings](#)

[Create a management level](#)

[Learn more](#)

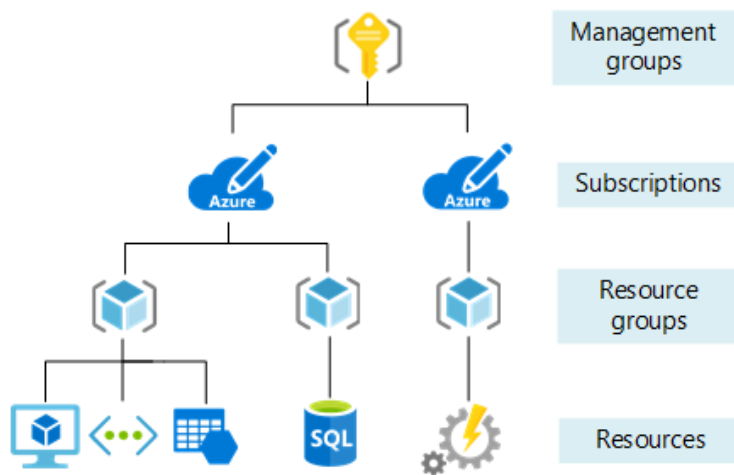
Use the following features and best practices to secure resources that are critical to your system. Tag resources so you can track them by values that make sense to your organization.

Azure management groups and hierarchy

Naming standards

Resource tags

The organizing structure for resources in Azure has four levels: management groups, subscriptions, resource groups, and resources. The following image shows the relationship of these levels.



- **Management groups:** These are containers that help you manage access, policy, and compliance for multiple subscriptions. All subscriptions in a management group automatically inherit the conditions applied to the management group.
- **Subscriptions:** A subscription groups together user accounts and the resources that have been created by those user accounts. For each subscription, there are limits or quotas on the amount of resources you can create and use. Organizations can use subscriptions to manage costs and the resources that are created by users, teams, or projects.
- **Resource groups:** A resource group is a logical container into which Azure resources like web apps, databases, and storage accounts are deployed and managed.
- **Resources:** Resources are instances of services that you create, like virtual machines, storage, or SQL databases.

Scope of management settings

You can apply management settings, like policies and role-based access controls, at any of the management levels. 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 to a subscription, that policy is also applied to all resource groups and resources in that subscription.

Usually, it makes sense to apply critical settings at higher levels and project-specific requirements at lower levels. For example, you may want to make sure all resources for your organization are deployed to certain regions. To do

that, apply a policy to the subscription that specifies the allowed locations. As other users in your organization add new resource groups and resources, the allowed locations are automatically enforced. Learn more about policies in the governance, security, and compliance section of this guide.

As you plan your compliance strategy, we recommend you work with people in your organization with these roles: security and compliance, IT administration, enterprise architect, networking, finance, and procurement.

Create a management level

You can create a management group, additional subscriptions, or resource groups.

Create management group

Create a management group to help you manage access, policy, and compliance for multiple subscriptions.

1. Go to [Management Groups](#).
2. Select **Add management group**.

Create subscription

Use subscriptions to manage costs and resources that are created by users, teams, or projects.

1. Go to [Subscriptions](#).
2. Select **Add**.

Create resource group

Create a resource group to hold resources like web apps, databases, and storage accounts that share the same lifecycle, permissions, and policies.

1. Go to [Resource Groups](#).
2. Select **Add**.
3. Select the **Subscription** that you want your resource group created under.
4. Enter a name for the **Resource group**.
5. Select a **Region** for the resource group location.

Learn more

To learn more, see:

- [Understanding resource access management in Azure](#)
- [Organize your resources with Azure Management Groups](#)
- [Subscription service limits](#)