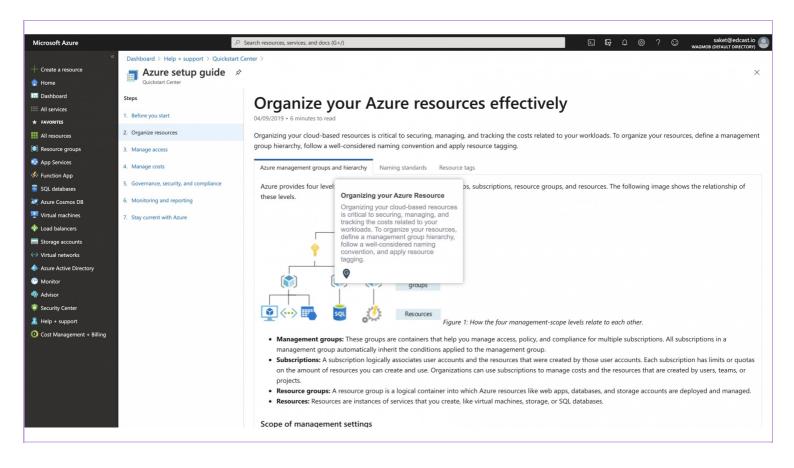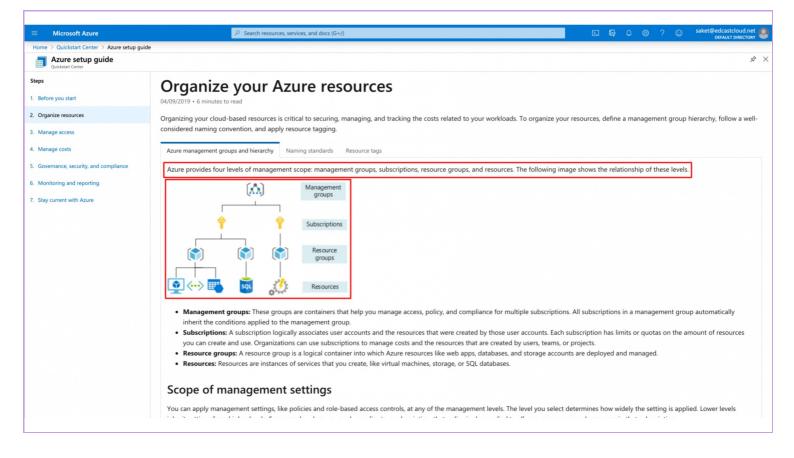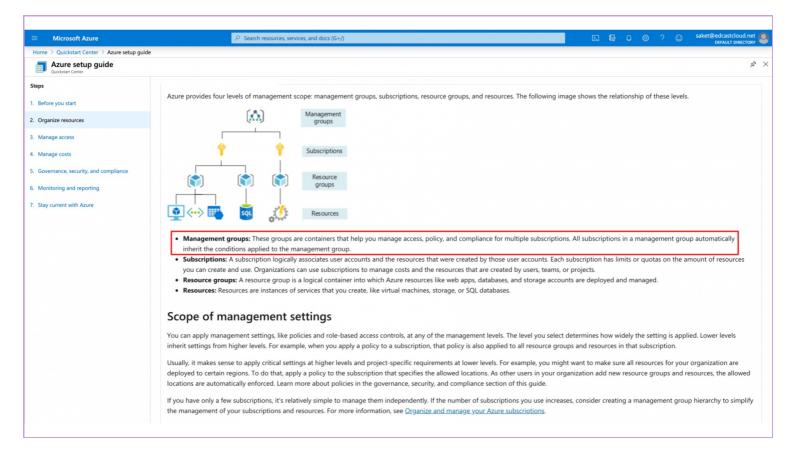# Azure Setup Guide - Organize Your Azure Resources
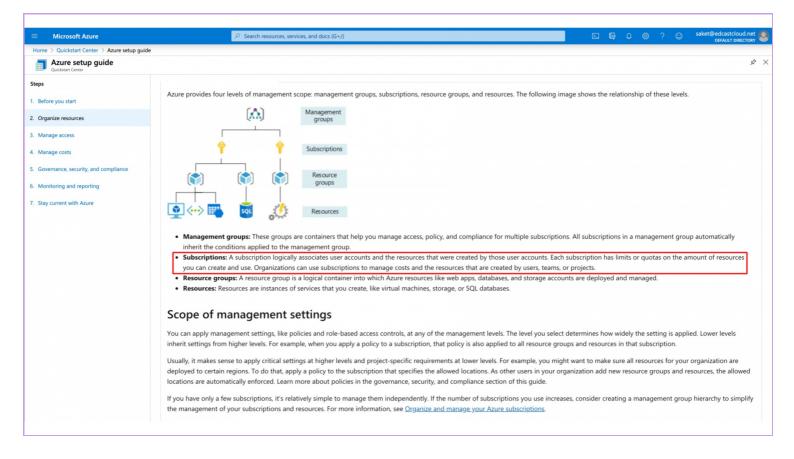
Organizing your Azure Resource

Organizing your cloud-based resources is critical to securing, managing, and tracking the costs related to your workloads. To organize your resources, define a management group hierarchy, follow a well-considered naming convention, and apply resource tagging.

myGuide
by edcast

Step: 02

Step: 03

Azure provides four levels of management scope: management groups, subscriptions, resource groups, and resources. The following image shows the relationship of these levels.

- **Management groups:** These groups 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 logically associates user accounts and the resources that were created by those user accounts. Each subscription has 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 might 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.

If you have only a few subscriptions, it's relatively simple to manage them independently. If the number of subscriptions you use increases, consider creating a management group hierarchy to simplify the management of your subscriptions and resources. For more information, see Organize and manage your Azure subscriptions.

Step: 04

Step: 05

Azure setup guide
Quickstart Center

Steps

1. Before you start
2. Organize resources
3. Manage access
4. Manage costs
5. Governance, security, and compliance
6. Monitoring and reporting
7. Stay current with Azure

Azure provides four levels of management scope: management groups, subscriptions, resource groups, and resources. The following image shows the relationship of these levels.

- **Management groups:** These groups 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 logically associates user accounts and the resources that were created by those user accounts. Each subscription has 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 might 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.

If you have only a few subscriptions, it's relatively simple to manage them independently. If the number of subscriptions you use increases, consider creating a management group hierarchy to simplify the management of your subscriptions and resources. For more information, see Organize and manage your Azure subscriptions.

Step: 06

Step: 07

myGuide
by edcast

Step: 08

Thank You!

myguide.org