Introduction to Role based access control

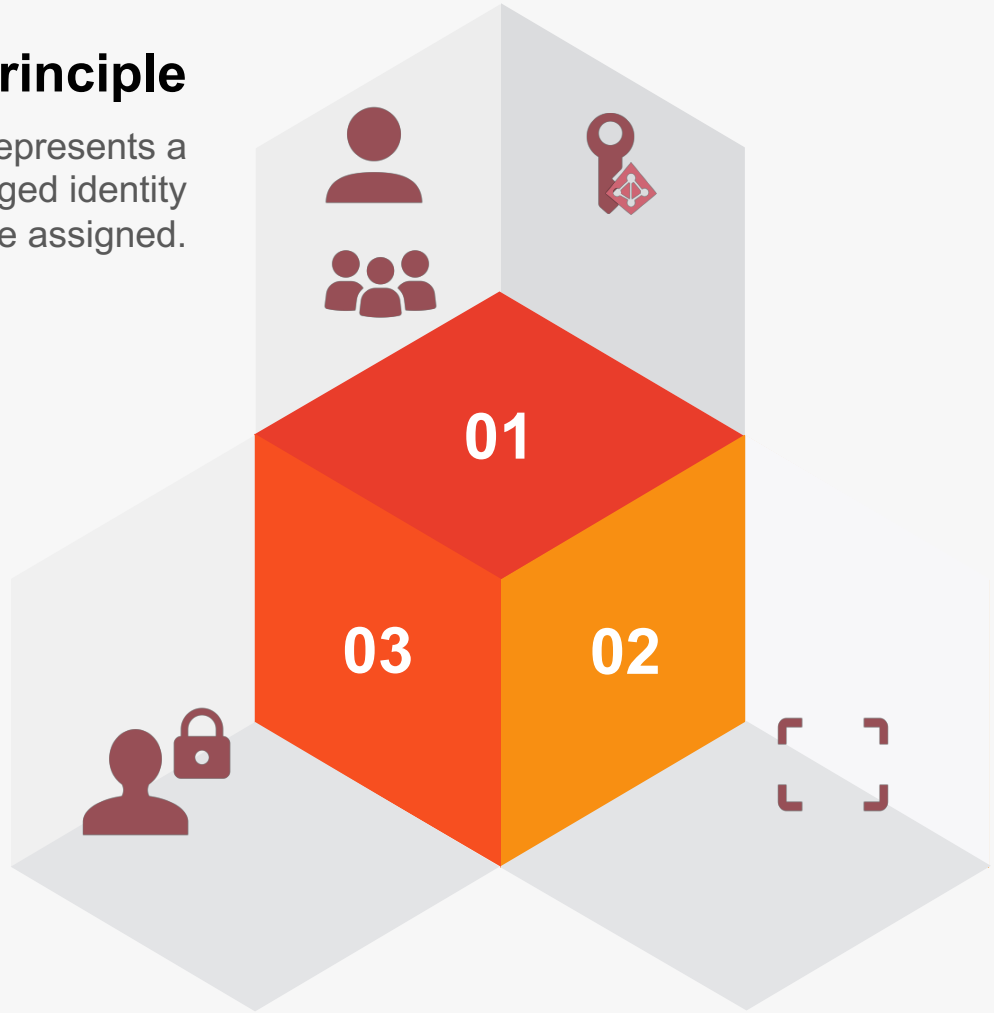
Overview of Role based access control (RBAC)

RUDRA PRODUCTS & SERVICES

RBAC is an authorization system built on Azure Resource Manager that provides fine-grained access management of Azure resources.

Security Principle

A security principle is an object that represents a user, group, service principle or managed identity to which access to resources are assigned.



Role definition

A role definition is a collection of permissions. It's sometimes just called a role. A role definition lists the operations that can be performed, such as read, write, and delete.

Scope

Scope is the set of resources that the access applies to. When you assign a role, you can further limit the actions allowed by defining a scope.

Security principle

- **User** - An individual who has a profile in Azure Active Directory. You can also assign roles to users in other tenants. For information about users in other organizations, see Azure Active Directory B2B.

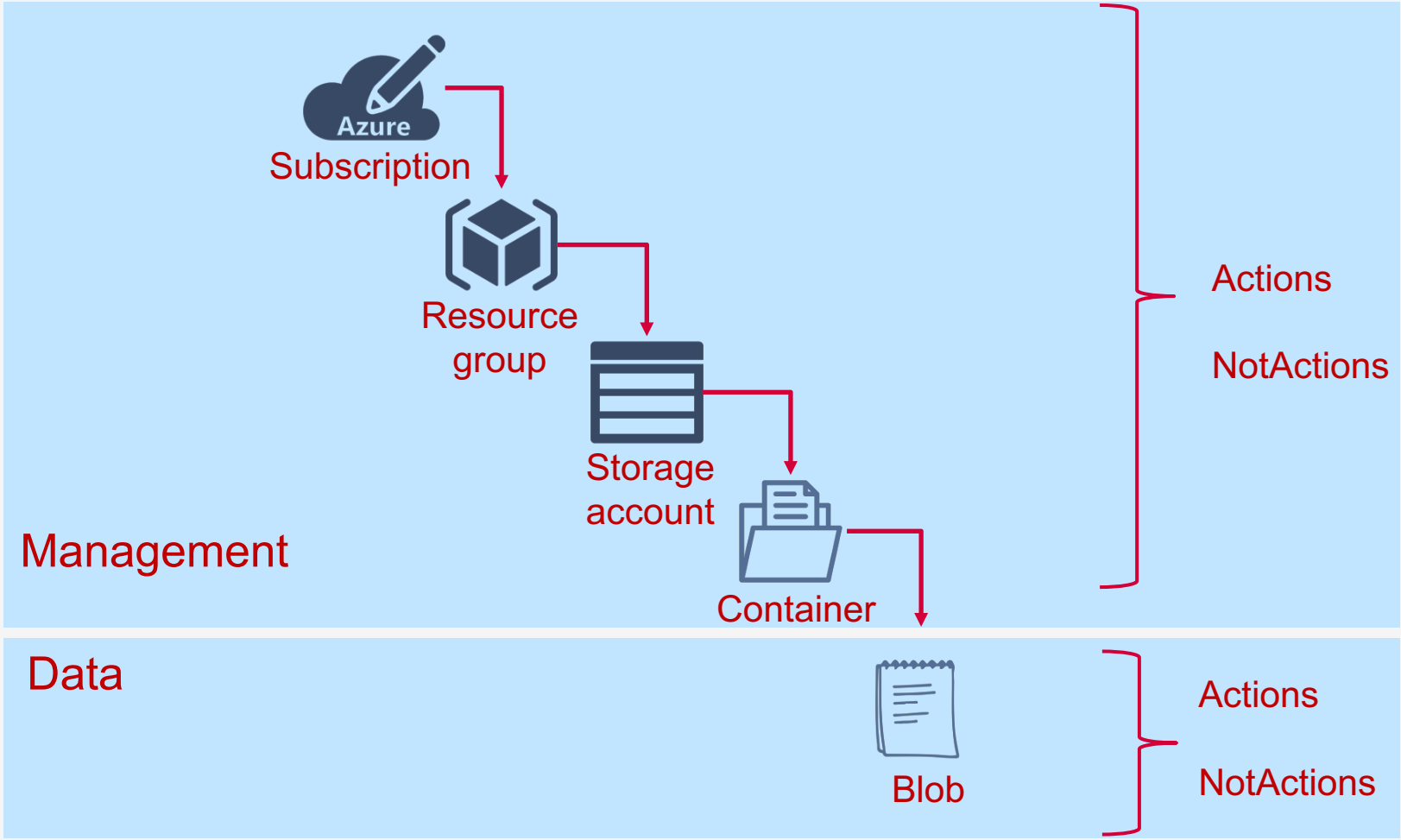
- **Group** - A set of users created in Azure Active Directory. When you assign a role to a group, all users within that group have that role.

- **Service principal** - A security identity used by applications or services to access specific Azure resources. You can think of it as a user identity (username and password or certificate) for an application.

- **Managed identity** - An identity in Azure Active Directory that is automatically managed by Azure. You typically use managed identities when developing cloud applications to manage the credentials for authenticating to Azure services.

Role definition

A role definition lists the operations that can be performed, such as read, write, and delete. It can also list the operations that can't be performed or operations related to underlying data.



Role types

RBAC roles - Azure RBAC includes over 70 built-in roles. There are four fundamental RBAC roles

- Owner
- Contributor
- Reader
- User Access administrator

Azure AD administrator roles - Azure AD administrator roles are used to manage Azure AD resources in a directory such as create or edit users, assign administrative roles to others, reset user passwords, manage user licenses, and manage domains.

Scope

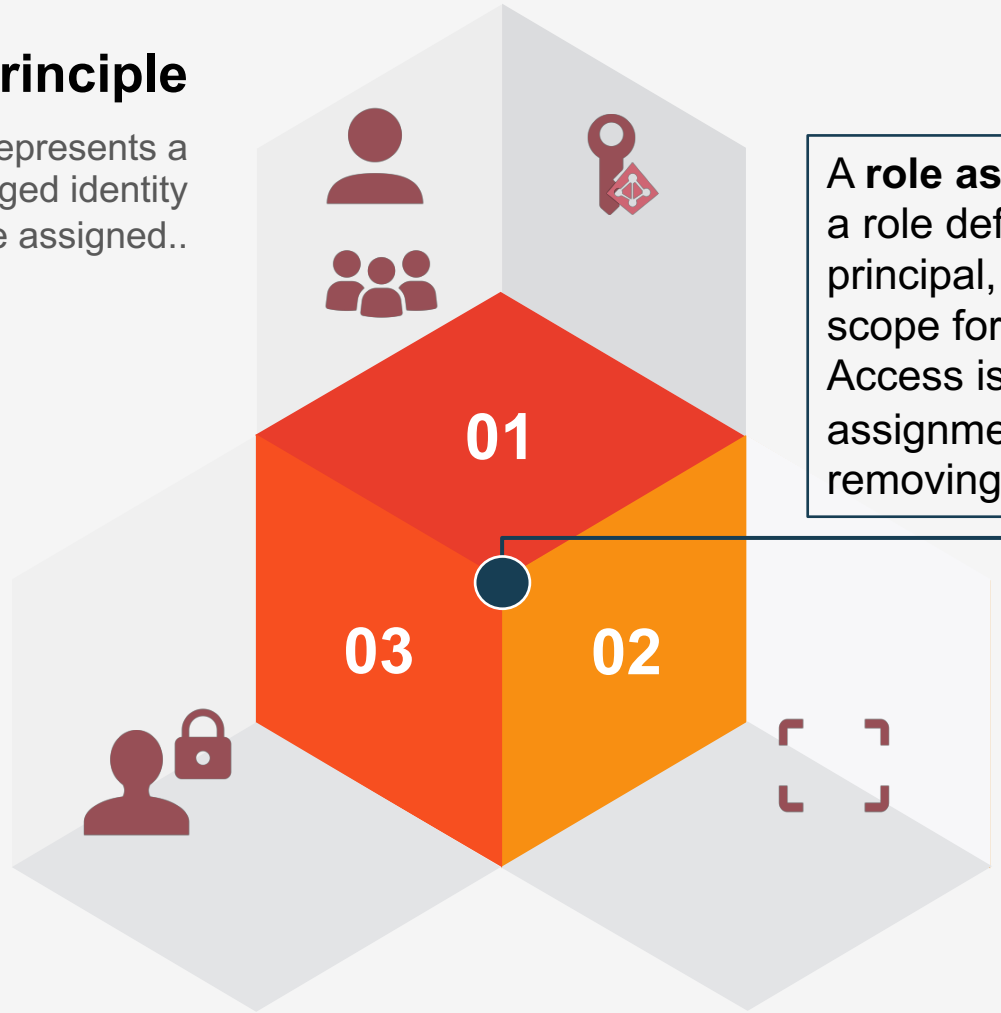
- *Scope* is the set of resources that the access applies to. When you assign a role, you can further limit the actions allowed by defining a scope

- In Azure, you can specify a scope at multiple levels: management group, subscription, resource group, or resource. Scopes are structured in a parent-child relationship.

Role assignment

Security Principle

A security principle is an object that represents a user, group, service principle or managed identity to which access to resources are assigned..



A **role assignment** is the process of attaching a role definition to a user, group, service principal, or managed identity at a particular scope for the purpose of granting access. Access is granted by creating a role assignment, and access is revoked by removing a role assignment.

Role definition

A role definition is a collection of permissions. It's sometimes just called a role. A role definition lists the operations that can be performed, such as read, write, and delete.

Scope

Scope is the set of resources that the access applies to. When you assign a role, you can further limit the actions allowed by defining a scope.