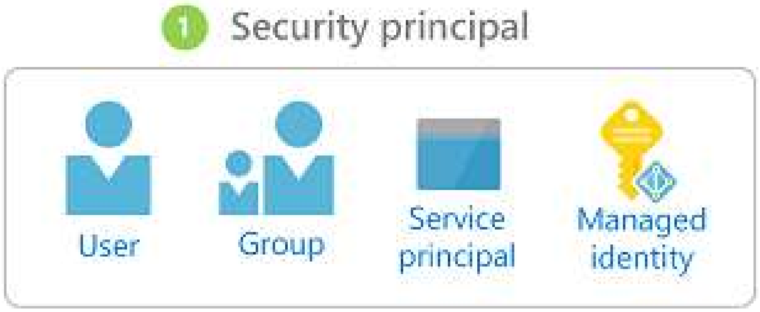
Azure IAM – Identity and Access Management - RBAC

RBAC - Role-Based Access Control

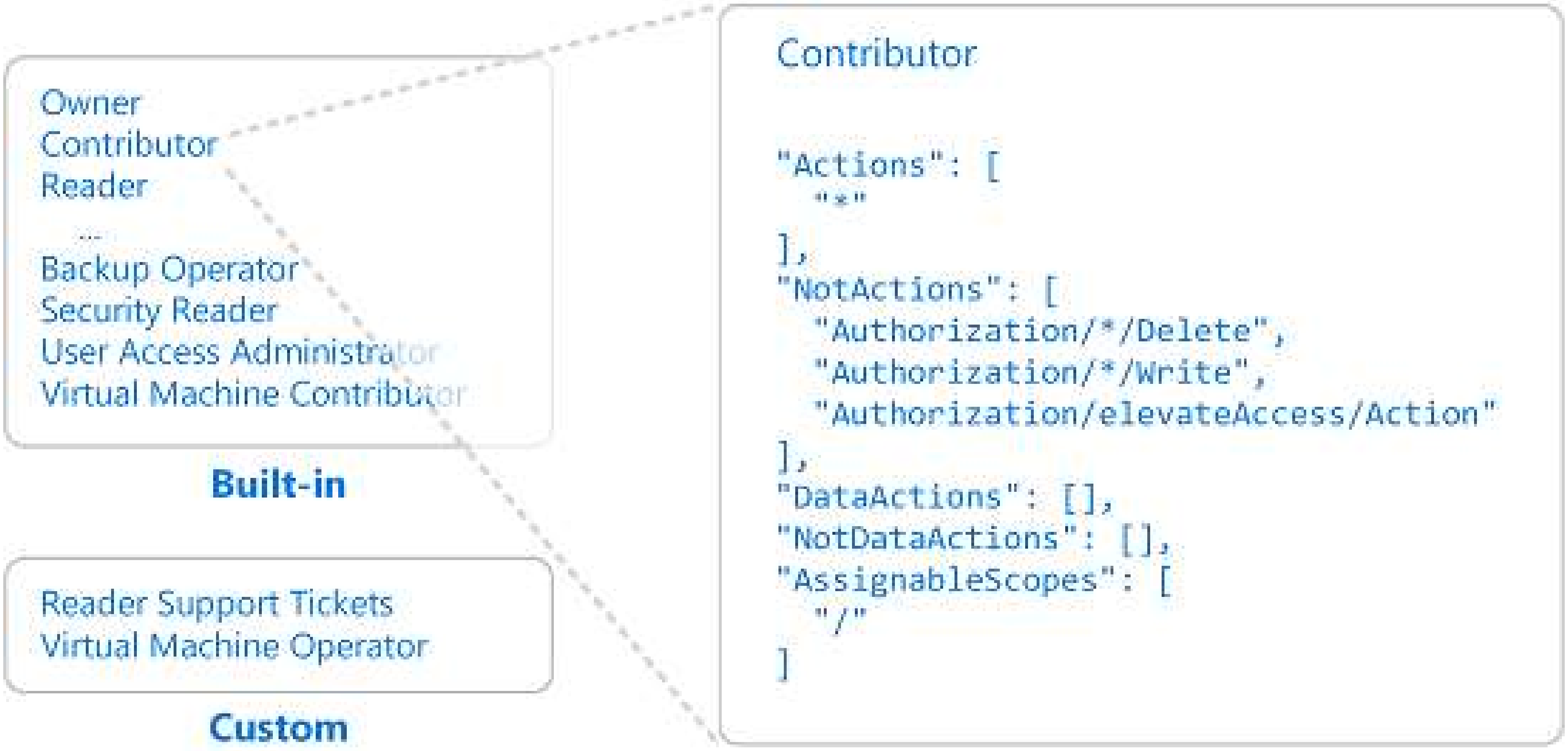
- Helps to
  - Manage who has access to Azure resources,
  - What they can do with those resources, and
  - What areas they have access to.
- Provides fine-grained access management of Azure resources.

Security principal

- Represents a user, group, service principal, or managed identity
- SP requests access to Azure resources.



Role definition



Owner
Contributor
Reader
...
Backup Operator
Security Reader
User Access Administrator
Virtual Machine Contributor

Built-in

Reader Support Tickets
Virtual Machine Operator

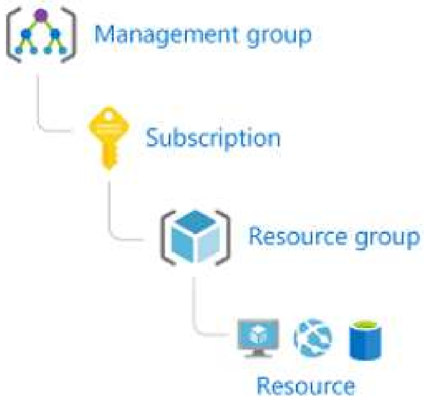
Custom

Contributor

```
"Actions": [
  "*"
],
"NotActions": [
  "Authorization/*/Delete",
  "Authorization/*/Write",
  "Authorization/elevateAccess/Action"
],
"DataActions": [],
"NotDataActions": [],
"AssignableScopes": [
  "/"
]
```

Scope

- 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.



Azure RBAC roles

Azure RBAC role	**Permissions**
Owner	• Full access to all resources • Delegate access to others
Contributor	• Create and manage all of types of Azure resources • Create a new tenant in Azure Active Directory • Cannot grant access to others
Reader	• View Azure resources
User Access Administrator	• Manage user access to Azure resources

Thanks