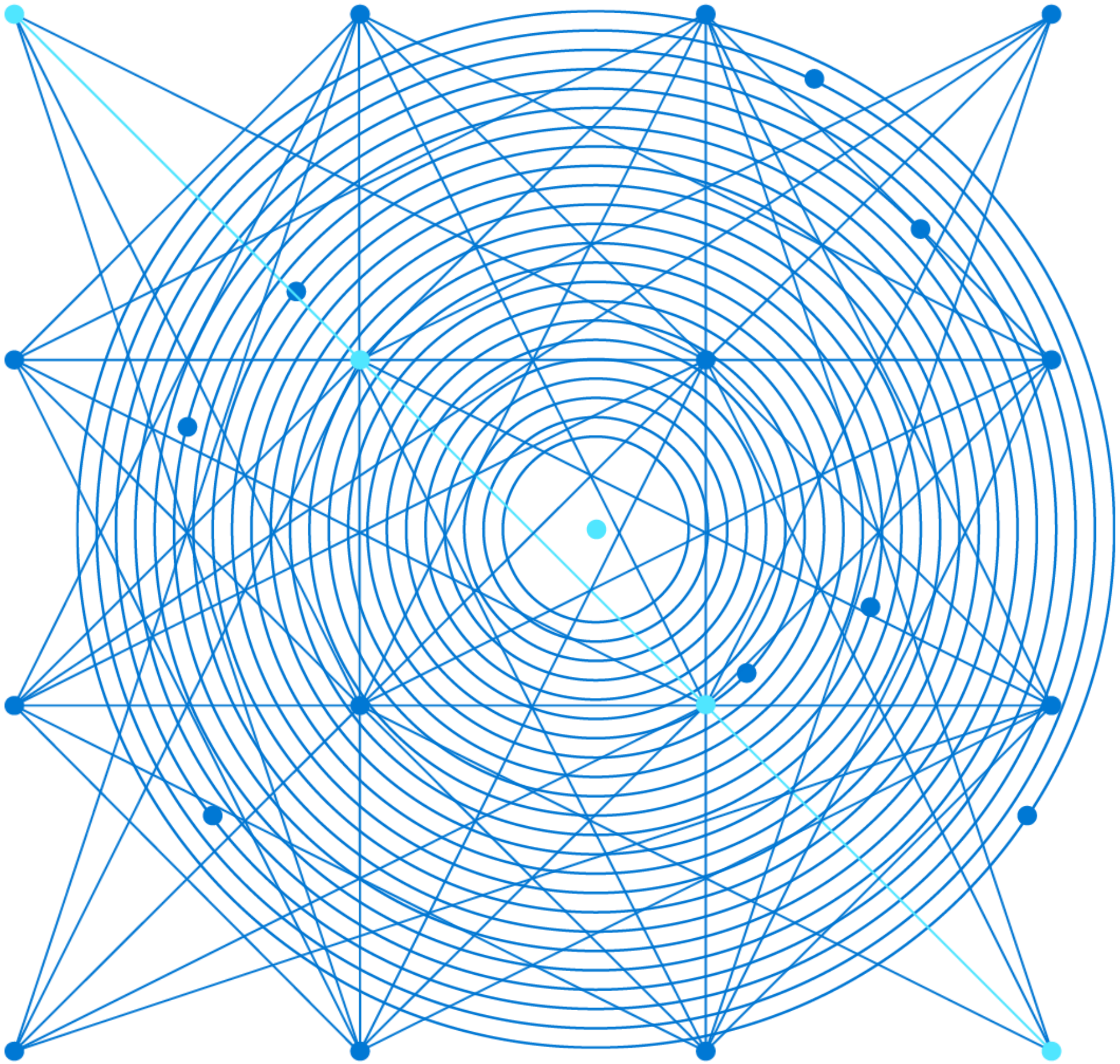
AZ-303: Microsoft Azure Architect Technologies



Module 10: Implement and Manage Azure Governance Solutions

Azure Role-Based Access Control (RBAC), Azure Policy, and Azure Blueprints

Learning Objectives (1 of 2)

You will learn the following:

- Overview of Role-Based Access Control (RBAC)
- Role-based Access Control (RBAC) Roles
- Azure AD Access Reviews
- Implement and Configure an Azure Policy
- Azure Blueprints

Overview of Role-Based Access Control (RBAC)

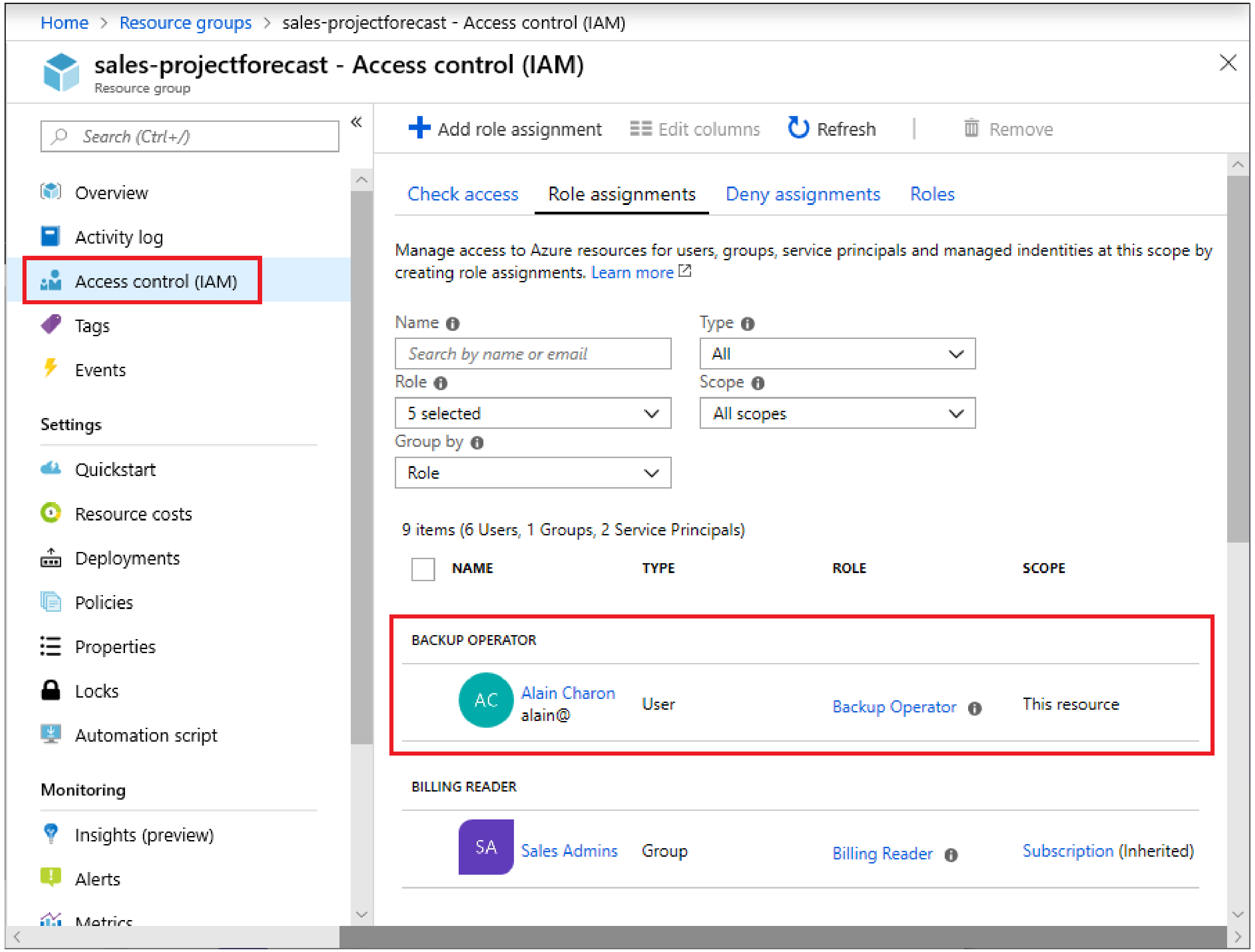
Role-Based Access Control (RBAC)

- Provides fine-grained access management of resources in Azure.
- Built on Azure Resource Manager.
- Segregate duties within your team.
- Grant only the amount of access to users that they need to perform their jobs.
- Users can grant access described in a role definition by creating an assignment.
- Deny assignments are currently read-only and are set by Azure Blueprints and Azure Managed Apps.

Concept	Definition
Security principal	Object that represents something that is requesting access to resources
Role definition	Collection of permissions that lists the operations that can be performed
Scope	Boundary for the level of access that is requested
Assignment	Attaching a role definition to a security principal at a particular scope

RBAC in the Azure Portal

An IAM pane for a resource group:



sales-projectforecast - Access control (IAM)
Resource group

Manage access to Azure resources for users, groups, service principals and managed indentities at this scope by creating role assignments. Learn more

Name: Search by name or email

Type: All

Role: 5 selected

Scope: All scopes

Group by: Role

9 items (6 Users, 1 Groups, 2 Service Principals)

□ NAME	TYPE	ROLE	SCOPE
BACKUP OPERATOR			
AC Alain Charon alain@	User	Backup Operator	This resource
BILLING READER			
SA Sales Admins	Group	Billing Reader	Subscription (Inherited)

How RBAC Works (1 of 4)

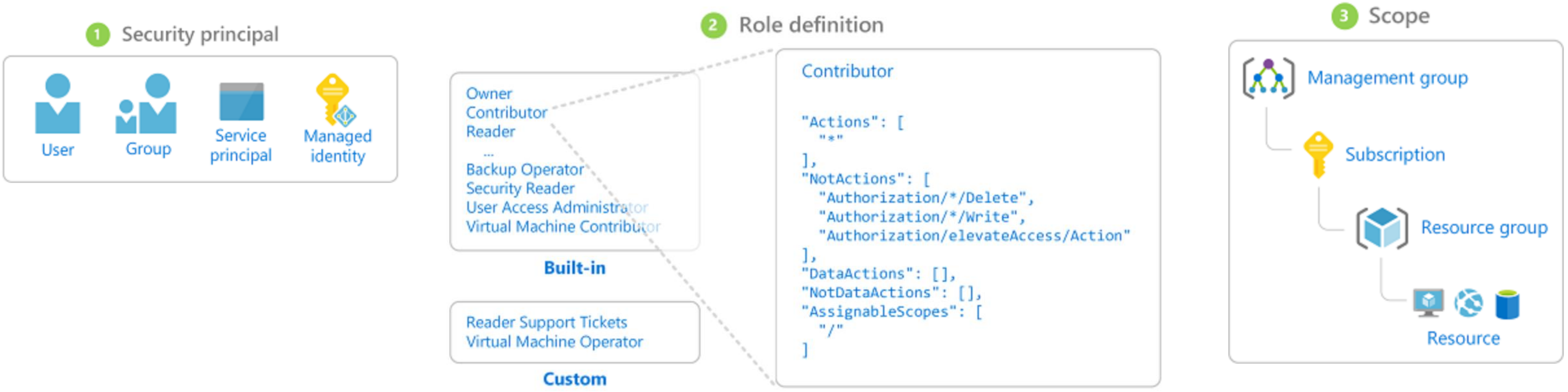
- You control access to resources using RBAC by creating role assignments

- To create a role assignment, you need three elements
  - a security principal
  - a role definition
  - a scope

- You can think of these elements as "who", "what", and "where".

How RBAC Works (2 of 4)

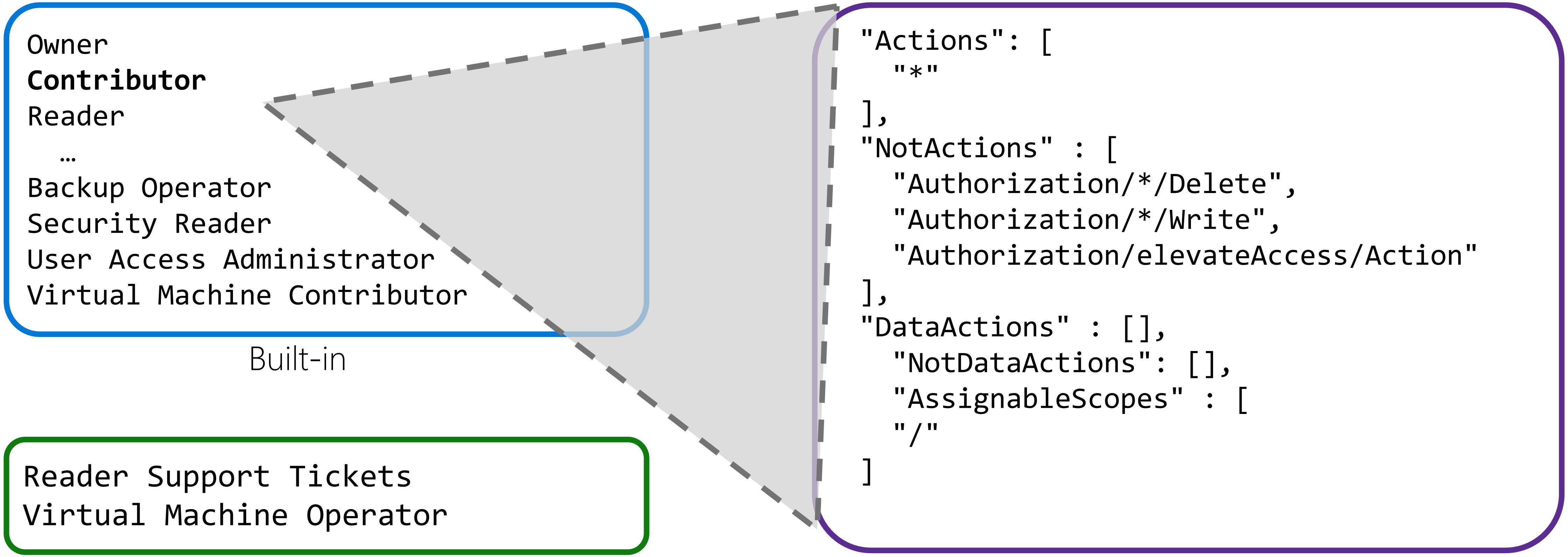
- Security principal
- Role definition
- Scope



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

How RBAC Works (3 of 4)

Collection of permissions that lists the operations that can be performed



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

Built-in

Reader Support Tickets
Virtual Machine Operator

Custom

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

Contributor

How RBAC Works (4 of 4)

RBAC supports ***deny assignments***:

- Attaches a set of deny actions to a user, group, service principal, or managed identity at a particular scope for the purpose of denying access.
- Deny assignments block users from performing specified actions even if a role assignment grants them access.
- Deny assignments take precedence over role assignments.

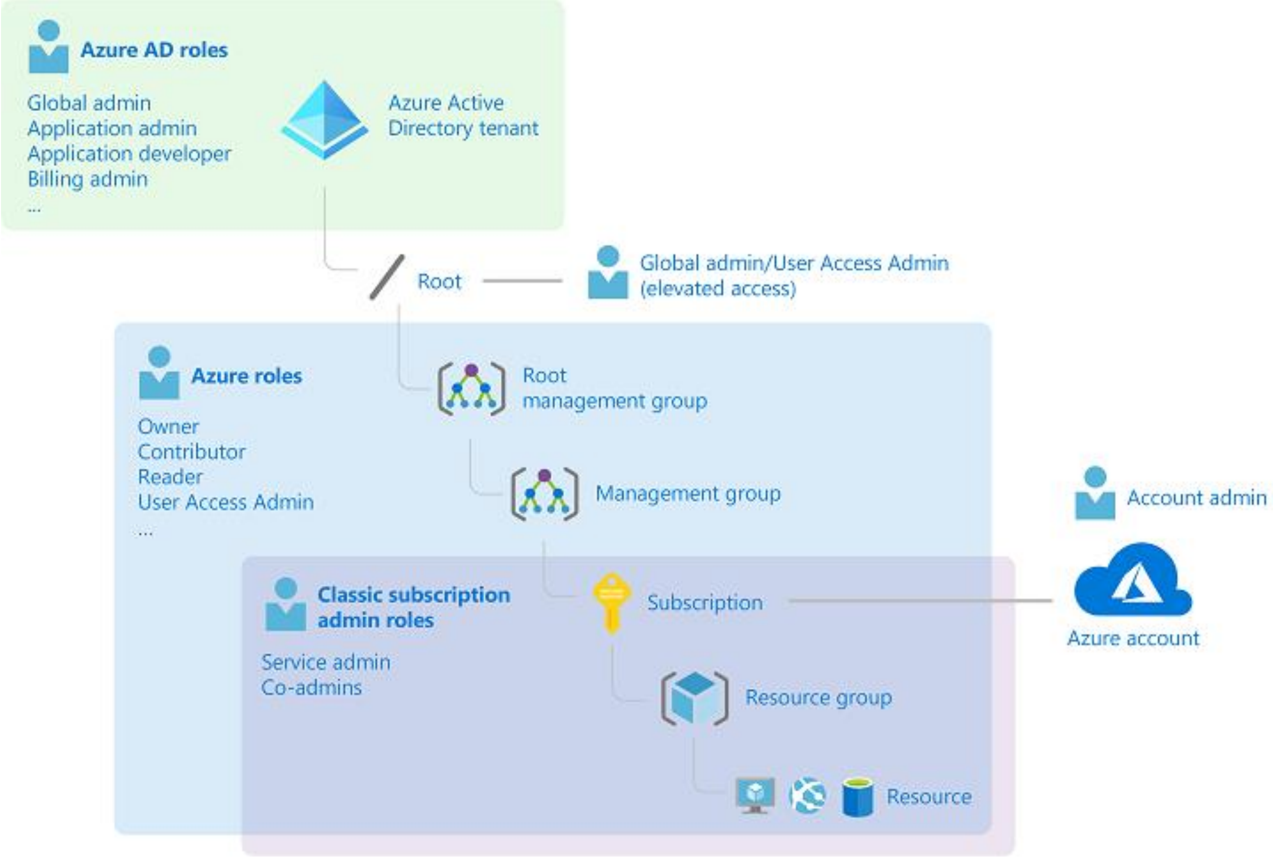
Role-Based Access Control (RBAC)

Administrator Roles, Azure Roles, and Azure AD Roles (1 of 4)

There are three general groups of roles in the context of Azure and Azure AD

- Classic subscription administrator roles
- Azure roles
- Azure AD roles

- How the roles are related



Administrator Roles, Azure Roles, and Azure AD Roles (2 of 4)

Classic subscription administration roles

Role	Limit	Permissions	Notes
Account Administrator	1 per Azure account	Access the Azure Account Center Manage all subscriptions in an account Change the Service Administrator	The Account Administrator has no access to the Azure portal.
Service Administrator	1 per Azure subscription	Manage services in the Azure portal Assign users to the Co-Administrator role	The Service Administrator has the equivalent access of a user who is assigned the Owner role at the subscription scope.
Co-Administrator	200 per subscription	Same access privileges as the Service Administrator, but can't change the association of subscriptions to Azure directories Assign users to the Co-Administrator role, but cannot change the Service Administrator	The Co-Administrator has the equivalent access of a user who is assigned the Owner role at the subscription scope.

Administrator Roles, Azure Roles, and Azure AD Roles (3 of 4)

Azure RBAC roles

Azure role	Permissions	Notes
Owner	Full access to all resourcesDelegate access to others	The Service Administrator and Co-Administrators are assigned the Owner role at the subscription scope Applies to all resource types.
Contributor	Create and manage all of types of Azure resources Create a new tenant in Azure Active Directory Cannot grant access to others	Applies to all resource types.
Reader	View Azure resources	Applies to all resource types.
User Access Administrator	Manage user access to Azure resources	

Administrator Roles, Azure Roles, and Azure AD Roles (4 of 4)

Global Administrator (Azure AD Role)

The following permissions apply:

- Manage access to all administrative features in Azure Active Directory, as well as services that federate to Azure Active Directory
- Assign administrator roles to others
- Reset the password for any user and all other administrators

User Administrator (Azure AD Role)

The following permissions apply:

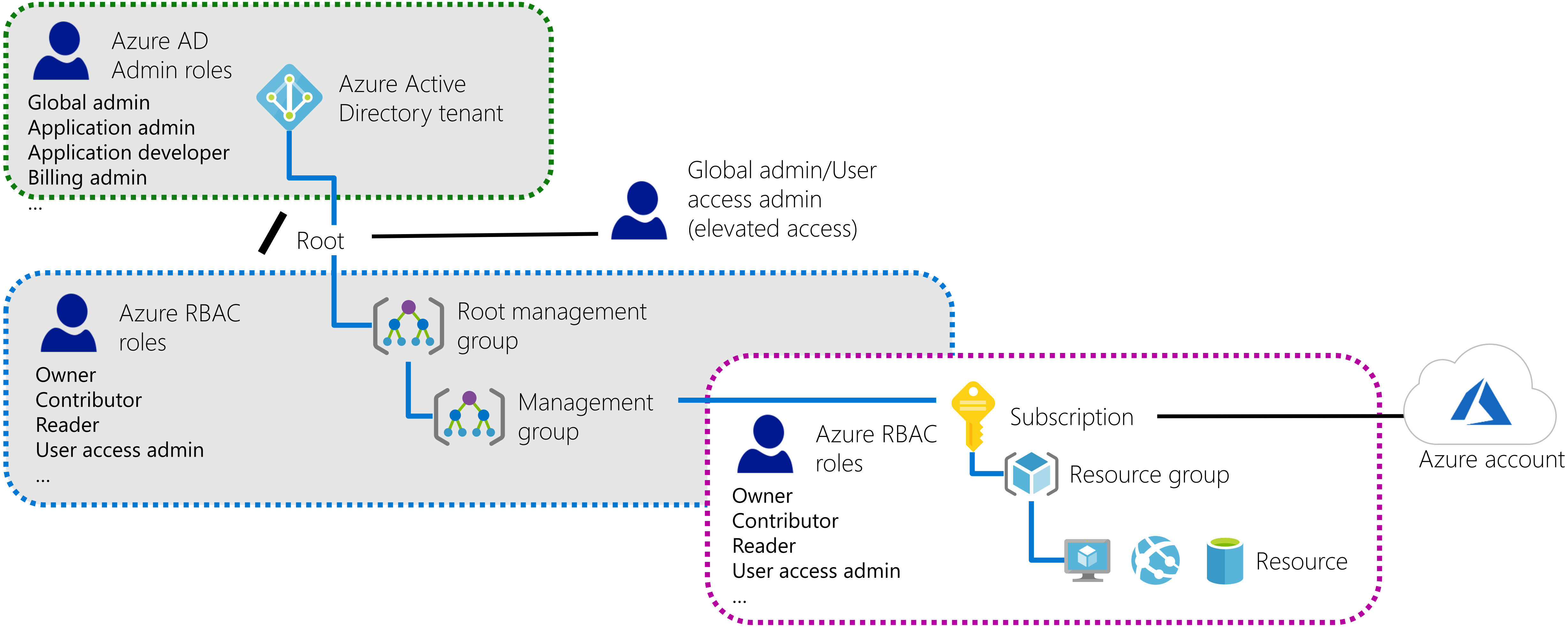
- Create and manage all aspects of users and groups
- Manage support tickets
- Monitor service health
- Change passwords for users, Helpdesk administrators, and other User Administrators

Billing Administrator (Azure AD Role)

The following permissions apply:

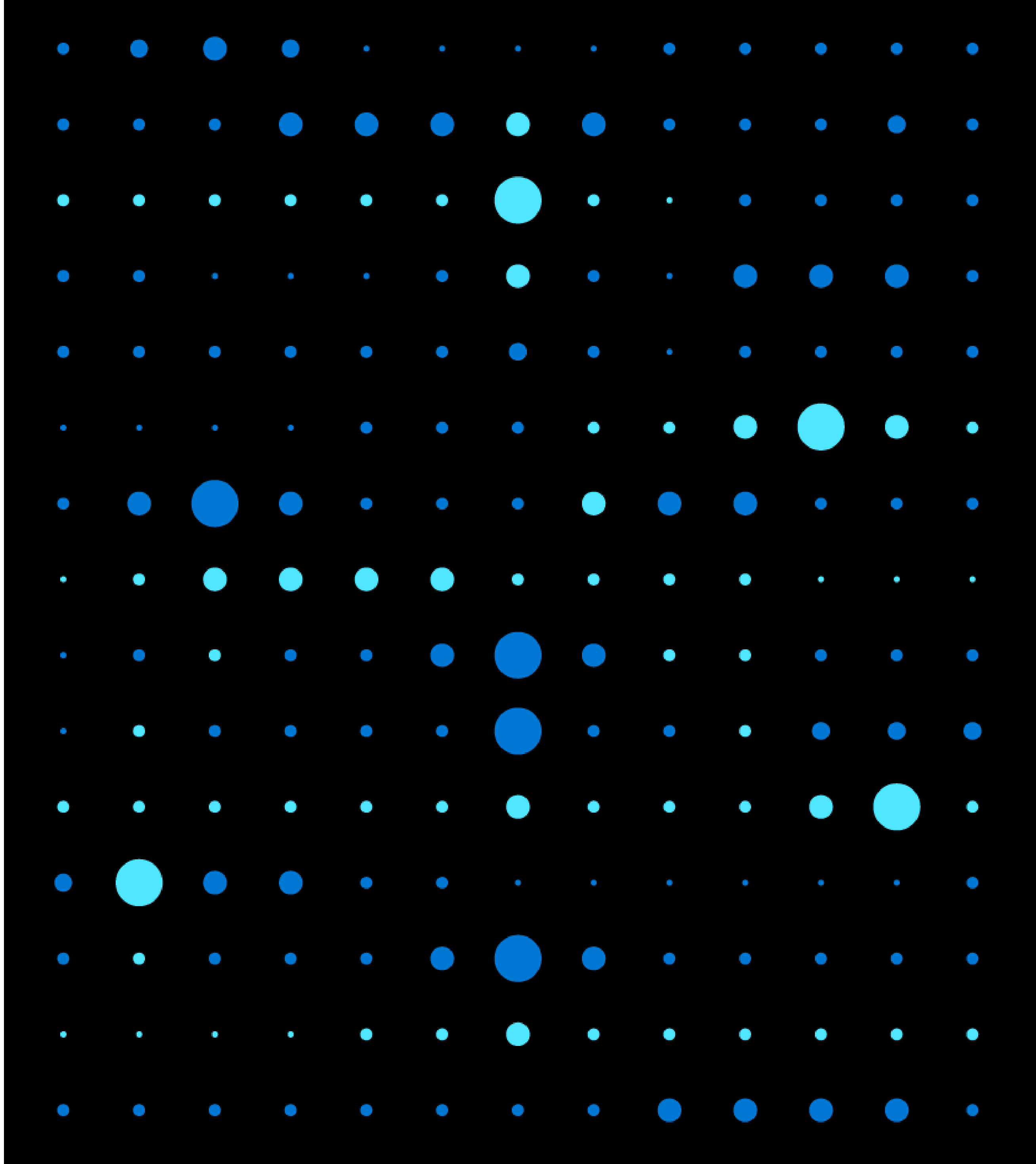
- Make purchases
- Manage subscriptions
- Manage support tickets
- Monitors service health

RBAC Authentication



Demonstration: Add an Azure Role Assignment

- Add a role assignment



Azure AD Access Reviews

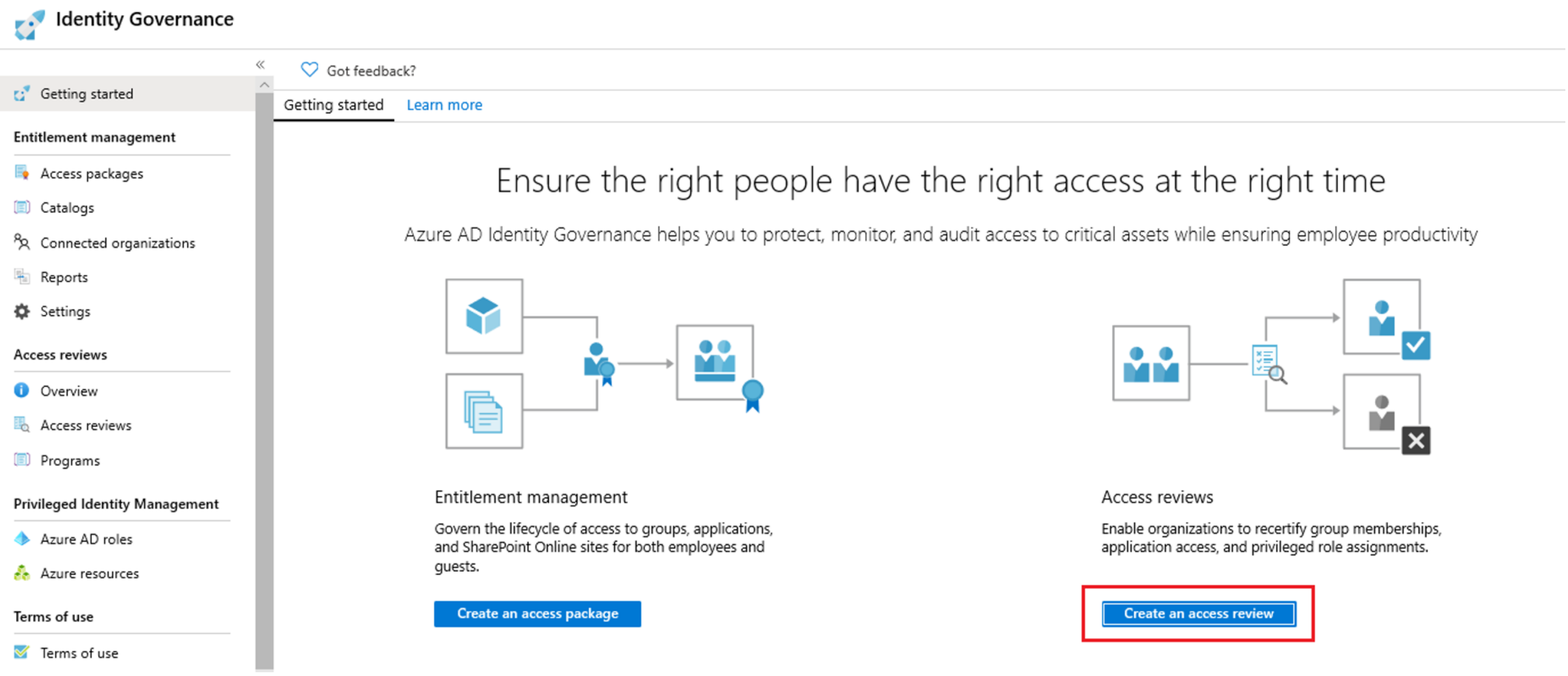
Azure AD Access Reviews

- Why are access reviews important?
- When to use access reviews?
- Where do you create reviews?

Access rights of users	Reviewers can be	Review created in	Reviewer experience
Security group members Office group members	Specified reviewers Group owners Self-review	Azure AD access reviews Azure AD groups	Access panel
Assigned to a connected app	Specified reviewers Self-review	Azure AD access reviews Azure AD enterprise apps (in preview)	Access panel
Azure AD role	Specified reviewers Self-review	Azure AD PIM	Azure portal
Azure resource role	Specified reviewers Self-review	Azure AD PIM	Azure portal

Create an Azure AD Access Review

Manage access reviews in Azure portal



Ensure the right people have the right access at the right time

Azure AD Identity Governance helps you to protect, monitor, and audit access to critical assets while ensuring employee productivity

Entitlement management

Govern the lifecycle of access to groups, applications, and SharePoint Online sites for both employees and guests.

Access reviews

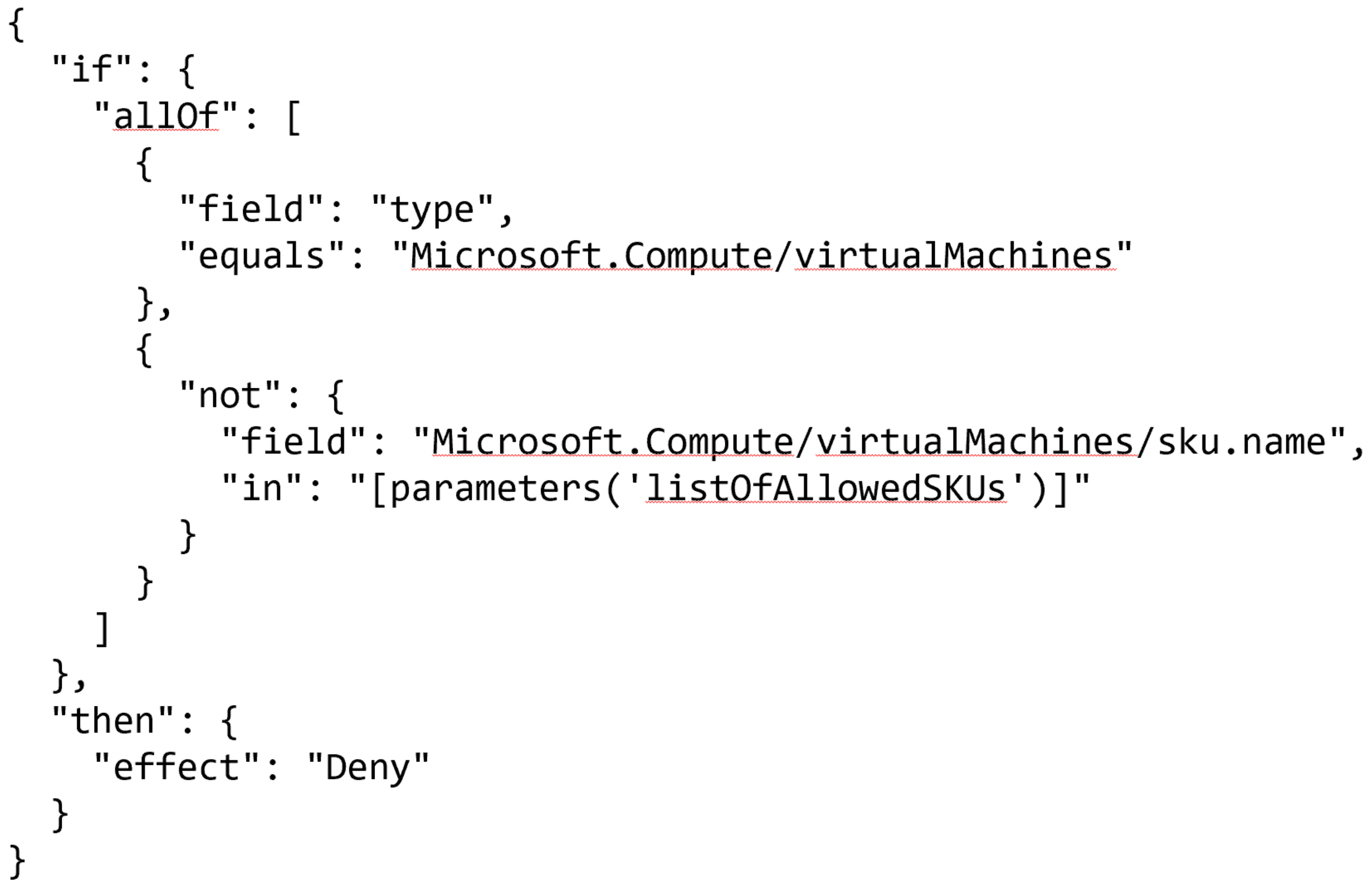
Enable organizations to recertify group memberships, application access, and privileged role assignments.

Implement and Configure an Azure Policy

Azure Policy Overview (1 of 2)

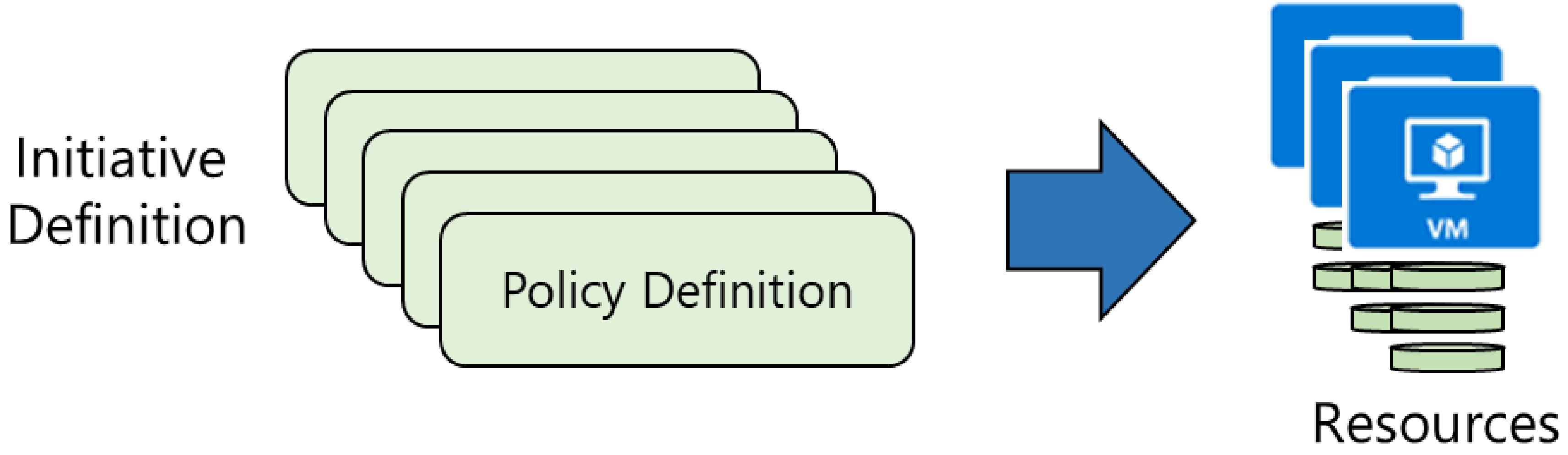
- How are Azure Policy and RBAC different
- Applying a policy
  - Create a policy definition
  - Assign a definition to a scope of resources
  - View policy evaluation results
- What is a policy definition?
  - Allowed storage account SKUs
  - Allowed resource type
  - Allowed locations
  - Allowed virtual machine SKUs
  - Not allowed resource types

Azure Policy Overview (2 of 2)



```
{
  "if": {
    "allOf": [
      {
        "field": "type",
        "equals": "Microsoft.Compute/virtualMachines"
      },
      {
        "not": {
          "field": "Microsoft.Compute/virtualMachines/sku.name",
          "in": "[parameters('listOfAllowedSKUs')]"
        }
      }
    ]
  },
  "then": {
    "effect": "Deny"
  }
}
```

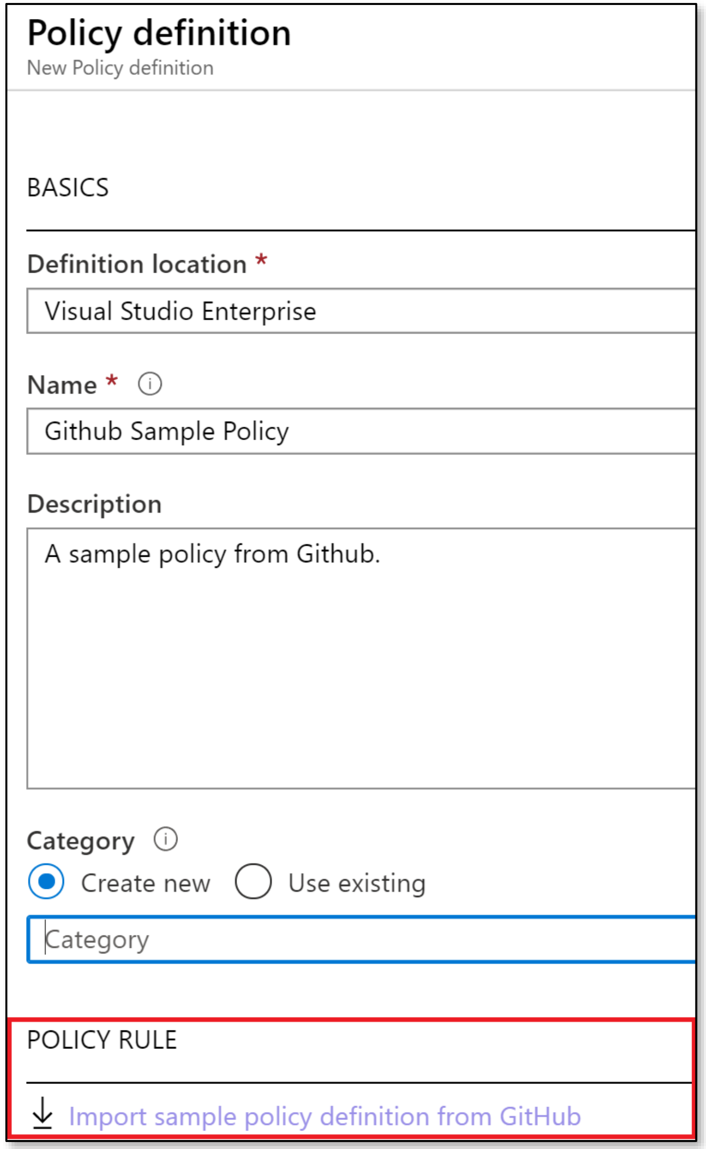
Azure Initiative Definitions



1. Browse policy definitions
2. Create initiative definitions
3. Scope the initiative definition
4. View Policy evaluation results

Policy Definitions

- Many policy definitions are available.
- You can import policies from GitHub.
- Policy definitions have a specific JSON format.
- You can create custom policy definitions.



Policy definition

New Policy definition

BASICS

Definition location *: Visual Studio Enterprise

Name * ⓘ: Github Sample Policy

Description: A sample policy from Github.

Category ⓘ

● Create new ○ Use existing

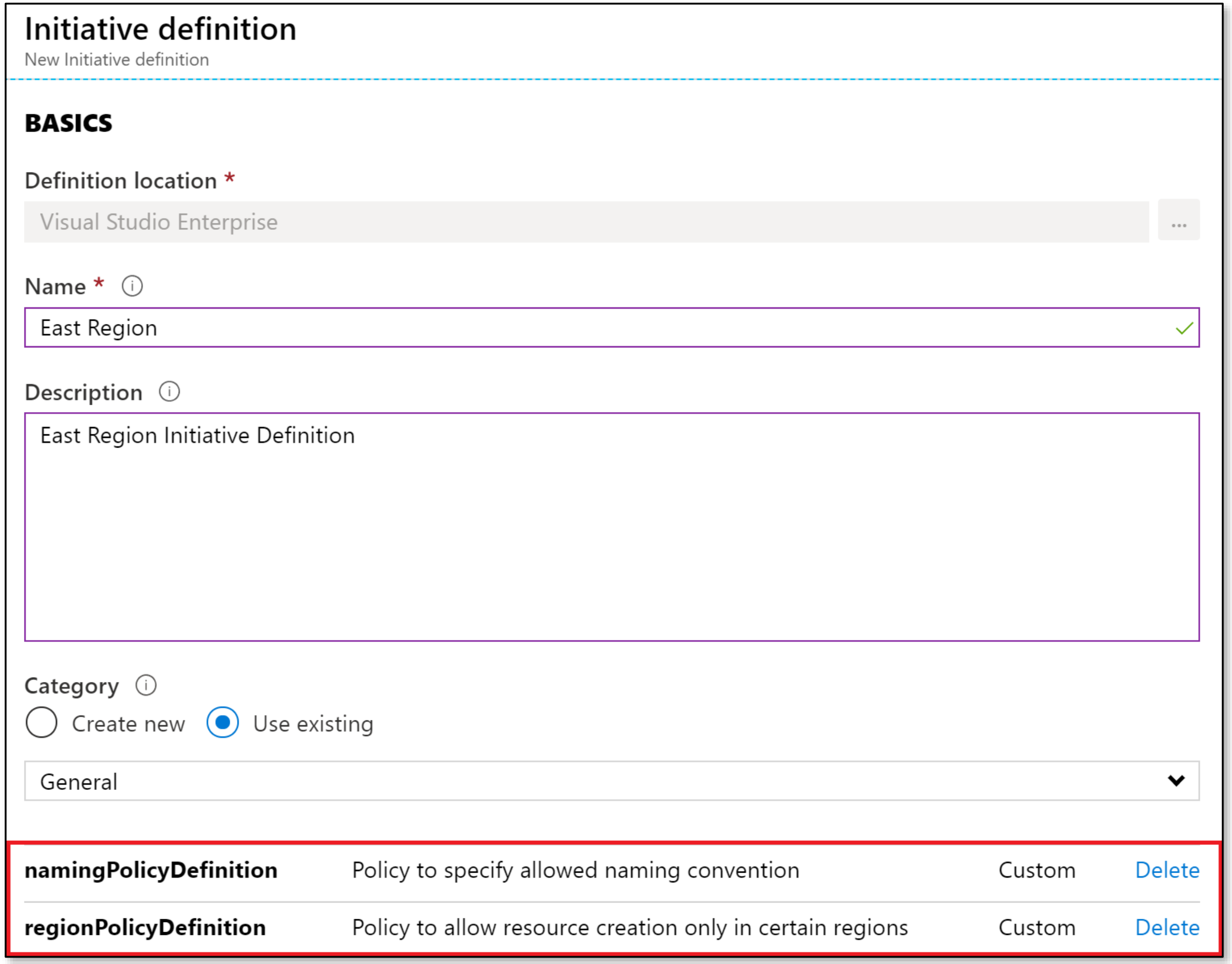
Category

POLICY RULE

Import sample policy definition from GitHub

Create Initiative Definitions

- Group policy definitions
- Include one or more policies
- Requires planning



Initiative definition

New Initiative definition

BASICS

Definition location *

Visual Studio Enterprise

Name *

East Region

Description

East Region Initiative Definition

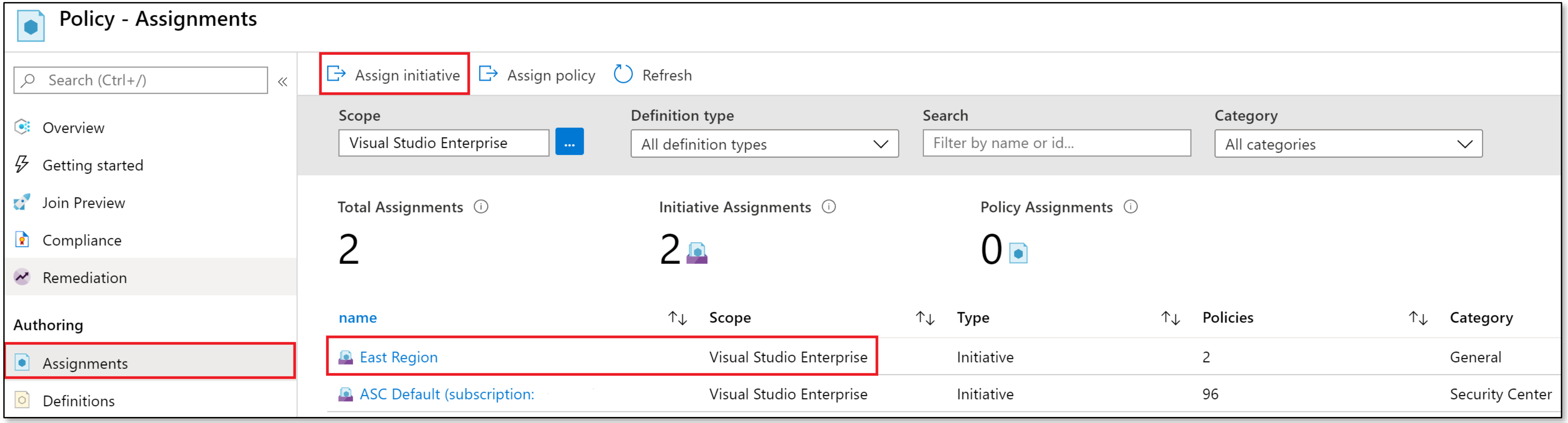
Category

○ Create new ● Use existing

General

namingPolicyDefinition	Policy to specify allowed naming convention	Custom	Delete
regionPolicyDefinition	Policy to allow resource creation only in certain regions	Custom	Delete

Scope the Initiative Definition



Scope: Visual Studio Enterprise

Definition type: All definition types

Search: Filter by name or id...

Category: All categories

Total Assignments: 2

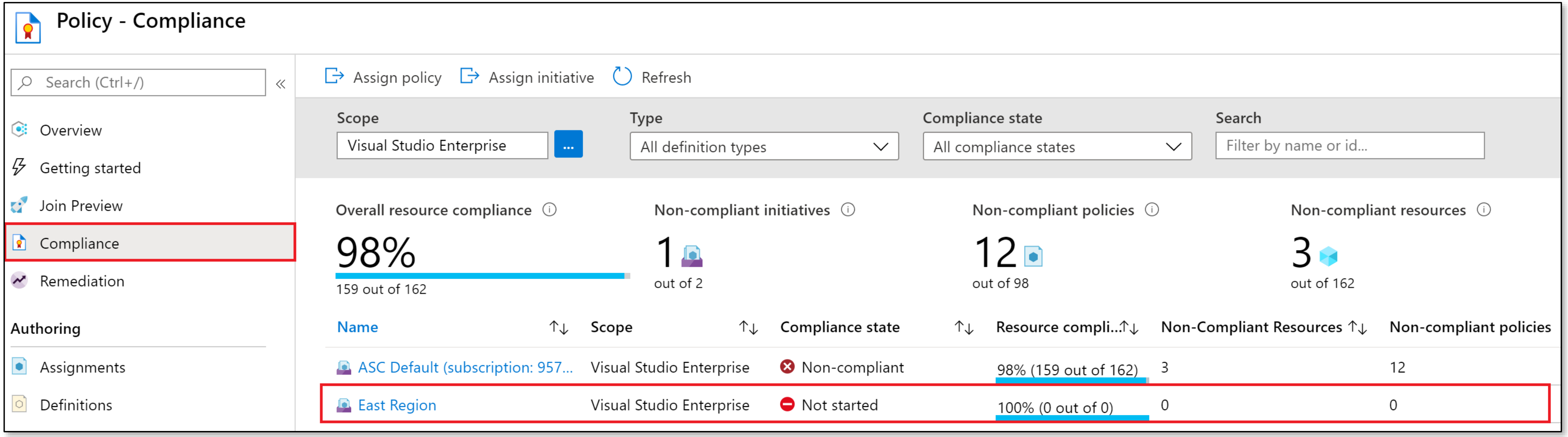
Initiative Assignments: 2

Policy Assignments: 0

name	Scope	Type	Policies	Category
East Region	Visual Studio Enterprise	Initiative	2	General
ASC Default (subscription:	Visual Studio Enterprise	Initiative	96	Security Center

- Assign the definition to a scope
- The scope enforces the policy
- Select the subscription, and optionally the resource group

Determine Compliance



Policy - Compliance

Scope: Visual Studio Enterprise

Type: All definition types

Compliance state: All compliance states

Search: Filter by name or id...

Overall resource compliance: 98% — 159 out of 162

Non-compliant initiatives: 1 — out of 2

Non-compliant policies: 12 — out of 98

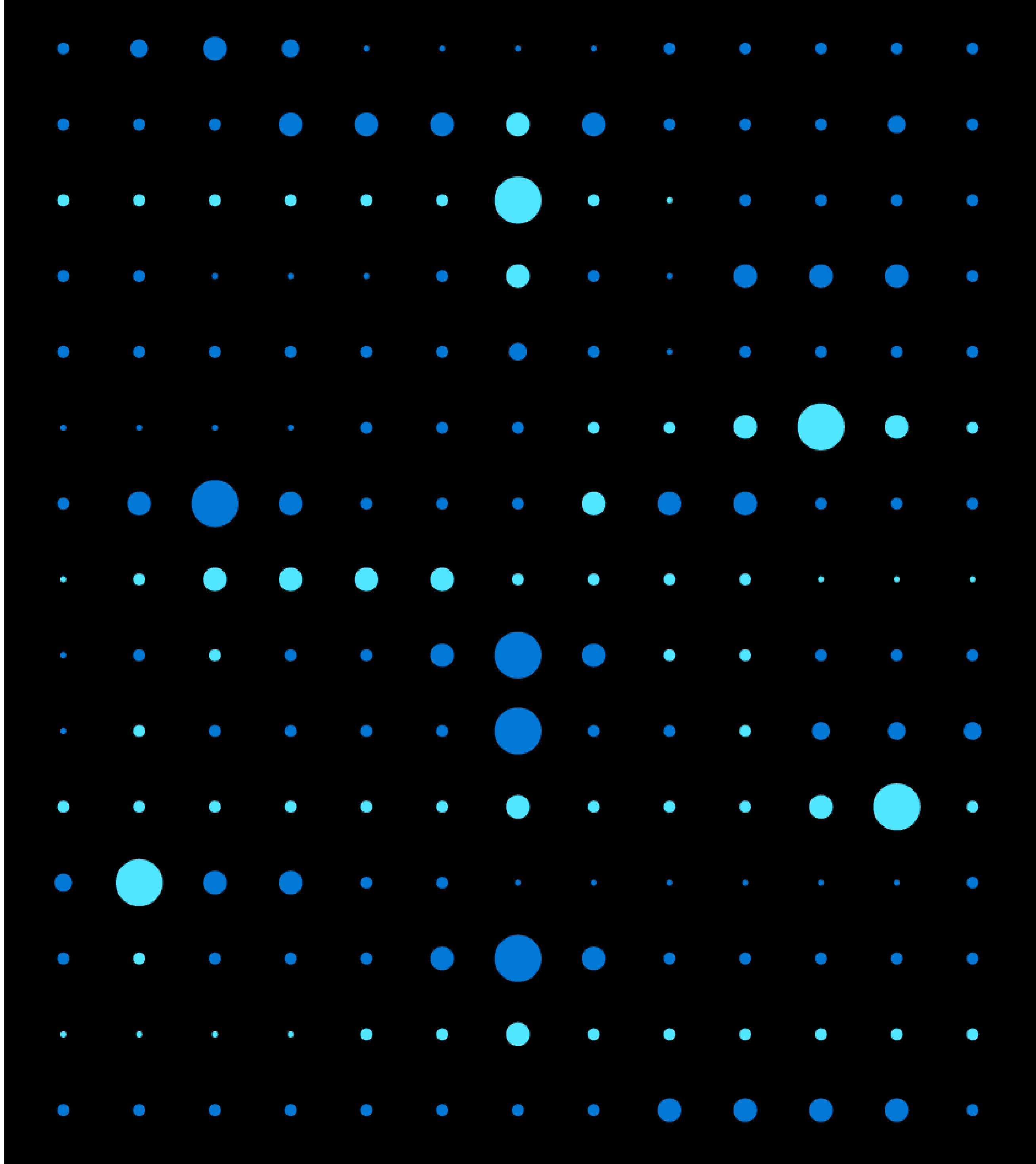
Non-compliant resources: 3 — out of 162

Name ↑↓	Scope ↑↓	Compliance state ↑↓	Resource compli...↑↓	Non-Compliant Resources ↑↓	Non-compliant policies
ASC Default (subscription: 957...	Visual Studio Enterprise	✖ Non-compliant	98% (159 out of 162)	3	12
East Region	Visual Studio Enterprise	⛔ Not started	100% (0 out of 0)	0	0

- Non-compliant initiatives
- Non-compliant policies
- Non-compliant resources

Demonstration: Create and Manage Policies to Enforce Compliance

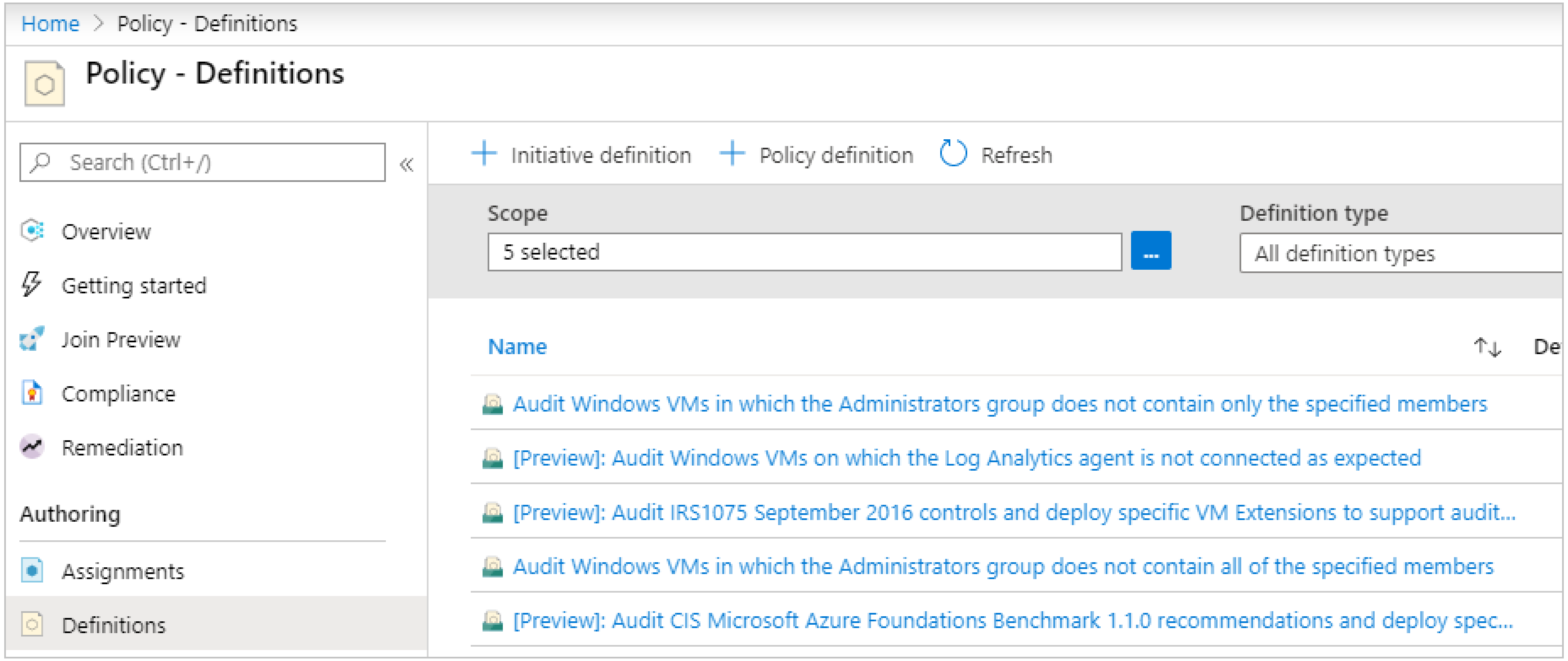
- Assign a policy



Implement a New Custom Policy

Scenario: create a new custom policy to save costs by validating that VMs created in your environment can't be in the G series.

Every time a user in your organization tries to create VM in the G series, the request is denied.



Scope: 5 selected

Definition type: All definition types

Name
Audit Windows VMs in which the Administrators group does not contain only the specified members
[Preview]: Audit Windows VMs on which the Log Analytics agent is not connected as expected
[Preview]: Audit IRS1075 September 2016 controls and deploy specific VM Extensions to support audit...
Audit Windows VMs in which the Administrators group does not contain all of the specified members
[Preview]: Audit CIS Microsoft Azure Foundations Benchmark 1.1.0 recommendations and deploy spec...

Azure Blueprints

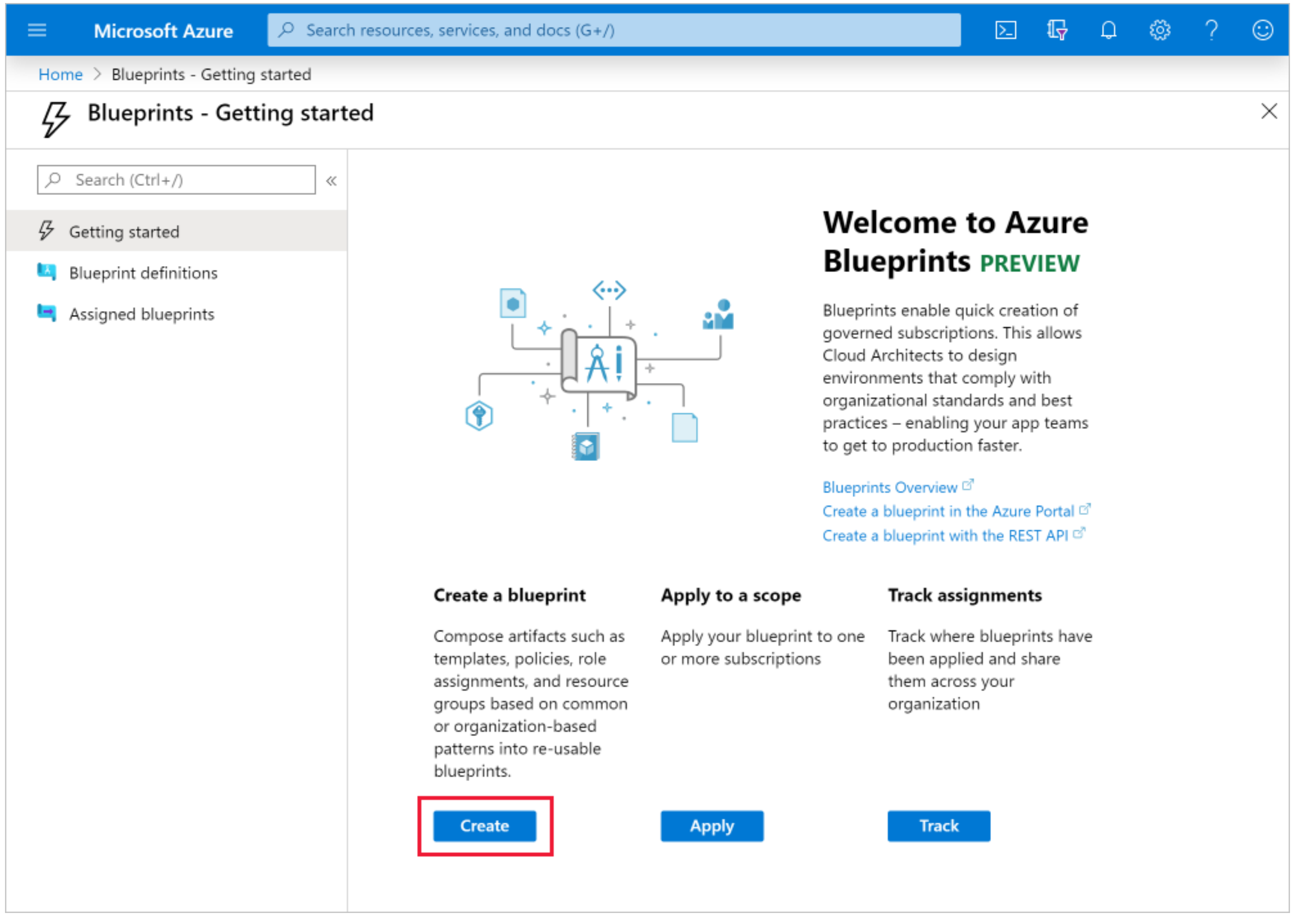
Azure Blueprints

Azure Blueprints is a declarative way to orchestrate the deployment of such artifacts as policy

- Role assignments
- Policy assignments
- ARM templates
- Resource groups

- How is this different from ARM templates

- How is this different from Azure policy


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Blueprints - Getting started
Blueprints - Getting started
Search (Ctrl+/)
Getting started
Blueprint definitions
Assigned blueprints

Welcome to Azure Blueprints PREVIEW

Blueprints enable quick creation of governed subscriptions. This allows Cloud Architects to design environments that comply with organizational standards and best practices – enabling your app teams to get to production faster.

Blueprints Overview
Create a blueprint in the Azure Portal
Create a blueprint with the REST API

Create a blueprint

Compose artifacts such as templates, policies, role assignments, and resource groups based on common or organization-based patterns into re-usable blueprints.

Apply to a scope

Apply your blueprint to one or more subscriptions

Track assignments

Track where blueprints have been applied and share them across your organization

Azure Policy vs. Azure Blueprints

Azure Policy

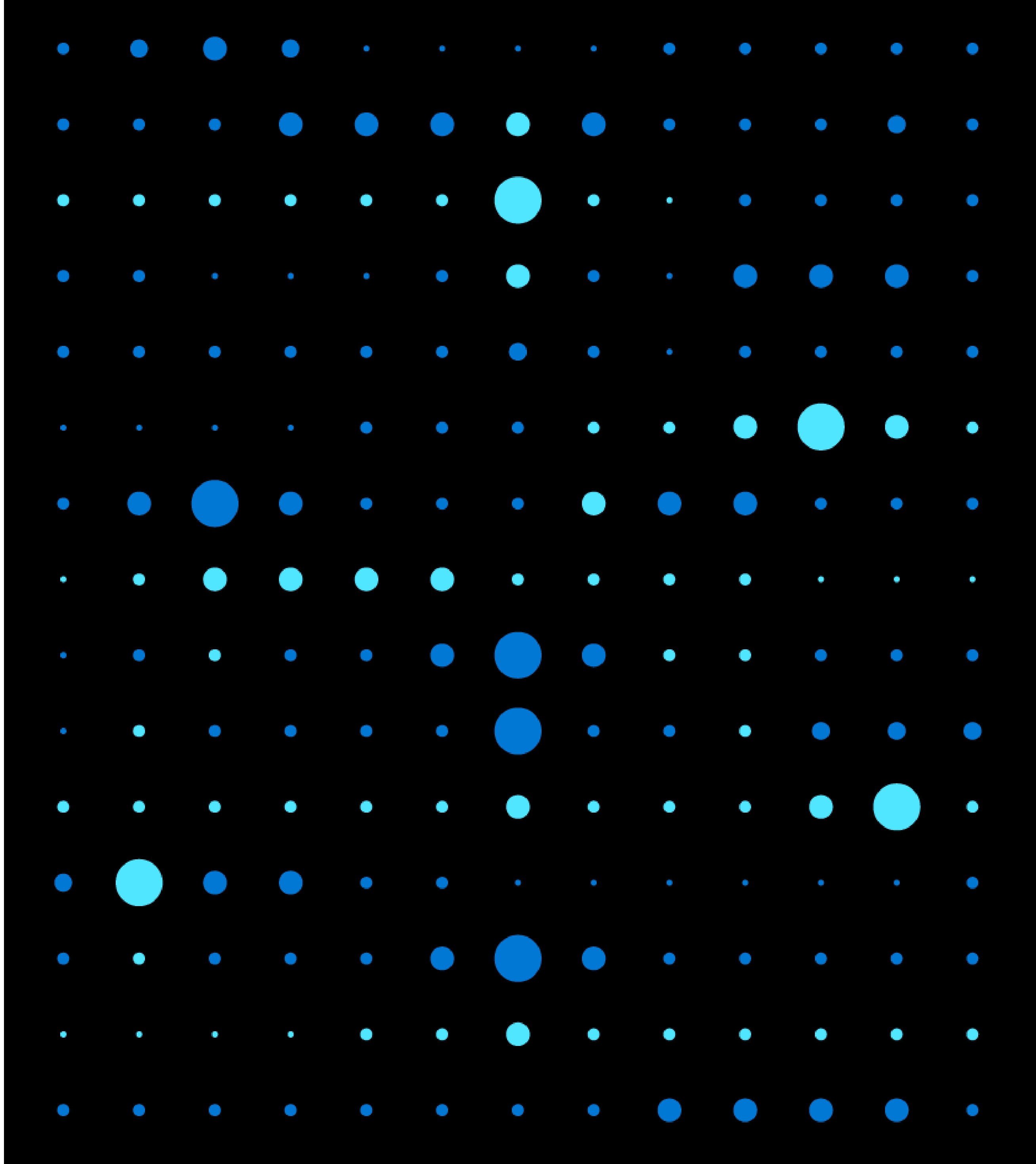
- Helps to enforce organizational standards and to assess compliance at-scale
- Provides an aggregated view to evaluate the overall state of the environment
- Helps to bring your resources to compliance through bulk remediation for existing resources and automatic remediation for new resources

Azure Blueprints

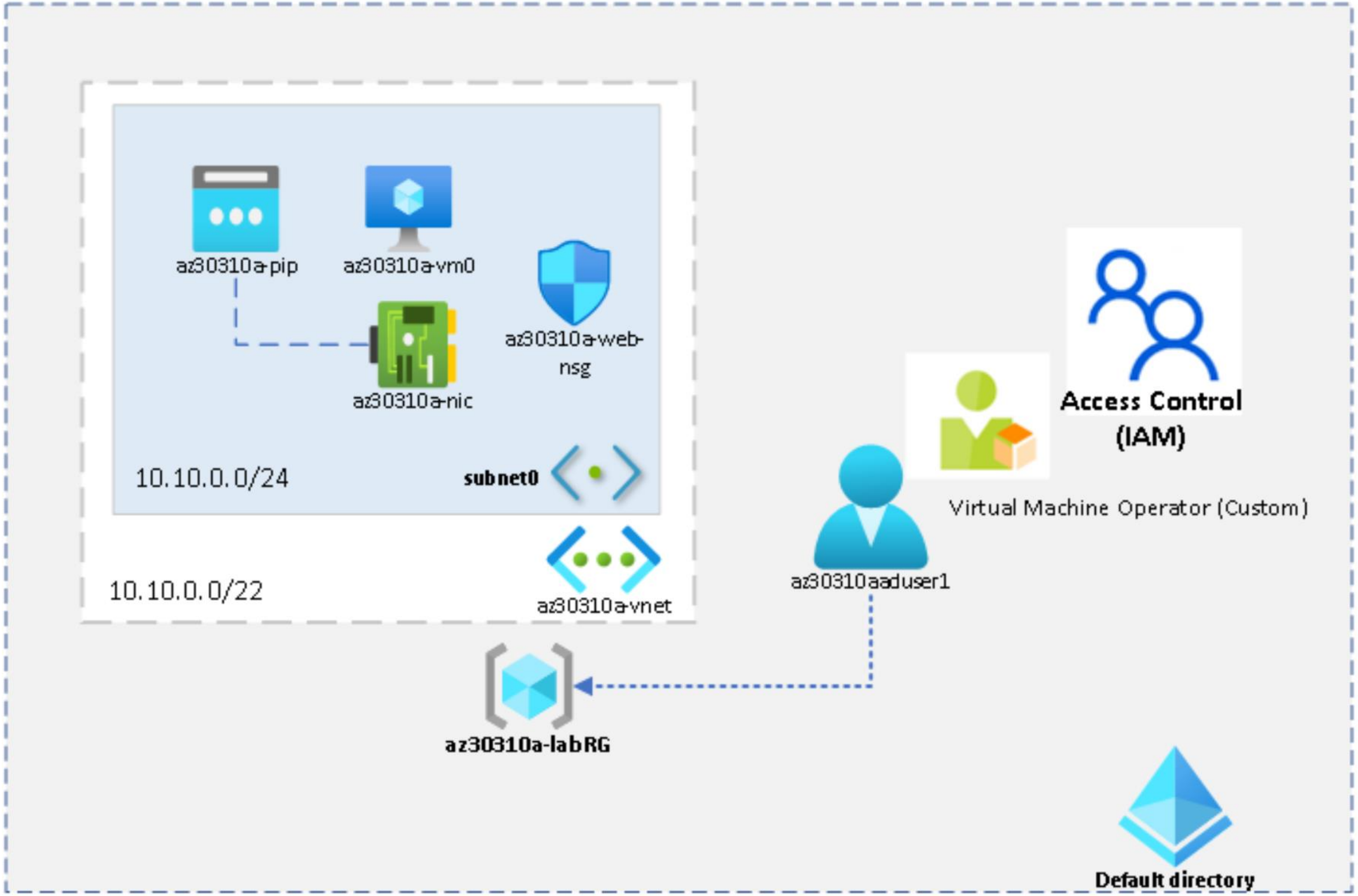
- Enables cloud architects and central information technology groups to define a repeatable set of Azure resources that implements and adheres to an organization's standards, patterns, and requirements
- Makes it possible for development teams to rapidly build and stand up new environments with trust they're building within organizational compliance

Demonstration: Create a Blueprint

- Create a blueprint



Lab: Managing Azure Role-Based Access Control



Module Review Questions

Microsoft Azure

Online Role-based training resources:

Microsoft Learn
https://docs.microsoft.com/en-us/learn/

Microsoft Azure

Thank you.