Governance and compliance

Sinuhé Díaz

rodolfo.diaz@wizeline.com

Sinuhé Díaz

- SWE Level 3
- 14+ of experience as fullstack and backend
- 4+ of experience with Azure

Important Notes

Identify yourself in Zoom, using your name and last name

Mute your microphone along the course unless you have questions

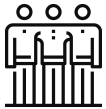
Raise the hand if you have questions during the session

Focus your questions on the presented topic

Turn off your camera in case of connection issues

DSA Code of Conduct

Be respectful, there are no bad questions or ideas.



Be welcoming and patient

Be careful in the words that you choose

Session Goal

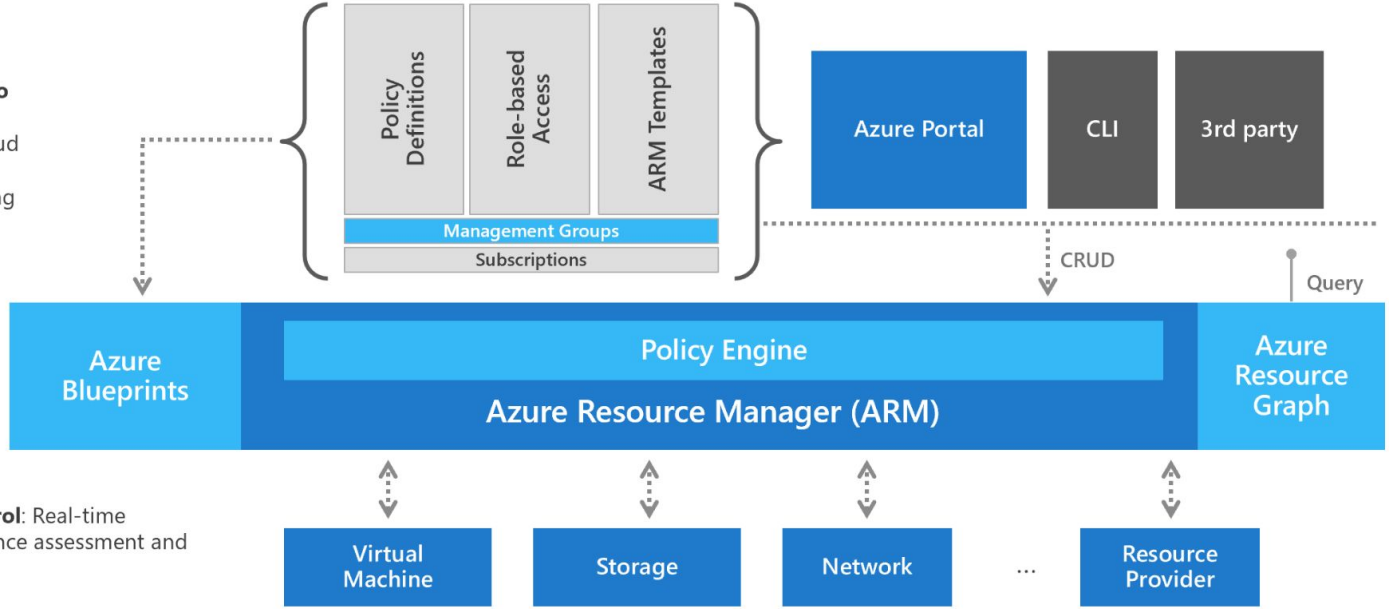
At the end of this session, you will be able to:

- Describe the purpose of cloud governance and compliance
- Identify the benefits to use cloud governance
- List the tools available to implement governance and compliance on Azure
- Define your own set of policies and how to implement them on your organization
- Discover sources of best practices for governance and compliance with examples ready to implement them on your organization

Table of Contents

Azure Governance Architecture

1. DevOps approach to Infrastructure:
Deploy and update cloud environments in a repeatable manner using composable artifacts



2. Policy-based Control: Real-time enforcement, compliance assessment and remediation at scale

3. Resource Visibility: Query, explore & analyze cloud resources at scale

Source: https://www.microsoft.com/en-us/us-partner-blog/2019/07/24/azure-governance/

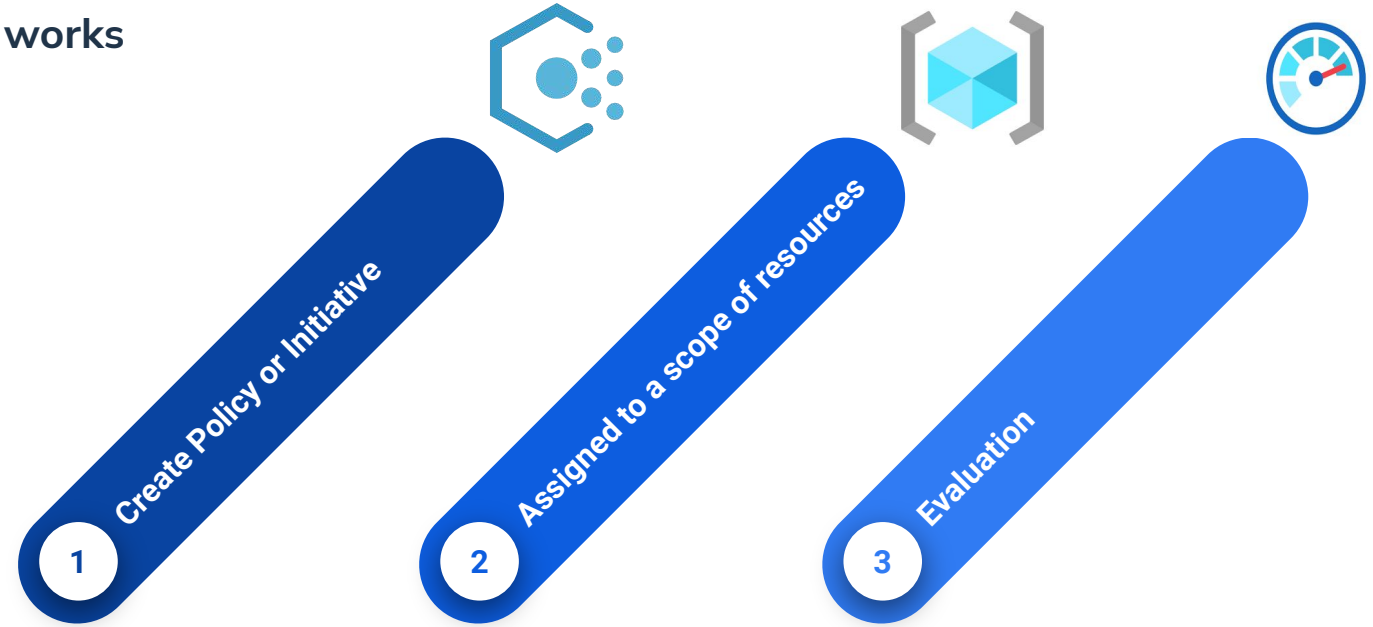
Azure Policy

Enforce settings and policies at scale

Key information

- ➔ Helps with governance, security, compliance and cost management
- ➔ Policy apply over resource properties (location, size, etc)
- ➔ Policy vs Initiative 1 vs N
- ➔ Build-in Policies - Library of already defined, common Policies
- ➔ Applied at time of creation of the resources
- ➔ Remediation (apply to existing resources)

How it works



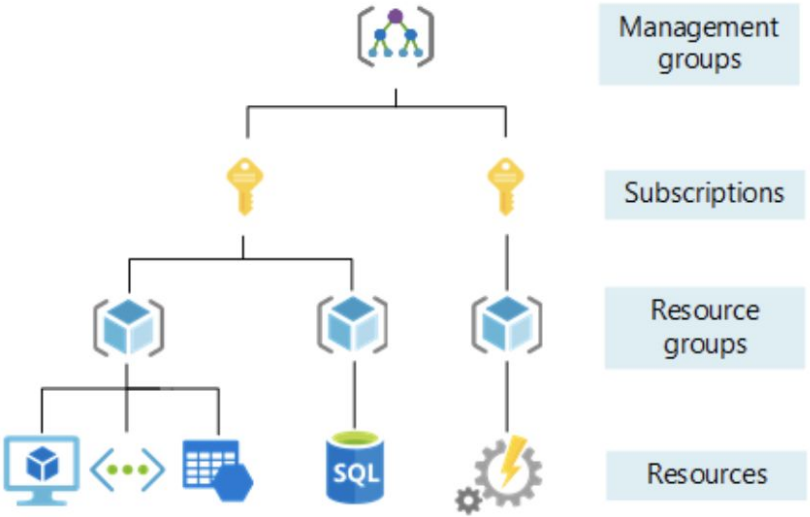
Create a Policy

- ➔ Parameters
- ➔ Rule
  - ◆ Evaluation
  - ◆ Effect

- ➔ Specify what to check
- ➔ Rule
  - ◆ Logical Evaluation
  - ◆ Result

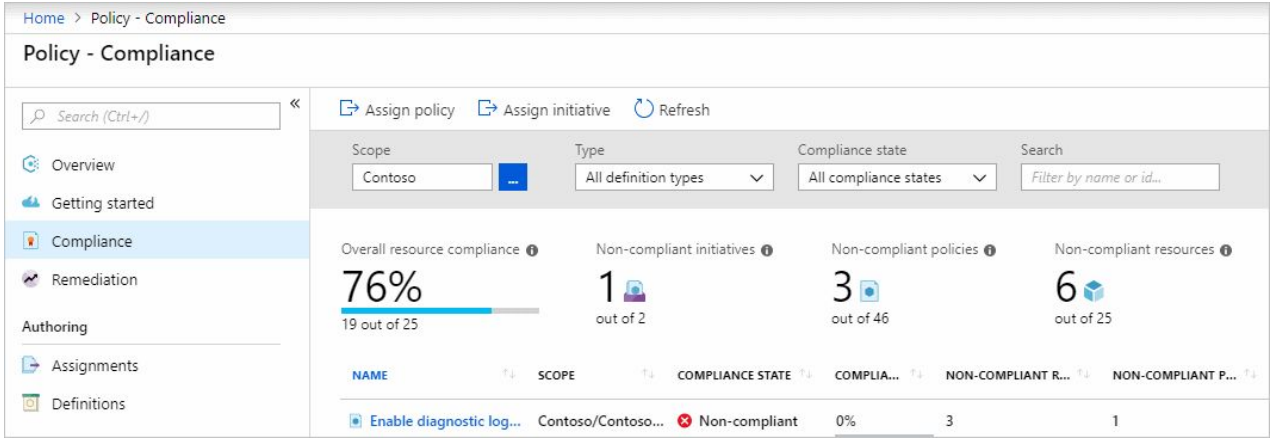
- ➔ Location of resource, list of allowed locations
- ➔ Rule
  - ◆ Location on of allowed location
  - ◆ If true, continue task, otherwise show error / stop task

Assigned to a scope of resources



Evaluation triggers

- ➔ A policy or initiative is newly assigned to a scope
- ➔ A policy or initiative already assigned to a scope is updated
- ➔ A policy exemption is created, updated, or deleted.
- ➔ Standard compliance evaluation cycle
- ➔ On-demand scan



Azure Blueprints

Enforce settings and policies at scale

Azure Blueprints

Helps you deploy and update your cloud environments in a repeatable manner using composable **artifacts**. Blueprints are a great way to accelerate the creation of your compliant environments!

Artifacts

- Resource Groups
- ARM template
- Policy Assignment
- Role Assignment

Blueprint definition

Resource		Description
1	Resource Groups	Create a new resource group for use by other artifacts within the blueprint. These placeholder resource groups enable you to organize resources exactly the way you want them structured and provides a scope limiter for included policy and role assignment artifacts and ARM templates.
2	ARM template	Templates, including nested and linked templates, are used to compose complex environments. Example environments: a SharePoint farm, Azure Automation State Configuration, or a Log Analytics workspace.
3	Policy Assignment	Allows assignment of a policy or initiative to the subscription the blueprint is assigned to. The policy or initiative must be within the scope of the blueprint definition location. If the policy or initiative has parameters, these parameters are assigned at creation of the blueprint or during blueprint assignment.
4	Role Assignment	Add an existing user or group to a built-in role to make sure the right people always have the right access to your resources. Role assignments can be defined for the entire subscription or nested to a specific resource group included in the blueprint.

Roles available

Azure role	Description
Owner	In addition to other permissions, includes all Azure Blueprints related permissions.
Contributor	In addition to other permissions, can create and delete blueprint definitions, but doesn't have blueprint assignment permissions.
Blueprint Contributor	Can manage blueprint definitions, but not assign them.
Blueprint Operator	Can assign existing published blueprints, but can't create new blueprint definitions. Blueprint assignment only works if the assignment is done with a user-assigned managed identity.

Resource locks

Prevents resources from being accidentally deleted or changed.

Locking modes and states

Mode	Artifact	State	Description
Don’t Lock	*	Not Locked	Resources aren't protected by Azure Blueprints. This state is also used for resources added to a Read Only or Do Not Delete resource group artifact from outside a blueprint assignment.
Read Only	Resource group	Cannot Edit / Delete	The resource group is read only and tags on the resource group can't be modified. Not Locked resources can be added, moved, changed, or deleted from this resource group.
Read Only	Non-resource group	Read Only	The resource can't be altered in any way. No changes and it can't be deleted.
Do Not Delete	*	Cannot Delete	The resources can be altered, but can't be deleted. Not Locked resources can be added, moved, changed, or deleted from this resource group.

Service Trust Portal

Access to best compliance practices

Service Trust Portal

You can access the service on this url https://servicetrust.microsoft.com/

The Service Trust Portal features and content are accessible from the main menu. The categories on the main menu are:

- Service Trust Portal provides a quick access hyperlink to return to the Service Trust Portal home page.
- My Library lets you save (or pin) documents to quickly access them on your My Library page. You can also set up to receive notifications when documents in your My Library are updated.
- All Documents is a single landing place for documents on the service trust portal. From All Documents, you can pin documents to have them show up in your My Library.

Q&A

Please answer the survey form of this session:

Thank you