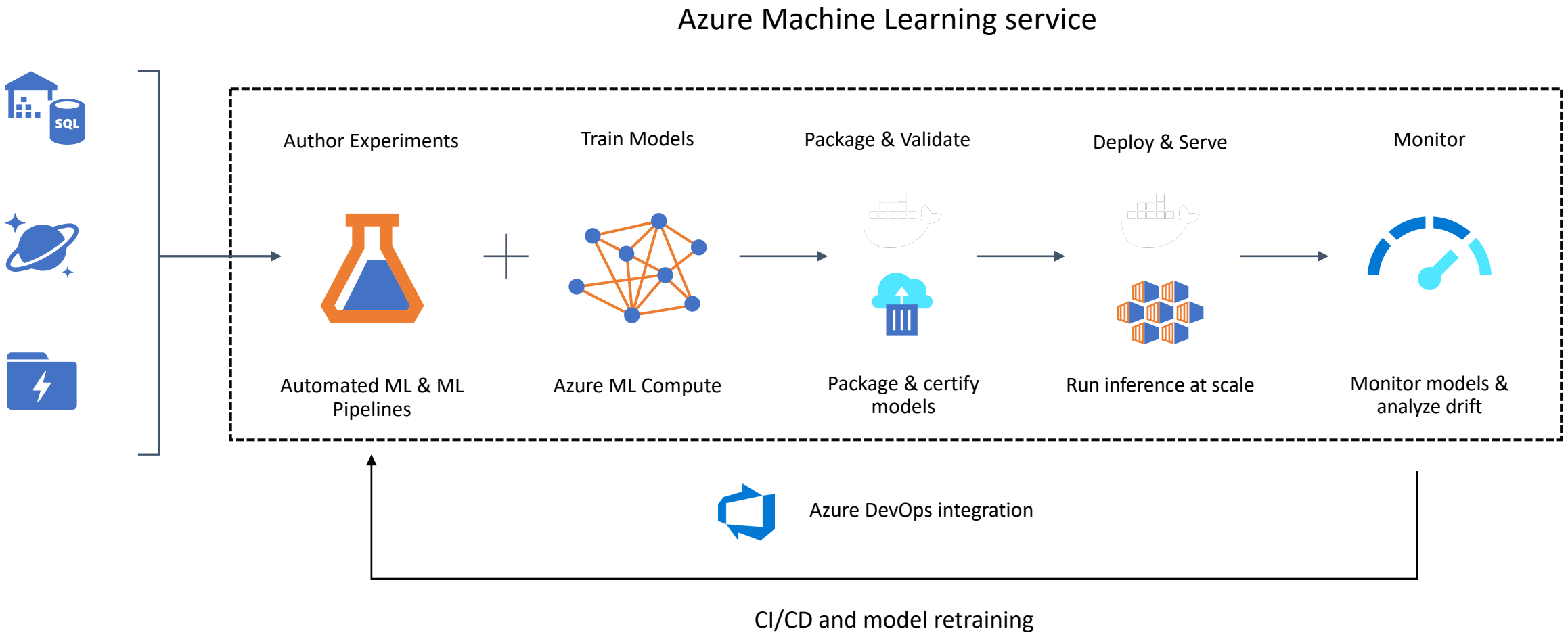
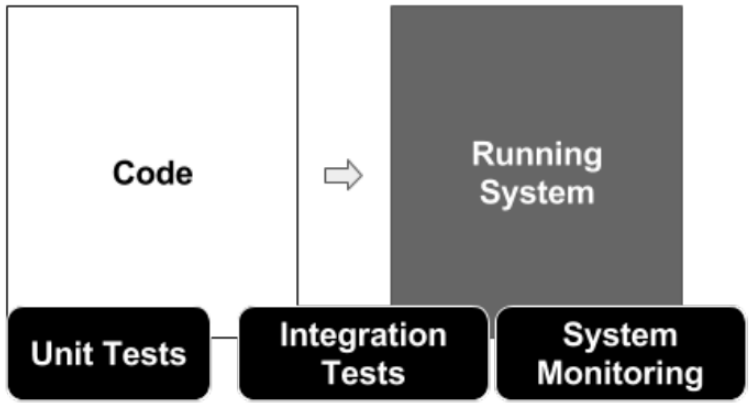
Azure Machine Learning MlOPs & RBAC

Mufajjul Ali
Alan Weaver

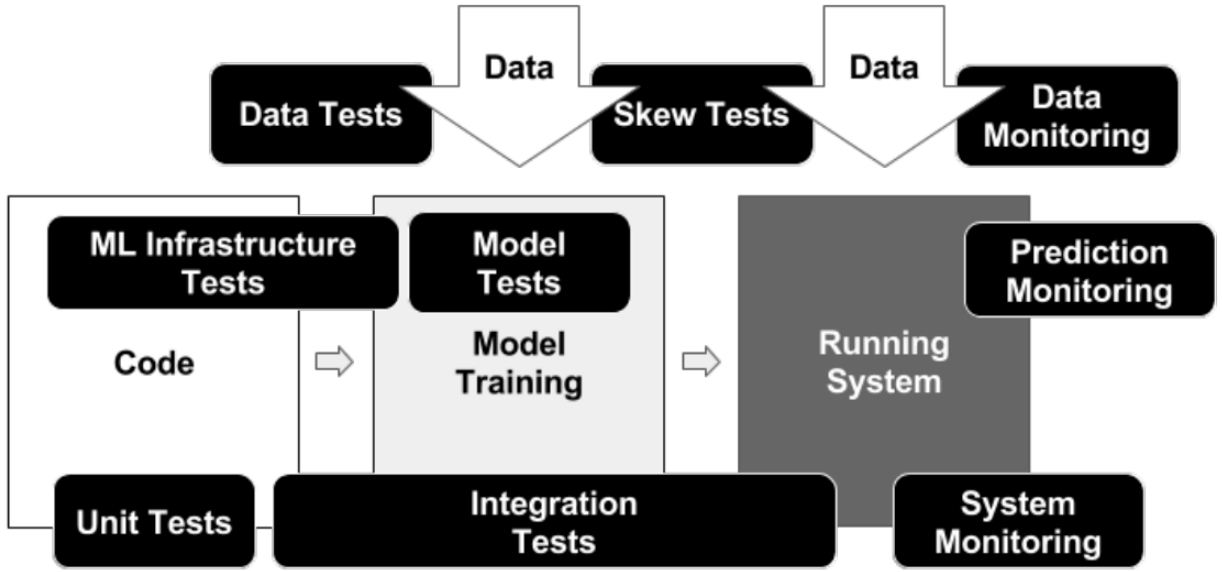
Bring ML models to production



Traditional vs. ML infused systems



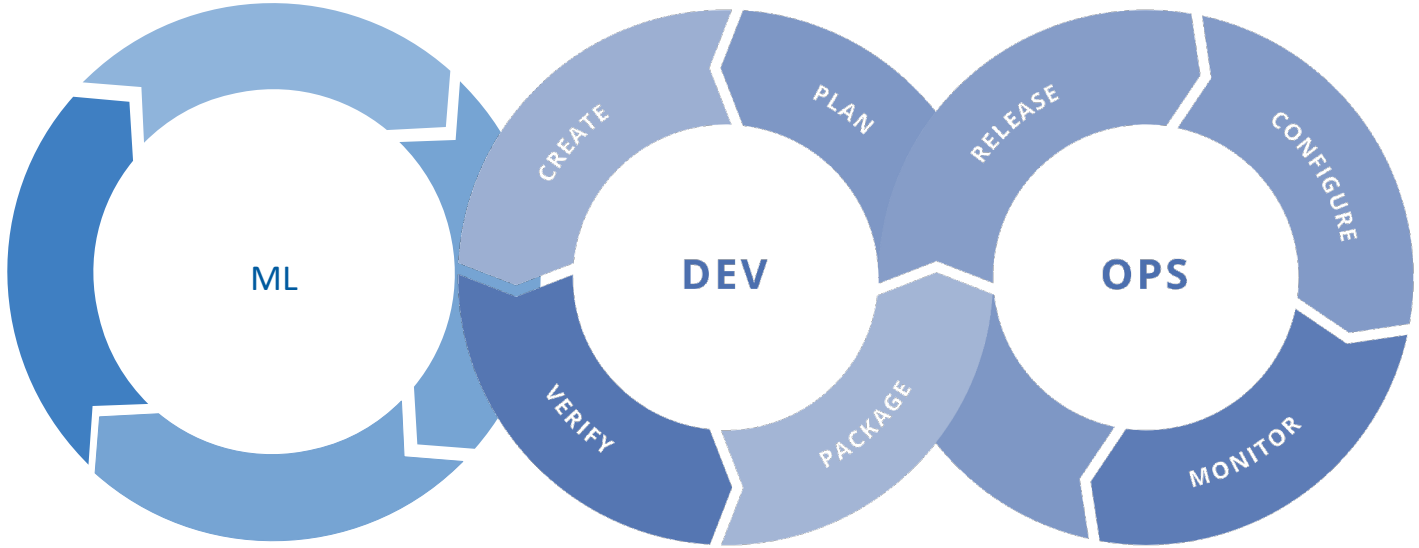
Traditional System Testing and Monitoring



ML-Based System Testing and Monitoring

MLOps = ML + DEV + OPS

Help bring models to production



Experiment

Data Acquisition
Business Understanding
Initial Modeling

Develop

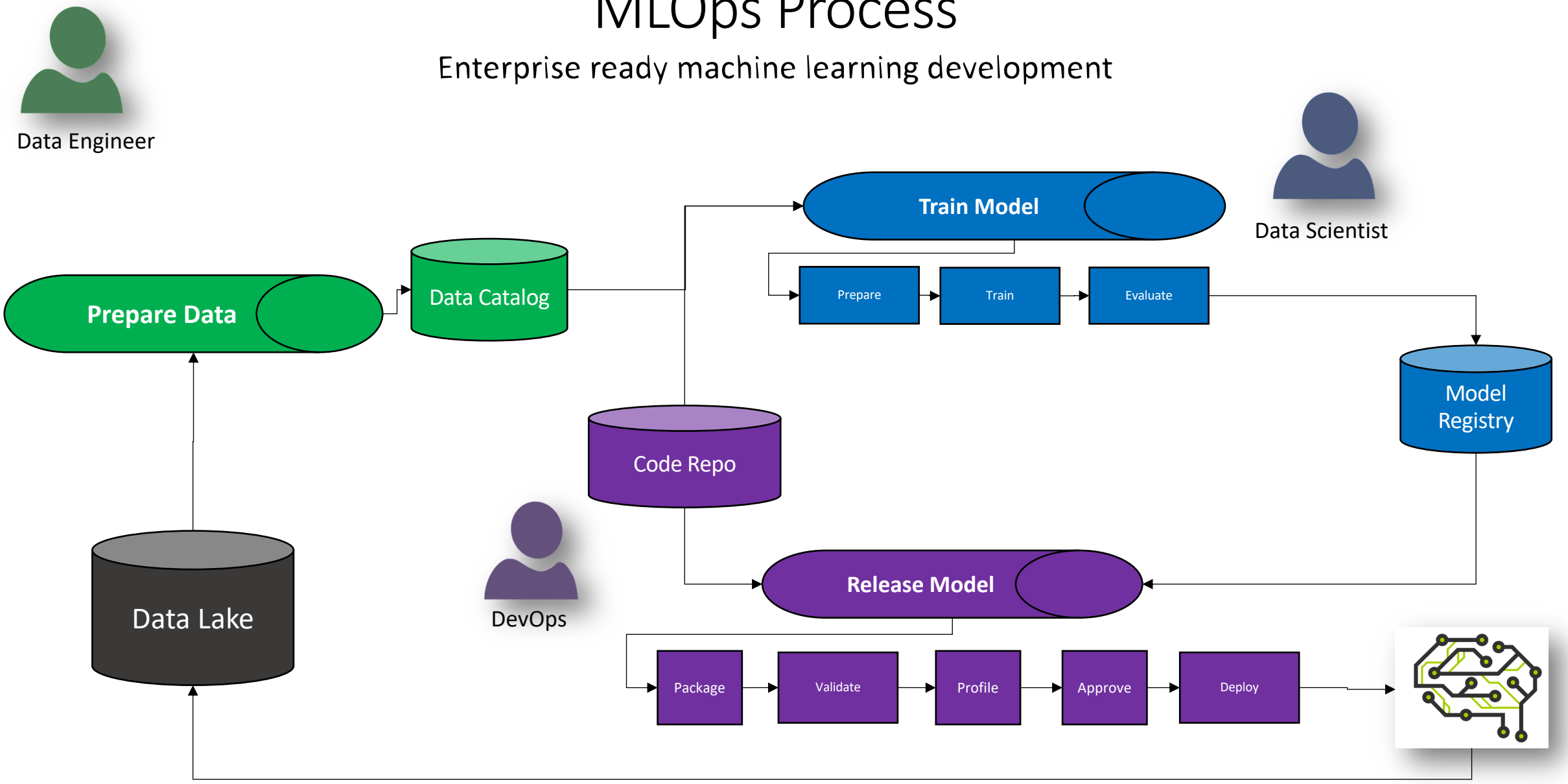
Modeling + Testing
Continuous Integration
Continuous Deployment

Operate

Continuous Delivery
Data Feedback Loop
System + Model Monitoring

MLOps Process

Enterprise ready machine learning development



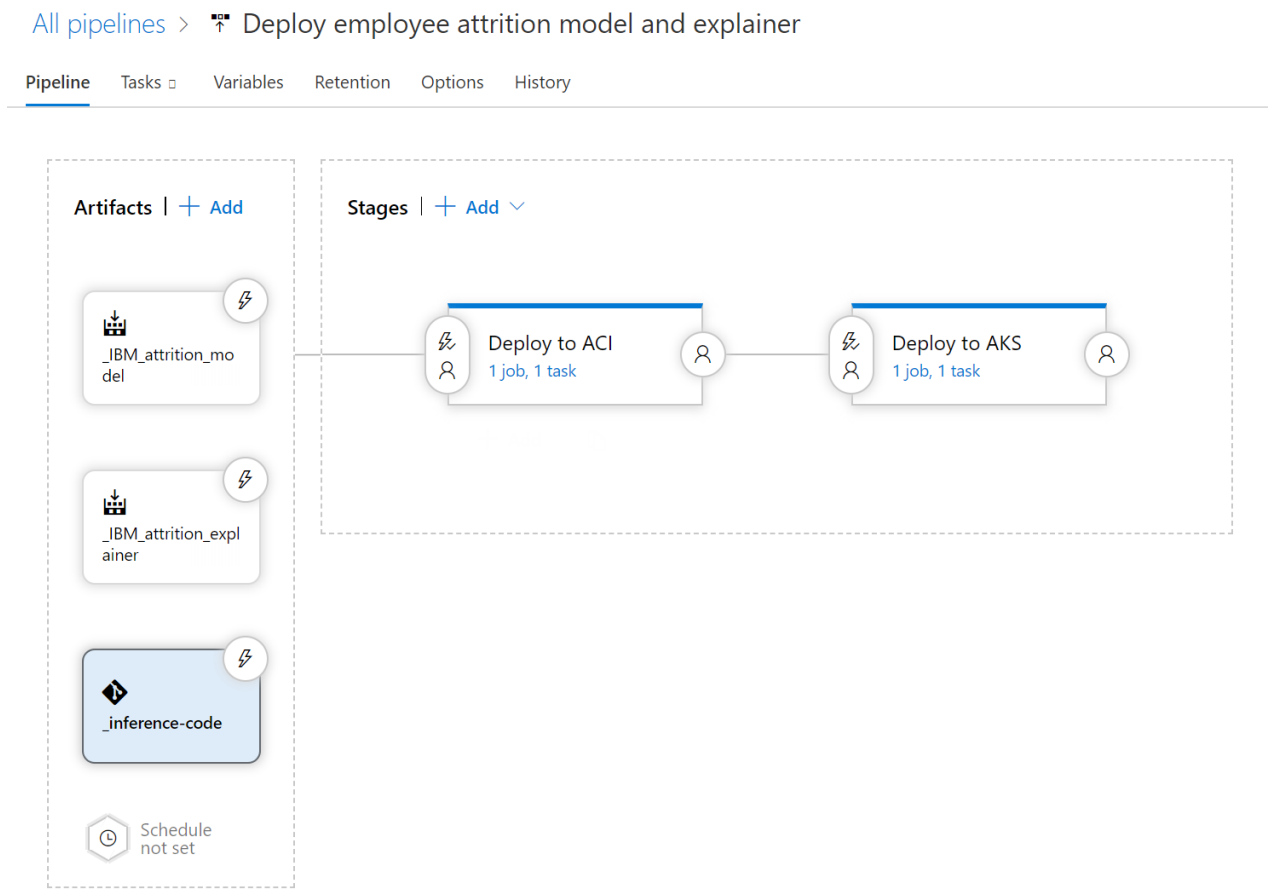
Automate model deployment with Azure DevOps

Trigger release on:

New model(s) available

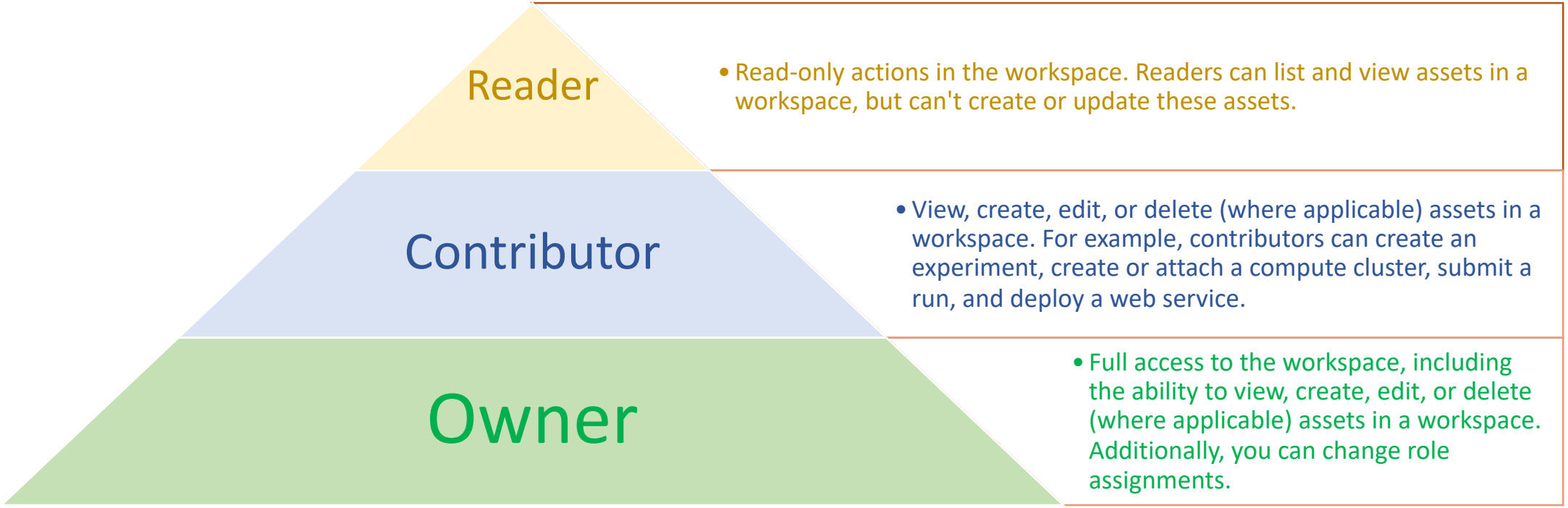
New inference code

New base image / dependencies available



Standard RBAC in AML

Role – Defines a collection of permissions



Advance RBAC in AML

Control Plane

- Workspace operations (like create, upgrade Edition)
- Compute operations (like create, update, delete)

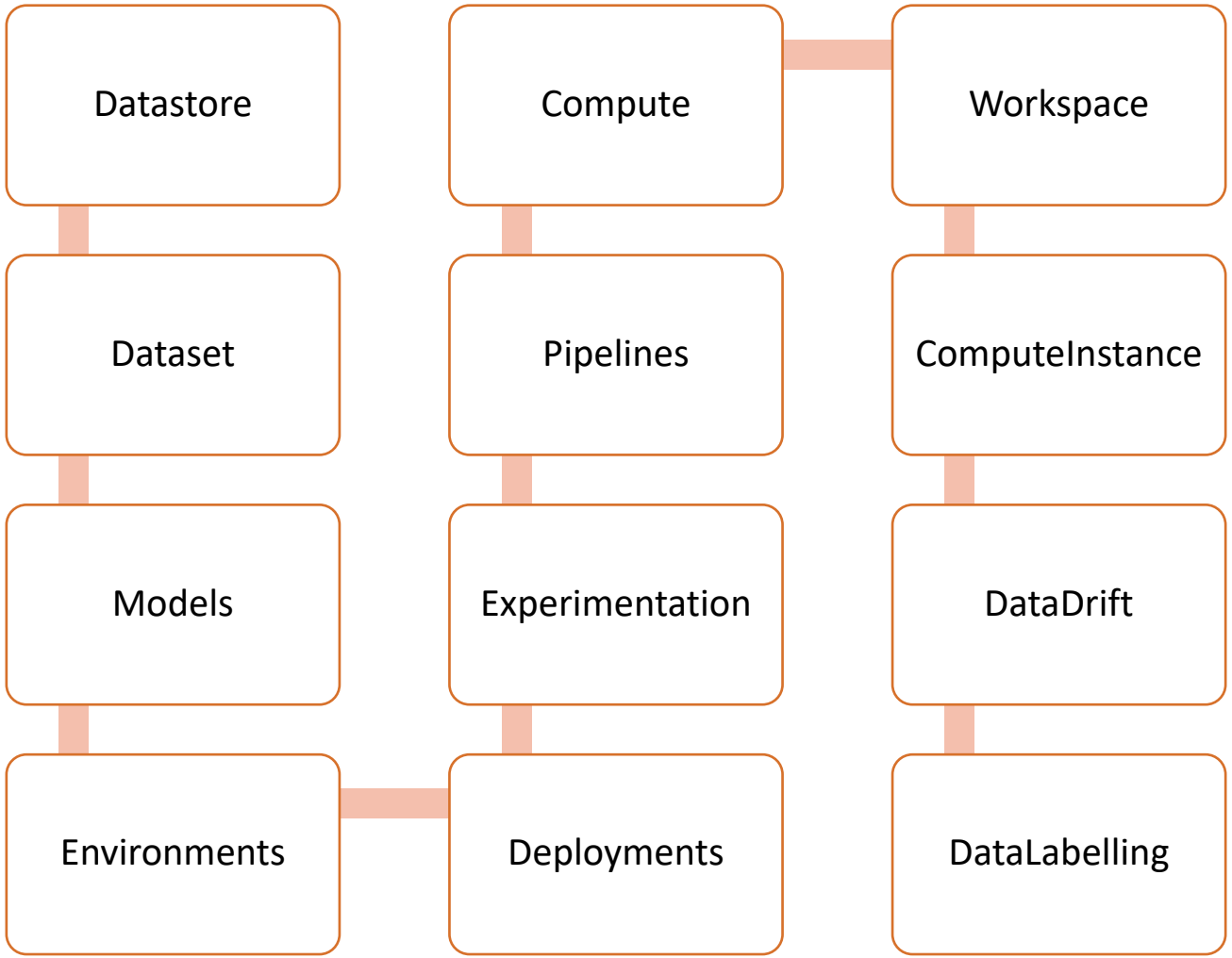
Data Plane

- Controlling experimentation, deployment, pipelines and data

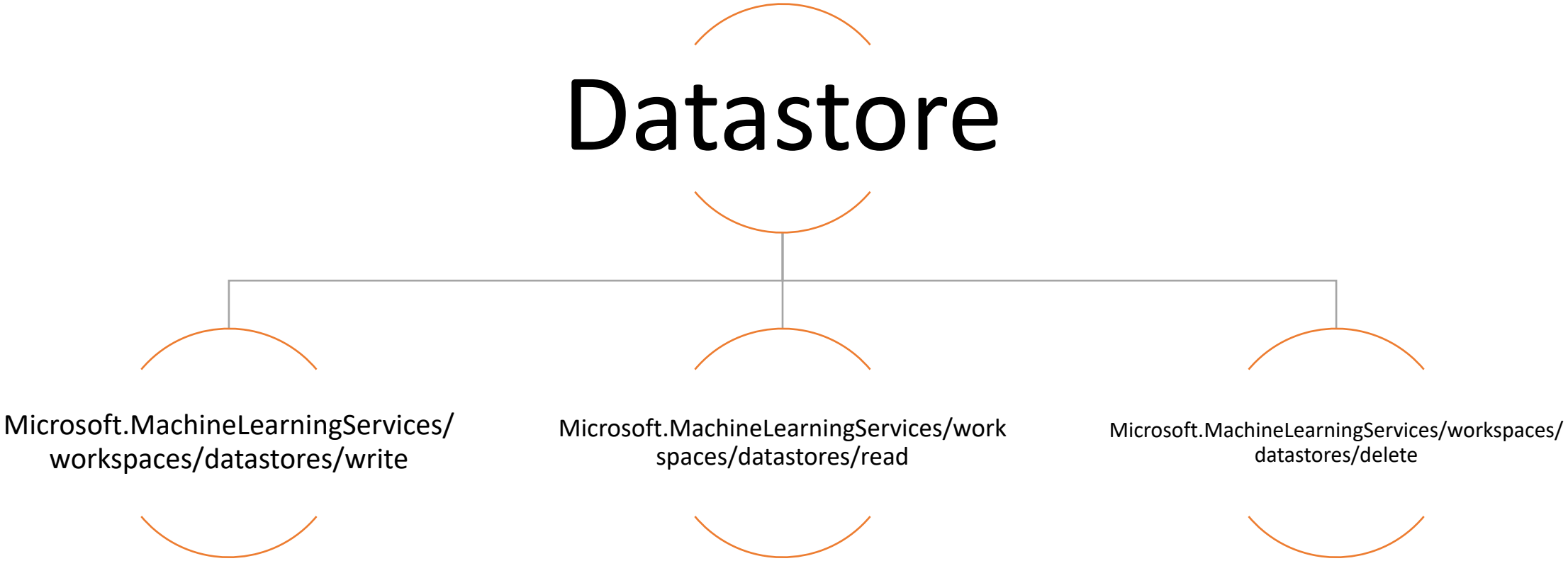
Studio also supports RBAC out of the box

- UX operations will show/hide button based on your role

Component Level RBAC



Example of Permissions



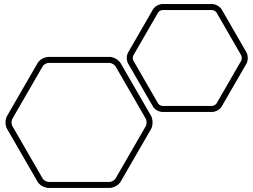
Out of the box roles

Technical Roles

- Data Scientist
- Data Scientist Super User
- Office Data Scientist

Operational Roles

- IT Admin
- Workspace Admin
- Subscription Admin



Data Scientist

Allowed

Able to create experiment and submit runs

Able to deploy to an ACI but not to a PROD aks cluster

Able to create a draft pipeline but not publish a pipeline endpoint

Able to complete a Hyperdrive or an AutoML run

Able to register datastores and datasets

Can view workspace and subscription level quota allocated for that workspace

Can do all data plane operations within the workspace that are part of a data scientists lifecycle

Not Allowed

Not able to create a compute instance or a training cluster

Not able to upgrade the workspace

Cannot create a new workspace but can use an existing workspace created by the subscription admin

Cannot create new roles or assign users any roles within that workspace

Data Scientist Super User

Allowed

Able to do all operations in the workspace

Able to add new users to the workspace against a pre-created role or a custom role, but not create a new role

Not Allowed

Not able to allocate workspace level quota

Not able to update the Edition of the workspace

Office Data Scientist

Allowed

Start, stop, and restart Notebook VMs

Access the Azure ML workspace portal and see experiments, pipelines, computes, models and deployments.

Create, publish, clone, and delete experiments and pipelines

Run pipelines from SDK and portal

Download log files and statistics

Register and unregister models

List, read and write on any registered datastore

List, read, register and unregister datasets

Not Allowed

Create, update, or delete an AML workspace

Create, update, or delete a Notebook VM

Create, update, delete, or attach computes

Deploy models to any service other than single node AKS cluster

Register/Unregister datastores

Update any type of roles

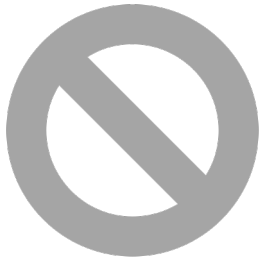
IT Admin

Allowed

Can create workspace and update Editions of the workspace

Can set workspace level quota

Same as sub level admin (owner)



Not Allowed

Rest are not allowed

Workspace Admin

Allowed

Can create a new workspace and also use an existing workspace created by the subscription admin

Can view workspace and subscription level quota allocated for that workspace

Can create new compute within the bounds of the workspace level quota that the sub admin set on their workspace

Can do all data plane operations within the workspace that are part of a data scientists lifecycle

Can create a compute instance and assign it to a specific data scientist as a personal compute instance

Not allowed

Cannot create new roles but can assign users specific roles within that workspace

Custom Roles

- Can be any combination of data or control plane actions
- Useful for creating scoped roles to a specific action like an MLOps Engineer.

```
[
  {
    "assignableScopes": [
      "/subscriptions/{subscriptionId1}",
      "/subscriptions/{subscriptionId2}",
      "/providers/Microsoft.Management/managementGroups/{groupId1}"
    ],
    "description": "Can monitor and restart virtual machines.",
    "id": "/subscriptions/{subscriptionId1}/providers/Microsoft.Authorization/roleDefinitions/88888888-
    "name": "88888888-8888-8888-8888-888888888888",
    "permissions": [
      {
        "actions": [
          "Microsoft.Storage/*/read",
          "Microsoft.Network/*/read",
          "Microsoft.Compute/*/read",
          "Microsoft.Compute/virtualMachines/start/action",
          "Microsoft.Compute/virtualMachines/restart/action",
          "Microsoft.Authorization/*/read",
          "Microsoft.ResourceHealth/availabilityStatuses/read",
          "Microsoft.Resources/subscriptions/resourceGroups/read",
          "Microsoft.Insights/alertRules/*",
          "Microsoft.Insights/diagnosticSettings/*",
          "Microsoft.Support/*"
        ],
        "dataActions": [],
        "notActions": [],
        "notDataActions": []
      }
    ],
    "roleName": "Virtual Machine Operator",
    "roleType": "CustomRole",
    "type": "Microsoft.Authorization/roleDefinitions"
  }
]
```

Any Questions