Microsoft

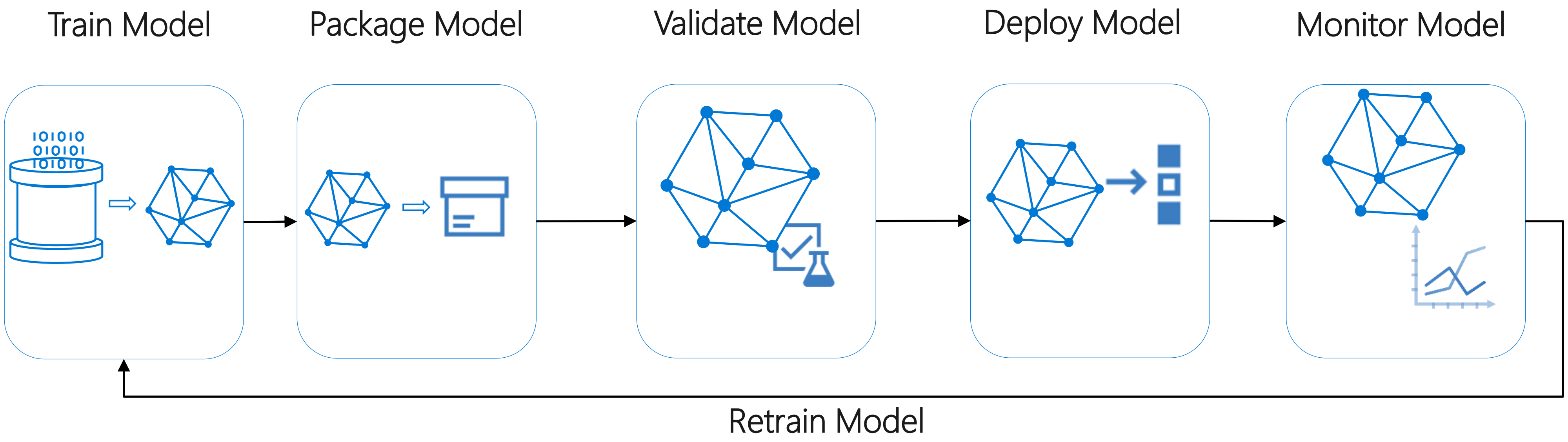
Understanding enterprise readiness for machine learning solutions

Aashish Bhateja (Microsoft)
Senior Program Manager

Quick intro to Azure Machine Learning

What does the Machine Learning Lifecycle look like?

- **Develop & train model** that solves a real business problem
- **Package model** so you can use it somewhere else
- **Validate model behavior –** functionally, in terms of responsiveness, in terms of regulatory compliance
- **Deploy model –** use the model to make predictions
- **Monitor model** behavior & business value, know **when to replace / deprecate a stale model**



Machine Learning on Azure

Domain specific pretrained models To reduce time to market	Vision	Speech	Language	Search
Familiar Data Science tools To simplify model development	PyCharm	Jupyter	Visual Studio Code	Command line
Popular frameworks To build advanced deep learning solutions	Pytorch	TensorFlow	Scikit-Learn	Onnx
Productive services To empower data science and development teams	Azure Databricks	Azure Machine Learning		Machine Learning VMs
Powerful infrastructure To accelerate deep learning	CPU	GPU		FPGA

From the Intelligent Cloud to the Intelligent Edge

What is Azure Machine Learning service?

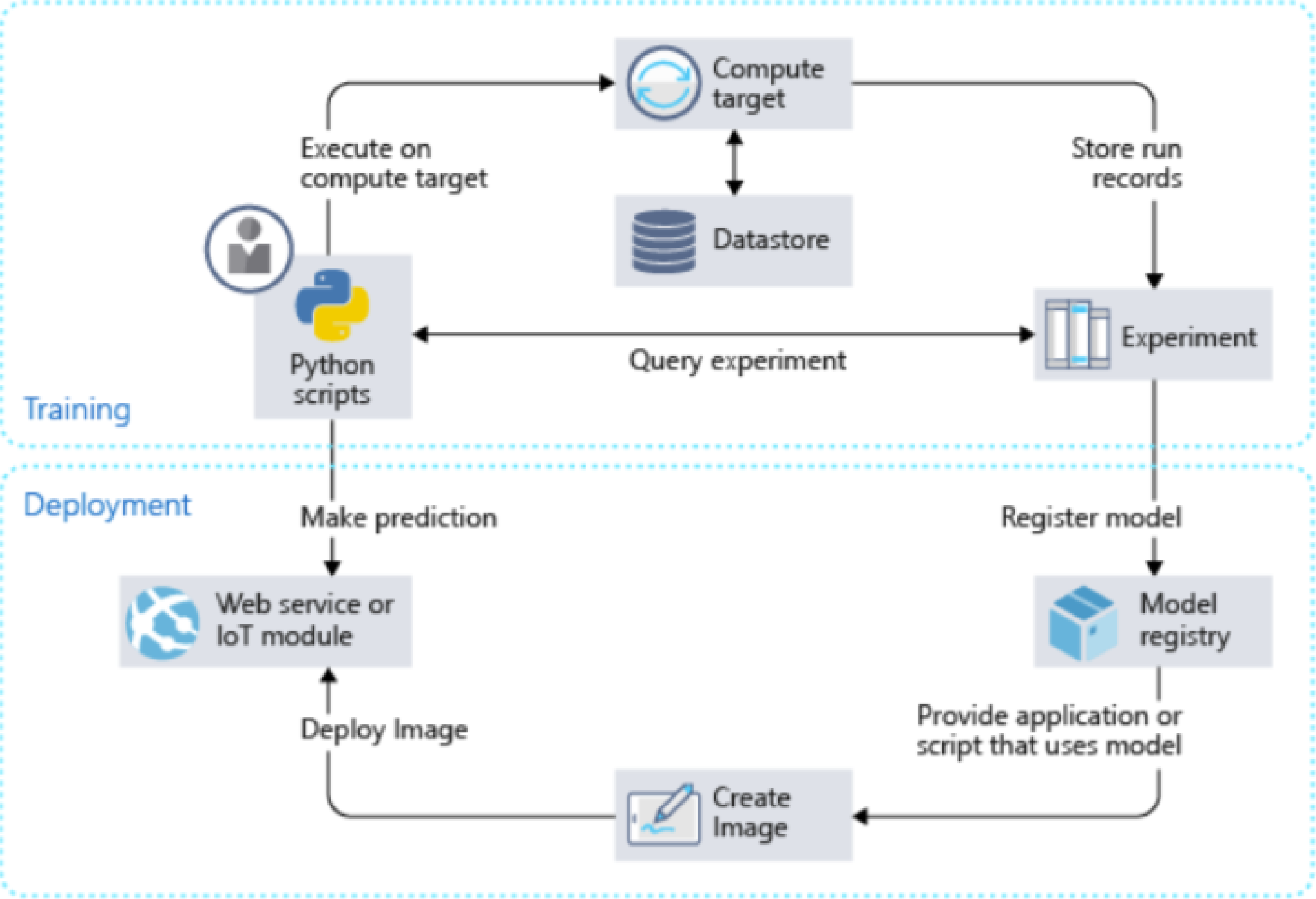
Set of Azure Cloud Services + Python SDK

That enables you to:

- ✓ Prepare Data
- ✓ Build Models
- ✓ Train Models

- ✓ Manage Models
- ✓ Track Experiments
- ✓ Deploy Models

Implement ML Lifecycle with Azure ML service



Workflow Steps

Develop machine learning training scripts in **Python**.

Create and configure a **compute target**.

Submit the scripts to the configured compute target to run in that environment. During training, the compute target stores run records to a **datastore**. Records pf execution are saved as **runs** in the **workspace** and grouped under **experiments**.

Query the experiment for logged metrics from the current and past runs. If the metrics do not indicate a desired outcome, loop back to step 1 and iterate on your scripts.

Once a satisfactory run is found, register the persisted model in the **model registry**.

Develop a scoring script.

Create an Image and register it in the **image registry**.

Deploy the image as a **web service** in Azure.

Azure ML service

Key Artifacts

Workspace

- Models
- Experiments
- Pipelines
- Compute Target
- Images
- Deployment
- Data Stores

Enterprise Readiness for Azure Machine Learning

Enterprise requirements for ML

ACCESS CONTROLS

EASE OF SETUP

REDUCE TIME TO MARKET

SECURELY RUN EXPERIMENTS

END TO END DATA ENCRYPTION

MANAGE COSTS

UNDERSTAND LINEAGE

MONITOR AND SET ALERTS

Being Enterprise Ready

Security

Cost Efficiency

Automate

Security

- Authentication
- Authorization
- Network security
- Data encryption
- Monitoring

Authentication

- AML Workspace Authentication
  - Interactive Login Authentication
  - Azure CLI Authentication
  - Managed Service Identity (MSI) Authentication
  - Service Principal Authentication
- Managed VM Authentication
  - AAD
- Managing Runs
  - SSH into AML Compute nodes
  - Passing secrets during runs
- Scoring endpoint Authentication
  - Token or Key based auth for AKS; Key based auth for ACI

Workspace roles and scope

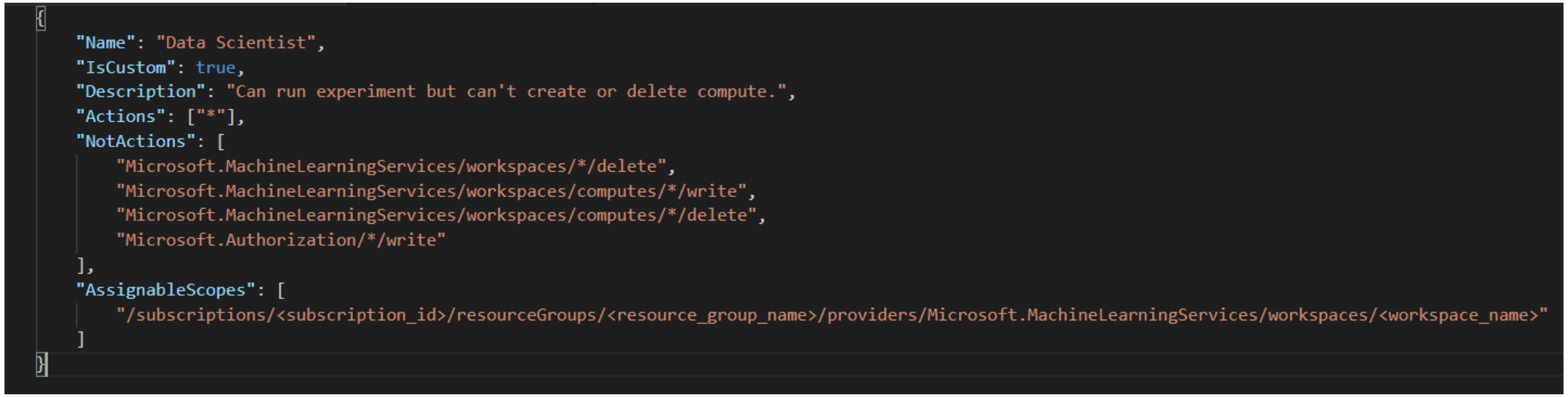
Built-in ML roles

- Data Scientist
- ML Ops
- Data Scientist Super User

Standard Azure roles

- Owner
- Contributor
- Reader

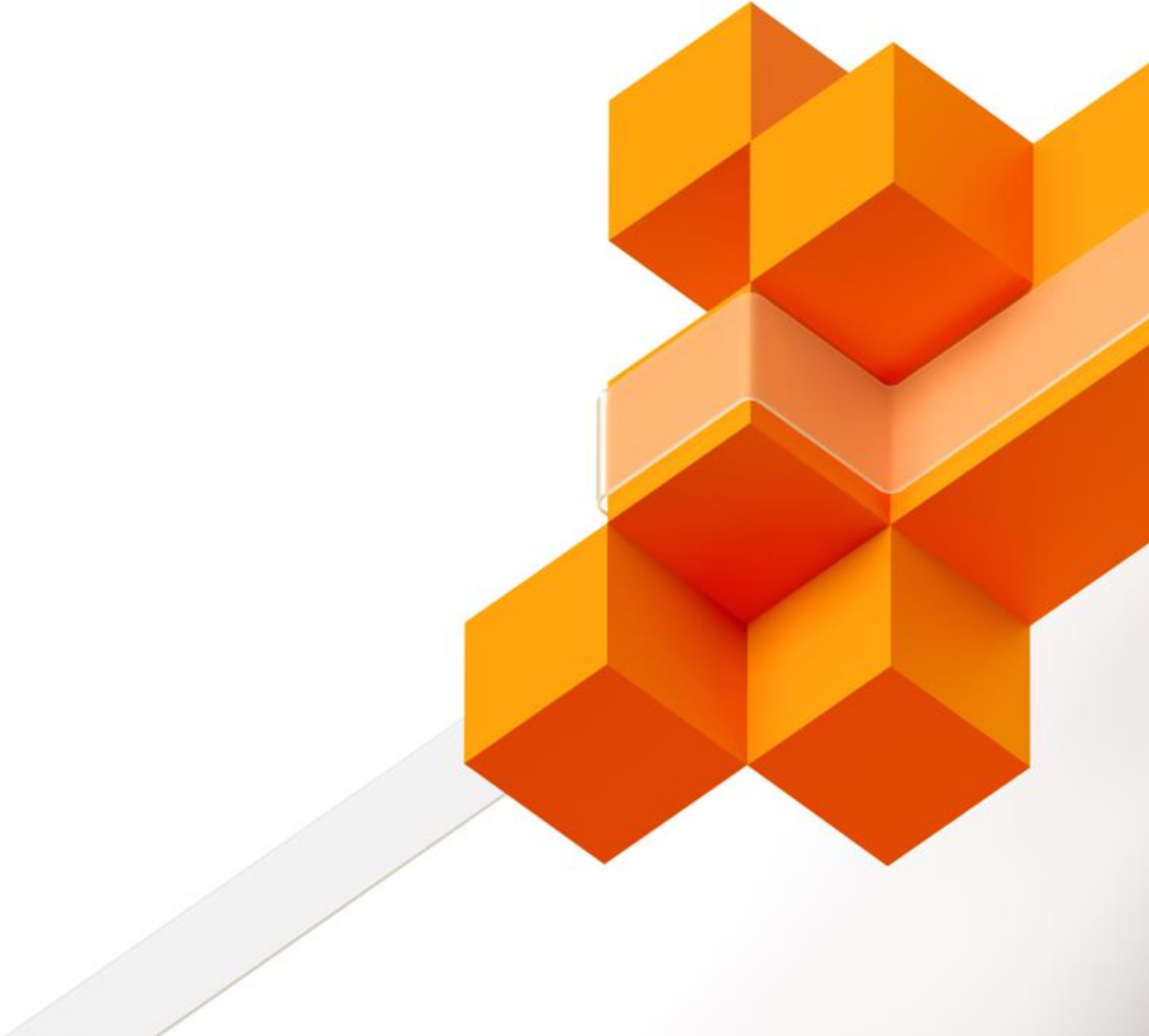
Custom role



```json
{
    "Name": "Data Scientist",
    "IsCustom": true,
    "Description": "Can run experiment but can't create or delete compute.",
    "Actions": ["*"],
    "NotActions": [
        "Microsoft.MachineLearningServices/workspaces/*/delete",
        "Microsoft.MachineLearningServices/workspaces/computes/*/write",
        "Microsoft.MachineLearningServices/workspaces/computes/*/delete",
        "Microsoft.Authorization/*/write"
    ],
    "AssignableScopes": [
        "/subscriptions/<subscription_id>/resourceGroups/<resource_group_name>/providers/Microsoft.MachineLearningServices/workspaces/<workspace_name>"
    ]
}
```

Demo (RBAC)

Aashish Bhateja



Data Security

Encryption at rest

- Azure Blob Storage: snapshots, outputs, logs in attached storage account (your or service keys)
- Azure Container Registry
- Cosmos DB: job metadata and metrics (managed by service)
- Machine Learning Compute VM images (service keys)

Encryption in transit

- All internal Azure ML service traffic encrypted
- Enable SSL using your cert or a cert provided by Microsoft

Azure Key Vault

- Connection Strings to data stores
- Secrets for remote runs
- Passwords to Azure Container Repository instances

Network Security

Secure Training

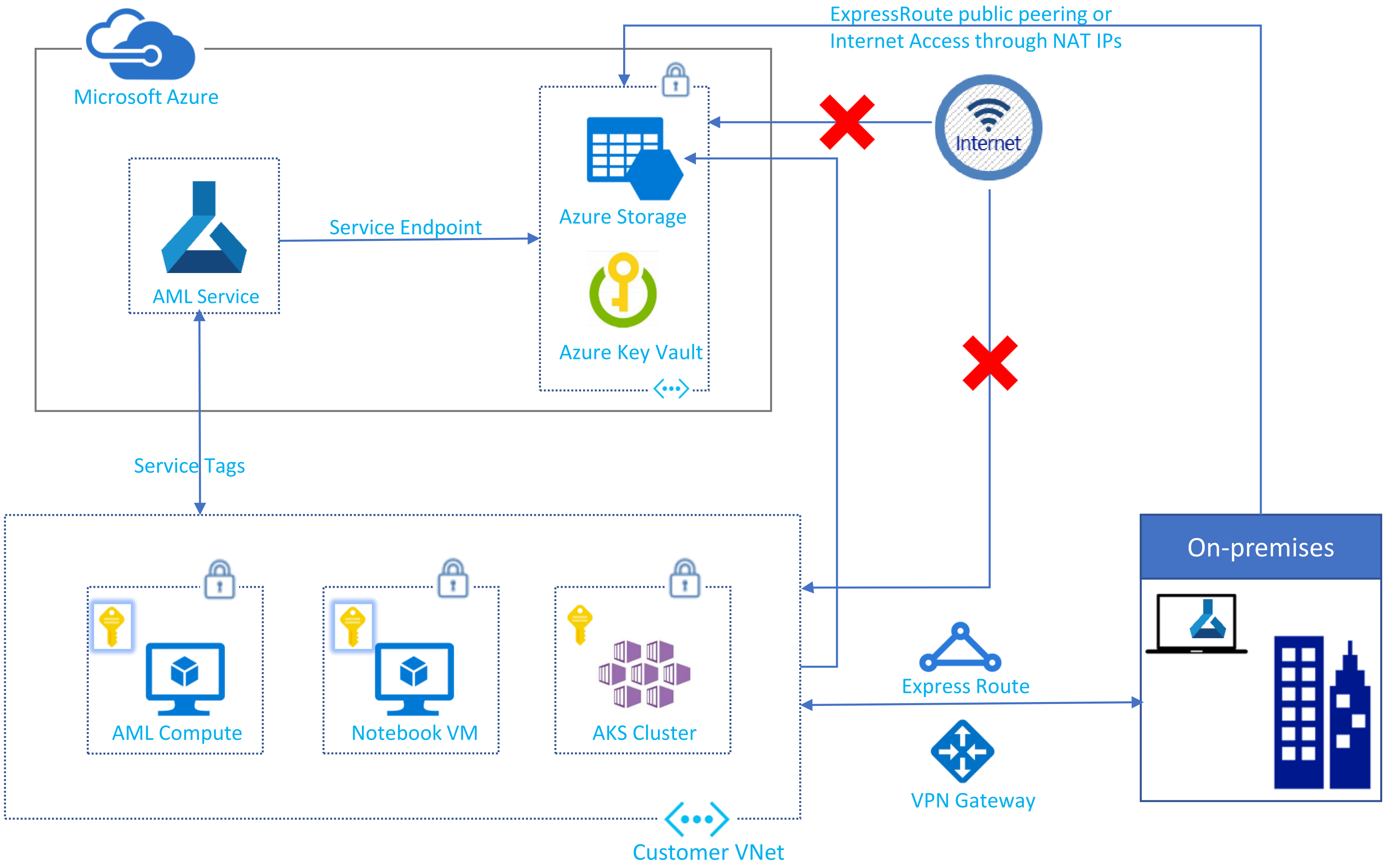
- AML Compute
- Blob Storage
- Key Vault

Secure Inference

- AKS Cluster
- Blob Storage

Managed notebook VM

Network Security



Demo (Virtual Networks)

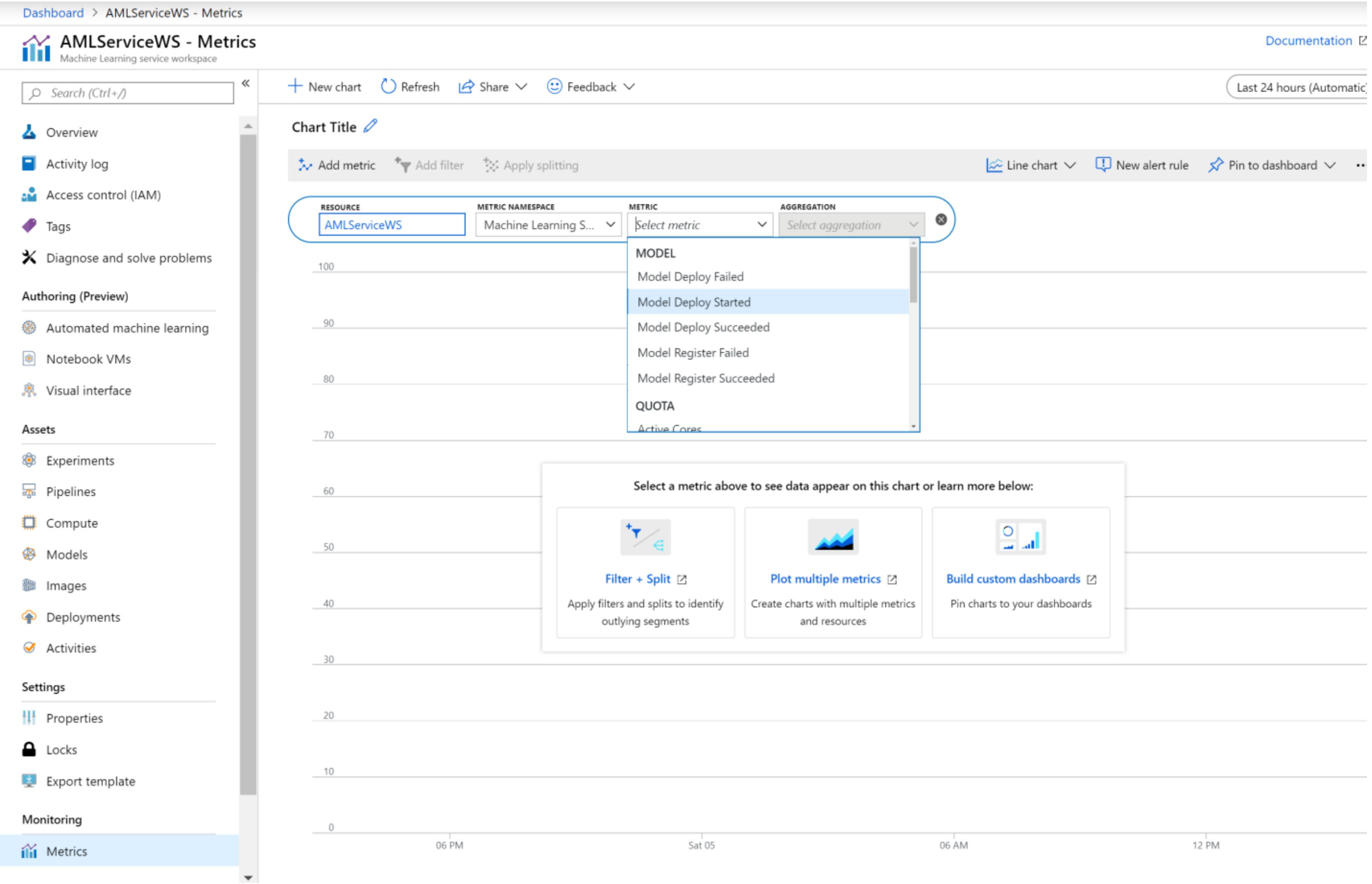
Aashish Bhateja

Monitoring

Azure Monitor

AppInsights for scoring requests

Activity log for Workspace



Dashboard > AMLServiceWS - Metrics

AMLServiceWS - Metrics
Machine Learning service workspace

Chart Title

RESOURCE: AMLServiceWS

METRIC NAMESPACE: Machine Learning S...

METRIC: Select metric

AGGREGATION: Select aggregation

MODEL
Model Deploy Failed
Model Deploy Started
Model Deploy Succeeded
Model Register Failed
Model Register Succeeded
QUOTA
Active Cores

Select a metric above to see data appear on this chart or learn more below:

Filter + Split
Apply filters and splits to identify outlying segments

Plot multiple metrics
Create charts with multiple metrics and resources

Build custom dashboards
Pin charts to your dashboards

Demo (Azure Monitor)

Aashish Bhateja

Cost Management

- Automatic resource management
  - Auto-scaling compute clusters (clusters can scale to zero after user defined timeout)
  - Max limits on run time
  - Early termination policy in Hyperparameter tuning/Automated ML runs

- Leveraging price discounts
  - Low Priority pre-emptable compute for some workloads
  - Reserved instance support for dedicated capacity

- Resource usage and cost reporting
  - Ability to set alerts on low utilization
  - Ability to set limits on usage on entire subscription and for a workspace

Automation

- REST APIs allow you to develop clients that use REST calls to work with the service
- Provide flexibility in automating your machine learning activities such as submitting an experiment
- Super critical for Infra as Code (IaC) scenarios like MLOps

Enterprise Readiness Roadmap

RBAC	• Role based access for workspace resources
Encryption	• AML Compute disk encryption for local SSD
Network Security	• VNet for workspace, ACR, and Notebook VMs • Private IPs (AML Compute nodes, Notebook VMs) • Limit scoring endpoint access within the VNet
AML Compute	• Auto patching • Workspace move
Auth	• Managed identity for AML Compute and ACI • AAD for scoring endpoint
Azure Monitor	• Metrics for various AML feature areas like AML Compute and inference
Audit Trail	• Trail of actions a user has performed on the workspace

Questions?