

The background features a vibrant blue gradient with subtle, wavy horizontal lines. In the bottom right corner, there are abstract, flowing shapes in shades of purple, pink, and orange. The AWS logo is positioned on the left, followed by the word 'SUMMIT' in a large, bold, sans-serif font.

# aws SUMMIT

INDIA | MAY 25, 2023

AIML008

# AI governance, security, collaboration with Amazon SageMaker - New features

Sudhanshu Hate

Principal AI & ML Specialist Architect  
AWS India



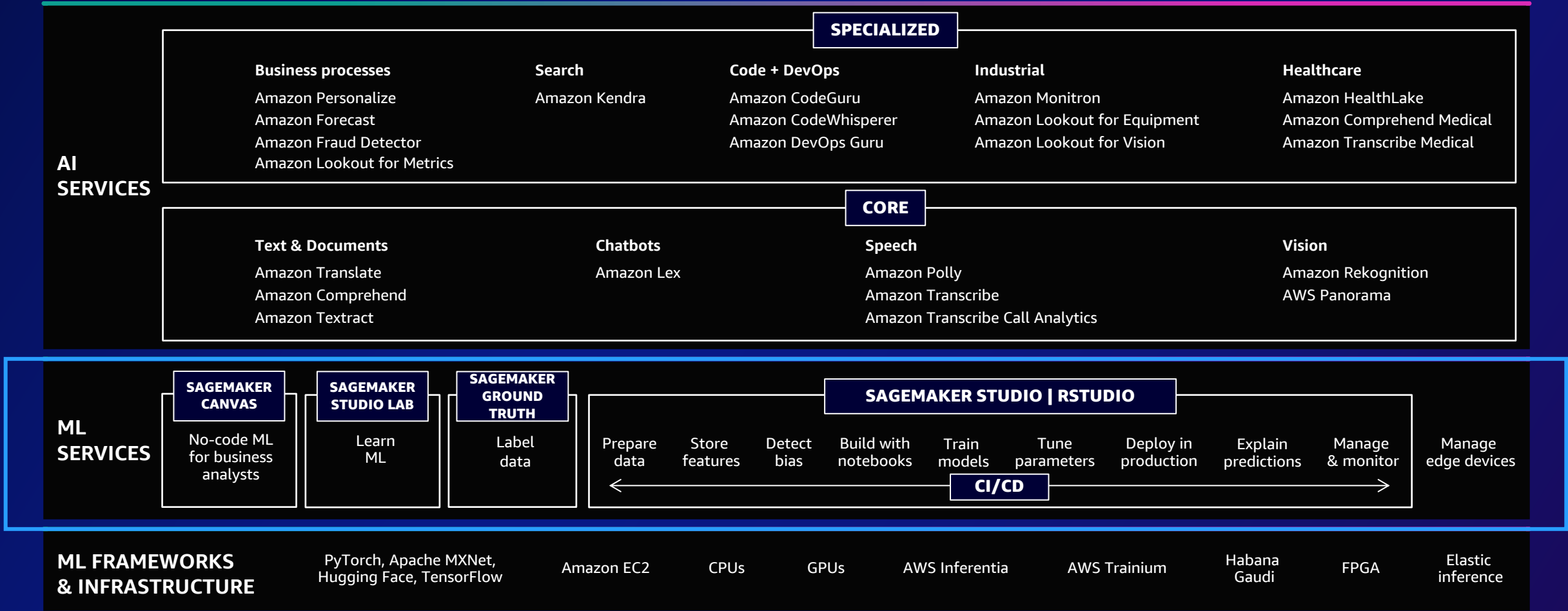
© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Agenda

- AWS ML Stack – SageMaker overview
- New security features - Domain(s), SageMaker roles
- New collaboration features – Real time code collaboration
- New governance features - Model cards, Model dashboards, Resource tagging

# The AWS ML stack

BROADEST AND MOST COMPLETE SET OF MACHINE LEARNING CAPABILITIES

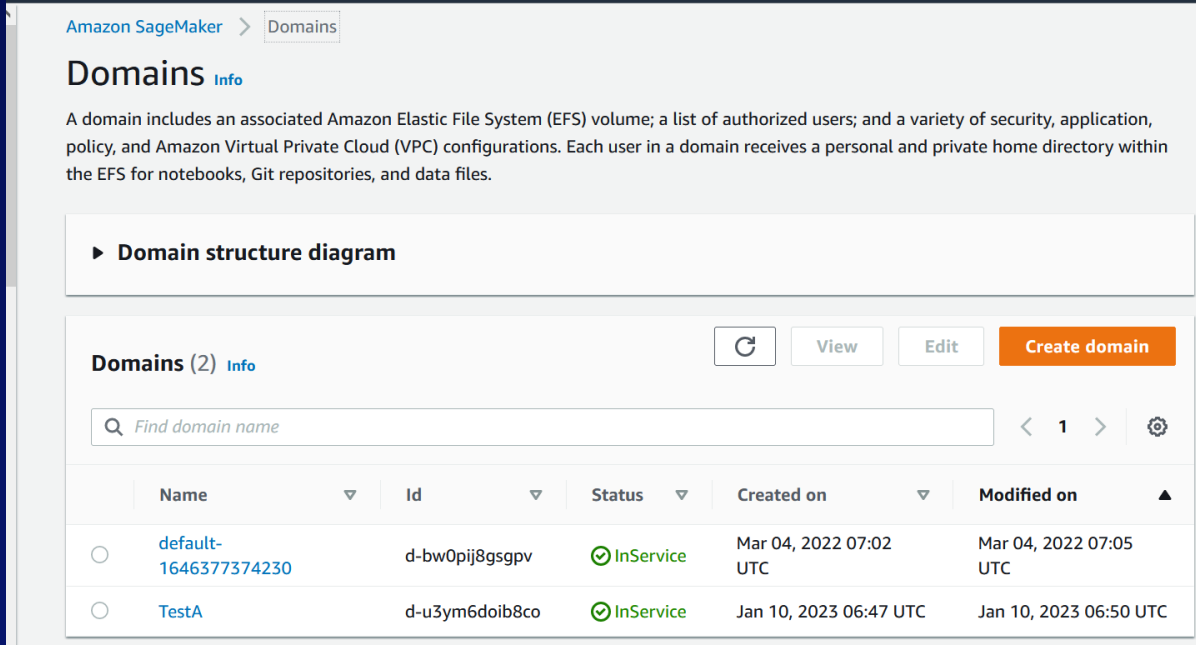


# Amazon SageMaker Security



# Multiple domains under same AWS accounts

CONFIGURING GIT REPOSITORY AT DOMAIN LEVEL OR USER PROFILE LEVEL



The screenshot shows the Amazon SageMaker Domains console. At the top, there's a breadcrumb 'Amazon SageMaker > Domains'. Below it, the title 'Domains' is followed by an 'Info' link. A descriptive paragraph explains that a domain includes an associated Amazon Elastic File System (EFS) volume, a list of authorized users, and a variety of security, application, policy, and Amazon Virtual Private Cloud (VPC) configurations. Each user in a domain receives a personal and private home directory within the EFS for notebooks, Git repositories, and data files.

Below the description is a section titled 'Domain structure diagram'. Underneath is a table of domains. The table has columns for Name, Id, Status, Created on, and Modified on. There are two domains listed: 'default-1646377374230' and 'TestA'. Both are in 'InService' status.

Name	Id	Status	Created on	Modified on
default-1646377374230	d-bw0pij8gsgpv	InService	Mar 04, 2022 07:02 UTC	Mar 04, 2022 07:05 UTC
TestA	d-u3ym6doib8co	InService	Jan 10, 2023 06:47 UTC	Jan 10, 2023 06:50 UTC

- Administrators now can provision multiple SageMaker domains within the same AWS account
- Scope access and isolate resources to different team or business units in your organization in a region in order to separate different lines of business within a single AWS account



# Amazon SageMaker Role Manager

DEFINE CUSTOM USER PERMISSIONS IN MINUTES

Step 1  
Enter role information

Step 2  
**Configure ML activities**

Step 3  
Add additional policies & tags

Step 4  
Review role

## Configure ML activities

Configure your role with the help of available ML activities.

### Configure new role [Info](#)

Choose specific ML activities and enable customizations of the activity settings.

Amazon SageMaker Role Manager recommends the selected ML activities based on the persona you chose in Step 1. Select the checkboxes below to remove or add additional ML activities.

#### ML activities (2 activities selected)

	Name	Description
<input checked="" type="checkbox"/>	Run Studio Applications	Permissions to operate within a Studio environment. Required for domain and user-profile execution roles.
<input checked="" type="checkbox"/>	Manage Experiments	Permissions to manage experiments and trials.
<input type="checkbox"/>	Search and visualize experiments	Permissions to audit, query lineage and visualize experiments.
<input type="checkbox"/>	Manage ML Jobs	Permissions to manage SageMaker jobs across their lifecycles.
<input type="checkbox"/>	Manage Endpoints	Permissions to manage SageMaker Endpoint deployments and updates.
<input type="checkbox"/>	Manage Models	Permissions to manage SageMaker models and Model Registry.
<input type="checkbox"/>	Manage Model Monitoring	Permissions to manage monitoring schedules for SageMaker Model Monitor.
<input type="checkbox"/>	Manage Pipelines	Permissions to manage SageMaker Pipelines and pipeline executions.
<input type="checkbox"/>	Access Required AWS Services	Permissions to access S3, ECR, Cloudwatch and EC2. Required for execution roles for jobs and endpoints.
<input type="checkbox"/>	S3 Full Access	Permissions to perform all S3 operations

- Simplify permissions for ML activities
- Use guided workflows for role creation
- Accelerate user onboarding
- Define custom permissions for SageMaker users in minutes

# Amazon SageMaker Collaboration



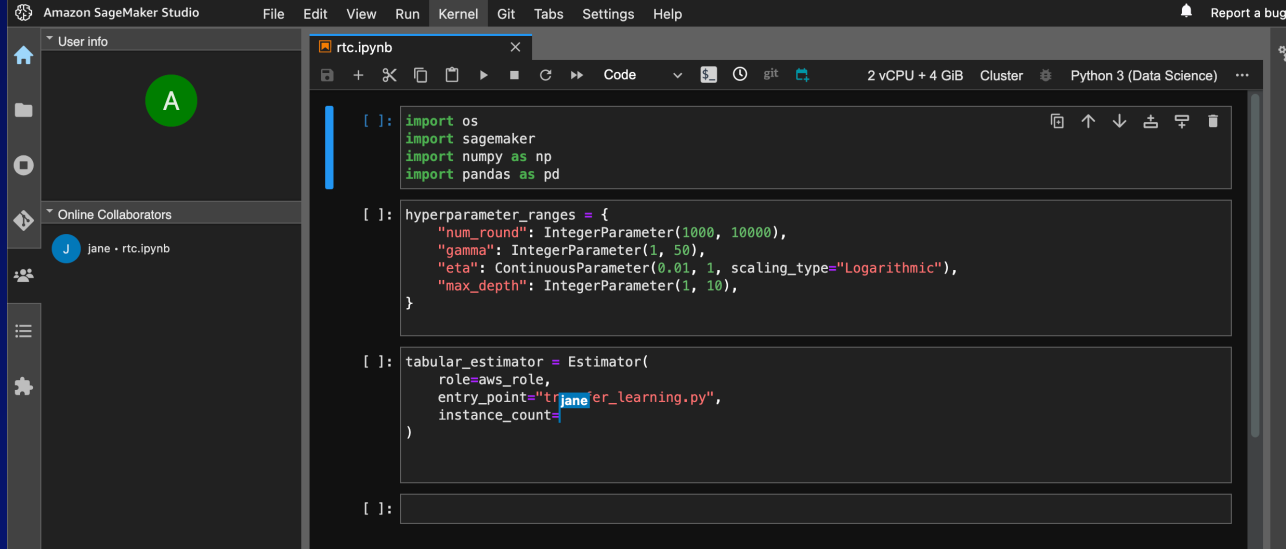
© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.



# Amazon SageMaker notebook collaboration

ACCELERATE COLLABORATION ACROSS DATA SCIENCE TEAMS

GA NOVEMBER 30 2022



1

Read, edit, and run notebooks together in real time with your teams to streamline collaboration and communication

2

Automatically tag and filter resources in SageMaker Spaces to easier monitor costs and plan budget

3

Users can now configure a list of suggested Git repository URLs at the SageMaker domain or user profile level to aid collaboration using version control

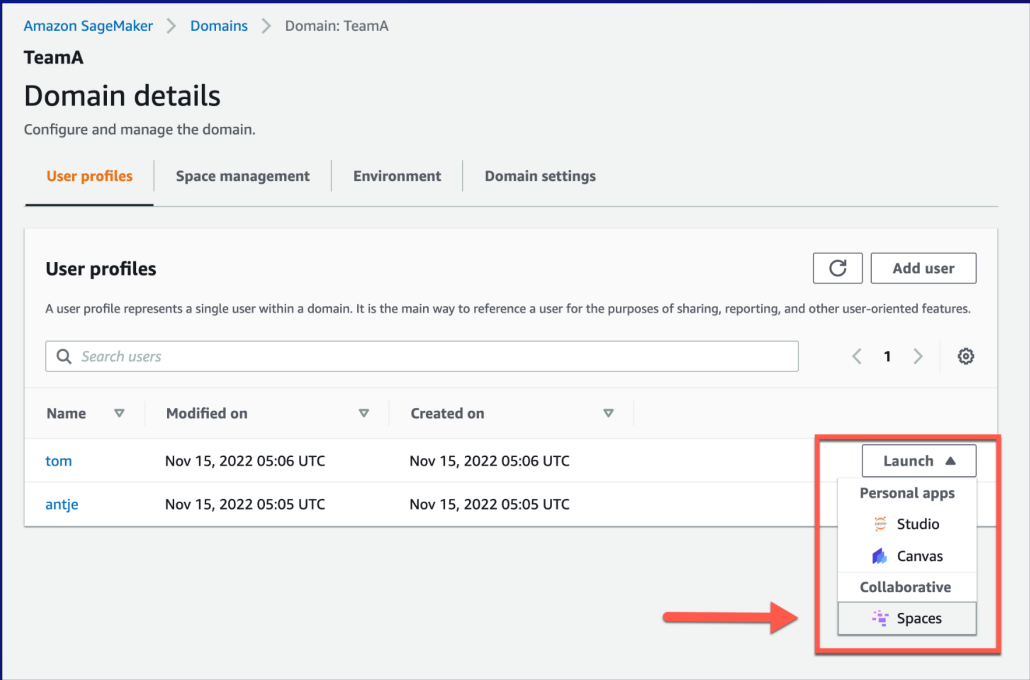
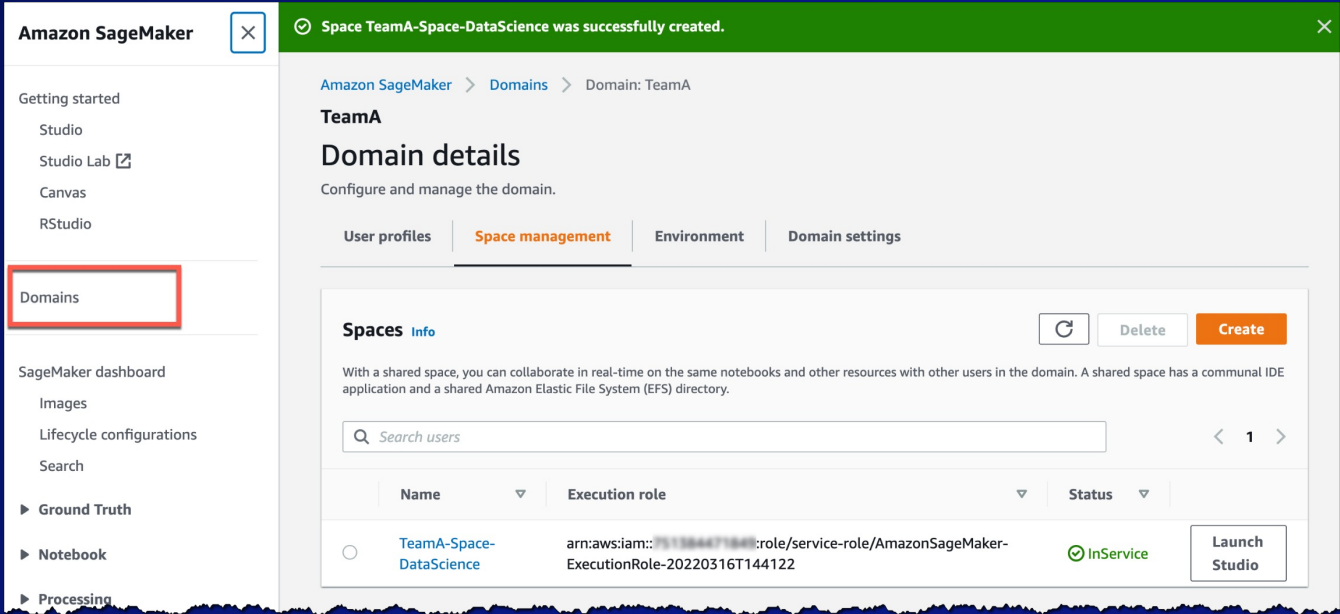
4

Quickly start collaborating on code without manually clone Git repositories or manage credentials



# Shared workspaces

Users in this SageMaker domain can now launch and join the shared space through their SageMaker domain user profiles.



# Shared workspaces - to accelerate real time collaboration across ML teams

- By creating shared spaces in SageMaker Studio, users can now access, read, edit, and share the same notebooks in real time
- Shared spaces provide a shared [Amazon EFS](#) directory that you can utilize to share files within a shared space

# SageMaker Governance



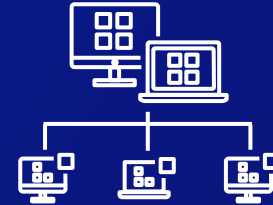
# Introducing ML governance tools

Simplify access control and enhance transparency



## Amazon SageMaker Model Cards

Create a single  
source of truth for  
model information



## Amazon SageMaker Model Dashboard

Audit performance and  
lineage of all your  
models, in one place

# Amazon SageMaker model cards

EASILY DOCUMENT, RETRIEVE, AND SHARE THE NECESSARY MODEL INFORMATION

The screenshot shows the Amazon SageMaker console interface for a model card titled "customer-churn-model-card". The breadcrumb navigation at the top reads "Amazon SageMaker > Model cards > customer-churn-model-card". The main heading is "Model card - customer-churn-model-card", followed by "Edit", "Clone", and "Actions" buttons. The interface is divided into two main sections: "Model card overview" and "Model overview".

**Model card overview**

Model card version 1	KMS encryption key <a href="#">arn:aws:kms:us-east-2:364732211972:key/77ad1ad6-cabc-46a2-af0b-905dce65337b</a>
Model card status Draft	Model card ARN <a href="#">arn:aws:sagemaker:us-east-2:364732211972:model-card/customer-churn-model-card</a>
Created date 11/15/2022, 1:27:47 PM	

**Model overview**

Model name Customer-Churn-Model	Inference environment <a href="#">257758044811.dkr.ecr.us-east-2.amazonaws.com/sagemaker-xgboost:1.3-1</a>
Model description xgboost model for customer churn prediction for mobile phone customers	Problem type Binary Classification
Model versions 1	Algorithm type Logistic regression
Model arn <a href="#">arn:aws:sagemaker:us-east-2:364732211972:model/customer-churn-model</a>	Model creator alice
Model artifacts <a href="#">s3://sagemaker-studio-us-east-2-364732211972/xgboost-churn/output/workshop-xgboost-customer-churn-2022-11-10-23-13-38-509/output/model.tar.gz</a>	Model owner alice

At the bottom, there are five tabs: "Intended uses" (selected), "Training details", "Evaluation results", "Additional details", and "Version history".

- Streamline model documentation
- Capture model information, such as input datasets, training environments, training results, model purpose, performance goals
- Attach and visualize evaluation results, such as bias and quality metrics
- Share model cards with business stakeholders, internal teams, or your customers



# Amazon SageMaker model dashboard

UNIFIED VIEW ACROSS ALL YOUR MODELS TO AUDIT PERFORMANCE

Amazon SageMaker > Model dashboard

### Model dashboard info

Display all SageMaker models, endpoints, and monitor alerts.

**Models** info

Filter models or endpoints by property or value

Model Name	Risk Rating	Model Quality	Data Quality	Bias Drift	Feature Attribution Drift	Endpoints	Last batch transform job	Model creation time
Customer-Churn-Model	High	Nov 16, 2022 02:13 UTC	Nov 16, 2022 02:13 UTC	Scheduled	Scheduled	Customer-Churn-Model-Endpoint and 1 more	Customer-Churn-Model--2022-11-16-00-53-43-505	Nov 14, 2022 03:35 UTC
Fraud-Detection-Model	Low	-	Nov 16, 2022 02:03 UTC	-	-	Fraud-Detection-Model-Endpoint	-	Nov 13, 2022 20:43 UTC
Loan-Approval-Model	High	-	Nov 16, 2022 02:12 UTC	-	-	Loan-Approval-Model-Endpoint	-	Nov 14, 2022 03:23 UTC
Product-Recommendation-Model	High	-	Nov 16, 2022 02:07 UTC	-	-	Product-Recommendation-Model-Endpoint	-	Nov 14, 2022 03:18 UTC
Sentiment-Analysis-Model	High	-	Nov 16, 2022 02:09 UTC	-	-	Sentiment-Analysis-Model-Endpoint	-	Nov 15, 2022 03:58 UTC

Amazon SageMaker > Model dashboard > Customer-Churn-Model

### Customer-Churn-Model info

[Edit Model Card](#)

**Model overview** info

Model card customer-churn-model-card	Model lineage <a href="#">View lineage</a>	Additional model details <a href="#">Customer-Churn-Model</a>	Model card risk rating High
---	---	--	--------------------------------

**Endpoints** info

Endpoint name	Endpoint status	Creation Date	Last modification time
Customer-Churn-Model-Endpoint	In Service	Nov 14, 2022 03:35 UTC	Nov 14, 2022 03:38 UTC

**Monitor schedule** info

[Deactivate monitor schedule](#) [Edit alert](#)

Schedule name	Endpoint name	Monitor type	Monitor frequency	Schedule status	Alert details	Alert status
monitoring-schedule-2022-11-14-04-22-56-077	Customer-Churn-Model-Endpoint	ModelBias	Every hour	Scheduled	Alert if 1 out of 1 monitoring executions fail	OK
customer-churn-monitoring-schedule-2022-11-14-0403	Customer-Churn-Model-Endpoint	ModelQuality	Every hour	Scheduled	Alert if 1 out of 1 monitoring executions fail	InAlert
customer-churn-monitor-schedule-2022-11-14-03-47-26	Customer-Churn-Model-Endpoint	DataQuality	Every hour	Scheduled	Alert if 1 out of 1 monitoring executions fail	InAlert
monitoring-schedule-2022-11-14-17-14-04-278	Customer-Churn-Model-Endpoint	ModelExplainability	Every hour	Scheduled	Alert if 1 out of 1 monitoring executions fail	OK

- Track model behavior
- Integrates with SageMaker Model Monitor and SageMaker Clarify
- Monitor model behavior for data quality, model quality, bias drift, and feature attribution drift
- Automate alerts
- Troubleshoot model deviations

# Governance - Tagging and cost allocation

- All resources in a [Shared Spaces](#) are filtered and tagged, making it easier to focus on ML projects and manage costs
- All taggable SageMaker resources that you create in a shared space are automatically tagged to help you organize and have a filtered view of your ML resources, such as training jobs, experiments, and models, that are relevant to the business problem you work on in the space
- This also helps you monitor costs and plan budgets using tools such as [AWS Budgets](#) and [AWS Cost Explorer](#) capability

# Summary

- Ability to create multiple Sagemaker Domains in a single AWS region for each account
- Independent domains help isolate work boundary for each team
- Pre-configured Sagemaker roles that can be further customized
- Real time Code collaboration across various users under the same domain enabled through Sharedworkspaces
- Improved ML Governance through usage of Model Cards, and Model Dashboards
- Fine grained cost control through resource tagging

skillbuilder.aws 

# **Your time is now**

Build in-demand cloud skills your way



© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Thank you!

Sudhanshu Hate

Principal AI & ML Specialist Architect

AWS India



Please complete the  
session survey

