
AWS
re:Invent

AIM309

Secure and compliant machine learning for regulated industries

Stefan Natu

Sr. Machine Learning Specialist Solutions Architect

AWS

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Objectives

- Understand requirements for secure machine learning
- Dive deep into Amazon SageMaker Studio security with demos
- Automating secure machine learning environments



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Requirements for secure ML environments

Compute and network isolation



Authentication and authorization



Data protection



Artifact management



Auditability, governance, and compliance



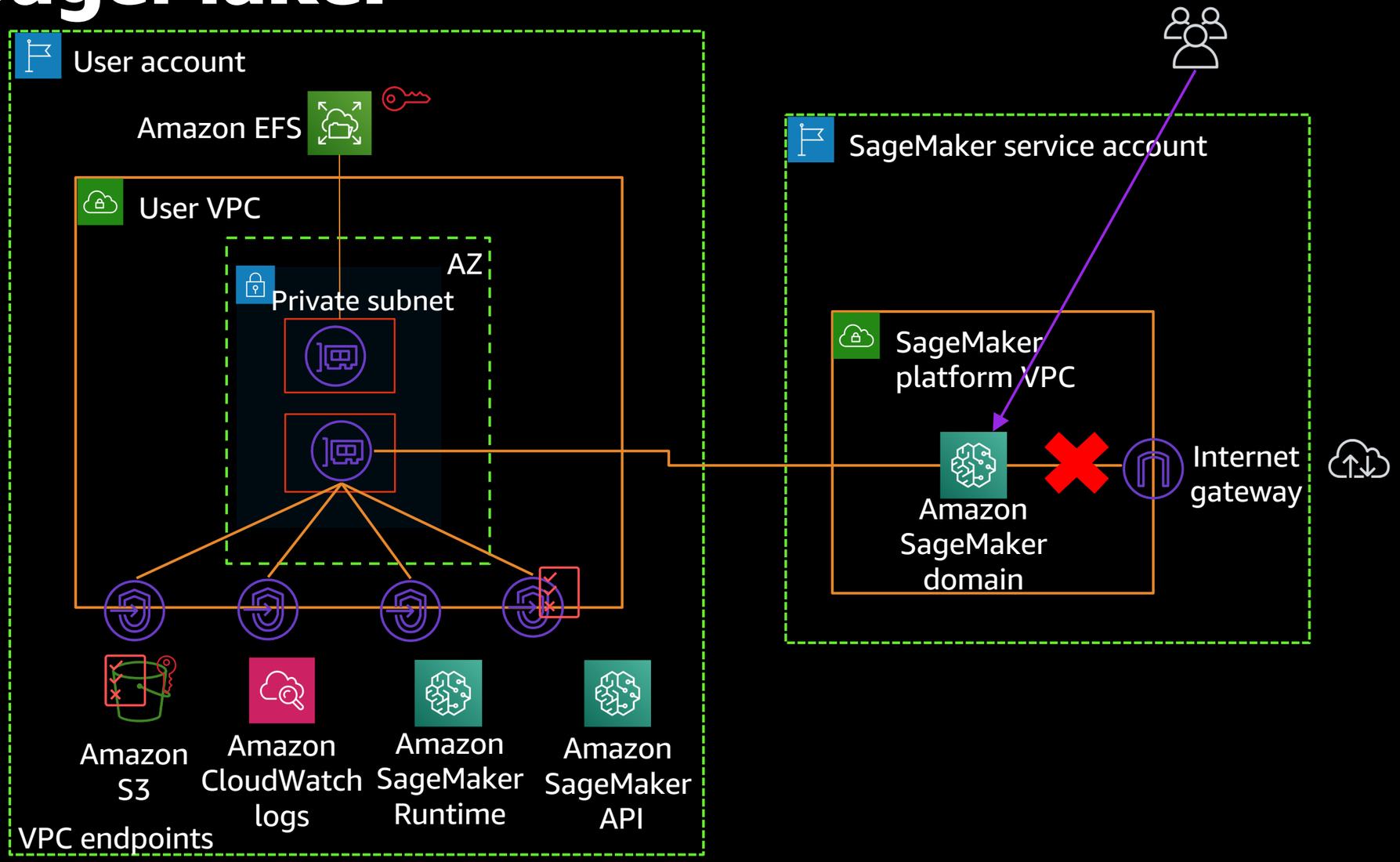
Secure ML: Compute and network isolation



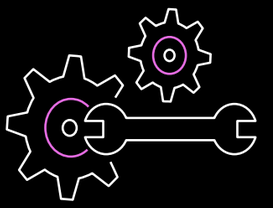
AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Compute and network isolation for Amazon SageMaker



Network isolation while training



Pass these as

env variables in a python file

```
xgb = sagemaker.estimator.Estimator(
    image,
    role,
    instance_count=1,
    instance_type='ml.m5.xlarge',
    output_kms_key=output_key,
    volume_kms_key=cmk_id,
    max_run=3600,
    output_path='s3://{}/{}/models'.format(output_bucket, prefix),
    sagemaker_session=sess,
    use_spot_instances=True,
    max_wait=3600,
    subnets=subnets,
    security_group_ids= sec_groups,
    encrypt_inter_container_traffic=True,
    enable_network_isolation = True
)
```

Secure ML: Authentication and authorization



AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Authentication for Amazon SageMaker



SSO mode

Map federated identity pools to users (AWS SSO, Microsoft AD, Azure AD, Okta)

Avoids giving users AWS Management Console access



IAM mode

Fully Integrated with AWS Identity and Access Management (IAM)

Avoids giving users AWS Management Console access via *CreatePresignedDomainUrl* API

Common IAM permissions for ML environments

Analysts / data engineers

Development

Launch apps / notebooks
Data access
Processing jobs
Code repo access
Package repo access

Data scientists / ML engineers

Training

Training job
Hyperparameter tuning job
Transform job
Auto ML job
Experiments / trials / components
Amazon Elastic Container Registry (Amazon ECR) access

DevOps engineers

Deployment

Create endpoint
Transform job
Invoke endpoint
Monitoring job

Permissions to encrypt decrypt data, training artifacts and models

Permissions to create Elastic network interfaces (ENIs) during training, hosting

Permissions to pass role to a service

Permissions to create Amazon Elastic File System (Amazon EFS) volume and manage users

Limit domain access by user or group

```
{
"Effect": "Allow",
"Action": [
"sagemaker:CreatePresignedDomainUrl”,
"sagemaker:UpdateApp”,
"sagemaker:UpdateDomain”,
"sagemaker:DeleteApp”,
“sagemaker:DeleteDomain”
],
"Resource": "*",
"Condition": {
     "StringLike": {
          "sagemaker:ResourceTag/owner":"${aws:userid}"
          }
     }
}
```

```
aws sts get-caller-identity
{
    "UserId": ”#####",
    "Account": ”#####",
    "Arn": "arn:aws:iam::###:user/##"
}
```

For SAML federated users

aws:userid = *role-id:caller-specified-role-name*

Secure ML:
Data protection



AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

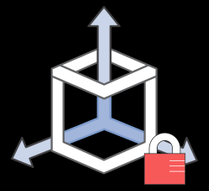
Common patterns for data protection



Volumes and file system encryption



Bucket encryption and deny policies



Inter-container traffic encryption

Encryption during training



```
xgb = sagemaker.estimator.Estimator(
    image,
    role,
    instance_count=1,
    instance_type='ml.m5.xlarge',
    output_kms_key=output_key,
    volume_kms_key=cmk_id,
    max_run=3600,
    output_path='s3://{}/{}/models'.format(output_bucket, prefix),
    sagemaker_session=sess,
    use_spot_instances=True,
    max_wait=3600,
    subnets=subnets,
    security_group_ids= sec_groups,
    encrypt_inter_container_traffic=True,
    enable_network_isolation = True
)
```

Encryption at rest

Encryption in transit

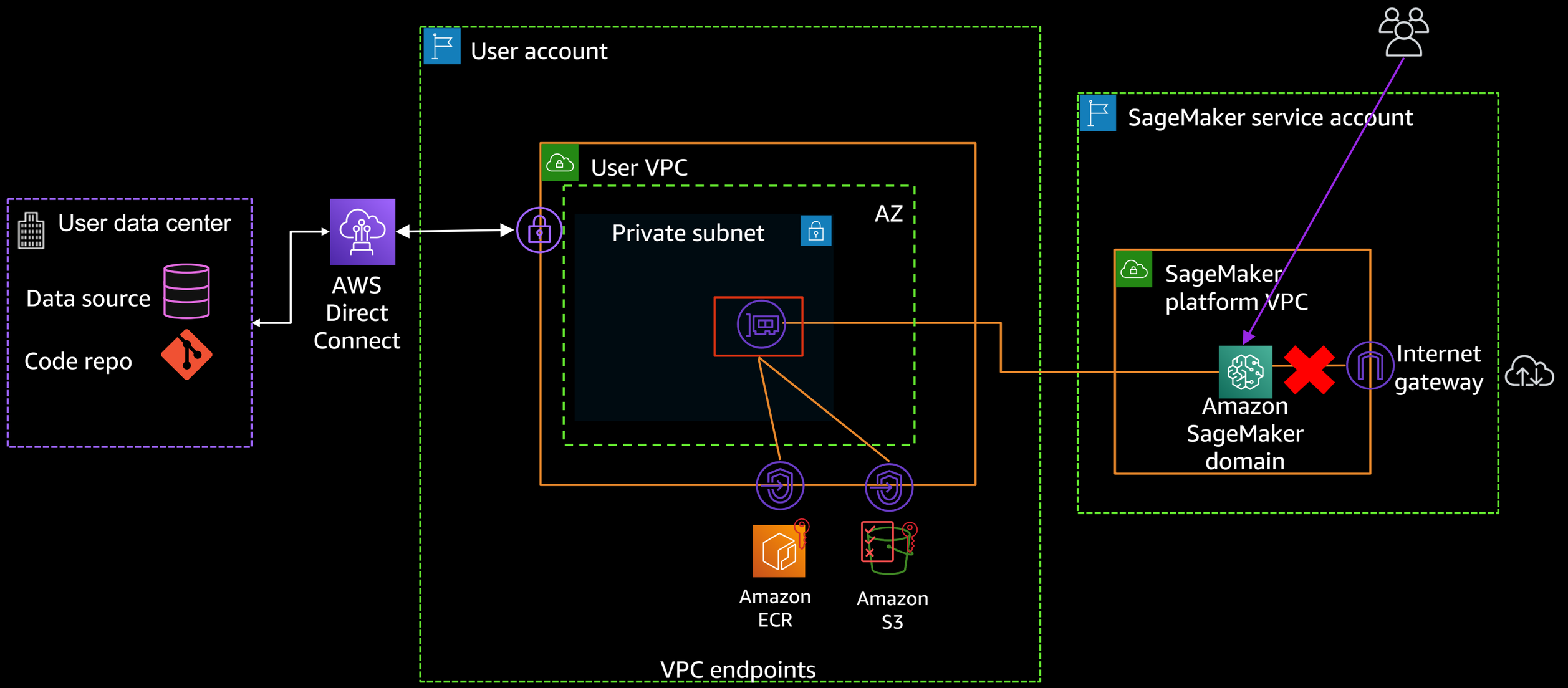
Secure ML:
Artifact management



AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Artifact management



Amazon SageMaker Studio custom images

Write dockerfile with custom packages

Upload to Amazon ECR

Attach to Studio domain

```
FROM tensorflow/tensorflow:2.3.0

RUN pip install ipykernel && \
        python -m ipykernel install --sys-prefix && \
        pip install --quiet --no-cache-dir \
        'boto3>1.0<2.0' \
        'sagemaker>2.0<3.0' \
        'sagemaker-training'

#Run a vulnerability test
RUN curl -sfL https://raw.githubusercontent.com/aquasecurity/trivy/master/contrib/install.sh | sh -s -- -b /usr/local/bin \
    && trivy filesystem --exit-code 1 --severity CRITICAL --no-progress /

# Copies the training code inside the container
COPY train.py /root/train.py
```

```
# Build the docker image and push to Amazon ECR (modify image tags and name as required)
$(aws --region ${REGION} ecr get-login --no-include-email)
docker build . -t tfkernel -t ${ACCOUNT_ID}.dkr.ecr.${REGION}.amazonaws.com/smstudio-custom:tf2
docker push ${ACCOUNT_ID}.dkr.ecr.${REGION}.amazonaws.com/smstudio-custom:tf2


# Using with SageMaker Studio
## Create SageMaker Image with the image in ECR (modify image name as required)
ROLE_ARN=arn:aws:iam::            :role/service-role/AmazonSageMaker-ExecutionRole-20190823T110499

aws --region ${REGION} sagemaker create-image \
    --image-name ${IMAGE_NAME} \
    --role-arn ${ROLE_ARN}3

aws --region ${REGION} sagemaker create-image-version \
    --image-name ${IMAGE_NAME} \
    --base-image "${ACCOUNT_ID}.dkr.ecr.${REGION}.amazonaws.com/smstudio-custom:tf2"
```

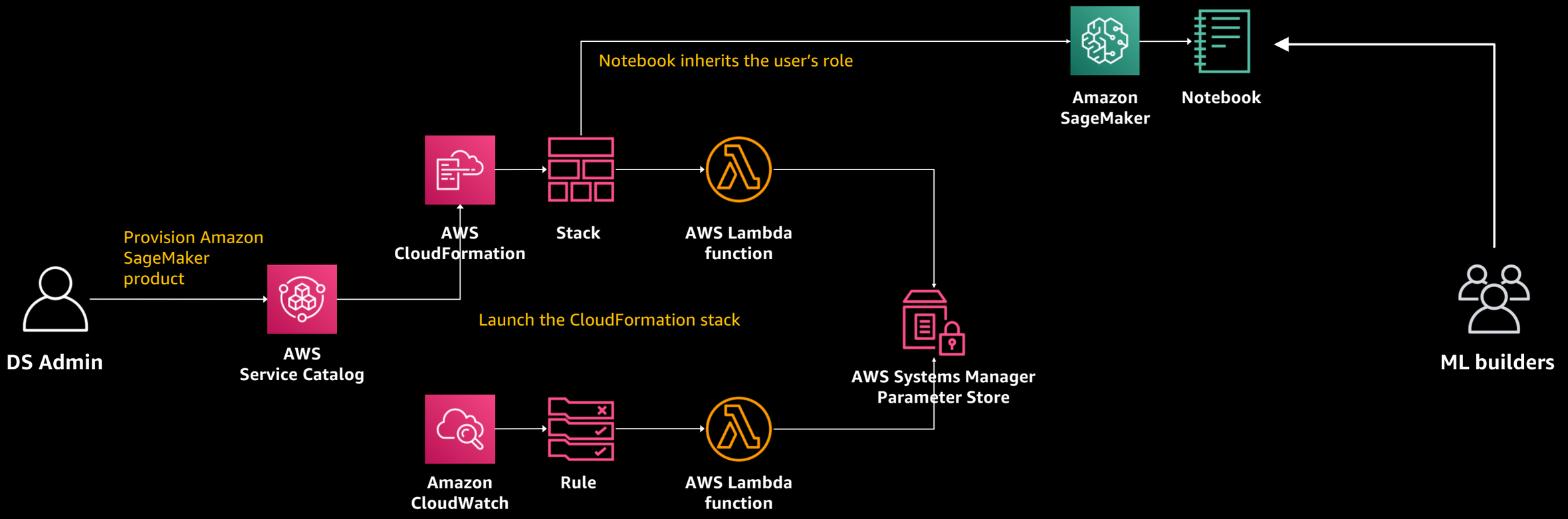
Automate Secure ML Environments



AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Secure notebook provisioning architecture



Secure ML: Auditability, governance, and compliance scope

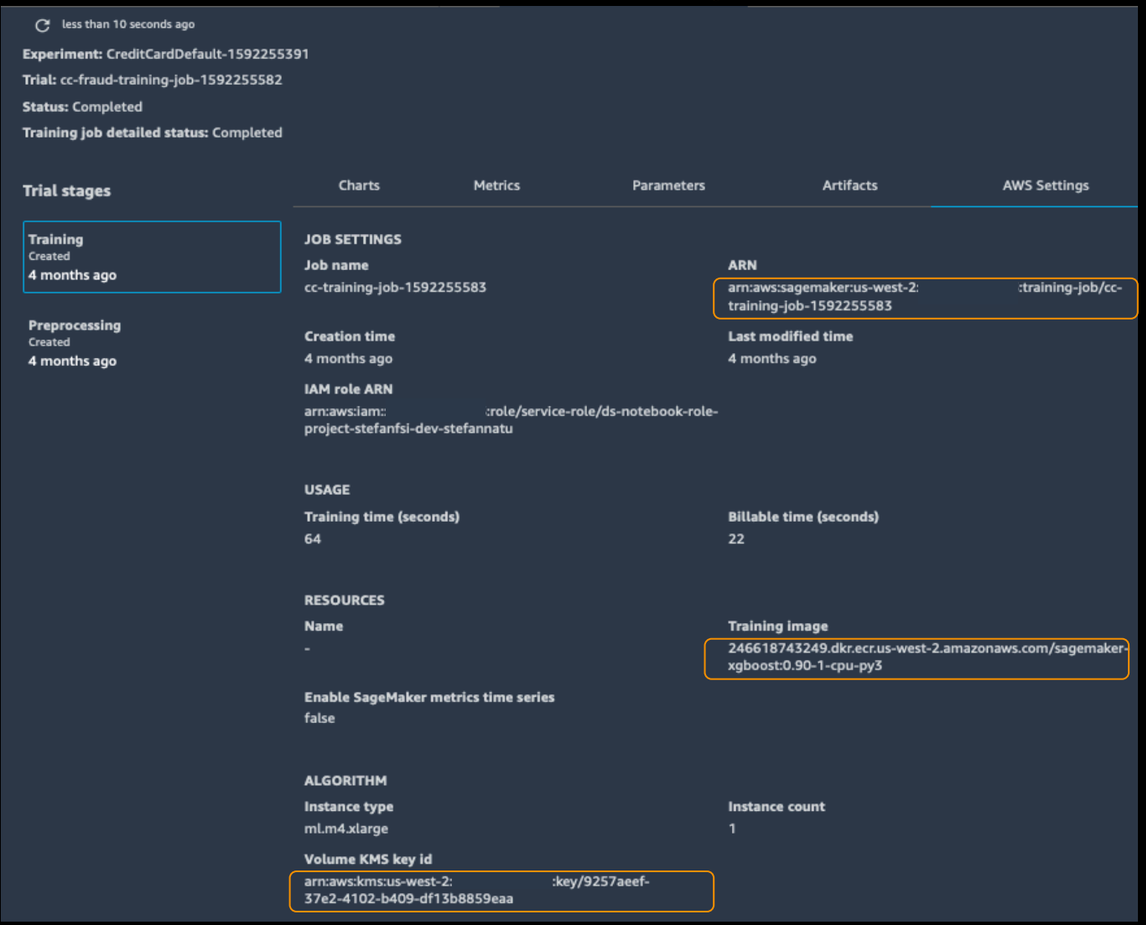


AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Traceability

SageMaker Experiments to track training jobs




```
trial_name = f"cc-fraud-training-job-{int(time.time())}"
cc_trial = Trial.create(
    trial_name=trial_name,
    experiment_name=cc_experiment.experiment_name,
    sagemaker_boto_client=sm)

cc_trial.add_trial_component(preprocessing_trial_component)
cc_training_job_name = "cc-training-job-{}".format(int(time.time()))
xgb = sagemaker.estimator.Estimator(
    image,
    role,
    instance_count=1,
    instance_type='ml.m4.xlarge',
    output_kms_key=output_key,
    max_run=3600,
    output_path='s3://{}/{}/models'.format(output_bucket, prefix),
    sagemaker_session=sess,
    use_spot_instances=True,
    max_wait=3600,
    subnets=subnets,
    security_group_ids=
    sec_groups,
    volume_kms_key=cmk_id,
    encrypt_inter_container_traffic=True,
    enable_network_isolation = True
)


xgb.fit(
    inputs={'train': s3_input_train},
    job_name=cc_training_job_name,
    experiment_config={
        "TrialName":
        cc_trial.trial_name,  #log training job in Trials for lineage
        "TrialComponentDisplayName": "Training",
    })
```

Auditability: Ensure apps are tagged

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": ”EnforceAppTag",
            "Effect": "Allow",
            "Action": [
                "sagemaker:CreateApp”
            ],
            "Resource": "*",
            "Condition": {
                "ForAllValues:StringLike": {
                    "aws:RequestTag/Project": "sandbox"
                }
            }
        }
    ]
}
```

Principal :

IAM user

IAM role for SAML federated user

```
bash-4.2$ aws --region us-west-2 sagemaker create-app --domain-id d-r2fxlveq03rh --user-profile-name apptester --app-type KernelGateway
--app-name KernelGateway --tags Key=Project,Value=production

An error occurred (AccessDeniedException) when calling the CreateApp operation: User: arn:aws:sts::            :assumed-role/AmazonSageM
aker-ExecutionRole-20190823T110499/SageMaker is not authorized to perform: sagemaker:CreateApp on resource: arn:aws:sagemaker:us-west-2:
            :app/d-r2fxlveq03rh/apptester/kernelgateway/kernelgateway
bash-4.2$
```

AWS CloudTrail logs



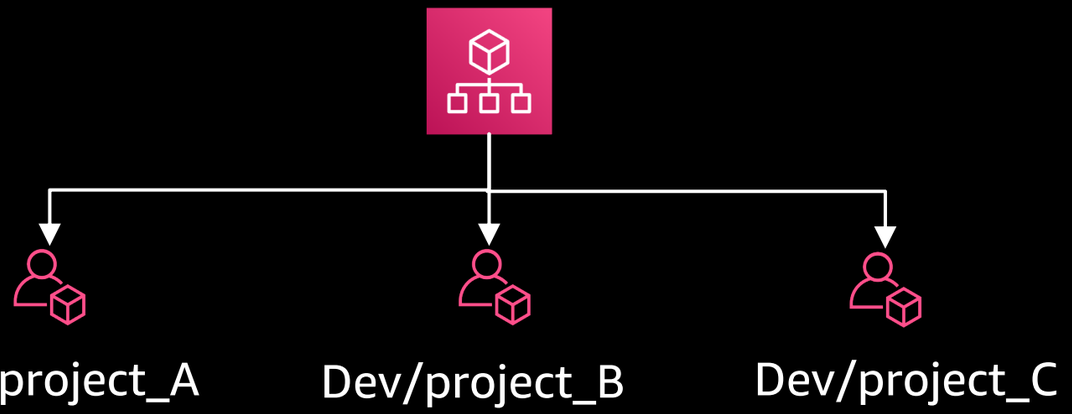
CreateApp Info

Details Info

Event time October 07, 2020, 17:51:58 (UTC-04:00)	AWS access key [redacted]	AWS region us-west-2
User name studio	Source IP address [redacted]	Error code -
Event name CreateApp	Event ID 5120b836-ee16-4ead-8439-9917eb1f9d75	Read-only -
Event source sagemaker.amazonaws.com	Request ID 06b7b7ab-1ce9-4e88-8ea3-c198298eb23a	


```
"eventTime": "2020-10-07T21
"eventSource": "sagemaker.ar
"eventName": "CreateApp",
"awsRegion": "us-west-2",
"sourceIPAddress": "100.20.
"userAgent": "Coral/Netty4"
"requestParameters": {
    "domainId": "d-r2fxlveq03rh",
    "userProfileName": "apptester",
    "appType": "JupyterServer",
    "appName": "default"
},
"responseElements": {
    "appArn": "arn:aws:sagemaker:us-west-2:            :app/d-r2fxlveq03rh/apptester/jupyterserver/default"
},
"requestID": "06b7b7ab-1ce9-4e88-8ea3-c198298eb23a",
"eventID": "5120b836-ee16-4ead-8439-9917eb1f9d75",
"eventType": "AwsApiCall",
"recipientAccountId": "            "
```

Governance




```
{
"Sid": ”VPCDeployment",
"Effect": ”Deny",
"Action": [
   "sagemaker:CreateAutoMLJob",
   "sagemaker:CreateTrainingJob",
   "sagemaker:CreateProcessingJob",
   "sagemaker:CreateModel",
   "sagemaker:CreateHyperParameterTuningJob"
      ],
"Resource": "*",
"Condition": {
   ”ArnNotEquals": {
      "sagemaker:OutputKmsKey":”arn:aws:kms:####”
,
      },
    }
}
```

Next steps



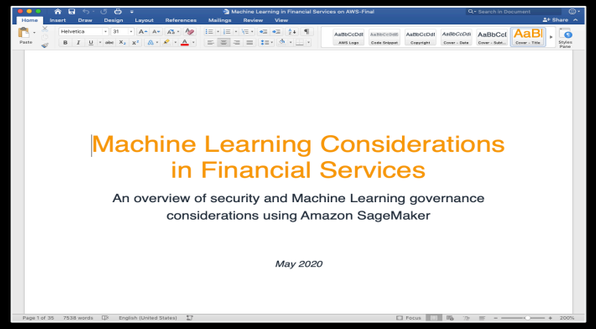
AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Resources

ML best practices in regulated industries whitepaper

https://d1.awsstatic.com/whitepapers/machine-learning-in-financial-services-on-aws.pdf



YouTube video on secure and compliant ML for Financial Services

https://aws.amazon.com/sagemaker/developer-resources/



Workshop on building and automating secure ML environments for admins and data scientists

https://sagemaker-workshop.com/security_for_sysops.html

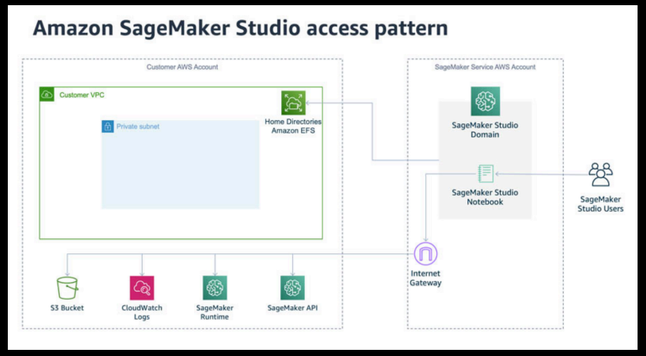
https://sagemaker-workshop.com/security_for_users.html



Resources

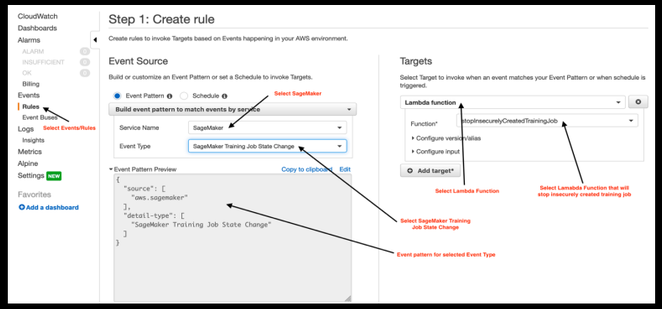
Blog – Securing SageMaker Studio connectivity using a private VPC

https://aws.amazon.com/blogs/machine-learning/securing-amazon-sagemaker-studio-connectivity-using-a-private-vpc/



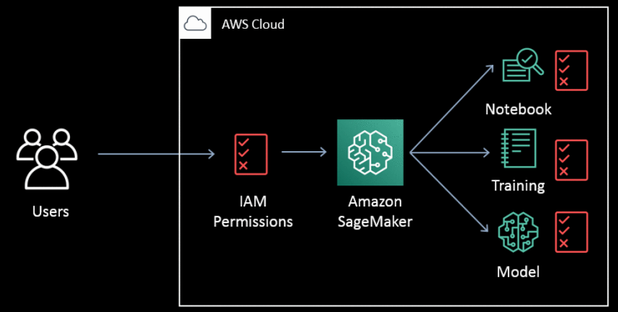
Blog – Secure Deployment of SageMaker resources

https://aws.amazon.com/blogs/security/secure-deployment-of-amazon-sagemaker-resources/



Blog – Millennium Management use of SageMaker security

https://aws.amazon.com/blogs/machine-learning/millennium-management-secure-machine-learning-using-amazon-sagemaker/



Thank you!



AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Please complete the session survey

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.