**AWS Macie**

**( Discover and protect your sensitive data at scale )**

Amazon Macie is a fully managed data security and data privacy service that uses machine learning and pattern matching to discover and protect your sensitive data in AWS.

As organizations manage growing volumes of data, identifying and protecting their sensitive data at scale can become increasingly complex, expensive, and time-consuming. Amazon Macie automates the discovery of sensitive data at scale and lowers the cost of protecting your data. Macie automatically provides an inventory of Amazon S3 buckets including a list of unencrypted buckets, publicly accessible buckets, and buckets shared with AWS accounts outside those you have defined in AWS Organizations. Then, Macie applies machine learning and pattern matching techniques to the buckets you select to identify and alert you to sensitive data, such as personally identifiable information (PII).

Macie’s alerts, or findings, can be searched and filtered in the AWS Management Console and sent to Amazon EventBridge, formerly called Amazon CloudWatch Events, for easy integration with existing workflow or event management systems, or to be used in combination with AWS services, such as AWS Step Functions to take automated remediation actions. This can help you meet regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) and General Data Privacy Regulation (GDPR). You can get started with Amazon Macie by leveraging the 30-day free trial for bucket evaluation. The trial includes 30-days of Amazon S3 bucket inventory and bucket-level security and access control assessment at no cost. Note that sensitive data discovery is not included in the 30-day free trial for bucket evaluation.

**Benefits**

**Discover your sensitive data at scale**

Amazon Macie uses machine learning and pattern matching to cost efficiently discover sensitive data at scale. Macie automatically detects a large and growing list of sensitive data types, including personal identifiable information (PII) such as names, addresses, and credit card numbers. The service also allows you to define your own custom sensitive data types so you can discover and protect the sensitive data that may be unique to your business or use case.

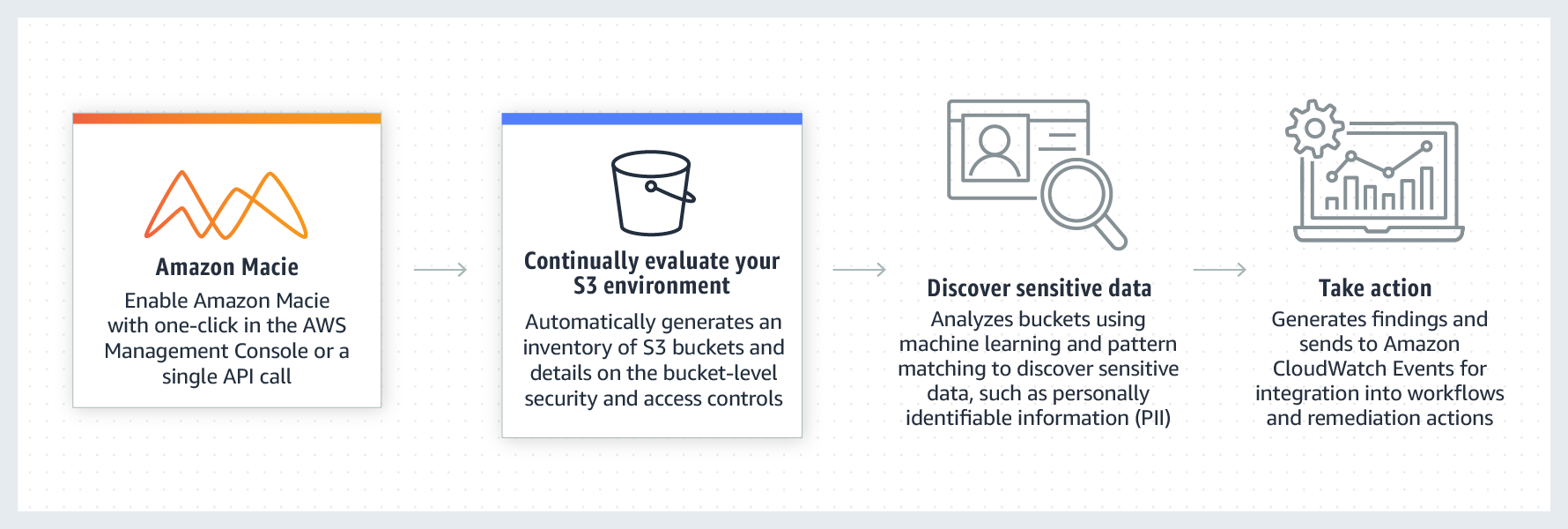
**Visibility of your data security posture**

Amazon Macie gives you constant visibility of the data security and data privacy of your data stored in Amazon S3. Macie automatically and continually evaluates all of your S3 buckets and alerts you to any unencrypted buckets, publicly accessible buckets, or buckets shared with AWS accounts outside those you have defined in the AWS Organizations. Macie provides native multi-account support so you can view your data security posture across your entire S3 environment from a single Macie administrator account.

**Easy to setup and manage**

Getting started with Amazon Macie is fast and easy with one-click in the AWS Management Console or a single API call. Macie provides multi-account support using AWS Organizations, so you can enable Macie across all of your accounts with a few clicks. Macie maintains a fully-managed set of sensitive data types, so there is no custom configuration required.

**How it works**



**Use cases**

**Assessing your data privacy and security**

An important aspect in maintaining the right level of data security is to be able to continuously identify your sensitive data and evaluate security and access controls. Amazon Macie allows you to do this across your entire Amazon S3 environment, generating actionable findings that you can use to quickly respond where needed. Macie also gives you the flexibility to identify sensitive data residing in other data stores by temporarily moving it to S3. For example, you can initiate Amazon Relational Database Service (RDS) or Amazon Aurora snapshots to export data in these services to Amazon S3 where it can be evaluated for sensitive data using Macie. This allows you to utilize Macie to help you maintain data privacy and security.

**Maintaining regulatory compliance**

Compliance teams are required to monitor where sensitive data resides, protect it properly, and provide evidence that they are enforcing data security and privacy to meet regulatory compliance requirements. Amazon Macie provides different options

for scheduling your data analysis, such as one-time, daily, weekly, or monthly sensitive data discovery jobs to help you meet and maintain your data privacy and

compliance requirements. Macie automatically sends all sensitive data discovery job outputs, including findings, evaluation results, time stamps, and a historical record of all buckets and objects scanned for sensitive data to an S3 bucket you own. These sensitive data discovery detail reports can be used in data privacy and protection audits and for long term retention.

**Identifying sensitive data in data migrations**

When migrating large volumes of data to AWS, you can set up a secure Amazon S3 environment to use as an initial staging area where you use Macie to discover sensitive data. You can also extract files from applications such as email, file share, collaboration tools, and transfer to S3 for evaluation by Macie. The results can be used to inform where the migration data should be stored and what security controls, such as encryption and resource tagging, need to be applied. Using Macie’s findings, you can automate the configuration of data protection and role-based access policies as your data moves into AWS.

Demo :

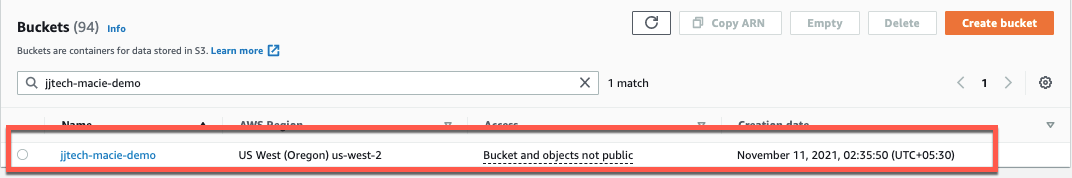
Agenda:

1. You have a S3 bucket name “jjtech-macie-demo” and as per your organizations policy, you need to ensure that no files uploaded to this bucket has Employee ID info. In order to do the same you need to come up with a solution that can monitor this bucket on daily basis and look for specific PII (Personal Identifiable Information )
2. Someone from your team uploads a csv file containing employee info including their Employee ID
3. You need to create a Macie Job to identify this data breach

Step 1:

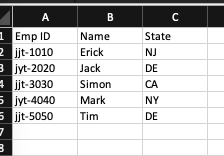
* Create a S3 bucket named “jjtech-macie-demo”
* Try to create different bucket since bucket names should be unique

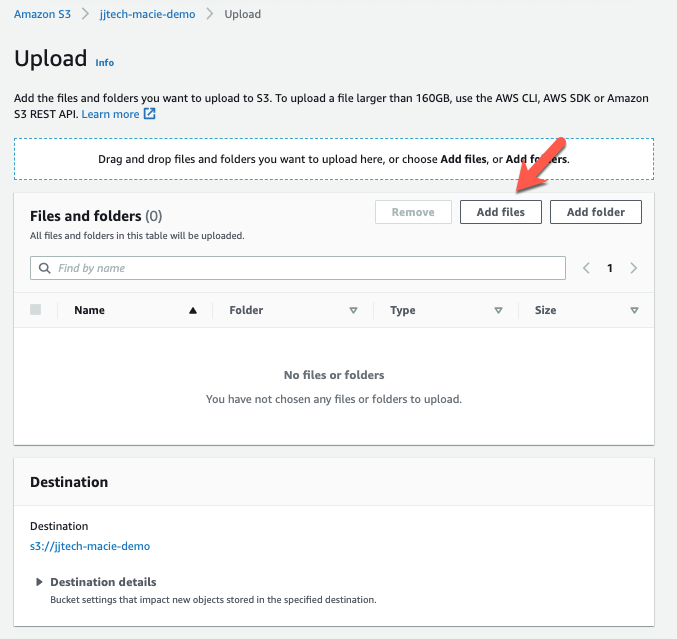
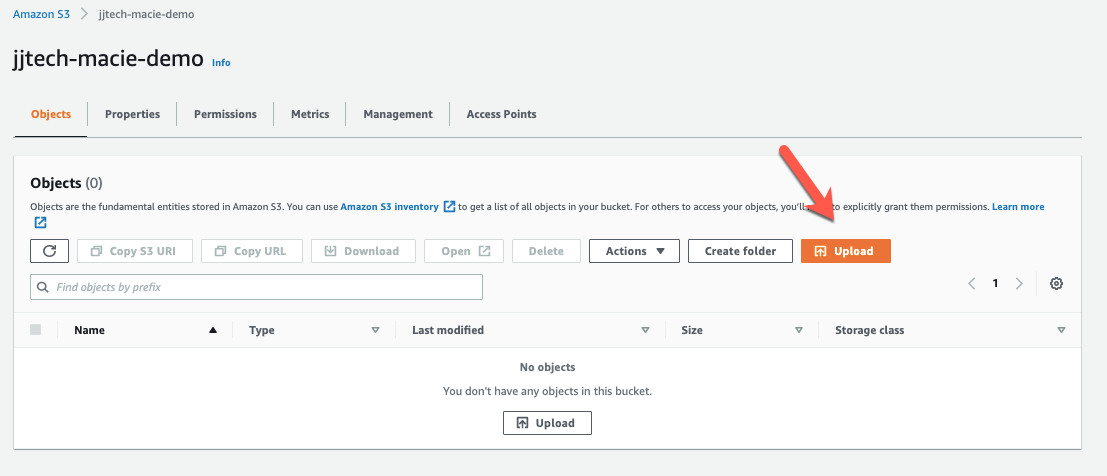


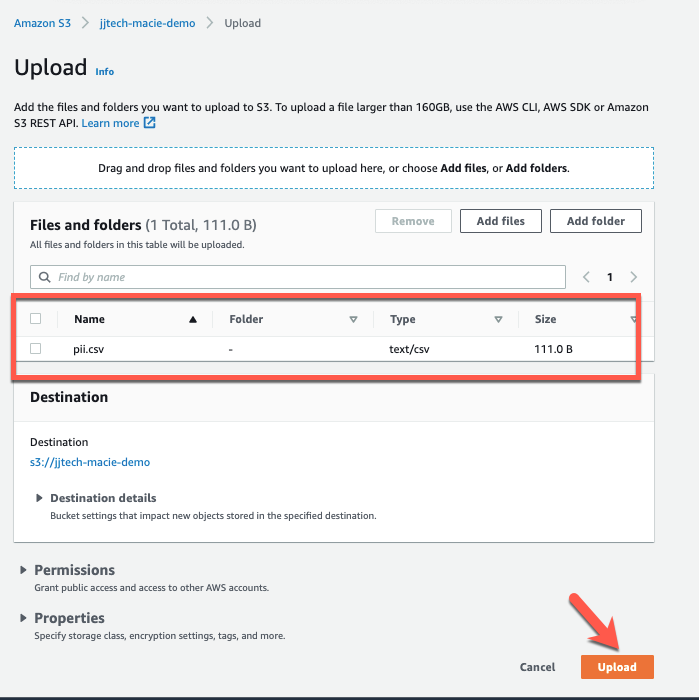


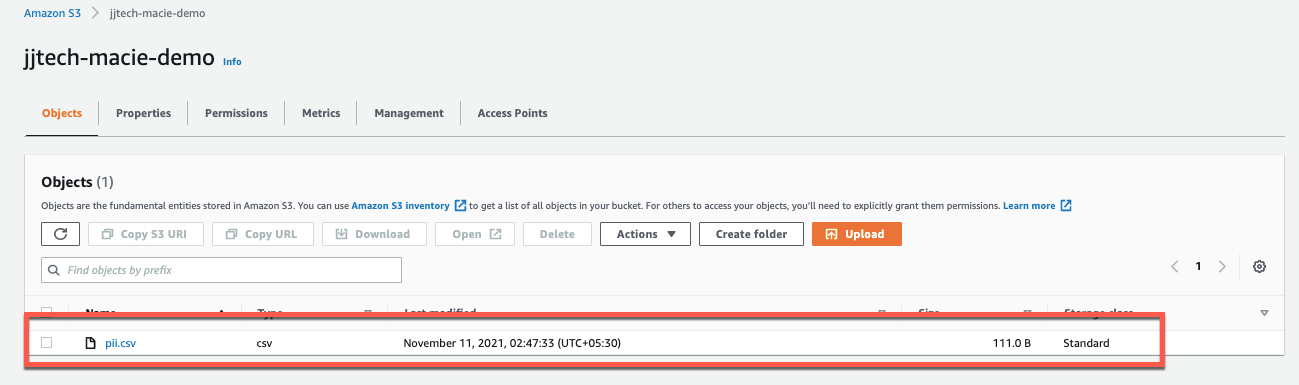
Step 2:

* I have created an excel sheet with employee data. You can download it from below link and upload it to the above S3 bucket
* <https://drive.google.com/file/d/1tlVZVLr1fNtkERG-Yy2mglzdf2qntwQn/view?usp=sharing>



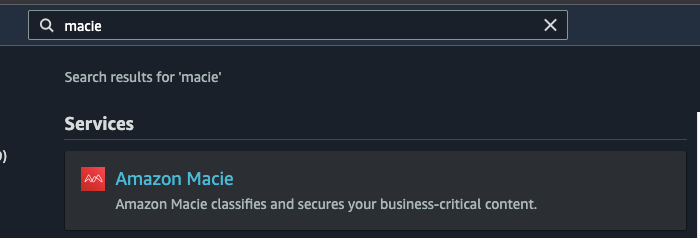


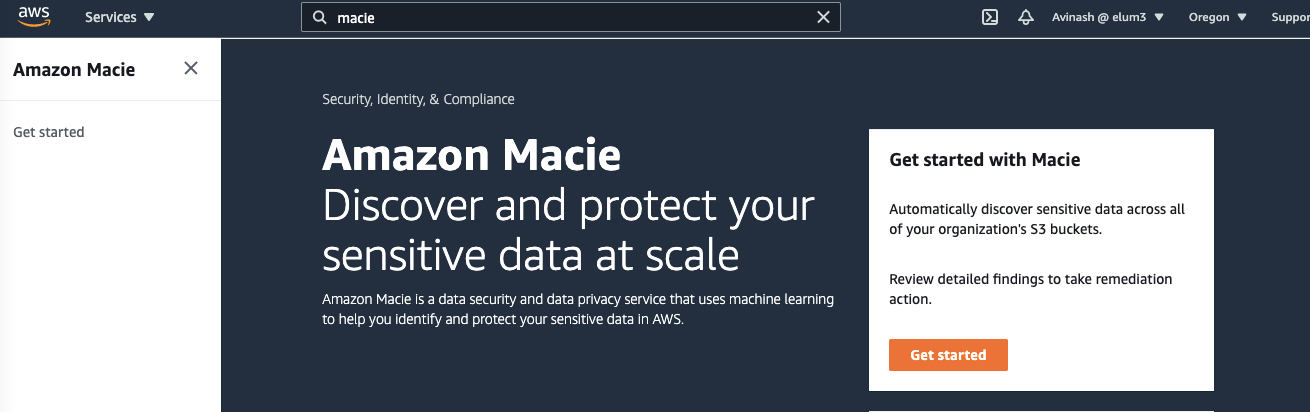


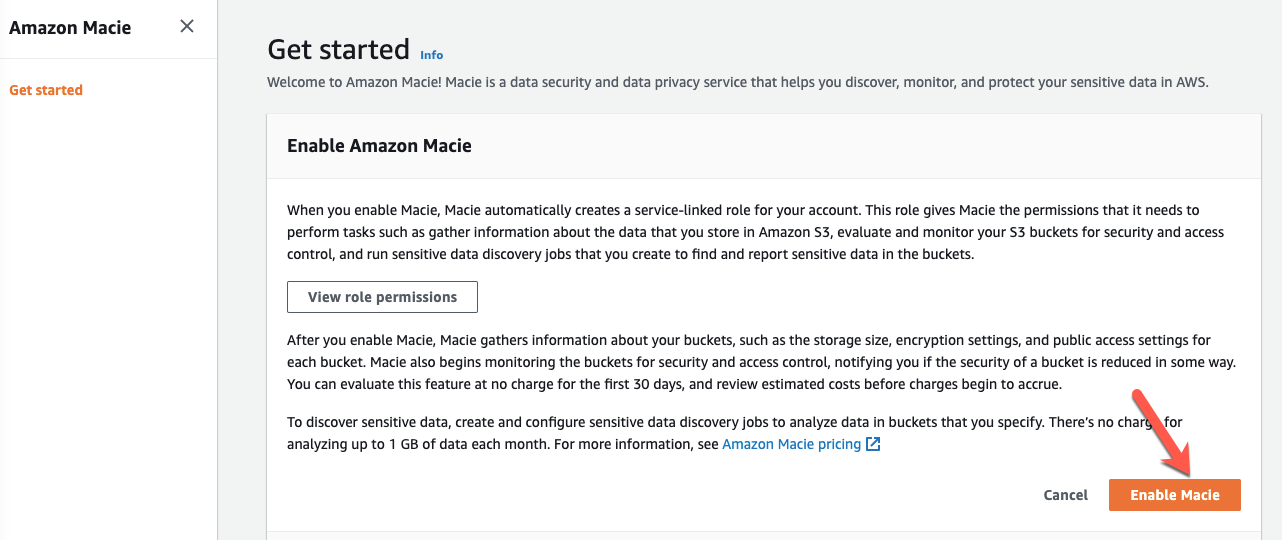


Step 3:

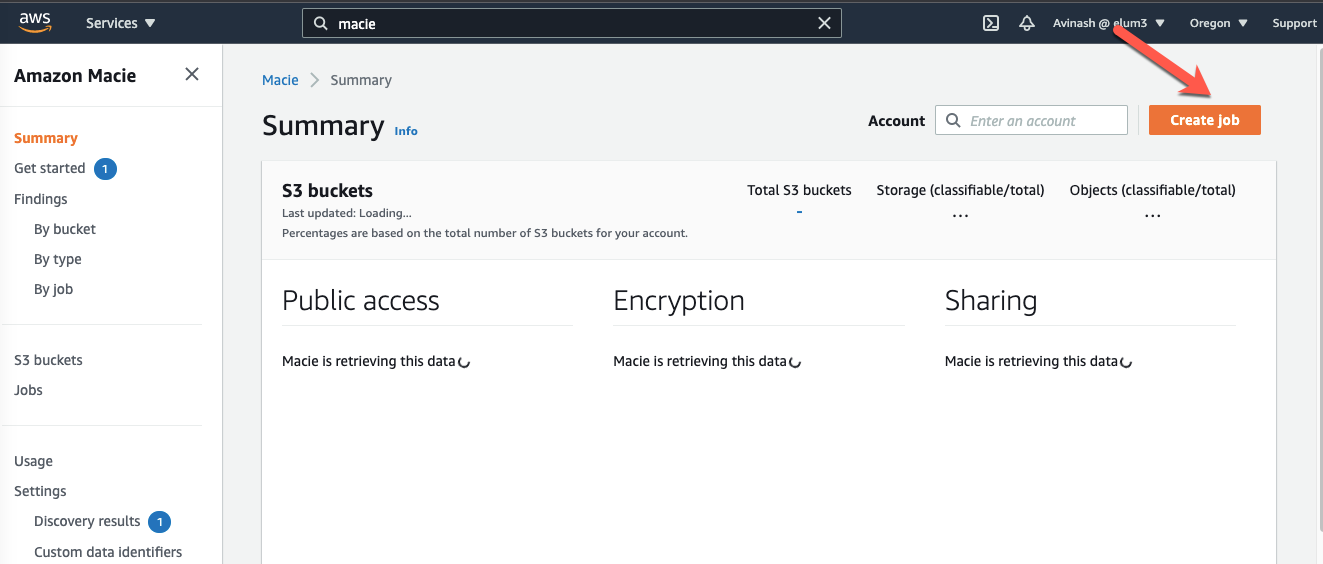
* Navigate to AWS Macie console

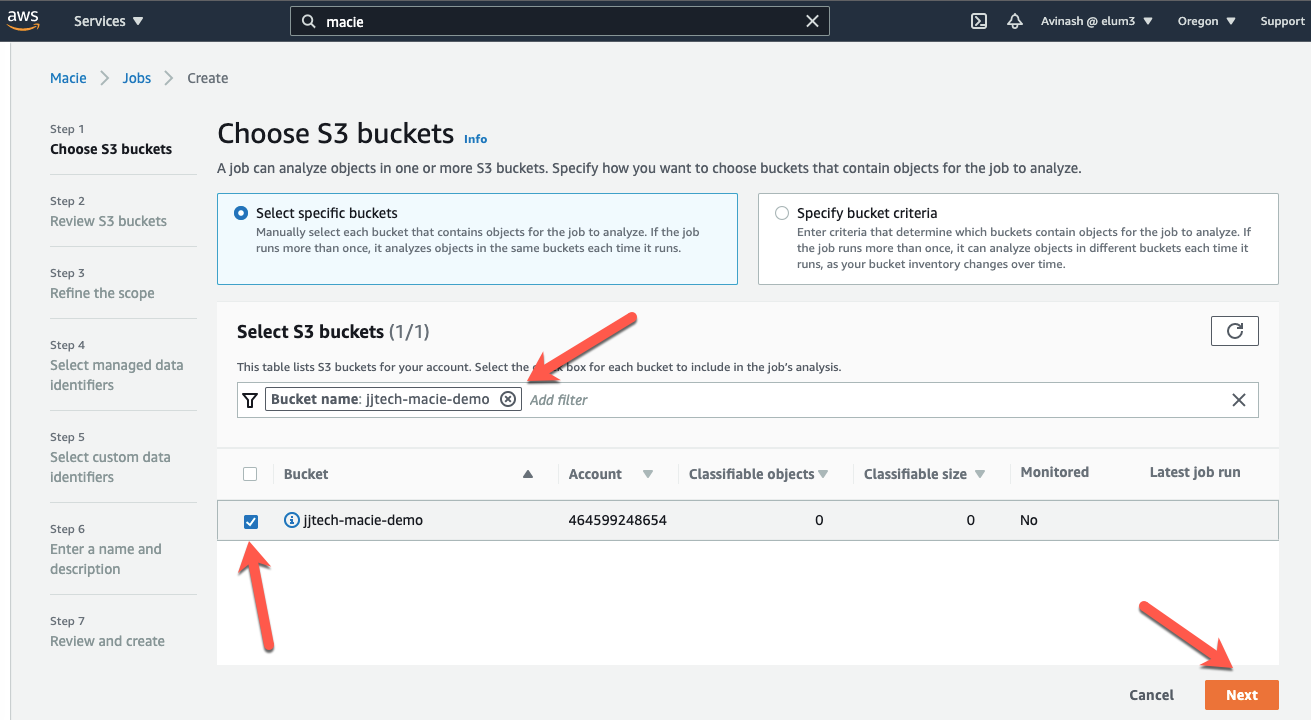


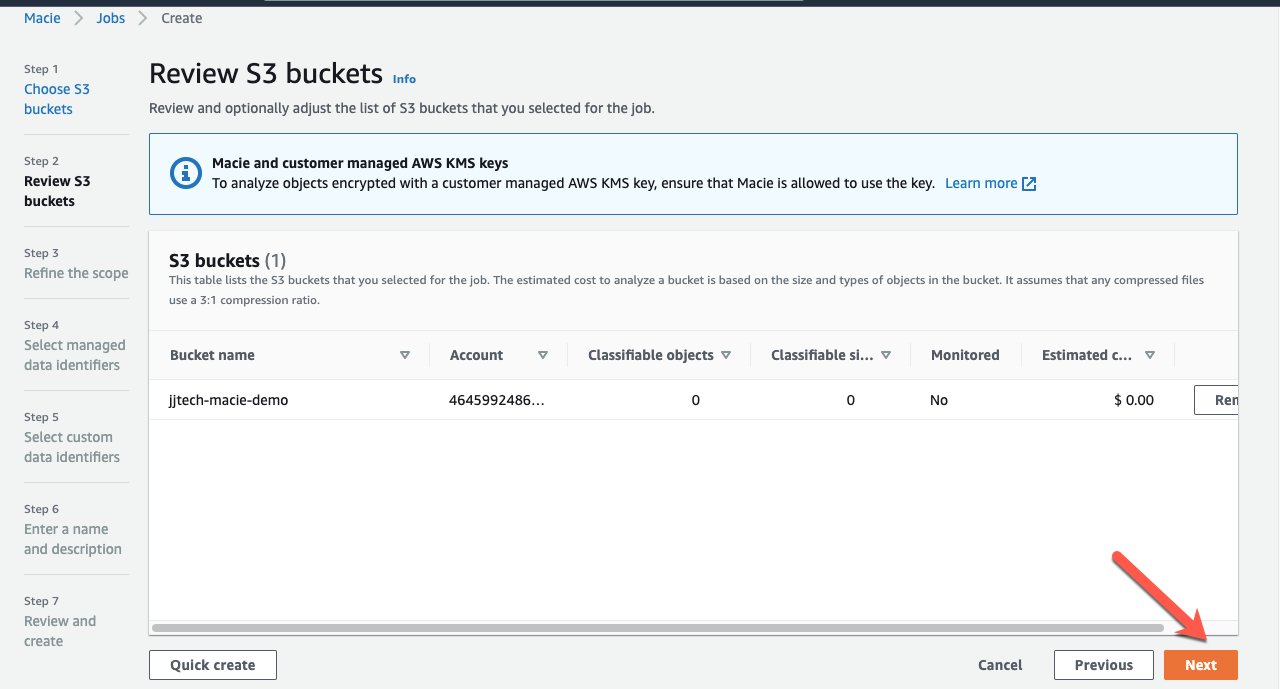


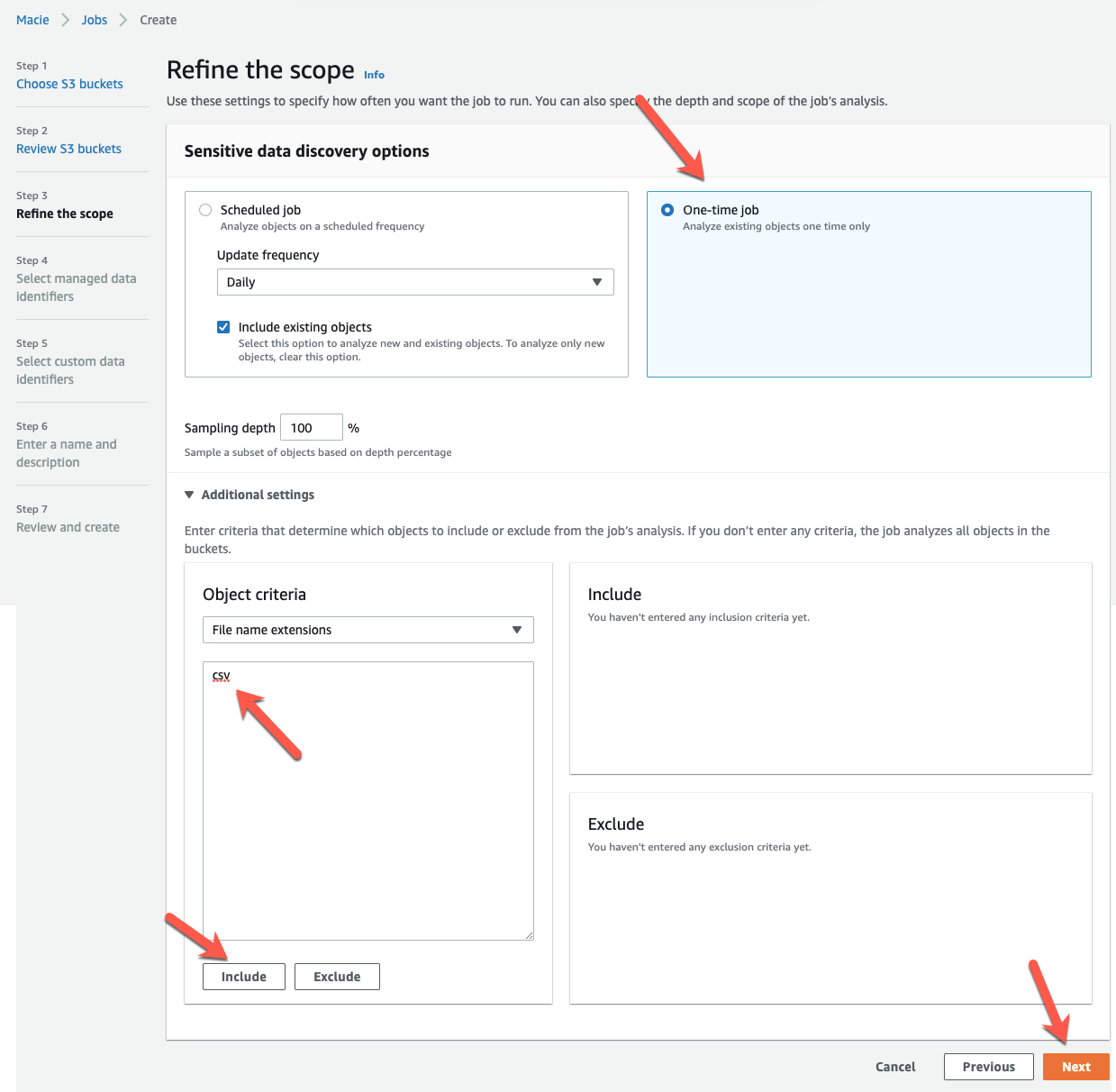


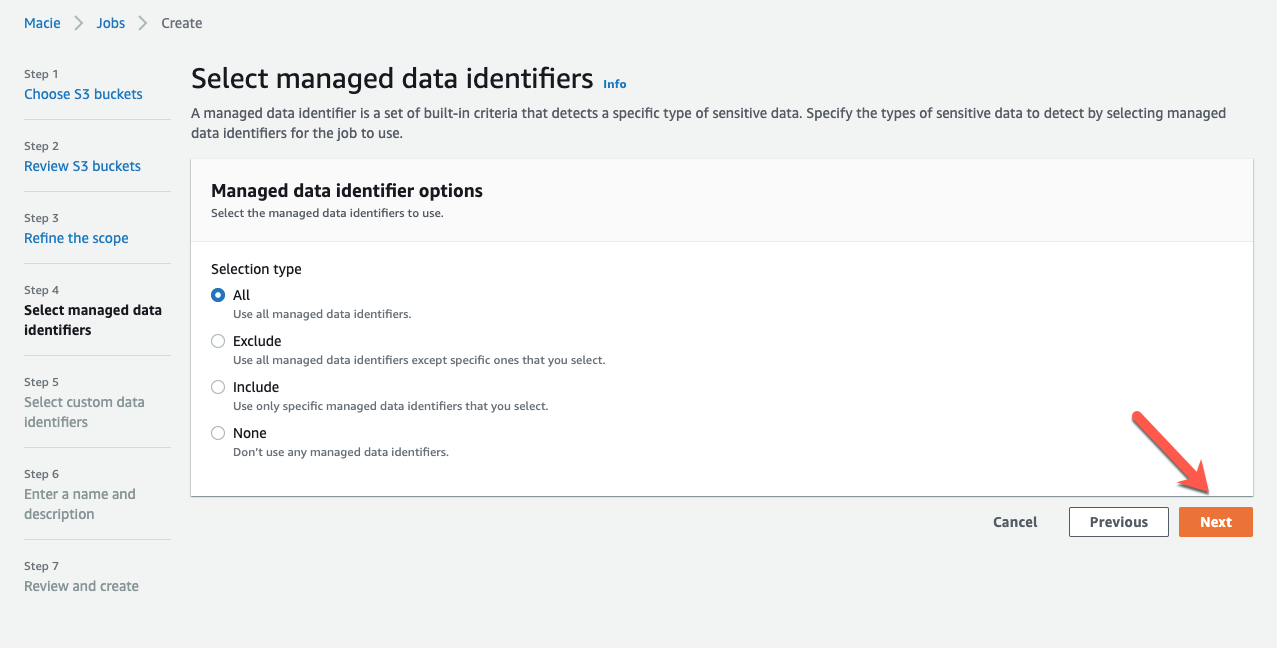
* Create a Macie job

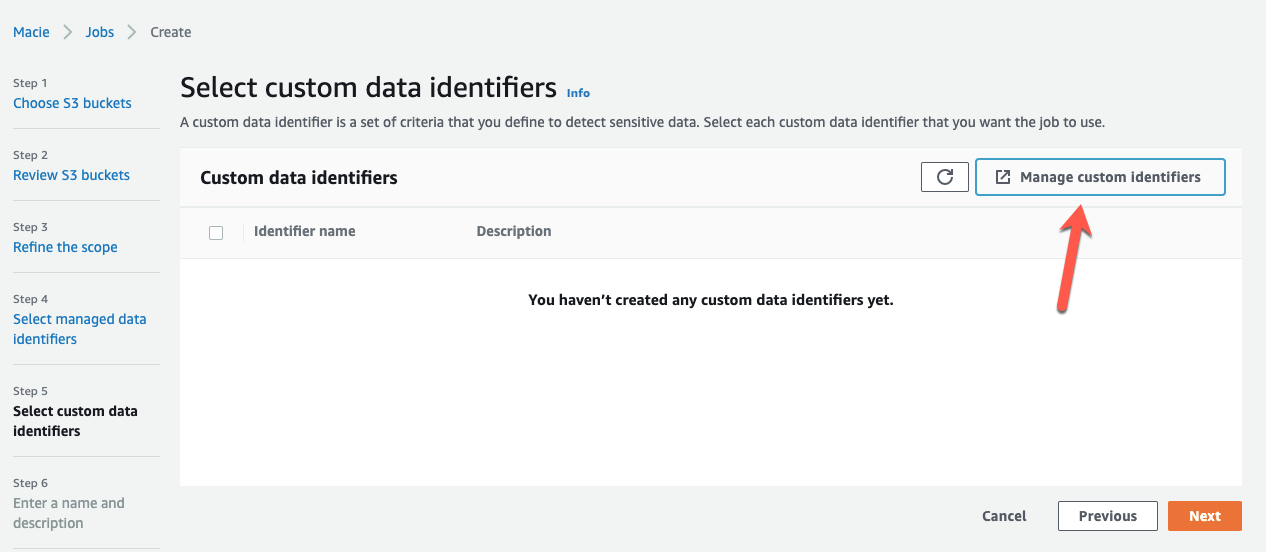


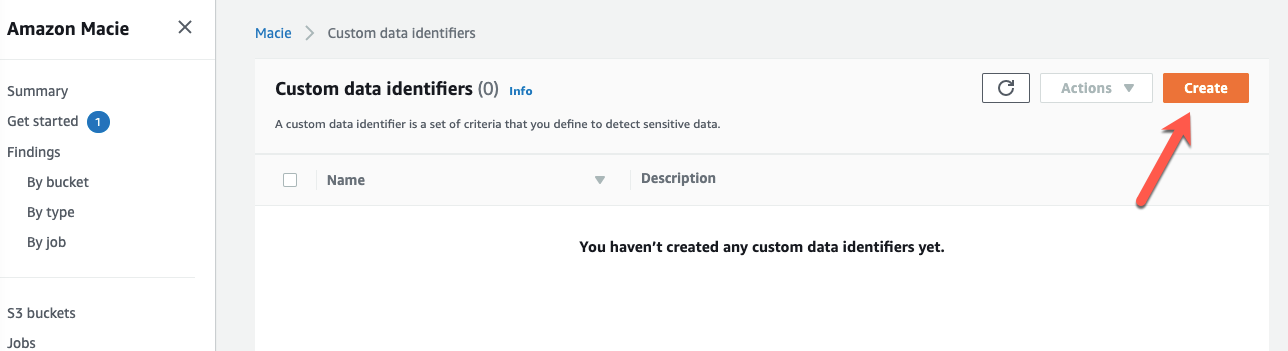


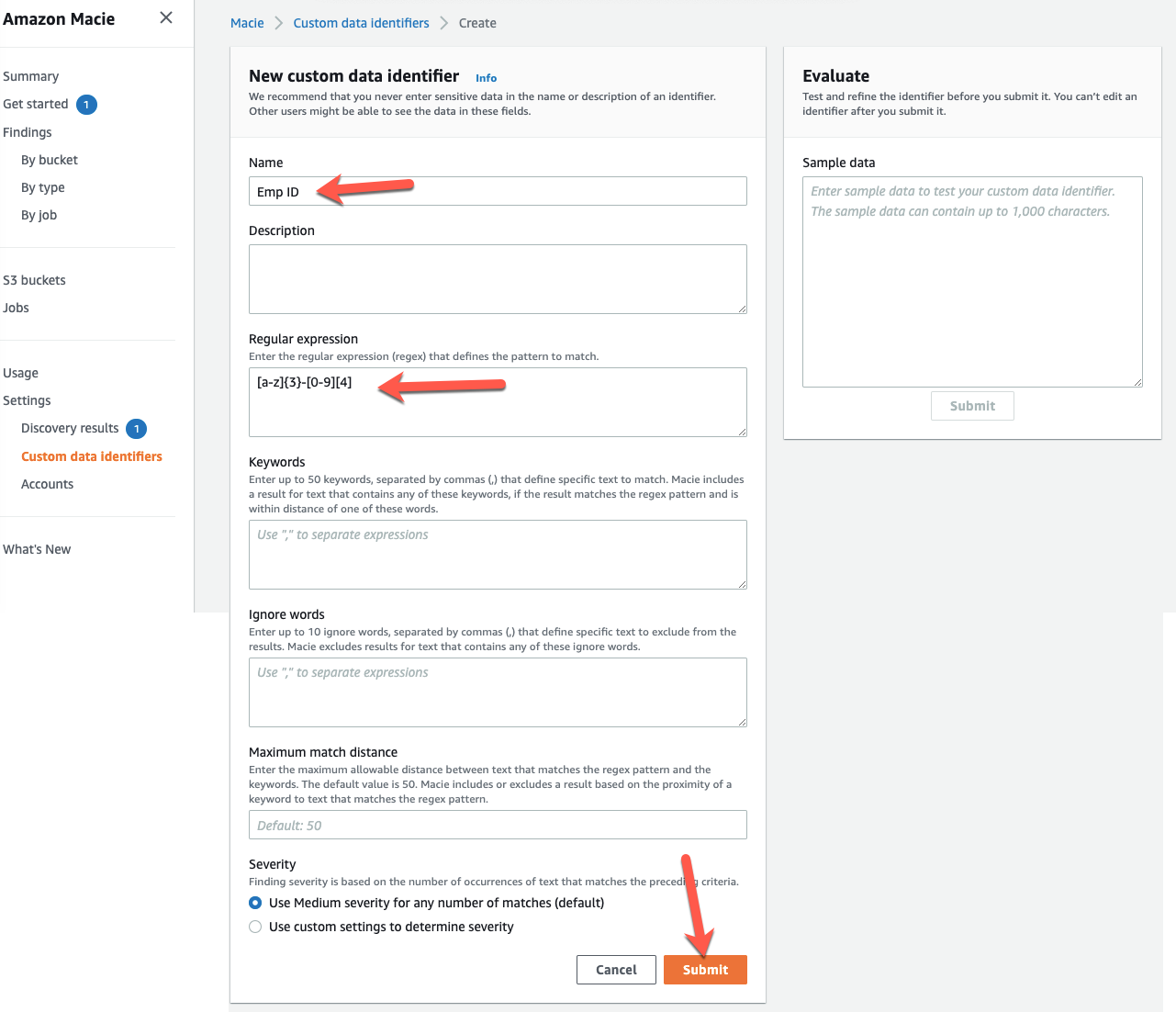


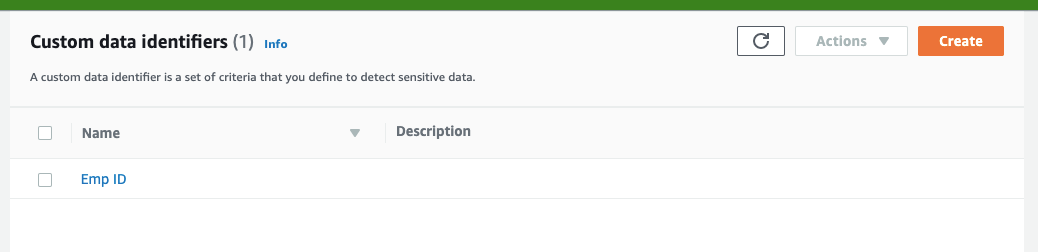


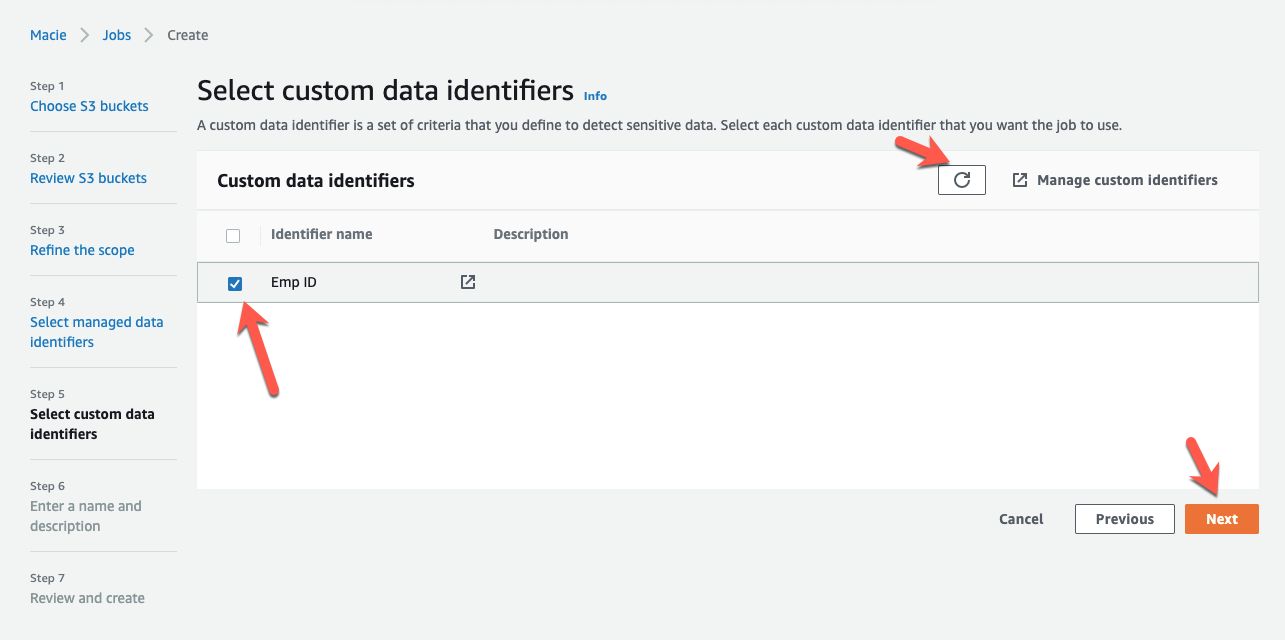


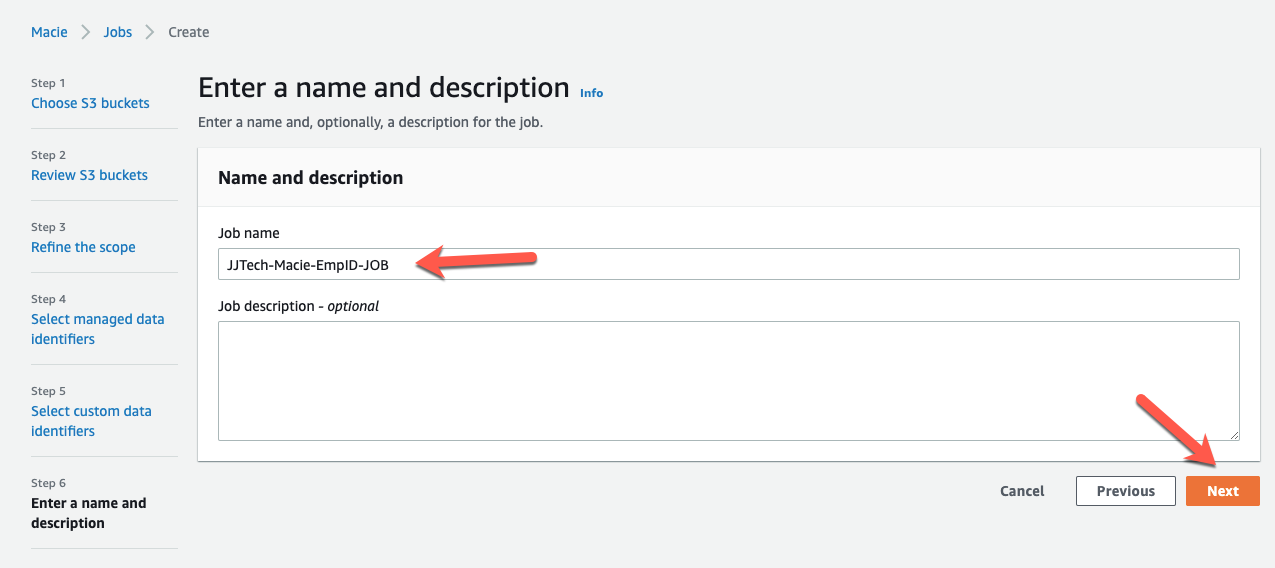


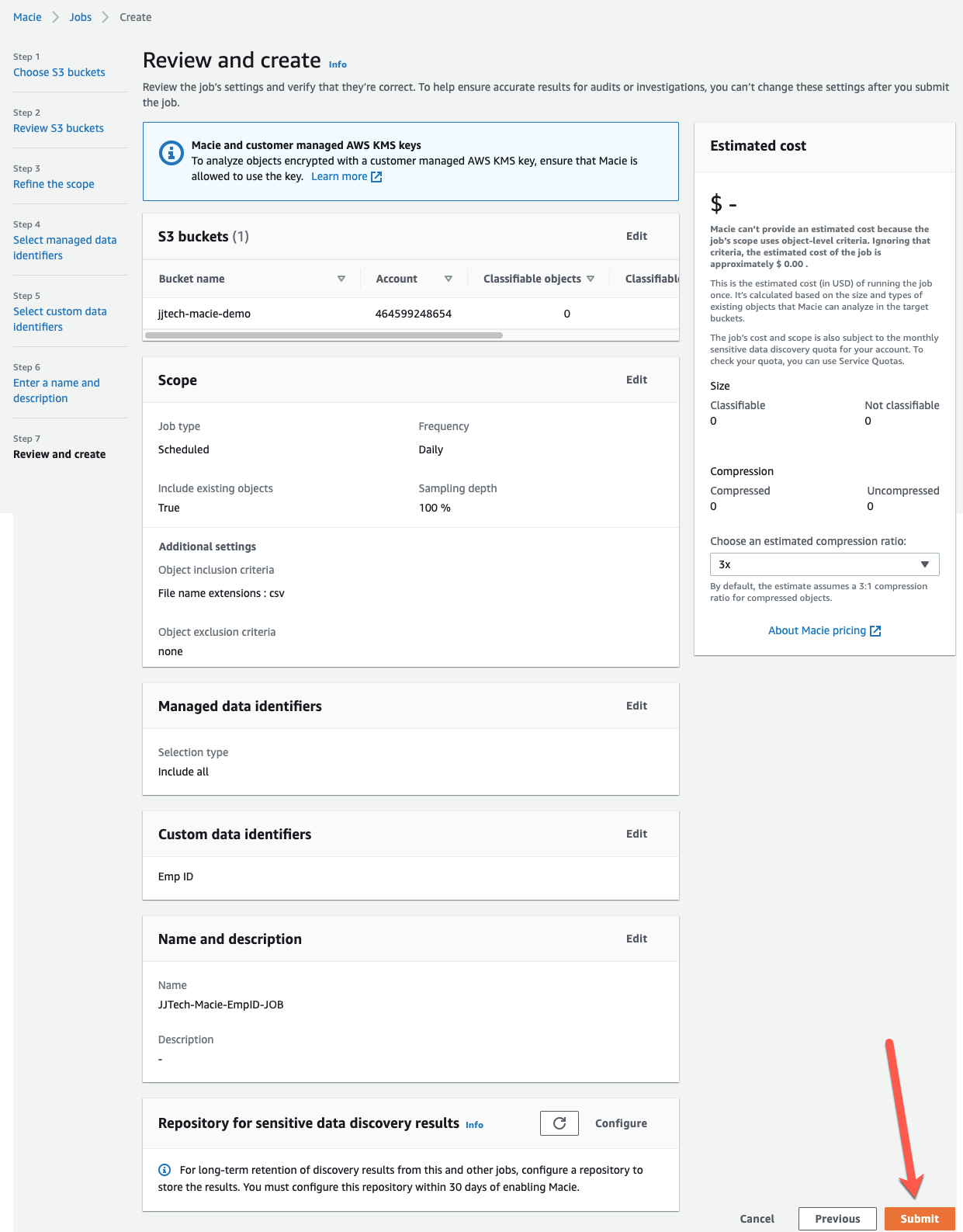












* We have to wait for approx. 10 mins to so that Macie Job will scan the whole S3 bucket we created and read all the contents in the objects and find PII data

