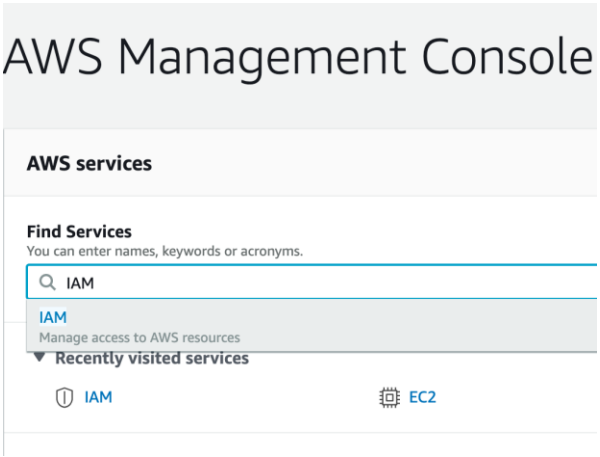
CYBRAICS

nLighten™

AWS S3 Read Access Configuration Guide

Stage 1: Create IAM Security Credentials in AWS

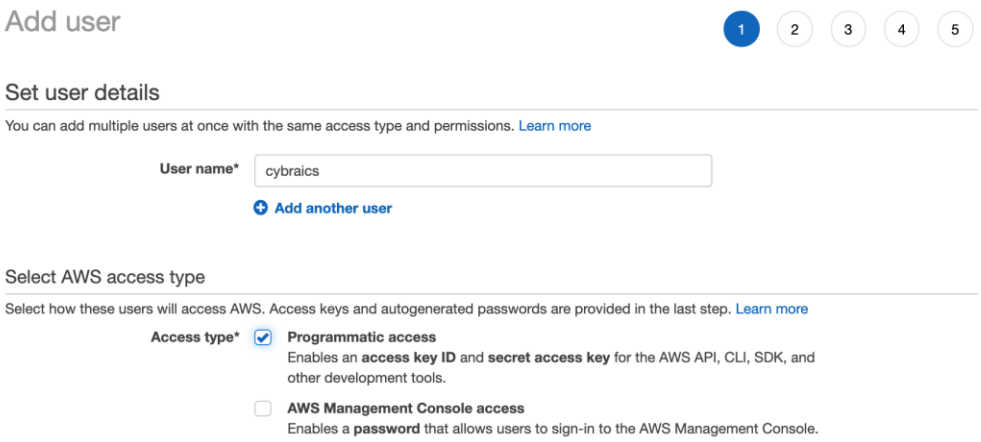
1. Add an access key to your Amazon Web Services account to allow for remote access and give the ability to read files in S3. Log into AWS and type **IAM** in the search field.



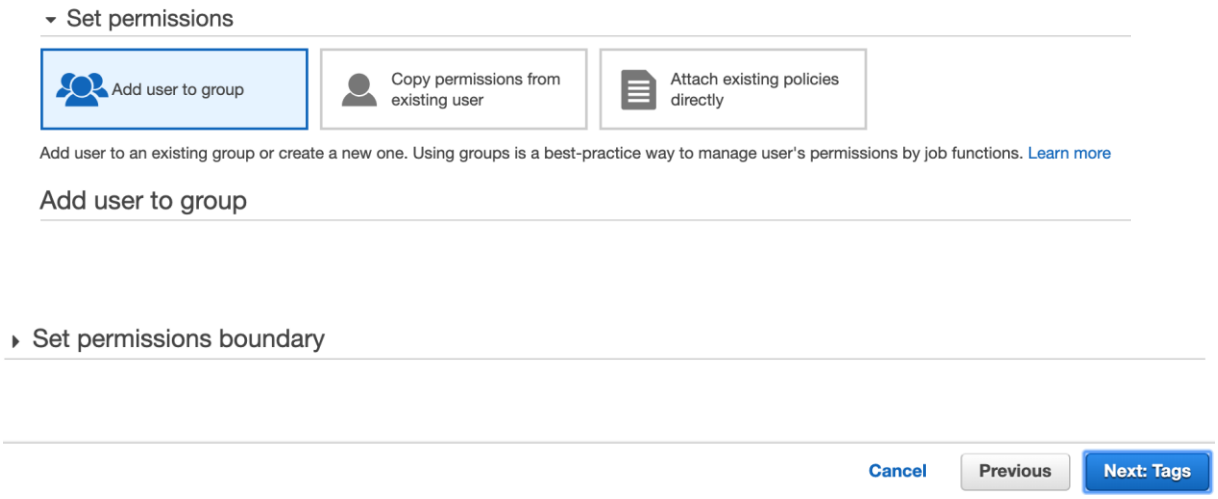
2. By creating a Cybraics IAM user account, you can give the IAM user a unique set of security credentials. You can also grant different permissions to the user. If necessary, you can change or revoke an IAM user's permissions at any time.

   For more information on IAM users and AWS best practice, read here: http://docs.aws.amazon.com/IAM/latest/UserGuide/IAMBestPractices.html

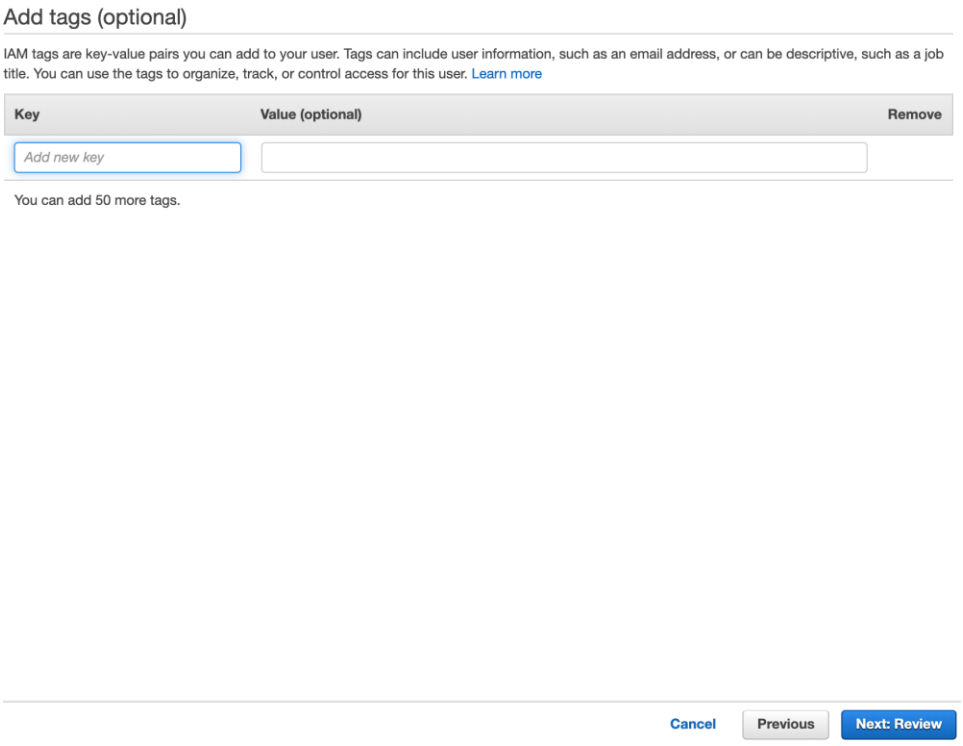
3. Create an IAM cybraics user to access your S3 bucket by clicking **Add User**. You're taken to a screen where you can create an IAM User. Select **Programmatic access**



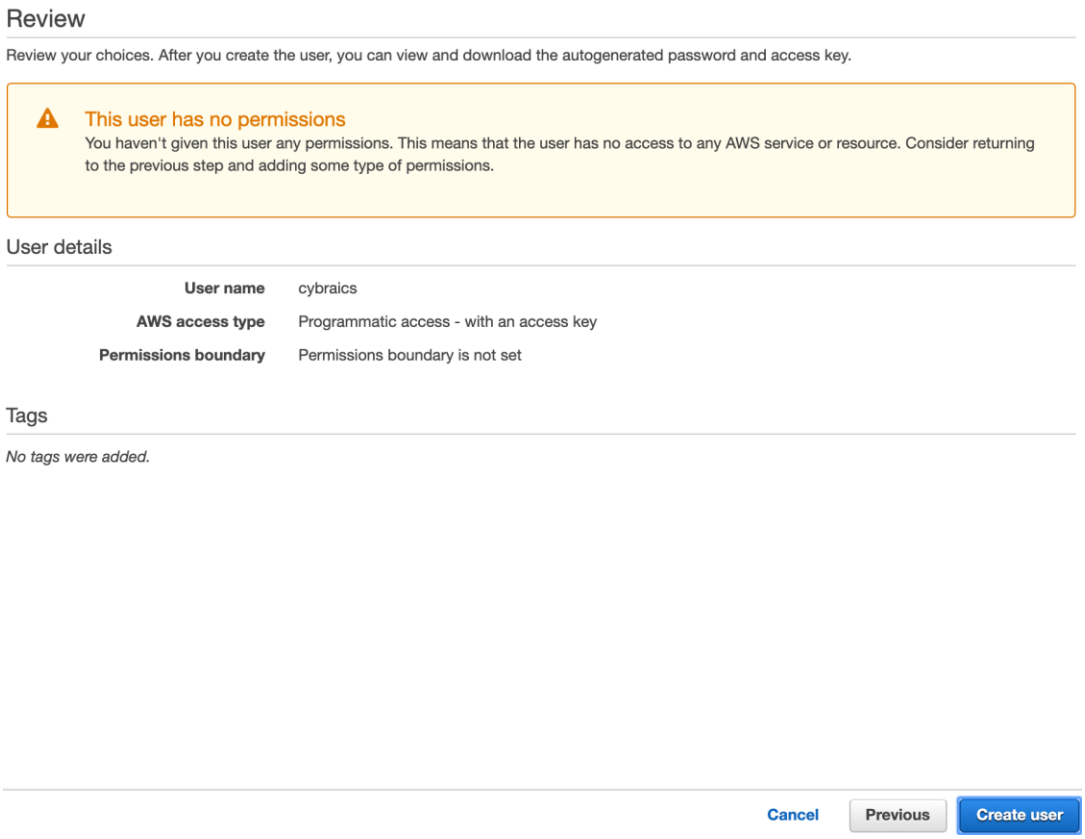
4. Click **Next: Permission**, do not apply group or policy configuration. Select **Next: Tags**



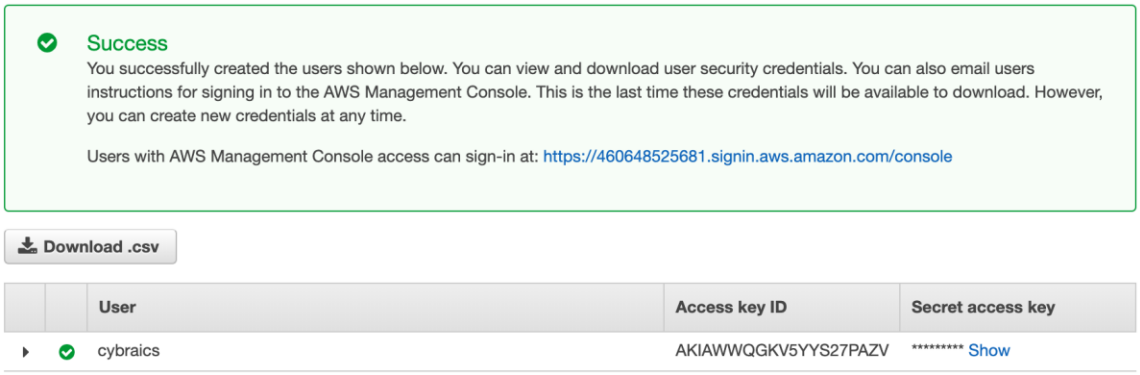
5. Click **Next: Review**, Optional: apply tag information



6. Click: **Create User**



7. After creating the user account, send the AWS Access and Secret keys to a Cybraics Engineer. **Ensure to send via encrypted email or other secure means**.



Stage 2: Configuring your S3 Bucket Policy

1. Select the S3 Bucket where the cybraics user will download the required logs. Choose **Bucket Policy** and paste JSON below. Edit to match your AWS account settings. **In some cases, you may need to merge the policy listed with existing permissions. Consult with your AWS IAM team to ensure there will be no conflict.**


```
{
    "Statement": [
        {
            "Sid": "CybraicsReadOnlyAccess",
            "Effect": "Allow",
            "Principal": {
                "AWS": [

"arn:aws:iam::123456789:user/cybraics"
                ]
            },
            "Action": [
```