IAM Policies for Vantage AWS S3 Workflows

Overview

In order for Vantage workflows to interact with buckets in an AWS S3 system, the AWS user specified in each action in the workflow (as identified by the Access Key ID) accessing the bucket must apply appropriate permissions to enable the action to perform its task (reading or writing files, for example).

Specific SNS and SQS policies must also be set for Vantage workflows using Watch or Associate actions.

This document details which permissions must be specified in the IAM policy for the Vantage actions to perform the specified tasks. If the policies are not configured correctly, the Vantage workflow reports an Access Denied error.

Note: Telestream does not recommend a specific cloud security policy and Telestream does not recommend how you configure your object store. These examples demonstrate the IAM permission elements utilized by Vantage. You are responsible for granting these permissions to Vantage services in accordance with your organization's cloud security policy.

Refer to AWS guides for information about applying IAM policies:

- Getting Started: https://docs.aws.amazon.com/IAM/latest/UserGuide/getting-started.html
- IAM Best Practices: https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html
- Access Permissions to Amazon S3 Resources: https://docs.aws.amazon.com/AmazonS3/latest/dev/s3-access-control.html
- Amazon Resource Names (ARNs): https://docs.aws.amazon.com/general/latest/gr/aws-arns-and-namespaces.html
- Bucket Policy Examples: https://docs.aws.amazon.com/AmazonS3/latest/dev/example-bucket-policies.html

Bucket Action Permissions	Vantage Action Task	Resource Scope
s3:ListAllMyBuckets	Required for all actions when Browse: All Buckets is checked. Optionally, each action must be configured with Browse: Single Bucket and specify the ARN of the target bucket.	Global [*]
s3:ListBucket	Required for each action unless it is configured with Browse: All Buckets.	Target bucket [ARN of bucket]
s3:GetObject	Required for Copy | Deploy | Move actions configured to download files.	All files in target bucket [ARN of bucket]/*
s3:PutObject	Required for Copy | Deploy | Move actions configured to upload files.	All files in target bucket [ARN of bucket]/*
s3:DeleteObject	Required for Delete | Move actions configured to delete files.	All files in target bucket [ARN of bucket]/*
s3: ListObjects	Required for Watch | Associate actions configured to monitor buckets for new files.	Global [*]
S3:GetBucketLocation	Required for Watch | Associate actions configured to monitor buckets for new files.	Target bucket(s) [ARN of bucket(s)]
s3:GetBucketNotification		
s3:PutBucketNotification		

Amazon Simple Storage Service (S3)

Syntax: `arn:aws:s3:::bucket_name`

Amazon S3 does not require an account-id or region in ARNs. You can optionally use a wildcard ("*") character in the ARN resource component.

Example S3 Bucket Policy

```
{
  "Version": "<YOUR_S3_BUCKET_POLICY_VERSION>",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "s3:GetBucketLocation",
        "s3:GetBucketNotification",
        "s3:PutBucketNotification"
      ],
      "Resource": "arn:aws:s3:::<TARGET_BUCKET>/*"
    },
    {
      "Effect":"Allow",
      "Action":[
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:PutObject",
        “s3:ListBucket”
      ],
      "Resource": "arn:aws:s3:::<TARGET_BUCKET>/*"
    },
  ]
}
```

SNS Action Permissions	Vantage Action Task	Resource Scope
sns:CreateTopic	Required for Watch | Associate actions configured to monitor buckets.	Topic created by Vantage: VantageS3Watcher_[target-bucket-name] [ARN of topic created by Vantage]
sns:DeleteTopic		
sns:GetTopicAttributes		
sns:ListSubscriptionsByTopic		
sns:SetTopicAttributes		
sns:Subscribe		
sns:Unsubscribe		Global [*]

Amazon Simple Notification Service (SNS)

Syntax: `arn:aws:sns:region:account-id:topicname`

Example SNS Policy

```
{
  "Version":"<YOUR_SNS_POLICY_VERSION>",
  "Statement":[
     {
       "Effect":"Allow",
       "Action":[
         "sns:CreateTopic",
         "sns:DeleteTopic",
         "sns:GetTopicAttributes",
         "sns:ListSubscriptionsByTopic",
         "sns:SetTopicAttributes",
         "sns:Subscribe"
       ],
       "Resource”:”arn:aws:sns:<YOUR_REGION>:<YOUR_ACCOUNT_ID>:<YOUR_TOPIC_NAME>/*"
    },
    {
      "Effect":"Allow",
      "Action":"sns:Unsubscribe",
      "Resource":"*"
    }
  ]
}
```

SQS Action Permissions	Vantage Action Task	Resource Scope
sqs:CreateQueue	Required for Watch | Associate actions configured to monitor buckets.	Queue Topic created by Vantage: VantageS3Watcher<GUID> Note: The GUID is created by Vantage. The use of a wildcard in place of <GUID> above is required.
sqs:DeleteMessage		
sqs:DeleteMessageBatch		
sqs:DeleteQueue		
sqs:GetQueueAttributes		
sqs:GetQueueUrl		
sqs:PurgeQueue		
sqs:ReceiveMessage		
sqs:SetQueueAttributes		
sqs:ListQueues		Global [*]

Amazon Simple Queue Service (SQS)

Syntax: `arn:aws:sqs:region:account-id:queuename`

Example SQS Policy

```
{
  “Version”:”YOUR_SQS_POLICY_VERSION”,
  “Statement”:[
    {
      “Effect”:”Allow”,
      “Action”:[
        “sqs:DeleteMessage”,
        “sqs:GetQueueUrl”,
        “sqs:DeleteMessageBatch”,
        “sqs:PurgeQueue”,
        “sqs:ReceiveMessage”,
        “sqs:DeleteQueue”,
        “sqs:GetQueueAttributes”,
        “sqs:CreateQueue”,
        “sqs:SetQueueAttributes”
      ],
        “Resource”:”arn:aws:sqs:*:*:<TARGET_BUCKET>/*”
    },
    {
      “Effect”:”Allow”,
      “Action”:”sqs:ListQueues”,
      “Resource”:”*”
    }
  ]
}
```