AWS S3 Connector Configuration Setup Details

This article reviews the permissions that must be assigned in your S3 bucket policy and what you are required to do if you have a **SourceIP condition block** specified in your bucket policy.

Required Permissions

The AWS S3 connector requires specific permissions in your S3 bucket policy to ensure that you can successfully import data from S3, publish to S3, and automate importing from an S3 source. In summary:

- The connector requires the `s3:ListBucket` permission on the bucket.
- For import and publish, the bucket contents requires the permissions `s3:ListBucket` and `s3:GetObject`
- For export, the bucket contents requires the permission `s3:PutObject` .

Sample bucket policy example:

```
{
	"Version": "2012-10-17",
	"Statement": [
		{
			"Sid": "Stmt1965292834357",
			"Effect": "Allow",
			"Principal": {
				"AWS": [
					"arn:aws:iam::123456781234:user/pax01",
					"arn:aws:iam::432143214321:user/pax02",
					"arn:aws:iam::121212343434:user/pax03"
				]
			},
			"Action": "s3:ListBucket",
			"Resource": "arn:aws:s3:::paxhh-session1"
		},
		{
			"Sid": "Stmt1965293102818",
			"Effect": "Allow",
			"Principal": {
				"AWS": [
					"arn:aws:iam::123456781234:user/pax01",
					"arn:aws:iam::432143214321:user/pax02",
					"arn:aws:iam::121212343434:user/pax03"
				]
			},
			"Action": [
				"s3:DeleteObject",
				"s3:DeleteObjectVersion",
				"s3:GetObject",
				"s3:GetObjectAcl",
				"s3:GetObjectTorrent",
				"s3:GetObjectVersion",
				"s3:GetObjectVersionAcl",
				"s3:GetObjectVersionTorrent",
				"s3:PutObject",
				"s3:PutObjectAcl",
				"s3:PutObjectVersionAcl"
			],
			"Resource": "arn:aws:s3:::paxhh-session1/*"
		}
	]
}
```

Important:
The minimum policy permissions for reading from an S3 bucket are:

```
{
     "Version": "2012-10-17",
     "Statement": [
          { "Effect": "Allow", "Action": "s3:ListBucket", "Resource":
          "arn:aws:s3:::mybucketname"
          },
     { "Effect": "Allow", "Action": [ "s3:ListBucket", "s3:GetObject" ],
     "Resource": "arn:aws:s3:::mybucketname/*" }
     ]
}
```

The minimum policy permissions for writing to an S3 bucket are:

```
{
     "Version": "2012-10-17",
     "Statement": [
          { "Effect": "Allow", "Action": "s3:ListBucket", "Resource":
          "arn:aws:s3:::mybucketname"
          },
     { "Effect": "Allow", "Action": [ "s3:ListBucket", "s3:GetObject",
     "s3:PutObject" ], "Resource": "arn:aws:s3:::mybucketname/*" }
     ]
}
```

For a detailed explanation of S3 buckets, refer to: Working with Amazon S3 Buckets (http://docs.aws.amazon.com/AmazonS3/latest/dev/UsingBucket.html).

SourceIP condition block

If there is a **SourceIP condition block** specified in your bucket policy, then you must include the IP addresses of your Paxata cloud servers or Paxata Core Server (depending on your Paxata deployment) in the **Source IP Condition block**. In addition, if you have a dedicated Paxata server for automation, you must also include the automation server IP addresses in the **SourceIP Condition block**.

Please consult with Paxata's Customer Success team to obtain the list of IP addresses for Paxata cloud servers.

For details on the `condition block` element, and exmaples, see Specifying Conditions in a Policy (http://docs.aws.amazon.com/AmazonS3/latest/dev/amazon-s3-policy-keys.html) and Identity and Access Management (IAM) Policy Elements Reference (http://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements.html#Condition).