# AWS CLOUD DISCOVERY



Agent-less discovery for no-scan always on detection powered by ThreatWatch



## **CONFIGURING YOUR AWS ENVIRONMENT**

Identify the instances that you need vulnerability tracking for via the AWS Console or AWS CLI.

Ensure each of those instances have the SSM agent installed on them. More information can be found here,

- Installing SSM on Linux: https://docs.aws.amazon.com/systemsmanager/latest/userguide/ sysman-install-ssm-agent.html
- Installation SSM on Windows (if needed):
   https://docs.aws.amazon.com/systemsmanager/latest/userguide/sysman-install-ssm-win.html



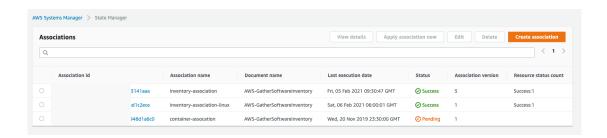
### **ROLE ASSIGNMENT**

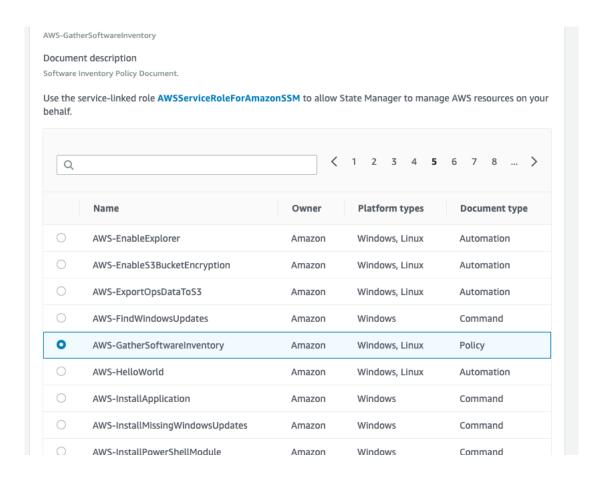
Ensure that each of those instances have the Systems Manager role assigned to them. This is necessary for your EC2 instances to talk to Systems Manager using the SSM agents.



# **SETUP ASSOCIATION**

Setup an association between Systems Manager and State Manager using an AWS document (AWSGatherSoftwareInventory).





# SETUP INVENTORY COLLECTION & DESTINATION S3 BUCKET

Select the type of inventory that you would like to collect and a S3 bucket that will collect that inventory with bucket policy. Bucket prefix is not required to be specified in the policy.

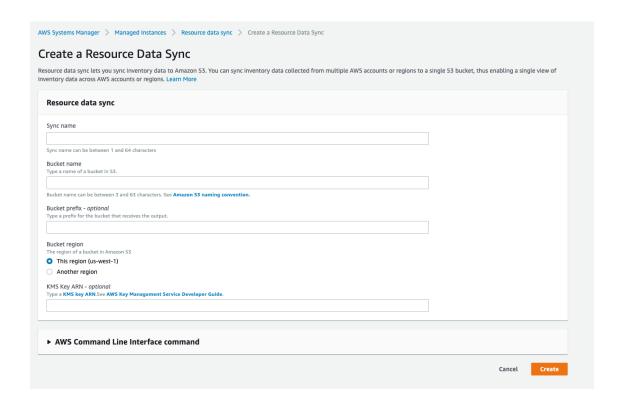
etup Inventory eate an inventory association to collect info	formation about software and settings for a target set of managed instances.
Provide inventory details	
Name - Optional	
Inventory-Association	
Provide a name for your Inventory.	
Targets	
Specify targets by	
Selecting all managed instances in thi	s account
Specifying a tag     Manually selecting instances	
Schedule	
(Requires SSMAgent version 2.0.790.0 and above	
Collect inventory data every 30	Minute(s) ▼
Parameters	

```
Bucket policy
The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. Learn more 

{
    "Sid": "SSMBucketPermissionsCheck",
    "Effect": "Allow",
    "Principal": {
        "Service": "ssm.amazonaws.com"
        },
        "Action": "s3:GetBucketAcl",
        "Resource": "arn:av
        },
        {
        "Sid": "SSMBucketDelivery",
        "Effect": "Allow",
        "Principl": {
        "Service": "ssm.amazonaws.com"
        },
        "Action": "s3:PutObject",
        "Resource": "arn:aws:s3::in
        "/*/accountid=00
        ",
        "Condition": {
        "StringEquals": {
              "S3:a-amz-acl": "bucket-owner-full-control"
        }
    }
```

## SETUP RESOURCE DATA SYNC

Setup the resource data sync in the systems manager by specifying the name of the provisioned S3 bucket.



6

#### **INVENTORY IN S3 BUCKET**

You should now see inventory in the S3 bucket for each instance that is configured for inventory collection. There will be a single JSON file corresponding to each instance.

7

### PULL ASSET INVENTORY INTO THREATWATCH

Using the twigs CLI you can now pull the inventory into your ThreatWatch instance (threatwatch.io for public SaaS or yourcompany.threatwatch.io for dedicated).

```
twigs -v aws --aws_account "[ACCOUNT_ID]" --
aws_access_key "[AWS_ACCESS_KEY]" --aws_secret_key "
[AWS_SECRET_KEY]" --aws_region "[AWS_REGION]" --
aws_s3_bucket "[S3_BUCKET]"
```

Checkout twigs guide & help videos for additional options including CIS benchmark checks for your cloud,

https://threatwatch.io/twigs-user-guide/#aws-discovery

## THREATWATCH 13 CONSOLE

Analytics, security vulnerabilities, mis-configurations, static and dynamic analysis for base images, running apps and containers can now be managed from the I3 console.

