AWS CLOUD WORKLOAD PROTECTION

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

threatworx

amazon web services

1 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/systems-manager/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

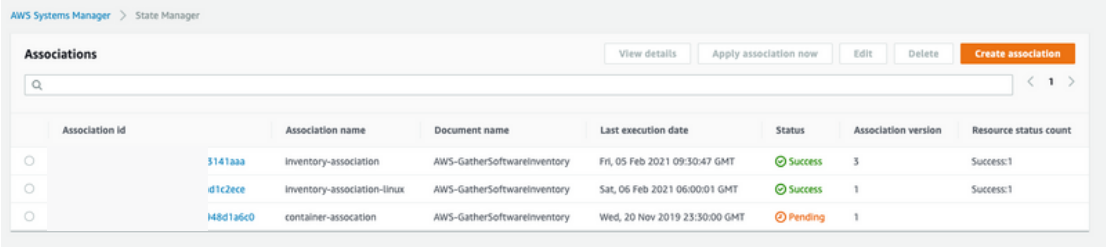
2 ROLE ASSIGNMENT

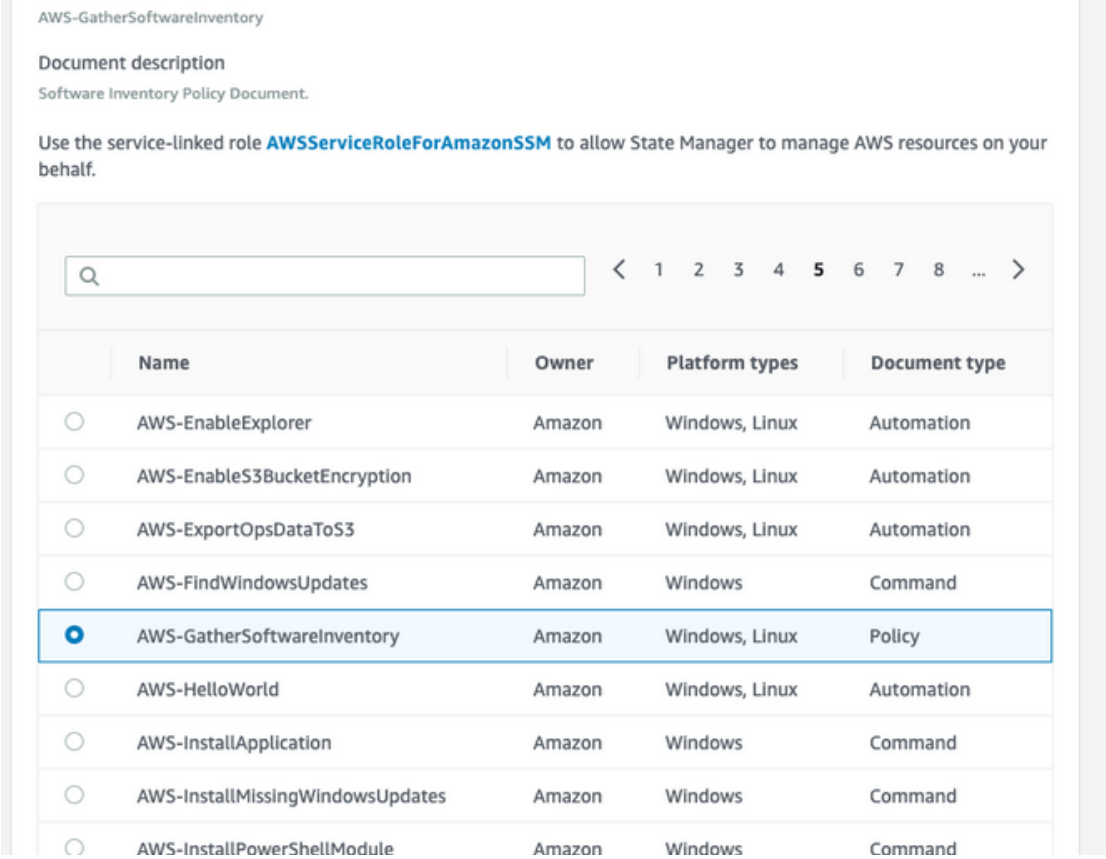
Ensure that each of those instances have the Systems Manager role assigned to them. This is necessary for your EC2 instances to talk to Systems Manager using the SSM agents.

3

SETUP ASSOCIATION

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

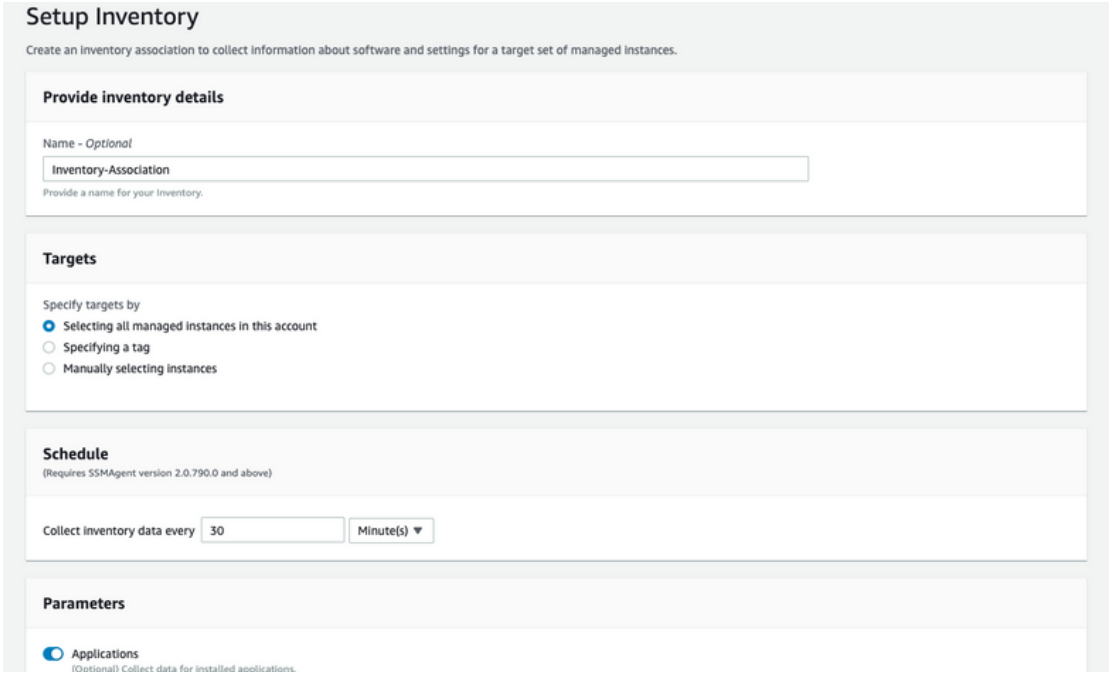


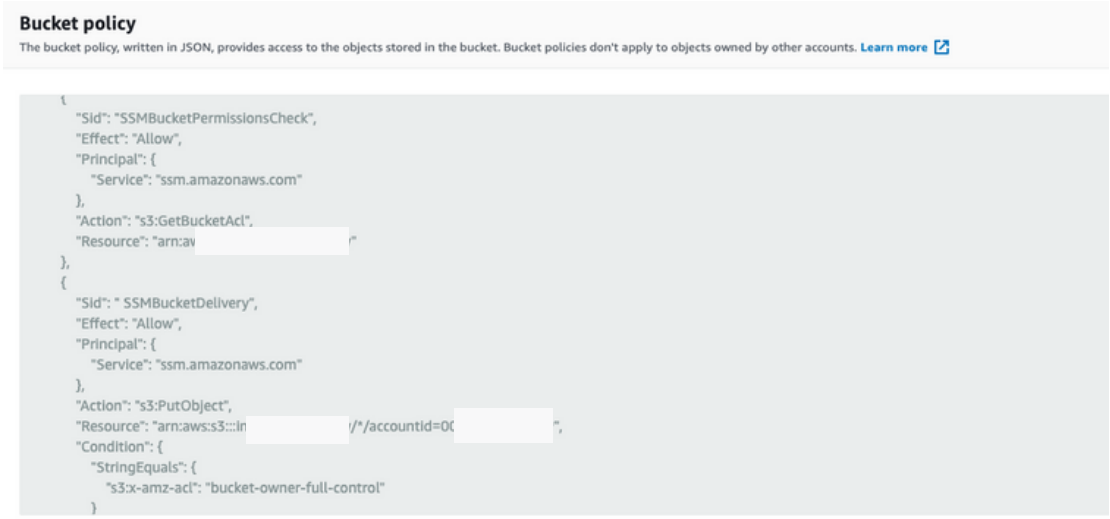


4

SETUP INVENTORY COLLECTION & DESTINATION S3 BUCKET

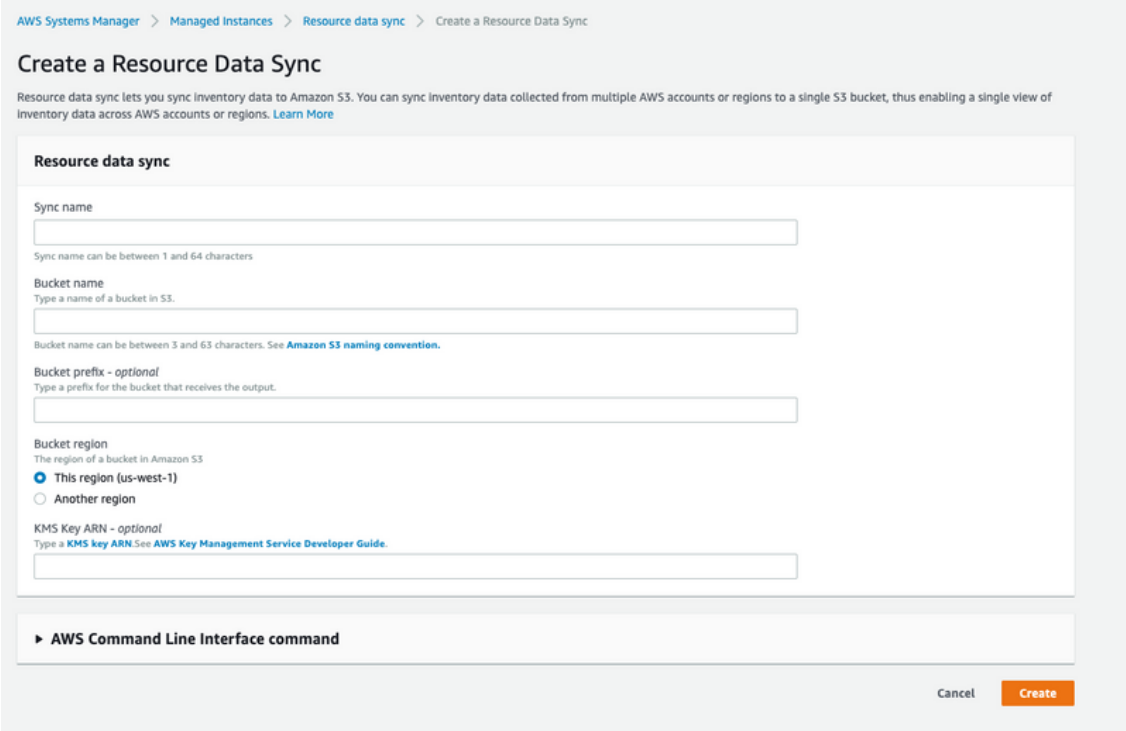
Select the type of inventory that you would like to collect and a S3 bucket that will collect that inventory with bucket policy. Bucket prefix is not required to be specified in the policy.





5 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 THREATWORX

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

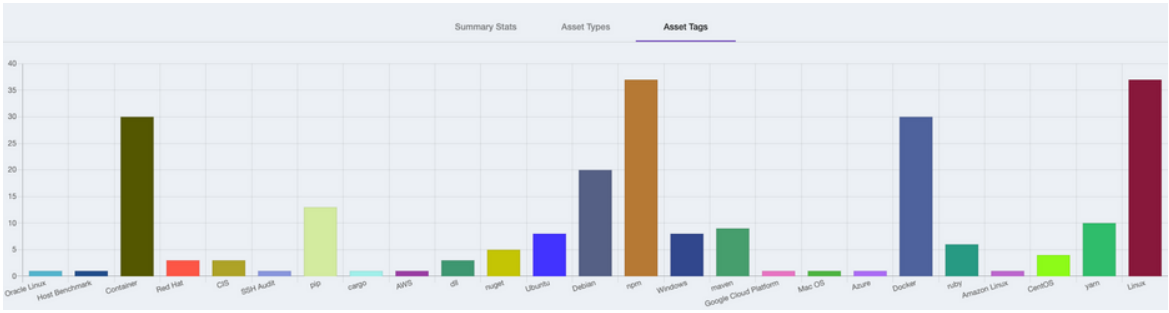
```
twigs -v aws --aws_account "[ACCOUNT_ID]" --
aws_access_key "[AWS_ACCESS_KEY]" --aws_secret_key "
[AWS_SECRET_KEY]" --aws_region "[AWS_REGION]" --
aws_s3_bucket "[S3_BUCKET]"
```

Checkout twigs guide & help videos for additional options including CIS benchmark checks for your cloud,
https://twigs.threatworx.io/guide

8

THREATWORX 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.



Date	Title	Rating	Resource	Type	Status
Mar 6, 2020	Level 1 [check11] Avoid the use of the root account (Scored)	Critical	Not Applicable	Misconfiguration	OPEN
Mar 6, 2020	Level 1 [check12] Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a console password (Scored)	Critical	Not Applicable	Misconfiguration	OPEN
Mar 6, 2020	Level 1 [check13] Ensure credentials unused for 90 days or greater are disabled (Scored)	Critical	Not Applicable	Misconfiguration	OPEN
Mar 6, 2020	Level 1 [check14] Ensure access keys are rotated every 90 days or less (Scored)	Critical	Not Applicable	Misconfiguration	OPEN
Mar 6, 2020	Level 1 [check15] Ensure IAM password policy requires at least one uppercase letter (Scored)	Critical	Not Applicable	Misconfiguration	OPEN
Mar 6, 2020	Level 1 [check16] Ensure IAM password policy require at least one lowercase letter (Scored)	Critical	Not Applicable	Misconfiguration	OPEN
Mar 6, 2020	Level 1 [check17] Ensure IAM password policy require at least one symbol (Scored)	Critical	Not Applicable	Misconfiguration	OPEN
Mar 6, 2020	Level 1 [check18] Ensure IAM password policy require at least one number (Scored)	Critical	Not Applicable	Misconfiguration	OPEN
Mar 6, 2020	Level 1 [check19] Ensure IAM password policy requires minimum length of 14 or greater (Scored)	Critical	Not Applicable	Misconfiguration	OPEN
Mar 6, 2020	Level 1 [check110] Ensure IAM password policy prevents password reuse: 24 or greater (Scored)	Critical	Not Applicable	Misconfiguration	OPEN

	Risk Score	Recorded On	CVE / Advisory	Affected Product	Rating	Priority	Status
	60	Nov 5, 2020	CVE-2019-14287	sudo 1.8.6p3-29.27.amzn1.x86_64	Critical	Now	OPEN
	55	Nov 5, 2020	T1181944	kernel 4.9.62-21.56.amzn1.x86_64	Critical	Later	OPEN
	55	Nov 5, 2020	T1181944	kernel 4.14.51-60.38.amzn1.x86_64	Critical	Later	OPEN
	55	Nov 5, 2020	T1181944	kernel-tools 4.14.51-60.38.amzn1.x86_64	Critical	Later	OPEN
	34	Nov 5, 2020	T1212637	kernel 4.9.62-21.56.amzn1.x86_64	Critical	Later	OPEN
	34	Nov 5, 2020	T1212637	kernel 4.14.51-60.38.amzn1.x86_64	Critical	Later	OPEN
	34	Nov 5, 2020	T1212637	kernel-tools 4.14.51-60.38.amzn1.x86_64	Critical	Later	OPEN