

AWS CLOUD WORKLOAD PROTECTION

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



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`).

AWS Systems Manager > State Manager

Associations View details Apply association now Edit Delete Create association

Q

Association Id	Association name	Document name	Last execution date	Status	Association version	Resource status count
<input type="radio"/>	3141aaa	Inventory-association	AWS-GatherSoftwareInventory	Fri, 05 Feb 2021 09:30:47 GMT	Success	3
<input type="radio"/>	d1c2ece	Inventory-association-linux	AWS-GatherSoftwareInventory	Sat, 06 Feb 2021 06:00:01 GMT	Success	1
<input type="radio"/>	148d1a6c0	container-association	AWS-GatherSoftwareInventory	Wed, 20 Nov 2019 23:30:00 GMT	Pending	1

AWS-GatherSoftwareInventory

Document description

Software Inventory Policy Document.

Use the service-linked role [AWSServiceRoleForAmazonSSM](#) to allow State Manager to manage AWS resources on your behalf.

Q

< 1 2 3 4 5 6 7 8 ... >

	Name	Owner	Platform types	Document type
<input type="radio"/>	AWS-EnableExplorer	Amazon	Windows, Linux	Automation
<input type="radio"/>	AWS-EnableS3BucketEncryption	Amazon	Windows, Linux	Automation
<input type="radio"/>	AWS-ExportOpsDataToS3	Amazon	Windows, Linux	Automation
<input type="radio"/>	AWS-FindWindowsUpdates	Amazon	Windows	Command
<input checked="" type="radio"/>	AWS-GatherSoftwareInventory	Amazon	Windows, Linux	Policy
<input type="radio"/>	AWS-HelloWorld	Amazon	Windows, Linux	Automation
<input type="radio"/>	AWS-InstallApplication	Amazon	Windows	Command
<input type="radio"/>	AWS-InstallMissingWindowsUpdates	Amazon	Windows	Command
<input type="radio"/>	AWS-InstallPowerShellModule	Amazon	Windows	Command

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.

Setup Inventory

Create an Inventory association to collect information 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 this 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

Applications

(Optional) Collect data for installed applications.

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:aws:s3:::in-[redacted]",
},
{
  "Sid": "SSMBucketDelivery",
  "Effect": "Allow",
  "Principal": {
    "Service": "ssm.amazonaws.com"
  },
  "Action": "s3:PutObject",
  "Resource": "arn:aws:s3:::in-[redacted]/*",
  "Condition": {
    "StringEquals": {
      "s3:x-amz-acl": "bucket-owner-full-control"
    }
  }
}
```

5

SETUP RESOURCE DATA SYNC

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

The screenshot shows the AWS Systems Manager console interface for creating a Resource Data Sync. The breadcrumb trail is: AWS Systems Manager > Managed Instances > Resource data sync > Create a Resource Data Sync. The main heading is 'Create a Resource Data Sync'. Below this is a descriptive paragraph: 'Resource data sync lets you sync inventory data to Amazon S3. You can sync inventory data collected from multiple AWS accounts or regions to a single S3 bucket, thus enabling a single view of inventory data across AWS accounts or regions. [Learn More](#)'. The form itself is titled 'Resource data sync' and contains several fields: 'Sync name' (with a note that it can be between 1 and 64 characters), 'Bucket name' (with a note that it can be between 3 and 63 characters and a link to 'Amazon S3 naming convention'), 'Bucket prefix - optional' (with a note that it's a prefix for the bucket), 'Bucket region' (with radio buttons for 'This region (us-west-1)' and 'Another region'), and 'KMS Key ARN - optional' (with a note to see the 'AWS Key Management Service Developer Guide'). At the bottom of the form is a section for the 'AWS Command Line Interface command'. On the right side of the form are 'Cancel' and 'Create' buttons.

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>

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