

Very easy to enable Sysdig security and compliance tools on AWS and Containers running on ECS, Fargate and EKS.

1/ Workshop step by step guide - <https://sysdig.awsworkshop.io/> very easy to follow

2/ Free Sysdig trial account sign up - https://sysdig.com/company/free-trial/?utm_campaign=aws-workshop (good for 1 month)

3/ Sysdig learning videos - <https://learn.sysdig.com/series/secure-101>

4/ Screen dumps of different features in the workshop as follows

4.1/ easy to add Sysdig with their CF template at <https://cf-templates-cloudvision-ci.s3-eu-west-1.amazonaws.com/latest/entry-point.yaml>

Easy onboarding: <https://us2.app.sysdig.com/secure/#/onboarding>

4.2/ default AWS best practices/policy:

Your free trial will expire in a month. [Upgrade to Enterprise](#)

Runtime Policies

Search... High Medium Low Info Capture Enabled Select policy type... [Add Policy](#)

Severity	Tag	Description	Last Updated	Rules	Action
High	aws	Sysdig AWS Best Practices Entire Infrastructure	Updated 25 minutes ago	40 rules Notify Only	Edit Delete More
High		Disallow K8s Activity Entire Infrastructure	Updated 25 minutes ago	3 rules Notify Only	Edit Delete More
Medium		Create Privileged Pod Entire Infrastructure	Updated 25 minutes ago	1 rules Notify Only	Edit Delete More
Medium		Inadvised K8s Activity Entire Infrastructure	Updated 25 minutes ago	6 rules Notify Only	Edit Delete More
High		Suspicious K8s User Activity Entire Infrastructure	Updated 25 minutes ago	2 rules Notify Only	Edit Delete More
Medium		Inadvised K8s User Activity Entire Infrastructure	Updated 25 minutes ago	6 rules Notify Only	Edit Delete More
Medium		Suspicious K8s Activity Entire Infrastructure	Updated 25 minutes ago	4 rules Notify Only	Edit Delete More
Low		All K8s Object Modifications Entire Infrastructure	Updated 25 minutes ago	10 rules Notify Only	Edit Delete More
Low		All K8s User Modifications Entire Infrastructure	Updated 25 minutes ago	6 rules Notify Only	Edit Delete More
Info		All K8s Activity Entire Infrastructure	Updated 25 minutes ago	1 rules Notify Only	Edit Delete More
Info		Access Cryptomining Network Entire Infrastructure	Updated 25 minutes ago	2 rules Notify Only	Edit Delete More
Medium		Suspicious Network Activity Entire Infrastructure	Updated 25 minutes ago	8 rules Notify Only	Edit Delete More
Medium		User Management Changes Entire Infrastructure	Updated 25 minutes ago	1 rules Notify Only	Edit Delete More
High		Disallow Container Activity Entire Infrastructure	Updated 25 minutes ago	1 rules Notify Only	Edit Delete More
High		Suspicious Container Activity Entire Infrastructure	Updated 25 minutes ago	15 rules Notify Only	Edit Delete More
Info		Dale from Sysdig	Activity	Updated 25 minutes ago	Edit Delete More
Info		Hi Walter, I'm Dale from Sysdig!	Activity	Updated 25 minutes ago	Edit Delete More
Medium		We're really excited to have you o...	Activity	Updated 25 minutes ago	Edit Delete More
Medium		Inadvised Container Activity		Updated 25 minutes ago	Edit Delete More

4.3/ many ready to use security rules in AWS policy:

Your free trial will expire in a month. [Upgrade to Enterprise](#)

Runtime Policies

aws Sysdig AWS Best Practices

Description
The Sysdig AWS Best Practices policy is a set of rules that detect when your AWS accounts and resources deviate from security best practices.

Scope
Entire Infrastructure

Rules

- rule: Deactivate Hardware
- rule: Disable Security Hub
- rule: CloudTrail Trail
- rule: Stop Configuration
- rule: Create IAM Policy
- rule: Deactivate MFA for
- rule: CloudTrail Multi-
- rule: Disable CMK Rotation
- rule: Create Access Key for
- rule: CloudWatch Delete
- rule: Security Hub Delete
- rule: Console Root Login
- rule: Create Security Group

Severity	Source	Name	Last Update	Rules
High	aws	Sysdig AWS Best Practices	Updated 26 minutes ago	40 rules Notify Only
High	aws	Disallow K8s Activity	Updated 26 minutes ago	3 rules Notify Only
Medium	aws	Create Privileged Pod	Updated 26 minutes ago	1 rules Notify Only
Medium	aws	Inadvised K8s Activity	Updated 26 minutes ago	6 rules Notify Only
High	aws	Suspicious K8s User Activity	Updated 26 minutes ago	2 rules Notify Only
Medium	aws	Inadvised K8s User Activity	Updated 26 minutes ago	6 rules Notify Only
Medium	aws	Suspicious K8s Activity	Updated 26 minutes ago	4 rules Notify Only
Low	aws	All K8s Object Modifications	Updated 26 minutes ago	10 rules Notify Only
Low	aws	All K8s User Modifications	Updated 26 minutes ago	6 rules Notify Only
Info	aws	All K8s Activity	Updated 26 minutes ago	1 rules Notify Only
Info	aws	Access Cryptomining Network	Updated 26 minutes ago	2 rules Notify Only
Medium	aws	Suspicious Network Activity	Updated 26 minutes ago	8 rules Notify Only
Medium	aws	User Management Changes	Updated 26 minutes ago	1 rules Notify Only
High	aws	Disallow Container Activity	Updated 26 minutes ago	1 rules Notify Only
Info	aws	Suspicious Container Activity	Updated 26 minutes ago	15 rules Notify Only
Medium	aws	Dale from Sysdig	Activity	2 rules Notify Only
Medium	aws	Hi Walter, I'm Dale from Sysdig!	Activity	2 rules Notify Only
Medium	aws	We're really excited to have you o...	Activity	2 rules Notify Only
Medium	aws	Inadvised Container Activity	Activity	Updated 26 minutes ago

4.4/ easy to monitor with Sysdig scanning and others running as ECS Fargate tasks:

The screenshot shows the AWS ECS Cluster details page for the cluster named "Sysdig-CloudVision-ECSFargateClusterStack-10WDEXNV5IJRC".

Cluster ARN: arn:aws:ecs:us-east-1:554051034976:cluster/Sysdig-CloudVision-ECSFargateClusterStack-10WDEXNV5IJRC

Status: ACTIVE

Registered container instances: 0

Pending tasks count: 0 Fargate, 0 EC2, 0 External

Running tasks count: 3 Fargate, 0 EC2, 0 External

Active service count: 3 Fargate, 0 EC2, 0 External

Draining service count: 0 Fargate, 0 EC2, 0 External

Services:

Service Name	Status	Service type	Task Definition	Desired tasks	Running tasks	Launch type	Platform version
Sysdig-CloudVision-CloudScanningStack-1AJ...	ACTIVE	REPLICAS	Sysdig-Clou...	1	1	FARGATE	LATEST(1.4)
Sysdig-CloudVision-CloudBenchStack-1VKEC...	ACTIVE	REPLICAS	Sysdig-Clou...	1	1	FARGATE	LATEST(1.4)
Sysdig-CloudVision-CloudConnectorStack-BY...	ACTIVE	REPLICAS	Sysdig-Clou...	1	1	FARGATE	LATEST(1.4)

4.5/ Sysdig Secure Compliance report for HIPAA:

Your free trial will expire in a month. [Upgrade to Enterprise](#)

REGULATORY COMPLIANCE Reports

Compliance HIPAA All Clusters... Download

Common Fixes

- Enable Kubernetes Auditing Affects 22 control(s)
- Enable a Policy with Falco Rules Affects 17 control(s)
- Assign Image Scanning Policy Affects 5 control(s)
- Enable a Policy with Falco Rules and Captures Affects 4 control(s)
- Enable Admission Controller feature Affects 2 control(s)
- Schedule CIS Benchmark Affects 2 control(s)

0% * 0 Passed 22 Failed Total Control: 22

Administrative safeguards 0 of 10 Controls Passed

164.308(a)(1)(ii)(D) Procedures to review system activity 14 of 22 Checks Passed

What is this check?: Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

How is this check addressed?: Using Sysdig Secure platform on-prem or SaaS, you control hosts, containers and Kubernetes security, detecting static and runtime security issues, getting capture data for audit, and preventing and blocking insecure situations. Enabling Kubernetes audit log lets Falco rules monitor a cluster for security issues on Kubernetes events. Falco runtime rules detect security relevant events on kernel syscalls and Kubernetes audit log in real time.

Remediation Procedure

- Enable "Notable Filesystem Changes" Policy with Falco rule "Write below etc" [Enable a Policy with Falco Rules](#)
- Enable "Notable Filesystem Changes" Policy with Falco rule "Write below root" [Enable a Policy with Falco Rules](#)
- Enable Kubernetes auditing by following the instructions in the Sysdig docs [Enable Kubernetes Auditing](#)
- Install the Sysdig Agent using the instructions in the Onboarding page [Install the Agent](#)

Date from Sysdig
Hi Walter, I'm Dale from Sysdig!

4.6/ Sysdig Secure sample rules, e.g. ALL k8s Audit events:

The screenshot shows the Sysdig Secure Policies Library interface. A red arrow points to the 'POLICIES' tab in the top navigation bar. Another red arrow points to the 'All K8s Audit Events' row in the main table. A third red arrow points to the detailed description of the rule on the right.

Your free trial will expire in a month. [Upgrade to Enterprise](#)

POLICIES Rules Library

Your agent version is unknown.

Custom rules with exception objects are not supported for Sysdig-Agent older than Version 11.2.0. If there are any exception objects in a custom rules file, the older agents will not get any of the custom rules. Please upgrade all agents to version 11.2.0 or newer.

Check Agent Versions in this Environment
Upgrade Agents to Latest Version

Rules	Published By	Last Upd
Accept VPC Peering Connection	Sysdig 0.20.0	6 days ago
Add AWS User to Group	Sysdig 0.20.0	6 days ago
All K8s Audit Events	Sysdig 0.20.0	6 days ago
Allocate New Elastic IP Address to AWS Account	Sysdig 0.20.0	6 days ago
Anonymous Request Allowed	Sysdig 0.20.0	6 days ago
Associate Elastic IP Address to AWS Network Interface	Sysdig 0.20.0	6 days ago
Associate VPC with Hosted Zone	Sysdig 0.20.0	6 days ago
Attach Administrator Policy	Sysdig 0.20.0	6 days ago
Attach IAM Policy to User	Sysdig 0.20.0	6 days ago
Attach Internet Gateway	Sysdig 0.20.0	6 days ago
Attach to cluster-admin Role	Sysdig 0.20.0	6 days ago
Attach/Exec Pod	Sysdig 0.20.0	6 days ago
Authorize DB Security Group Ingress	Sysdig 0.20.0	6 days ago
Authorize Security Group Egress	Sysdig 0.20.0	6 days ago
Authorize Security Group Ingress	Sysdig 0.20.0	6 days ago
AWS Command Executed on Unused Region	Sysdig 0.20.0	6 days ago
Batch Disable Standards	Sysdig 0.20.0	6 days ago
Change Resource Record Sets	Sysdig 0.20.0	6 days ago
Change thread namespace	Sysdig 0.20.0	6 days ago
Clear L Dale from Sysdig	Sysdig 0.20.0	6 days ago
Clouds Hi Walter, I'm Dale from Sysdig!	Sysdig 0.20.0	6 days ago

All K8s Audit Events

Kubernetes Audit

- rule: All K8s Audit Events

condition: kall

output: K8s Audit Event received (user=%ka.user.name verb=%ka.verb uri=%ka.uri obj=%jevt.obj)

source: k8s_audit

description: Match all K8s Audit Events

tags: k8s

k8s

Usage

DISABLED - This rule is used by 1 disabled policy:

Status	Policy Name
Disabled	All K8s Activity

4.7/ Sysdig Secure sample rules, e.g. k8s audit attach/exec pods:

Your free trial will expire in a month. [Upgrade to Enterprise](#)

POLICIES

Rules Library

SECURE
Review
Planning
Compliance
Policies
Network
Events
Investigate
Started
WL

Search: Select usage Select Tags

Your agent version is unknown.

Custom rules with exception objects are not supported for Sysdig-Agent older than Version 11.2.0. If there are any exception objects in a custom rules file, the older agents will not get any of the custom rules. Please upgrade all agents to version 11.2.0 or newer.

Check Agent Versions in this Environment
Upgrade Agents to Latest Version

Rules	Published By	Last Upd
Accept VPC Peering Connection	Sysdig 0.20.0	6 days ago
Add AWS User to Group	Sysdig 0.20.0	6 days ago
All K8s Audit Events	Sysdig 0.20.0	6 days ago
Allocate New Elastic IP Address to AWS Account	Sysdig 0.20.0	6 days ago
Anonymous Request Allowed	Sysdig 0.20.0	6 days ago
Associate Elastic IP Address to AWS Network Interface	Sysdig 0.20.0	6 days ago
Associate VPC with Hosted Zone	Sysdig 0.20.0	6 days ago
Attach Administrator Policy	Sysdig 0.20.0	6 days ago
Attach IAM Policy to User	Sysdig 0.20.0	6 days ago
Attach Internet Gateway	Sysdig 0.20.0	6 days ago
Attach to cluster-admin Role	Sysdig 0.20.0	6 days ago
Attach/Exec Pod	Sysdig 0.20.0	6 days ago
Authorize DB Security Group Ingress	Sysdig 0.20.0	6 days ago
Authorize Security Group Egress	Sysdig 0.20.0	6 days ago
Authorize Security Group Ingress	Sysdig 0.20.0	6 days ago
AWS Command Executed on Unused Region	Sysdig 0.20.0	6 days ago
Batch Disable Standards	Sysdig 0.20.0	6 days ago
Change Resource Record Sets	Sysdig 0.20.0	6 days ago
Change thread namespace	Sysdig 0.20.0	6 days ago
Clear Local Cache	Dale from Sysdig	6 days ago
CloudWatch Metrics	Hi Walter, I'm Dale from Sysdig!	6 days ago

Attach/Exec Pod

Kubernetes Audit

Updated 6 days ago

- rule: Attach/Exec PodSysdig 0.20.0

condition: kevt_started a pod_subresource and kcreate and ka.target.subresource in (exec,attach) and not user_known_exec_pod_active

output: Attach/Exec to pod (user=%ka.user.name pod=%ka.target.name ns=%ka.target.namespace action=%ka.target.subresource command=%ka.uri.param[command])

source: k8s_audit

description: Detect any attempt to attach/exec to pod

tags: NIST_800-53_AU-2, SOC2_CC6.1, NIST_800-53_AC-2(4), k8s, NIST_800-53, NIST_800-53_AC-17b, NIST_800-53_AC-2g

exceptions (2) ▾

NIST_800-53

NIST_800-53_AC-17b

4.8/ sample Events when I create CMK with rotation disabled:

Your free trial will expire in a month. [Upgrade to Enterprise](#)

Events

Everywhere

Search by event title and label

High Med Low Info All Types

Filters...

Load Older...

aws Create Customer Master Key - Sysdig AWS Best Practices

Triggered on Wed Jun 09 2021 at 10:55:21 AM | a minute ago

aws Create Customer Master Key - Sysdig AWS Best Practices

High Severity Event ID: 1686fb9238c82951821f7

Policy & Triggered Rules

Edit Policy

name Create Customer Master Key - Sysdig AWS Best Practices

ruleType AWS CloudTrail

ruleName Create Customer Master Key

A new CMK user has been created with rotation disabled (requesting user=TeamRole, requesting IP=cloudformation.amazonaws.com, AWS Region=us-east-1, new key created=f23d6491-3-41db-be00-5f8bf924ee02)

cloud

aws

aws_kms

pci_dss_3.6.4

pci_dss_kms.1

Scope

aws.accountId 554051034976

aws.eventId 7a0cb7af-5923-4f46-be59-8ea737b14bc6

aws.kms.keyId f23d6491-7f63-41db-be00-5f8bf924ee02

aws.region us-east-1

aws.requestId 6c1b46fc-0fad-4f67-92f6-7112eb35def6

aws.sourceIP cloudformation.amazonaws.com

aws.user TeamRole

resourceCategory Security

resourceType AWS Key Management Service

Date from Sysdig
Hi Walter, I'm Dale from Sysdig!

Started WL

4.9/ Sysdig Monitor – get started with k8s easily:

Your free trial will expire in a month. [Buy Enterprise](#)

Get Started

Get started with Sysdig Monitor to maximize the performance and availability of your cloud infrastructure, services, and applications.

Connect your data sources

Install the Agent

10m ▾

Kubernetes Helm Docker Linux

Installing the agent on your infrastructure allows Sysdig to collect data for monitoring and security purposes. Copy and paste the command below to set up your agent.

Cluster Name:

AWS, AZURE, GKE

```
curl -s https://download.sysdig.com/stable/install-agent-kubernetes | sudo bash -s -- --access_key d4262f03-8c12-4f8a-b4f4-200cce16d467 --collector ingest-us2.app.sysdig.com --collector_port 6443 -- analysismanager https://us2.app.sysdig.com/internal/scanning/scanning-analysis-collector --imageanalyzer
```

OpenShift

```
curl -s https://download.sysdig.com/stable/install-agent-kubernetes | sudo bash -s -- --access_key d4262f03-8c12-4f8a-b4f4-200cce16d467 --collector ingest-us2.app.sysdig.com --collector_port 6443 -- analysismanager https://us2.app.sysdig.com/internal/scanning/scanning-analysis-collector --imageanalyzer --openshift
```

Monitor your infrastructure

Create a dashboard

10m ▾

Configure a notification channel

2m ▾

Dale from Sysdig

Hi Walter, I'm Dale from Sysdig!

5m ▾

Resources

[Documentation](#) [Sysdig Monitor Release Note](#) [Blog](#)

[Self Paced Training](#) [Support](#) [Application Status](#)

Started

WL

?

4.10/ Sample Cloud Activity/Event:

Your free trial will expire in a month. [Upgrade to Enterprise](#)

Cloud Activity **BETA**
Account > Region > Resource Category > Resource Type > Resource

Search for Name, Label, Ruletag or Severity... Tab, Space or Enter ...

All Activity

Summary Events

1 Create Customer Master Key

aws 554051034976 us-east-1 Security AWS Key Management Service

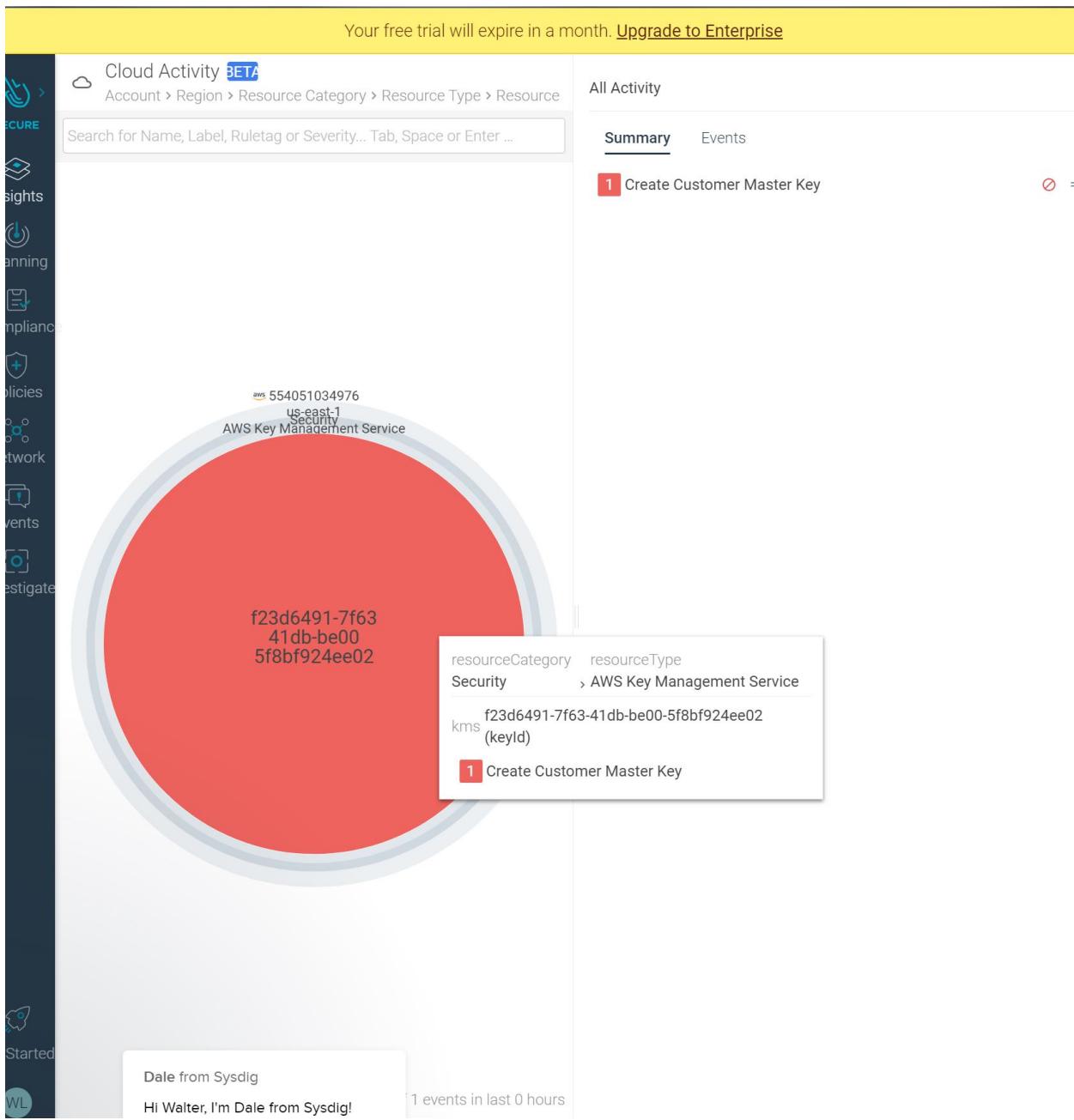
f23d6491-7f63-41db-be00-5f8bf924ee02

resourceCategory resourceType
Security > AWS Key Management Service
kms f23d6491-7f63-41db-be00-5f8bf924ee02
(keyId)

1 Create Customer Master Key

Date from Sysdig
Hi Walter, I'm Dale from Sysdig!

1 events in last 0 hours



4.11/ Sample Codebuild failure when we got vulnerability in our docker build packages:

The screenshot shows the AWS CodeBuild console for a project named "Sysdig-CloudVision-ScanningCodeBuildStack-XGWZ7T7SV62L-BuildProject". The "Build project" section is selected in the sidebar. The main area displays the "Configuration" tab with settings for source provider (No source), primary repository (-), artifacts upload location (-), and build badge (Disabled). Below this is the "Build history" tab, which lists five build runs. The first three builds are marked as "Failed" (indicated by a red circle with a question mark icon) and have red arrows pointing to their status column. The fourth build is marked as "Succeeded" (green circle with a checkmark icon). The fifth build is also marked as "Failed". Each build row includes a checkbox, a link to the build run, its status, build number, source version, and submitter.

Build run	Status	Build number	Source version	Submitter
Sysdig-CloudVision-ScanningCodeBuildStack-XGWZ7T7SV62L-BuildProject:a67380e-2beb-4822-a8c1-a2dead3dc9b8	Failed	5	-	Sysdig-CloudVision-CloudScanningStack-1AJ-TaskRoleQM2TB0XURHAG/07869f5b3be94c3baa982beac48b45
Sysdig-CloudVision-ScanningCodeBuildStack-XGWZ7T7SV62L-BuildProject:1f793aff-c26c-4cfb-b5b3-2714705256bb	Failed	4	-	Sysdig-CloudVision-CloudScanningStack-1AJ-TaskRoleQM2TB0XURHAG/07869f5b3be94c3baa982beac48b45
Sysdig-CloudVision-ScanningCodeBuildStack-XGWZ7T7SV62L-BuildProject:fbbbf367-661f-4755-ba1d-b6fc6eaadb7	Failed	1	-	Sysdig-CloudVision-CloudScanningStack-1AJ-TaskRoleQM2TB0XURHAG/07869f5b3be94c3baa982beac48b45
Sysdig-CloudVision-ScanningCodeBuildStack-XGWZ7T7SV62L-BuildProject:fd5d9c95-de4a-4cf5-9d34-2cee9742d2a5	Succeeded	2	-	Sysdig-CloudVision-CloudScanningStack-1AJ-TaskRoleQM2TB0XURHAG/07869f5b3be94c3baa982beac48b45
Sysdig-CloudVision-ScanningCodeBuildStack-XGWZ7T7SV62L-BuildProject:74a9291e-9e7c-493f-ab7d-e822e6c3fa8f	Failed	3	-	Sysdig-CloudVision-CloudScanningStack-1AJ-TaskRoleQM2TB0XURHAG/07869f5b3be94c3baa982beac48b45

4.12/ ECR Vulnerabilities:

Screenshot of the AWS Amazon Container Services - ECR Vulnerabilities page. The sidebar shows navigation for ECS, EKS, and ECR. The main content displays an overview of vulnerabilities and a detailed list of findings.

Overview:

Critical	High	Medium	Low	Informational	Undefined
3	46	174	154	366	28

Vulnerabilities (771):

Name	Package	Severity	Description
CVE-2019-19814	linux:4.9.246-2	CRITICAL	In the Linux kernel 5.0.21, mounting a crafted f2fs filesystem image can cause __remove_dirty_segment slab-out-of-bounds write access because an array is bounded by the number of dirty types (8) but the array index can exceed this.
CVE-2019-19816	linux:4.9.246-2	CRITICAL	In the Linux kernel 5.0.21, mounting a crafted btrfs filesystem image and performing some operations can cause slab-out-of-bounds write access in __bttrfs_map_block in fs/btrfs/volumes.c, because a value of 1 for the number of data stripes is mishandled.
CVE-2021-27928	mariadb-10.1:10.1.48-0+deb9u1	CRITICAL	A remote code execution issue was discovered in MariaDB 10.2 before 10.2.37, 10.3 before 10.3.28, 10.4 before 10.4.18, and 10.5 before 10.5.9; Percona Server through 2021-03-03; and the wsrep patch through 2021-03-03 for MySQL. An untrusted search path leads to eval injection, in which a database SUPER user can execute OS commands after modifying wsrep_provider and wsrep_notify_cmd. NOTE: this does not affect an Oracle product.
CVE-2019-12900	bzip2:1.0.6-8.1	HIGH	BZ2_decompress in decompress.c in bzip2 through 1.0.6 has an out-of-bounds write when there are many selectors.
CVE-2018-6485	glibc:2.24-11+deb9u4	HIGH	An integer overflow in the implementation of the posix_memalign in memalign functions in the GNU C Library (aka glibc or libc6) 2.26 and earlier could cause these functions to return a pointer to a heap area that is too small, potentially leading to heap corruption.
CVE-2018-6551	glibc:2.24-11+deb9u4	HIGH	The malloc implementation in the GNU C Library (aka glibc or libc6), from version 2.24 to 2.26 on powerpc, and only in version 2.26 on i386, did not properly handle malloc calls with arguments close to SIZE_MAX and could return a pointer to a heap region that is smaller than requested, eventually leading to heap corruption.
CVE-2018-100001	glibc:2.24-11+deb9u4	HIGH	In glibc 2.26 and earlier there is confusion in the usage of getcwd() by realpath() which can be used to write before the destination buffer leading to a buffer underflow and potential code execution.
CVE-2019-9169	glibc:2.24-11+deb9u4	HIGH	In the GNU C Library (aka glibc or libc6) through 2.29, proceed_next_node in posix/regexec.c has a heap-based buffer over-read via an attempted case-insensitive regular-expression match.
CVE-2021-33574	glibc:2.24-11+deb9u4	HIGH	The mq_notify function in the GNU C Library (aka glibc) versions 2.32 and 2.33 has a use-after-free. It may use the notification thread attributes object (passed through its struct sigevent parameter) after it has been freed by the caller, leading to a denial of service (application crash) or possibly unspecified other impact.
CVE-2019-25013	glibc:2.24-11+deb9u4	HIGH	The iconv feature in the GNU C Library (aka glibc or libc6) through 2.32, when processing invalid multi-byte input sequences in the EUC-KR encoding, may have a buffer over-read.
CVE-2021-20244	imagemagick:8.6.9.4+dfsg-1	HIGH	A flaw was found in ImageMagick in MagickCore/visual-effects.c. An attacker who submits a crafted file that is processed by ImageMagick

4.13/ show Vulnerabilities ID and fix (non-OS)

Your free trial will expire in a month. [Upgrade to Enterprise](#)

IMAGE SCANNING
Scan Results > 554051034976.dkr.ecr.us-east-1.amazonaws.com/aws-work... latest Add to List

OS debian 9 Layers 13 Size 957.02 MB Added by AWS Registry on AM Image ID ca1ae266... [i](#)

INSIGHTS [Download CSV](#)

SCANNING

COMPLIANCE

POLICIES

NETWORK

EVENTS

INVESTIGATE

Get Started

Dale from Sysdig
Hi Walter, I'm Dale from Sysdig!
We're really excited to have you o...

Summary Non-operating System

Scan Policy DefaultPolicy

Vulnerabilities Operating System Non-operating System [Select...](#)

Showing 12 of 12 vulnerabilities

Vuln ID	Severity ↓	Package Name and Version	Fix	Type
CVE-2017-17458	Critical	mercurial-4.0	~	python
CVE-2018-13347	Critical	mercurial-4.0	~	python
CVE-2017-1000116	Critical	mercurial-4.0	~	python
CVE-2017-18589	High	cookie-0.4.0	~	npm
CVE-2018-13346	High	mercurial-4.0	~	python
CVE-2017-9462	High	mercurial-4.0	~	python
CVE-2017-1000115	High	mercurial-4.0	~	python
CVE-2018-13348	High	mercurial-4.0	~	python
VULNDB-255658	Medium	path-parse-1.0.6	~	npm
VULNDB-255659	Medium	path-parse-1.0.6	~	npm
VULNDB-176819	Medium	mercurial-4.0	4.5.2	python
CVE-2019-3902	Medium	mercurial-4.0	~	python

4.14/ show Vulnerabilities ID and fix (OS):

The screenshot shows the Sysdig Secure interface for a scanned Docker image. The top bar displays a trial expiration notice: "Your free trial will expire in a month. Upgrade to Enterprise". The main header includes "IMAGE SCANNING", "Scan Results > 554051034976.dkr.ecr.us-east-1.amazonaws.com/aws-work...", "latest", and "Add to List". On the left sidebar, under the "SECURE" section, the "Scanning" icon is highlighted. The main content area shows the "Operating System" tab selected, displaying 20 of 4905 vulnerabilities. A red arrow points to the "Operating System" link in the sidebar. Another red arrow points to the "Showing 20 of 4905 vulnerabilities" message. The table lists vulnerabilities with columns: Vuln ID, Severity, Package Name and Version, Fix, and Type. Most vulnerabilities are of severity "High" and type "dpkg". The table includes entries for libc6, libmariadbclient-dev-compat, imagemagick, libmagickcore, libbz2-dev, libwebp-dev, libc-dev-bin, libc6-dev, libwebpdemux2, and linux-libc-dev.

Vuln ID	Severity	Package Name and Version	Fix	Type
CVE-2018-6551	High	libc6-2.24-11+deb9u4	~	dpkg
CVE-2018-100001	High	libc-bin-2.24-11+deb9u4	~	dpkg
CVE-2019-0145	High	linux-libc-dev-4.9.246-2	~	dpkg
CVE-2021-20309	High	imagemagick-8:6.9.7.4+dfsg-11+deb9i	8:6.9.7.4+dfsg-11+deb9u13	dpkg
CVE-2021-27928	High	libmariadbclient-dev-compat-10.1.48-c	10.1.48-0+deb9u2	dpkg
CVE-2021-20312	High	imagemagick-6.q16-8:6.9.7.4+dfsg-11-	8:6.9.7.4+dfsg-11+deb9u13	dpkg
CVE-2019-25013	High	libc-bin-2.24-11+deb9u4	~	dpkg
CVE-2021-20312	High	libmagickcore-6.q16-3-extra-8:6.9.7.4+	8:6.9.7.4+dfsg-11+deb9u13	dpkg
CVE-2021-20246	High	imagemagick-8:6.9.7.4+dfsg-11+deb9i	8:6.9.7.4+dfsg-11+deb9u12	dpkg
CVE-2021-3177	High	libpython2.7-stdlib-2.7.13-2+deb9u4	~	dpkg
CVE-2019-12900	High	libbz2-dev-1.0.6-8.1	~	dpkg
CVE-2018-25014	High	libwebp-dev-0.5.2-1	0.5.2-1+deb9u1	dpkg
CVE-2019-9169	High	libc-dev-bin-2.24-11+deb9u4	~	dpkg
CVE-2018-100001	High	libc6-dev-2.24-11+deb9u4	~	dpkg
CVE-2020-36328	High	libwebpdemux2-0.5.2-1	0.5.2-1+deb9u1	dpkg
CVE-2021-1942	High	linux-libc-dev-4.9.246-2	~	dpkg
CVE-2021-1943	High	libbz2-1.0-1.0.6-8.1	~	dpkg

Dale from Sysdig
Hi Walter, I'm Dale from Sysdig!
We're really excited to have you o...

4.15/ Image scanning results:

Your free trial will expire in a month. [Upgrade to Enterprise](#)

IMAGE SCANNING
Scan Results > 554051034976.dkr.ecr.us-east-1.amazonaws.com/aws-work... latest [Add to List](#)

OS debian 9 Layers 13 Size 957.02 MB Added by AWS Registry on 9th June, 2021 [View Log](#) Image ID ca1ae266... [Details](#)

INSIGHTS [Download PDF](#)

Scanning [Re-evaluate policies](#)

Vulnerabilities Updated at 9th June, 2021 11:08 AM

Total	OS	Non-OS
0	0	0

Policies Evaluated at 9th June, 2021 11:09 AM

FAILED	STOPS	WARNS
98	31	

Breakdown

	STOPS	WARNS
DefaultPolicy	98	31
files : uid_or_guid_set	0	29
vulnerabilities : package	98	0
dockerfile : instruction	0	2

Dale from Sysdig
Hi Walter, I'm Dale from Sysdig!
We're really excited to have you o...

4.16/ Default Scan Policy Rule:

Your free trial will expire in a month. [Upgrade to Enterprise](#)

IMAGE SCANNING
Scan Results > 554051034976.dkr.ecr.us-east-1.amazonaws.com/aws-work... latest Add to List

OS debian 9 Layers 13 Size 957.02 MB Added by AWS Registry or Image ID ca1ae266...

Summary DefaultPolicy [Re-evaluate policies](#)

Scan Policy DefaultPolicy

Vulnerabilities Operating System Non-operating System

Content Gem Npm Python Files Java Operating System

Rule dockerfile : instruction : instruction=HEALTHCHECK, check=not_exists
Triggers if any directives in the list are found to match the described condition in the dockerfile.

WARN Dockerfile directive 'HEALTHCHECK' not found, matching condition 'not_exists' check

WARN Dockerfile directive 'USER' not found, matching condition 'not_exists' check

Rule vulnerabilities : package : package_type=all, severity_comparison=>=, severity=high, fix_available...
Triggers if a found vulnerability in an image meets the comparison criteria.

Severity	CVE ID	Description	Patches
STOP	CVE-2021-20244	HIGH Vulnerability found in os package type (dpkg)	8:6.9.7.4+dfsg-11+deb9u12
STOP	CVE-2021-20245	HIGH Vulnerability found in os package type (dpkg)	8:6.9.7.4+dfsg-11+deb9u13
STOP	CVE-2021-20246	HIGH Vulnerability found in os package type (dpkg)	8:6.9.7.4+dfsg-11+deb9u12
STOP	CVE-2021-20309	HIGH Vulnerability found in os package type (dpkg)	8:6.9.7.4+dfsg-11+deb9u13
STOP	CVE-2021-20312	HIGH Vulnerability found in os package type (dpkg)	8:6.9.7.4+dfsg-11+deb9u13
STOP	CVE-2021-20244	HIGH Vulnerability found in os package type (dpkg)	8:6.9.7.4+dfsg-11+deb9u12
STOP	CVE-2021-20245	HIGH Vulnerability found in os package type (dpkg)	8:6.9.7.4+dfsg-11+deb9u13
STOP	CVE-2021-20246	HIGH Vulnerability found in os package type (dpkg)	8:6.9.7.4+dfsg-11+deb9u12
STOP	CVE-2021-20309	HIGH Vulnerability found in os package type (dpkg)	8:6.9.7.4+dfsg-11+deb9u13
STOP	CVE-2021-20312	HIGH Vulnerability found in os package type (dpkg)	8:6.9.7.4+dfsg-11+deb9u13
STOP	CVE-2021-20244	HIGH Vulnerability found in os package type (dpkg)	8:6.9.7.4+dfsg-11+deb9u12
STOP	CVE-2021-20245	HIGH Vulnerability found in os package type (dpkg)	8:6.9.7.4+dfsg-11+deb9u13
STOP	CVE-2021-20246	HIGH Vulnerability found in os package type (dpkg)	8:6.9.7.4+dfsg-11+deb9u12
STOP	CVE-2021-20309	HIGH Vulnerability found in os package type (dpkg)	8:6.9.7.4+dfsg-11+deb9u13
STOP	CVE-2021-20312	HIGH Vulnerability found in os package type (dpkg)	8:6.9.7.4+dfsg-11+deb9u13
STOP	CVE-2021-20244	HIGH Vulnerability found in os package type (dpkg)	8:6.9.7.4+dfsg-11+deb9u12
STOP	CVE-2021-20245	HIGH Vulnerability found in os package type (dpkg)	8:6.9.7.4+dfsg-11+deb9u13
STOP	CVE-2021-20246	HIGH Vulnerability found in os package type (dpkg)	8:6.9.7.4+dfsg-11+deb9u12
STOP	CVE-2021-20309	HIGH Vulnerability found in os package type (dpkg)	8:6.9.7.4+dfsg-11+deb9u13
STOP	CVE-2021-20312	HIGH Vulnerability found in os package type (dpkg)	8:6.9.7.4+dfsg-11+deb9u13

Dale from Sysdig
Hi Walter, I'm Dale from Sysdig!
We're really excited to have you o... [CVE-2021-20309](#)

4.17/ Image scanning result for sample aws-workshop image:

Your free trial will expire in a month. [Upgrade to Enterprise](#)

IMAGE SCANNING Scan Results

Scan Image

Search... Registries Passed Failed Origins :

Showing 2 of 2 images

2 Images Scanned 2 Origins

1 Passed 1 Not Evaluated 1 AWS Fargate 1 AWS Registry

Image	Image ID	Status	Origin
554051034976.dkr.ecr.us-east-1.amazonaws.com / aws-workshop 🚧 latest	ca1ae266...	Not Evaluate	AWS Registry
docker.io / sysdiglabs/cloud-connector-s3-bucket-config 🟢 latest	ddc6574...	Passed	AWS Fargate

Dale from Sysdig
Hi Walter, I'm Dale from Sysdig!
We're really excited to have you o...

SECURE Insights Scanning Compliance Policies Network Events Investigate Get Started WL

4.18/ Image scanning content:

The screenshot shows the Sysdig Secure interface for image scanning. At the top, a yellow bar displays a trial expiration notice: "Your free trial will expire in a month. [Upgrade to Enterprise](#)". Below this, the main header includes "IMAGE SCANNING", "Scan Results > 554051034976.dkr.ecr.us-east-1.amazonaws.com/aws-work...", "latest", and "Add to List". The left sidebar lists various security categories: SECURE, Insights, Scanning, Compliance, Policies, Network, Events, Investigate, and Get Started. The "Content" section under "Vulnerabilities" is currently selected, with "Python" highlighted. The main content area shows a table of vulnerabilities found in the image. The table has columns for License, Location, Origin, and Package. The data is as follows:

License	Location	Origin	Package
PSF or ZPL	/usr/lib/python2.7	Phillip J. Eby <web-sig@python.org> wsgiref	
MIT	/usr/lib/python2.7/dist-packages	Benjamin Peterson <benjamin@pytl six	
GNU GPLv2 or an	/usr/lib/python2.7/dist-packages	Matt Mackall and many others <me mercurial	
UNKNOWN	/usr/lib/python2.7/dist-packages	Rob Dennis, Eli Courtwright (Michae configobj	
GNU GPL v2	/usr/lib/python2.7/dist-packages	Canonical Ltd <bazaar@lists.canoni bsr	
Python Software	/usr/lib/python2.7	Steven Bethard <steven.bethard@gr argparse	

A tooltip at the bottom left reads: "Dale from Sysdig. Hi Walter, I'm Dale from Sysdig! We're really excited to have you o...".

4.19/ Image scanning Vul. details:

Your free trial will expire in a month. [Upgrade to Enterprise](#)

IMAGE SCANNING
Scan Results > 554051034976.dkr.ecr.us-east-1.amazonaws.com

OS debian 9 **Layers** 13 **Size** 957.02 MB **Added by**

Vulnerabilities

Operating System

Showing 20 of 4905 vulnerabilities

Vuln ID	Severity ↓	Package Name a
CVE-2021-20309	High	libmagickcore-6-h
CVE-2020-29569	High	linux-libc-dev-4.9.2
CVE-2021-20245	High	libmagickcore-6-h
CVE-2018-25011	High	libwebpdemux2-0.
CVE-2021-20245	High	libmagickcore-6.q
CVE-2021-3493	High	linux-libc-dev-4.9.2
CVE-2021-20309	High	libmagickcore-6-a
CVE-2021-27928	High	libmariadbclient-d
CVE-2020-29363	High	libp11-kit0-0.23.3-
CVE-2018-25014	High	libwebpmux2-0.5.3
CVE-2021-20246	High	libmagickcore-6.q
CVE-2018-6485	High	libc-bin-2.24-11+d
CVE-2018-12930	High	linux-libc-dev-4.9.2
CVE-2021-28660	High	linux-libc-dev-4.9.2
CVE-2021-33574	High	libc6-2.24-11+deb
CVE-2021-19	High	imagemagick-6-cc
CVE-2021-21	High	linux-libc-dev-4.9.2

Description

A flaw was found in ImageMagick in versions before 7.0.11 and before 6.9.12, where a division by zero in WavImage() of MagickCore/visual-effects.c may trigger undefined behavior via a crafted image file submitted to an application using ImageMagick. The highest threat from this vulnerability is to system availability.

Package Name and Version

libmagickcore-6-headers8:6.9.7.4+dfsg-11+deb9u11

Dale from Sysdig
Hi Walter, I'm Dale from Sysdig!
We're really excited to have you o...

Severity **High** from Debian Security Tracker

Type **OS** **dpkg**

Fixed in version 8:6.9.7.4+dfsg-11+deb9u13

Add exception X

4.20/ easy to add custom image scanning rules/policies:

Your free trial will expire in a month. [Upgrade to Enterprise](#)

IMAGE SCANNING Policies > New Policy

Name: Default Configuration Policy - Dockerfile Best Practices (copy2)

Description: Description of policy

Rules:

Category	Type	Condition	Action	Severity	Remove
Vulnerabilities	Stale feed data	Max days since sync: 7	Warn	X	
Dockerfile	Instruction	Instruction: RUN; Check: like; Value: .*apt-get upgrade.*	Warn	X	
Dockerfile	Instruction	Instruction: RUN; Check: like; Value: .*yum upgrade.*	Warn	X	
Dockerfile	Effective user	Instruction: HEALTHCHECK; Check: not_exists	Warn	X	
Dockerfile	Exposed ports	Type: blacklist; Users: root	Warn	X	
Dockerfile	Instruction	Type: blacklist; Ports: 22	Warn	X	
Dockerfile	Instruction	Instruction: LABEL; Check: =; Value: latest	Warn	X	
Dockerfile	Instruction	Instruction: ENV; Check: like; Value: .*(password PASSW...)	Warn	X	
Dockerfile	Instruction	Instruction: USER; Check: not_exists	Warn	X	
Dockerfile	Instruction	Instruction: ADD; Check: exists	Warn	X	

Select gate... ▾

Dale from Sysdig
Hi Walter, I'm Dale from Sysdig!
We're really excited to have you o...

Cancel Save

4.21/ sample docker image scanning rules:

Your free trial will expire in a month. [Upgrade to Enterprise](#)

IMAGE SCANNING Policies > Edit Policy 

 Insights Scanning Compliance Policies Network Events Investigate Get Started 

 Default policies are read-only. Duplicate this policy to make changes.

Name: Default Configuration Policy - Dockerfile Best Practices

Description: This policy provides out of the box rules around Dockerfile best practices. We frequently update these policies and if you'd like to modify the policy you should use this as a base template to avoid modifications being overwritten.

Rules:

Vulnerabilities	Stale feed data	Max days since sync: 7	Warn	X
Dockerfile	Instruction	Instruction: RUN; Check: like; Value: .*apt-get upgrade.*	Warn	X
Dockerfile	Instruction	Instruction: RUN; Check: like; Value: .*yum upgrade.*	Warn	X
Dockerfile	Instruction	Instruction: HEALTHCHECK; Check: not_exists	Warn	X
Dockerfile	Effective user	Type: blacklist; Users: root	Warn	X
Dockerfile	Exposed ports	Type: blacklist; Ports: 22	Warn	X
Dockerfile	Instruction	Instruction: LABEL; Check: =; Value: latest	Warn	X
Dockerfile	Instruction	Instruction: ENV; Check: like; Value: .*(password PASSW...)	Warn	X
Dockerfile	Instruction	Instruction: USER; Check: not_exists	Warn	X
Dockerfile	Instruction	Instruction: ADD; Check: exists	Warn	X

Select gate... 

Dale from Sysdig
Hi Walter, I'm Dale from Sysdig!
We're really excited to have you o...

4.22/ sample runtime disallowed k8s activity:

Your free trial will expire in a month. [Upgrade to Enterprise](#)

Runtime Policies

Secure Insights Scanning Compliance Policies Network Events Investigate Get Started

Disallow K8s Activity

High Severity

Entire Infrastructure

Updated an hour ago
3 rules | Notify Only

Disallow K8s Activity

High Severity

Description: Identify K8s audit activity outside of an explicitly allowed set (images, users, etc).

Scope: Entire Infrastructure

Rules:

- rule: Create Disallowed
- rule: Create Disallowed Pod
- rule: Disallowed K8s User

Dale from Sysdig
Hi Walter, I'm Dale from Sysdig!
We're really excited to have you o...

4.23/ easy to set up alert:

Your free trial will expire in a month. [Upgrade to Enterprise](#)

IMAGE SCANNING
Alerts > New Runtime Alert 

SECURE

Insights 

Scanning 

Compliance 

Policies 

Network 

Events 

Investigate 

Get Started 

WL

Alert Type Runtime

Name alert1

Description Alert Description

Scope Entire Infrastructure 

Trigger

Unscanned Image 

Scan Result Change  Any Change 

CVE Update

Notification Channels

Select notification channel...  Learn about the supported channels for scanning alerts.

Email Channel    

Dale from Sysdig
Hi Walter, I'm Dale from Sysdig!
We're really excited to have you o...

4.24/ sample Image scan reports:

Your free trial will expire in a month. [Upgrade to Enterprise](#)

IMAGE SCANNING Reports BETA

Type Vulnerability Package Policy

Scope Static Registry (e.g. docker.io) Repository (e.g. sysdig/agent) Tag (e.g. latest)

Condition Vuln Type OS +

Run Reset

Search... Download CSV

Package Name	Package Version	Vuln ID	Image Name
apt	1.4.11	CVE-2011-3374	554051034976.dkr.ecr.us-east-1.amazonaws.com/aws-workshop:latest
base-files	9.9+deb9u13	CVE-2010-0834	554051034976.dkr.ecr.us-east-1.amazonaws.com/aws-workshop:latest
bash	4.4-5	CVE-2010-0002	554051034976.dkr.ecr.us-east-1.amazonaws.com/aws-workshop:latest
binutils	2.28-5	CVE-2006-0646	554051034976.dkr.ecr.us-east-1.amazonaws.com/aws-workshop:latest

[Load More...](#)

Get Started

Dale from Sysdig
Hi Walter, I'm Dale from Sysdig!
We're really excited to have you o...

Your free trial will expire in a month. [Upgrade to Enterprise](#)

 SECURE

 Insights

 Scanning

 Compliance

 Policies

 Network

 Events

 Investigate

 Get Started

 WL

IMAGE SCANNING Reports BETA

Type Vulnerability Package Policy

Scope Static Registry (e.g. docker.io) Repository (e.g. sysdig/agent) Tag (e.g. latest)

Condition Vuln Type OS

[Run](#) [Reset](#)

Search... [Download CSV](#)

Vuln ID	Severity	Package Name	Package Version	Fixed In	Image Name
CVE-2021-20244	High	imagemagick	8:6.9.7.4+dfsg...	6.9.7.4+dfsg-11+deb9u12	554051034976.dkr.ecr.us-east-1.amazonaws.com/aw...
CVE-2020-3909	High	libxml2	2.9.4+dfsg1-2...	None	554051034976.dkr.ecr.us-east-1.amazonaws.com/aw...
CVE-2021-3177	High	python3.5	3.5.3-1+deb9u3	3.5.3-1+deb9u4	554051034976.dkr.ecr.us-east-1.amazonaws.com/aw...
CVE-2021-20309	High	imagemagick	8:6.9.7.4+dfsg...	6.9.7.4+dfsg-11+deb9u13	554051034976.dkr.ecr.us-east-1.amazonaws.com/aw...
CVE-2019-12900	High	bzip2	1.0.6-8.1	None	554051034976.dkr.ecr.us-east-1.amazonaws.com/aw...
CVE-2021-20246	High	imagemagick	8:6.9.7.4+dfsg...	6.9.7.4+dfsg-11+deb9u12	554051034976.dkr.ecr.us-east-1.amazonaws.com/aw...
CVE-2020-3910	High	libxml2	2.9.4+dfsg1-2...	None	554051034976.dkr.ecr.us-east-1.amazonaws.com/aw...
CVE-2021-3517	High	libxml2	2.9.4+dfsg1-2...	2.9.4+dfsg1-2.2+deb9u4	554051034976.dkr.ecr.us-east-1.amazonaws.com/aw...
CVE-2021-20312	High	imagemagick	8:6.9.7.4+dfsg...	6.9.7.4+dfsg-11+deb9u13	554051034976.dkr.ecr.us-east-1.amazonaws.com/aw...
CVE-2021-20245	High	imagemagick	8:6.9.7.4+dfsg...	6.9.7.4+dfsg-11+deb9u13	554051034976.dkr.ecr.us-east-1.amazonaws.com/aw...
CVE-2016-2779	High	util-linux	2.29.2-1+deb9...	None	554051034976.dkr.ecr.us-east-1.amazonaws.com/aw...
CVE-2019-5827	High	sqlite-libs	3.26.0	None	docker.io/sysdiglabs/cloud-connector-s3-bucket-confi...
CVE-2021-3177	High	python2.7	2.7.13-2+deb9...	None	554051034976.dkr.ecr.us-east-1.amazonaws.com/aw...
CVE-2019-8905	Medium	file	1:5.30-1+deb9...	None	554051034976.dkr.ecr.us-east-1.amazonaws.com/aw...
CVE-2018-12886	Medium	gcc-6	6.3.0-18+deb9...	None	554051034976.dkr.ecr.us-east-1.amazonaws.com/aw...
CVE-2018-7642	Medium	binutils	2.28-5	None	554051034976.dkr.ecr.us-east-1.amazonaws.com/aw...
CVE-2021-23841	Medium	openssl	1.1.0l-1~deb9...	1.1.0l-1~deb9u3	554051034976.dkr.ecr.us-east-1.amazonaws.com/aw...
CVE	Dale from Sysdig		1:2.11.0-3+de...	None	554051034976.dkr.ecr.us-east-1.amazonaws.com/aw...
CVE	Hi Walter, I'm Dale from Sysdig! We're really excited to have you o...		2.9.4+dfsg1-2...	2.9.4+dfsg1-2.2+deb9u4	554051034976.dkr.ecr.us-east-1.amazonaws.com/aw...

4.25/ Benchmarks of AWS security – many checks:

Your free trial will expire in a month. [Upgrade to Enterprise](#)

BENCHMARKS
Tasks > AWS Foundations Benchmark

Type: CIS Amazon Web Services Foundations Compliance Benchmark V1.3.0

Schedule:

Scope: Entire Infrastructure

Summary

Identity and Access Management

- 1.4 Ensure no root user account access key exists Level 1 Passed
- 1.5 Ensure MFA is enabled for the 'root user' account Level 1 Failed
- 1.6 Ensure hardware MFA is ... Level 2 Passed
- 1.7 Eliminate use of the root ... Level 1 Passed
- 1.8 Ensure IAM password pol... Level 1 Passed
- 1.9 Ensure IAM password pol... Level 1 Passed
- 1.10 Ensure multi-factor auth... Level 1 Passed
- 1.12 Ensure credentials unus... Level 1 Passed
- 1.13 Ensure there is only one ...Level 1 Passed
- 1.14 Ensure access keys are ... Level 1 Passed
- 1.15 Ensure IAM Users Recei... Level 1 Passed
- 1.16 Ensure IAM policies that... Level 1 Passed
- 1.17 Ensure a support role ha...Level 1 Passed
- 1.19 Ensure that all the expire...Level 1 Passed
- 1.20 Ensure that S3 Buckets ... Level 1 Passed

Logging

- 3.1 Ensure CloudTrail is enable...Level 1 Passed
- 3.2 Ensure CloudTrail log file ... Level 2 Passed
- 3.4 Ensure CloudTrail trails ar...Level 1 Passed
- 3.5 Ensure AWS Config is ena...Level 1 Passed
- 3.6 Ensure S3 bucket access ...Level 1 Passed
- 3.7 Dale from Sysdig
- 3.8 Hi Walter, I'm Dale from Sysdig! We're really excited to have you o...

99% *
of Resources Pass
1682 Resources Passing
10 Resources Failing
1692 Total Resources

Identity and Access Management 1670 of 1677 resources passed

1.4 Ensure no root user account access key exists 1 of 1 resources passed

1.5 Ensure MFA is enabled for the 'root user' account 0 of 1 resources passed

What is this check?:
The root user account is the most privileged user in an AWS account. Multi-factor Authentication (MFA) adds an extra layer of protection on top of a username and password. With MFA enabled, when a user signs in to an AWS website, they will be prompted for their username and password as well as for an authentication code from their AWS MFA device.

How is this check addressed?:
Enabling MFA provides increased security for console access as it requires the authenticating principal to possess a device that emits a time-sensitive key and have knowledge of a credential.

Affected Resources (account):
account_id
554051034976

Remediation Procedure
Perform the following to establish MFA

1.6 Ensure hardware MFA is enabled for the 'root user' account 0 of 1 resources passed

Your free trial will expire in a month. [Upgrade to Enterprise](#)

BENCHMARKS

Tasks > AWS Foundations Benchmark

Account Id: 5540510349... Region: eu-central-1 Evaluation Date: ... Download CSV

Schedule: Entire Infrastructure

99%* of Resources Pass

1682 Resources Passing **10** Resources Failing

Total 1692 Resources

Summary

- Identity and Access Management**
 - 1.4 Ensure no root user account is used Level 1
 - 1.5 Ensure MFA is enabled for root user Level 1
 - 1.6 Ensure hardware MFA is enabled Level 2
 - 1.7 Eliminate use of the root user for AWS Lambda Level 1
 - 1.8 Ensure IAM password policies are strong Level 1
 - 1.9 Ensure IAM password policies are unique Level 1
 - 1.10 Ensure multi-factor authentication is used Level 1
 - 1.12 Ensure credentials are rotated regularly Level 1
 - 1.13 Ensure there is only one root user Level 1
 - 1.14 Ensure access keys are rotated regularly Level 1
 - 1.15 Ensure IAM Users Receive Periodic Password Changes Level 1
 - 1.16 Ensure IAM policies that restrict access are used Level 1
 - 1.17 Ensure a support role has limited permissions Level 1
 - 1.19 Ensure that all the expire after 90 days Level 1
 - 1.20 Ensure that S3 Buckets are encrypted Level 1
- Logging**
 - 3.1 Ensure CloudTrail is enabled Level 1
 - 3.2 Ensure CloudTrail log file rotation is enabled Level 2
 - 3.4 Ensure CloudTrail trails are rotated Level 1
 - 3.5 Ensure AWS Config is enabled Level 1
 - 3.6 Ensure S3 bucket access logging is enabled Level 1
 - 3.7 Ensure CloudTrail logs are rotated Level 2
 - 3.8 Ensure rotation for custom logs is enabled Level 2
 - 3.9 Ensure VPC flow logging is enabled in all VPCs Level 2
- Networking**
 - 5.2 Ensure no security group rules allow inbound traffic from the Internet Level 1

3.9 Ensure VPC flow logging is enabled in all VPCs 0 of 1 resources passed

What is this check?
VPC Flow Logs is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC. After you've created a flow log, you can view and retrieve its data in Amazon CloudWatch Logs. It is recommended that VPC Flow Logs be enabled for packet 'rejects' for VPCs.

How is this check addressed?
VPC Flow Logs provide visibility into network traffic that traverses the VPC and can be used to detect anomalous traffic or insight during security workflows.

Affected Resources (vpc):
VpcId
vpc-17970e7d

Remediation Procedure

Perform the following to determine if VPC Flow logs is enabled:

From Console:

1. Sign into the management console
2. Select Services then VPC
3. In the left navigation pane, select Your VPCs
4. Select a VPC
5. In the right pane, select the Flow Logs tab.
6. If no Flow Log exists, click Create Flow Log
7. For Filter, select Reject

Your free trial will expire in a month. [Upgrade to Enterprise](#)

BENCHMARKS

Tasks > AWS Foundations Benchmark

Account Id: 5540510349... Region: eu-central-1 Evaluation Date: ... Download CSV

Schedule: Entire Infrastructure

Summary: 99%* of Resources Pass

1682 Resources Passing, 10 Resources Failing, Total 1692 Resources

sg-d26554a0 default

Remediation Procedure

Security Group Members: Perform the following to implement the prescribed state:

- Identify AWS resources that exist within the default security group
- Create a set of least privilege security groups for those resources
- Place the resources in those security groups
- Remove the resources noted in #1 from the default security group

Security Group State:

- Login to the AWS Management Console at <https://console.aws.amazon.com/vpc/home>
- Repeat the next steps for all VPCs - including the default VPC in each AWS region:
 - In the left pane, click Security Groups
 - For each default security group, perform the following:
 - Select the default security group
 - Click the Inbound Rules tab
 - Remove any inbound rules
 - Click the Outbound Rules tab
 - Remove any outbound rules

Recommended: IAM groups allow you to edit the "name" field. After remediating default groups rules for all VPCs in all regions, edit

Your free trial will expire in a month. [Upgrade to Enterprise](#)

BENCHMARKS

Tasks > AWS Foundations Benchmark

Account Id: 5540510349... Region: eu-central-1 Evaluation Date:

[Download CSV](#)

Schedule: Entire Infrastructure

99%* of Resources Pass

1682 Resources Passing, 10 Resources Failing

Total 1692 Resources

Summary

- Identity and Access Management**
 - 1.4 Ensure no root user account is used Level 1
 - 1.5 Ensure MFA is enabled for root user Level 1
 - 1.6 Ensure hardware MFA is enabled Level 1
 - 1.7 Eliminate use of the root user for administrative tasks Level 1
 - 1.8 Ensure IAM password policies are strong Level 1
 - 1.9 Ensure IAM password policies are unique Level 1
 - 1.10 Ensure multi-factor authentication is used Level 1
 - 1.12 Ensure credentials are rotated regularly Level 1
 - 1.13 Ensure there is only one root user Level 1
 - 1.14 Ensure access keys are rotated regularly Level 1
 - 1.15 Ensure IAM Users Receive Periodic Password Changes Level 1
 - 1.16 Ensure IAM policies that restrict root user access Level 1
 - 1.17 Ensure a support role has limited permissions Level 1
 - 1.19 Ensure that all the expire after 90 days Level 1
 - 1.20 Ensure that S3 Buckets are encrypted Level 1
- Logging**
 - 3.1 Ensure CloudTrail is enabled Level 1
 - 3.2 Ensure CloudTrail log file rotation is enabled Level 2
 - 3.4 Ensure CloudTrail trails are encrypted Level 1
 - 3.5 Ensure AWS Config is enabled Level 1
 - 3.6 Ensure S3 bucket access logging is enabled Level 1
 - 3.7 Ensure CloudTrail logs are encrypted Level 2
 - 3.8 Ensure rotation for custom logs is enabled Level 2
 - 3.9 Ensure VPC flow logging is enabled Level 2
- Networking**
 - 5.2 Ensure no security groups allow ingress from 0.0.0.0/0 to remote server administration ports Level 1

Check Details:

5.2 Ensure no security groups allow ingress from 0.0.0.0/0 to remote server administration ports (1 of 1 resources passed)

5.3 Ensure the default security group of every VPC restricts all traffic (0 of 1 resources passed)

What is this check?:
A VPC comes with a default security group whose initial settings deny all inbound traffic, allow all outbound traffic, and allow all traffic between instances assigned to the security group. If you don't specify a security group when you launch an instance, the instance is automatically assigned to this default security group. Security groups provide stateful filtering of ingress/egress network traffic to AWS resources. It is recommended that the default security group restrict all traffic. The default VPC in every region should have its default security group updated to comply. Any newly created VPCs will automatically contain a default security group that will need remediation to comply with this recommendation.

How is this check addressed?:
Configuring all VPC default security groups to restrict all traffic will encourage least privilege security group development and mindful placement of AWS resources into security groups which will in-turn reduce the exposure of those resources.

Affected Resources (security-group):

GroupId	GroupName
sg-d26554a0	default

Remediation Procedure

Security Group Members

Your free trial will expire in a month. [Upgrade to Enterprise](#)

BENCHMARKS

Tasks > AWS Foundations Benchmark

Account Id: 5540510349... Region: eu-central-1 Evaluation Date: [Change](#) Download CSV

Schedule: Entire Infrastructure

Summary: 99%* of Resources Pass

Logs: 1682 Resources Passing, 10 Resources Failing, Total 1692 Resources

Identity and Access Management (Level 1):

- 1.4 Ensure no root user account is used Level 1
- 1.5 Ensure MFA is enabled for root user Level 1
- 1.6 Ensure hardware MFA is enabled for root user Level 2
- 1.7 Eliminate use of the root user for AWS Lambda functions Level 1
- 1.8 Ensure IAM password policies are configured Level 1
- 1.9 Ensure IAM password policies are configured Level 1
- 1.10 Ensure multi-factor authentication is used for IAM users Level 1
- 1.12 Ensure credentials are rotated regularly Level 1
- 1.13 Ensure there is only one root user account Level 1
- 1.14 Ensure access keys are rotated regularly Level 1
- 1.15 Ensure IAM Users Received MFA Level 1
- 1.16 Ensure IAM policies that grant permissions are least privilege Level 1
- 1.17 Ensure a support role has been created Level 1
- 1.19 Ensure that all the expire after 90 days Level 1
- 1.20 Ensure that S3 Buckets are encrypted Level 1

Logging (Level 1):

- 3.1 Ensure CloudTrail is enabled on all regions Level 1
- 3.2 Ensure CloudTrail log file rotation is enabled Level 2
- 3.4 Ensure CloudTrail trails are encrypted at rest using KMS CMKs Level 1
- 3.5 Ensure AWS Config is enabled in all regions** Level 1 (highlighted)
- 3.6 Ensure S3 bucket access logging is enabled on the CloudTrail S3 bucket Level 1
- 3.7 Ensure CloudTrail logs are encrypted at rest using KMS CMKs Level 2
- 3.8 Ensure rotation for customer created CMKs is enabled Level 2

What is this check?: AWS Config is a web service that performs configuration management of supported AWS resources within your account and delivers log files to you. The recorded information includes the configuration item (AWS resource), relationships between configuration items (AWS resources), any configuration changes between resources. It is recommended to enable AWS Config be enabled in all regions.

How is this check addressed?: The AWS configuration item history captured by AWS Config enables security analysis, resource change tracking, and compliance auditing.

Affected Resources (account):

account_id: 554051034976

Remediation Procedure:

To implement AWS Config configuration: [View Details](#)

3.5 Ensure AWS Config is enabled in all regions: 0 of 1 resources passed

3.6 Ensure S3 bucket access logging is enabled on the CloudTrail S3 bucket: 4 of 4 resources passed

3.7 Ensure CloudTrail logs are encrypted at rest using KMS CMKs: 2 of 2 resources passed

3.8 Ensure rotation for customer created CMKs is enabled: 0 of 0 resources passed

Dale from Sysdig
Hi Walter, I'm Dale from Sysdig!
We're really excited to have you on board!

4.26/ CloudTrail – can see ALL events in Sysdig as in AWS, e.g. delete a test s3 bucket event below:

The screenshot shows the AWS CloudTrail Dashboard. On the left sidebar, 'CloudTrail' is selected, and 'Dashboard' is highlighted. The main content area displays the 'Dashboard' page. At the top, there are two notifications: one about IAM Access Analyzer and another about creating an organization trail. Below these, the 'CloudTrail > Dashboard' breadcrumb is shown. The 'Dashboard' section contains two tables: 'Trails' and 'CloudTrail Insights'. The 'Trails' table lists two trails: 'EventEngineTrail' and 'Sysdig-CloudVision-CloudTrailStack-97FL9HGJT4MB-Trail', both of which are 'Logging'. The 'CloudTrail Insights' table is currently disabled. The 'Event history' section is the primary focus, showing a table of recent events. The first event listed is 'DeleteBucketEncr...', with its event time and source ('s3.amazonaws.com') highlighted by a red box and a red arrow pointing to it. Other events listed include 'CreateBucket', 'UpdateInstanceState...', 'UpdateInstanceState...', and 'CreateLogStream'. A 'View full Event history' link is at the bottom of the table.

Event name	Event time	Event source
DeleteBucketEncr...		s3.amazonaws.com
CreateBucket		s3.amazonaws.com
UpdateInstanceState...		ssm.amazonaws.com
UpdateInstanceState...		ssm.amazonaws.com
CreateLogStream		logs.amazonaws.com

Sales Services ▾ Search for services, features, marketplace products, and docs [Alt+S] TeamRole/MasterKey @ 5540-S103-4976 N. Virginia ▾ Support

CloudTrail X

CloudTrail > Event history > DeleteBucketEncryption

DeleteBucketEncryption Info

Details Info

Event time	AWS access key	AWS region
User name	ASIAVCAAD35QBSXZBQE	us-east-1
Event name	Source IP address	Error code
DeleteBucketEncryption	18.213.118.152	-
Event source	Event ID	Read-only
s3.amazonaws.com	ffe7c0a4-73c1-4ad0-9f3f-f954de067a32	false
Request ID	DFDCZZAR15ARSNR1	

Resources referenced (1) Info

Resource type	Resource name	AWS Config resource timeline
AWS::S3::Bucket	wl123456-1623265087	Enable AWS Config resource recording

Event record Info

Copy

```
{  
    "eventVersion": "1.08",  
    "userIdentity": {  
        "type": "AssumedRole",  
        "principalId": "AROAVCAAD35QH71GGNYX5:i-09fa3ae61bd597c18",  
        "arn": "arn:aws:ssts::1554051034976:assumed-role/Sysdig-Workshop-Admin/i-09fa3ae61bd597c18",  
        "accountId": "554051034976",  
        "accessKeyId": "ASIAVCAAD35QBSXZBQE",  
        "sessionContext": {  
            "sessionIssuer": {  
                "type": "Role",  
                "principalId": "AROAVCAAD35QH71GGNYX5",  
                "arn": "arn:aws:iam::1554051034976:role/Sysdig-Workshop-Admin",  
                "accountId": "554051034976",  
                "userName": "Sysdig-Workshop-Admin"  
            },  
            "webIdFederationData": {},  
            "attributes": {  
                "creationDate": "2021-06-09T18:12:50Z",  
                "mfaAuthenticated": "false"  
            },  
            "ec2RoleDelivery": "2.0"  
        }  
    },  
    "eventTime": "2021-06-09T18:12:50Z",  
    "eventSource": "s3.amazonaws.com",  
    "eventName": "DeleteBucketEncryption",  
    "awsRegion": "us-east-1",  
    "sourceIPAddress": "18.213.118.152",  
    "userAgent": "[aws-cli/2.2.10 Python/3.8.8 Linux/4.14.232-176.381.amzn2.x86_64 exe/x86_64.amzn.2 prompt/off  
command/s3api.delete-bucket-encryption]",  
    "requestParameters": {  
        "bucketName": "wl123456-1623265087",  
        "Host": "wl123456-1623265087.s3.us-east-1.amazonaws.com"  
    }  
}
```

Red arrows point to the event time, event name, and event ID fields in the Details section, and to the event time field in the Event record section.

Your free trial will expire in a month. [Upgrade to Enterprise](#)

Events

Everywhere

Search by event title and label High Med Low Info All Types Filters...

12:02:55 PM • aws Delete Bucket Encryption - Sysdig AWS Best Practices

10:55:21 AM • aws Create Customer Master Key - Sysdig AWS Best Practices

Load Older...

Triggered on
aws Delete Bucket Encryption - Sysdig AWS Best Practices
High Severity Event ID: 1686ff422c6cc39a5261ce712

Policy & Triggered Rules
name Delete Bucket Encryption - Sysdig AWS Best Practices
ruleType AWS CloudTrail
ruleName Delete Bucket Encryption

A encryption configuration for a bucket has been deleted (requesting user=Sysdig-Workshop-admin, requesting IP=18.213.118.152, AWS region us-east-1, bucket=w123456-1623265087)

cloud
aws
aws_s3
mitre_TA0005-defense-evasion
mitre_T1070-indicator-removal-on-host

Scope
aws.accountId 554051034976
aws.eventId ffe7c0a4-73c1-4ad0-0f3f-f954de067a32
aws.region us-east-1
aws.requestId DFDCZZAR15ARSNR1
aws.s3.bucket w123456-1623265087
aws.sourceIP 18.213.118.152
aws.user Sysdig-Workshop-Admin
resourceCategory Storage
resourceType AWS Simple Storage Service

Can see the same eventId in Sysdig as in AWS CloudTrail!