



Search in this guide

Contact Us

English ▾

[AWS](#) > [Documentation](#) > [Amazon GuardDuty](#) > [Amazon GuardDuty User Guide](#) [Feedback](#) [Preferences](#)

EKS Pro tect ion find ing typ es

[PDF](#) | [RSS](#)

The
followin
g
findings
are

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

Amazon
EKS
resource
s and
have a
resource
_type of



Contact Us



and
details
of the
findings
differ
based on
finding
type.

For all
EKS
audit
logs
type
findings
we
recomm
end that
you
examine
the
resource

in
question
to
determin
e if the
activity
is
expected
or
potential
ly
maliciou

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



ing a
compro
mised
EKS
audit
logs
resource
identifie
d by a
GuardDu
ty
finding,
see
[Remedia](#)
[ting EKS](#)
[Protecti](#)
[on](#)
[findings.](#)

Note

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



u
s
e
o
f
w
h
i
c
h
t
h
e
s
e
f
i
n
d
i
n
g

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

g
e
n
e
r
a
t
e



Contact Us



[AWS](#) > [Documentation](#) > [Amazon GuardDuty](#) > [Amazon GuardDuty User Guide](#) [Feedback](#) [Preferences](#)

x p e c t e d . ' c o m s i d e r a d i c a l i n g .

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



i
n
G
u
a
r
d
D
u
t
y
t
o
p
r
e
v
e
n
t
f
u

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



alAc

cess:

Kub

erne

tes/

Mali

ciou

sIPC

aller

- Cred

enti

alAc

cess:

Kub

erne

tes/

Mali

ciou

sIPC

aller

.Cus

tom

- Cred

enti

alAc

cess:

Kub

erne

tes/

Succ

essf

ulAn

ony

mou

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



alAc

cess:

Kub

erne

tes/

Torl

PCal

ler

- Defe

nseE

vasi

on:K

uber

nete

s/M

alici

ousl

PCal

ler

- Defe

nseE

vasi

on:K

uber

s/M

alici

ousl

PCal

ler.C

usto

m

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



uber

nete

s/Su

cces

sful

Ano

nym

ous

Acce

ss

- Defe

nseE

vasi

on:K

uber

nete

s/To

rIPC

aller

- Disc

over

y:Ku

bern

etes

etou

sIPC

aller

- Disc

over

y:Ku

bern

etes

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



.Cus

tom

- Disc

over

y:Ku

bern

etes

/Suc

cess

fulA

non

ymo

usAc

cess

- Disc

over

y:Ku

bern

etes

/Tor

IPCa

ller

- Exec

utio

Bern

etes

/Exe

clnK

ube

Syst

emP

od

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



tes/

Mali

ciou

sIPC

aller

- Imp

act:

Kub

erne

tes/

Mali

ciou

sIPC

aller

.Cus

tom

- Imp

act:

Kub

erne

tes/

Succ

essf

utAn

mod

sAcc

ess

- Imp

act:

Kub

erne

tes/

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



isten

ce:K

uber

nete

s/Co

ntai

ner

With

Sens

itive

Mou

nt

- Pers

isten

ce:K

uber

nete

s/M

alici

ousl

PCal

Ier

- Pers

isten

ce:K

uber

nete

s/M

alici

ousl

PCal

Ier.C

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



ce:K

uber

nete

s/Su

cces

sful

Ano

nym

ous

Acce

ss

- Pers

isten

ce:K

uber

nete

s/To

rIPC

aller

- Poli

cy:K

uber

nete

s/Ad

Acc

ssTo

Defa

ultS

ervic

eAcc

ount

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

Acc

ssTo

Defa

ultS

ervic

eAcc

ount



Contact Us



s/An

ony

mou

sAcc

essG

rant

ed

- Poli

cy:K

uber

nete

s/Ex

pose

dDa

shbo

ard

- Poli

cy:K

uber

nete

s/Ku

laf

owD

ashb

Exp

osed

- Privi

lege

Esca

latio

n:Ku

bern

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



- Credenti
 - malicious
 - Behaviors
 - aviation
 - r.Security
 - rets
 - Access
 - ssed
- Privelege Escalation

n:Ku
ber

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

OMA
lous
Beh
avio
r.Rol
eBin
ding



Contact Us



n:Ku

ber

etes

/An

oma

lous

Beh

avio

r.Exe

cInP

od

- Priva

lege

Esca

lati

n:Ku

ber

etes

/An

oma

lous

Beh

avio

r.Wo

eplo

yed!

Priva

lege

dCo

ntai

ner

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



nete

s/An

oma

lous

Beh

avio

r.Wo

rklo

adD

eplo

yed!

Cont

aine

rWit

hSe

nsiti

veM

ount

- Exec

utio

n:Ku

bern

etes

/An

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

Beh

avio

r.Wo

rklo

adD

eplo

yed!



Contact Us



n:Ku

ber

etes

/An

oma

lous

Beh

avio

r.Rol

eCre

ated

- Disc

over

y:Ku

ber

etes

/An

oma

lous

Beh

avio

r Per

miss

ionC

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

Note

B
e
f
o
r



Contact Us



e
r
n
e
t
e
s
v
e
r
s
i
o
n
1
.1
4
,t
h
e

s
y
S
y
m
u
n
a
u

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



t
i
c
a
t
e
d
g
r
o
u
p
w
a
s
a
s
s
o
c
i
a
t
e
o
s
y
s
t
e
m

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



c
o
v
e
r
y
a
n
d
s
y
s
t
e
m
:
b
a
s
i
c

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



s
b
y
d
e
f
a
u
l
t
.T
h
i
s
a
s
s
o
c
i
a

t
i
o
m
a
y
a
l
l
o
w

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



t
e
n
d
e
d
a
c
c
e
s
s
f
r
o
m
a
n
o
n
y
m

o
u
s
e
r
s
-
C
l
u

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



- ▶ What is GuardDuty?
 - Concepts and terminology
 - Getting started
 - Foundational data sources
- ▶ EKS Protection
- ▶ S3 Protection
- ▶ Runtime Monitoring
- ▶ Malware Protection for EC2
- ▶ Malware Protection for S3
- ▶ RDS Protection
- ▶ Lambda Protection
 - Protecting AI workloads
- ▶ Multiple accounts in GuardDuty
- ▼ GuardDuty finding types
 - EC2 finding types
 - IAM finding types
 - S3 Protection finding types
 - EKS Protection finding types**

| | |
|---|---|
| u | CredentialAccess:Kubernetes/MaliciousIPCaller |
| p | CredentialAccess:Kubernetes/MaliciousIPCaller.Custom |
| d | CredentialAccess:Kubernetes/SuccessfulAnonymousAccess |
| a | CredentialAccess:Kubernetes/TorIPCaller |
| t | DefenseEvasion:Kubernetes/MaliciousIPCaller |
| e | DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom |
| s | DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess |
| d | DefenseEvasion:Kubernetes/TorIPCaller |
| o | Discovery:Kubernetes/MaliciousIPCaller |
| n | Discovery:Kubernetes/MaliciousIPCaller.Custom |
| o | Discovery:Kubernetes/SuccessfulAnonymousAccess |
| t | Discovery:Kubernetes/TorIPCaller |
| r | Impact:Kubernetes/MaliciousIPCaller |
| e | Impact:Kubernetes/MaliciousIPCaller.Custom |
| v | Impact:Kubernetes/SuccessfulAnonymousAccess |
| o | Impact:Kubernetes/TorIPCaller |
| k | Execution:Kubernetes/ExecInKubeSys |
| e | Execution:Kubernetes/ExecInKubeSys.Impact:Kubernetes/MaliciousIPCaller |
| t | Execution:Kubernetes/ExecInKubeSys.Impact:Kubernetes/MaliciousIPCaller.Custom |
| h | Execution:Kubernetes/SuccessfulAnonymousAccess |
| e | Execution:Kubernetes/TorIPCaller |
| s | Impacts:Kubernetes/MaliciousIPCaller |

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

Malware Protection for S3

finding type

RDS Protection finding types

Lambda Protection finding types



Contact Us



n
i
f
y
o
u
u
p
d
a
t
e
d
y
o
u
r
c
l
u
s
t

e
r
r
v
e
r
s
i
o
n
1

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



r
h
i
g
h
e
r,
t
h
e
s
e
p
e
r
m
i
s
s
i
o

n
s
y
s
t
i
l
b
e

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



l
e
d
.W
e
r
e
c
o
m
m
e
n
d
t
h
a
t
y
o
u

d
i
S
S
o
c
i
a
t
e

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



e
p
e
r
m
i
s
s
i
o
n
s
f
r
o
m
t
h
e
s
y
s

t
e
u
n
a
u
t
h
e

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



a
t
e
d
g
r
o
u
p
.F
o
r
g
u
i
d
a
n
c
e
o

n
r
o
k
i
n
g
t
h

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



e
r
m
i
s
s
i
o
n
s
,s
e
e
S
e
c
u
r
i
t
y

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



A
m
a
z
o
n
E
K
S
i
n
t
h
e
A
m
a
z
o
n
E
K

S
U
S
T
R
G
u
i
d
e

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



[AWS](#) > [Documentation](#) > [Amazon GuardDuty](#) > [Amazon GuardDuty User Guide](#) [Feedback](#) [Preferences](#)

lAccess:Ku
bernetes/
Malicious/
PCaller

An API
communicated
only used
to access
credentials

Or secret
in a cluster
was invoked
from a

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



address

severity

Default severity
: High

- **Feature:**
EKS audit logs

This finding informs you that an API operation was invoked from an IP address associated with known malicious activity.

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

associate with known malicious activity. The API observes



Contact Us



d with
the
creden
tal access
tactics
where an
adversar
y is
attempti
ng to
collect
passwor
ds,
usernam
es, and
access
keys for
your
Kuberne
tes
cluster.

Remedi
ation
recomm
endati
ons.

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

If the
user
reported
in the
finding
under



Contact Us



s
section
is
system
:anonym
ous,
investiga
te why
the
anonym
ous user
was
permitte
d to
invoke
the API
and
revoke
the
permissi
ons, if
needed.
by
followin

ons in
Security
best
practices
for
Amazon
EKS in

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



the user
is an
authenticated
user,
investigate
to determine
if the
activity
was
legitimate
or
malicious.
If the
activity
was
malicious
revoke
access of
the user
and
reverse
any
changes
an
adversary
to your
cluster.
For more
information,
see
Remediation

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



Cred
entia
lAcce
ss:Ku
ber
netes/
Malic
iousl
PCall
er.Cu
stom

An
API
comm
only

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



**from
an IP
addre
ss on
a
custo
m
threat
list.**

**Default
severity
: High**

- **Feat
ure:
EKS
audi
t
logs**

This
finding
informs

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

an API
operation
n was
invoked
from an
IP
address
that is



Contact Us



you
upload
d. The
threat
list
associate
d with
this
finding
is listed
in the
Additio
nal
Informa
tion
section
of a
finding's
details.
The API
observe
d is
common
ly
associate
d with
the
credential
access
tactics
where an
adversar
y is
attempti

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



username
es, and
access
keys for
your
Kuberne
tes
cluster.

**Remedi
ation
recomm
endatio
ns:**

If the
user
reported
in the
finding
under
the

Kubern
etesUse
rDetail

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

selection
is
system
: anonym
ous,
investiga
te why
the



Contact Us



d to
invoke
the API
and and
revoke
the
permis
ons, if
needed,
by
followin
g the
instructi
ons in
[Security](#)
[best](#)
[practices](#)
for
[Amazon](#)
[EKS](#) in
the
[Amazon](#)

[EKS User](#)
[Guide](#). If
the user
is authenti
cated
as a user,
GuardDuty
investiga
tes the ac
tivity to
determin
e if the ac
tivity is a
privilege es
calation at
tempt. If the
attempt is
detected, a
GuardDuty
finding is
generated
and sent to
the user's
AWS Lambda
function or
Amazon
CloudWatch
Logs.

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



s. If the activity was malicious revoke access of the user and reverse any changes made by an adversary to your cluster. For more information, see [Remediating EKS Protection findings](#).

on findings.

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

Credentia
l Access:
Kuber
netes/
etcs/



Contact Us



**nym
ousA
ccess**

An API comm only used to access crede ntials or secret s in a Kuber netes cluste

I was invok ed by unaut hentic ated user.

Default severity

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



[AWS](#) > [Documentation](#) > [Amazon GuardDuty](#) > [Amazon GuardDuty User Guide](#) [Feedback](#) [Preferences](#)

EKS

audi

t

logs

This
finding
informs
you that
an API
operatio
n was
successf
ully
invoked
by the
system
:anonym
ous
user. API
calls
made by
system
:anonym
ous are

The
observe
d API is
common
ly
associate
d with

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



where an
adversar
y is
attempti
ng to
collect
passwor
ds,
usernam
es, and
access
keys for
your
Kuberne
tes
cluster.

This
activity
indicates
that
anonym
ous or

unauthen
ticated
access is
made to
the API
action
reported
in the
finding
and may
be

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



If this behavior is not expected, it may indicate a configuration mistake or that your credentials are compromised.

Remediation recommendations:

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

permissions that have been granted to the system



Contact Us



and
ensure
that all
the
permis
ons are
needed.
If the
permis
ons were
granted
mistaken
ly or
maliciou
sly, you
should
revoke
access of
the user
and
reverse
any
changes
made by

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

y to your
cluster.
For more
informat
ion, see
Security
best
practices



Contact Us



[AWS](#) > [Documentation](#) > [Amazon GuardDuty](#) > [Amazon GuardDuty User Guide](#) [Feedback](#) [Preferences](#)

*Amazon
EKS User
Guide.*

For more
informat
ion, see
[Remedia
ting EKS
Protecti
on
findings.](#)

**Cred
entia
lAcce
ss:Ku
ber
etes/**

**TorIP
Calle**

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

An
API
comm
only
used
to



Contact Us



**secret
s in a
Kuber
netes
cluste
r was
invok
ed
from
a Tor
exit
node
IP
addre
ss.**

**Default
severity
: High**

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

This
finding
informs
you that
an API



Contact Us



node IP
address.
The API
observe
d is
common
ly
associate
d with
the
credenti
al access
tactics
where an
adversar
y is
attempti
ng to
collect
passwor
ds,
usernam
es, and
access
keys for
Kuberne
tes
cluster.
Tor is
software
for
enabling
anonim

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

Kuberne
tes
cluster.
Tor is
software
for
enabling
anonim



Contact Us



encrypts
and
randoml
y
bounces
commun
ications
through
relays
between
a series
of
network
nodes.

The last
Tor node
is called
the exit
node.

This can
indicate
unautho

rized
access to

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

res
cluster
resource
s with
the
intent of
hiding
the



Contact Us



[AWS](#) > [Documentation](#) > [Amazon GuardDuty](#) > [Amazon GuardDuty User Guide](#) [Feedback](#) [Preferences](#)

Remediation

Action
recommendations:

If the user reported in the finding under the

KubernetesUserDetails

section is

system anonymous,

investigate why the

was permitted to invoke the API and revoke

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



by
followin
g the
instructi
ons in
[Security](#)
[best](#)
[practices](#)
for
[Amazon](#)
[EKS](#) in
the
Amazon
EKS User
Guide. If
the user
is an
authenti
cated
user,
investiga
te to
determin
e if the
activity

legitimat
e or
maliciou
s. If the
activity
was
maliciou
s revoke

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



any changes made by an adversary to your cluster. For more information, see [Remediating EKS Protection findings](#).

DefenseEvasio

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

iousl
PCall
er

An
API



Contact Us



**evade
defen
sive
meas
ures
was
invok
ed
from
a
know
n
malici
ous IP
addre
ss.**

**Default
severity
: High**

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

- Feature
- Performance
- Analytics
- Security
- Logs

This finding informs you that



Contact Us



from an IP address that is associate d with known maliciou s activity. The API observe d is common ly associate d with defense evasion tactics where an adversar y is trying to hide actions to avoid detectio n. Remediation recommen

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



[AWS](#) > [Documentation](#) > [Amazon GuardDuty](#) > [Amazon GuardDuty User Guide](#)

[Feedback](#)

[Preferences](#)

user

reported

in the

finding

under

the

Kubern

etesUse

rDetail

s

section

is

system

:anonym

ous ,

investiga

te why

the

anonym

ous user

was

permitte

d to

invoke

the API

revoke

the

perm issi

ons, if

needed,

by

followin

g the

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



practices
for
Amazon
EKS in
the
Amazon
EKS User
Guide. If
the user
is an
authenti
cated
user,
investiga
te to
determin
e if the
activity
was
legitim
e or
maliciou

s. If the
activity
was
revoke
access of
the user
and
reverse
any
changes
made by

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



For more information, see [Remediating EKS Protection findings](#).

DefenseEvasion:Kubernetes/Malicious/PCaller.CUSTOMER

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

An API comm only used to evade



Contact Us



**was
invok
ed
from
an IP
addre
ss on
a
custo
m
threat
list.**

**Default
severity
: High**

- **Feat
ure:**
EKS
audi

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

finding
informs
you that
an API
operatio
n was
invoked
from an



Contact Us



on a threat list that you uploaded. d. The threat list associate d with this finding is listed in the **Additio**
nal
Informa
tion section of a finding's details.

The API observe dis...
ly associate d with defense evasion tactics where an adversar...

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



actions
to avoid
detectio
n.

**Remedi
ation
recomm
endatio
ns:**

If the
user
reported
in the
finding
under
the
Kubern
etesUse
rDetail
s
section

is
system

investiga
te why
the
anonym
ous user
was
permitt

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



revoke
the
permis
ons, if
needed,
by
followin
g the
instructi
ons in
[Security](#)
[best](#)
[practices](#)
for
[Amazon](#)
[EKS](#) in
the
Amazon
EKS User
Guide. If
the user
is an
authenti
cated
user
attempt
to
determin
e if the
activity
was
legitimat
e or
maliciou

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



s revoke
access of
the user
and
reverse
any
changes
made by
an
adversar
y to your
cluster.
For more
informat
ion, see
[Remedia](#)
[ting EKS](#)
[Protecti](#)
[on](#)
[findings.](#)

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

DefenseE
n:Ku
ber
etes/
Succ
essfu
lAno



Contact Us



An
API
comm
only
used
to
evade
defen
sive
meas
ures
was
invok
ed by
an
unaut
hentic
ated
user

Select your cookie preferences

Default

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

- Feature: EKS audit logs



Contact Us



an API
operatio
n was
successf
ully
invoked
by the
system
:anonym
ous
user. API
calls
made by
system
:anonym
ous are
unauthe
nticated.

The
observe
d API is
common
ly
associate

evasion
tactics
where an
adversar
y is
trying to
hide

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



n. This activity indicates that anonymous or unauthenticated access is permitted on the API action reported in the finding and may be permitted on other actions.

If this behavior is not intended, it may indicate a configuration mistake or that your

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



Remediation recommendations:

You should examine the permissions that have been granted to the system: anonymous user on your cluster and ensure that all

permissions are needed. If the permissions were granted mistakenly

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



revoke
access of
the user
and
reverse
any
changes
made by
an
adversar
y to your
cluster.
For more
informat
ion, see
[Security
best
practices
for
Amazon
EKS in
the](#)

[Amazon
EKS User
Guide](#)
For more
informat
ion, see
[Remedia
ting EKS
Protecti
on
findings.](#)

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

[For more
informat
ion, see
\[Remedia
ting EKS
Protecti
on
findings.\]\(#\)](#)



Contact Us



vasio

n:Ku

bern

etes/

TorIP

Calle

r

An

API

comm

only

used

to

evade

defen

sive

meas

ures

was

invok

from

a Tor

exit

node

IP

addre

ss.

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



• **Find**

ure:
EKS
audi
t
logs

This
finding
informs
you that
an API
was
invoked
from a
Tor exit
node IP
address.
The API
observe
d is
common
lv
associate
d with

tactics
where an
adversar
y is
trying to
hide
their

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



software
for
enabling
anonym
ous
commun
ication.
It
encrypts
and
randoml
y
bounces
commun
ications
through
relays
between
a series
of
network
nodes.

The last
Tor node
is called
the exit
node.
This can
indicate
unautho
rized
access to
your
Kuberne

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



hiding
the
adversar
y's true
identity.

**Remedi
ation
recomm
endatio
ns:**

If the
user
reported
in the
finding
under
the
Kubern
etesUse
rDetail
s

section
is

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

ous,
investiga
te why
the
anonym
ous user
was



Contact Us



and
revoke
the
permis
ons, if
needed,
by
followin
g the
instructi
ons in
[Security](#)
[best](#)
[practices](#)
for
[Amazon](#)
[EKS](#) in
the
Amazon
EKS User
Guide. If
the user

is an
authenti
cated
investiga
te to
determin
e if the
activity
was
legitimat
e or

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

investiga
te to
determin
e if the
activity
was
legitimat
e or



Contact Us



malicious revoke access of the user and reverse any changes made by an adversary to your cluster. For more information, see [Remediating EKS Protection findings](#).

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

Disc
y: Ku
ber
etes/
Malic
iousl



Contact Us



An API comm only used to discov er resou rces in a Kuber netes cluste r was invok ed from an IP addre

ss.

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

Medium

- Feature: EKS audi



Contact Us



finding
informs
you that
an API
operatio
n was
invoked
from an
IP
address
that is
associate
d with
known
maliciou
s
activity.

The
observe
d API is
common
ly used
with the
discover
y stage

attack
wherein
an
attacker
is
gatherin
g
informat

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



tes
cluster is
suscepti
ble to a
broader
attack.



**For
unauthenticated
access**

M
a
l
i
c
i
o
u
s
I
P
C

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



e
n
o
t
g
e
n
e
r
a
t
e
d
f
o
r
u
n
a
u
t
h

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

c
a
t
e
d
a
c
c



Contact Us



S
u
c
c
e
s
s
f
u
l
A
n
o
n
y
m
o
u
s
A
c
c
e
s
i
n
d
i
n
g
s

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



e
n
e
r
a
t
e
d
f
o
r
u
n
a
u
t
h
e
n
t
i
c

a
t
e
r
a
n
o
n
y
m

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



C
C
e
s
s
.

Remediation recommendations:

If the user reported in the finding under the **Kubernetes** **Use**

Detail
s

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

system
: anonym
ous,
investiga
te why
the
anonym



Contact Us



invoke
the API
and
revoke
the
permis
ons, if
needed,
by
followin
g the
instructi
ons in
Security
best
practices
for
Amazon
EKS in
the
Amazon
EKS User
Guide. If
the user
is an
investiga
tor who
determin
es if the
activity
was

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

are required
to function
properly.
Performance
cookies help
us understand
how you use
our site so
we can make
it better.
Privacy
cookies are
used to
protect
your
privacy
and
security.



Contact Us



activity
was
maliciou
s revoke
access of
the user
and
reverse
any
changes
made by
an
adversar
y to your
cluster.
For more
informat
ion, see
[Remedia
ting EKS
Protecti
on](#)

findings.

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

over
y:Ku
ber
etes/
Malic



Contact Us



stom

An API comm only used to discov er resou rces in a Kuber netes cluste r was invok ed from an IP addre

a custo m threat list.

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



- **Feat**
ure:
EKS
audi
t
logs

This
finding
informs
you that
an API
was
invoked
from an
IP
address
that is
included
on a
threat
list that
you
upload

list
associate
d with
this
finding
is listed
in the

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



section
of a
finding's
details.
The
observe
d API is
common
ly used
with the
discover
y stage
of an
attack
wherein
an
attacker
is
gatherin
g
informat
ion to
determin
e if your
Kuberne
t cluster is
suscepti
ble to a
broader
attack.
Remedi
ation

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



in the user reported in the finding under the Kubern etesUse rDetail s section is system :anonym ous , investiga te why the anonym ous user was permitte d to invoke and revoke the permissions, if needed, by followin

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



best practices for Amazon EKS in the *Amazon EKS User Guide*. If the user is an authenticated user, investigate to determine if the activity was legitimate or malicious. If the activity was malicious, revoke access of the user and reverse any changes.

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



cluster.

For more information, see [Remediating EKS Protection findings](#).

Discovers Kubernetes/SuccessfullAno

nymousA

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

An API comm only used to



Contact Us



in a
Kuber
netes
cluste
r was
invok
ed by
an
unaut
hentic
ated
user.

**Default
severity**
:
Medium

- **Feat
ure:**
EKS

audi
t

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

This
finding
informs
you that
an API
operatio
n was
successf



Contact Us



:anonym

ous

user. API

calls

made by

system

:anonym

ous are

unauthe

nticated.

The

observe

d API is

common

ly

associate

d with

the

discover

y stage

of an

attack

when an

adversar

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

g
informat
ion on
your
Kuberne
tes
cluster.



Contact Us



anonym
ous or
unauthe
nticated
access is
permitte
d on the
API
action
reported
in the
finding
and may
be
permitte
d on
other
actions.
If this
behavior
is not
expected
, it may
indicate

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

ation
mistake
or that
your
creden
als are
compro
mised.



Contact Us



the
health
check
API
endpoint
s such as
`/healt`
`hz,`
`/livez,`
`/ready`
`z, and`
`/versi`
`on.`

**Remedi
ation
recomm
endatio
ns:**

You
should
examine
the
permis
sive
privile
ges
that
have
been
granted
to the
system
by anony
mous user
on your

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



the
permis
ons are
needed.
If the
permis
ons were
granted
mistaken
ly or
maliciou
sly, you
should
revoke
access of
the user
and
reverse
any
changes
made by
an

adversar
y to your
cluster
informat
ion, see
Security
best
practices
for
Amazon
EKS in

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



For more information, see [Remediating EKS Protection findings](#).

Discover why: Kubernetes/TorIP Caller

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

An API only used to discover resources



Contact Us



This finding was invoked from a Tor exit node IP address.

Default severity:
Medium

- Feature: EKS audit log

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

This finding was invoked from a Tor exit node IP address.



Contact Us



common
ly used
with the
discover
y stage
of an
attack
wherein
an
attacker
is
gatherin
g
informat
ion to
determin
e if your
Kuberne
tes
cluster is
suscepti
ble to a
broader
attack.

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

for
enabling
anonim
ous
commun
ication.
It
encrypts



Contact Us



communications through relays between a series of network nodes.

The last Tor node is called the exit node.

This can indicate unauthorized access to your Kuberne

tes cluster with the intent of

the adversary's true identity.

Remediation recommendations

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



[AWS](#) > [Documentation](#) > [Amazon GuardDuty](#) > [Amazon GuardDuty User Guide](#)

[Feedback](#)

[Preferences](#)

user

reported

in the

finding

under

the

Kubern

etesUse

rDetail

s

section

is

system

:anonym

ous ,

investiga

te why

the

anonym

ous user

was

permitte

d to

invoke

the

revoke

the

perm issi

ons, if

needed,

by

followin

g the

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

Almos

the

revoke

the

perm issi

ons, if

needed,

by

followin

g the



Contact Us



[AWS](#) > [Documentation](#) > [Amazon GuardDuty](#) > [Amazon GuardDuty User Guide](#) [Feedback](#) [Preferences](#)

practices
for
Amazon
EKS in
the
Amazon
EKS User
Guide. If
the user
is an
authenti
cated
user,
investiga
te to
determin
e if the
activity
was
legitim
e or
maliciou

s. If the
activity
was
revoke
access of
the user
and
reverse
any
changes
made by

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



For more information, see [Remediating EKS Protection findings](#).

Execution:Kubernetes/ExecelnKubeSytem

Pod

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

comm
and
was
execu
ted
inside
a pod



Contact Us



m
name
space

Default
severity
:
Medium

- **Feat**
ure:
EKS
audi
t
logs

This
finding
informs
you that
a
common

d was
executed
in a pod

the
kube-
system
namespa
ce using
Kubern
etes
exec

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



ce is a
default
namespa
ces,
which is
primarily
used for
system
level
compon
ents
such as
kube-
dns and
kube-
proxy.
It is very
uncomm
on to
execute
commanc
ds inside
pods or
containe

system
namespa
ce and
may
indicate
suspicio

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



[AWS](#) > [Documentation](#) > [Amazon GuardDuty](#) > [Amazon GuardDuty User Guide](#)

[Feedback](#)

[Preferences](#)

recomm

endatio

ns:

If the
executio
n of this
comman
d is
unexpect
ed, the
credenti
als of
the user
identity
used to
execute
the
comman
d may be
compro
mised.

Revoke
access of

reverse
any
changes
made by
an
adversar
y to your

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



[AWS](#) > [Documentation](#) > [Amazon GuardDuty](#) > [Amazon GuardDuty User Guide](#) [Feedback](#) [Preferences](#)

Remediation EKS Protection findings.

Impact:Kubernetes/Malicious API Call

An API command only used

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

can be used with resources in a Kuber



Contact Us



**ed
from
a
know
n
malici
ous IP
addre
ss.**

**Default
severity
: High**

- **Feat
ure:
EKS
audi
t
logs**

This
finding
informs

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

an API
operation
n was
invoked
from an
IP
address
that is



Contact Us



s
activity.
The
observe
d API is
common
ly
associate
d with
impact
tactics
where an
adversar
y is
trying to
manipul
ate,
interrupt
, or
destroy
data
within

your
AWS
envir

onment

Remedi
ation
recomm
endatio
ns:

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



finding
under
the
Kubern
etesUse
rDetail
s
section
is
system
:anonym
ous ,
investiga
te why
the
anonym
ous user
was
permitte
d to
invoke
the API
and
revoke

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

ons, if
needed,
by
followin
g the
instructi
ons in



Contact Us



Amazon
EKS in
the
Amazon
EKS User
Guide. If
the user
is an
authenti
cated
user,
investiga
te to
determin
e if the
activity
was
legitimat
e or
maliciou
s. If the
activity
was
maliciou
s revoke
the user
and
reverse
any
changes
made by
an
adversar

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

the user
and
reverse
any
changes
made by
an
adversar



Contact Us



ion, see
Remedia
ting EKS
Protecti
on
findings.

Impact:Kubernetes/Malicious/PCaller.CUSTOMER

An

API
comm
Used
to
tamp
er
with
resou
rces

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



**r was
invok
ed
from
an IP
addre
ss on
a
custo
m
threat
list.**

**Default
severity
: High**

- **Feat
ure:**
EKS
audi

t
logs

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

finding
informs
you that
an API
operatio
n was
invoked
from an



Contact Us



on a threat list that you uploaded. d. The threat list associate d with this finding is listed in the **Additio nal Information** section of a finding's details.

The findings observe d API us. They associate d with impact tactics where an adversary is

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



, or
destroy
data
within
your
AWS
environ
ment.

**Remedi
ation
recomm
endatio
ns:**

If the
user
reported
in the
finding
under
the

Kubern
etesUse
rDetail

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

selection
is
system
:anonym
ous,
investiga
te why
the



Contact Us



d to
invoke
the API
and
revoke
the
permis
ons, if
needed,
by
followin
g the
instructi
ons in
[Security](#)
[best](#)
[practices](#)
for
[Amazon](#)
[EKS](#) in
the
[Amazon](#)

[EKS User](#)
[Guide](#). If
the user
is authenti
cated
as a user,
GuardDuty
investiga
tes the ac
tivity to
determin
e if the ac
tivity is a
privilege es
calation at
tempt. If the
attempt is
detected, a
GuardDuty
finding is
generated
and sent to
the user's
AWS Lambda
function.

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



s. If the activity was malicious revoke access of the user and reverse any changes made by an adversary to your cluster. For more information, see [Remediating EKS Protection findings](#).

on findings.

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

Impact:Kubernetes/
Successful



Contact Us



ccess

An API command only used to tamper with resources in a Kubernetes cluster was invoked by an unauthorized user.

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

Default severity : High



Contact Us



t
logs

This
finding
informs
you that
an API
operatio
n was
successf
ully
invoked
by the
system
:anonim
ous
user. API
calls
made by
system
:anonim

ous are
unauthen
ticated.
The system
observe
d API is
common
ly
associate
d with
the
impact.

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



y is
tamperin
g with
resource
s in your
cluster.

This
activity
indicates
that
anonym
ous or
unauthe
nticated
access is
permitte
d on the
API
action
reported
in the
finding

and may
be
permitted
other
actions.
If this
behavior
is not
expected
, it may
indicate

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



or that
your
creden
tials are
compro
mised.

**Remedi
ation
recomm
endatio
ns:**

You
should
examine
the
permissi
ons that
have
been
granted
to the

system
: anonym

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

cluster
and
ensure
that all
the
permissi
ons are



Contact Us



granted
mistaken
ly or
maliciou
sly, you
should
revoke
access of
the user
and
reverse
any
changes
made by
an
adversar
y to your
cluster.
For more
informat
ion, see
[Security](#)

best
practices
for

EKS in
the
Amazon
EKS User
Guide.

For more
informat

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

EKS in
the
Amazon
EKS User
Guide.

For more
informat



Contact Us



[AWS](#) > [Documentation](#) > [Amazon GuardDuty](#) > [Amazon GuardDuty User Guide](#) [Feedback](#) [Preferences](#)

on
findings.

Impa
ct:Ku
ber
netes/
TorIP
Calle
r

An
API
comm
only
used
to
tamp
er

with
resources
in a
Kuber
netes
cluste
r was
invok

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



node

IP

addre

ss.

Default

severity

: High

- **Feat**
ure:
EKS
audi
t
logs

This
finding
informs
you that
an API

was
invoked

from a

Top exit

mobile

address.

The API

observe

d is

common

ly

associate

d with

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



y is
trying to
manipul
ate,
interrupt
, or
destroy
data
within
your
AWS
environ
ment.
Tor is
software
for
enabling
anonym
ous
commun
ication.

It
encrypts
and
random
bounces
commun
ications
through
relays
between
a series
of

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



is called
the exit
node.
This can
indicate
unautho
rized
access to
your
Kuberne
tes
cluster
with the
intent of
hiding
the
adversar
y's true
identity.

Remedi ation

RECOMM
ENDATIO
NS:

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

User
reported
in the
finding
under
the
Kubern



Contact Us



is
system
:anonym
ous ,
investiga
te why
the
anonym
ous user
was
permitte
d to
invoke
the API
and
revoke
the
permissi
ons, if
needed,
by
followin
g the
instructi

best
practices
for
Amazon
EKS in
the
Amazon

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



authenti
cated
user,
investiga
te to
determin
e if the
activity
was
legitim
e or
maliciou
s. If the
activity
was
maliciou
s revoke
access of
the user
and
reverse
any
changes
made by
an
y to your
cluster.
For more
informat
ion, see
Remedia
ting EKS
Protecti

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



Persi
stenc
e:Ku
ber
etes/
Cont
ainer
With
Sens
itive
Mou
nt

A
contai
ner
was
launc
hed
with a

ive
exter
nal
host
path
moun
ted

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



severity

:

Medium

- **Feat**
ure:
EKS
audi
t
logs

This
finding
informs
you that
a
containe
r was
launched
with a
configur
ation
that
included
a

path
with
write
access in
the
volume
Mounts

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



sensitive

host

path

accessibl

e and

writable

from

inside

the

containe

r. This

techniqu

e is

common

ly used

by

adversari

es to

gain

access to

the

host's

filessyste

m.

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

recomm

endatio

ns:

If this

containe

r launch



Contact Us



als of
the user
identity
used to
launch
the
containe
r may be
compro
mised.
Revoke
access of
the user
and
reverse
any
changes
made by
an
adversar
y to your
cluster.

For more
informat

ion see

[Using EKS](#)

[Protecti](#)

[on](#)

[findings.](#)

If this

containe

r launch

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

[are required](#)

[to provide](#)

[our services.](#)

[Performance](#)

[cookies](#)

[collect](#)

[anonymous](#)

[statistics](#)



Contact Us



ended
that you
use a
suppress
ion rule
consistin
g of a
filter
criteria
based on
the
resour
ce.Kube
rnetesD
etails.
Kuberne
tesWork
loadDet
ails.co
ntainer
s.image
Prefix
field. In
the filter

imageP
refix
field
should
be same
as the
imageP

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



To learn more about creating suppress ion rules see [Suppress ion rules.](#)

Persi
stenc
e:Ku
ber
etes/
Malic
iousl
PCall
er

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

API
comm
only
used
to
obtai



Contact Us



**to a
Kuber
netes
cluste
r was
invok
ed
from
a
know
n
malici
ous IP
addre
ss.**

**Default
severity
:
Medium**

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

- Feature
- ure:
- El
- aud
- t
- logs

This
finding
informs
you that



Contact Us



from an IP address that is associate d with known maliciou s activity. The API observe d is common ly associate d with persisten ce tactics where an adversar y has gained access to your cluster and is attempting to maintain that access.

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



ns:

If the user reported in the finding under the Kubern etesUse rDetail s section is system :anonym ous , investiga te why the anonym ous user was permi

tted to invoke the API and revoke the permissions, if needed,

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



ons in
Security
best
practices
for
Amazon
EKS in
the
Amazon
EKS User
Guide. If
the user
is an
authenti
cated
user,
investiga
te to
determin
e if the
activity
was

legitimat
e or
maliciou
s revoca
access of
the user
and
reverse

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



adversar
y to your
cluster.
For more
informat
ion, see
[Remedia
ting EKS
Protecti
on](#)
[findings.](#)

Persi
stenc
e:Ku
ber
netes/
Malic
iousl

PCall
er Cu
An
API
comm
only
used

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



**tent
access
to a
Kuber
netes
cluste
r was
invok
ed
from
an IP
addre
ss on
a
custo
m
threat
list.**

Default

severity:
:

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

- Feature
- EKS
- audit
- logs



Contact Us



an API
operatio
n was
invoked
from an
IP
address
that is
included
on a
threat
list that
you
upload
d. The
threat
list
associate
d with
this
finding
is listed

in the
Additio
nal
section
of a
finding's
details.
The API
observe
d is

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



persisten
ce tactics
where an
adversar
y has
gained
access to
your
Kuberne
tes
cluster
and is
attempti
ng to
maintain
that
access.

Remedi ation recomm endatio

ns.

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

in the
finding
under
the
Kubern
etesUse
rDetail



Contact Us



:anonym

ous ,

investiga

te why

the

anonym

ous user

was

permitte

d to

invoke

the API

and

revoke

the

permissi

ons, if

needed,

by

followin

g the

instructi

ons in

Security

host

for

Amazon

EKS in

the

Amazon

EKS User

Guide. If

the user

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



investiga
te to
determin
e if the
activity
was
legitim
e or
maliciou
s. If the
activity
was
maliciou
s revoke
access of
the user
and
reverse
any
changes
made by
an
adversar

y to your
cluster
informat
ion, see
Remediat
ing EKS
Protecti
on
findings.

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



e:Ku
bern
etes/
Succ
essfu
lAno
nym
ousA
ccess

An
API
comm
only
used
to
obtai
n

high-
level
permis
to a
Kuber
netes
cluste
r was
invok

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

to a
Kuber
netes
cluste
r was
invok



Contact Us



ated
user.

Default
severity
: High

- **Feat**
ure:
EKS
audi
t
logs

This
finding
informs
you that
an API
operatio
n was
successf

ility
invoked
by the
: anonym
ous
user. API
calls
made by
system
: anonym
ous. are

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



This API is commonly associated with the persistent tactics where an adversary has gained access to your cluster and is attempting to maintain that access.

This activity indicates that

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

ous or unauthenticated access is permitted on the API action



Contact Us



be
permitte
d on
other
actions.
If this
behavior
is not
expected
, it may
indicate
a
configur
ation
mistake
or that
your
creden
tials are
compro
mised.

Remedi
ation
recomm
endati
ons.

You
should
examine
the
permis
sions that

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



system
:anonym
ous user
on your
cluster
and
ensure
that all
the
permissi
ons are
needed.
If the
permissi
ons were
granted
mistaken
ly or
maliciou
sly, you
should
revoke
access of
the user
and
any
changes
made by
an
adversar
y to your
cluster.
For more

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



[AWS](#) > [Documentation](#) > [Amazon GuardDuty](#) > [Amazon GuardDuty User Guide](#) [Feedback](#) [Preferences](#)

practices
for
Amazon
EKS in
the
Amazon
EKS User
Guide.

For more
informat
ion, see
[Remedia
ting EKS
Protecti
on
findings.](#)

Persi stenc

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

An
API
comm



Contact Us



n
persis
tent
access
to a
Kuber
netes
cluste
r was
invok
ed
from
a Tor
exit
node
IP
addre
ss.

Default

severity
:

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

- Feature
- EKS
- audit
- logs



Contact Us



an API
was
invoked
from a
Tor exit
node IP
address.
The API
observe
d is
common
ly
associate
d with
persisten
ce tactics
where an
adversar
y has
gained
access to
your

Kuberne
tes
cluster
attempti
ng to
maintain
that
access.
Tor is
software
for

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



ication.

It
encrypts
and
randoml
y
bounces
commun
ications
through
relays
between
a series
of
network
nodes.

The last
Tor node
is called
the exit
node.

This can

indicate
unautho
rized

your
AWS
resource
s with
the
intent of
hiding
the

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



[AWS](#) > [Documentation](#) > [Amazon GuardDuty](#) > [Amazon GuardDuty User Guide](#) [Feedback](#) [Preferences](#)

Remediation

Action
recommendations:

If the user reported in the finding under the KubernetesUserDetails section is system anonymous, investigate why the user was permitted to invoke the API and revoke

the user was permitted to invoke the API and revoke

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



by
followin
g the
instructi
ons in
[Security](#)
[best](#)
[practices](#)
for
[Amazon](#)
[EKS](#) in
the
Amazon
EKS User
Guide. If
the user
is an
authenti
cated
user,
investiga
te to
determin

e if the
activity
legitimat
e or
maliciou
s. If the
activity
was
maliciou
s revoke

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



any changes made by an adversar y to your cluster. For more informat ion, see [Remedia ting EKS Protecti on findings.](#)

Polic y:Ku bern etes/

ToDe fault Servi ceAc

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



The
defau
lt
servic
e
accou
nt
was
grant
ed
admin
privil
eges
on a
Kuber
netes
cluste
r.

Default

severity

: High

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

EKS

audi

t

logs

This
finding
informs



Contact Us



account
for a
namespa
ce in
your
Kuberne
tes
cluster
was
granted
admin
privilege
S.
Kuberne
tes
creates a
default
service
account
for all
the
namespa
ces in
the
cluster
automati
cally
assigns
the
default
service
account
as an

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



been
explicitly
associate
d to
another
service
account.

If the
default
service
account
has
admin
privilege
s, it may
result in
pods
being
unintenti
onally
launched
with

admin
privilege
s. If this
behavior
is not
expected
, it may
indicate
a
configur
ation
mistake

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



compro
mised.

**Remedi
ation
recomm
endatio
ns:**

You
should
not use
the
default
service
account
to grant
permissi
ons to
pods.
Instead
you
should
create a
dedicate

for each
workloa
d and
grant
permissi
on to
that

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



fix this
issue,
you
should
create
dedicate
d service
accounts
for all
your
pods and
workloa
ds and
update
the pods
and
workloa
ds to
migrate
from the
default
service
account
to their
dedicate
accounts
. Then
you
should
remove
the
admin
permissi

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



account.

For more information, see [Remediating EKS Protection findings](#).

Policy:Kubernetes/AnonymousUserAccess

Granted

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



on a
Kuber
netes
cluste
r.

**Default
severity
: High**

- **Feat
ure:**
EKS
audi
t
logs

This
finding
informs
you that
a user on
your
Kuberne

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

successf
ully
created a
Cluste
rRoleBi
nding
or



Contact Us



system

:anonym

ous to a
role.

This
enables
unauthe
nticated
access to
the API
operatio
ns
permitte
d by the
role. If
this
behavior
is not
expected
, it may
indicate
a

configur
ation

your

creden

als are

compro

mised

Remedi

ation

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



You

should
examine
the
permis
ons that
have
been
granted
to the

system

:anonym
ous user
or
system
:unauth
enticat
ed

group on
your
cluster
and

revoke
unnecess

ary
ous

access.

For more
informat

ion, see
Security

best
practices

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



*Amazon
EKS User
Guide. If
the
permissi
ons were
granted
maliciou
sly, you
should
revoke
access of
the user
that
granted
the
permissi
ons and
reverse
any
changes
made by
an
adversar
y to your
cluster.
For more
information, see
Remediat
ing EKS
Protecti
on
findings.*

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

*For more
information, see
Remediat
ing EKS
Protecti
on
findings.*



Contact Us



[AWS](#) > [Documentation](#) > [Amazon GuardDuty](#) > [Amazon GuardDuty User Guide](#) [Feedback](#) [Preferences](#)

ber
etes/
Expo
sedD
ashb
oard

The
dashb
oard
for a
Kuber
netes
cluste
r was
expos
ed to
the
intern
et

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

Medium

- Feature: EKS audit



Contact Us



[AWS](#) > [Documentation](#) > [Amazon GuardDuty](#) > [Amazon GuardDuty User Guide](#) [Feedback](#) [Preferences](#)

finding
informs
you that
Kuberne
tes
dashboa
rd for
your
cluster
was
exposed
to the
internet
by a
Load
Balancer
service.
An
exposed
dashboa
rd makes
the
management
interface
accessible
from
the
internet
and
allows
adversari

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



cation
and
access
control
gaps
that may
be
present.

**Remedi
ation
recomm
endatio
ns:**

You
should
ensure
that
strong
authenti
cation
and
authoriz
ation is

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

Kuberne
tes
Dashboa
rd. You
should
also
impleme



Contact Us



to
restrict
access to
the
dashboa
rd from
specific
IP
addresse
s.

For more
informat
ion, see
[Remedia
ting EKS
Protecti
on
findings.](#)

Polic

y:Ku
ber
n
et
w
or
k
s
Kube
flow
Dash
boar
dExp
os

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



[AWS](#) > [Documentation](#) > [Amazon GuardDuty](#) > [Amazon GuardDuty User Guide](#) [Feedback](#) [Preferences](#)

oard
for a
Kuber
netes
cluste
r was
expos
ed to
the
Intern
et

Default
severity
:
Medium

- **Feat**
ure:
EKS
audi

t
logs

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

finding
informs
you that
Kubeflo
w
dashboa
rd for
your



Contact Us



Internet

by a

Load

Balancer

service.

An

exposed

Kubeflo

w

dashboa

rd makes

the

manage

ment

interface

of your

Kubeflo

w

environ

ment

accessibl

e from

the

Internet

and

adversari

es to

exploit

any

authenti

cation

and

access

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

allow us to

exploit

any

authenti

cation

and

access



Contact Us



present.

**Remedi
ation
recomm
endatio
ns:**

You
should
ensure
that
strong
authenti
cation
and
authoriz
ation is
enforced
on

Kubeflo

w
Dashboa
rd. You
should

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

nt
network
access
control
to
restrict
access to



Contact Us



IP
addresse
S.

For more
informat
ion, see
[Remedia
ting EKS
Protecti
on
findings.](#)

Privi
lege
Escal
ation
:Kub
erne

tes/
Privi

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

dCon
taine
r

A
privil



Contact Us



**root
level
access
was
launc
hed
on
your
Kuber
netes
cluste
r.**

**Default
severity
:
Medium**

- **Feat
ure:
EKS**

**audi
t**

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

**This
finding
informs
you that
a
privileg
e
containe**



Contact Us



tes
cluster
using an
image
has
never
before
been
used to
launch
privilege
d
containe
rs in
your
cluster.
A
privilege
d
containe
r has
root
level
access to
the host

ies can
launch
privilege
d
containe
rs as a
privilege
escalatio

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



compro
mise the
host.

**Remedi
ation
recomm
endatio
ns:**

If this
containe
r launch
is
unexpect
ed, the
credenti
als of
the user
identity
used to
launch
the

containe
r may be

Revoke
access of
the user
and
reverse
any
changes

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



cluster.

For more information, see [Remediating EKS Protection findings](#).

Credential Access:Kubernetes/Anonymous/malicious

USB behavior

having

crests

Accessed

As

Kuber

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



used
to
access
secret
S was
invok
ed in
an
anom
alous
way.

Default
severity
:
Medium

- **Feat**
ure:
EKS
audi

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

finding
informs
you that
an
anomalo
us API
operatio
n to



Contact Us



was
invoked
by a
Kuberne
tes user
in your
cluster.

The
observe
d API is
common
ly
associate
d with
credenti
al access
tactics
that can
lead to
privilege
d
escalatio

n and
further

access
within
your
cluster.
If this
behavior
is not
expected
, it may
indicate

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



or that
your
AWS
credenti
als are
compro
mised.

The
observe
d API
was
identifie
d as
anomalo
us by the
GuardDu
ty
anomaly
detectio
n
machine
learning
(ML)
model.

evaluate
s all user
API
activity
within
your EKS
cluster

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



us
events
that are
associate
d with
techniqu
es used
by
unautho
rized
users.
The ML
model
tracks
multiple
factors
of the
API
operatio
n such as
the user
making
the
request,
the
request
was
made
from,
user
agent
used,

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



operated
. You can
find the
details
of the
API
request
that are
unusual,
in the
finding
details
panel in
the
GuardDu
ty
console.

**Remedi
ation
recomm
endatio**

ns.

Examine

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

ons
granted
to the
Kuberne
tes user
in your
cluster



Contact Us



permissions are needed. If the permissions were granted mistakenly or maliciously, revoke user access and reverse any changes made by an unauthorized user to your cluster.

user to your cluster. For more information, see [Remediating EKS Protection findings](#).

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



compro
mised,
see
Remedia
ting
potential
ly
compro
mised
AWS
creden
tials.

Prive lege Escal ation :Kub erne

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



A

RoleB
inding

or

Clust
erRol
eBindi

ng to
an

overl

y
permi
ssive

role

or

sensit
ive
name
space

was

create
d or

ted in
your
Kuber
netes
cluste
r.

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



*
 Note

This finding is defined in the following sections:

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



u
m
.H
o
w
e
v
e
r,
i
f
a
R
o
l
e
B
i
n
d

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



B
i
n
d
i
n
g
i
n
v
o
l
v
e
s
t
h
e
C
l
u
s

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



1
u
s
t
e
r
-
a
d
m
i
n
,,
t
h
e
s
e
v
e
r
::

t
y
s
H
i
g
h
..

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



t
logs

This
finding
informs
you that
a user in
your
Kuberne
tes
cluster
created a
RoleBi
nding
or
Cluste
rRoleBi
nding
to bind a
user to a
role with

admin
permissi
ons or
namespa
ces. If
this
behavior
is not
expected
, it may
indicate

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



or that
your
AWS
credenti
als are
compro
mised.

The
observe
d API
was
identifie
d as
anomalo
us by the
GuardDu
ty
anomaly
detectio
n
machine
learning
(ML)
model.

evaluate
s all user
API
activity
within
your EKS
cluster.

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



S
anomalo
us
events
that are
associate
d with
the
techniqu
es used
by an
unautho
rized
user. The
ML
model
also
tracks
multiple
factors
of the
API
operatio
n, such
as the
making
the
request,
the
location
the
request
was

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



used,
and the
namespa
ce that
the user
operated
. You can
find the
details
of the
API
request
that are
unusual,
in the
finding
details
panel in
the
GuardDu
ty
console.

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

Remedi
ation

Examine
the
permis
ons
granted

Examine
the
permis
ons
granted



Contact Us



permissions are defined in the role and subjects involved in

RoleBinding and ClusterRoleBinding.

If the permissions were granted mistakenly or maliciously,

revoke user

reverse any changes made by an unauthorized

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



information, see [Remediating EKS Protection findings](#).

If your AWS credentials are compromised, see [Remediating potential AWS Identity](#) credentials.

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

[Execution:Kubernetes/Annotations](#)



Contact Us



or.Ex ecln Pod

A
comm
and
was
execu
ted
inside
a pod
in an
anom
alous
way.

Default
severity
:

Medium

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

Feature
Logs
EKS
audit
logs

This
finding
informs



Contact Us



executed
in a pod
using
the
Kuberne
tes exec
API. The
Kuberne
tes exec
API
allows
running
arbitrary
commans
ds in a
pod. If
this
behavior
is not
expected
for the
user,
namespa
ce, or
pod it
indicate
either a
configur
ation
mistake
or that
your
AWS

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



The
observe
d API
was
identify
d as
anomalo
us by the
GuardDu
ty
anomaly
detectio
n
machine
learning
(ML)
model.
The ML
model
evaluate
s all user
API
activity
within

This ML
model
also
identify
s
anomalo
us

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



the
techniqu
es used
by an
unautho
rized
user. The
ML
model
also
tracks
multiple
factors
of the
API
operatio
n, such
as the
user
making
the
request,

the
location
the
was
made
from,
the user
agent
used,
and the
namespa

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



find the details of the API request that are unusual, in the finding details panel in the GuardDuty console.

Remediation recommendations:

If the execution of this

unexpected, the credentials of the user identity used to

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



have
been
compro
mised.
Revoke
user
access
and
reverse
any
changes
made by
an
unautho
rized
user to
your
cluster.
For more
informat
ion, see
[Remedia](#)

ting EKS
Protecti
on

If your
AWS
creden
tials are
compro
mised,
see

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



[AWS](#) > [Documentation](#) > [Amazon GuardDuty](#) > [Amazon GuardDuty User Guide](#) [Feedback](#) [Preferences](#)

compro

mised

AWS

credenti

als.

Prive lege Escal ation :Kub erne tes/A nom alou sBeh avior

.vor
kloa
tive
d!Pri
vileg
edCo
ntain
er

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



launched with a privileged container in an anomalous way.

Default severity : High

- Feature: EKS audit logs

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

This informs you that a workload was launched with a privilege



Contact Us



EKS
cluster.
A
privilege
d
containe
r has
root
level
access to
the host.
Unautho
rized
users
can
launch
privilege
d
containe
rs as a
privilege
escalatio
n tactic
to first
gain
the host
and then
compro
mise it.

The
observe
d

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



modification was identified as anomalous by the GuardDuty anomaly detection model. The ML model evaluates all user API and container images activity within your EKS cluster. This ML model also identifies suspicious anomalous events.

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

This ML model also identifies suspicious anomalous events.



Contact Us



technique used by an unauthorized user. The ML model also tracks multiple factors of the API operation, such as the user making the request, the location of the request made from the user agent used, container images observed

location of the request made from the user agent used, container images observed

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



ce that
the user
operated
. You can
find the
details
of the
API
request
that are
unusual,
in the
finding
details
panel in
the
GuardDu
ty
console.

Remedi ation

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

containe
r launch
is
unexpect
ed, the
credenti
als of



Contact Us



the
contain
r may
have
been
compro
mised.
Revoke
user
access
and
reverse
any
changes
made by
an
unautho
rized
user to
your
cluster.

For more

informat
ion, see

[Remedia](#)

[Protect](#)

on

findings.

If your
AWS
credenti
als are

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

[Protect](#)

on

findings.

If your
AWS
credenti
als are



Contact Us



ting
potential
ly
compro
mised
AWS
credenti
als.

If this
containe
r launch
is
expected
, it is
recomm
ended
that you
use a
suppress
ion rule
with a
filter
criteria
based on

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

Resource
ce.Kube
nnetesD
etails.
Kuberne
tesWork
loadDet
ails.co



Contact Us



the filter criteria, the imageP refix field must have the same value as the imageP refix field specified in the finding. For more information, see [Suppression rules](#)

In GuardDu

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

Persi
stenc
e:Ku
berne
ttes/



Contact Us



havi
or.W
orklo
adDe
ploy
ed!C
ontai
ner
With
Sens
itive
Mou
nt

A
workl
oad

was
deplo
ved in
anom
alous
way,
with a
sensit
ive
host

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



the
workl
oad.

**Default
severity
: High**

- **Feat
ure:
EKS
audi
t
logs**

This
finding
informs
you that
a
workloa
d was

launched
with a
containe
included
a
sensitive
host
path in
the
volume
Mounts

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



the
sensitive
host
path
accessibl
e and
writable
from
inside
the
containe
r. This
techniqu
e is
common
ly used
by
unautho
rized
users to
gain
access to
the
host's
file

The
observe
d
containe
r
creation
or

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



anomalo
us by the
GuardDu
ty
anomaly
detectio
n
machine
learning
(ML)
model.
The ML
model
evaluate
s all user
API and
containe
r image
activity
within
your EKS
cluster.

This ML
model
also
gatherin
g
anomalo
us
events
that are
associate
d with
the

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



rized
user. The
ML
model
also
tracks
multiple
factors
of the
API
operatio
n, such
as the
user
making
the
request,
the
location
the
request
was
made
from,

the user
used,
contain
r images
observe
d in your
account,
and the
namespa

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



find the details of the API request that are unusual, in the finding details panel in the GuardDuty console.

Remediation recommendations:

If this container launch

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

ed, the credentials of the user identity used to launch



Contact Us



been
compro
mised.
Revoke
user
access
and
reverse
any
changes
made by
an
unautho
rized
user to
your
cluster.
For more
informat
ion, see
[Remedia
ting EKS](#)

Protecti
on
findings
if your
AWS
creden
tials are
compro
mised,
see
[Remedia](#)

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



mised
AWS
creden
als.

If this
containe
r launch
is
expected
, it is
recomm
ended
that you
use a
suppress
ion rule
with a
filter
criteria
based on
the

Resource
ce.Kube
ernetesD
EKS
Kuberne
tesWork
loadDet
ails.co
ntainer
s.image
Prefix
field. In

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



refix
field
must
have the
same
value as
the
imageP
refix
field
specified
in the
finding.
For more
informat
ion, see
[Suppress
ion rules](#)
in
GuardDu
ty.

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



adDe
ploy
ed

A
workl
oad
was
launc
hed in
an
anom
alous
way.

Default
severity
: Low*

Note

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



i
t
y
i
s
L
o
w
.H
o
w
e
v
e
r
,i
f
t
h
e

w
o
r
o
a
d
c
o
n
t

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



a
p
o
t
e
n
t
i
a
l
l
y
s
u
s
p
i
c
i
o
u
s

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



a
k
n
o
w
n
p
e
n
t
e
s
t
t
o
o
l
,o
r
a
c

o
n
t
i
n
e
r
r
u
n

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



p
o
t
e
n
t
i
a
l
l
y
s
u
s
p
i
c
i
o
u
s
c

o
m
n
d
a
t
l
a
u
n

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



u
c
h
a
s
r
e
v
e
r
s
e
s
h
e
l
l
c
o
m
m
a
n
d
S
t
h
e
n
t
h
e
s

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



i
t
y
o
f
t
h
i
s
f
i
n
d
i
n
g
t
y
p
e
w
i

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



M
e
d
i
u
m
. .

- Feature: EKS audit logs

This finding informs you that a Kuberne tes workloa d was created

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

modified in an anomalo us way, such as an API activity, new



Contact Us



d
configur
ation,
within
your
Amazon
EKS
cluster.
Unautho
rized
users
can
launch
containe
rs as a
tactic to
execute
arbitrary
code to
first gain
access to
the host
and then
compro
mise it.

The
observe
d
containe
r
creation
or
modifica

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



us by the
GuardDu
ty
anomaly
detectio
n
machine
learning
(ML)
model.
The ML
model
evaluate
s all user
API and
containe
r image
activity
within
your EKS
cluster.
This ML
model
also
identifie

anomalo
us
events
that are
associate
d with
the
techniqu

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

anomalo
us
events
that are
associate
d with
the
techniqu



Contact Us



user. The
ML
model
also
tracks
multiple
factors
of the
API
operatio
n, such
as the
user
making
the
request,
the
location
the
request
was
made

from,
the user
agent
contain
r images
observe
d in your
account,
and the
namespa
ce that

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



details
of the
API
request
that are
unusual,
in the
finding
details
panel in
the
GuardDu
ty
console.

**Remedi
ation
recomm
endatio
ns:**

If this
containe
r launch
is

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

credenti
als of
the user
identity
used to
launch
the



Contact Us



compro
mised.
Revoke
user
access
and
reverse
any
changes
made by
an
unautho
rized
user to
your
cluster.
For more
informat
ion, see
[Remedia
ting EKS
Protecti](#)

on
findings.

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

AWS
creden
tials are
compro
mised,
see
[Remedia
ting](#)



Contact Us



[AWS](#) > [Documentation](#) > [Amazon GuardDuty](#) > [Amazon GuardDuty User Guide](#) [Feedback](#) [Preferences](#)

AWS
creden
als.

If this
containe
r launch
is
expected
, it is
recomm
ended
that you
use a
suppress
ion rule
with a
filter
criteria
based on
the
resour

ce.Kube
rnetesD
etails.
Ming
tesWork
loadDet
ails.co
ntainer
s.image
Prefix
field. In
the filter

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



field
must
have the
same
value as
the
imageP
refix
field
specified
in the
finding.
For more
informat
ion, see
[Suppress
ion rules](#)
in
[GuardDu
ty](#).

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

Priva
lege
:Kub
erne
tes/A
nom



Contact Us



.Role Crea ted

A
highly
permi
ssive
Role
or
Clust
erRol
e was
create
d or
modif
ied in
an
anom
alous
way.

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

severity
: Low

- Feature: EKS audit



Contact Us



finding
informs
you that
an
anomalo
us API
operatio
n to
create a
Role or
Cluste
rRole
with
excessiv
e
permissi
ons was
called by
a
Kuberne
tes user
in your

Amazon
EKS
cluster.
can use
role
creation
with
powerful
permissi
ons to
avoid

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



and
avoid
detectio
n. The
excessiv
e
permissi
ons can
lead to
privilege
d
escalatio
n,
remote
code
executio
n, and
potential
ly
control
over a
namespa
ce or
cluster.
If this
behavior
is not
expected
, it may
indicate
either a
configur
ation
mistake

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



compro

mised.

The

observe

d API

was

identifie

d as

anomalo

us by the

GuardDu

ty

anomaly

detectio

n

machine

learning

(ML)

model.

The ML

model

evaluate

s all user

API

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

within

your

Amazon

EKS

cluster

and

identifie

s



Contact Us



associate
d with
the
techniqu
es used
by
unautho
rized
users.

The ML
model
also
tracks
multiple
factors
of the
API
operatio
n, such
as the
user
making

the
request,
the
information
the
request
was
made
from,
the user
agent
used,

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



account,
and the
namespa
ce that
the user
operated
. You can
find the
details
of the
API
request
that are
unusual,
in the
finding
details
panel in
the
GuardDu
ty
console.

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

Remedi
ation

Examine
the
permis
sions:
ns:

Examine
the
permis
sions
defined



Contact Us



to
ensure
that all
the
permis
ons are
needed
and
follow
least
privilege
principle
s. If the
permis
ons were
granted
mistaken
ly or
maliciou
sly,
revoke
user
access
and

changes
made by
an
unautho
rized
user to
your
cluster.

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

changes
made by
an
unautho
rized
user to
your
cluster.



Contact Us



[AWS](#) > [Documentation](#) > [Amazon GuardDuty](#) > [Amazon GuardDuty User Guide](#) [Feedback](#) [Preferences](#)

ting EKS
Protecti
on
findings.

If your
AWS
creden
tials are
compro
mised,
see
Remedia
ting
potential
ly
compro
mised
AWS
creden
tials.

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

Disc
y-Ku
ber
etes/
Ano
malo
usBe



Contact Us



sion Che ked

A user check ed their access permission in an anomalous way.

Default severity : Low

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

• Feature
ture:
Edu
audi
t
logs

This
finding
informs
you that



Contact Us



cluster
successf
ully
checked
whether
or not
the
known
powerful
permissi
ons that
can lead
to
privilege
d
escalatio
n and
remote
code
executio
n, are
allowed.

For
example,
a
common
d used
to check
permissi
ons for a
user is
kubect
l auth

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



expected
, it may
indicate
either a
configur
ation
mistake
or that
your
creden
tials have
been
compro
mised.

The
observe
d API
was
identifie
d as
anomalo
us by the
GuardDu

ty
n
machine
learning
(ML)
model.
The ML
model

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



within
your
Amazon
EKS
cluster
and
identifie
s
anomalo
us
events
that are
associate
d with
the
techniqu
es used
by
unautho
rized
users.

The ML

model

also

tracks

factors

of the

API

operatio

n, such

as the

user

making

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



the request was made from, permissi on being checked, and the namespa ce that the user operated . You can find the details of the API request that are unusual, in the

finding details panel in

GuardDu

ty

console.

Remedi

ation

recomm

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



[AWS](#) > [Documentation](#) > [Amazon GuardDuty](#) > [Amazon GuardDuty User Guide](#) [Feedback](#) [Preferences](#)

the
permissi
ons
granted
to the
Kuberne
tes user
to
ensure
that all
the
permissi
ons are
needed.
If the
permissi
ons were
granted
mistaken
ly or
maliciou
sly,
revoke
user
access

any
changes
made by
an
unautho
rized
user to

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies



Contact Us



ion, see
Remedia
ting EKS
Protecti
on
findings.

If your
AWS
creden
tials are
compro
mised,
see
Remedia
ting
potential
ly
compro
mised
AWS
creden
tials

↓

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

Do you want us to remember your preferences? This will help us to provide you with a better service in the future.

Yes

No



Contact Us



Next

topic: [Runtime](#)
[Monitoring](#)
[finding](#)
[types](#)

Previous

topic: [S3](#)
[Protection](#)
[finding](#)
[types](#)

Need

help?

- [Try](#)
[AWS](#)
[re:Post](#)
- [Connect](#)
[with](#)
[an](#)
[AWS](#)
[IQ](#)

[expert](#)

Select your cookie preferences

We use essential cookies and similar tools that are necessary to provide our site and services. We use performance cookies to collect anonymous statistics so we can understand how customers use our site and make improvements. Essential cookies

[Terms](#) | [Cookie](#)

[preferences](#) |

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.