Re: Your Amazon EC2 Abuse Report [10452973108] [AWS ID 406909412436]

Lan Yang

Sun 6/16/2019 7:44 PM

To:Amazon EC2 Abuse <ec2-abuse@amazon.com>;

Cc:Lan Yang <lyang@cpp.edu>;

We resolved the issue by changing the inbound security group rules to allow all inbound traffic but only from source originating from our instances (identified by their IP address) and our local computer. Now when we ran a Hadoop job and we no longer saw YARN jobs being submitted from any unknown sources. Thank you!

Sincerely,

Lan Yang

From: Amazon EC2 Abuse <ec2-abuse@amazon.com>
Sent: Sunday, June 16, 2019 4:05 AM
To: Lan Yang
Subject: Re: Your Amazon EC2 Abuse Report [10452973108] [AWS ID 406909412436]

Hello,

Thank you for your response. Our records show that you left the Hadoop Cluster Master security group open to the public. This cause the cluster to be contro

AWS recommends that you keep the Hadoop Cluster security group secured on all Hadoop clusters. If there is a reason to update this security group, your re

You are responsible for the security of your instances. Please update us once you have finished your investigation and taken necessary steps.

Regards,
AWS Abuse Team

At Sun, 2019 Jun 16, 03:10 AM +0200, lyang@cpp.edu wrote:

We installed Hadoop on EC2 and were trying to test one of the java mapreduce examples on hadoop streaming.

When checking the running jobs on hadoop via the url provided when submitting the job we noticed that someone a "dr.who" (default name for unknown user

Our security group rules/setting like in tutorial (as shown in the picture attached). Right now we have stopped all the instances and will try to re-configure the

Sincerely,

Lan Yang

____
From: Amazon EC2 Abuse <ec2-abuse@amazon.com>
Sent: Saturday, June 15, 2019 1:14:37 PM
To: Lan Yang
Subject: Your Amazon EC2 Abuse Report [10452973108] [AWS ID 406909412436]

[Amazon Web Services] <https://www.amazon.com/gp/f.html?
C=2SPW7SC9W35FL&M=urn:rtn:msg:201906152014371b8f045479b44f53ba482d125ad0p0na&R=1UMZ4N8BP15RY&T=C&U=http%3A%2F%2Fwww.ama
Hello,

We've received a report(s) that your AWS resource(s)

AWS ID: 406909412436 Region: us-west-1 EC2 Instance Id: i-0c6bb362b8a1dd53d [13.56.197.195]

has been implicated in activity that resembles a Denial of Service attack against remote hosts; please review the information provided below about the activit

Please take action to stop the reported activity and reply directly to this email with details of the corrective actions you have taken. If you do not consider the a

If you're unaware of this activity, it's possible that your environment has been compromised by an external attacker, or a vulnerability is allowing your machine

We are unable to assist you with troubleshooting or technical inquiries. However, for guidance on securing your instance, we recommend reviewing the follov

* Amazon EC2 Security Groups User Guide:
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html (Linux)
https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/using-network-security.html (Windows)

* Tips for Securing EC2 Instances:
https://aws.amazon.com/articles/1233 (Linux)
https://aws.amazon.com/articles/1767 (Windows)

* AWS Security Best Practices:
https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf

If you require further assistance with this matter, you can take advantage of our developer forums:

https://forums.aws.amazon.com/index.jspa

Or, if you are subscribed to a Premium Support package, you may reach out for one-on-one assistance here:

https://console.aws.amazon.com/support/home#/case/create?issueType=technical

Please remember that you are responsible for ensuring that your instances and all applications are properly secured. If you require any further information to

Regards,
AWS Abuse

Abuse Case Number: 10452973108-1

---Beginning of forwarded report(s)---

* Log Extract:
<<<
Please investigate your instance(s) and reply detailing the corrective measures you have taken to address this activity. To assist you, we have taken the follo
Region: us-west-1
Instances:
Instance Id Remote IP Port Protocol Action Taken
i-0c6bb362b8a1dd53d 134.255.251.56 80 17 Outgoing Port 80 Blocked

Details of the abusive activity:

Instance Id: i-0c6bb362b8a1dd53d
Report begin time: 2019-06-15 20:05:14 UTC
Report end time: 2019-06-15 20:06:14 UTC

Protocol: UDP
Remote IP: 134.255.251.56
Remote port(s): 80

Total bytes sent: 402581340
Total packets sent: 745521
Total bytes received: 0
Total packets received: 0

>>>

* Comments:
<<<

>>>

____
How can I contact a member of the Amazon EC2 abuse team?
Send an e-mail to ec2-abuse@amazon.com<mailto:ec2-abuse@amazon.com>; remember to include your case number.

Amazon Web Services<https://www.amazon.com/gp/f.html?
C=2SPW7SC9W35FL&M=urn:rtn:msg:201906152014371b8f045479b44f53ba482d125ad0p0na&R=2PRJXJQ0QNU1W&T=C&U=http%3A%2F%2Fwww.am

Amazon Web Services LLC is a subsidiary of Amazon.com, Inc. Amazon.com is a registered trademark of Amazon.com, Inc. This message produced and dis

--------------- Plus (1) Attachments---------------

How can I contact a member of the Amazon EC2 abuse team?
Send an e-mail to ec2-abuse@amazon.com; remember to include your case number.

Amazon Web Services