AWS Summit

AWS技术峰会 2015 · 上海

亚马逊 aws

AWS安全及其自动化

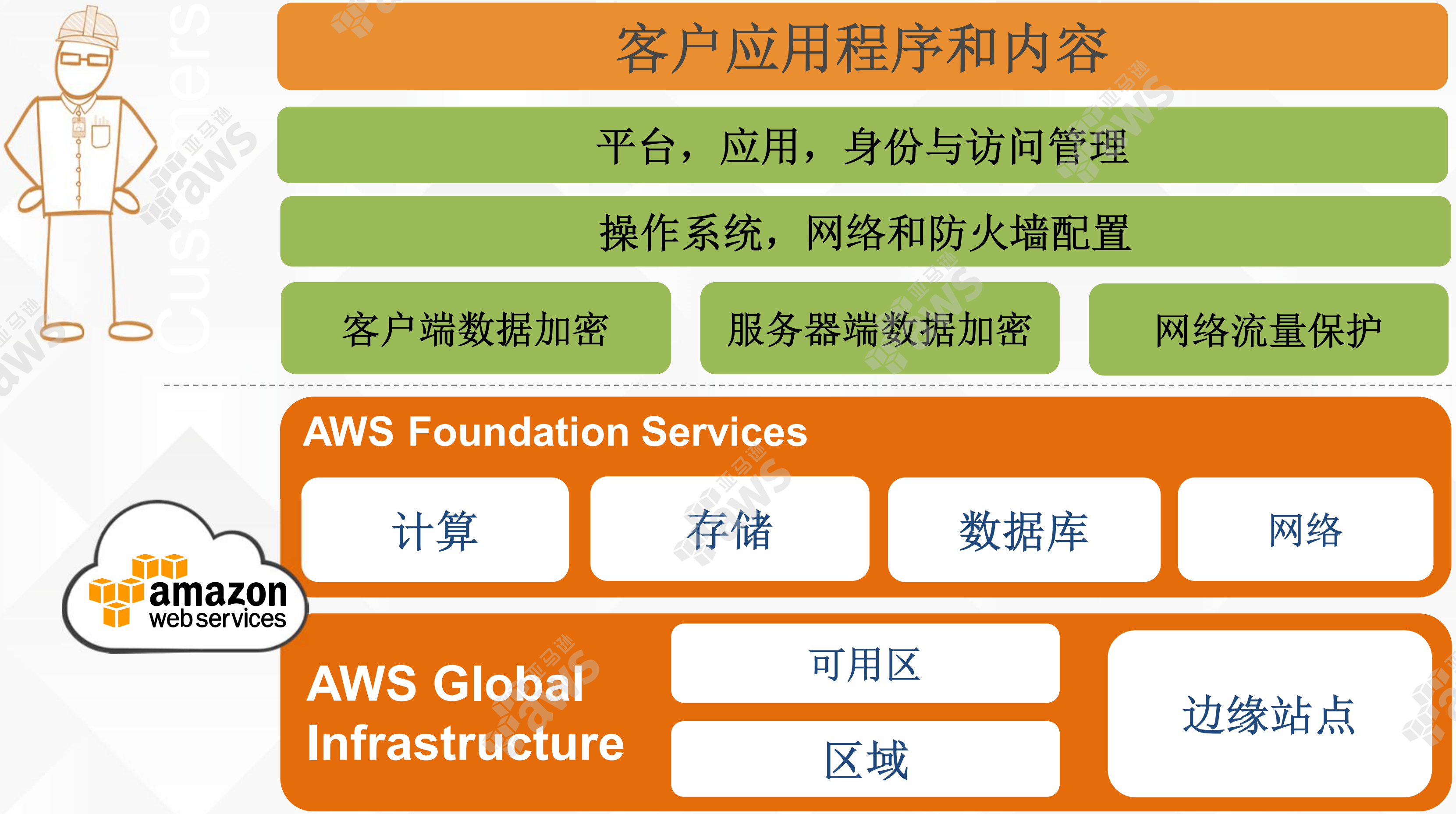
资深技术客户经理

姜振勇

议题

- AWS安全相关的服务
- 通过这些AWS服务实现高效安全运维

安全责任共担模型



客户应用程序和内容

平台，应用，身份与访问管理

操作系统，网络和防火墙配置

客户端数据加密

服务器端数据加密

网络流量保护

AWS Foundation Services

计算

存储

数据库

网络

AWS Global Infrastructure

可用区

区域

边缘站点

AWS提供的安全服务

审计

- 合规报告

监控

- Amazon CloudWatch
- AWS CloudTrail
- AWS Config
- “Describe” APIs

控制

- IAM 认证及访问控制
- AWS CloudHSM
- AWS CloudFormation
- AWS KMS
- Amazon Inspector
- AWS WAF

AICPA SOC
ISAE 3402 TYPE 2
SOC3
HIPAA
ISO 27001 Certified
PCI DSS
FIPS 140-2 CRYPTOGRAPHY
ITAR
FedRAMP
ISO 9001
MOTION PICTURE ASSOCIATION OF AMERICA, INC.

AWS提供的安全服务

审计

- 合规报告

监控

- Amazon CloudWatch
- AWS CloudTrail
- AWS Config
- “Describe” APIs

控制

- IAM 认证及访问控制
- AWS CloudHSM
- AWS CloudFormation
- AWS KMS
- Amazon Inspector
- AWS WAF

AICPA SOC
ISAE 3402 TYPE 2
SOC3
HIPAA
ISO 27001 Certified
PCI DSS LEVEL 1 SERVICE PROVIDER
FIPS 140-2 CRYPTOGRAPHY
ITAR
FedRAMP
ISO 9001
MOTION PICTURE ASSOCIATION OF AMERICA, INC.

相关的部分服务和工具

- 通过AWS IAM (身份和访问管理) 安全地控制用户对 AWS 服务和资源的访问权限。
- AWS Config 和 AWS Config Rules 提供了AWS 资源库存，配置历史记录和配置更改通知，以增强安全性和方便管理。
- AWS WAF（Web 应用程序防火墙） 保护您的 Web 应用程序不遭受常见 Web 漏洞的攻击
- Amazon Inspector (分析应用程序安全性) 有助于提高在 AWS 上部署的应用程序的安全性与合规性。
- Trusted Advisor会检查您的 AWS 环境并发现可以节省开支、提高系统性能和可靠性或帮助弥补安全漏洞的机会。

IAM有什么特性？

- 为您提供 AWS 账户的共享访问
- 细粒度的权限控制
- 支持对运行在EC2上的应用程序进行安全访问控制
- 多因素身份验证（MFA）
- 联合身份认证（Identity federation）
- 身份信息确认
- PCI DSS 合规性
- 与 AWS 服务集成
- 免费使用

AWS Config 的特点

- 列出AWS资源的清单，甚至是已经删除的资源
- 持续的记录配置的变化
- 在配置变化的时候能够通知管理员
- 完全托管
- 合作伙伴解决方案的生态系统

AWS Config Rules 的特点

使用规则监控资源的修改

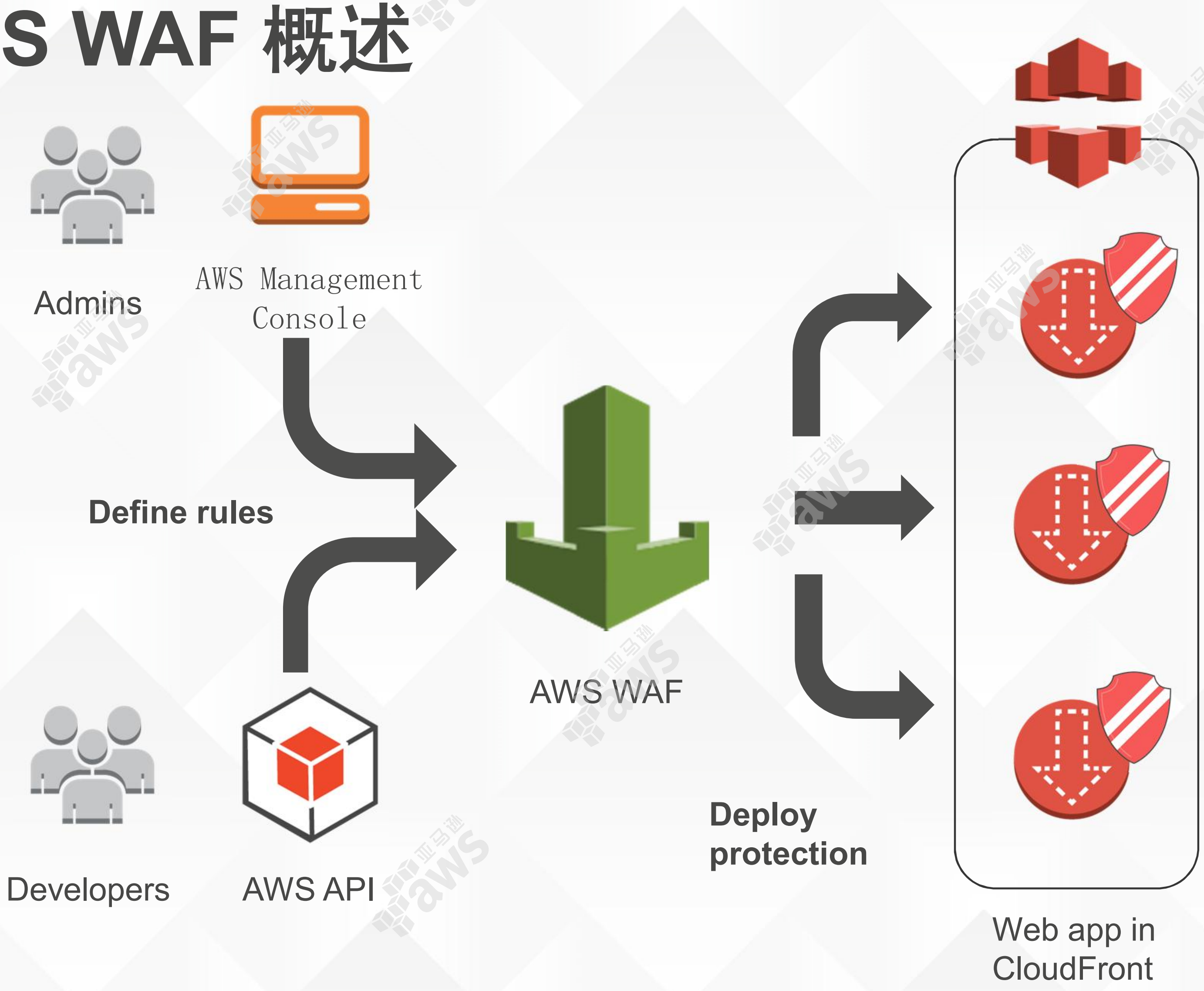
全局的合规性检查

通过可视化工具简化管理

AWS WAF的特点?

- AWS WAF 通过根据您创建的规则筛选流量，从而实现保护您的 Web 应用程序免受攻击的功能。
- 和Amazon CloudFront服务集成
- 易于部署，可以集中化定义规则
- 近乎实时地查看您的 Web 流量
- 通过 AWS WAF API 或 AWS 管理控制台进行配置，易于自动化部署

AWS WAF 概述



Admins
AWS Management Console
Define rules
Developers
AWS API
AWS WAF
Deploy protection
Web app in CloudFront

Amazon Inspector有什么功能和特性？

- 应用程序的安全评估
- 丰富的内置规则
- 安全问题汇总和建议
- 可以通过API完成自动化
- 找出您的 Web 应用程序中的安全问题
- 实施组织的安全标准
- 在不影响安全性的情况下提高灵活性
- 将 AWS 安全专业知识应用至您的应用程序
- 简化安全合规性

AWS CloudTrail 介绍

使用CloudTrail的场景

- IT和安全管理员需要执行安全分析

- IT管理员和运维工程师需要跟踪AWS资源的变化

- 运维工程师需要分析一些问题、

- IT审计可以使用Cloutrail日志来满足合规性要求
  Security at Scale: Logging in AWS White Paper

什么是Trusted Advisor?

Trusted Advisor 通过检查 AWS 环境并发现可以节省开支、提高系统性能和可靠性或帮助弥补安全漏洞的机会。

自 2013 年以来，客户已经看到了超过 260 万个最佳实践推荐项目，估计实现了 3.5 亿多美元的成本节省。

Trusted Advisor能够提供什么样的帮助？

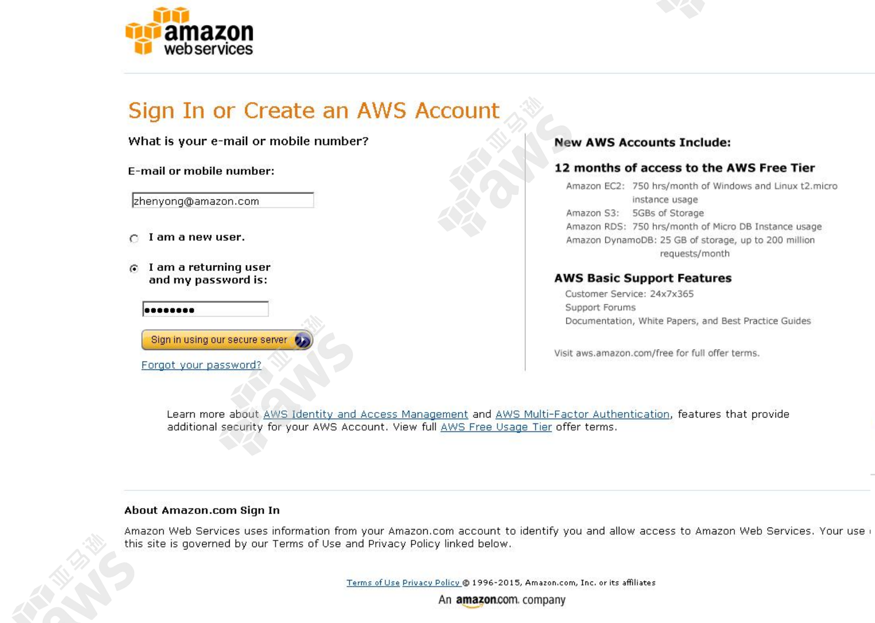
- 费用优化 Cost Optimization
- 性能优化 Performance
- 容错建议 Fault Tolerance
- 安全检查 Security

- 一旦发现新的建议，会通过邮件通知客户。

AWS企业安全及其自动化
最佳实践及其自动化Demo

IAM最佳实践

- 隐藏您的 AWS 账户（根）访问密钥
- 创建单独的 IAM 用户
- 使用组向 IAM 用户分配权限
- 授予最小权限
- 为您的用户配置强密码策略
- 为特权用户启用 MFA
- 针对在 Amazon EC2 实例上运行的应用程序使用角色
- 通过使用角色而非共享证书来委托访问
- 定期交替轮换证书
- 删除不需要的证书
- 使用策略条件来增强安全性
- 在您的 AWS 账户中保留活动历史记录



Sign In or Create an AWS Account

What is your e-mail or mobile number?

E-mail or mobile number: zhenyong@amazon.com

○ I am a new user.

● I am a returning user and my password is: ●●●●●●●●●

Forgot your password?

New AWS Accounts Include:

12 months of access to the AWS Free Tier

Amazon EC2: 750 hrs/month of Windows and Linux t2.micro instance usage

Amazon S3: 5GBs of Storage

Amazon RDS: 750 hrs/month of Micro DB Instance usage

Amazon DynamoDB: 25 GB of storage, up to 200 million requests/month

AWS Basic Support Features

Customer Service: 24x7x365

Support Forums

Documentation, White Papers, and Best Practice Guides

Visit aws.amazon.com/free for full offer terms.

Learn more about AWS Identity and Access Management and AWS Multi-Factor Authentication, features that provide additional security for your AWS Account. View full AWS Free Usage Tier offer terms.

About Amazon.com Sign In

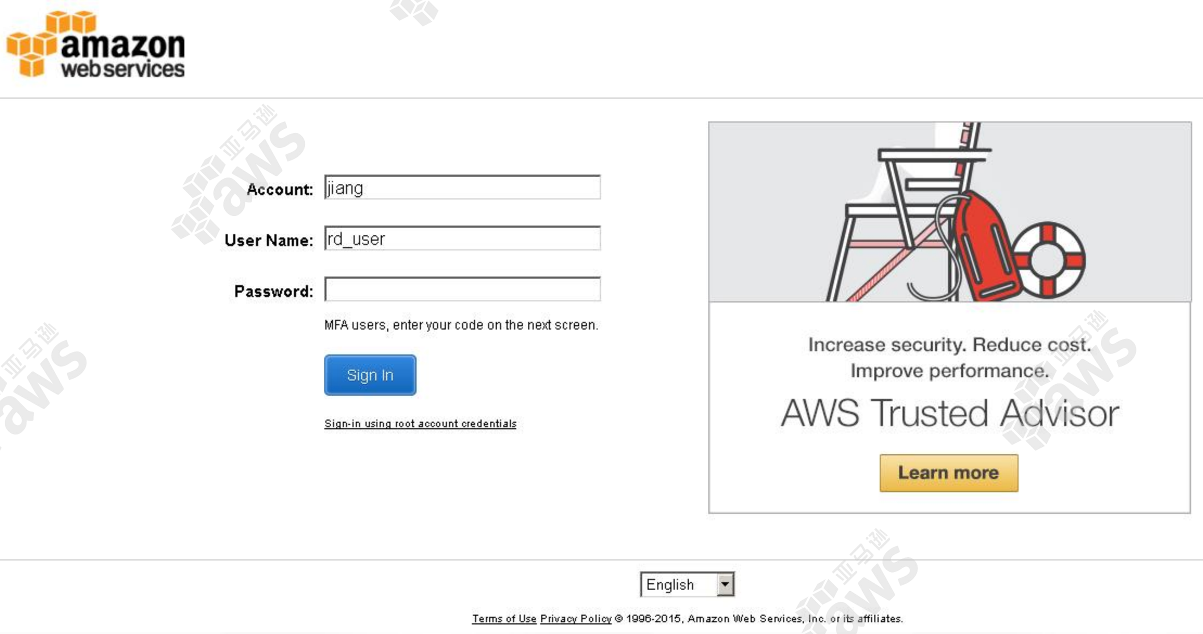
Amazon Web Services uses information from your Amazon.com account to identify you and allow access to Amazon Web Services. Your use this site is governed by our Terms of Use and Privacy Policy linked below.

Terms of Use Privacy Policy © 1996-2015, Amazon.com, Inc. or its affiliates

An amazon.com. company

使用根用户登录AWS控制台

使用IAM登录AWS控制台



Account: jiang

User Name: rd_user

Password:

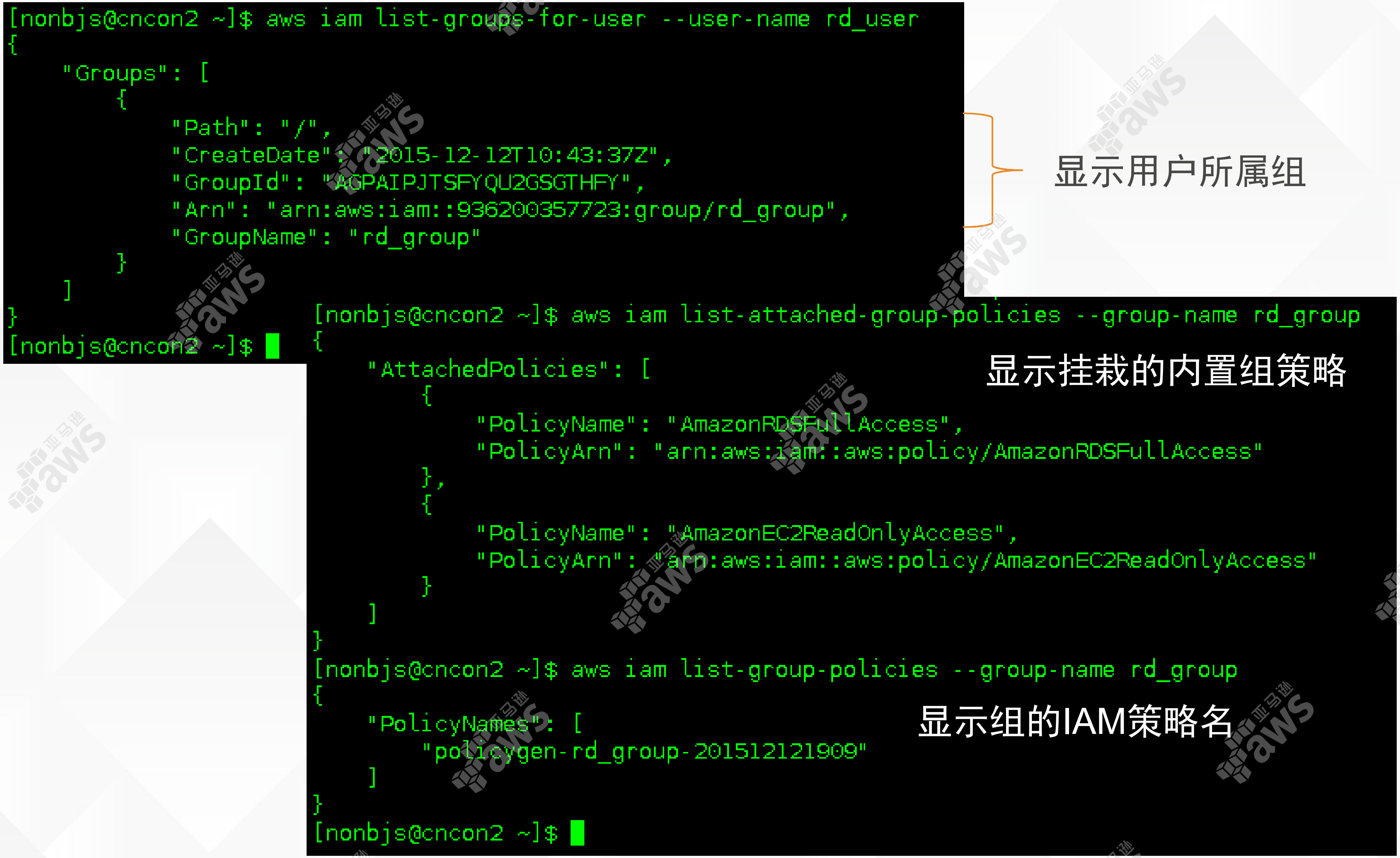
MFA users, enter your code on the next screen.

Sign-in using root account credentials

Increase security. Reduce cost. Improve performance.

AWS Trusted Advisor

Terms of Use Privacy Policy © 1996-2015, Amazon Web Services, Inc. or its affiliates.



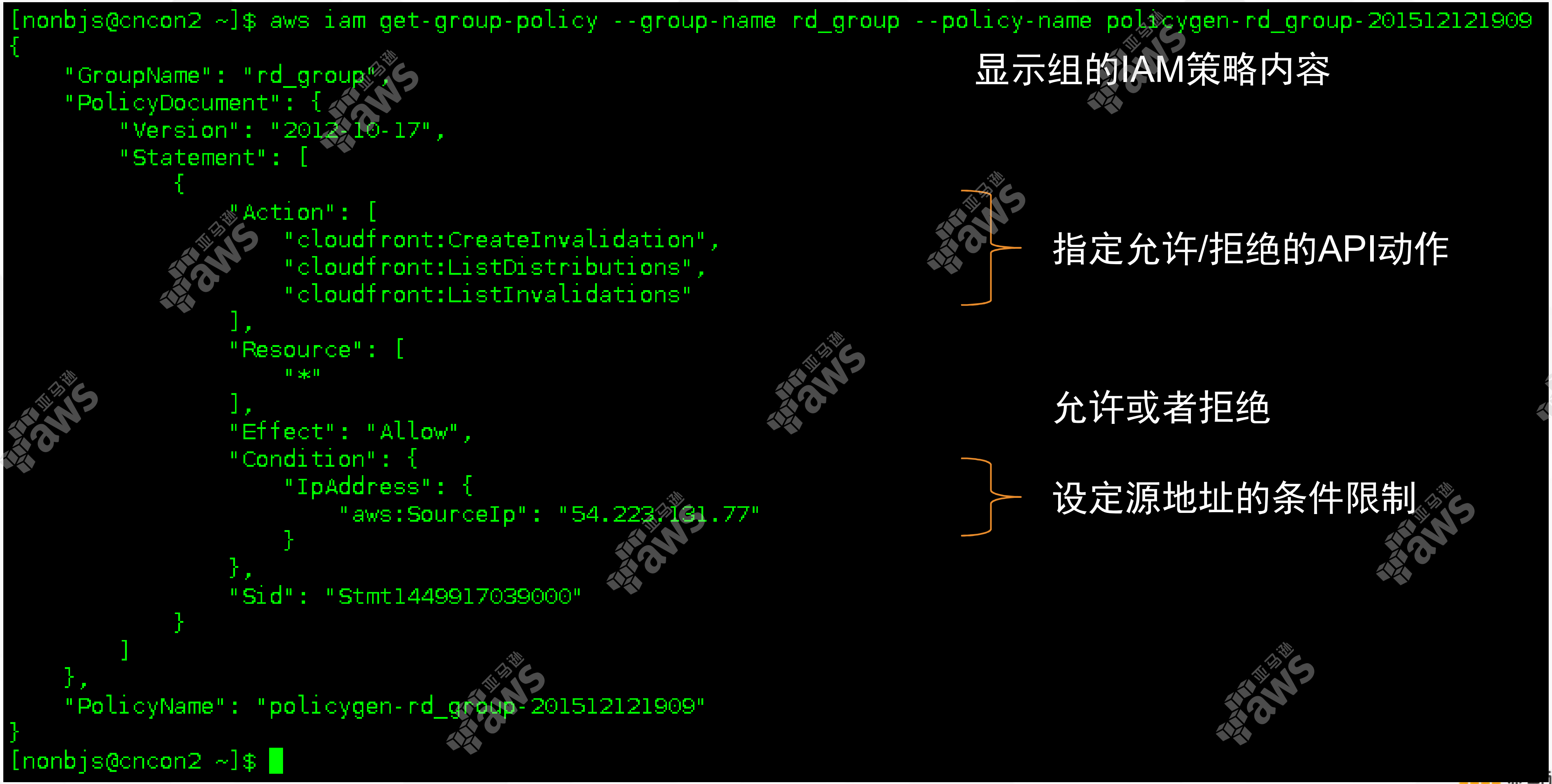
```
[nonbjs@cncon2 ~]$ aws iam list-groups-for-user --user-name rd_user
{
    "Groups": [
        {
            "Path": "/",
            "CreateDate": "2015-12-12T10:43:37Z",
            "GroupId": "AGPAIPJTSFYQU2GSGTHFY",
            "Arn": "arn:aws:iam::936200357723:group/rd_group",
            "GroupName": "rd_group"
        }
    ]
}
[nonbjs@cncon2 ~]$
```

显示用户所属组

```
[nonbjs@cncon2 ~]$ aws iam list-attached-group-policies --group-name rd_group
{
    "AttachedPolicies": [
        {
            "PolicyName": "AmazonRDSFullAccess",
            "PolicyArn": "arn:aws:iam::aws:policy/AmazonRDSFullAccess"
        },
        {
            "PolicyName": "AmazonEC2ReadOnlyAccess",
            "PolicyArn": "arn:aws:iam::aws:policy/AmazonEC2ReadOnlyAccess"
        }
    ]
}
[nonbjs@cncon2 ~]$ aws iam list-group-policies --group-name rd_group
{
    "PolicyNames": [
        "policygen-rd_group-201512121909"
    ]
}
[nonbjs@cncon2 ~]$
```

显示挂栽的内置组策略

显示组的IAM策略名



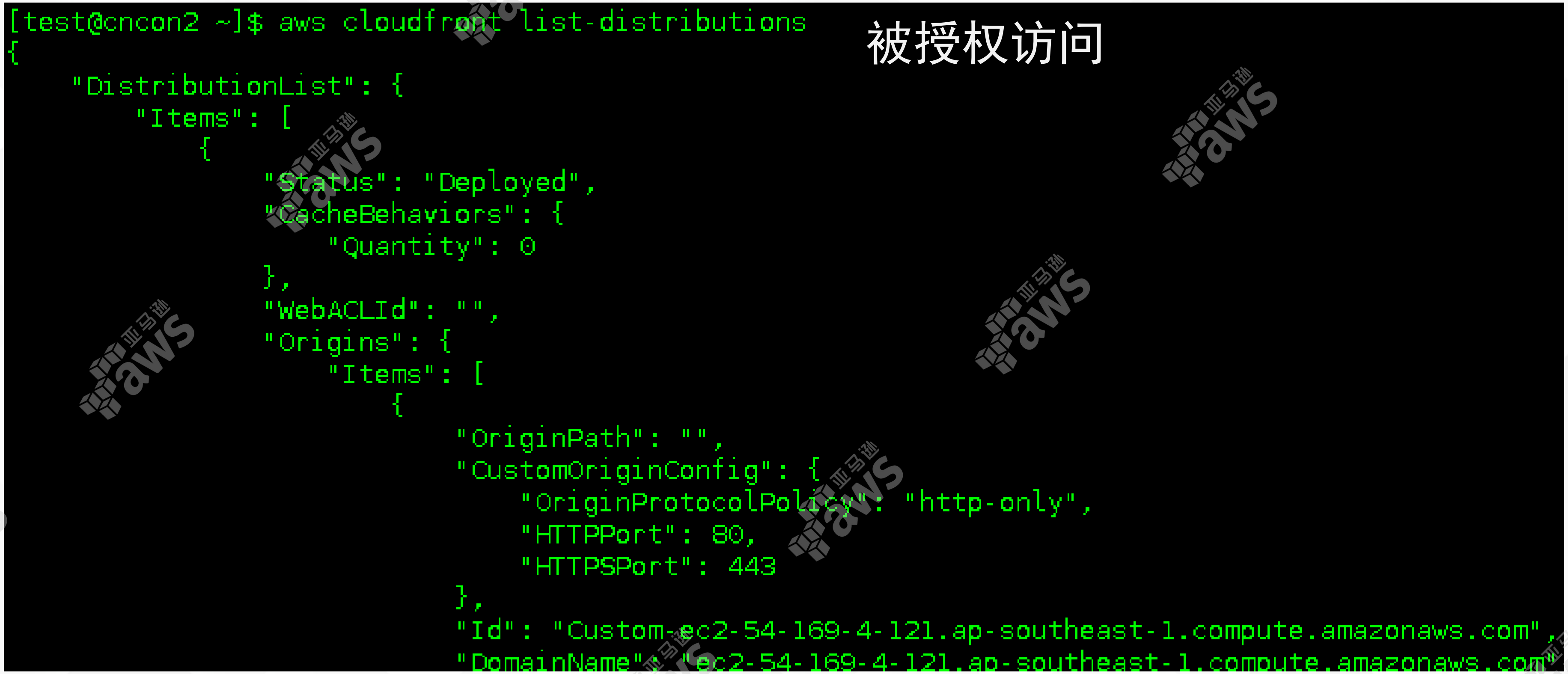
```
[nonbjs@cncon2 ~]$ aws iam get-group-policy --group-name rd_group --policy-name policygen-rd_group-201512121909
{
    "GroupName": "rd_group",
    "PolicyDocument": {
        "Version": "2012-10-17",
        "Statement": [
            {
                "Action": [
                    "cloudfront:CreateInvalidation",
                    "cloudfront:ListDistributions",
                    "cloudfront:ListInvalidations"
                ],
                "Resource": [
                    "*"
                ],
                "Effect": "Allow",
                "Condition": {
                    "IpAddress": {
                        "aws:SourceIp": "54.223.131.77"
                    }
                },
                "Sid": "Stmt1449917039000"
            }
        ]
    },
    "PolicyName": "policygen-rd_group-201512121909"
}
[nonbjs@cncon2 ~]$ █
```

显示组的IAM策略内容

指定允许/拒绝的API动作

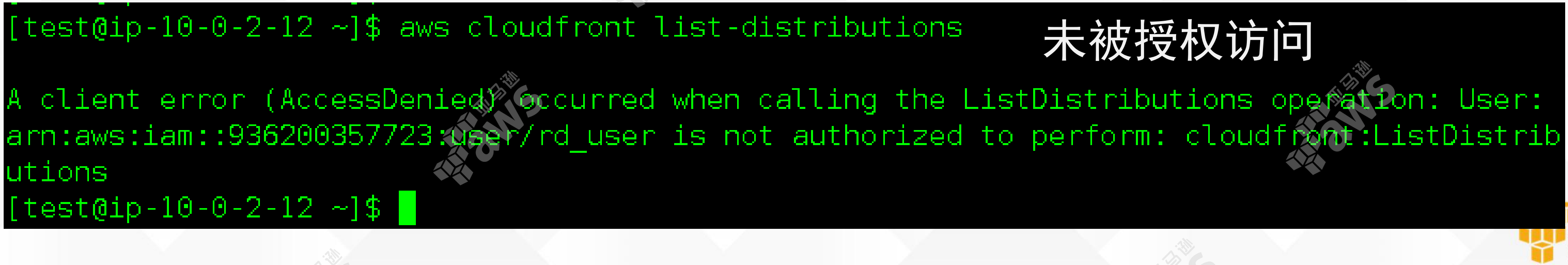
允许或者拒绝

设定源地址的条件限制



被授权访问

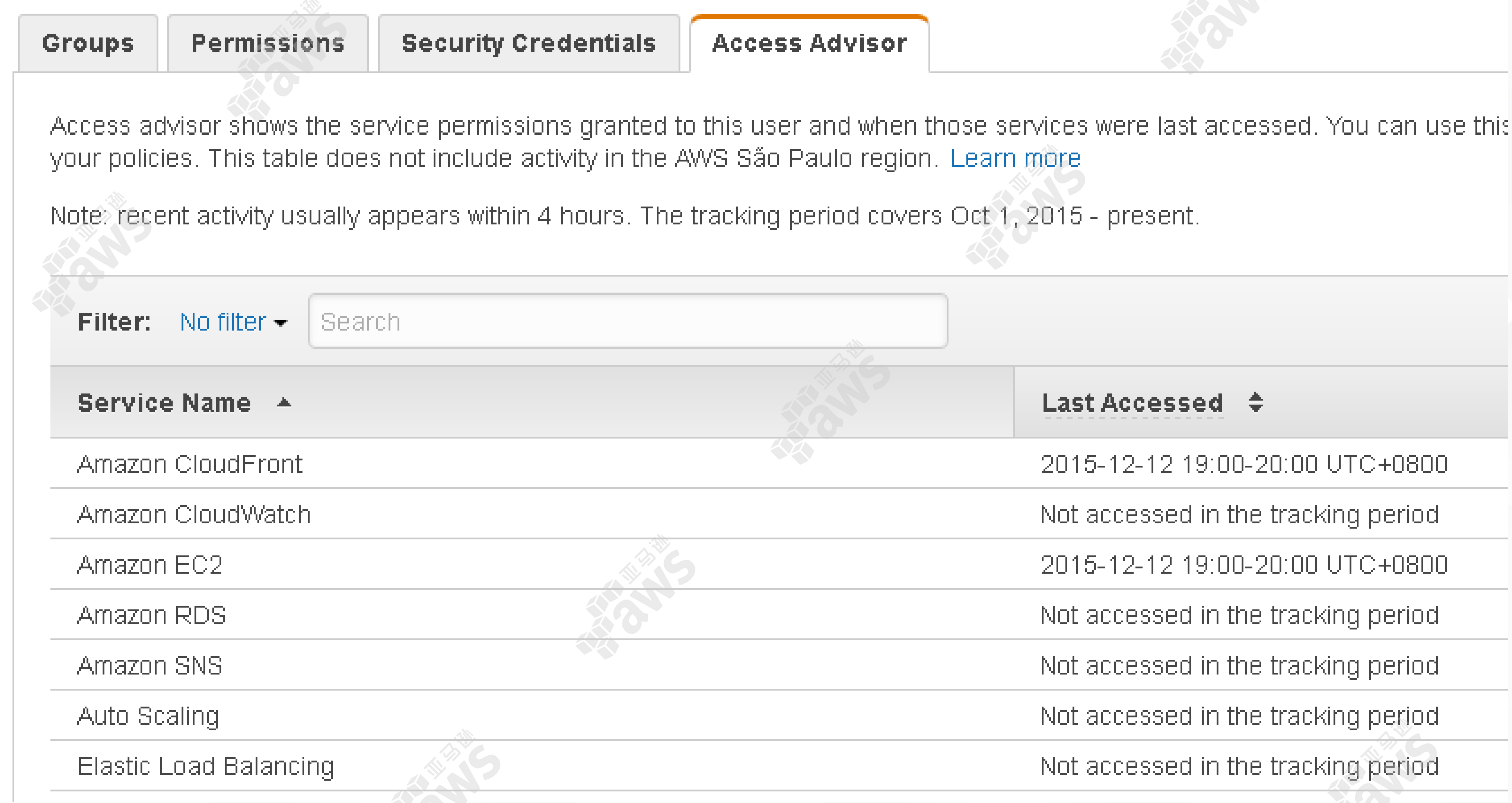
```
[test@cncon2 ~]$ aws cloudfront list-distributions
{
    "DistributionList": {
        "Items": [
            {
                "Status": "Deployed",
                "CacheBehaviors": {
                    "Quantity": 0
                },
                "WebACLId": "",
                "Origins": {
                    "Items": [
                        {
                            "OriginPath": "",
                            "CustomOriginConfig": {
                                "OriginProtocolPolicy": "http-only",
                                "HTTPPort": 80,
                                "HTTPSPort": 443
                            },
                            "Id": "Custom-ec2-54-169-4-121.ap-southeast-1.compute.amazonaws.com",
                            "DomainName": "ec2-54-169-4-121.ap-southeast-1.compute.amazonaws.com"
```



未被授权访问

```
[test@ip-10-0-2-12 ~]$ aws cloudfront list-distributions

A client error (AccessDenied) occurred when calling the ListDistributions operation: User:
arn:aws:iam::936200357723:user/rd_user is not authorized to perform: cloudfront:ListDistrib
utions
[test@ip-10-0-2-12 ~]$ 
```



Access advisor shows the service permissions granted to this user and when those services were last accessed. You can use this your policies. This table does not include activity in the AWS São Paulo region. Learn more

Note: recent activity usually appears within 4 hours. The tracking period covers Oct 1, 2015 - present.

Filter: No filter ▾ Search

Service Name ▲	Last Accessed ⇕
Amazon CloudFront	2015-12-12 19:00-20:00 UTC+0800
Amazon CloudWatch	Not accessed in the tracking period
Amazon EC2	2015-12-12 19:00-20:00 UTC+0800
Amazon RDS	Not accessed in the tracking period
Amazon SNS	Not accessed in the tracking period
Auto Scaling	Not accessed in the tracking period
Elastic Load Balancing	Not accessed in the tracking period

使用Cloudtrail记录和追踪API操作

- Who：谁（root/IAM user）执行的API动作
- When: 什么时间执行的API动作
- What: API的内容是什么
- Which: API操作的对象是谁？
- Where: API操作是从哪一个地方（IP地址）来的？

```
{
        "eventVersion": "1.01",
        "userIdentity": {
                "type": "IAMUser", // Who?
                "principalId": "AIDAJDPLRKLG7UEXAMPLE",
                "arn": "arn:aws:iam::123456789012:user/Alice", //Who?
                "accountId": "123456789012",
                "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
                "userName": "Alice",
                "sessionContext": {
                        "attributes": {
                                "mfaAuthenticated": "false",
                                "creationDate": "2014-03-18T14:29:23Z"
                        }
                }
        },
        "eventTime": "2014-03-18T14:30:07Z", //When?
        "eventSource": "cloudtrail.amazonaws.com",
        "eventName": "StartLogging", //What?
        "awsRegion": "us-west-2",//Where to?
        "sourceIPAddress": "72.21.198.64", // Where from?
        "userAgent": "AWSConsole, aws-sdk-java/1.4.5 Linux/x.xx.fleetxen Java_HotSpot(TM)_64-Bit_Server_VM/xx",
        "requestParameters": {
                "name": "Default“ // Which resource?
        },
        // more event details
}
```

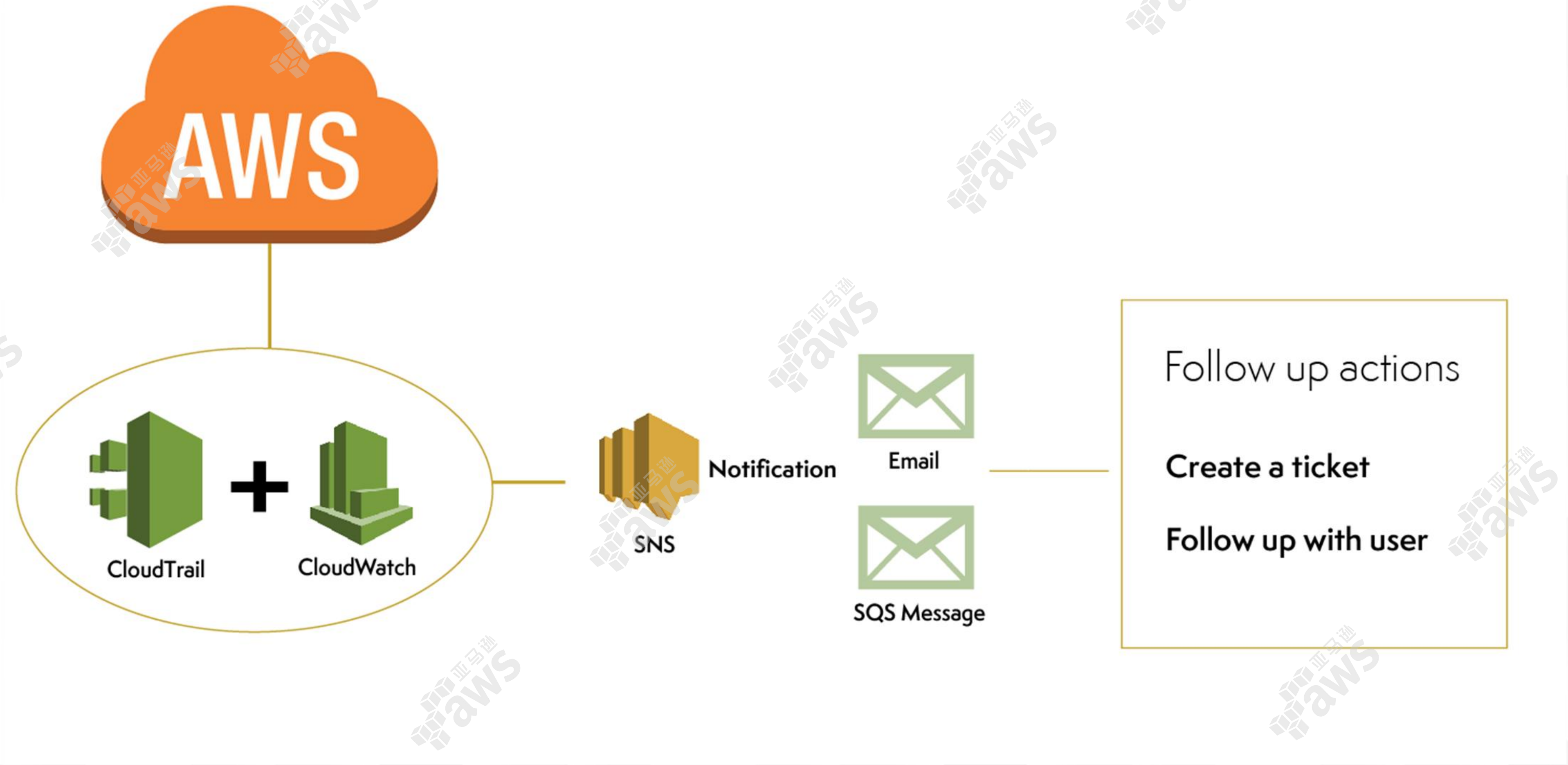
如何监控日志?

- 可以监控特定的API操作并发送报警
- 监控安全和网络相关的高敏感的操作
- 一些常见的监控
  - 创建，删除和修改安全组或VPC
  - 修改IAM的策略和S3的桶策略
  - 失败的AWS控制台登陆事件
  - 登陆/认证失败的API操作
  - 对EC2的创建，启动，关闭，停机，重启等动作

- 可以通过CloudFormation的预定义的脚本方便设定CloudTrail的报警功能

  http://docs.aws.amazon.com/zh_cn/awscloudtrail/latest/userguide/use-cloudformation-template-to-create-cloudwatch-alarms.html

在特定的API/事件发生的时候发送报警（SNS）

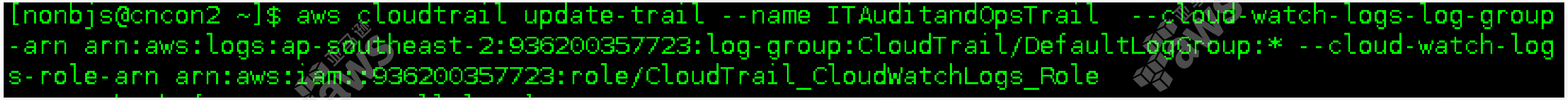


Follow up actions

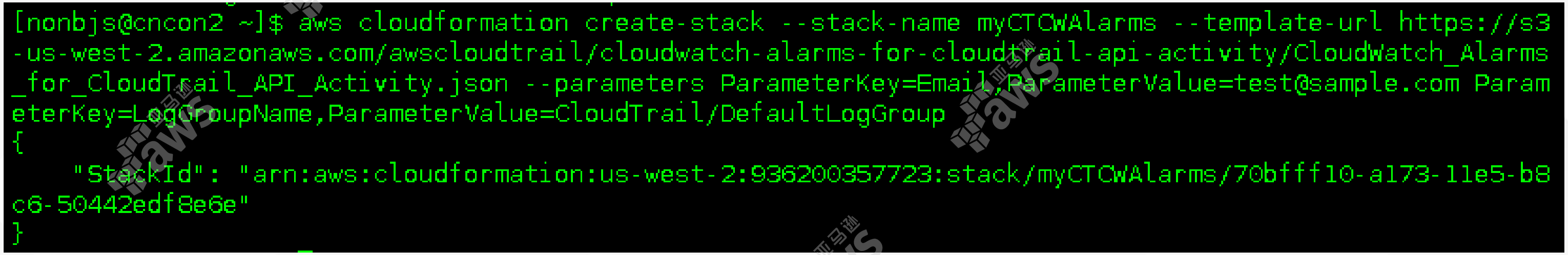
Create a ticket

Follow up with user

命令行配置方式

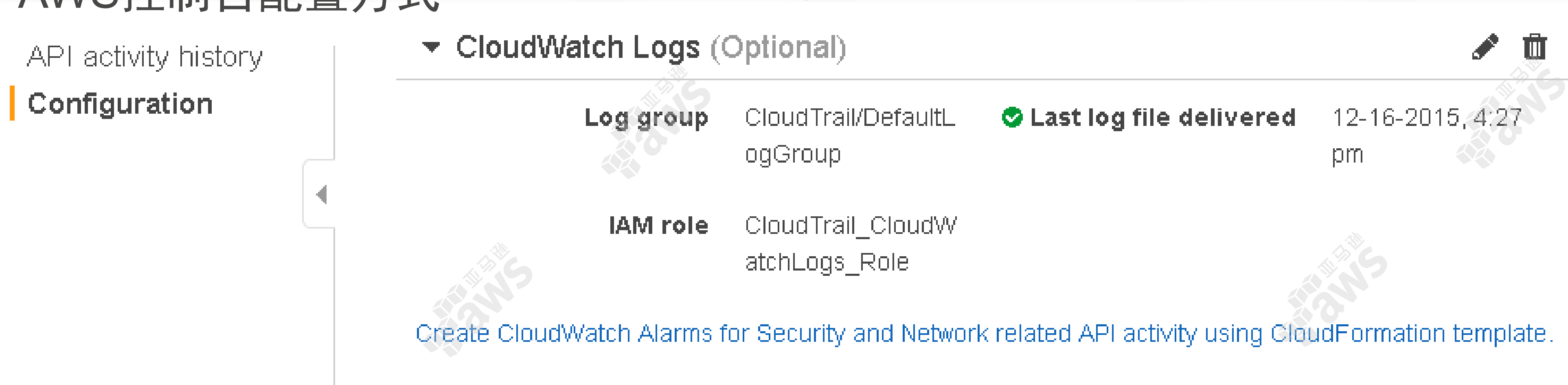


```
[nonbjs@cncon2 ~]$ aws cloudtrail update-trail --name ITAuditandOpsTrail  --cloud-watch-logs-log-group
-arn arn:aws:logs:ap-southeast-2:936200357723:log-group:CloudTrail/DefaultLogGroup:* --cloud-watch-log
s-role-arn arn:aws:iam::936200357723:role/CloudTrail_CloudWatchLogs_Role
```



```
[nonbjs@cncon2 ~]$ aws cloudformation create-stack --stack-name myCTCWAlarms --template-url https://s3
-us-west-2.amazonaws.com/awscloudtrail/cloudwatch-alarms-for-cloudtrail-api-activity/CloudWatch_Alarms
_for_CloudTrail_API_Activity.json --parameters ParameterKey=Email,ParameterValue=test@sample.com Param
eterKey=LogGroupName,ParameterValue=CloudTrail/DefaultLogGroup
{
    "StackId": "arn:aws:cloudformation:us-west-2:936200357723:stack/myCTCWAlarms/70bfff10-a173-11e5-b8
c6-50442edf8e6e"
}
```

AWS控制台配置方式



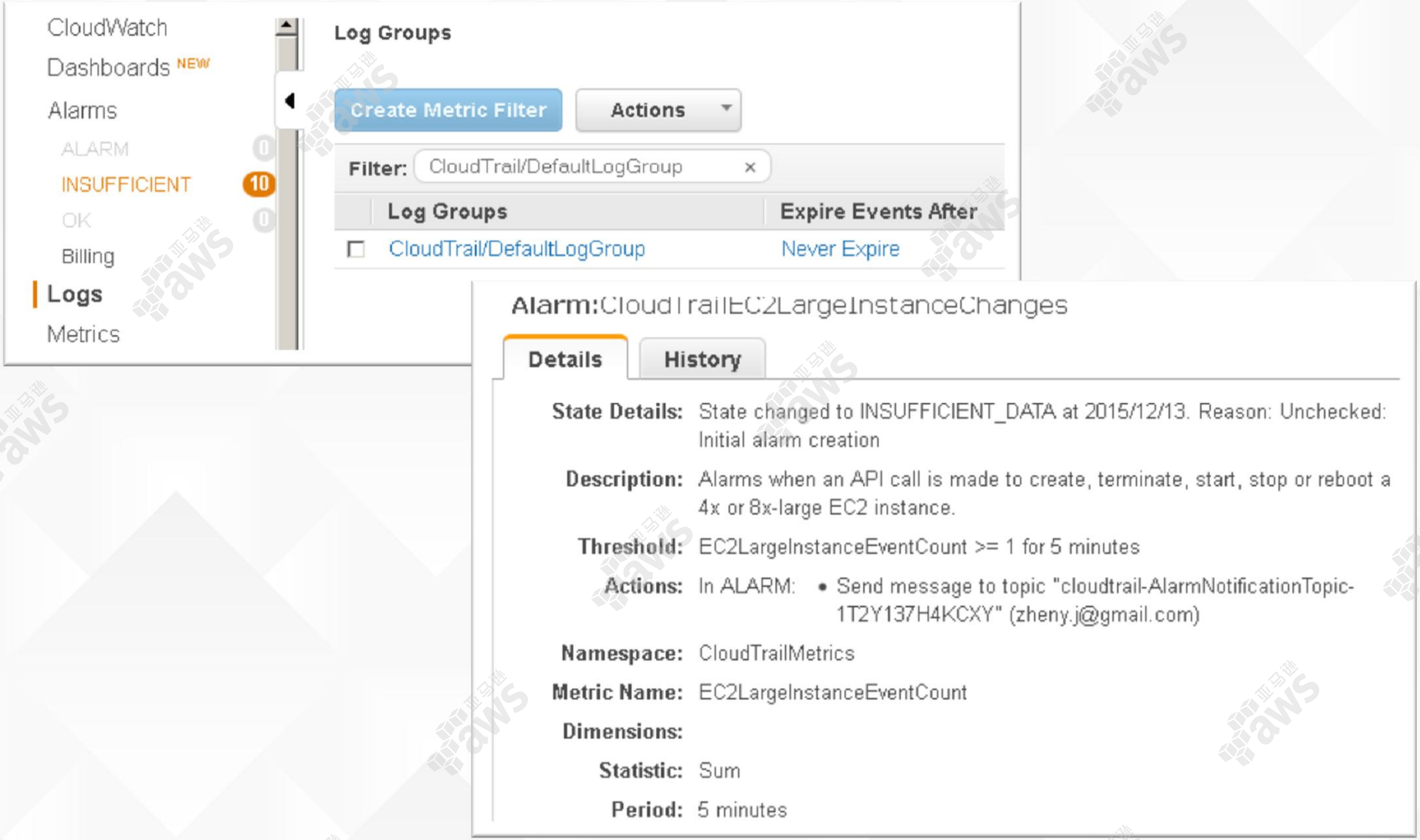
CloudWatch Logs (Optional)

Log group CloudTrail/DefaultLogGroup

✓ **Last log file delivered** 12-16-2015, 4:27 pm

IAM role CloudTrail_CloudWatchLogs_Role

Create CloudWatch Alarms for Security and Network related API activity using CloudFormation template.



Log Groups

Filter: CloudTrail/DefaultLogGroup ×

	Log Groups	Expire Events After
□	CloudTrail/DefaultLogGroup	Never Expire

Alarm:CloudTrailEC2LargeInstanceChanges

State Details: State changed to INSUFFICIENT_DATA at 2015/12/13. Reason: Unchecked: Initial alarm creation

Description: Alarms when an API call is made to create, terminate, start, stop or reboot a 4x or 8x-large EC2 instance.

Threshold: EC2LargeInstanceEventCount >= 1 for 5 minutes

Actions: In ALARM: • Send message to topic "cloudtrail-AlarmNotificationTopic-1T2Y137H4KCXY" (zheny.j@gmail.com)

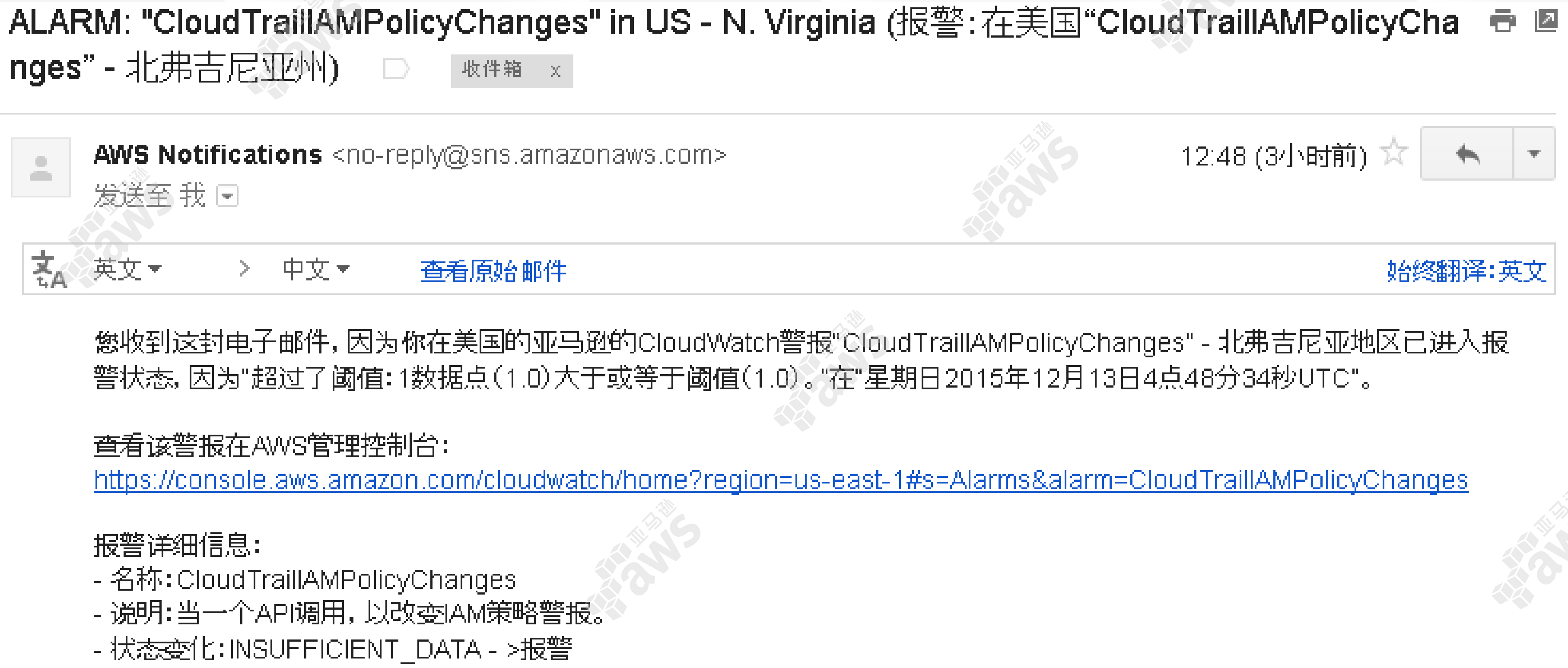
Namespace: CloudTrailMetrics

Metric Name: EC2LargeInstanceEventCount

Dimensions:

Statistic: Sum

Period: 5 minutes



ALARM: "CloudTrailIAMPolicyChanges" in US - N. Virginia (报警：在美国“CloudTrailIAMPolicyChanges” - 北弗吉尼亚州)

AWS Notifications <no-reply@sns.amazonaws.com>

发送至 我

12:48 (3小时前)

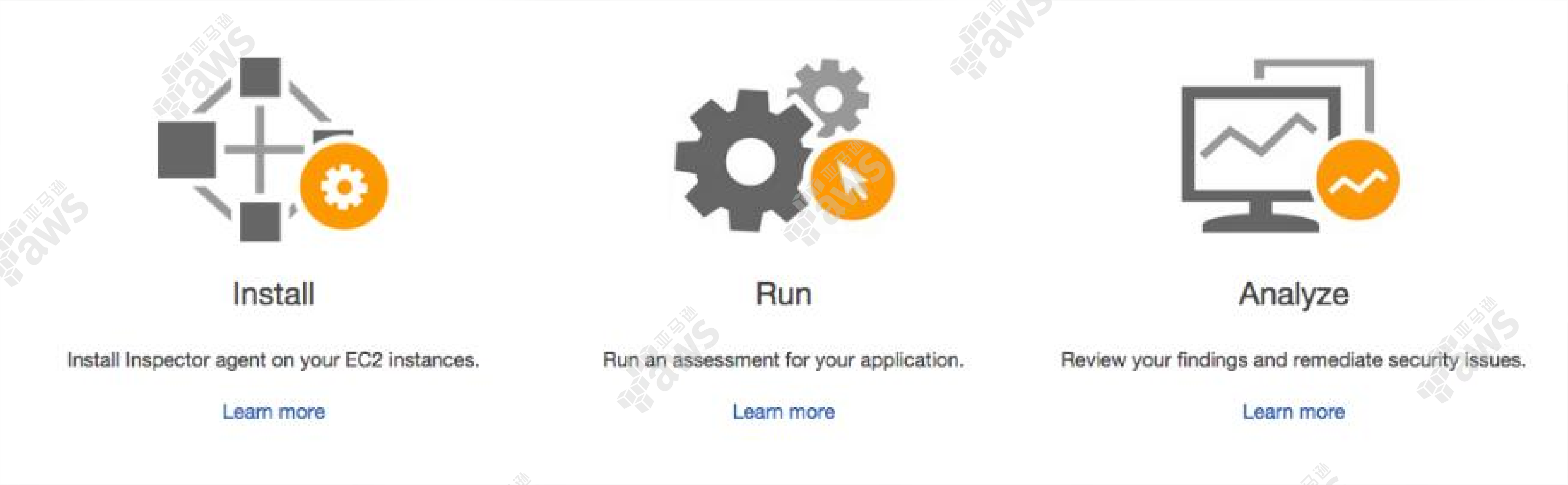
您收到这封电子邮件，因为你在美国的亚马逊的CloudWatch警报"CloudTrailIAMPolicyChanges" - 北弗吉尼亚地区已进入报警状态，因为"超过了阈值：1数据点(1.0)大于或等于阈值(1.0)。"在"星期日2015年12月13日4点48分34秒UTC"。

查看该警报在AWS管理控制台：
https://console.aws.amazon.com/cloudwatch/home?region=us-east-1#s=Alarms&alarm=CloudTrailIAMPolicyChanges

报警详细信息：
- 名称：CloudTrailIAMPolicyChanges
- 说明：当一个API调用，以改变IAM策略警报。
- 状态变化：INSUFFICIENT_DATA - >报警

通过Amazon Inspector保护客户操作系统的安全

- 对现有系统中的软件进行CVE检查
- 网络设定的最佳实践检查
- 认证设定的最佳实践检查
- 应用程序安全的最佳实践检查
- PCI DCSS 3.0的合规性检查



Install

Install Inspector agent on your EC2 instances.

Learn more

Run

Run an assessment for your application.

Learn more

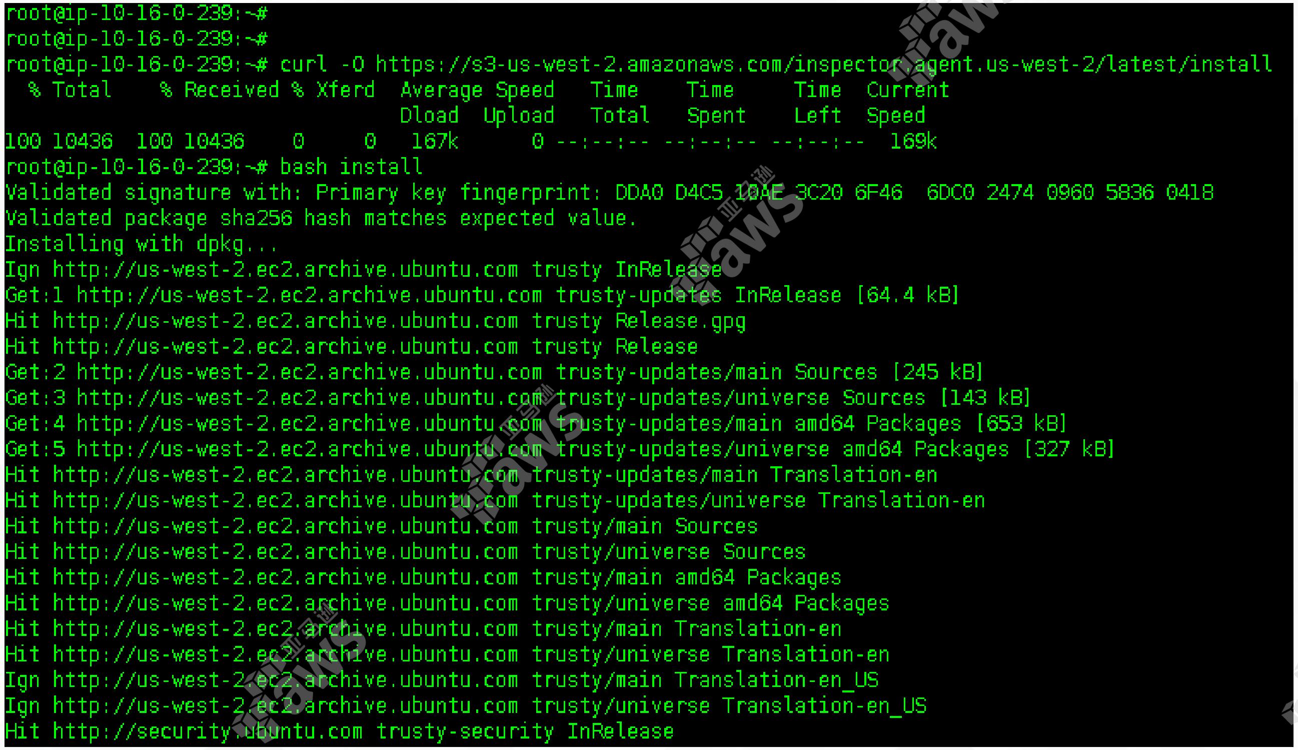
Analyze

Review your findings and remediate security issues.

Learn more

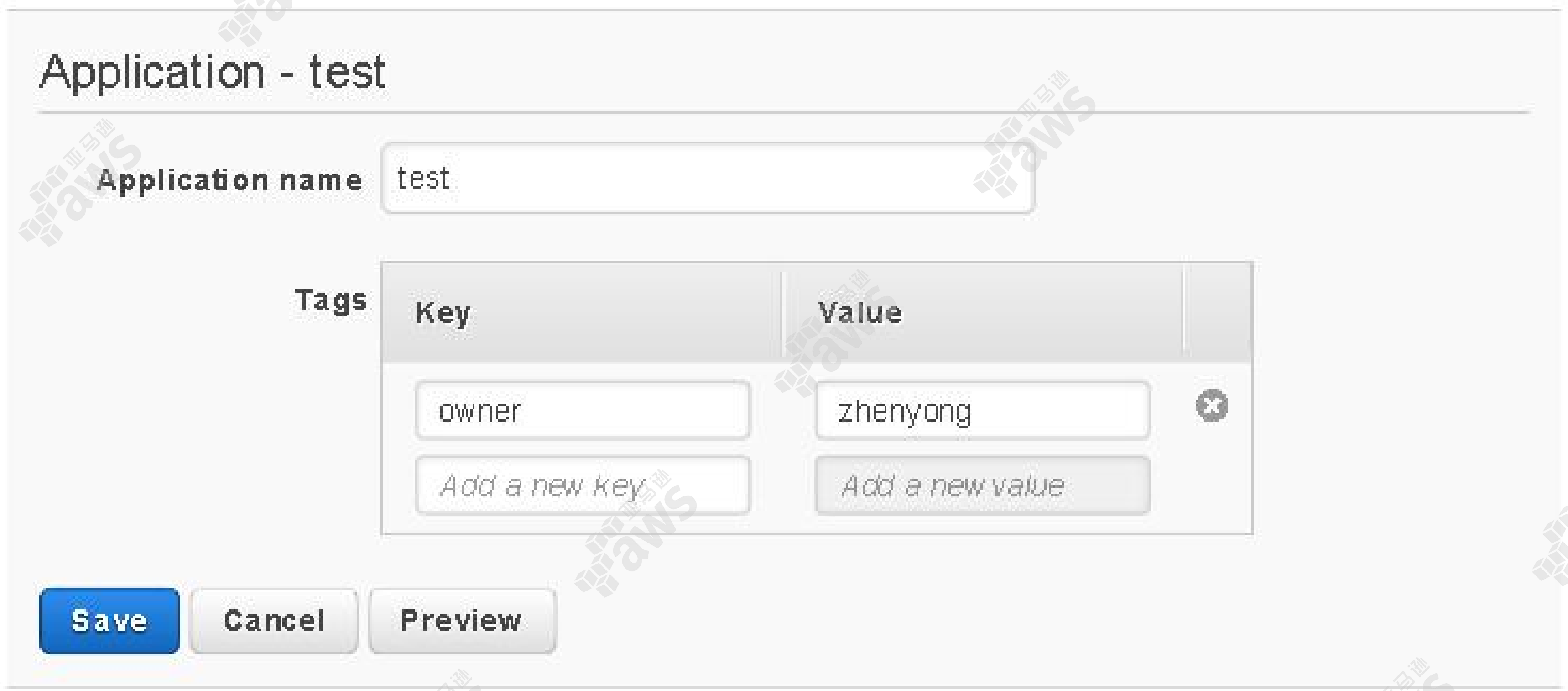
启用Amazon Inspector的步骤

- 在EC2上安装代理程序



```
root@ip-10-16-0-239:~#
root@ip-10-16-0-239:~#
root@ip-10-16-0-239:~# curl -O https://s3-us-west-2.amazonaws.com/inspector.agent.us-west-2/latest/install
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 10436  100 10436    0     0   167k      0 --:--:-- --:--:-- --:--:--  169k
root@ip-10-16-0-239:~# bash install
Validated signature with: Primary key fingerprint: DDA0 D4C5 10AE 3C20 6F46  6DC0 2474 0960 5836 0418
Validated package sha256 hash matches expected value.
Installing with dpkg...
Ign http://us-west-2.ec2.archive.ubuntu.com trusty InRelease
Get:1 http://us-west-2.ec2.archive.ubuntu.com trusty-updates InRelease [64.4 kB]
Hit http://us-west-2.ec2.archive.ubuntu.com trusty Release.gpg
Hit http://us-west-2.ec2.archive.ubuntu.com trusty Release
Get:2 http://us-west-2.ec2.archive.ubuntu.com trusty-updates/main Sources [245 kB]
Get:3 http://us-west-2.ec2.archive.ubuntu.com trusty-updates/universe Sources [143 kB]
Get:4 http://us-west-2.ec2.archive.ubuntu.com trusty-updates/main amd64 Packages [653 kB]
Get:5 http://us-west-2.ec2.archive.ubuntu.com trusty-updates/universe amd64 Packages [327 kB]
Hit http://us-west-2.ec2.archive.ubuntu.com trusty-updates/main Translation-en
Hit http://us-west-2.ec2.archive.ubuntu.com trusty-updates/universe Translation-en
Hit http://us-west-2.ec2.archive.ubuntu.com trusty/main Sources
Hit http://us-west-2.ec2.archive.ubuntu.com trusty/universe Sources
Hit http://us-west-2.ec2.archive.ubuntu.com trusty/main amd64 Packages
Hit http://us-west-2.ec2.archive.ubuntu.com trusty/universe amd64 Packages
Hit http://us-west-2.ec2.archive.ubuntu.com trusty/main Translation-en
Hit http://us-west-2.ec2.archive.ubuntu.com trusty/universe Translation-en
Ign http://us-west-2.ec2.archive.ubuntu.com trusty/main Translation-en_US
Ign http://us-west-2.ec2.archive.ubuntu.com trusty/universe Translation-en_US
Hit http://security.ubuntu.com trusty-security InRelease
```

定义Amazon Inspector的应用



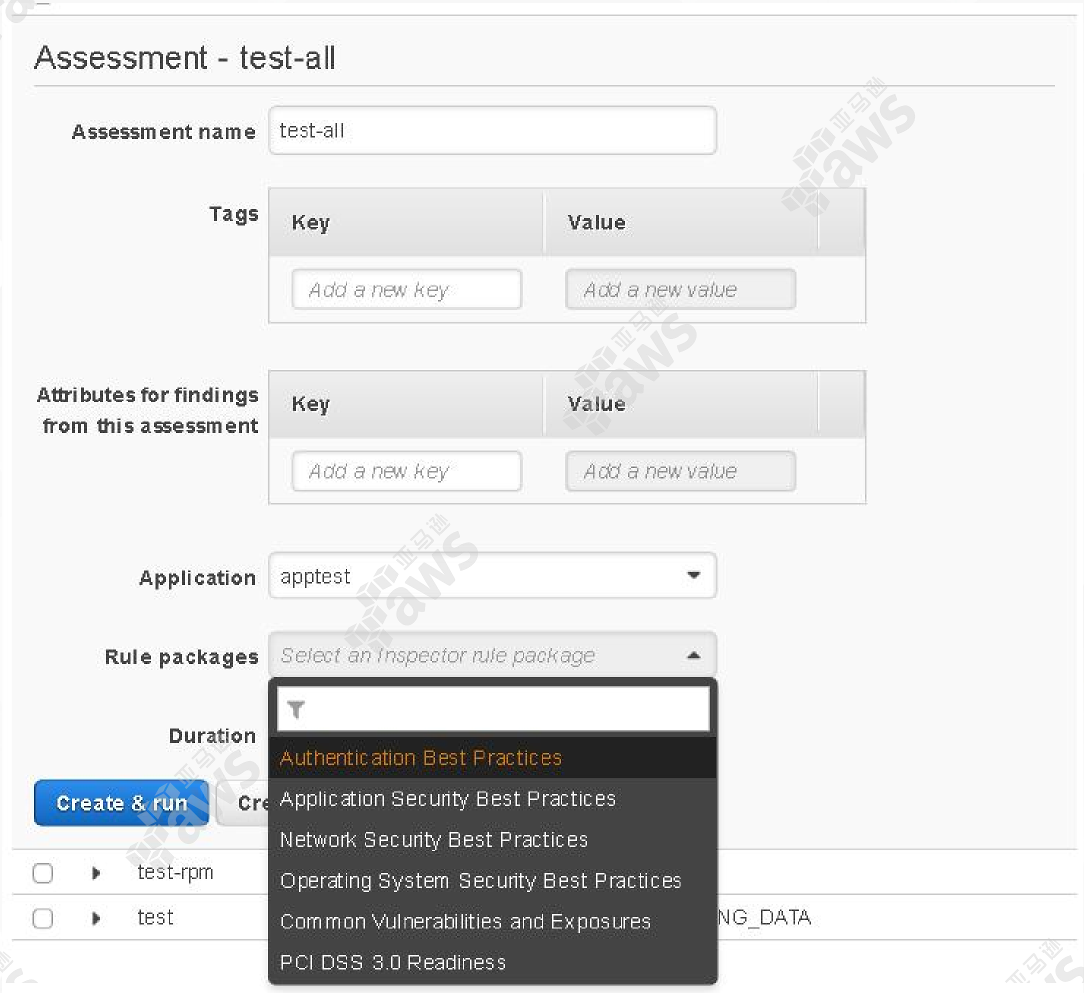
Application - test

Application name	test

Tags

Key	Value	
owner	zhenyong	⊗
Add a new key	Add a new value	

创建Amazon Inspector的评估设定



Assessment - test-all

Assessment name: test-all

Tags

Key	Value
Add a new key	Add a new value

Attributes for findings from this assessment

Key	Value
Add a new key	Add a new value

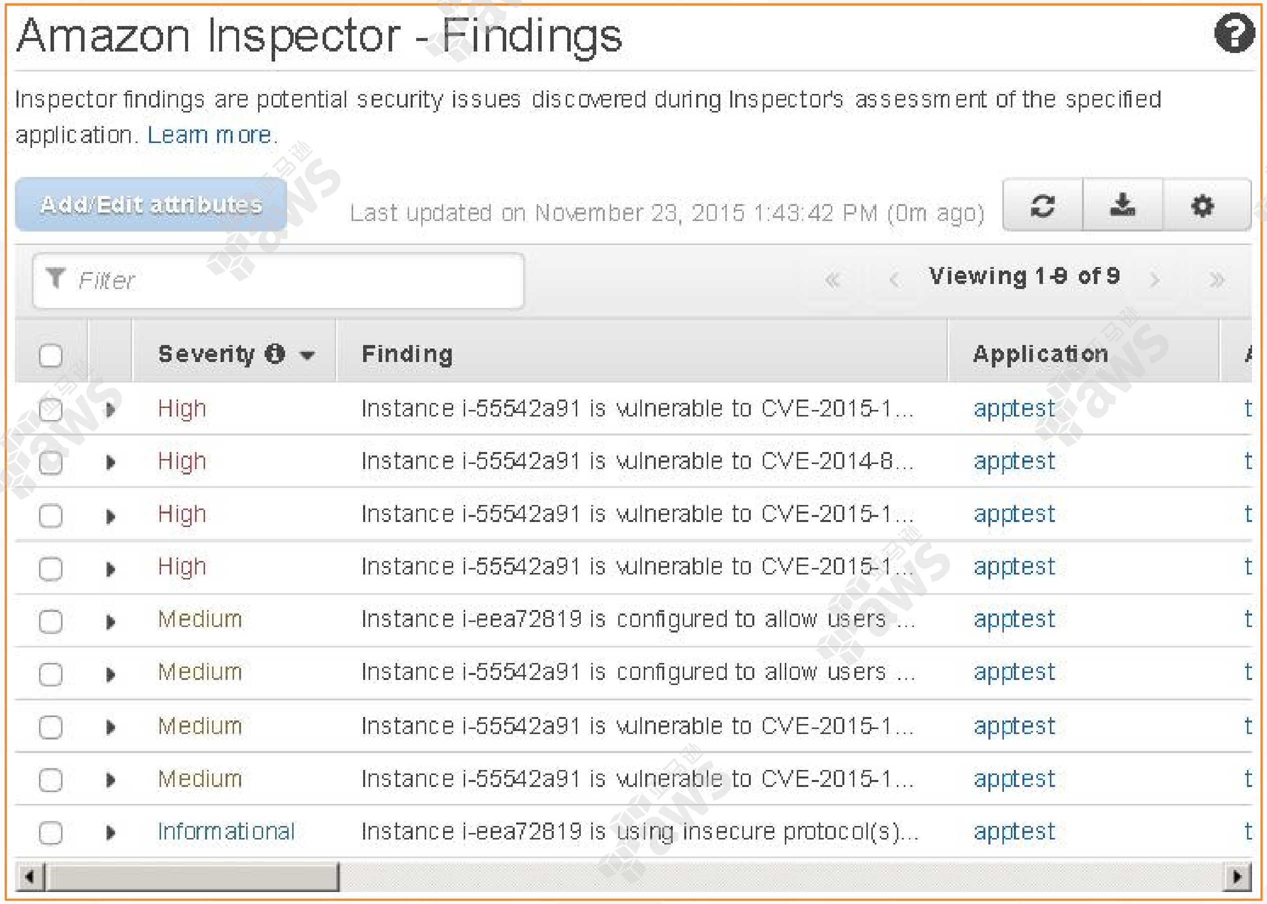
Application: apptest

Rule packages: Select an Inspector rule package

- Authentication Best Practices
- Application Security Best Practices
- Network Security Best Practices
- Operating System Security Best Practices
- Common Vulnerabilities and Exposures
- PCI DSS 3.0 Readiness

Duration

显示Amazon Inspector的查找结果

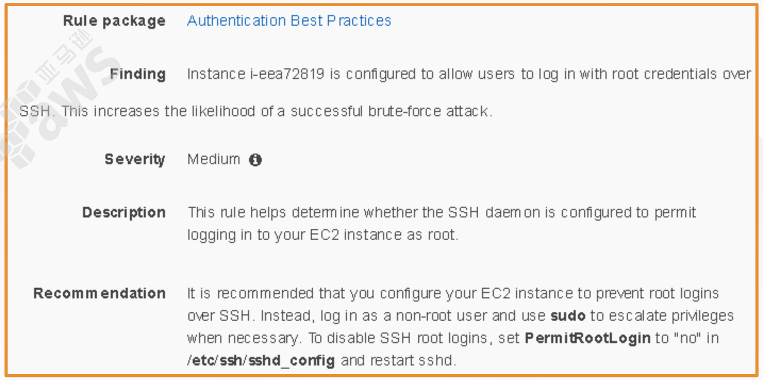


Amazon Inspector - Findings

Inspector findings are potential security issues discovered during Inspector's assessment of the specified application. Learn more.

Last updated on November 23, 2015 1:43:42 PM (0m ago)

☐		Severity	Finding	Application	A
☐	▸	High	Instance i-55542a91 is vulnerable to CVE-2015-1...	apptest	t
☐	▸	High	Instance i-55542a91 is vulnerable to CVE-2014-8...	apptest	t
☐	▸	High	Instance i-55542a91 is vulnerable to CVE-2015-1...	apptest	t
☐	▸	High	Instance i-55542a91 is vulnerable to CVE-2015-1...	apptest	t
☐	▸	Medium	Instance i-eea72819 is configured to allow users ...	apptest	t
☐	▸	Medium	Instance i-55542a91 is configured to allow users ...	apptest	t
☐	▸	Medium	Instance i-55542a91 is vulnerable to CVE-2015-1...	apptest	t
☐	▸	Medium	Instance i-55542a91 is vulnerable to CVE-2015-1...	apptest	t
☐	▸	Informational	Instance i-eea72819 is using insecure protocol(s)...	apptest	t



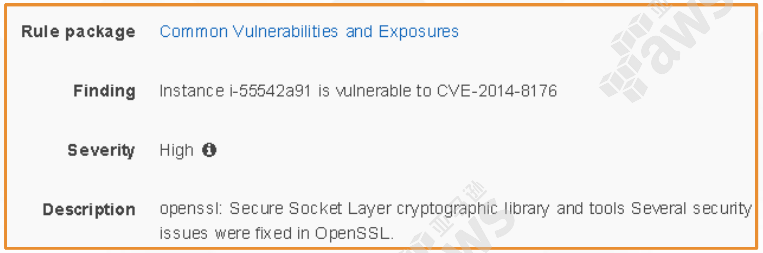
Rule package Authentication Best Practices

Finding Instance i-eea72819 is configured to allow users to log in with root credentials over SSH. This increases the likelihood of a successful brute-force attack.

Severity Medium

Description This rule helps determine whether the SSH daemon is configured to permit logging in to your EC2 instance as root.

Recommendation It is recommended that you configure your EC2 instance to prevent root logins over SSH. Instead, log in as a non-root user and use **sudo** to escalate privileges when necessary. To disable SSH root logins, set **PermitRootLogin** to "no" in **/etc/ssh/sshd_config** and restart sshd.



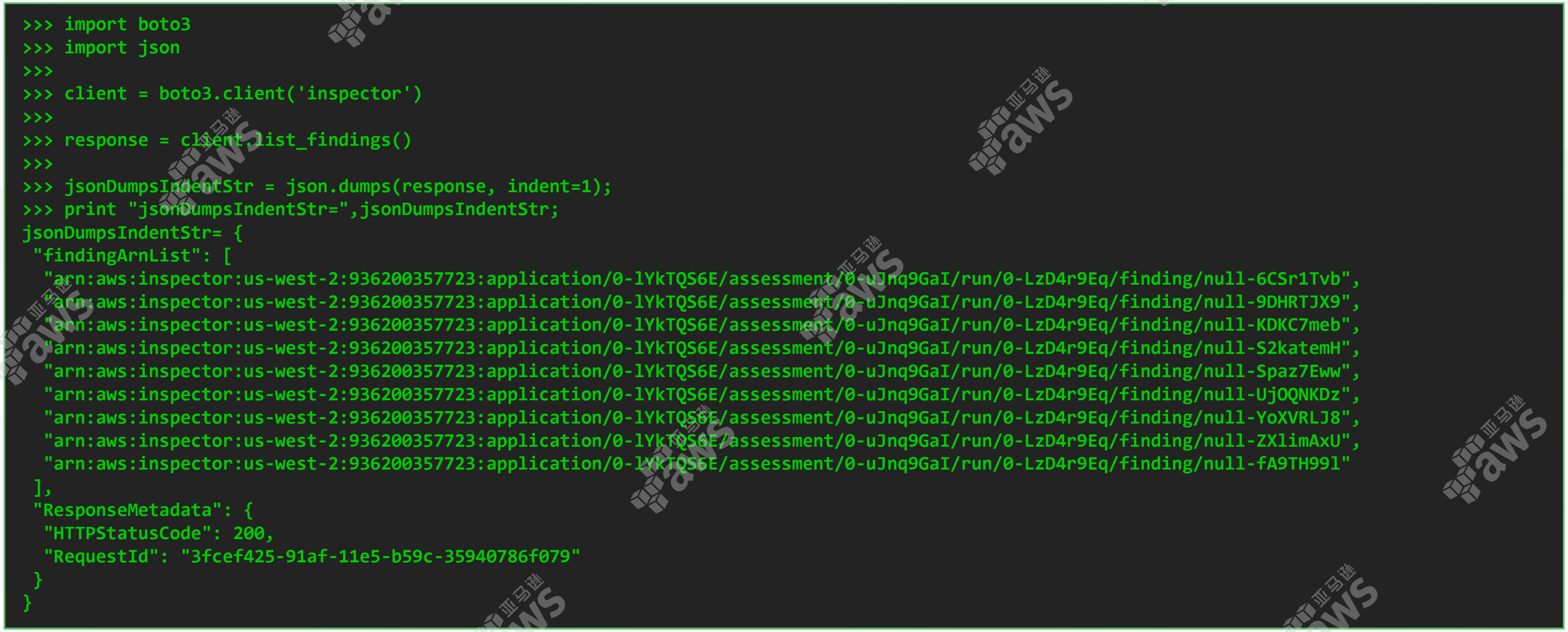
Rule package Common Vulnerabilities and Exposures

Finding Instance i-55542a91 is vulnerable to CVE-2014-8176

Severity High

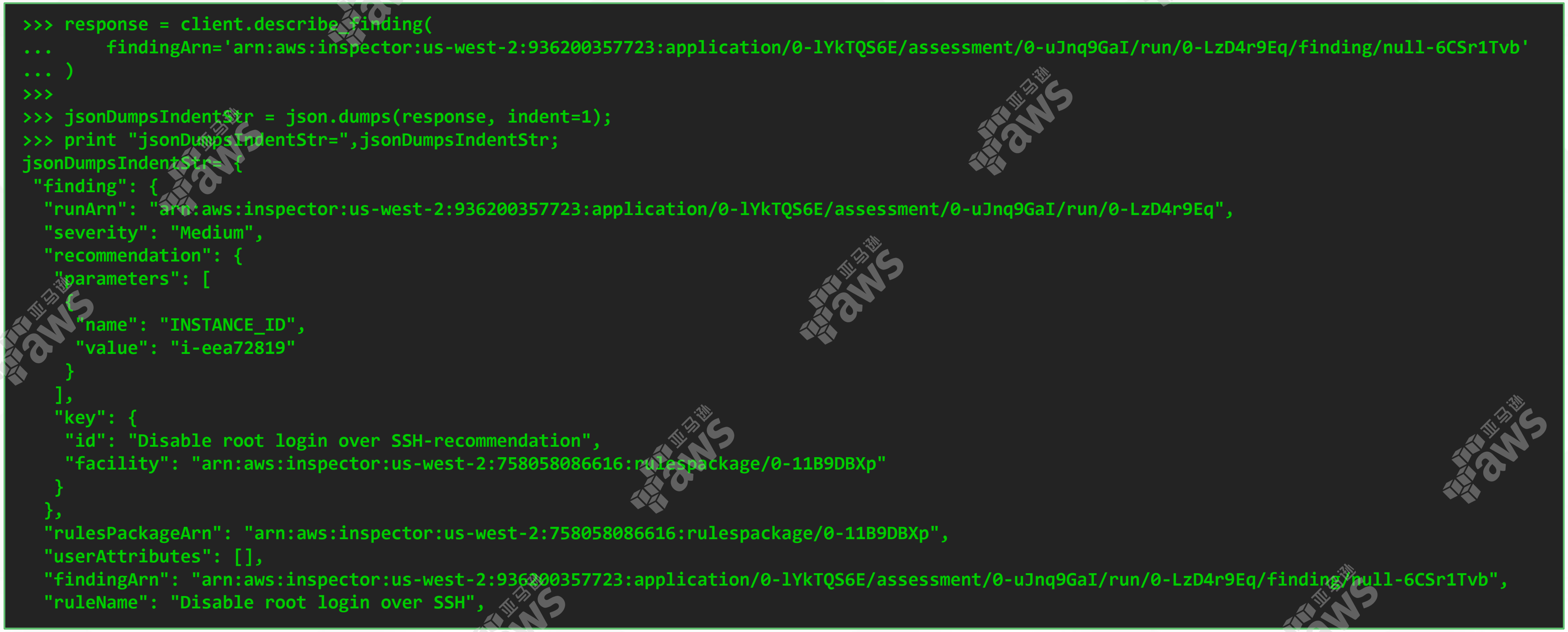
Description openssl: Secure Socket Layer cryptographic library and tools Several security issues were fixed in OpenSSL.

用代码处理检查结果的例子



```
>>> import boto3
>>> import json
>>>
>>> client = boto3.client('inspector')
>>>
>>> response = client.list_findings()
>>>
>>> jsonDumpsIndentStr = json.dumps(response, indent=1);
>>> print "jsonDumpsIndentStr=",jsonDumpsIndentStr;
jsonDumpsIndentStr= {
 "findingArnList": [
  "arn:aws:inspector:us-west-2:936200357723:application/0-lYkTQS6E/assessment/0-uJnq9GaI/run/0-LzD4r9Eq/finding/null-6CSr1Tvb",
  "arn:aws:inspector:us-west-2:936200357723:application/0-lYkTQS6E/assessment/0-uJnq9GaI/run/0-LzD4r9Eq/finding/null-9DHRTJX9",
  "arn:aws:inspector:us-west-2:936200357723:application/0-lYkTQS6E/assessment/0-uJnq9GaI/run/0-LzD4r9Eq/finding/null-KDKC7meb",
  "arn:aws:inspector:us-west-2:936200357723:application/0-lYkTQS6E/assessment/0-uJnq9GaI/run/0-LzD4r9Eq/finding/null-S2katemH",
  "arn:aws:inspector:us-west-2:936200357723:application/0-lYkTQS6E/assessment/0-uJnq9GaI/run/0-LzD4r9Eq/finding/null-Spaz7Eww",
  "arn:aws:inspector:us-west-2:936200357723:application/0-lYkTQS6E/assessment/0-uJnq9GaI/run/0-LzD4r9Eq/finding/null-UjOQNKDz",
  "arn:aws:inspector:us-west-2:936200357723:application/0-lYkTQS6E/assessment/0-uJnq9GaI/run/0-LzD4r9Eq/finding/null-YoXVRLJ8",
  "arn:aws:inspector:us-west-2:936200357723:application/0-lYkTQS6E/assessment/0-uJnq9GaI/run/0-LzD4r9Eq/finding/null-ZXlimAxU",
  "arn:aws:inspector:us-west-2:936200357723:application/0-lYkTQS6E/assessment/0-uJnq9GaI/run/0-LzD4r9Eq/finding/null-fA9TH99l"
 ],
 "ResponseMetadata": {
  "HTTPStatusCode": 200,
  "RequestId": "3fcef425-91af-11e5-b59c-35940786f079"
 }
}
```

用代码处理检查结果的例子

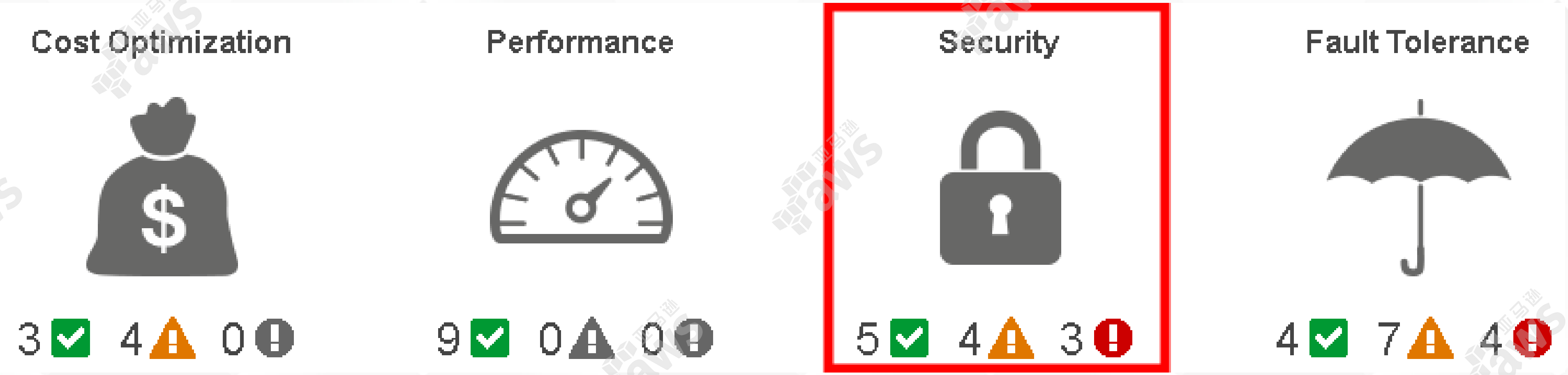


```
>>> response = client.describe_finding(
...     findingArn='arn:aws:inspector:us-west-2:936200357723:application/0-lYkTQS6E/assessment/0-uJnq9GaI/run/0-LzD4r9Eq/finding/null-6CSr1Tvb'
... )
>>>
>>> jsonDumpsIndentStr = json.dumps(response, indent=1);
>>> print "jsonDumpsIndentStr=",jsonDumpsIndentStr;
jsonDumpsIndentStr= {
 "finding": {
  "runArn": "arn:aws:inspector:us-west-2:936200357723:application/0-lYkTQS6E/assessment/0-uJnq9GaI/run/0-LzD4r9Eq",
  "severity": "Medium",
  "recommendation": {
   "parameters": [
    {
     "name": "INSTANCE_ID",
     "value": "i-eea72819"
    }
   ],
   "key": {
    "id": "Disable root login over SSH-recommendation",
    "facility": "arn:aws:inspector:us-west-2:758058086616:rulespackage/0-11B9DBXp"
   }
  },
  "rulesPackageArn": "arn:aws:inspector:us-west-2:758058086616:rulespackage/0-11B9DBXp",
  "userAttributes": [],
  "findingArn": "arn:aws:inspector:us-west-2:936200357723:application/0-lYkTQS6E/assessment/0-uJnq9GaI/run/0-LzD4r9Eq/finding/null-6CSr1Tvb",
  "ruleName": "Disable root login over SSH",
```

自动化部署Amazon Inspector

- 通过设定EC2 UserData在启动的过程中自动部署代理程序
- AWS CloudFormation
  - 部署新的环境
  - 升级现有软件堆栈
- 其他常见的运维工具: ansible, chef, puppet, salt
  - 在现有的系统上安装和配置代理程序
- 通过APIs完成自动化运维

Trusted Advisor



Cost Optimization

3 ✓ 4 ⚠ 0 ❗

Performance

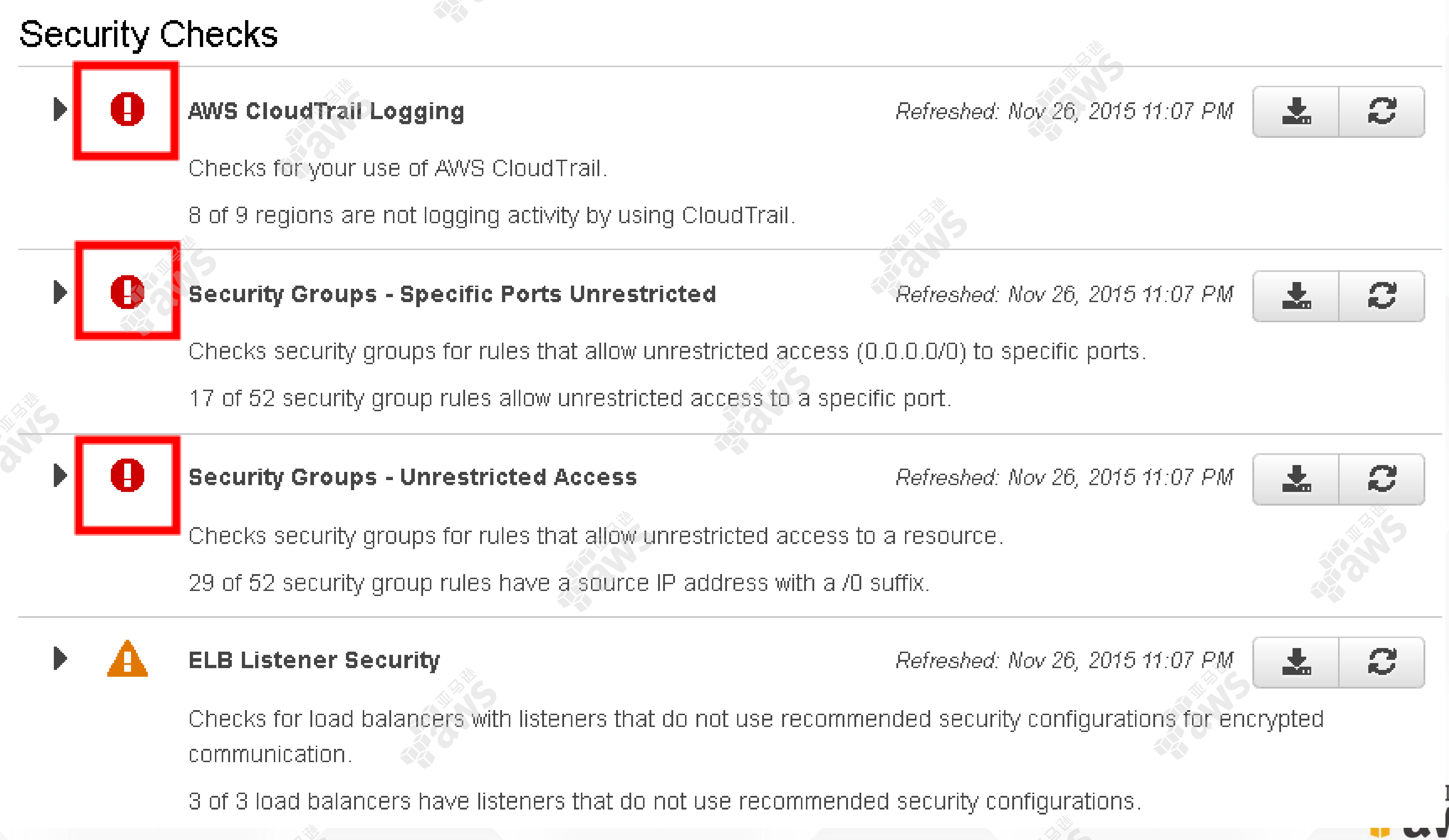
9 ✓ 0 ⚠ 0 ❗

Security

5 ✓ 4 ⚠ 3 ❗

Fault Tolerance

4 ✓ 7 ⚠ 4 ❗



Security Checks

▸ ❗ **AWS CloudTrail Logging** *Refreshed: Nov 26, 2015 11:07 PM*

Checks for your use of AWS CloudTrail.

8 of 9 regions are not logging activity by using CloudTrail.

▸ ❗ **Security Groups - Specific Ports Unrestricted** *Refreshed: Nov 26, 2015 11:07 PM*

Checks security groups for rules that allow unrestricted access (0.0.0.0/0) to specific ports.

17 of 52 security group rules allow unrestricted access to a specific port.

▸ ❗ **Security Groups - Unrestricted Access** *Refreshed: Nov 26, 2015 11:07 PM*

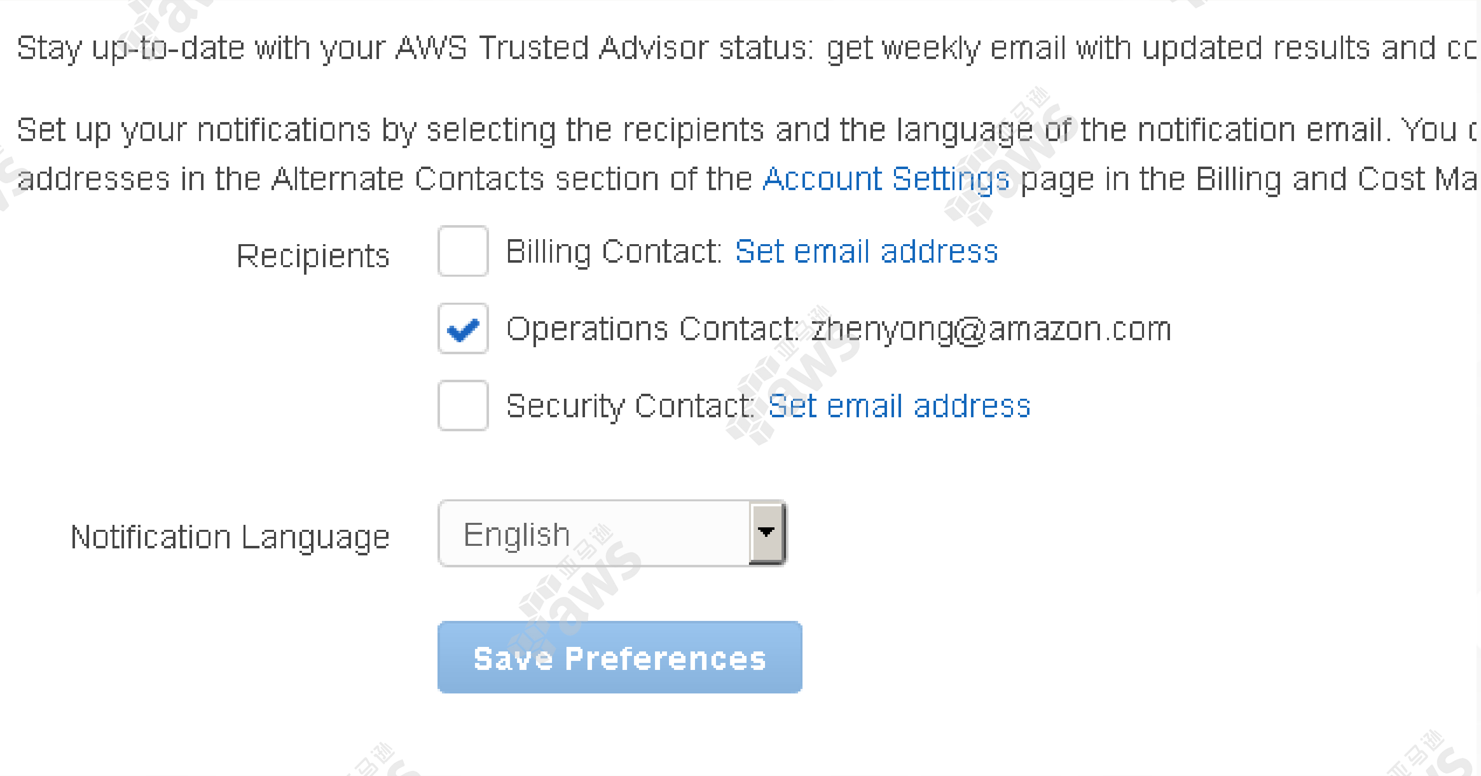
Checks security groups for rules that allow unrestricted access to a resource.

29 of 52 security group rules have a source IP address with a /0 suffix.

▸ ⚠ **ELB Listener Security** *Refreshed: Nov 26, 2015 11:07 PM*

Checks for load balancers with listeners that do not use recommended security configurations for encrypted communication.

3 of 3 load balancers have listeners that do not use recommended security configurations.



Stay up-to-date with your AWS Trusted Advisor status: get weekly email with updated results and cc

Set up your notifications by selecting the recipients and the language of the notification email. You c addresses in the Alternate Contacts section of the Account Settings page in the Billing and Cost Ma

Recipients
□ Billing Contact: Set email address
☑ Operations Contact: zhenyong@amazon.com
□ Security Contact: Set email address

Notification Language: English

Thank You

亚马逊 aws