**AWS动手实验CloudWatch收集EC2实例日志**

**实验目的**

通过 CloudWatch 日志，您可以聚合、监控并存储日志。能够收集常见服务的日志(此章节以系统messages的日志举例)

**实验要求**

了解Amazon Web Services  
了解EC2  
了解IAM  
有Linux基础

**实验原理**

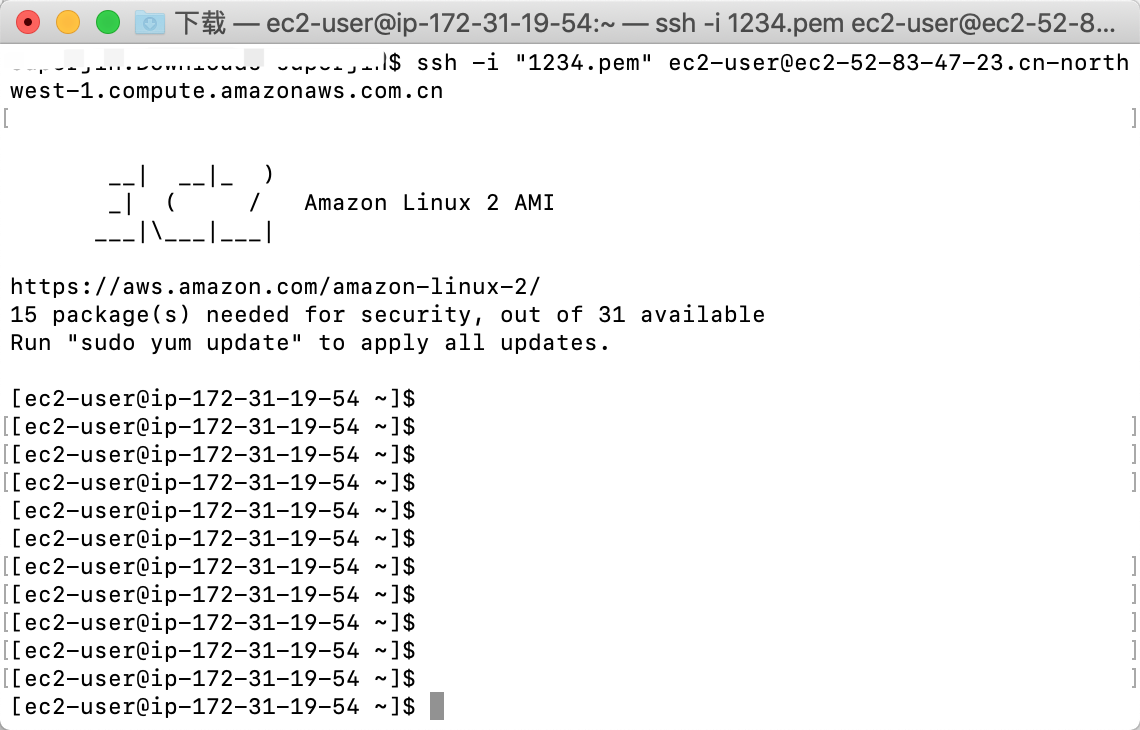
使用 CloudWatch Logs 代理，可以从运行 Linux 或 Windows Server 的 Amazon EC2 实例发布日志数据，可以从 AWS CloudTrail 发布记录的事件。

**实验步骤**

1、点击【服务】，选择【CloudWatch】,点击创建日志组。  


2、取名为Logdemo，点击【创建日志组】按钮。至此我们就创建完成了一个日志组，随后我们开始收集日志。  


3、切换到Ec2服务，创建一个新的实例。(使用Amazon Linux2镜像)  

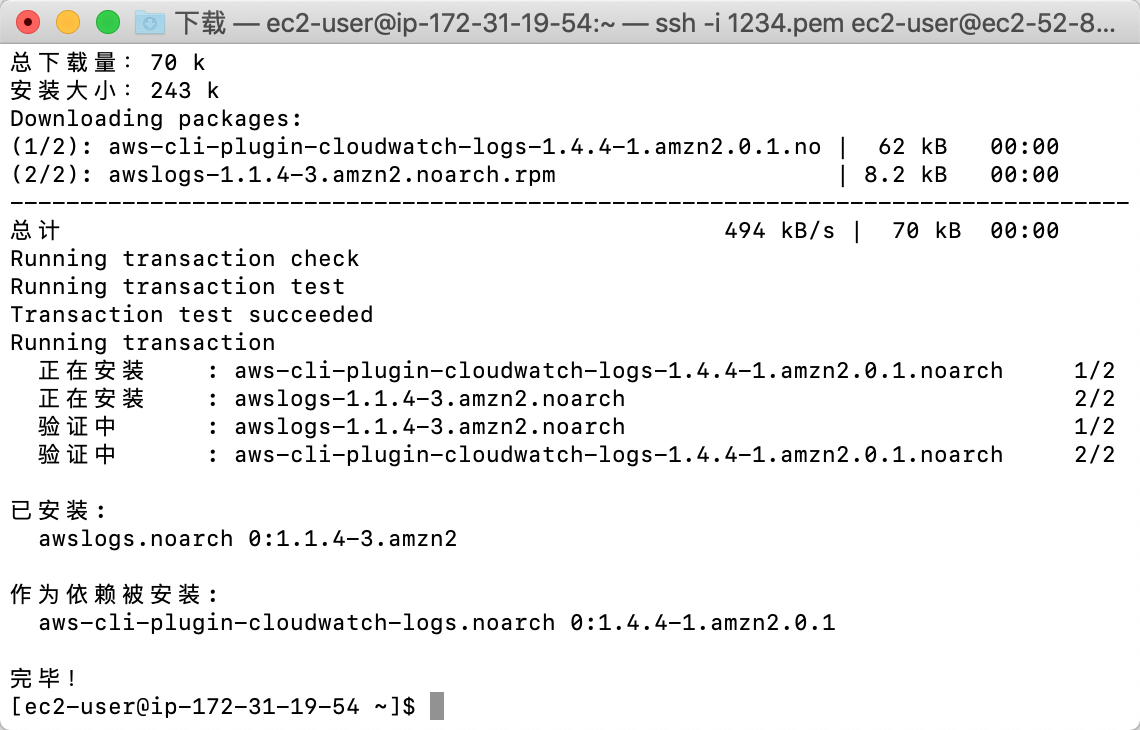

4、使用ssh工具进行连接。  


5、我们开始安装cloudwatch logs代理 “awslogs”。  
首先更新软件包

sudo yum update -y

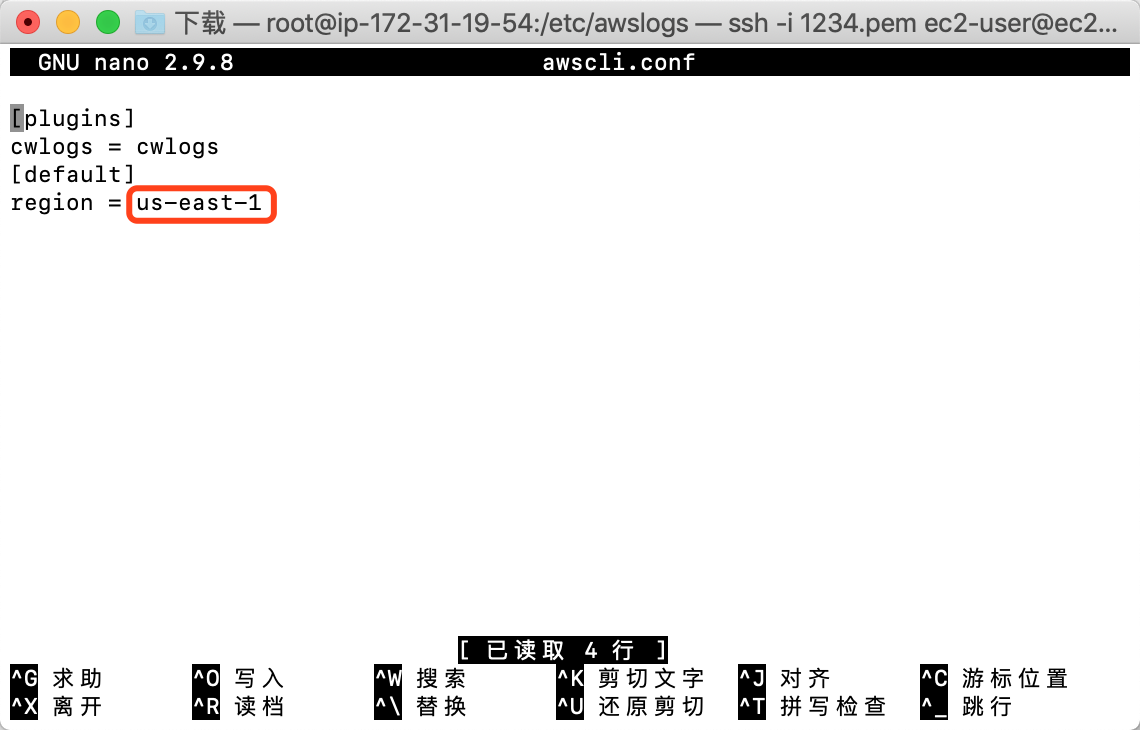
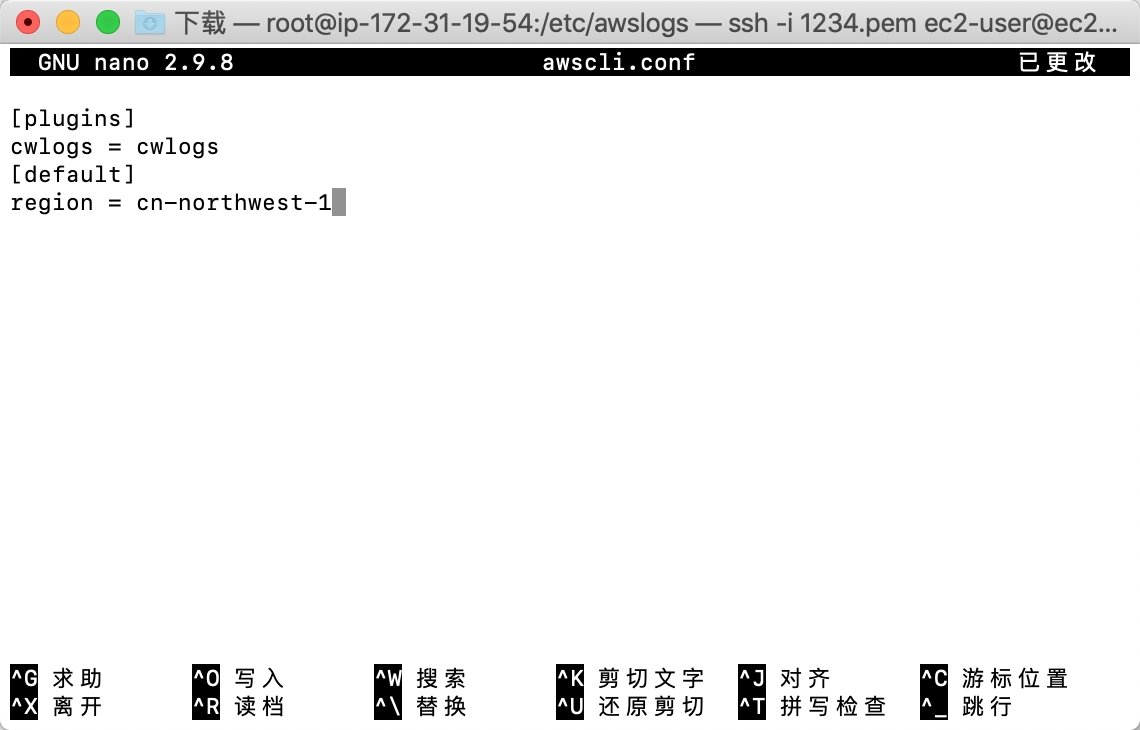
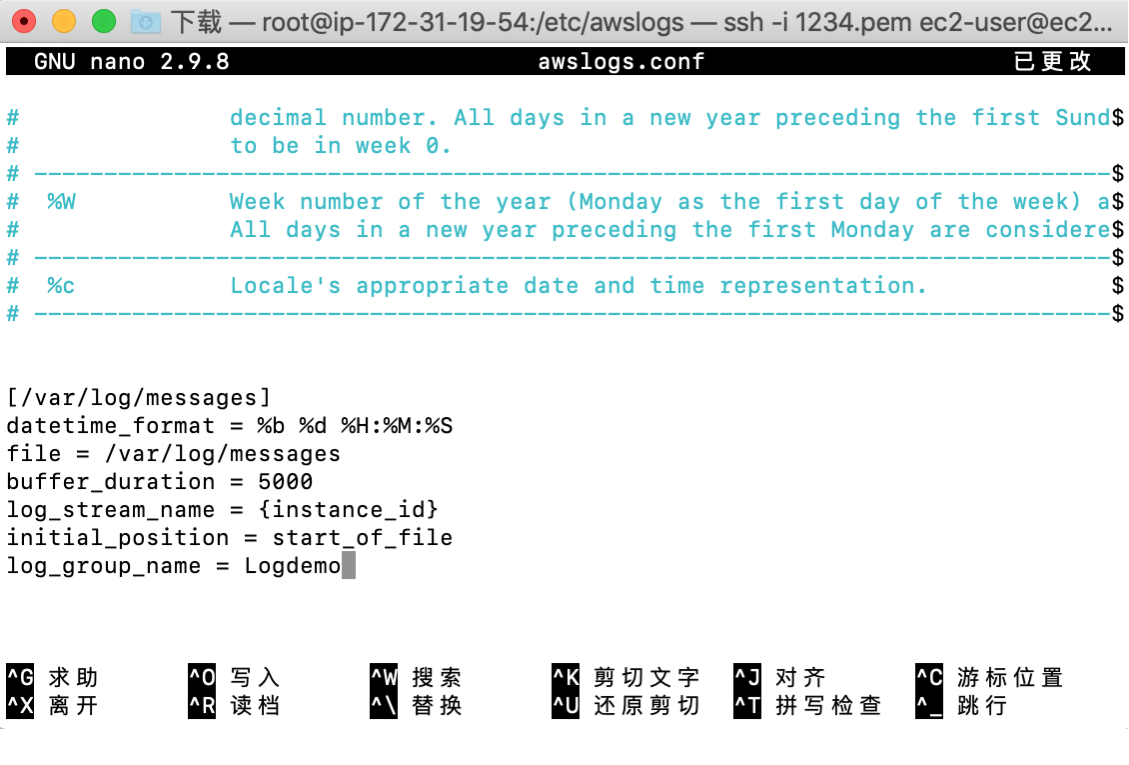
随后安装awslogs软件包

sudo yum install -y awslogs

  
至此awslogs安装完毕

6、开始配置awslogs。  
首先进入awslogs目录

cd /etc/awslogs

  
首先编辑配置文件awscli.conf，修改region为现在所使用的region(我的是cn-northwest-1)  
  
  
保存退出  
编辑文件awslogs.conf，跳转到文件末尾开始编辑  
  
修改log\_group\_name为我们创建的日志组名称Logdemo。  
其中file为日志文件的位置在/var/log/messages，保持默认即可  
log\_stream\_name为实例id，保持默认即可  
  
保存退出

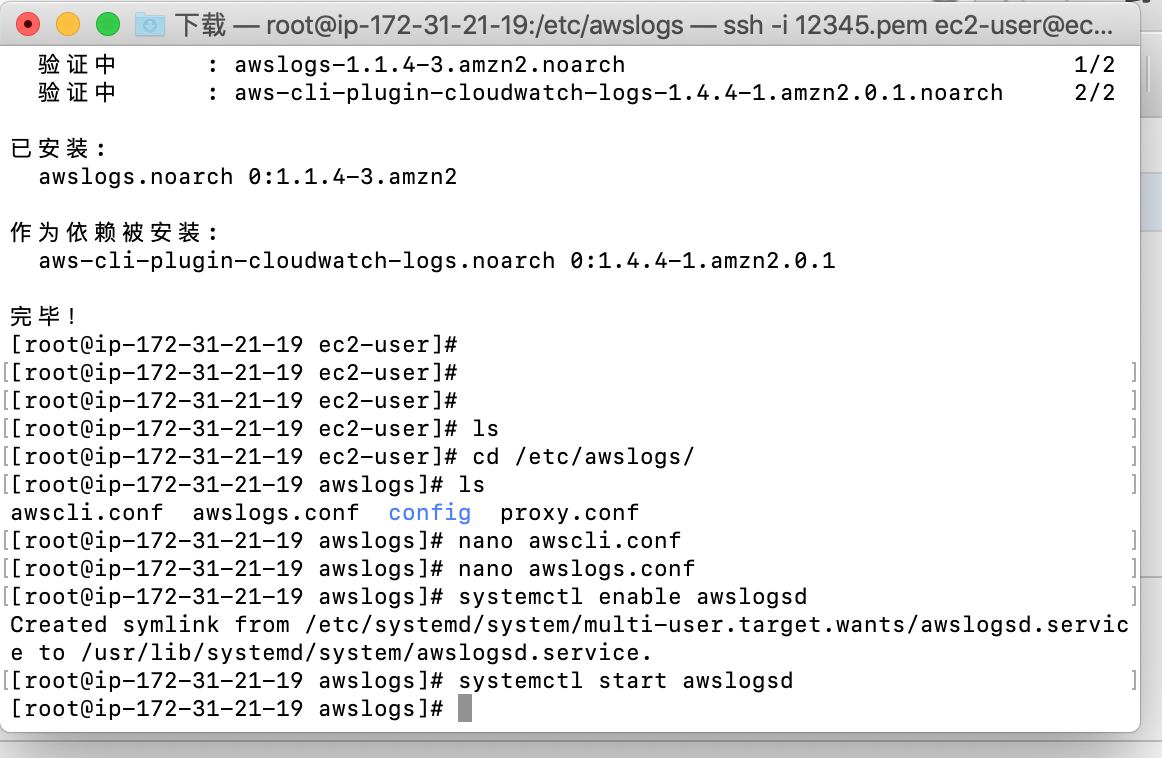
7、配置服务开机启动。以及启动该服务

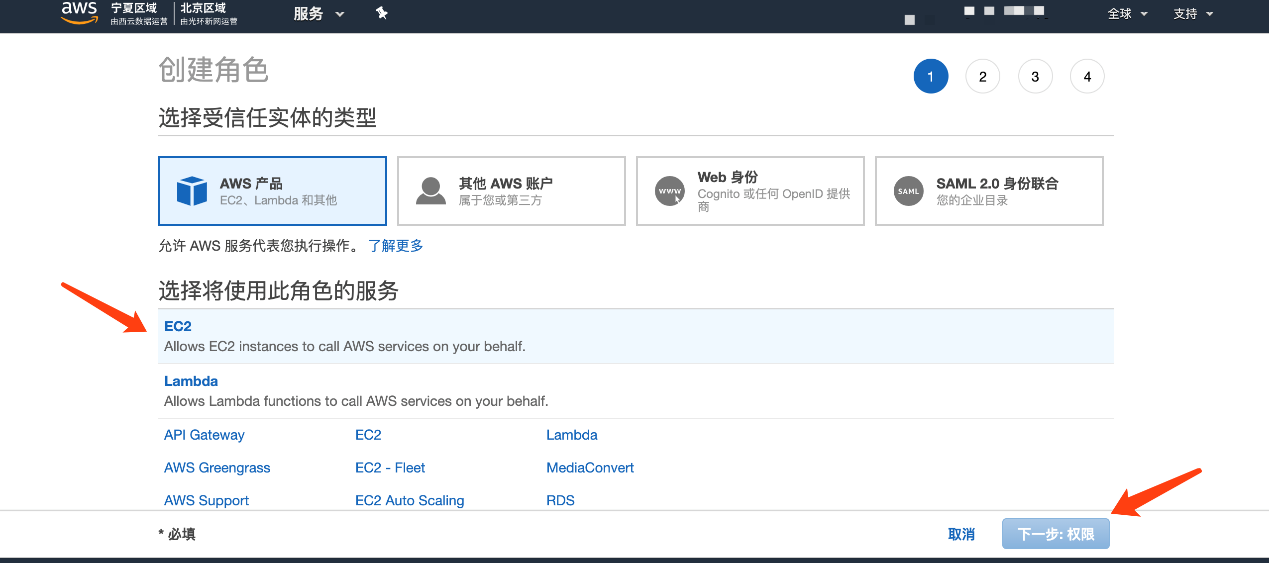
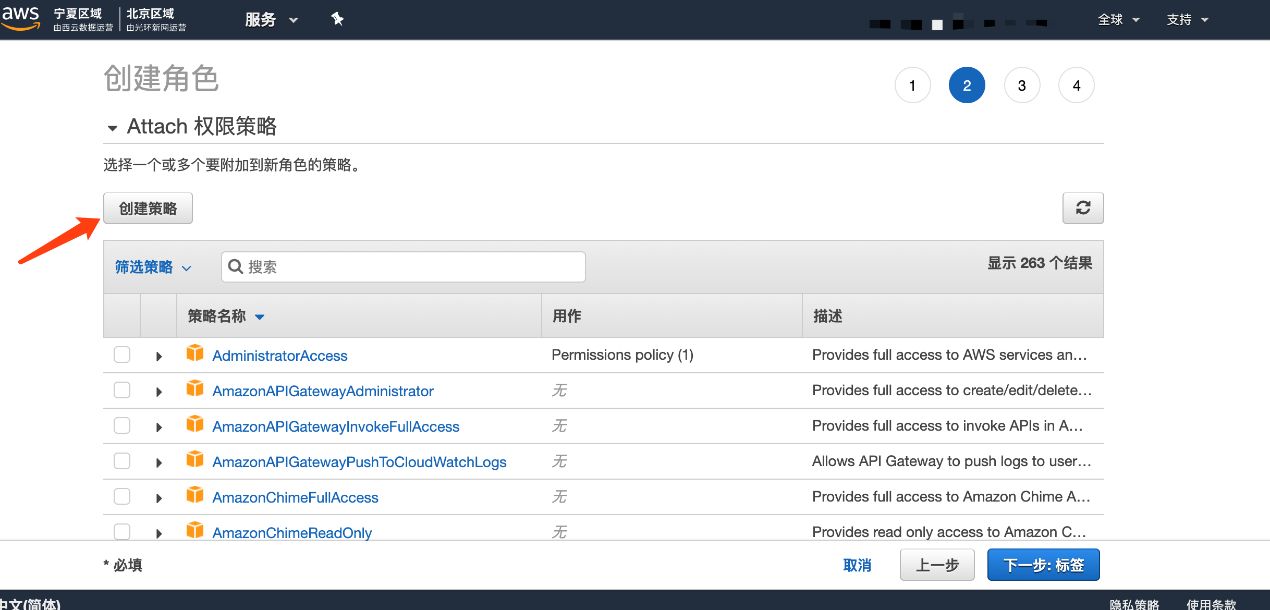
systemctl enable awslogsd

systemctl start awslogsd

如果服务已经运行，则

systemctl restart awslogsd



8、配置IAM角色，使EC2实例可以访问日志组。  
首先切换到IAM服务选择角色，然后点击【创建角色】  
  
随后选择将使用此角色的服务为EC2，点击【下一步】  
  
在此处，需要创建一个新的策略。点击【创建策略】，此时弹出一个新的窗口。  
  
选择json  
粘贴策略文本:

{

"Version": "2012-10-17",

"Statement": [

{

"Effect": "Allow",

"Action": [

"logs:CreateLogGroup",

"logs:CreateLogStream",

"logs:PutLogEvents",

"logs:DescribeLogStreams"

],

"Resource": [

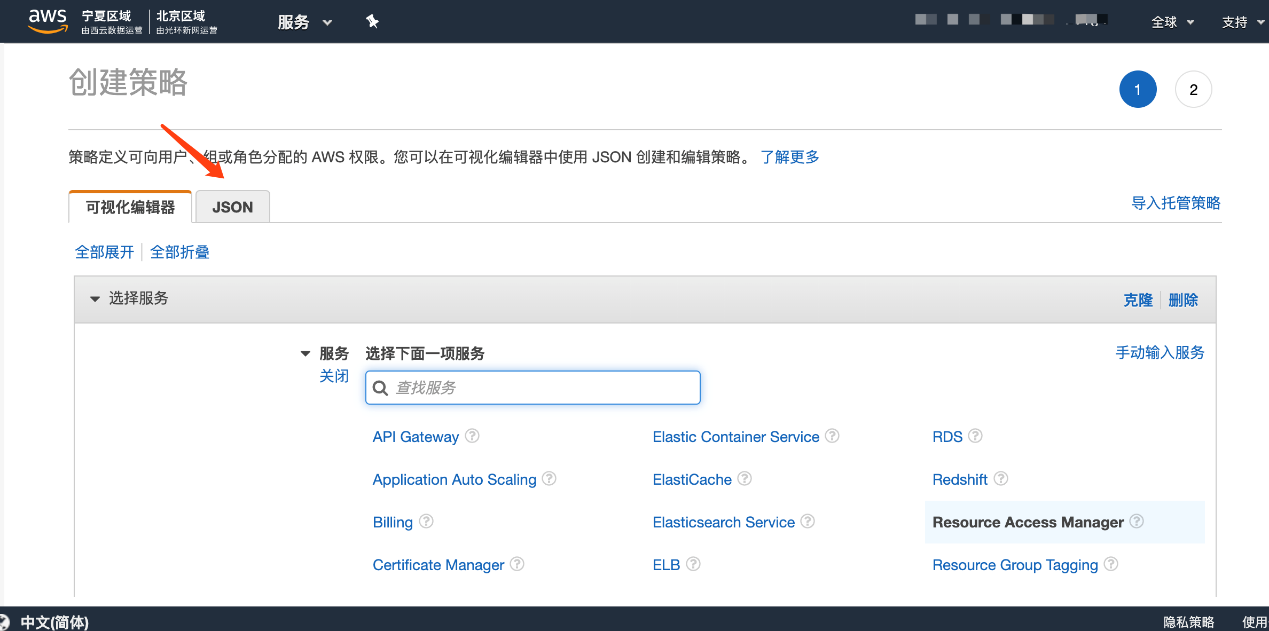
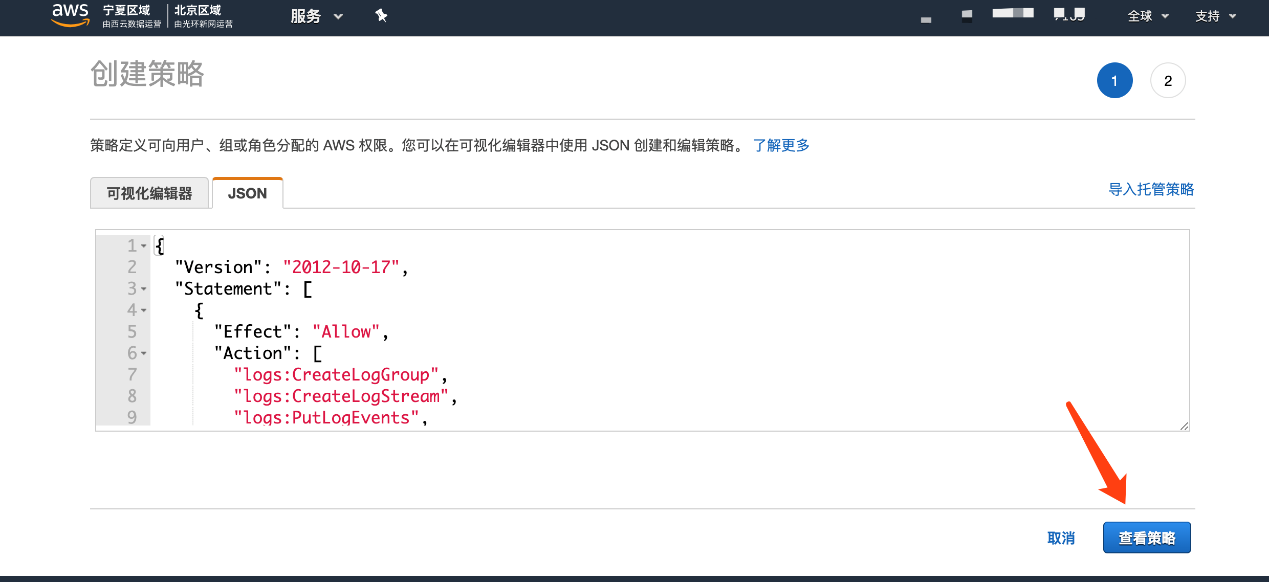
"arn:aws-cn:logs:\*:\*:\*"

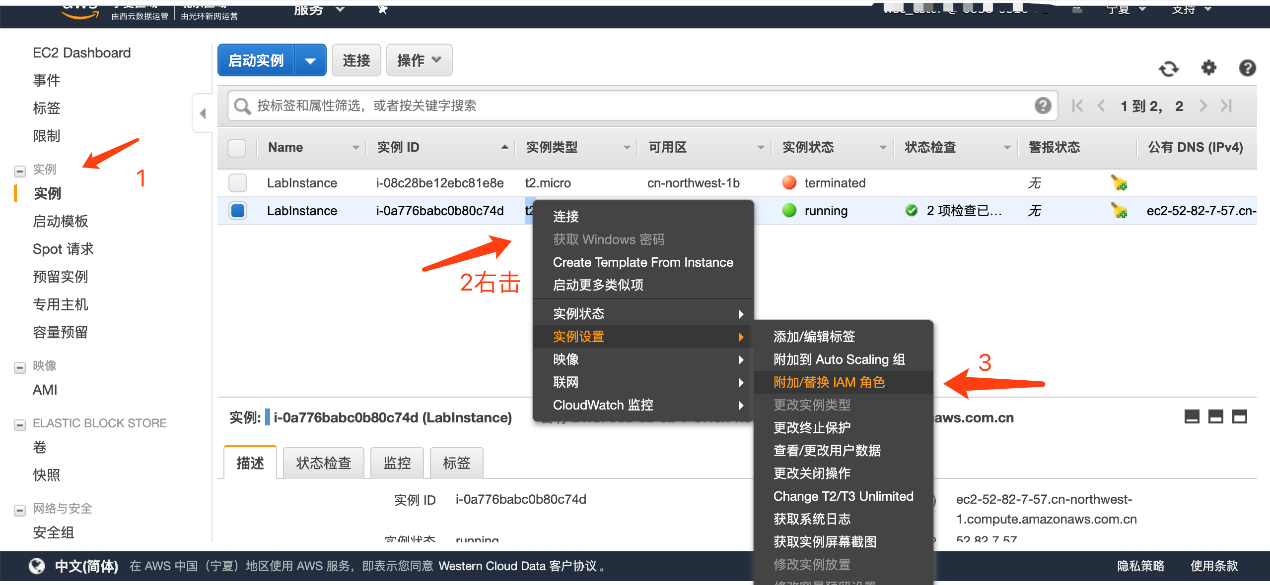
]

}

]

}

  
  
输入一个名称后点击【创建策略】  
  
  
之后我们切换回创建角色页面。刷新并搜索我们刚刚创建的策略。  
  
  
为新建的角色输入名称。点击【创建角色】  


9、切换服务到ec2。附加刚刚创建的角色。  
  
最后点击【应用】  


**实验结果**

切换到cloudwatch服务，选择【日志】，发现多了一条日志流  
  
内容为messages日志  
