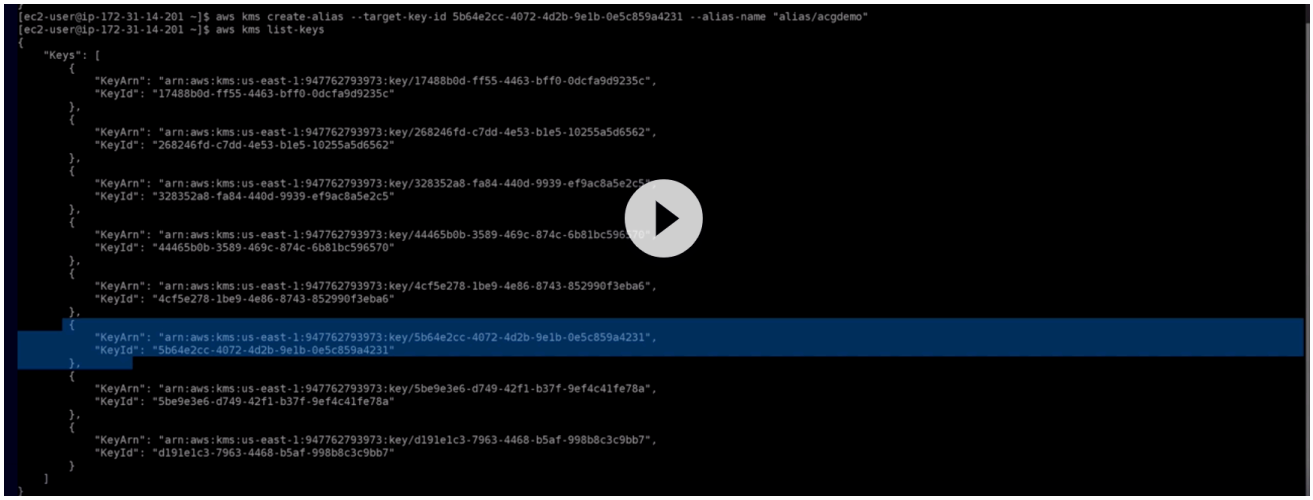
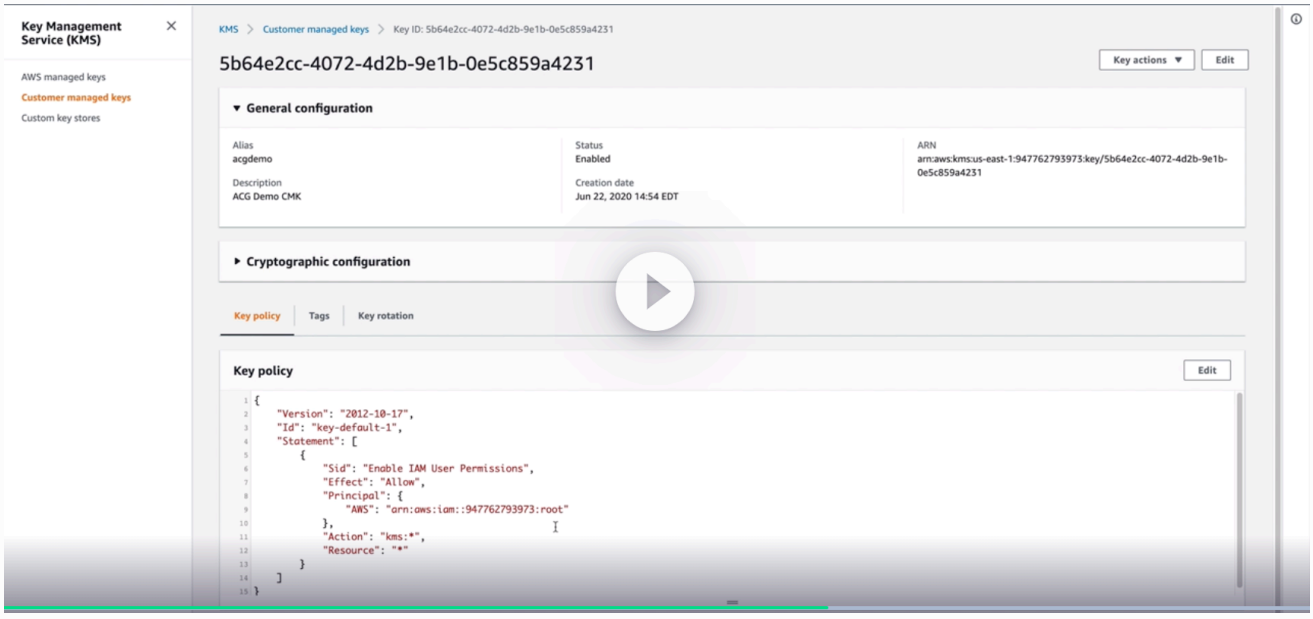
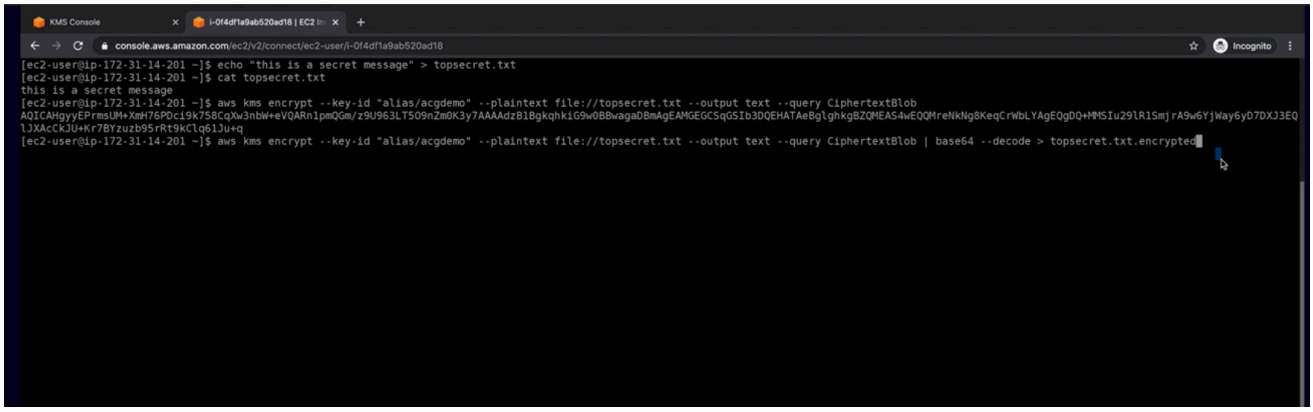
Security

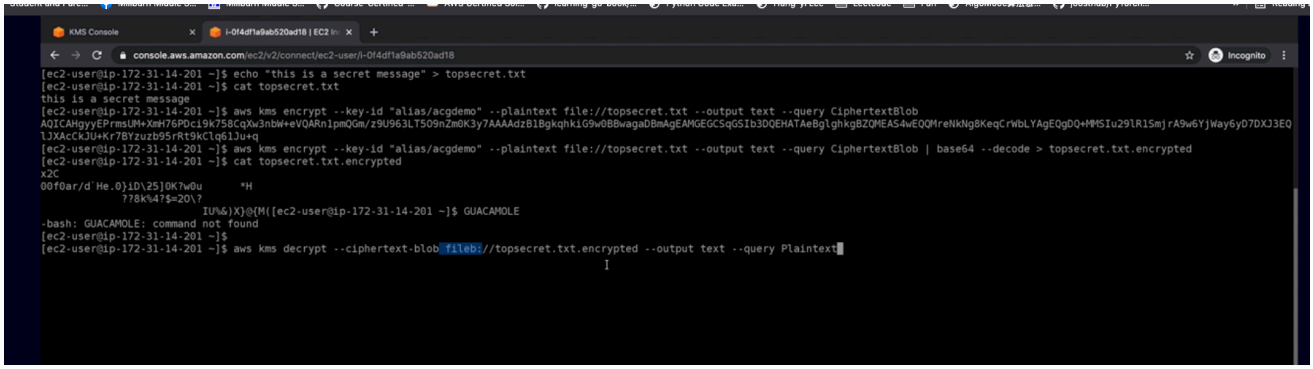

KMS Console
i-0f4df1a9ab520ad18 | EC2
console.aws.amazon.com/ec2/v2/connect/ec2-user/i-0f4df1a9ab520ad18
Incognito
[ec2-user@ip-172-31-14-201 ~]$ aws kms create-key --description "ACG Demo CMK"
{
"KeyMetadata": {
"Origin": "AWS_KMS",
"KeyId": "5b64e2cc-4072-4d2b-9e1b-0e5c859a4231",
"Description": "ACG Demo CMK",
"KeyManager": "CUSTOMER",
"EncryptionAlgorithms": [
"SYMMETRIC_DEFAULT"
],
"Enabled": true,
"CustomerMasterKeySpec": "SYMMETRIC_DEFAULT",
"KeyUsage": "ENCRYPT_DECRYPT",
"KeyState": "Enabled",
"CreationDate": 1592852045.65,
"Arn": "arn:aws:kms:us-east-1:947762793973:key/5b64e2cc-4072-4d2b-9e1b-0e5c859a4231",
"AWSAccountId": "947762793973"
}
}
[ec2-user@ip-172-31-14-201 ~]$

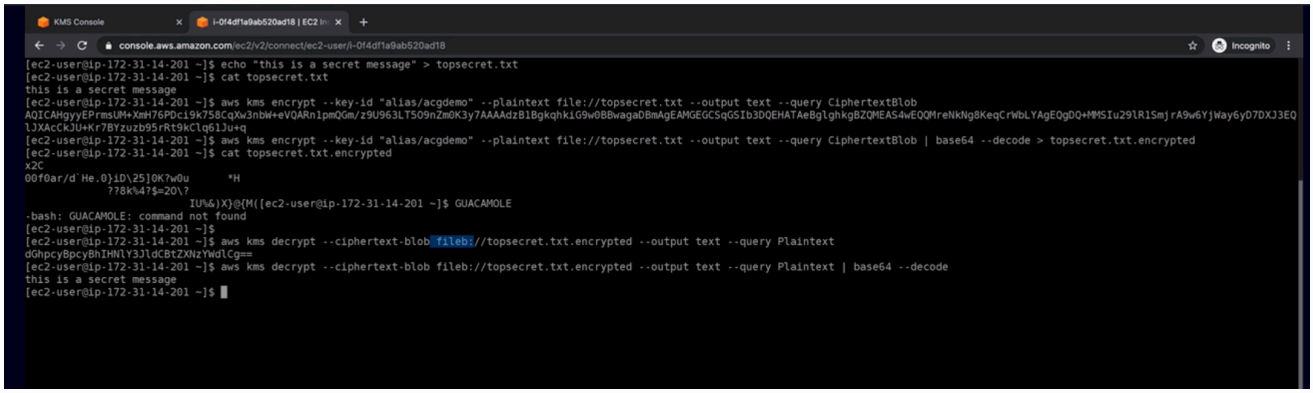

[ec2-user@ip-172-31-14-201 ~]$ aws kms create-alias --target-key-id 5b64e2cc-4072-4d2b-9e1b-0e5c859a4231 --alias-name "alias/acgdemo"
[ec2-user@ip-172-31-14-201 ~]$ aws kms list-keys
{
"Keys": [
{
"KeyArn": "arn:aws:kms:us-east-1:947762793973:key/17488b0d-ff55-4463-bff0-0dcfa9d9235c",
"KeyId": "17488b0d-ff55-4463-bff0-0dcfa9d9235c"
},
{
"KeyArn": "arn:aws:kms:us-east-1:947762793973:key/268246fd-c7dd-4e53-b1e5-10255a5d6562",
"KeyId": "268246fd-c7dd-4e53-b1e5-10255a5d6562"
},
{
"KeyArn": "arn:aws:kms:us-east-1:947762793973:key/328352a8-fa84-440d-9939-ef9ac8a5e2c5",
"KeyId": "328352a8-fa84-440d-9939-ef9ac8a5e2c5"
},
{
"KeyArn": "arn:aws:kms:us-east-1:947762793973:key/44465b0b-3589-469c-874c-6b81bc596570",
"KeyId": "44465b0b-3589-469c-874c-6b81bc596570"
},
{
"KeyArn": "arn:aws:kms:us-east-1:947762793973:key/4cf5e278-1be9-4e86-8743-852990f3eba6",
"KeyId": "4cf5e278-1be9-4e86-8743-852990f3eba6"
},
{
"KeyArn": "arn:aws:kms:us-east-1:947762793973:key/5b64e2cc-4072-4d2b-9e1b-0e5c859a4231",
"KeyId": "5b64e2cc-4072-4d2b-9e1b-0e5c859a4231"
},
{
"KeyArn": "arn:aws:kms:us-east-1:947762793973:key/5be9e3e6-d749-42f1-b37f-9ef4c41fe78a",
"KeyId": "5be9e3e6-d749-42f1-b37f-9ef4c41fe78a"
},
{
"KeyArn": "arn:aws:kms:us-east-1:947762793973:key/d191e1c3-7963-4468-b5af-998b8c3c9bb7",
"KeyId": "d191e1c3-7963-4468-b5af-998b8c3c9bb7"
}
]
}

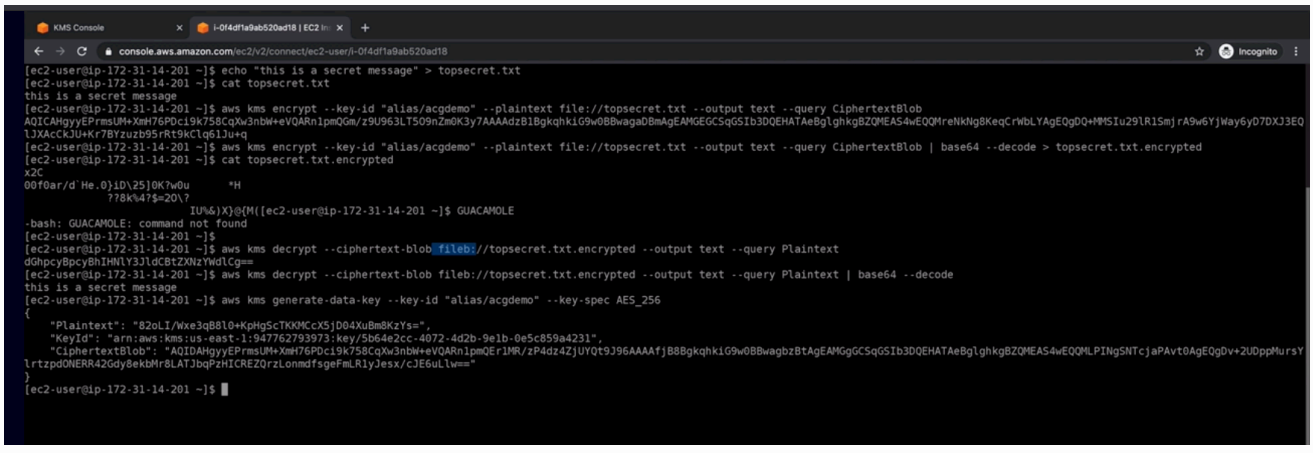

Key Management Service (KMS)
AWS managed keys
Customer managed keys
Custom key stores
KMS > Customer managed keys > Key ID: 5b64e2cc-4072-4d2b-9e1b-0e5c859a4231
5b64e2cc-4072-4d2b-9e1b-0e5c859a4231
Key actions
Edit
General configuration
Alias
acgdemo
Status
Enabled
ARN
arn:aws:kms:us-east-1:947762793973:key/5b64e2cc-4072-4d2b-9e1b-0e5c859a4231
Description
ACG Demo CMK
Creation date
Jun 22, 2020 14:54 EDT
Cryptographic configuration
Key policy
Tags
Key rotation
Key policy
Edit
{
"Version": "2012-10-17",
"Id": "key-default-1",
"Statement": [
{
"Sid": "Enable IAM User Permissions",
"Effect": "Allow",
"Principal": {
"AWS": "arn:aws:iam::947762793973:root"
},
"Action": "kms:*",
"Resource": "*"
}
]
}


KMS Console
i-0f4df1a9ab520ad18 | EC2
console.aws.amazon.com/ec2/v2/connect/ec2-user/i-0f4df1a9ab520ad18
Incognito
[ec2-user@ip-172-31-14-201 ~]$ echo "this is a secret message" > topsecret.txt
[ec2-user@ip-172-31-14-201 ~]$ cat topsecret.txt
this is a secret message
[ec2-user@ip-172-31-14-201 ~]$ aws kms encrypt --key-id "alias/acgdemo" --plaintext file://topsecret.txt --output text --query CiphertextBlob


KMS Console
i-0f4df1a9ab520ad18 | EC2
console.aws.amazon.com/ec2/v2/connect/ec2-user/i-0f4df1a9ab520ad18
Incognito
[ec2-user@ip-172-31-14-201 ~]$ echo "this is a secret message" > topsecret.txt
[ec2-user@ip-172-31-14-201 ~]$ cat topsecret.txt
this is a secret message
[ec2-user@ip-172-31-14-201 ~]$ aws kms encrypt --key-id "alias/acgdemo" --plaintext file://topsecret.txt --output text --query CiphertextBlob
AQICAHgyyEPrmsUM+XmH76PDci9k758CqXw3nbW+eVQARn1pmQGm/z9U963LT5O9nZm0K3y7AAAAdzB1BgkqhkiG9w0BBwagaDBmAgEAMGEGCSqGSIb3DQEHATAeBglghkgBZQMEAS4wEQQMreNkNg8KeqCrWbLYAgEQgDQ+MMSIu29lR1SmjrA9w6YjWay6yD7DXJ3EQ
lJXAcCkJU+Kr7BYzuzb95rRt9kClq61Ju+q
[ec2-user@ip-172-31-14-201 ~]$ aws kms encrypt --key-id "alias/acgdemo" --plaintext file://topsecret.txt --output text --query CiphertextBlob | base64 --decode > topsecret.txt.encrypted


KMS Console
i-0f4df1a9ab520ad18 | EC2
console.aws.amazon.com/ec2/v2/connect/ec2-user/i-0f4df1a9ab520ad18
Incognito
[ec2-user@ip-172-31-14-201 ~]$ echo "this is a secret message" > topsecret.txt
[ec2-user@ip-172-31-14-201 ~]$ cat topsecret.txt
this is a secret message
[ec2-user@ip-172-31-14-201 ~]$ aws kms encrypt --key-id "alias/acgdemo" --plaintext file://topsecret.txt --output text --query CiphertextBlob
AQICAHgyyEPrmsUM+XmH76PDci9k758CqXw3nbW+eVQARn1pmQGm/z9U963LT5O9nZm0K3y7AAAAdzB1BgkqhkiG9w0BBwagaDBmAgEAMGEGCSqGSIb3DQEHATAeBglghkgBZQMEAS4wEQQMreNkNg8KeqCrWbLYAgEQgDQ+MMSIu29lR1SmjrA9w6YjWay6yD7DXJ3EQ
lJXAcCkJU+Kr7BYzuzb95rRt9kClq61Ju+q
[ec2-user@ip-172-31-14-201 ~]$ aws kms encrypt --key-id "alias/acgdemo" --plaintext file://topsecret.txt --output text --query CiphertextBlob | base64 --decode > topsecret.txt.encrypted
[ec2-user@ip-172-31-14-201 ~]$ cat topsecret.txt.encrypted
x2C
00f0ar/d`He.0}iD\25]0K?w0u *H
??8k%4?$=2O\?
IU%&)X}@{M([ec2-user@ip-172-31-14-201 ~]$ GUACAMOLE
-bash: GUACAMOLE: command not found
[ec2-user@ip-172-31-14-201 ~]$
[ec2-user@ip-172-31-14-201 ~]$ aws kms decrypt --ciphertext-blob fileb://topsecret.txt.encrypted --output text --query Plaintext


KMS Console
i-0f4df1a9ab520ad18 | EC2
console.aws.amazon.com/ec2/v2/connect/ec2-user/i-0f4df1a9ab520ad18
Incognito
[ec2-user@ip-172-31-14-201 ~]$ echo "this is a secret message" > topsecret.txt
[ec2-user@ip-172-31-14-201 ~]$ cat topsecret.txt
this is a secret message
[ec2-user@ip-172-31-14-201 ~]$ aws kms encrypt --key-id "alias/acgdemo" --plaintext file://topsecret.txt --output text --query CiphertextBlob
AQICAHgyyEPrmsUM+XmH76PDci9k758CqXw3nbW+eVQARn1pmQGm/z9U963LT5O9nZm0K3y7AAAAdzB1BgkqhkiG9w0BBwagaDBmAgEAMGEGCSqGSIb3DQEHATAeBglghkgBZQMEAS4wEQQMreNkNg8KeqCrWbLYAgEQgDQ+MMSIu29lR1SmjrA9w6YjWay6yD7DXJ3EQ
lJXAcCkJU+Kr7BYzuzb95rRt9kClq61Ju+q
[ec2-user@ip-172-31-14-201 ~]$ aws kms encrypt --key-id "alias/acgdemo" --plaintext file://topsecret.txt --output text --query CiphertextBlob | base64 --decode > topsecret.txt.encrypted
[ec2-user@ip-172-31-14-201 ~]$ cat topsecret.txt.encrypted
x2C
00f0ar/d`He.0}iD\25]0K?w0u *H
??8k%4?$=2O\?
IU%&)X}@{M([ec2-user@ip-172-31-14-201 ~]$ GUACAMOLE
-bash: GUACAMOLE: command not found
[ec2-user@ip-172-31-14-201 ~]$
[ec2-user@ip-172-31-14-201 ~]$ aws kms decrypt --ciphertext-blob fileb://topsecret.txt.encrypted --output text --query Plaintext
dGhpcyBpcyBhIHNlY3JldCBtZXNzYWdlCg==
[ec2-user@ip-172-31-14-201 ~]$ aws kms decrypt --ciphertext-blob fileb://topsecret.txt.encrypted --output text --query Plaintext | base64 --decode
this is a secret message
[ec2-user@ip-172-31-14-201 ~]$


KMS Console
i-0f4df1a9ab520ad18 | EC2
console.aws.amazon.com/ec2/v2/connect/ec2-user/i-0f4df1a9ab520ad18
Incognito
[ec2-user@ip-172-31-14-201 ~]$ echo "this is a secret message" > topsecret.txt
[ec2-user@ip-172-31-14-201 ~]$ cat topsecret.txt
this is a secret message
[ec2-user@ip-172-31-14-201 ~]$ aws kms encrypt --key-id "alias/acgdemo" --plaintext file://topsecret.txt --output text --query CiphertextBlob
AQICAHgyyEPrmsUM+XmH76PDci9k758CqXw3nbW+eVQARn1pmQGm/z9U963LT5O9nZm0K3y7AAAAdzB1BgkqhkiG9w0BBwagaDBmAgEAMGEGCSqGSIb3DQEHATAeBglghkgBZQMEAS4wEQQMreNkNg8KeqCrWbLYAgEQgDQ+MMSIu29lR1SmjrA9w6YjWay6yD7DXJ3EQ
lJXAcCkJU+Kr7BYzuzb95rRt9kClq61Ju+q
[ec2-user@ip-172-31-14-201 ~]$ aws kms encrypt --key-id "alias/acgdemo" --plaintext file://topsecret.txt --output text --query CiphertextBlob | base64 --decode > topsecret.txt.encrypted
[ec2-user@ip-172-31-14-201 ~]$ cat topsecret.txt.encrypted
x2C
00f0ar/d`He.0}iD\25]0K?w0u *H
??8k%4?$=2O\?
IU%&)X}@{M([ec2-user@ip-172-31-14-201 ~]$ GUACAMOLE
-bash: GUACAMOLE: command not found
[ec2-user@ip-172-31-14-201 ~]$
[ec2-user@ip-172-31-14-201 ~]$ aws kms decrypt --ciphertext-blob fileb://topsecret.txt.encrypted --output text --query Plaintext
dGhpcyBpcyBhIHNlY3JldCBtZXNzYWdlCg==
[ec2-user@ip-172-31-14-201 ~]$ aws kms decrypt --ciphertext-blob fileb://topsecret.txt.encrypted --output text --query Plaintext | base64 --decode
this is a secret message
[ec2-user@ip-172-31-14-201 ~]$ aws kms generate-data-key --key-id "alias/acgdemo" --key-spec AES_256
{
"Plaintext": "82oLI/Wxe3qB8l0+KpHgScTKKMCcX5jD04XuBm8KzYs=",
"KeyId": "arn:aws:kms:us-east-1:947762793973:key/5b64e2cc-4072-4d2b-9e1b-0e5c859a4231",
"CiphertextBlob": "AQIDAHgyyEPrmsUM+XmH76PDci9k758CqXw3nbW+eVQARn1pmQEr1MR/zP4dz4ZjUYQt9J96AAAAfjB8BgkqhkiG9w0BBwagbzBtAgEAMGgGCSqGSIb3DQEHATAeBglghkgBZQMEAS4wEQQMLPINgSNTcjaPAvt0AgEQgDv+2UDppMursY
lrtzpdONERR42Gdy8ekbMr8LATJbqPzHICREZQrzLonmdfsgeFmLR1yJesx/cJE6uLlw=="
}
[ec2-user@ip-172-31-14-201 ~]$