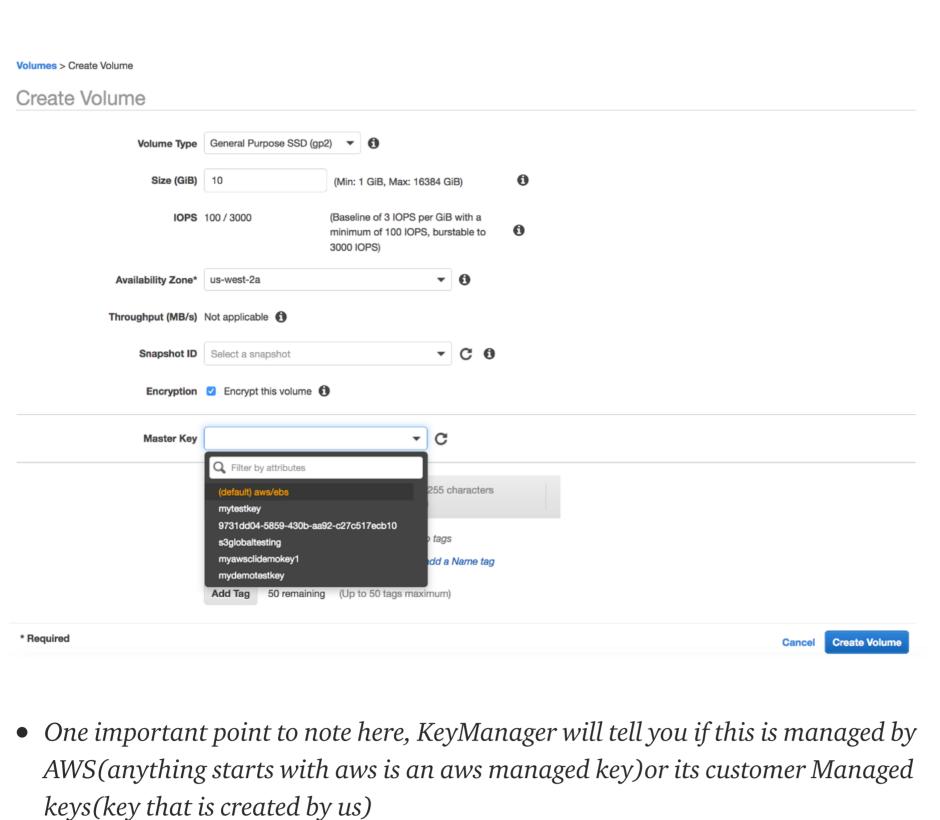


100 Days of DevOps — Day 23- How to encrypt Welcome to Day 23 of 100 Days of DevOps, Let continue our journey with terraform

How it's integrated with particular service is service specific, the responsibility of KMS is to generate Customer Master Key(CMK) and Data Keys and then handover Data Key to that Particular service at this point KMS responsibility ends

**Encrypt EBS Volume using KMS Key** 

AWS Console --> EC2 --> ELASTIC BLOCK STORE --> Volumes --> Create Volume



If you go back to the Volume, you will see something like this

\* Check the Encryption tab

To summarize this how it works

```
<u>GenerateDataKeyWithoutPlaintext</u> request to AWS KMS, specifying the CMK
   that you chose for EBS volume encryption.
2. AWS KMS generates a new data key, encrypts it under the specified CMK, and
   then sends the encrypted data key to Amazon EBS to store with the volume
   metadata.
```

1. When you create an encrypted EBS volume, Amazon EBS sends a

the encrypted data key to AWS KMS with a <u>Decrypt</u> request.

(plaintext) data key to Amazon EC2.

4. AWS KMS decrypts the encrypted data key and then sends the decrypted

- 5. Amazon EC2 uses the plaintext data key in hypervisor memory to encrypt disk I/O to the EBS volume. The plaintext data key persists in memory as long as the EBS volume is attached to the EC2 instance.
- **Terraform Code**

## region = "us-west-2" 3 }

size

type

# Some changes

the below medium.

medium.com

Your email

1XGCP

Mar 4, 2019

provider "aws" {

*NOTE:* 

```
encrypted
                         = true
10
       kms_key_id
                         = "${var.kms_key}"
11 }
kms_ebs.tf hosted with \(\varphi\) by GitHub
                                                                                      view raw
• Most of the EBS code, I already explained in the EBS section
 100 Days of DevOps — Day 17- Creating EC2 Instance using
 Terraform
 Welcome to Day 17 of 100 Days of DevOps, Let continue our journey,
 so far I havr discussed terraform fundamentals and...
```

parameter Encrypted to be set.

\* encrypted: This is required to encrypt the disk \* kms\_key\_id: The ARN for the KMS encryption key

```
• Twitter: @100daysofdevops OR @lakhera2015
• Facebook: <a href="https://www.facebook.com/groups/795382630808645/">https://www.facebook.com/groups/795382630808645/</a>
• Medium: <u>https://medium.com/@devopslearning</u>
```

- Reference
- 100 Days of DevOps Day 0 D-day is just one day away and finally, this is a continuation of the post(I posted a month earlier)

Get an email whenever Prashant Lakhera publishes.

100 Days of DevOps — Day 22-Introduction to Key **Management System(KMS)** Welcome to Day 22 of 100 Days of DevOps, Let continue our journey with

Mar 3, 2019

100 Days of DevOps — Day 21- MySQL RDS Database Creation using **Terraform** Welcome to Day 21 of 100 Days of DevOps, Let continue our journey with terraform and today we

Mar 2, 2019

100 Days of DevOps — Day 20— Auto-Scaling

**Group using Terraform** 

Mar 1, 2019

AWS 3 min read

Welcome to Day 20 of 100 Days of DevOps, Let continue our terraform journey, yesterday we created an application load balancer, let expand th...

100 Days of DevOps — Day 19 - Application Load **Balancer using Terraform** 

Cloud Computing 4 min read Feb 28, 2019

using Terraform(CloudWatch and SNS) Check the updated 101 Days of DevOps Course Course Registration link: https://www.101daysofdevops.com/register/ Course Link:...

100 Days of DevOps — Day 18-Add monitoring to these instances

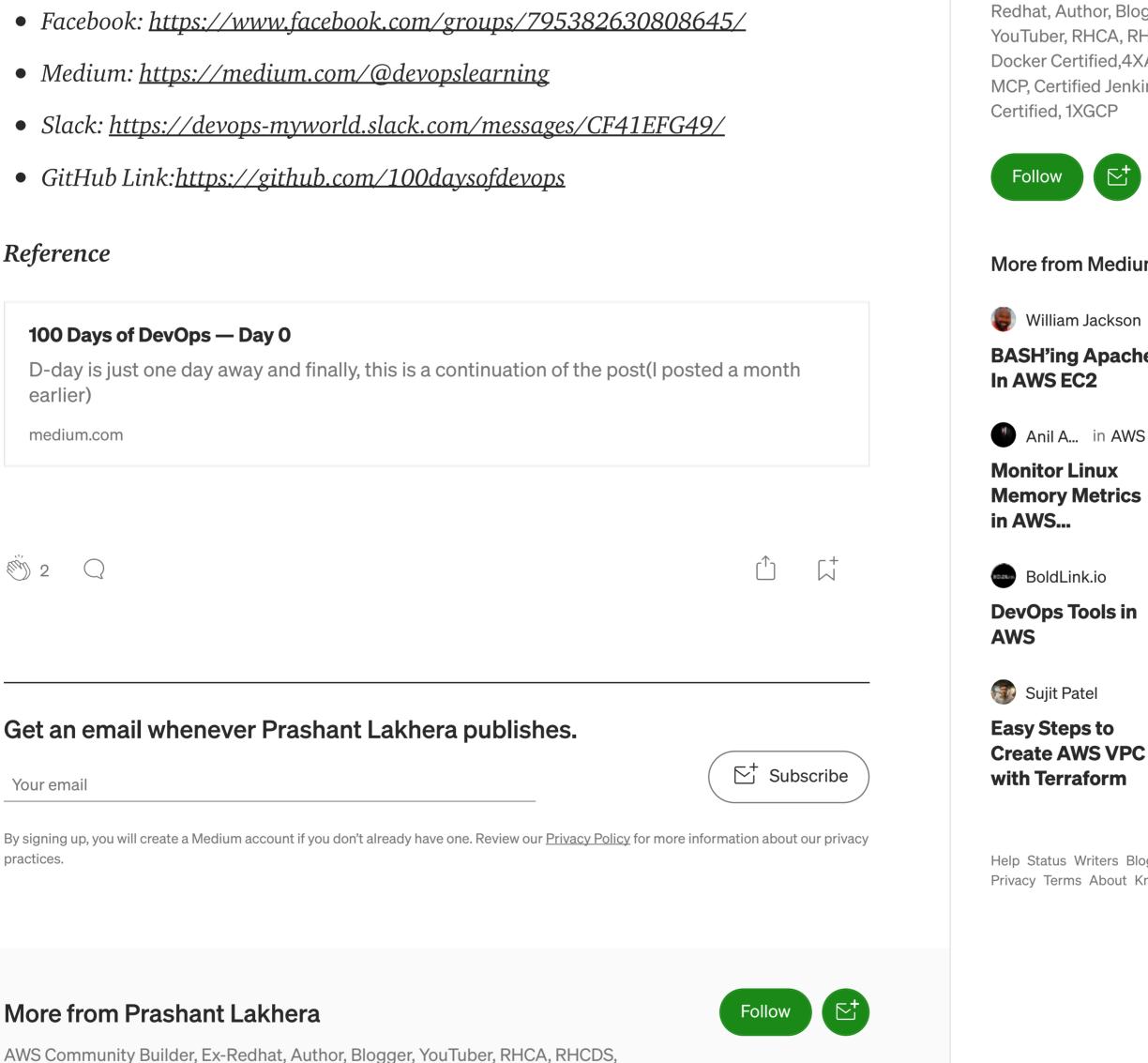
Love podcasts or audiobooks? Learn on the go with our new app. Try Knowable

Get started Q Search **Prashant Lakhera** 4.7K Followers AWS Community Builder, Ex-Redhat, Author, Blogger, YouTuber, RHCA, RHCDS, RHCE, Docker Certified, 4XAWS, CCNA, MCP, Certified Jenkins, Terraform Certified, 1XGCP More from Medium William Jackson **BASH'ing Apache** In AWS EC2 Anil A... in AWS ... **Monitor Linux Memory Metrics** in AWS... BoldLink.io **DevOps Tools in** 

Sign In

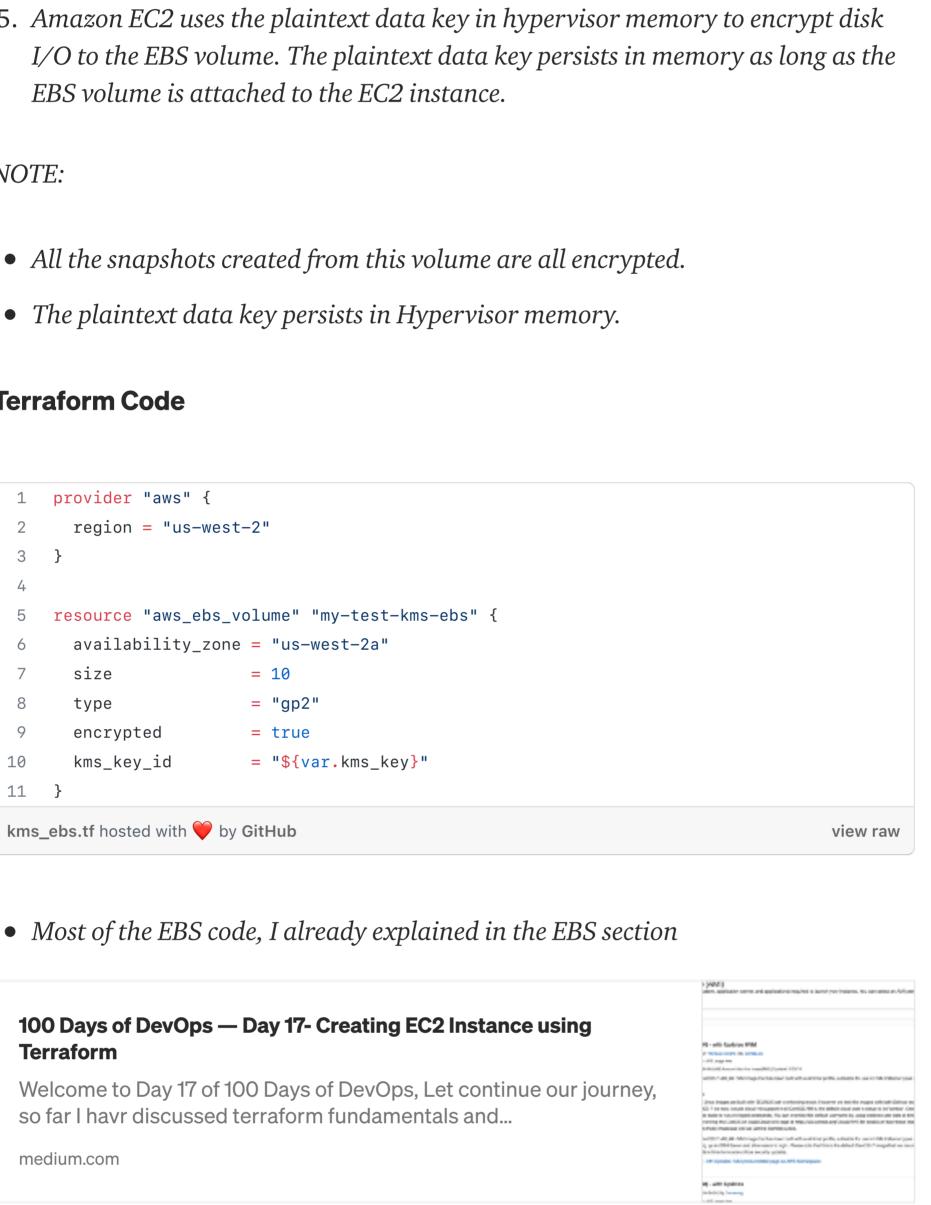
**APACHI** 

with Terraform Help Status Writers Blog Careers Privacy Terms About Knowable



 $\Box$ 

Auto Scaling group



2018-10-05 18:35 PST 2018-12-24 12:26 PST 2018-11-28 14:39 PST 2017-12-26 15:06 PST 2018-04-04 16:09 PST \* Under Master Key(Select the KMS we just created from the drop down)

\_ \_ \_

5648f699-12dd-4b9b-b040-8a110e79f6ca e7ba51c5-5ea4-43e5-8ae1-6a2a3162cf80 Enabled 50d7fea6-1ce4-4242-bbe0-dfc10ba6ac7d 4885ca03-c48b-484a-95ca-8b12e602c793 cc77aa20-b465-49bf-b216-23d76f4186e5 Enabled

KMS Key ID fcda51da-16bb-44fd-aeab-c2dda41b84d2

Volumes: vol-099ae24ffb3eb8b04 Created December 24, 2018 at 12:29:30 PM UTC-8

3. When you attach the encrypted volume to an EC2 instance, Amazon EC2 sends

• *The plaintext data key persists in Hypervisor memory.* 

resource "aws\_ebs\_volume" "my-test-kms-ebs" { availability\_zone = "us-west-2a"

= 10

= "gp2"

medium.com

\* aws\_ebs\_volume.my-test-kms-ebs: Error creating EC2 volume: InvalidParameterDependency: The parameter [KmsKeyId] requires the status code: 400, request id: feeb7131-82ea-48d2-854e-84e4fbb7e5e1

Looking forward from you guys to join this journey and spend a minimum an hour

every day for the next 100 days on DevOps work and post your progress using any of

NOTE: encrypted parameter is mandatory to set, else you will run into this error

• Slack: <a href="https://devops-myworld.slack.com/messages/CF41EFG49/">https://devops-myworld.slack.com/messages/CF41EFG49/</a> • *GitHub Link:*<u>https://github.com/100daysofdevops</u>

£179 2

practices. More from Prashant Lakhera **Follow** AWS Community Builder, Ex-Redhat, Author, Blogger, YouTuber, RHCA, RHCDS, RHCE, Docker Certified, 4XAWS, CCNA, MCP, Certified Jenkins, Terraform Certified,

K AWS 5 min read Share your ideas with millions of readers. Write on Medium

terraform and today we are going to create KMS keys using terraform....

are going to create MySql database using terraform What Is Amazon Relational Database Service... AWS 3 min read

 $\Box$ AWS 4 min read

Welcome to Day 19 of 100 Days of DevOps, Let continue our terraform journey and see how can we create Application Load Balancer using... K

 $\Box$