AWS re:Invent

CMP420-R2

Amazon EBS: Security best practices

Sandeep Kumar
Sr. SDE
Amazon Web Services

AWS re:Invent

aws

Agenda

Resource level-permissions

Encrypting Amazon Elastic Block Store (Amazon EBS) resources

Demo/Hands-on sessions

- Launching instances with encrypted boot volume
- Enabling encryption by default
- Protecting Amazon EBS snapshots from accidental public sharing

Q&A

Resource-level permissions

- Create scoped permissions for users and roles
- Allow specific actions; deny is default
- Scope permissions to specific resources

Encrypt Amazon EBS Resources

- Encrypt Amazon EBS resources by default
- Set account-level encryption setting (regional)
- Choose an AWS Key Management Service key for default encryption
  - AWS managed key
  - Customer managed key

Builder session worksheet

Please download this PDF document:

https://builder-session.s3.amazonaws.com/EBS-Builder-Session.pdf

Demo:
Launching instance with encrypted boot volume

Launch instance with encrypted boot volume

```
1. aws ec2 describe-images --image-ids "ami-00dc79254d0461090”

2. aws ec2 run-instances
--image-id "ami-00dc79254d0461090”
--count 1
--instance-type m4.large
--region us-east-1
--key-name <EC2 key name>
--block-device-mappings file://block-device-mapping.json


3. aws ec2 describe-volumes
--filters "Name=attachment.instance-id,Values=<instance id>"
```

```
Block-device-mapping file contents are
[
  {
    "DeviceName": "/dev/xvda",
    "Ebs": {
      "Encrypted": true,
      "KmsKeyId": ”KMS Key ARN”
    }
  }
]


#add security group with --security-group-ids
```

Demo:
Enable Amazon EBS encryption by default

AWS re:Invent

aws

Enable Amazon EBS encryption by default

```
#EBS Encryption Settings are Regional

1. #Change Default Key

aws ec2 modify-ebs-default-kms-key-id

--kms-key-id <KMS Key ARN>


2. #Enable Encryption by Default

aws ec2 enable-ebs-encryption-by-default
```

```
#Encryption by Default APIs

enable-ebs-encryption-by-default

get-ebs-encryption-by-default

disable-ebs-encryption-by-default


#EBS Default key APIs

modify-ebs-default-kms-key-id

get-ebs-default-kms-key-id

reset-ebs-default-kms-key-id
```

Enable encryption by default

```
aws ec2 run-instances
--image-id "ami-00dc79254d0461090”
--count 1
--instance-type m4.large
--region us-east-1
--block-device-mappings
--key-name <EC2 key name>


#Validate the encryption state

aws ec2 describe-volumes
--filters "Name=attachment.instance-
id,Values=<instance id>”



#Disable default encryption

disable-ebs-encryption-by-default
```

```
#add security group with --security-
group-ids
```

Demo:
Protecting Amazon EBS snapshots from accidental public sharing

AWS re:Invent

aws

Safeguarding Amazon EBS snapshots from public sharing

1. Make a snapshot public

```
aws ec2 modify-snapshot-attribute --snapshot-id <SnapshotId> \
--attribute createVolumePermission --operation-type add --group-names all
```

2. Describe public snapshots owned by you

```
aws ec2 describe-snapshots --restorable-by-user-ids all \
--region us-east-1 | jq '.Snapshots[] | .OwnerId + ", " + .SnapshotId' | grep ‘your
account id’
```

3. Remove the public access to snapshot

```
aws ec2 modify-snapshot-attribute --snapshot-id <SnapshotId> \
--attribute createVolumePermission --operation-type remove --group-names all
```

Safeguarding Amazon EBS Snapshots from public sharing

1. Create policy

```
aws iam create-policy --policy-name
BuilderSnapshotAccess --policy-document
file://modify-snapshot-attribute.json
```

2. Attach the policy to the user

```
aws iam attach-user-policy --user-name
<user name> --policy-arn <policy arn>
```

3. Attempt to share the snapshot again

```
aws ec2 modify-snapshot-attribute --
snapshot-id <Snapshot Id> --attribute
createVolumePermission --operation-type
add --group-names all
```

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "StandardAccess01",
            "Effect": "Deny",
            "Action":
"ec2:ModifySnapshotAttribute",
            "Resource": "*"
        }
    ]
}
```

Remember:

Clean up all resources to avoid future charges

Thank you!

Sandeep Kumar

sdk@amazon.com

AWS re:Invent

aws

Please complete the session survey in the mobile app.