
AWS
re:Invent

STG303-R

Deep Dive on Amazon Elastic Block Store

Marc Olson
Principal Engineer
Amazon EBS

Ashish Palekar
Product Manager
Amazon EBS

AWS re:Invent

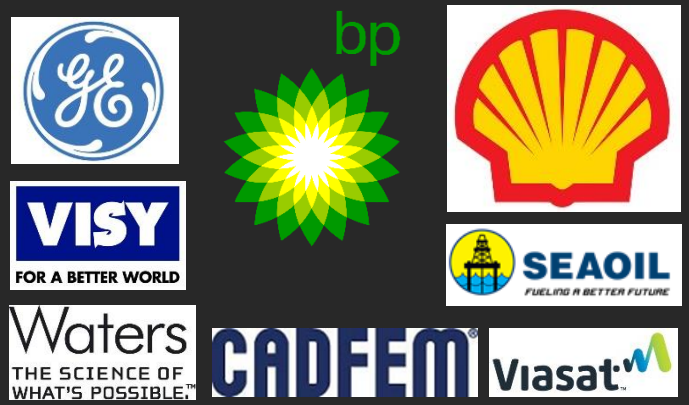
aws

Consumer

Enterprise Technology

Financial Services / Real Estate

Oil & Gas / Manufacturing / Telecom



Media & Gaming

Govt. / Education / Healthcare

Agenda for the session

Security and Encryption with EBS

Performance Best Practices for EBS

Availability / Durability for EBS

Saving Cost with EBS

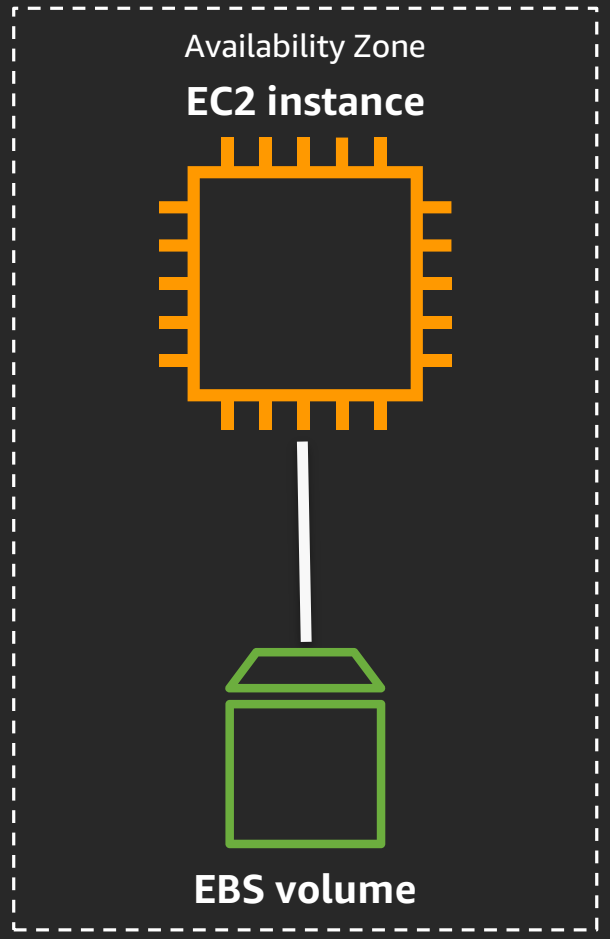
How a customer uses EBS – Teradata

Security and Encryption with EBS

AWS re:Invent

aws

Encryption – Amazon EBS



Integrates with Amazon Key Management Service (KMS) – AES-256 Encryption

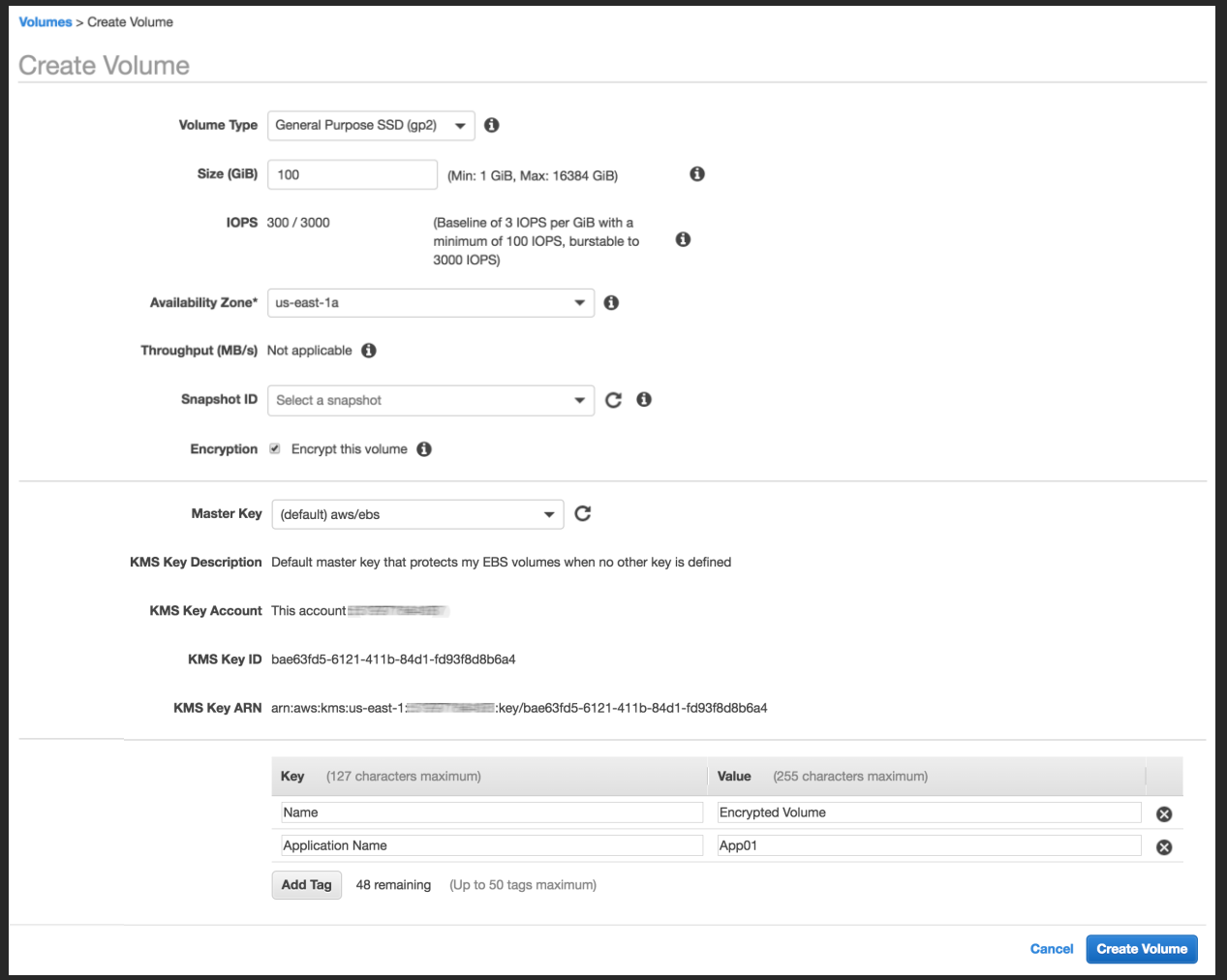
Uses Customer Master Keys (CMKs)

Encrypted EBS volume implies the following are encrypted:

- Data at rest inside the volume
- Data moving between the volume and instance
- Snapshots created from the volume
- Volumes created from such snapshots

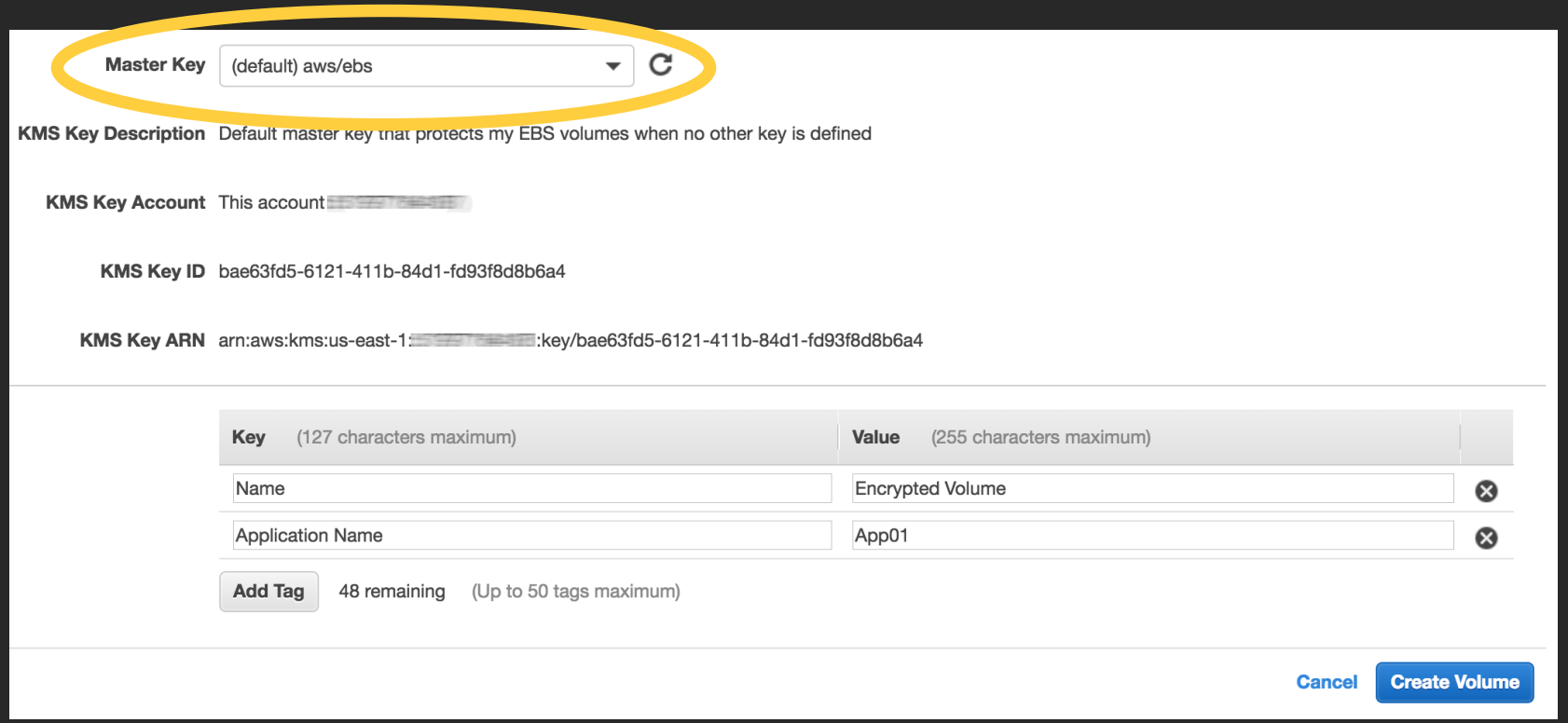
EBS Volume encryption

EBS encryption:
data volumes

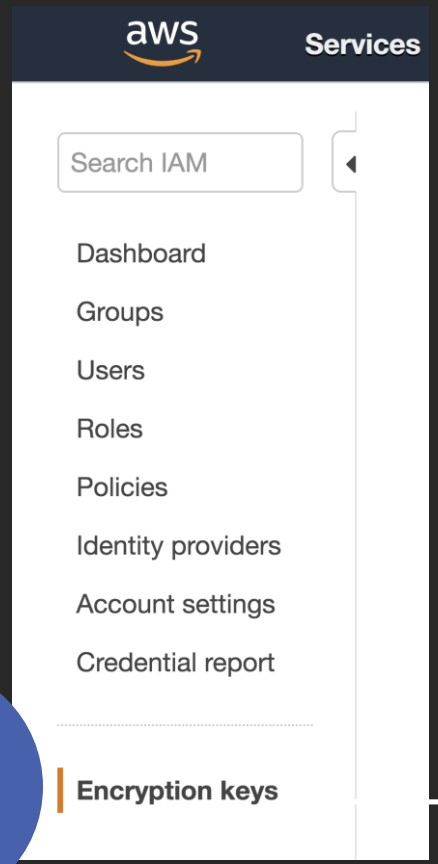


EBS Volume encryption

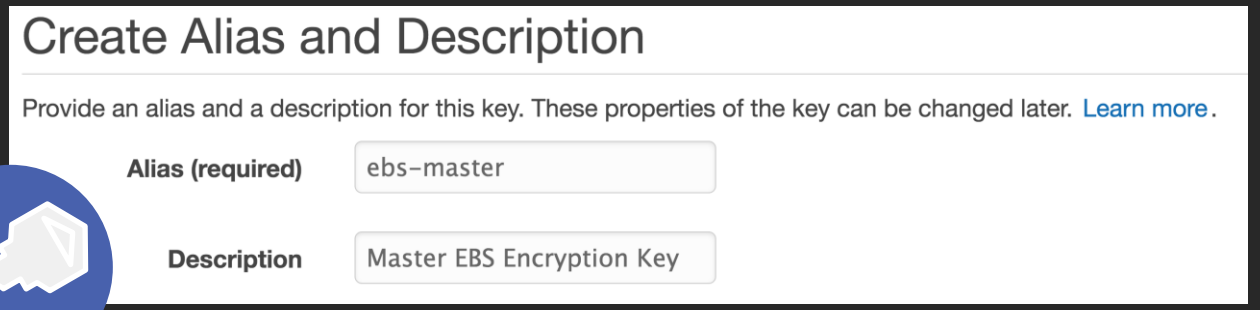
EBS encryption:
data volumes



EBS Volume encryption



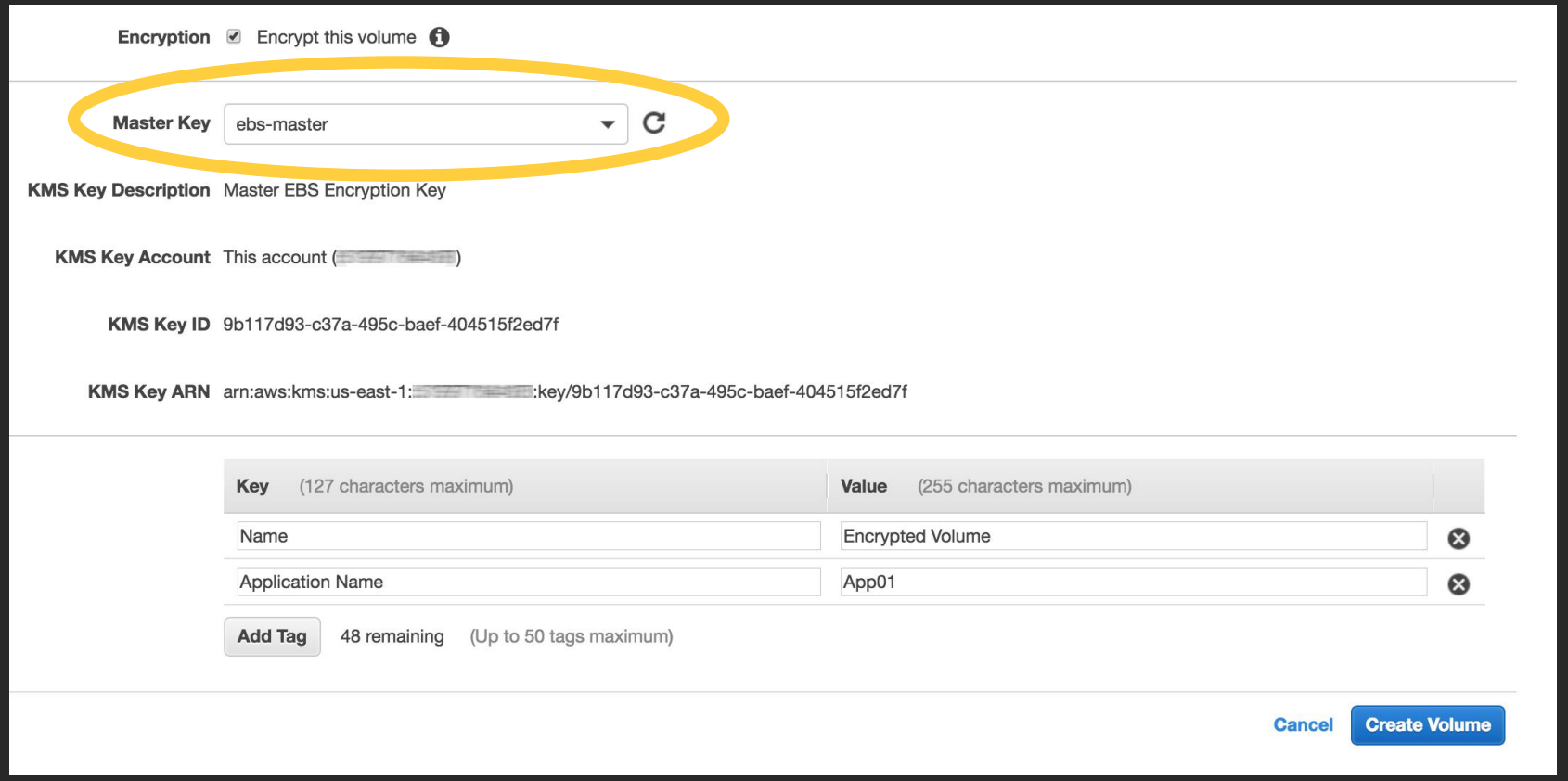
Create a new AWS KMS master key for EBS



- Define key rotation policy
- Enable AWS CloudTrail auditing
- Control who can use key
- Control who can administer key

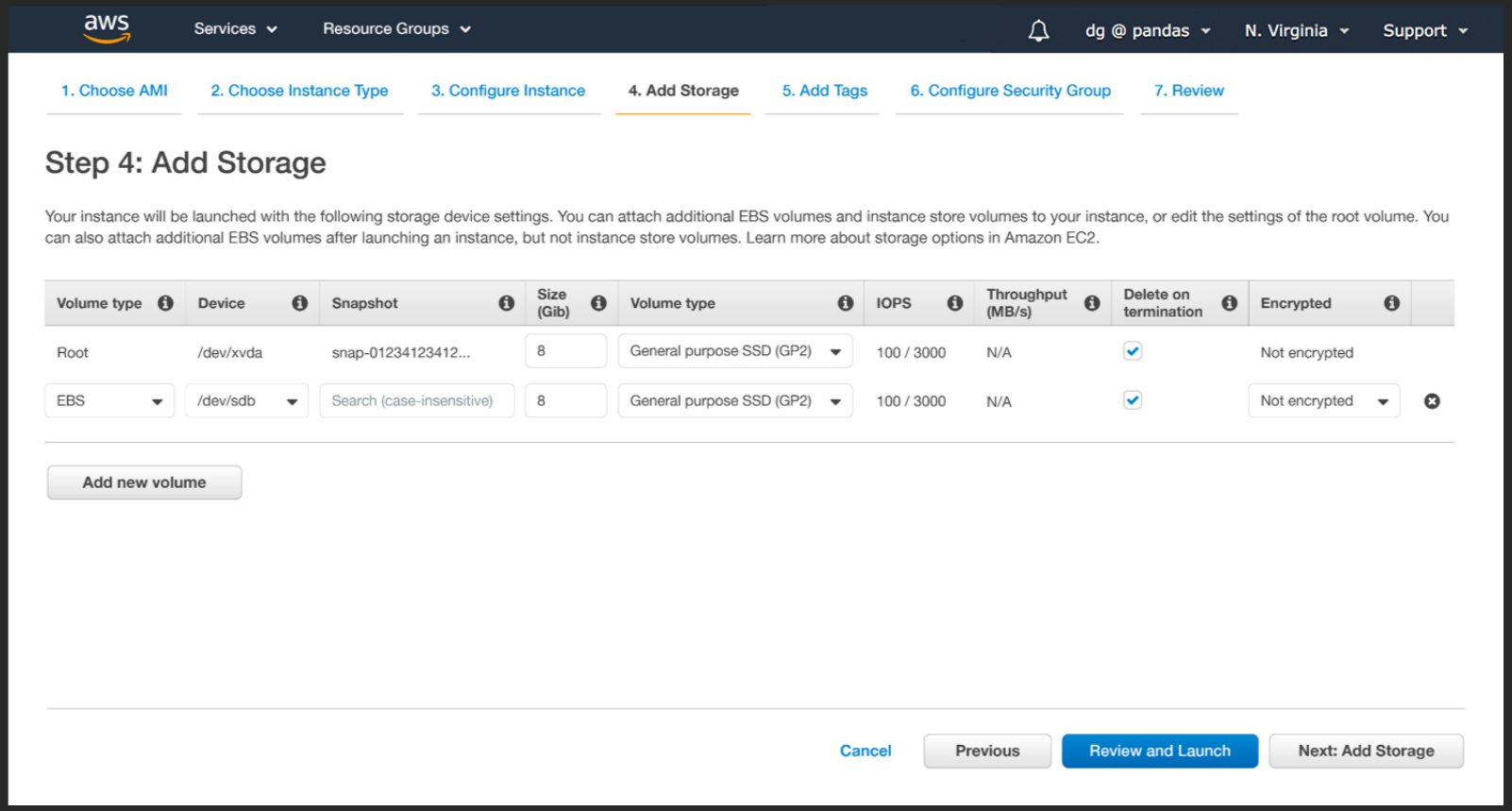
EBS Volume encryption

EBS encryption:
data volumes



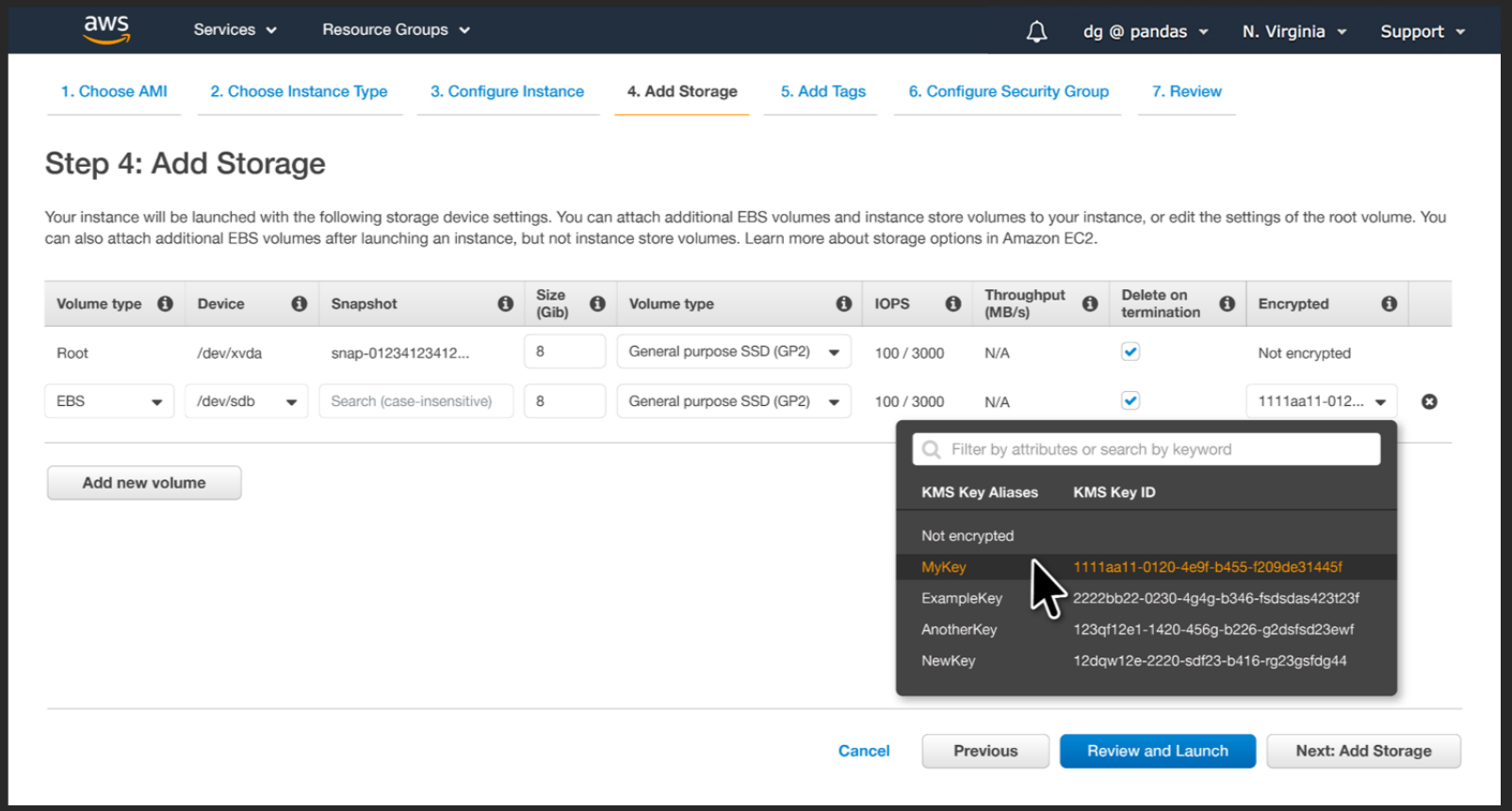
RunInstances with custom CMKs

EBS encryption:
data volumes



RunInstances with custom CMKs

EBS encryption:
data volumes



RunInstances with custom CMKs

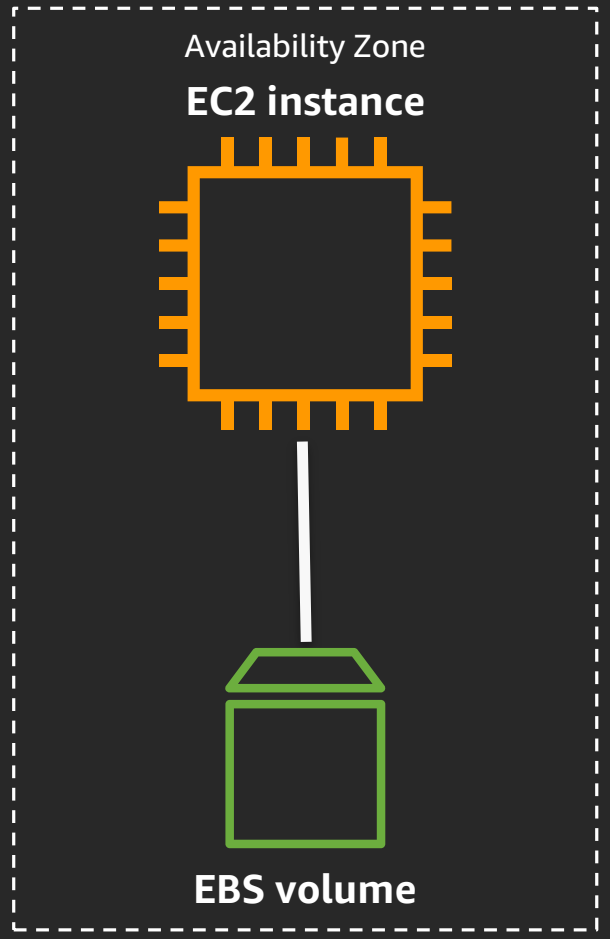
EBS encryption:
data volumes

```
$> aws ec2 run-instances –image-id ami-b42209de –count 1 –
instance-type m4.large –region us-east-1 –block-device-
mappings file://mapping.json
```

mapping.json

```
{
"DeviceName": "/dev/sda1",
"Ebs": {
"DeleteOnTermination": true,
"VolumeSize": 100,
"VolumeType": "gp2",
"Encrypted": true,
"kmsKeyID": "arn:aws:kms:us-east-1:012345678910:key/abcd1234-
a123-456a-a12b-a123b4cd56ef"
}
}
```

EBS Optimized Performance and EBS Encryption



Does choosing EBS Encryption reduce EBS Optimized Performance?

- EBS Optimized Performance is the same with and without encryption for the ‘4’ and ‘5’ family of instances
- In other words, encryption does not reduce the rated performance of an instance in the ‘4’ or ‘5’ family.

EBS snapshot encryption

- Snapshots of encrypted volumes are automatically encrypted
- Volumes created from encrypted snapshots are automatically encrypted
- You can encrypt an unencrypted snapshot when you copy a snapshot
- You can re-encrypt a snapshot you own with a different key when you copy a snapshot

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html

How are snapshots different?

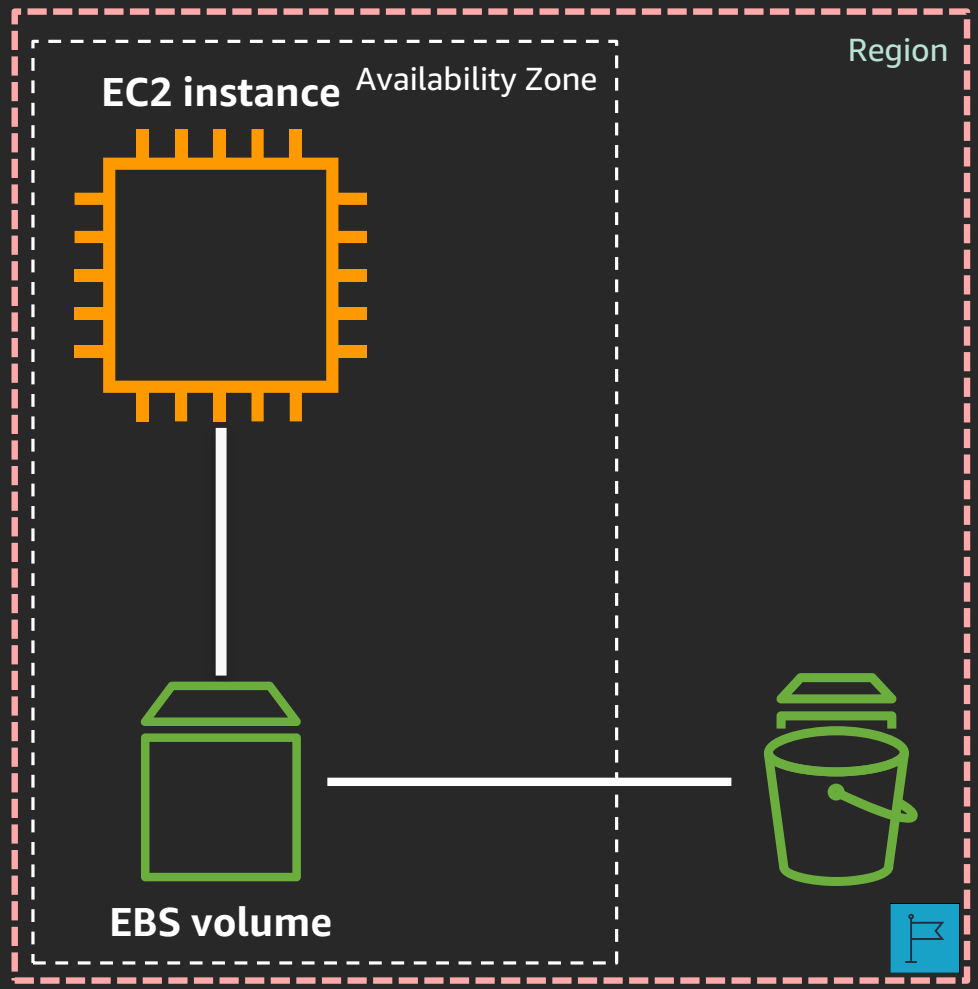
Snapshots can be shared across accounts

Snapshots can be copied across accounts

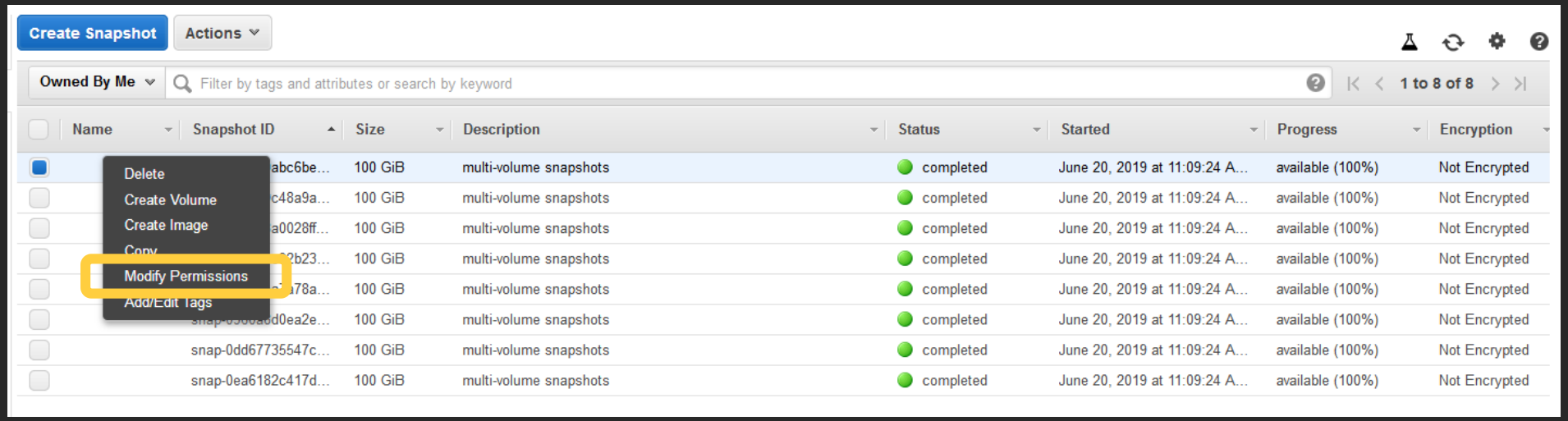
Snapshots can be copied within accounts

Snapshots can be copied across regions

Snapshots are used to create AMIs



Sharing Snapshots and AMIs

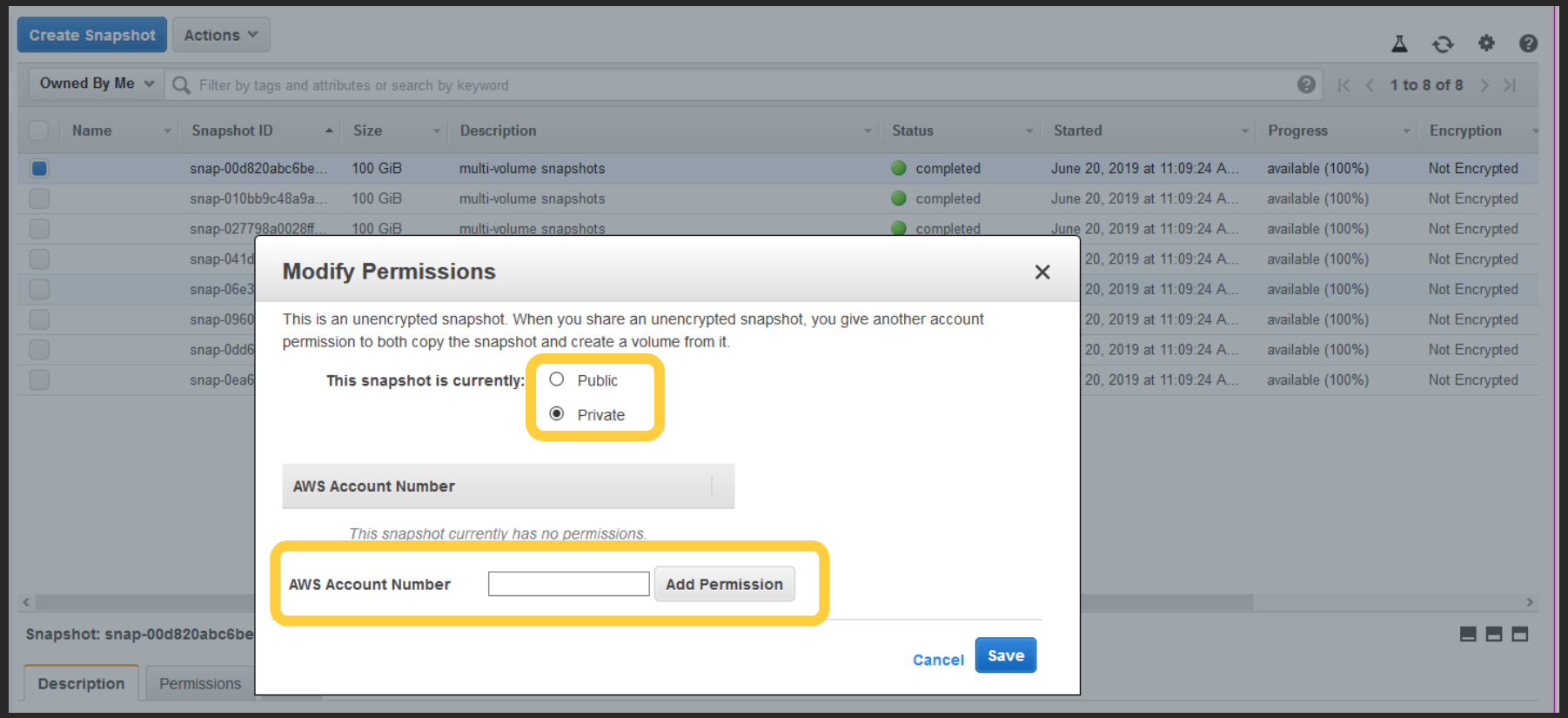



```
aws ec2 describe-snapshot-attribute --snapshot-id snap-00d820abc6be8d639 --attribute
createVolumePermission

aws ec2 modify-snapshot-attribute --snapshot-id snap-00d820abc6be8d639 --attribute
createVolumePermission

{
    "SnapshotId": "snap-00d820abc6be8d639",
    "CreateVolumePermissions": []
}
```

Sharing Snapshots and AMIs

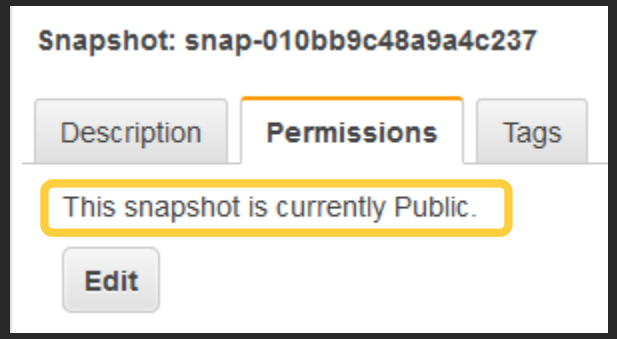


Sharing Snapshots and AMIs

Public sharing: Reasonable use case for AMIs – Marketplace AMIs

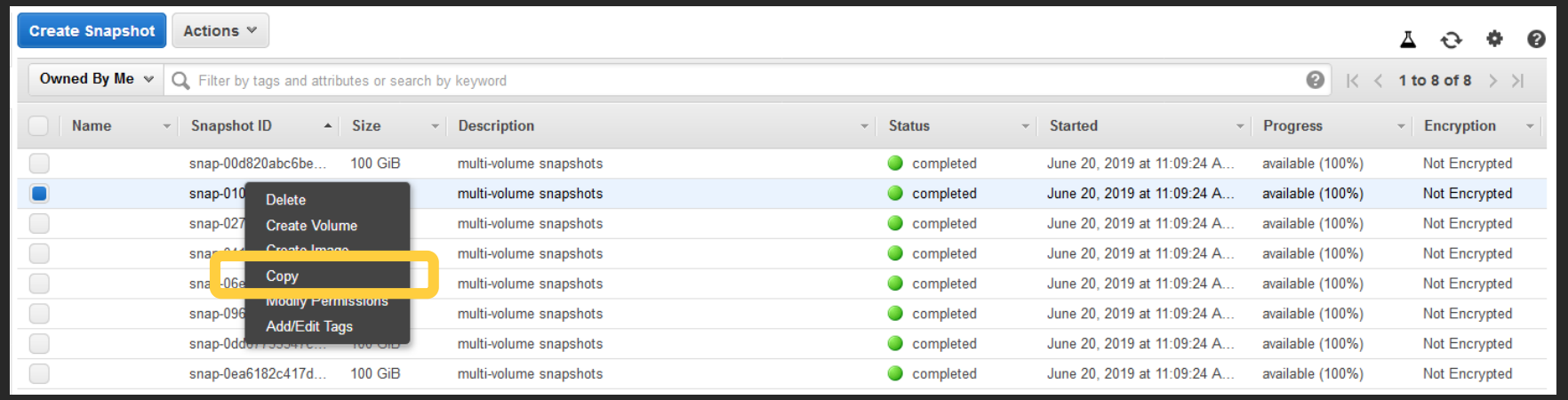
Share non-AMI snapshots with specific accounts

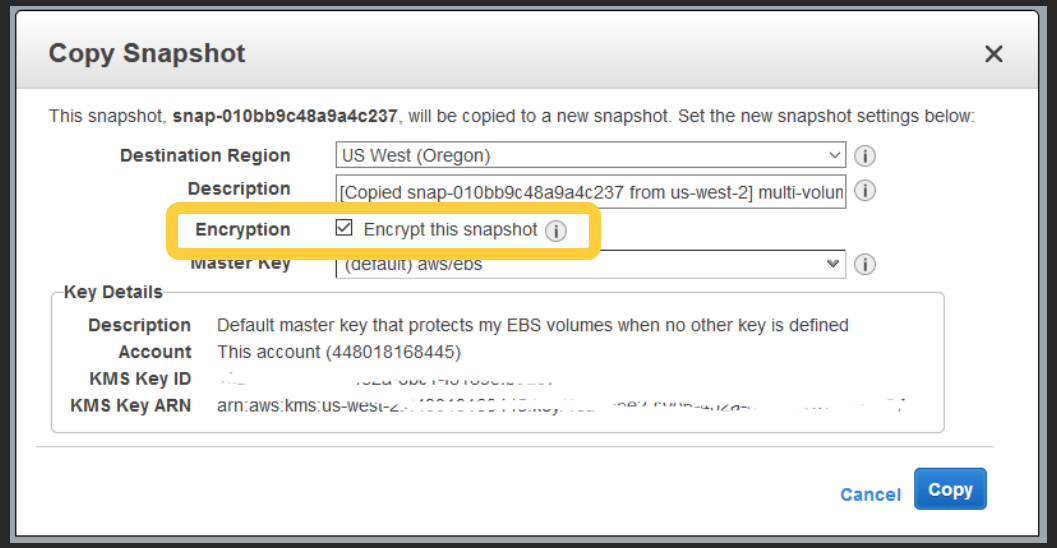
To launch a volume from a snapshot, you need a copy of snapshot in-region




```
snap-010bb9c48a9a4c237 --attribute createVolumePermission
{
    "SnapshotId": "snap-010bb9c48a9a4c237",
    "CreateVolumePermissions": [
        {
            "Group": "all"
        }
    ]
}
```

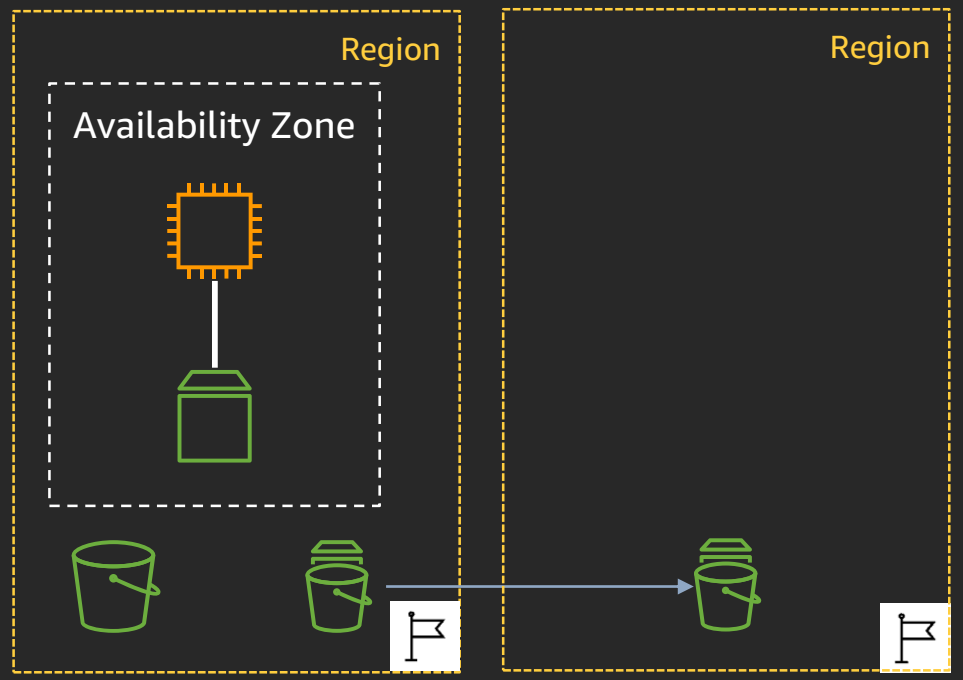
Copy Snapshots: Encrypt or Re-encrypt






```
aws ec2 copy-snapshot --source-snapshot-id
snap-010bb9c48a9a4c237 --destination-region
us-west-1 --encrypted --kms-key-id
key/1234abcd-12ab-34cd-56ef-1234567890ab
```

Copy Snapshots Across Regions



Copy Snapshots across accounts across regions

Lock down resource level permissions on target snapshot copy

Multi-region = Protection against regional events

Permission lock down = malicious or unintentional deletes of data

Three new features to make encryption easier

- Launch encrypted volumes from unencrypted snapshots / AMIs
  - Launch volumes encrypted with different CMK from encrypted snapshots / AMIs
- Share snapshots encrypted with custom CMKs across accounts
- Encryption By Default for EBS for an account in a region with a single setting

Feature: Encrypted Volumes from Unencrypted Snapshots or AMIs

Previously ...

Unencrypted Snapshot / AMI

Encrypted Snapshot / AMI

Encrypted EBS Volumes

Similar steps if you need to change encryption on a Snapshot / AMI

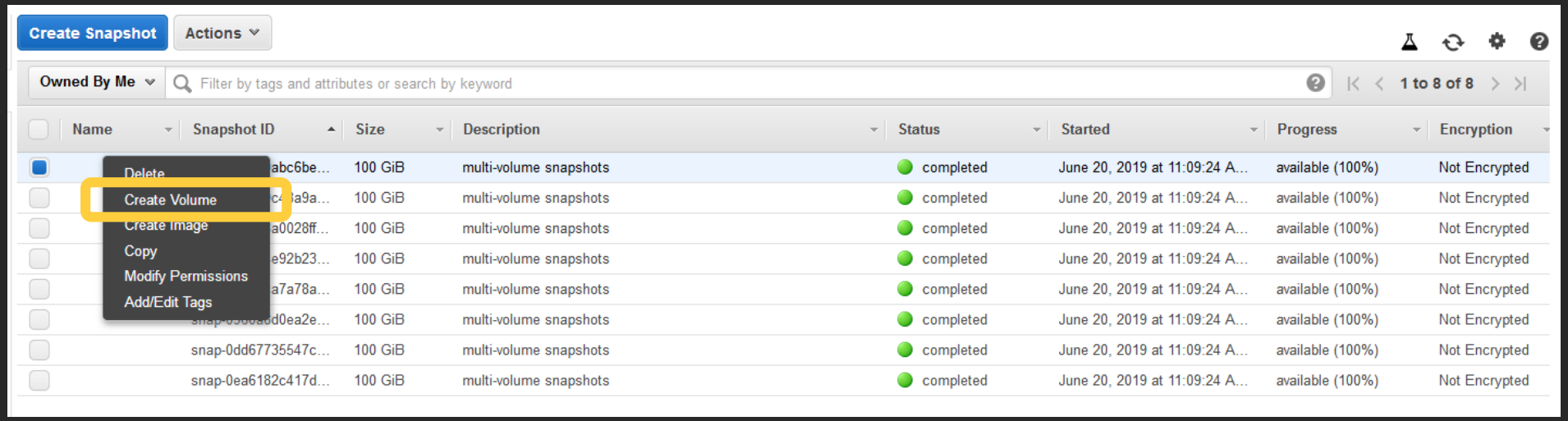
Now …

Unencrypted
Snapshot / AMI

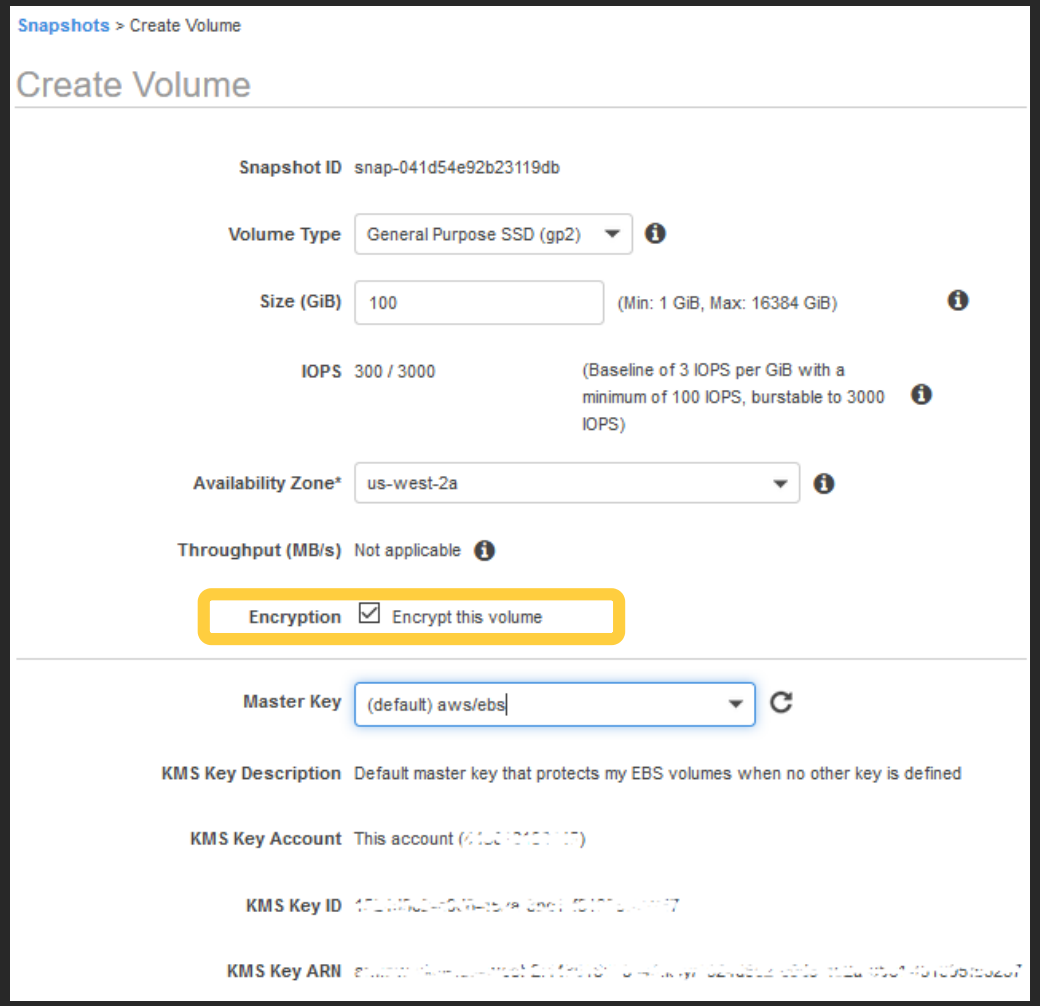
Encrypted EBS
Volumes

Similar steps if you need to change encryption on a Snapshot / AMI

How to do this



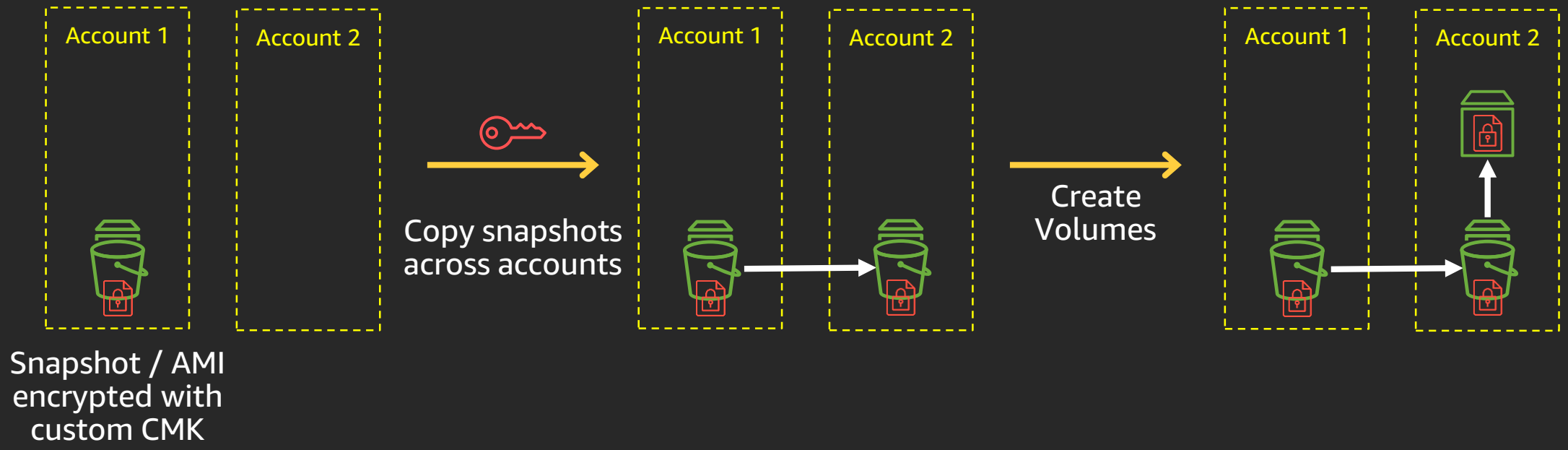
How to do this




```
aws ec2 create-volume --snapshot-id snap-010bb9c48a9a4c237 --availability-zone us-west-2a --encrypted --volume-type gp2
```

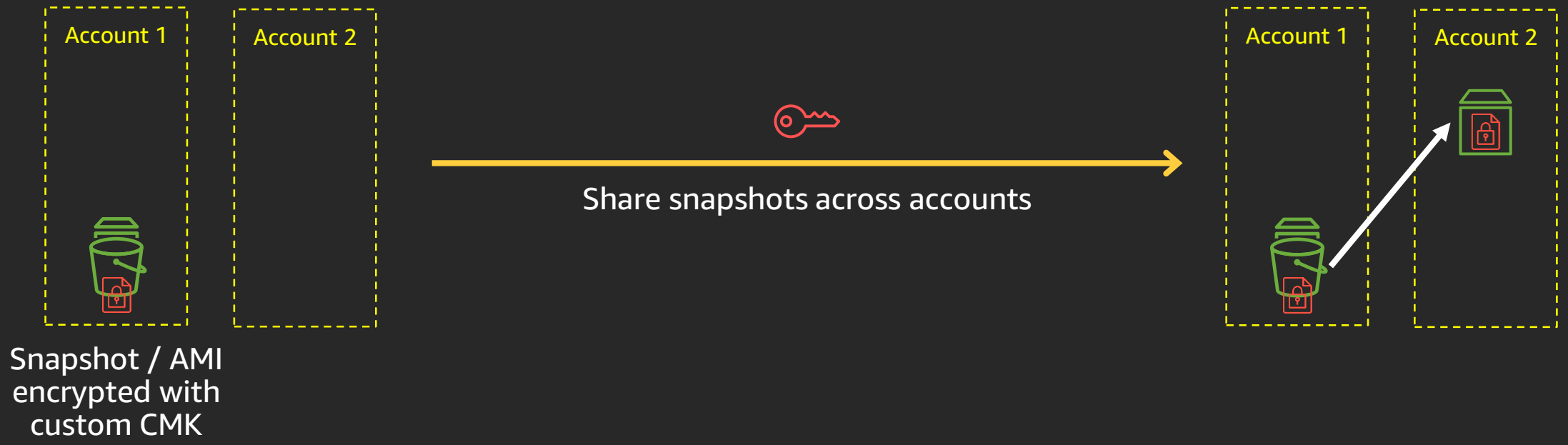
Feature: Share encrypted Snapshots / AMIs across accounts

Previously ...



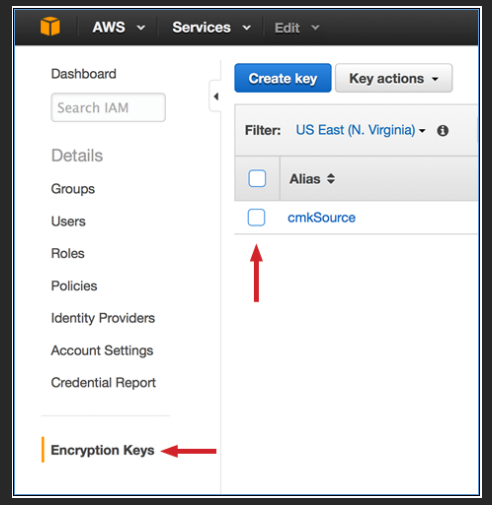
Encrypted snapshots could only be copied across accounts

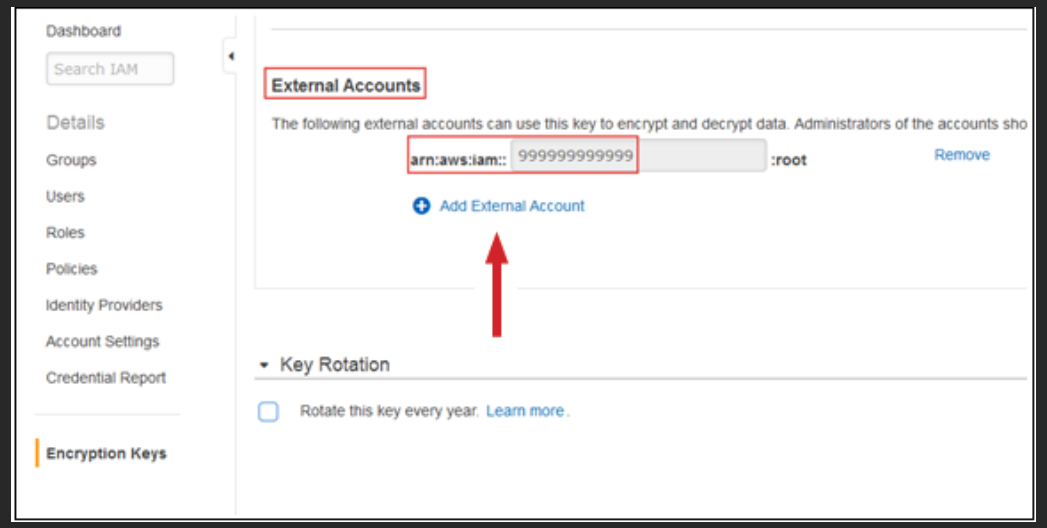
Now …



Share Snapshots/AMIs encrypted with custom CMKs across accounts
[NOTE: Snapshots / AMIs encrypted with Default CMKs cannot be shared across accounts]

How to do this






```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:DescribeKey",
                "kms:ReEncrypt*",
                "kms:CreateGrant",
                "kms:Decrypt"
            ],
            "Resource": [
                "arn:aws:kms:us-east-
1:<111111111111>:key/<key-id of cmkSource>"
            ]
        }
    ]
}
```

How to do this

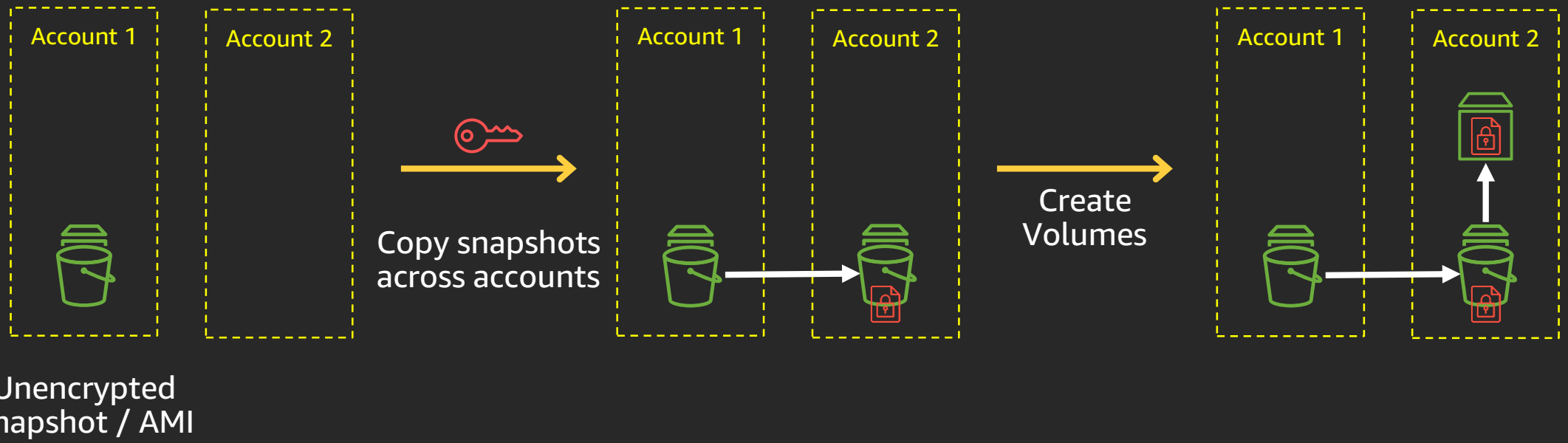
```
$> aws ec2 run-instances
    --image-id ami-XXXXX
    --count 1
    --instance-type m4.large
    --region us-east-1
    --subnet-id subnet-aec2fc86
    --key-name 2016KeyPair
    --security-group-ids sg-f7dbc78e
subnet-id subnet-aec2fc86
    --block-device-mappings
file://mapping.json
```

mapping.json

```
[
    {
        "DeviceName": "/dev/xvda",
        "Ebs": {
                "Encrypted": true,
                "KmsKeyId":
"arn:aws:kms:us-east-
1:<999999999999>:key/<abcd1234-a123-
456a-a12b-a123b4cd56ef>"
        }
    }
]
```

Combining the two features

Previously …


Account 1
Account 2
Unencrypted
Snapshot / AMI
Copy snapshots
across accounts
Account 1
Account 2
Create
Volumes
Account 1
Account 2

Now …

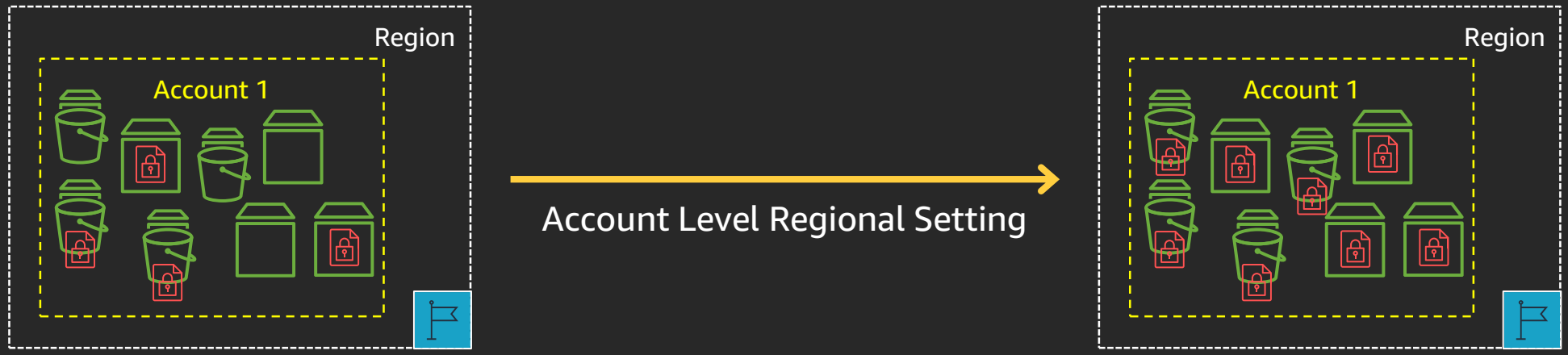
Launch encrypted volumes across accounts from unencrypted Snapshots / AMIs
[NOTE: Snapshots / AMIs encrypted with Default CMKs cannot be shared across accounts]

Feature: Enable EBS account level encryption by default

Previously …

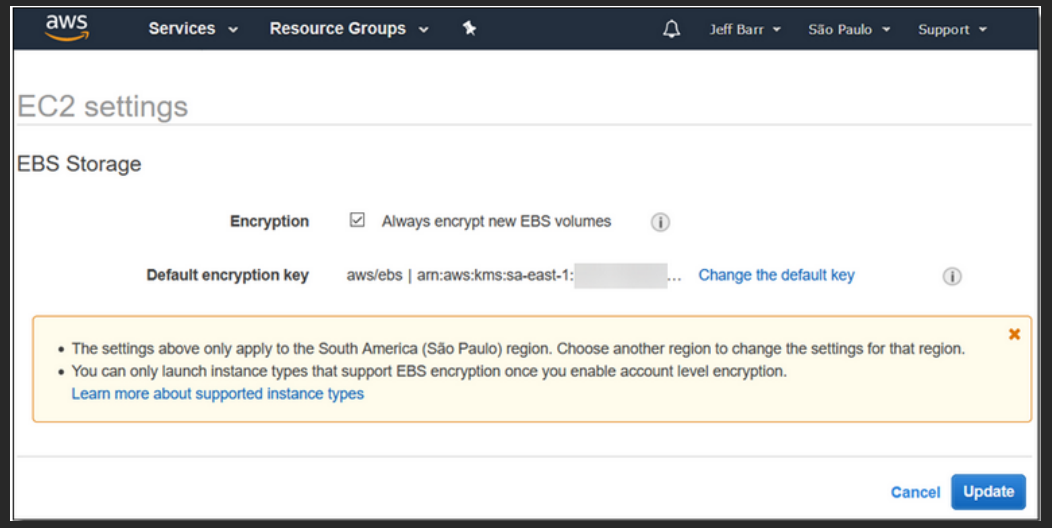
With IAM policies, you can prevent unencrypted volumes from launching

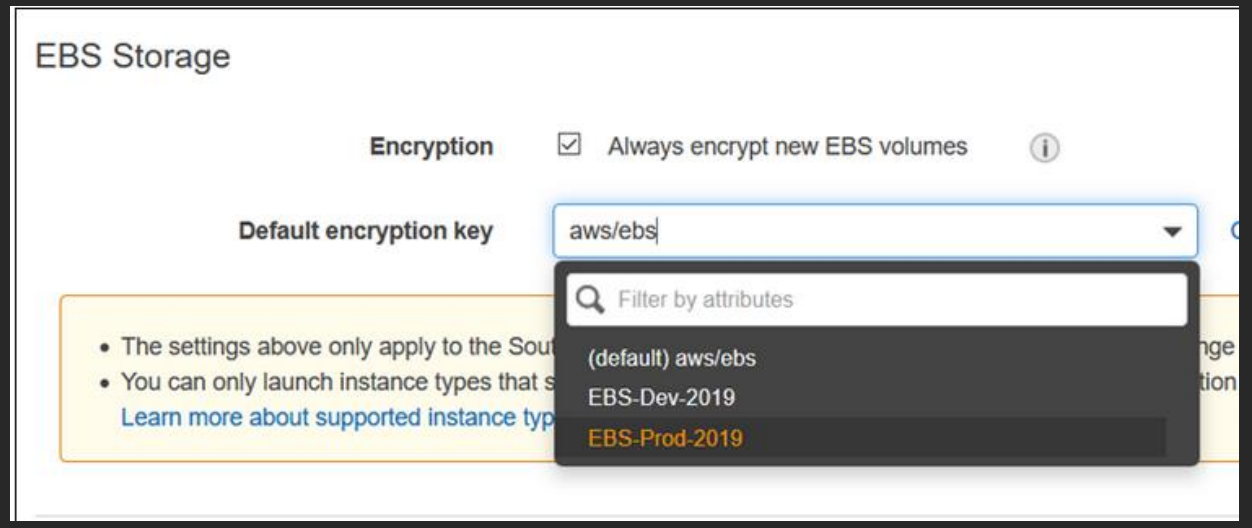
Now …



Without change to workflows, newly launched volumes + snapshots are encrypted

How to do this





And that's it!

If you remember nothing else …

Monitor access

Keep tabs on which snapshots you are sharing and why

Account Level Encryption

Encryption is a check-box – literally! Use it.

Building your application

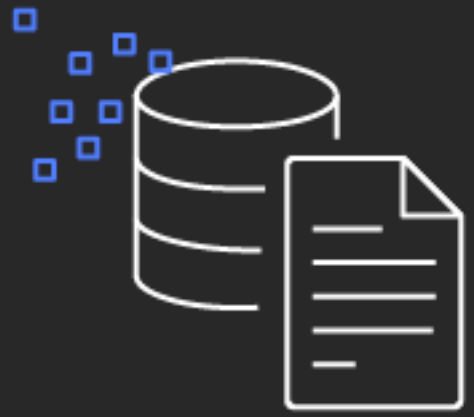
Understand your mission

Understand your mission

Understand your mission

Gather as much data as possible!

Understand your mission



Databases

PostgreSQL, MySQL

Cassandra, MongoDB

Data & Analytics

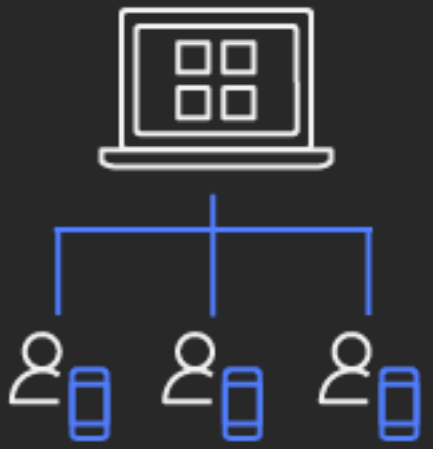
Kafka, Splunk, Hadoop,

Data Warehousing

Media

Transcoding, Encoding,

Render Farms

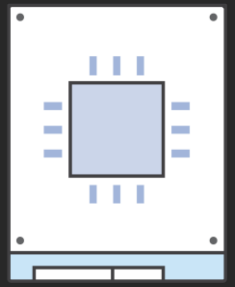


File

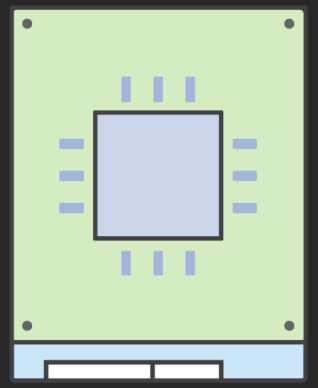
CIFS, NFS

Archive

Select the right volume for your workload

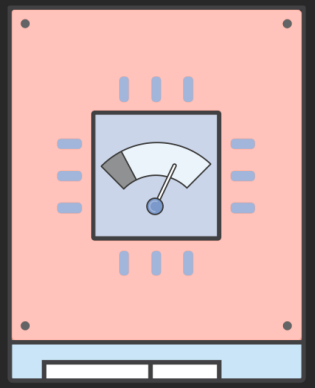


SSD



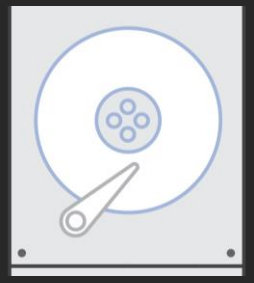
gp2

General Purpose SSD

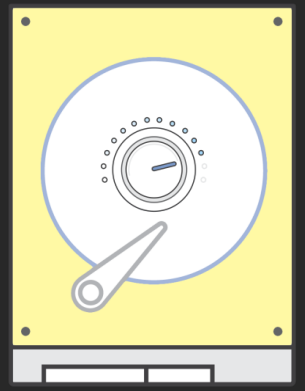


io1

Provisioned IOPS SSD

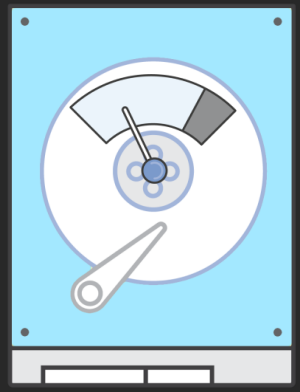


HDD



st1

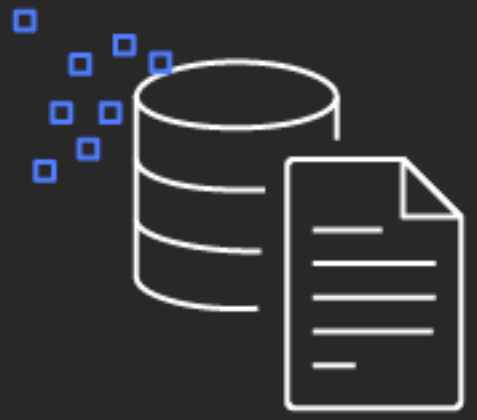
Throughput Optimized HDD



sc1

Cold HDD

Select the right volume



Databases

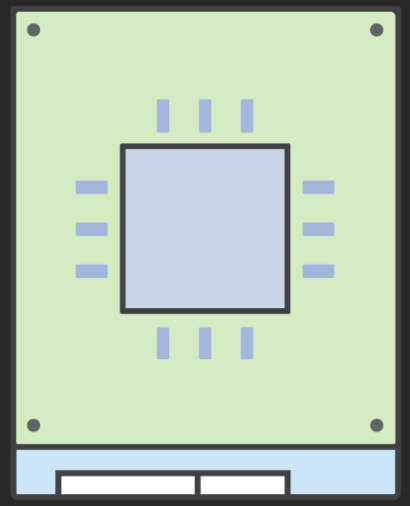
PostgreSQL, MySQL

Cassandra, MongoDB

- Typically high performance requirements
- Mostly random I/O
- Journal is sequential
- Highly workload dependent

Recommendation: SSD (+ HDD?)

Amazon EBS volume: General Purpose SSD



gp2

General Purpose SSD

Baseline: 100 to 16,000 IOPS @ 3 IOPS/GB

Burst: 3,000 IOPS (< 1000 GB)

Throughput: Up to 256 MiB/s

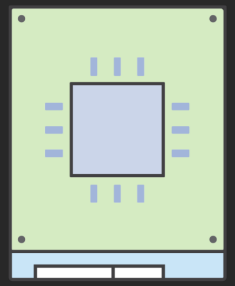
Latency: Single-digit ms

Capacity: 1 GiB to 16 TiB

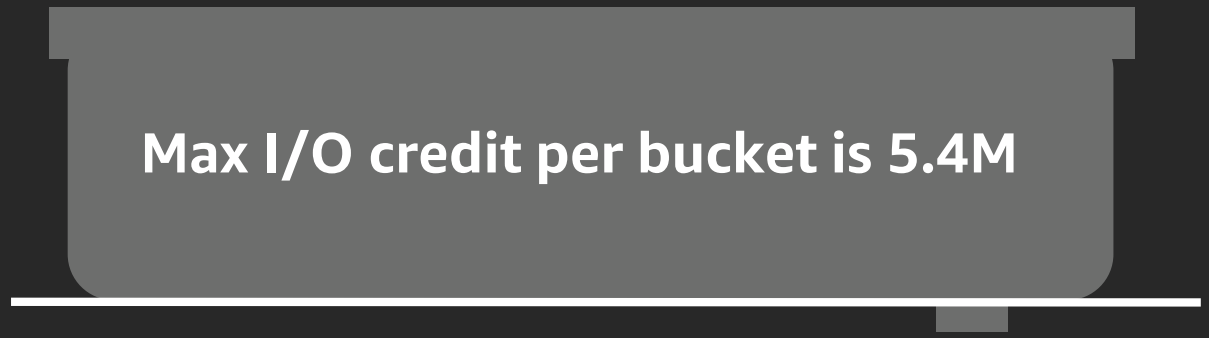
I/O Size: Up to 256 KiB (logical merge)

Great for boot volumes, low-latency applications, and bursty databases

Burst bucket: gp2

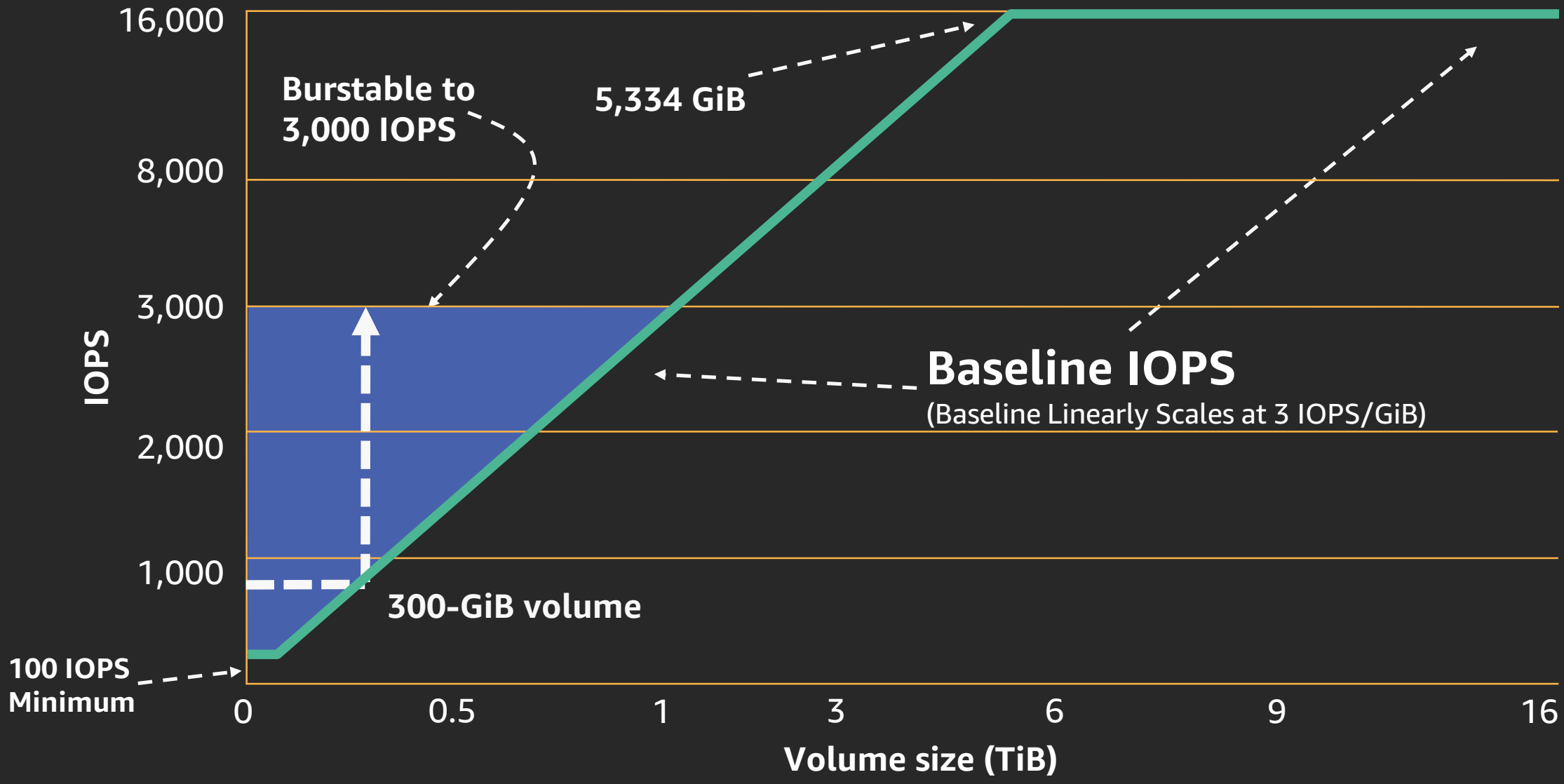


Baseline performance:
Always accumulating
3 IOPS per GiB per second

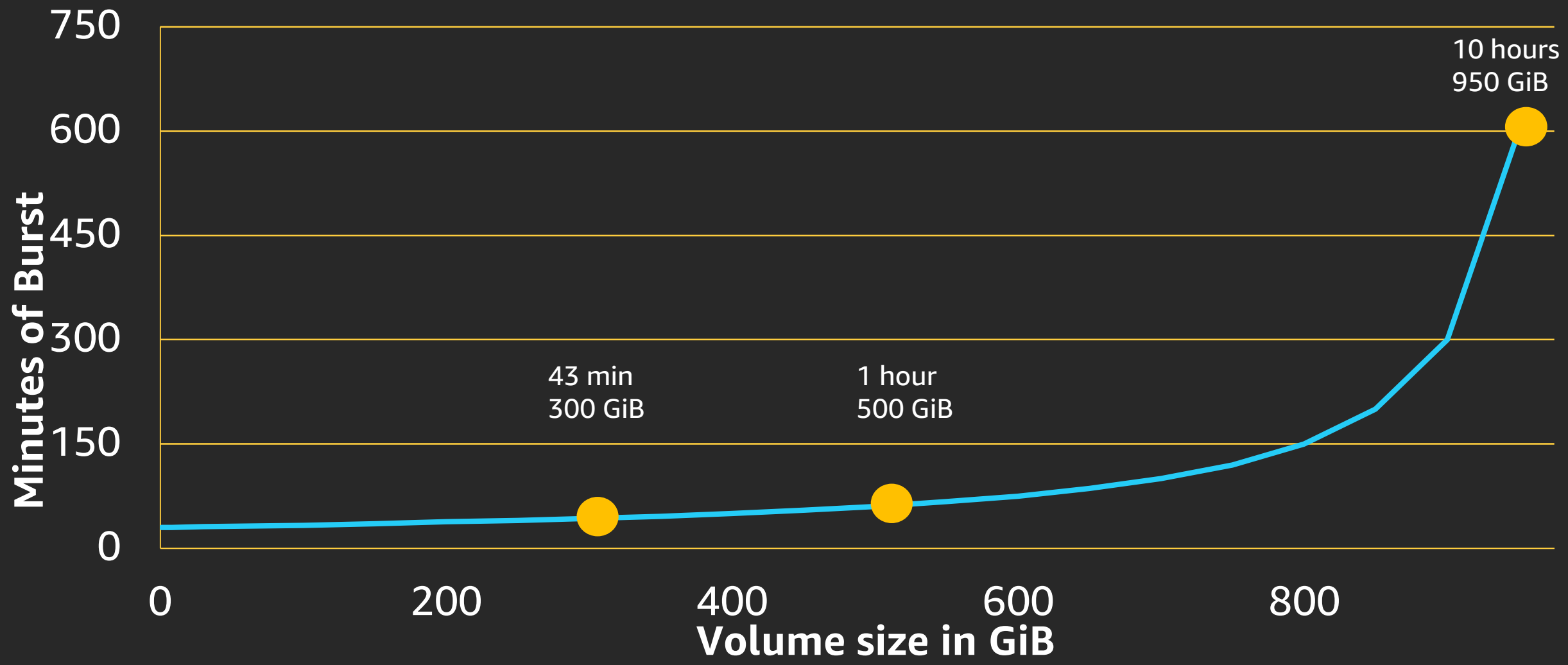


Burst performance:
You can spend up to
3,000 credits per second

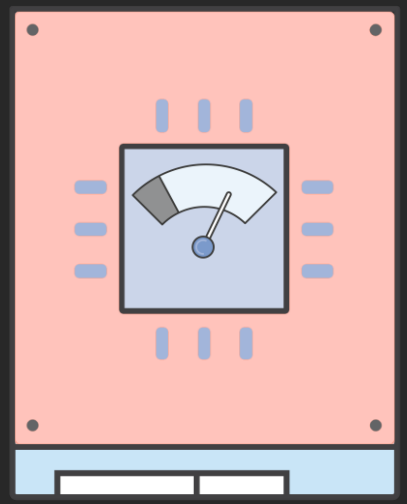
Burst and baseline: gp2



How long can I burst on gp2?



Amazon EBS volume: Provisioned IOPS



io1

Provisioned IOPS

Baseline: 100 – 64,000 IOPS

Throughput: Up to 1000 MiB/s

Latency: Single-digit ms

Capacity: 4GiB – 16 TiB

I/O Size: Up to 256 KiB (logical merge)

Ideal for critical applications and databases with sustained IOPS

Would my customers or my business be impacted by degredation or an outage?

Understand your mission

Tier 1 (critical)

Everything Else

Select the right volume

Media

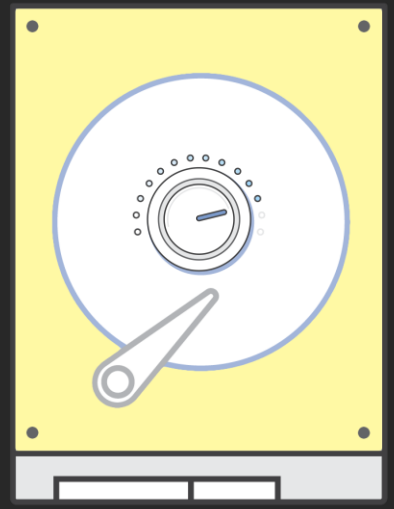
Transcoding, Encoding,

Render Farms

- Typically high throughput requirements
- Mostly sequential I/O
- Sustained I/O

Recommendation: Throughput Optimized HDD (st1)

Amazon EBS volume: Throughput Optimized



st1

Throughput Optimized HDD

Baseline: 40 MiB/s per TiB, up to 500 MiB/s

Burst: 250 MiB/s per TiB, up to 500 MiB/s

Capacity: 500 GiB to 16 TiB

I/O Size: Up to 1 MiB (logical merge)

Ideal for large-block, high-throughput sequential workloads

Select the right volume

Data & Analytics

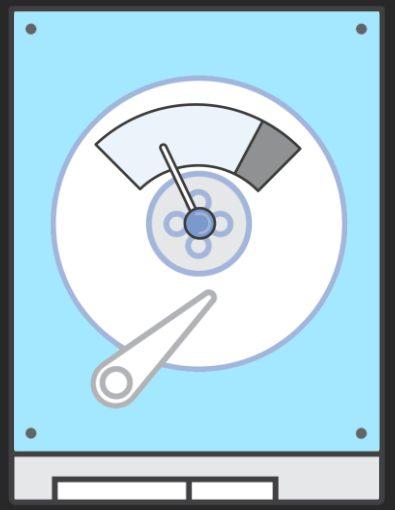
Kafka, Splunk, Hadoop,

Data Warehousing

- Typically high throughput requirements
- Mostly sequential I/O
- Daily periodicity

Recommendation: HDD

Amazon EBS volume: Cold HDD



sc1

Cold HDD

Baseline: 12 MiB/s per TiB, up to 192 MiB/s

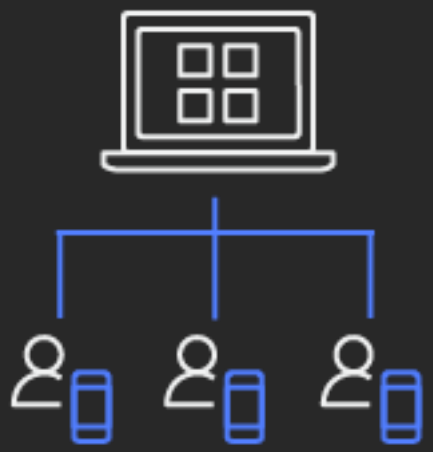
Burst: 80 MiB/s per TiB, up to 250 MiB/s

Capacity: 500 GiB to 16 TiB

I/O Size: Up to 1 MiB (logical merge)

Ideal for sequential throughput workloads, such as logging and backup

Select the right volume



File

CIFS, NFS

Archive

- Typically low throughput requirements
- Bursty workloads
- Cost sensitive

Recommendation: Cold HDD (sc1)

Understand your mission

Need more detail?

```
$ iostat -xdm /dev/nvme2n1 5
     :
Device:            rrqm/s   wrqm/s     r/s     w/s    rMB/s    wMB/s avgrq-sz avgqu-sz   ...
nvme2n1              0.00     0.00 24649.80 1564.80   995.53     6.11    78.25    40.31   ...
```

995.53 MB/s / 24650 reads/s ~= 40KiB / request

6.11 MB/s / 1565 writes/s ~= 4KiB / request

78 sectors / 512 B/sector ~= 39 KiB / request

Understand your mission

Going deeper with blktrace

```
$ sudo blktrace -w 300 /dev/nvme2n1
  :
$ blkparse -d nvme2n1.bin -i nvme2n1 -O
$ btt -i nvme2n1.bin -B blk_offsets
$ ./bt_analyze.py blk_offsets_259,4_r.dat blk_offsets_259,4_w.dat
```

Blktrace analysis

```
with open(tracefile) as f:
    for line in f:
        start, end = line.split()[1:]

        start = int(start)
        end = int(end)

        num_ios += 1

        # keep track of sequential segments
        if start != prev_segment:
            num_segments += 1
        prev_segment = end

        # convert sectors to bytes
        sz = (end - start) / 2
        iosize[sz] += 1
        total_size += sz
```

Understanding your mission

Going deeper with blktrace

Read

```
Sequential: 0.0006%
I/O by Size:
   0 - 4 KiB: 48
   4 - 8 KiB: 2
   8 - 16 KiB: 259776
   16 - 32 KiB: 65996
   32 - 64 KiB: 320934
   128 - 256 KiB: 2
```

Write

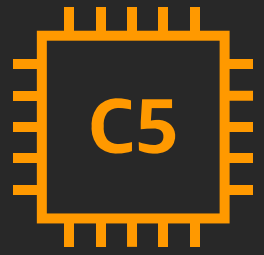
```
Sequential: 99.9879%
I/O by Size:
   0 - 4 KiB: 32973
```

Select the right volumes

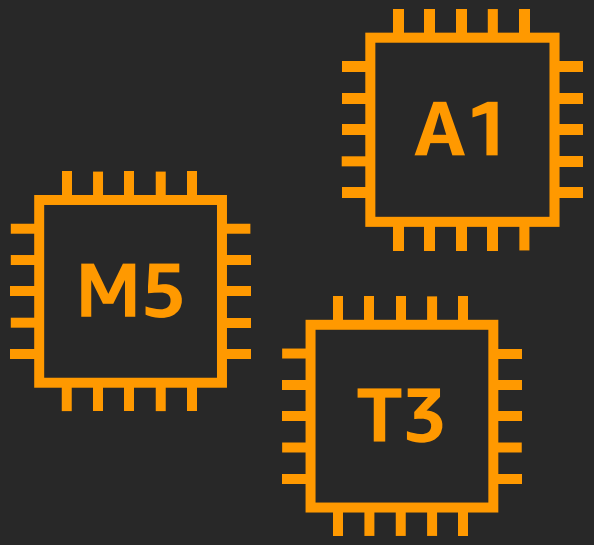
Multiple EBS volumes can be attached to an instance

Mix and match volume types for optimum performance

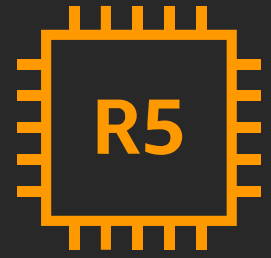
EC2 instance selection



Compute Optimized



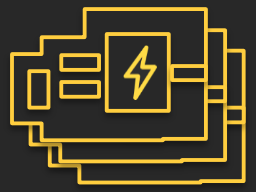
General Purpose



Memory Optimized

Nitro in three parts

Nitro Cards



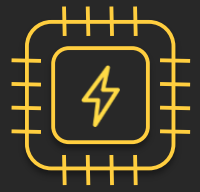
VPC Networking

Amazon Elastic Block Store (Amazon EBS)

Instance Storage

System Controller

Nitro Security Chip



Integrated into motherboard

Protects hardware resources

Hardware Root of Trust

Nitro Hypervisor

Lightweight hypervisor

Memory and CPU allocation

Bare Metal-like performance

Nitro Card for EBS

NVMe Controller

- Standard drivers broadly available

EBS Data Plane

- Encryption support
- NVM to remote storage protocol
- EBS Optimized by default

EBS Optimized

Dedicated EBS bandwidth

Up to 14 Gbps (1,750 MiB/s) per instance

Burst available for smaller instances

Tip: Ensure EBS optimized bandwidth can support your volumes

NEW

EBS Optimized

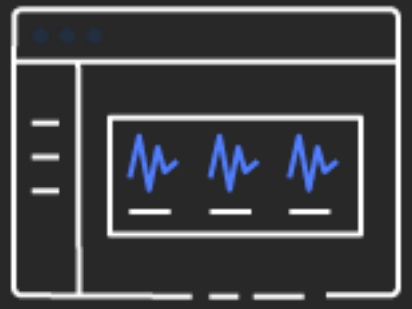
Dedicated EBS bandwidth

Up to **19** Gbps (**2,375** MiB/s) per instance

Burst available for smaller instances

Tip: Ensure EBS optimized bandwidth can support your volumes

Experiment and measure

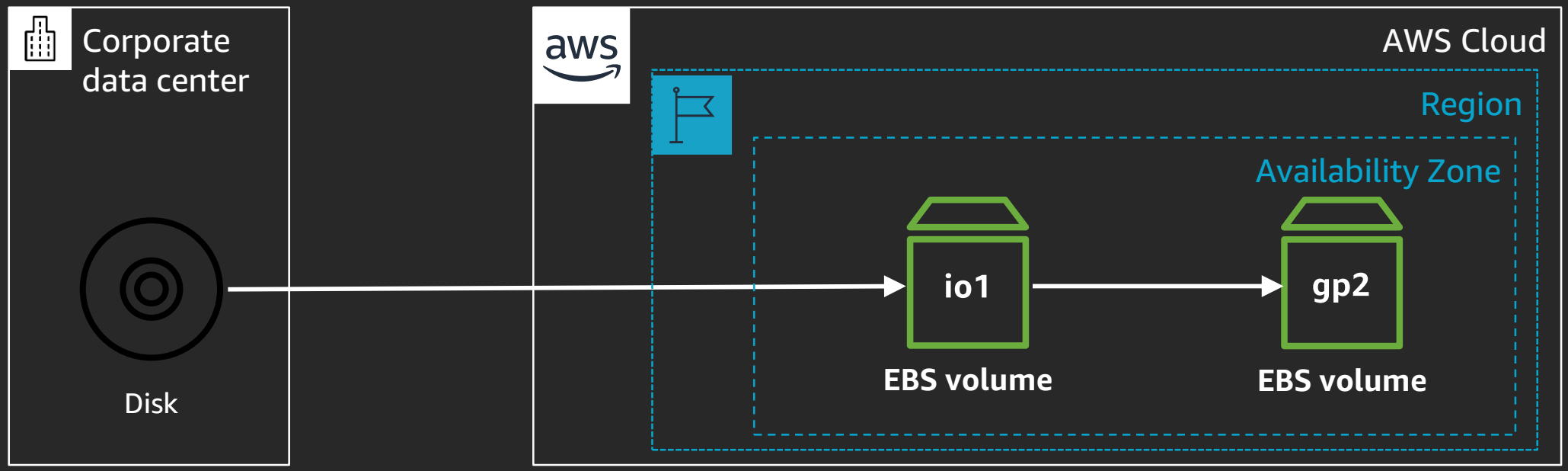


Use the scientific method!

Benchmarks give you a good baseline, but perform differently than real world data!

Monitor with CloudWatch and other tools

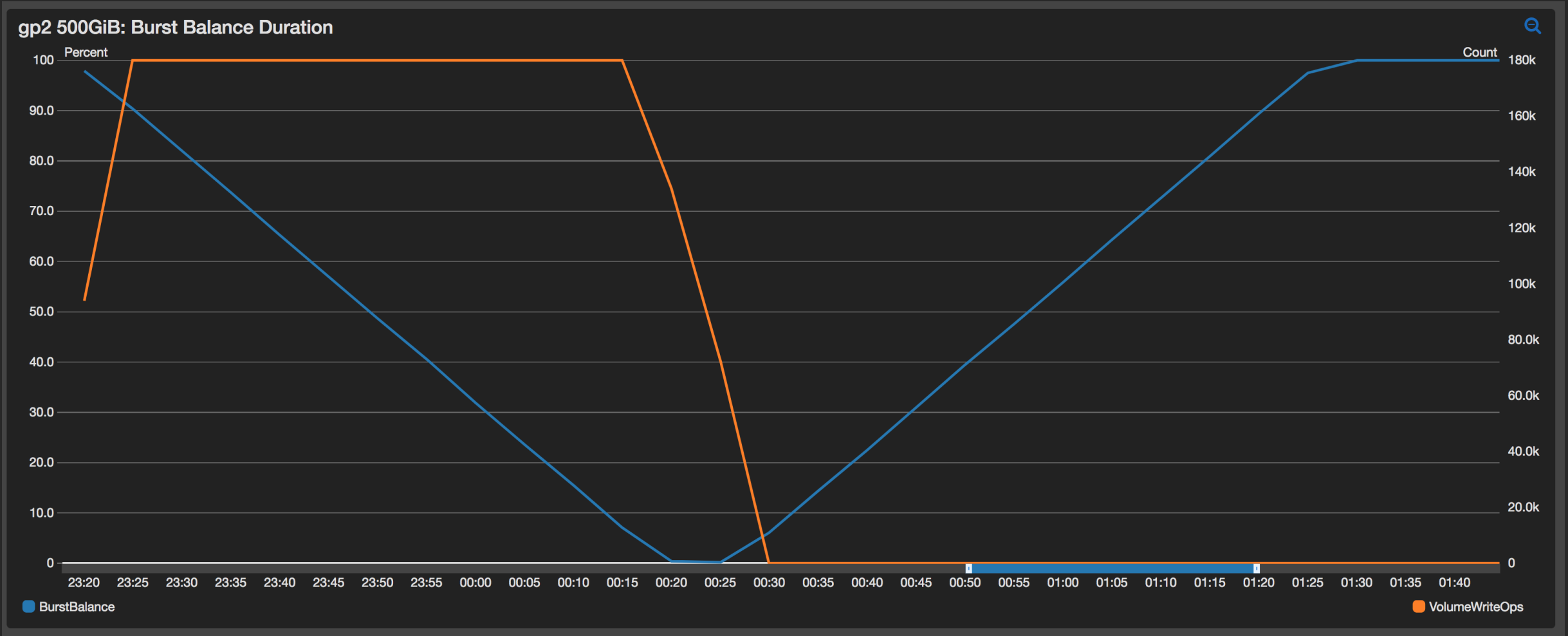
Elastic Volumes: Get to the right volume type



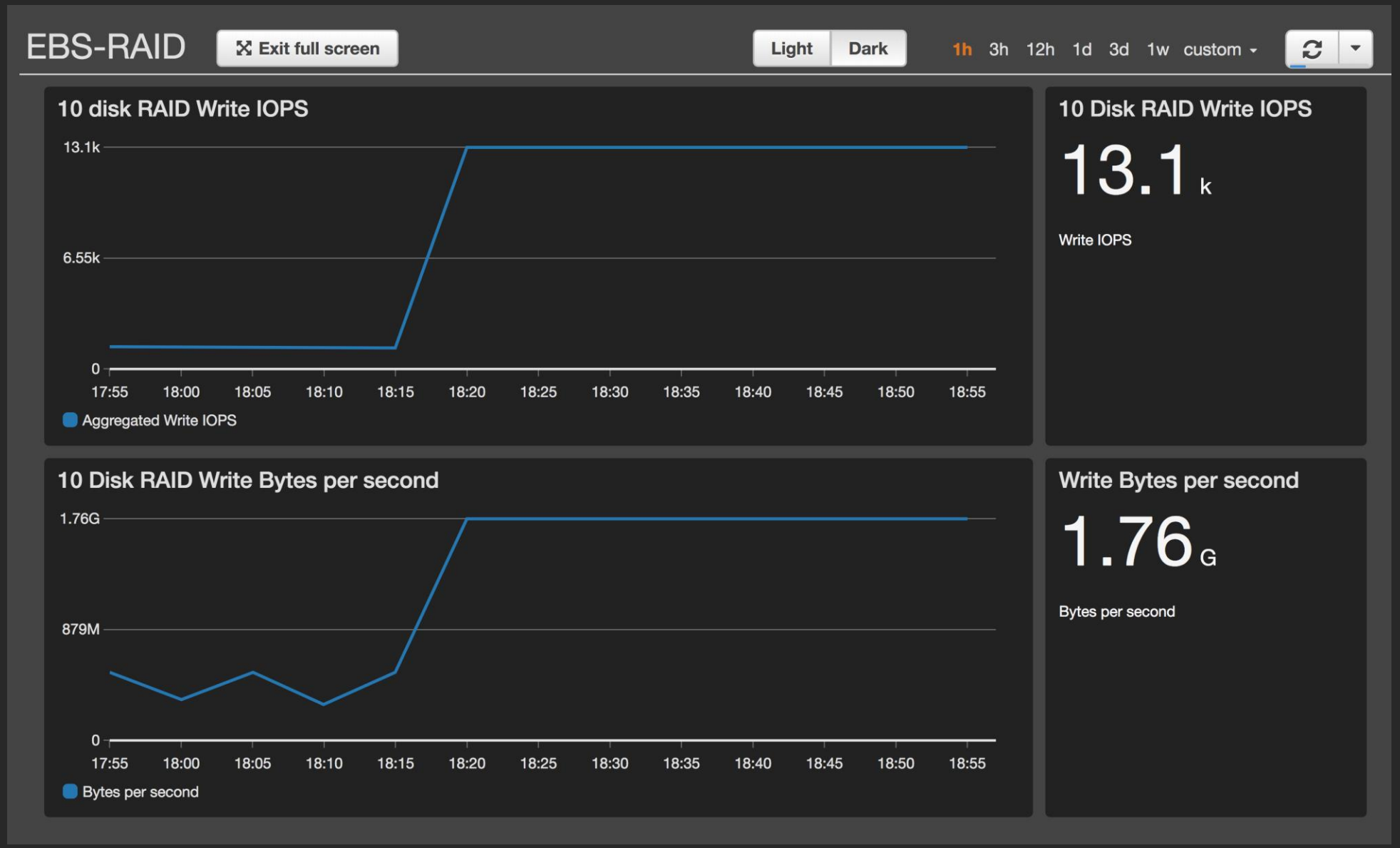

```
aws ec2 modify-volume --volume-id vol-00d820abc6be8d639 --volume-type gp2 --size 10000
```

Ensure that you have enough IOPS on gp2

CloudWatch monitoring



CloudWatch metric math



Availability and Durability

EBS is designed for…

99.999% service availability

0.1% to 0.2% annual failure rate (AFR)

EBS Snapshots

Point in time backup of modified volume data

Changed blocks stored in S3

Incremental and crash consistent

Can take consistent snapshot of all volumes attached to an instance

Amazon Data Lifecycle Manager

Automate snapshot lifecycle

Integrates with CloudFormation

EBS volume or instance level policies

EBS Fast Snapshot Restore

6x lower Recovery Time Objective

New on 11/20

Predictability

Manage RTO based on size and credits

Speed

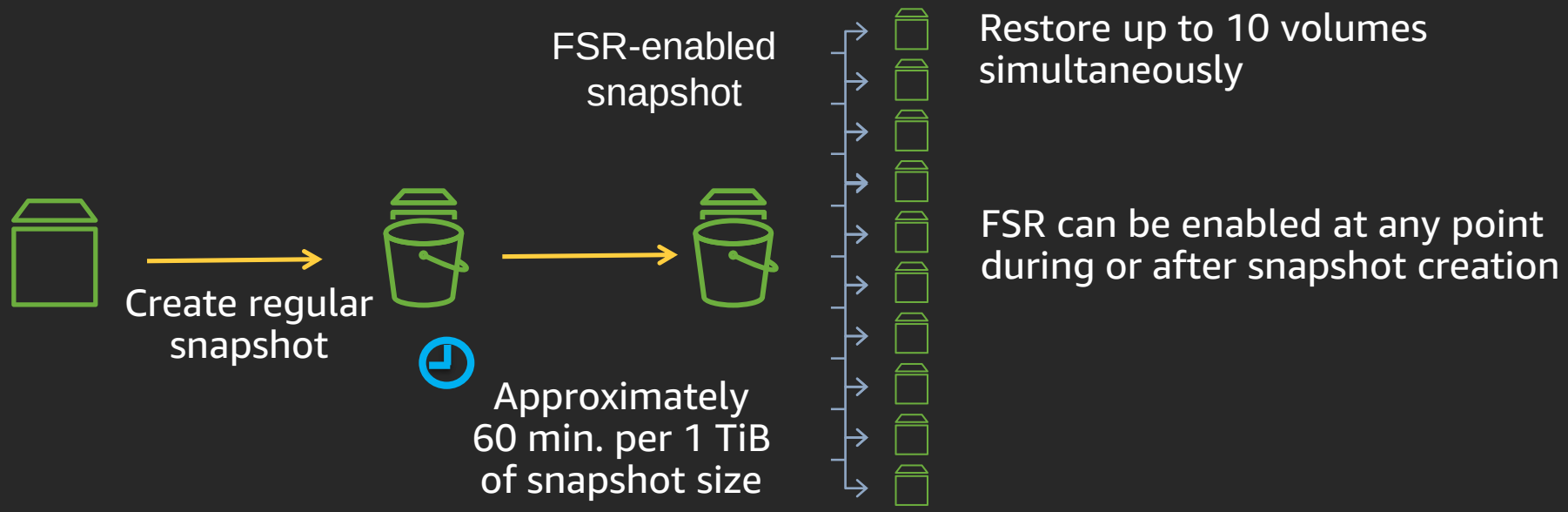
Instant access on volume from snapshots

Scale

Up to 10 volume restores instantly

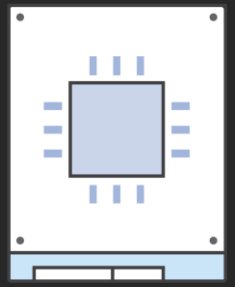
Cost

No need for additional EC2 instances

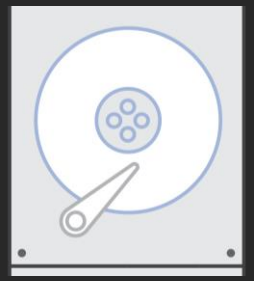


So you want to save cost on EBS

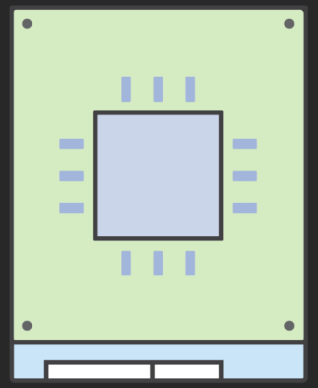
Select the right volume for your workload



SSD

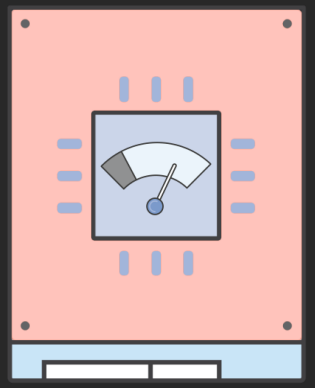


HDD



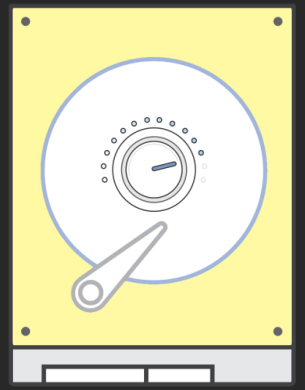
gp2

General Purpose SSD



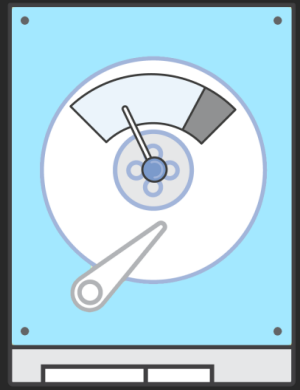
io1

Provisioned IOPS SSD



st1

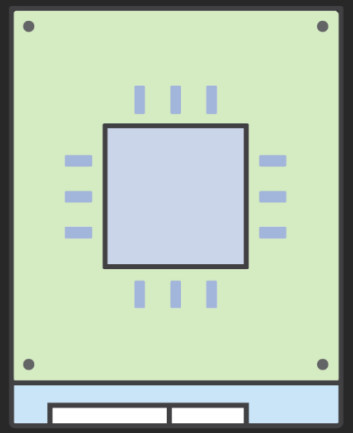
Throughput Optimized HDD



sc1

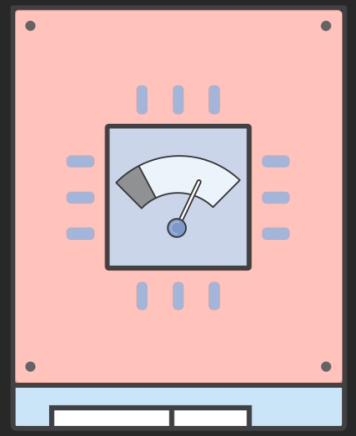
Cold HDD

I/O Provisioned Volumes



gp2

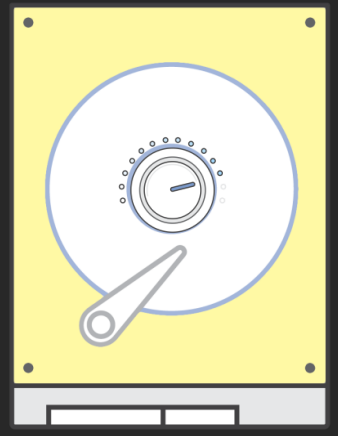
$0.10 per GiB



io1

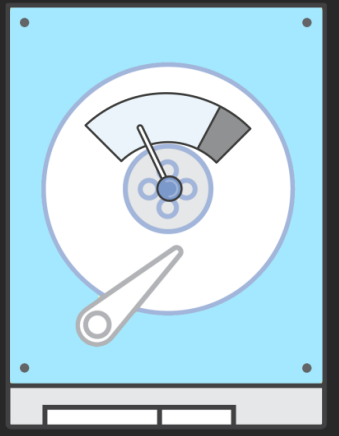
$0.125 per GiB
$0.065 per PIOPS

Throughput Provisioned Volumes



st1

$0.045 per GiB



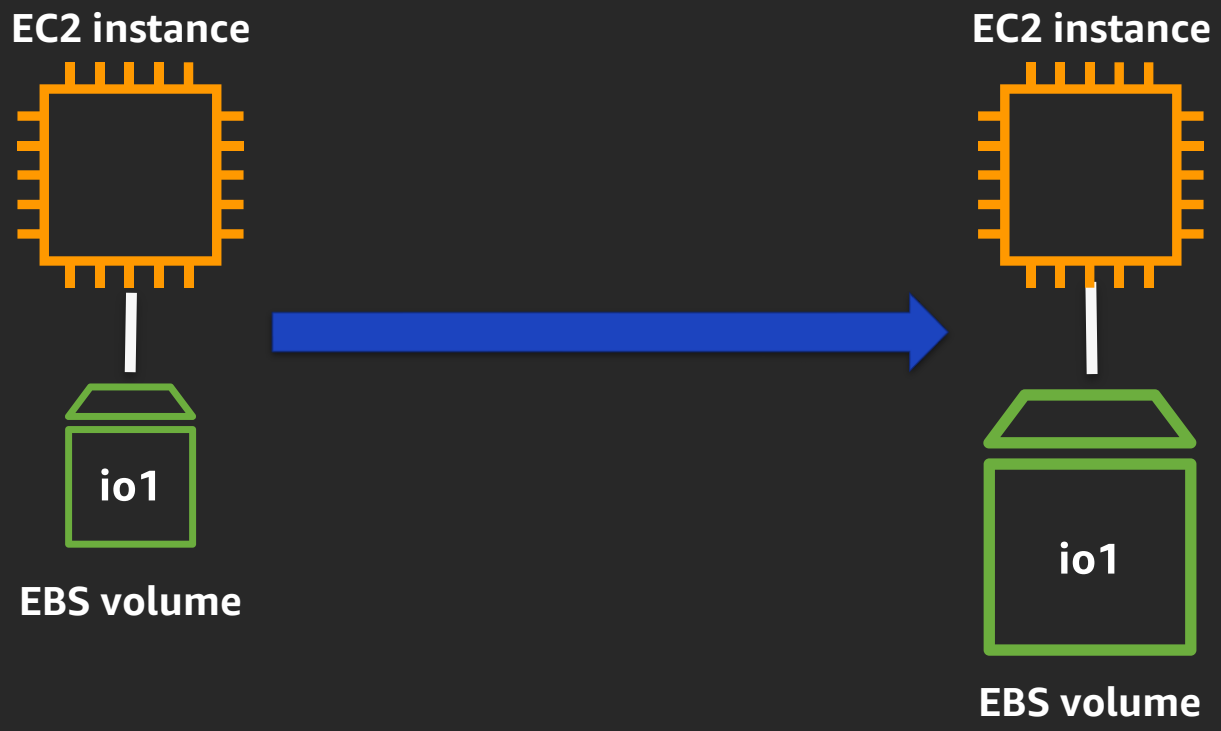
sc1

$0.025 per GiB

Snapshot storage for all volume types is $0.05 per GiB per month

* All prices are per month, prorated to the second, and from the us-west-2 Region as of Nov 2019

Elastic Volumes: Size your volumes correctly!

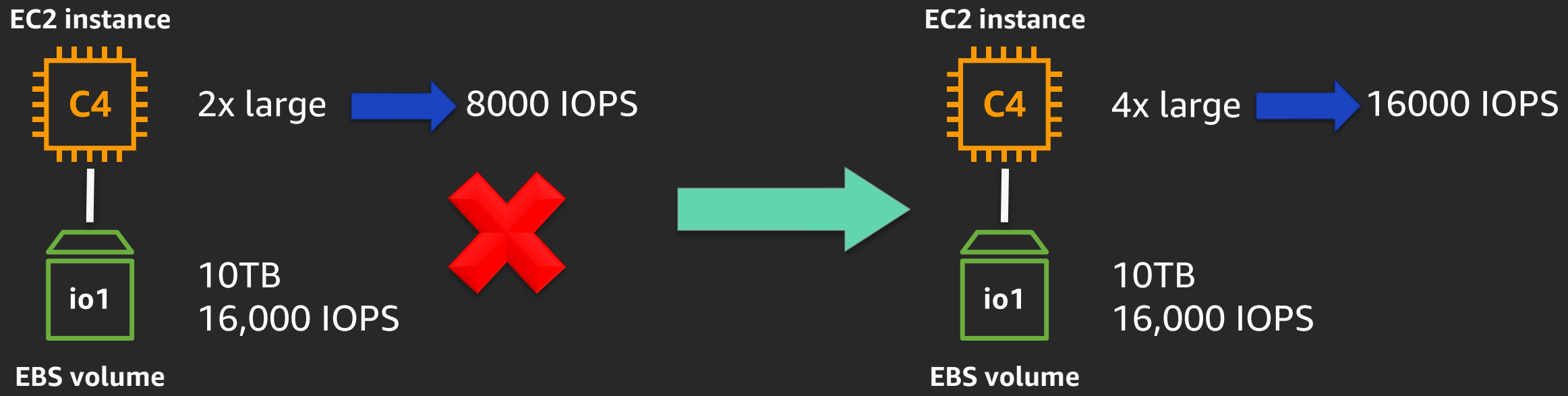


Increase the size of volumes and IOPS as you need it – rather than all up-front

```
aws ec2 modify-volume --volume-id vol-00d820abc6be8d639 --size 10000 --iops 32000
```

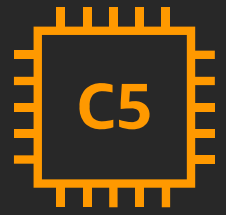
Remember to expand the file-system to take advantage of the increased capacity

Select the right instance size to match needs



Nitro: EBS Optimized Burst

- Nitro instances (*5*, i3n, t3, z1d) sizes < 4x large support EBS Optimized burst
- Burst IOPS and throughput run for up to 30 mins every 24h
- For workloads that need burst max < 30 mins, you could use a smaller size



Baseline			Burst	
65.525 MB/s	4000 IOPS	large	20000 IOPS	437.5 MB.s
100 MB/s	6000 IOPS	xlarge	20000 IOPS	437.5 MB/s
218.75 MB/s	10000 IOPS	2xlarge	20000 IOPS	437.5 MB/s

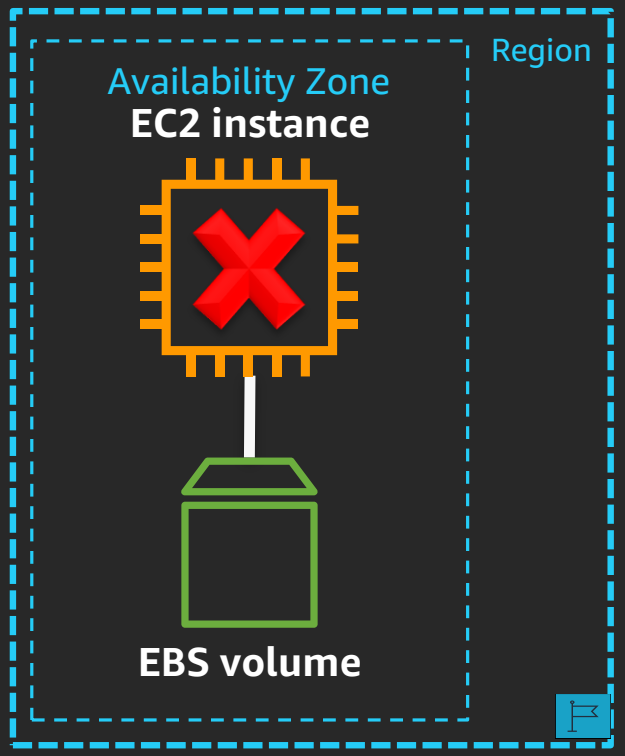
Tag Volumes and Snapshots on Create

- Tag volumes and snapshots at create time
- Delete volumes when instances and applications are terminated
- Use tags to keep track of resources and how they are created / allocated

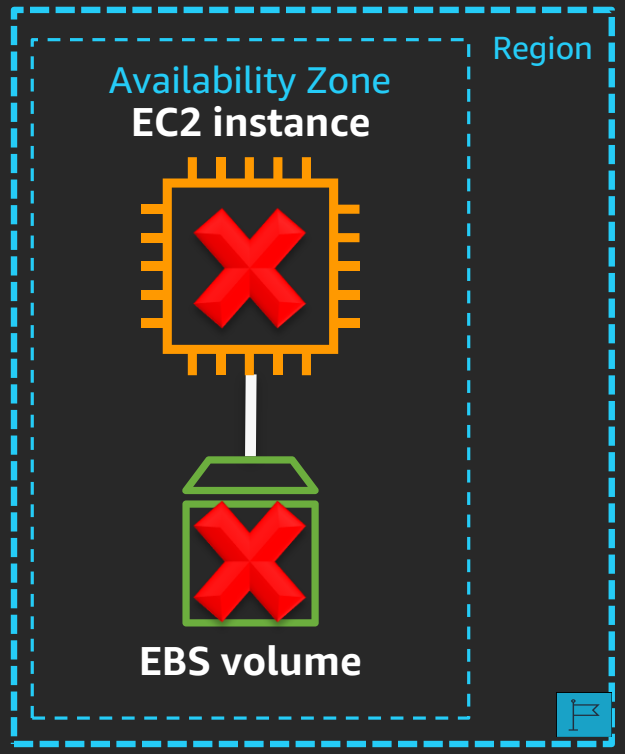
```
aws ec2 create-volume -snapshot-id snap-00d820abc6be8d639 --tag-specification
'ResourceType=volume Tags=[{Key=CostCenter,Value=115},{Key=IsProd,Value=Yes}]'
```

```
aws ec2 create-snapshot --volume-id vol-03f3c34ded2e3398f --tag-specification
'ResourceType=snapshot Tags=[{Key=CostCenter,Value=115},{Key=IsProd,Value=Yes}]'
```

Set DeleteOnTermination = TRUE if storage lifecycle = instance lifecycle



`DeleteOnTermination = FALSE`

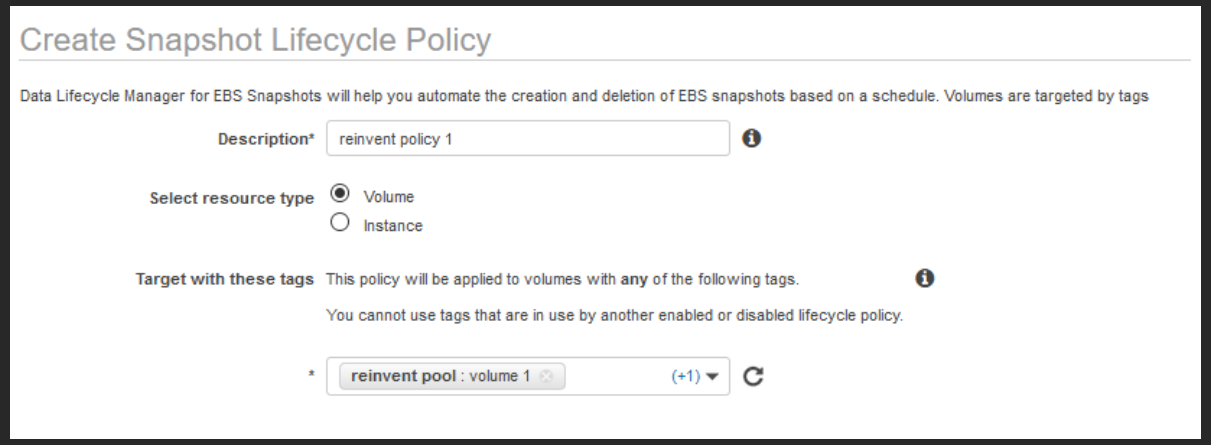


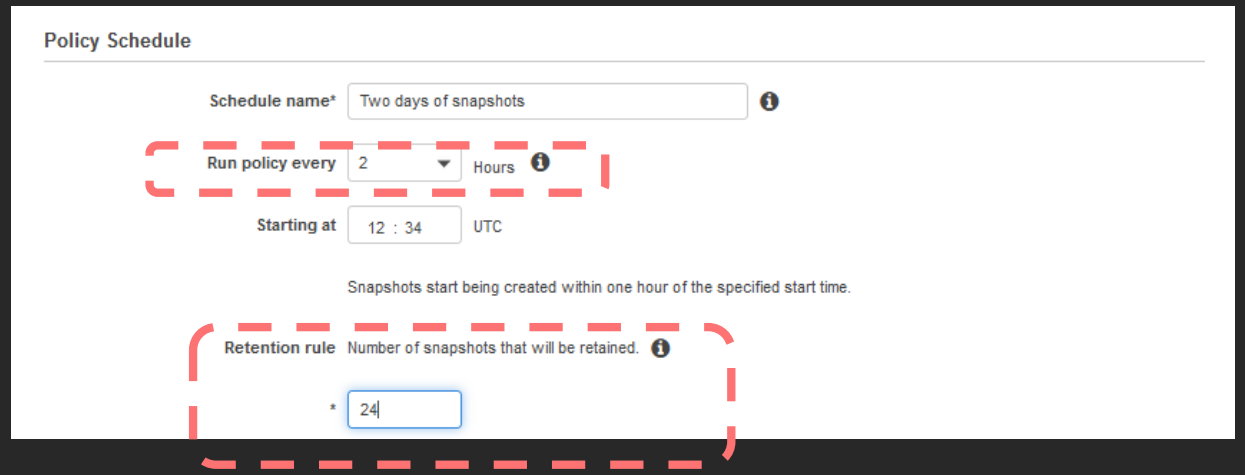
`DeleteOnTermination = TRUE`

USE WITH CARE – You might delete volumes you need

Manage Snapshot costs with Data Lifecycle Manager

- Set policies on when snapshots are taken and how many snapshots to keep in a lineage
- Use cost allocation tags to track snapshot costs

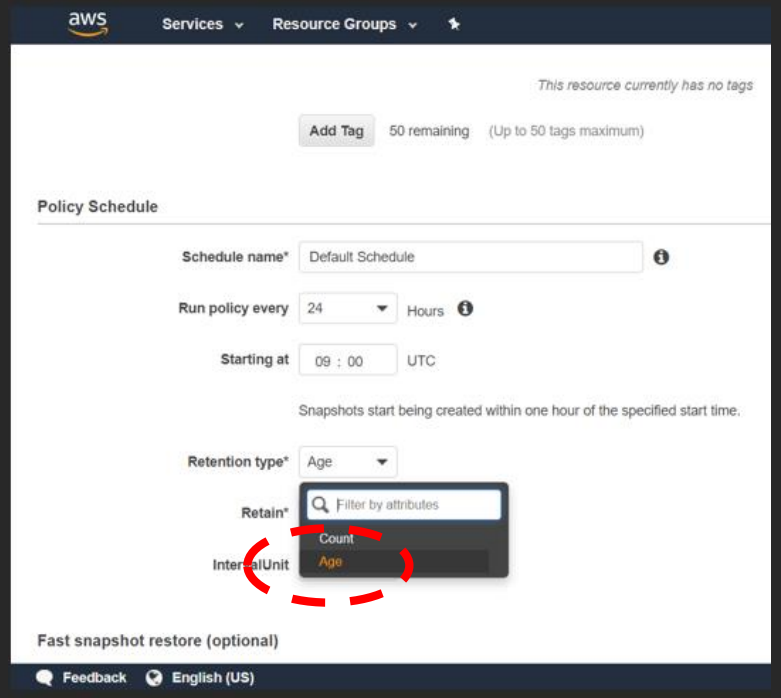


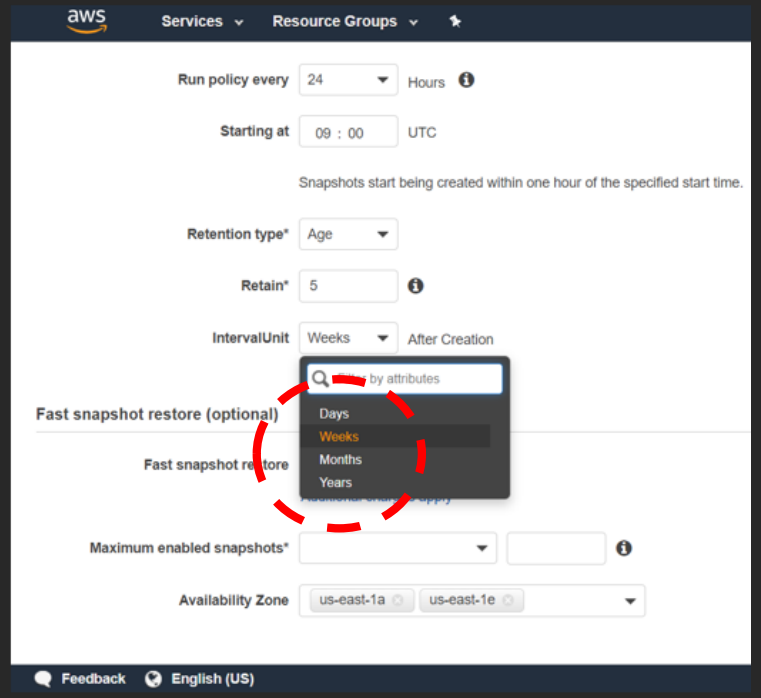


NEW

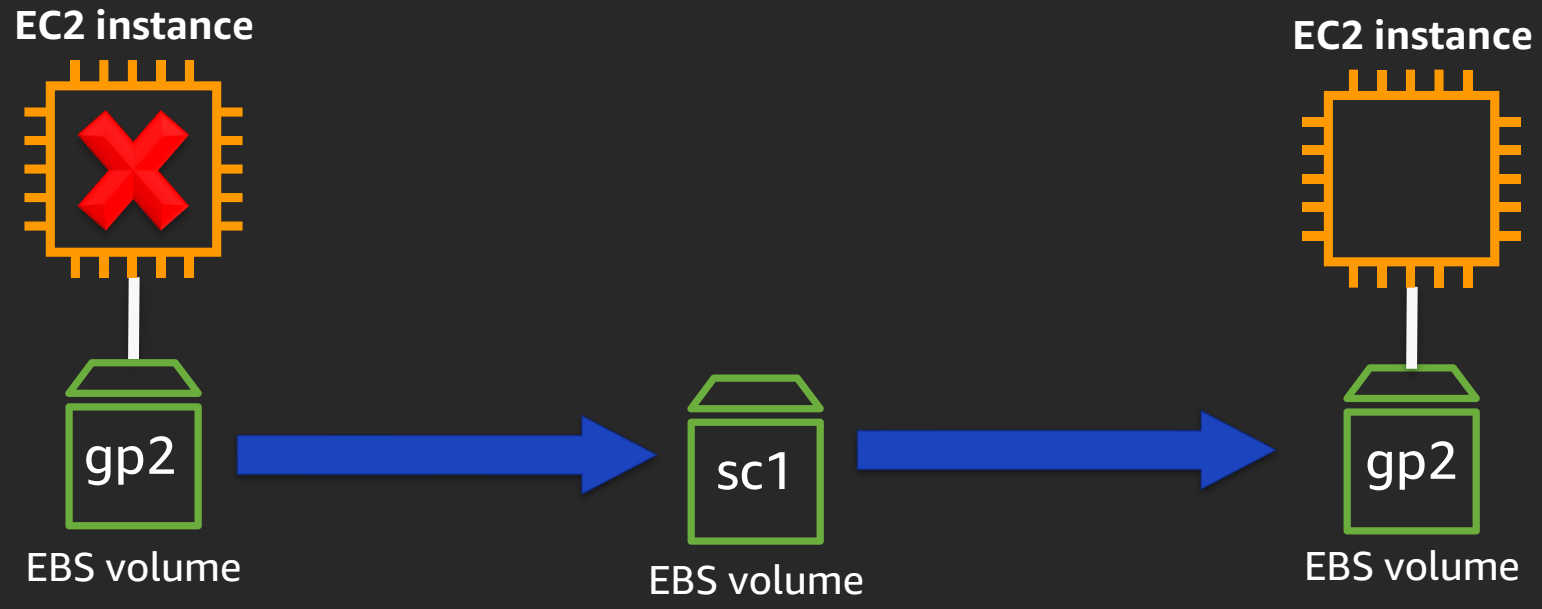
Snapshot Time-Based Data Lifecycle Manager Policies

- NEW: Create retention policies that are based on Snapshot Age
- Snapshot retention now possible based on # of days, weeks, months
- Meet your business compliance and DR needs





Tier to lower cost volume type if volume is not in use



- Move to lower cost tier if detached longer than
  - 6h (EV time limit) or
  - time to modify-volume
- Especially helpful for predictable schedules e.g. weekends, month ends

Use with care: Delete volumes you don’t need

- Figure out volumes that have been detached
- Using CloudWatch events (or tags), figure out how long these have been detached
- Set an explicit org policy for how long volumes can stay detached
- STRONGLY ADVISE: Take snapshots of these volumes
- Delete volumes

How Teradata uses EBS

Vinod Raman
Product Manager
Teradata

Mahesh Subramanian
Senior Director, Engineering
Teradata

AWS re:Invent

aws

Teradata is Cloud-First with Enterprise Scalability

ticketmaster · SIEMENS · PHILIPS · MONSANTO · AVIVA

Joint Customers with AWS

157 certifications

5,400 accreditations

9 Well-Architected reviews

$2.2B
Revenue

Consecutive leadership positions in analyst evals for 17+ years

9K
Employees

Worldwide Presence

Teradata Serves Industry-Leading Customers

18 of the top 20

Global Banks use Teradata to grow revenue across channels

19 of the top 20

Communication Providers use Teradata to optimize operations

15 of the top 20

Global Retailers use Teradata to improve customer experience

All of the top 6

Airlines uses Teradata to maximize customer experience

11 of the top 20

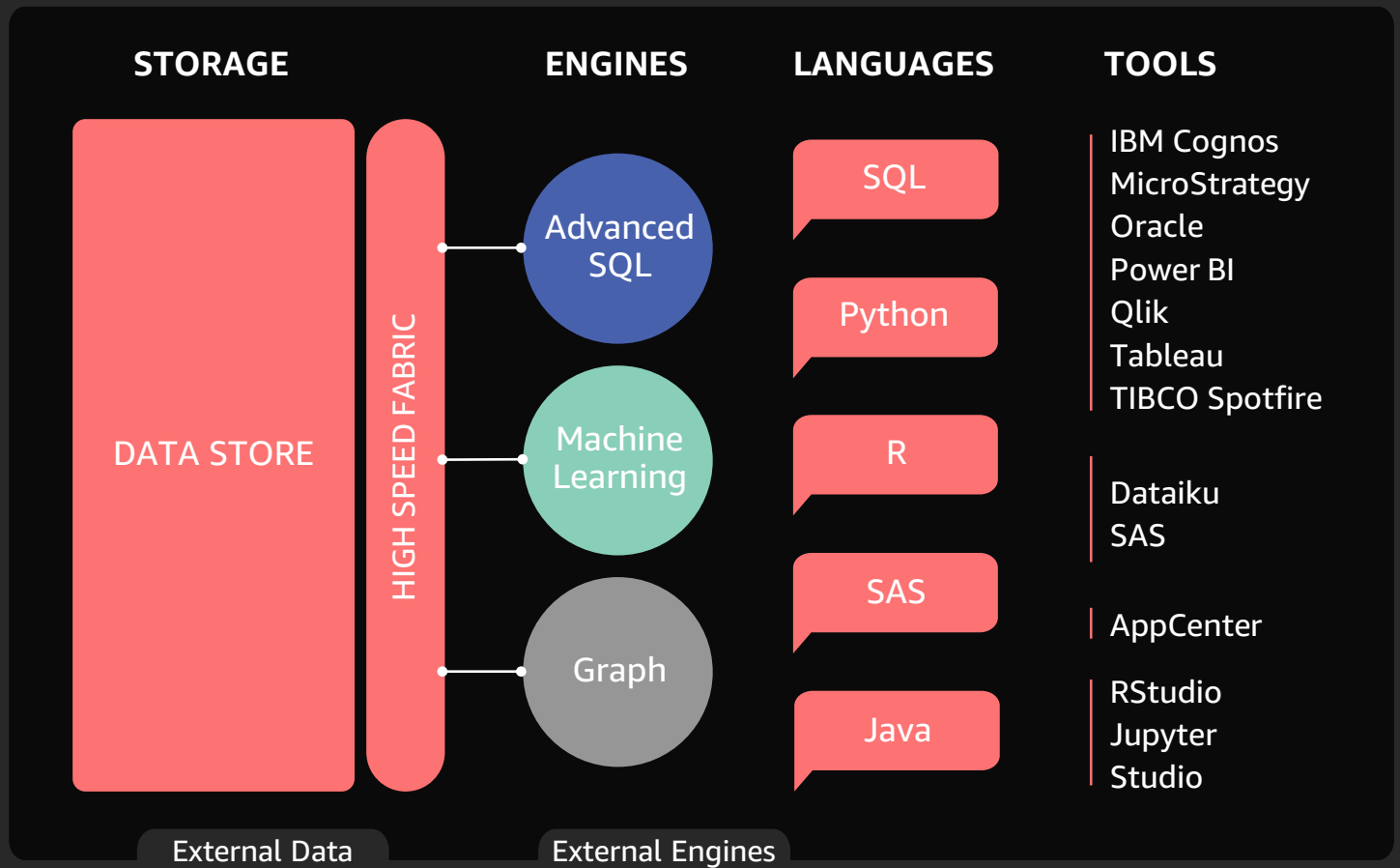
Healthcare companies use us to drive better medical outcomes

13 of the top 20

Global manufacturing firms use Teradata to increase throughput

Teradata Vantage: Analytics Platform Software

- **Any** tool
- **Any** language
- **100%** of the data



Customer Use Cases for Vantage on AWS

Millions of queries. Thousands of users. Hundreds of applications.

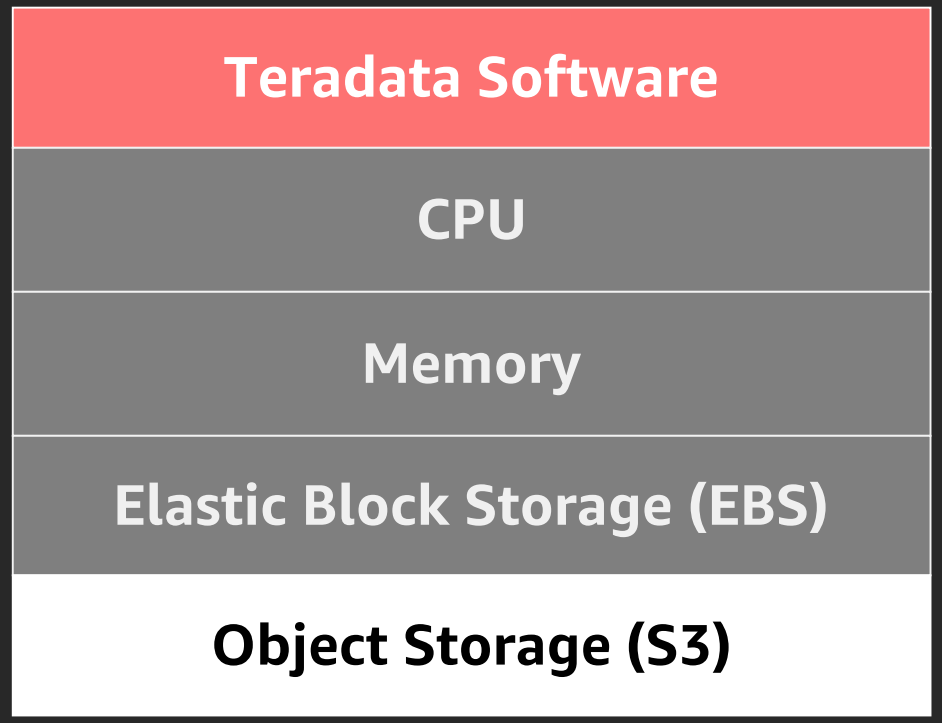
Production Analytics

Development & Test

Discovery Analytics

Disaster Recovery

Vantage Leverages Multiple Storage Types



- **Memory:** For the small small amounts of data that are frequently queried.
- **EBS:** For persistent data that needs to be accessed or updated often and needs performance SLAs
- **S3:** Large volumes of unstructured data in data lakes

Overall Workload Characteristics

Teradata Vantage is typically the “source of truth” for the enterprise

- **Enterprise Data Warehouse**
  - Advanced SQL Engine: Well-curated business-critical data used for reporting
  - Machine Learning and Graph Engines: Data science, model training and inference
- **Leverages both EBS and S3**
  - To ensure availability against isolated local failures and zonal events
- **Vantage can be CPU or Memory or Throughput-to-Storage intensive**
  - CPU-intensive: IOT sensor and time series analytics
  - Memory-intensive: Machine learning and model training
  - Throughput-intensive: Complex SQL queries
- **Vantage workload profile is 90% Read and 10% Write**
  - A balance of High Throughput and IOPS

Why GP2 SSD for Vantage

- Teradata Vantage leverages **General Purpose SSD (gp2)** EBS volumes to deliver optimal price and performance for our customers

- **Teradata Vantage primarily uses a 96KB IO**
  - Relatively small IO sizes ranging from 4KB to 512 KB

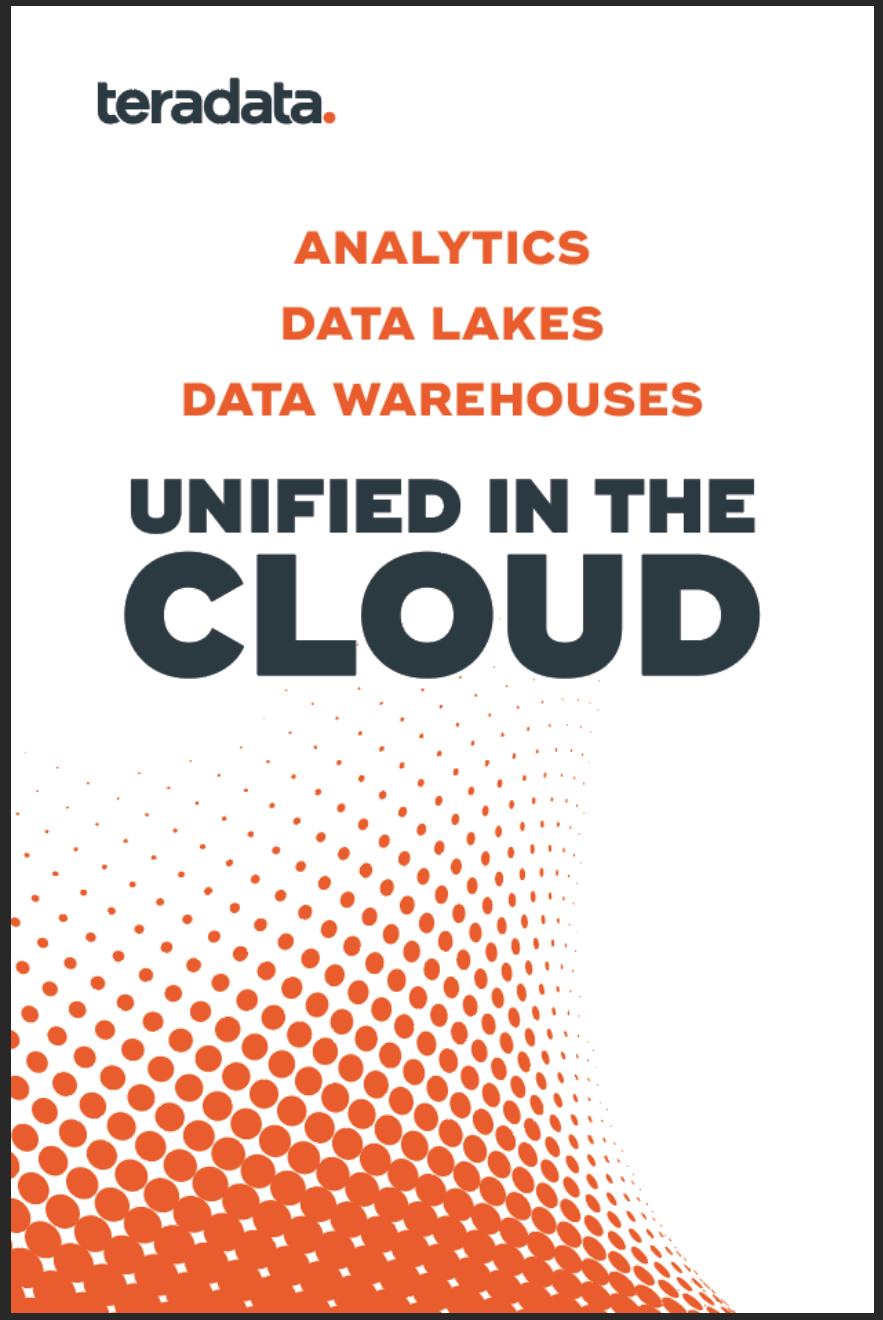
- Throughput Optimized HDD (st1) does not meet the performance needs of Vantage given the small IO size and the random nature of IO

- The price and consistency offered by Provisioned IOPS SSD (io1) is not needed to meet the needs of Vantage

Partnership with EBS

- **Expansion of EBS volumes using Elastic Volumes:**
  - Teradata was an early adopter of EBS APIs to expand volumes
  - This allows Teradata Vantage to expand EBS storage based on customer needs
  - No need to re-deploy clusters to expand storage

- **Crash-consistent EC2-wide snapshot:**
  - Teradata is an early partner to adopt this new feature
  - This allows Teradata Vantage to offer faster and smoother backups
  - Early tests show promising results that can speed up backups and let us offer lower RPOs
  - Teradata Vantage also leverages this capability to offer Disaster Recovery (DR) for customers with specific RTO/RPO SLAs



Visit Our Booth

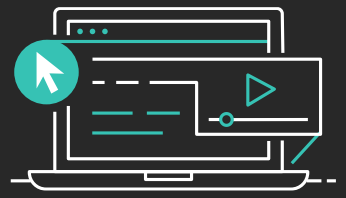
#405

teradata.com/AWS

#AnswersInTheCloud

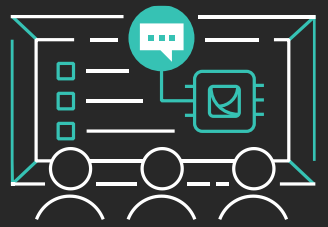
Learn storage with AWS Training and Certification

Resources created by the experts at AWS to help you build cloud storage skills



45+ free digital courses cover topics related to cloud storage, including:

- Amazon S3
- AWS Storage Gateway
- Amazon S3 Glacier
- Amazon Elastic File System (Amazon EFS)
- Amazon Elastic Block Store (Amazon EBS)



Classroom offerings, like Architecting on AWS, feature AWS expert instructors and hands-on activities

Visit aws.amazon.com/training/path-storage/

aws training and certification

Thank you!

AWS re:Invent

aws

Please complete the session survey in the mobile app.