DynamoDB Immersion Day!

For Operations and DBAs

Sean Shriver

DynamoDB/DAX SA
AWS

Girish Gangadharan

Enterprise Support Lead
AWS

April 2020

1

Overview

Best Practices
Security
Monitoring

2

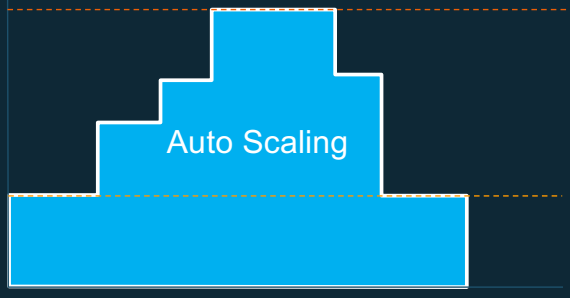
Best Practices

3

Choose the right capacity mode

Provisioned

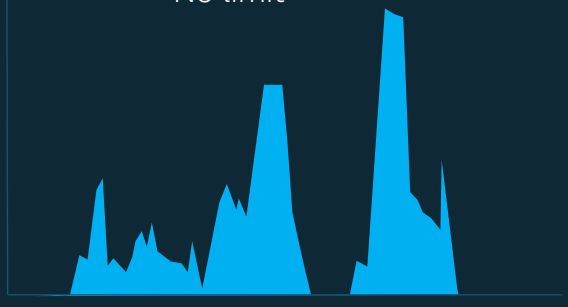
Govern max consumption



Set a minimum

On-Demand

No limit



Start at zero

4

Quantify the provisioned throughput needed for the event

- 1 RCU = One 4KB strongly consistent read
  - or 2 4KB eventually consistent reads
- 1 WCU = One 1KB write

- RCU Needed = Round Up (Item Size in KB/4KB) X Reads per second
- WCU Needed = Round Up (Item Size in KB/1KB) X Writes per second

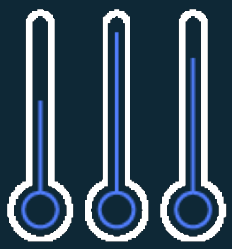
** Single partition can handle 3,000 RCUs or 1,000 WCUs.

aws

5

Know the account limits of your AWS account

- Each AWS account has initial limits on the maximum RCU/WCU
- Use **DescribeLimits** API to know the limits of your account
- Use CloudWatch



aws

6

Check if you need to store large item

- Identify access pattern
- Compress large attributes values
- Store it in S3

UserID	Ranking	Metadata
U001	1	Abcd……

Assuming total item size is 2.5KB
Consumption: 3 WCU

Assuming 2KB payload

pk	sk	Ranking	md
U001	Ranking	1	
U001	Metadata		Abcd….

Assuming total item size for storing ranking is 17byte
Consumption: 1 WCU

aws

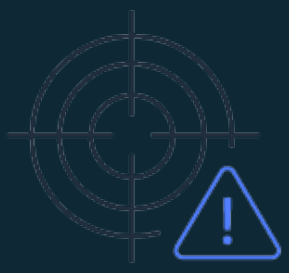
7

Enable monitoring and set up alarms

- ConsumedReadCapacityUnits
- ConsumedWriteCapacityUnits

- ReadThrottleEvents
- WriteThrottleEvents

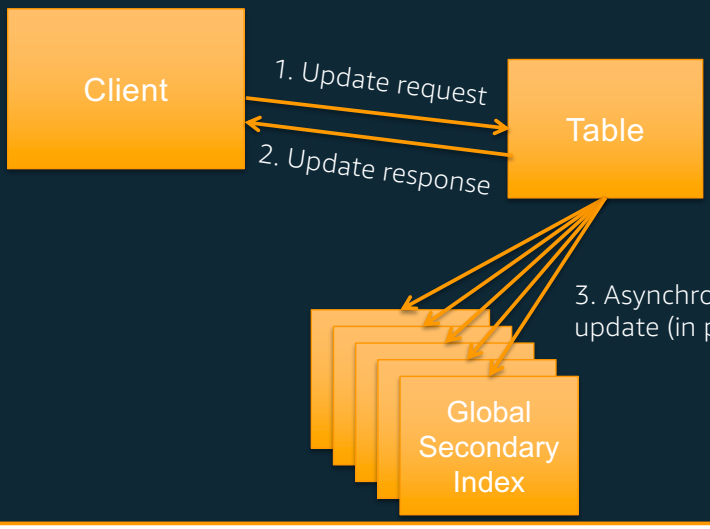
- ThrottledRequests
- SuccessfulRequestLatency
- SystemErrors



aws

8

Global secondary index (GSI) – understand the behavior



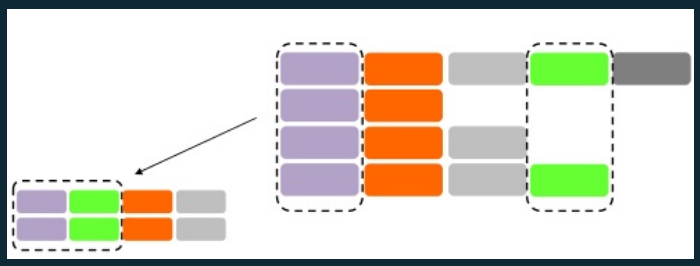
If GSIs don't have enough write capacity, table writes will be throttled

aws

9

Local secondary index (LSI) – understand the behavior

- 10 GB size limit per partition key value
- Capacity management
- LSI lifecycle



aws

10

Smaller attribute length improves efficiency

Per item size : **66 bytes**

```
{
   “pk”: {
      "S": "f0ba8d6c"
   },
   "fullname": {
      "S": “Gac Masudur"
   },
   "BirthDate": {
      "S": “10-Dec-1990"
   },
   "HomeAddress": {
      "S": "Sydney"
   }
}
```

1billion items X 66 bytes
66 GB Storage

Per item size: **44 bytes**

```
{
   “pk”: {
      "S": "f0ba8d6c"
   },
   "fn": {
      "S": “Gac Masudur"
   },
   "bd": {
      "S": “10-Dec-1990"
   },
   "ha": {
      "S": "Sydney"
   }
}
```

1billion items X 44 bytes
44 GB Storage
22 GB storage savings

aws

11

Smaller attribute length improves efficiency

Per item size : **1,025 bytes**


```
{
   "id": {
      "S": "f0ba8d6c"
   },
   "fullName": {
      "S": "Sayem"
   },
   "someData": {
      "S":
"dGhpcyB0ZXh0IGIzIGJhc2U2NC1lbmNvZGVkdGhpcyB0ZXh0IGIzIGJhc2U2NC1lbmNvZGVkdGhpcyB0ZXh0IGIz
IGJhc2U2NC1lbmNvZGVkdGhpcyB0ZXh0IGIzIGJhc2U2NC1lbmNvZGVkdGhpcyB0ZXh0IGIzIGJhc2U2NC1lbmN
vZGVkdGhpcyB0ZXh0IGIzIGJhc2U2NC1lbmNvZGVkdGhpcyB0ZXh0IGIzIGJhc2U2NC1lbmNvZGVkdGhpcyB0ZX
h0IGIzIGJhc2U2NC1lbmNvZGVdGhpcyB0ZXh0IGIzIGJhc2U2NC1lbmNvZGVkdGhpcyB0ZXh0IGIzIGJhc2U2NC1l
bmNvZGVkdGhpcyB0ZXh0IGIzIGJhc2U2NC1lbmNvZGVkdGhpcyB0ZXh0IGIzIGJhc2U2NC1lbmNvZGVkdGhpcy
B0ZXh0IGIzIGJhc2U2NC1lbmNvZGVkdGhpcyB0ZXh0IGIzIGJhc2U2NC1lbmNvZGVdGhpcyB0ZXh0IGIzIGJhc2U
2NC1lbmNvZGVkdGhpcyB0ZXh0IGIzIGJhc2U2NC1lbmNvZGVkdGhpcydGhpcyB0ZXh0IGIzIGJhc2U2NC1lbmNv
ZGVkdGhpcyB0ZXh0IGIzIGJhc2U2NC1lbmNvZGVkdGdGhpcyB0ZXh0IGIzIGJhc2U2NC1lbmNvZGVkdGhpcyB0Z
Xh0IGIzIGJhc2U2NC1lbmNvZGVkdGhpcyB0ZXh0IGIzIGJhc2U2NC1lbmNvZGVkhpcyB0ZXh0IGIzIGJhc2U2NC1l
bmNvZGVkdGhpcyB0ZXh0IGIzIGJhc2U2NC1lbmNvZGVkdGhpcyB0ZXh0IG2U2NC1lGhpcyBXh0IGNC1lbmNvZGVkIzI
GJhc2U2NC1lbmNvZGVkkkGVkdGhpcGIGJhcGh0IGhpcyBXh0IGIzIGJhcIGJhc2U2Nasdasdasw8734nhu3==“
   },
   "favouriteNumber": {
      "N": "-1E-130"
   },
   "foods": {
      "SS": [
         "pizza",
         "burger"
      ]
   }
}
```


10K writes per second
2WCU x 10K items = 20,000 WCU

Per item size: **995 bytes**

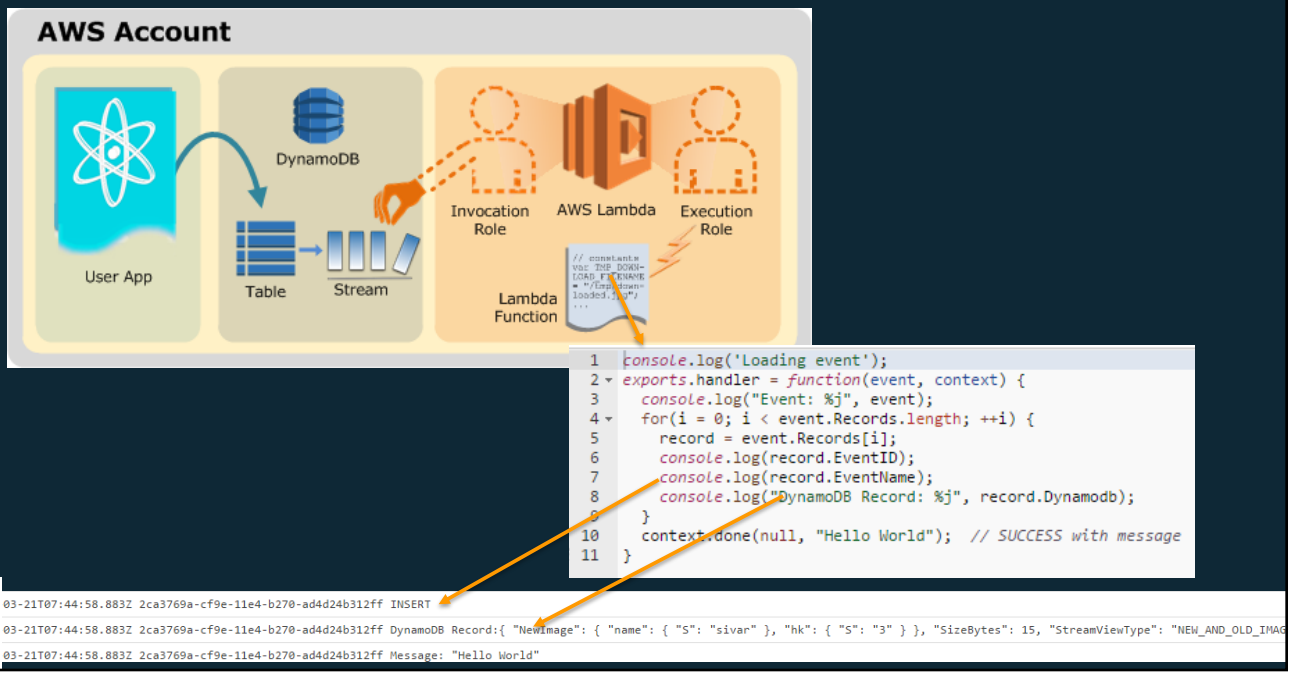

```
{
   "id": {
      "S": "f0ba8d6c"
   },
   "fln": {
      "S": "Sayem"
   },
   "sd": {
      "S":
"dGhpcyB0ZXh0IGIzIGJhc2U2NC1lbmNvZGVkdGhpcyB0ZXh0IGIzIGJhc2U2NC1lbmNvZGVkdGhpcyB0ZXh0IGIz
IGJhc2U2NC1lbmNvZGVkdGhpcyB0ZXh0IGIzIGJhc2U2NC1lbmNvZGVkdGhpcyB0ZXh0IGIzIGJhc2U2NC1lbmN
vZGVkdGhpcyB0ZXh0IGIzIGJhc2U2NC1lbmNvZGVkdGhpcyB0ZXh0IGIzIGJhc2U2NC1lbmNvZGVkdGhpcyB0ZX
h0IGIzIGJhc2U2NC1lbmNvZGVdGhpcyB0ZXh0IGIzIGJhc2U2NC1lbmNvZGVkdGhpcyB0ZXh0 IGIzIGJhc2U2NC1l
bmNvZGVkdGhpcyB0ZXh0IGIzIGJhc2U2NC1lbmNvZGVkdGhpcyB0ZXh0 IGIzIGJhc2U2NC1lbmNvZGVkdGhpcy
B0ZXh0 IGIzIGJhc2U2NC1lbmNvZGVkdGhpcyB0ZXh0 IGIzIGJhc2U2NC1lbmNvZGVdGhpcyB0ZXh0 IGIzIGJhc2U
2NC1lbmNvZGVkdGhpcyB0ZXh0 IGIzIGJhc2U2NC1lbmNvZGVkdGhpcydGhpcyB0ZXh0 IGIzIGJhc2U2NC1lbmNv
ZGVkdGhpcyB0ZXh0 IGIzIGJhc2U2NC1lbmNvZGVkdGdGhpcyB0ZXh0 IGIzIGJhc2U2NC1lbmNvZGVkdGhpcyB0Z
Xh0 IGIzIGJhc2U2NC1lbmNvZGVkdGhpcyB0ZXh0 IGIzIGJhc2U2NC1lbmNvZGVkhpcyB0ZXh0 IGIzIGJhc2U2NC1l
bmNZXhhpcyB0ZXh0 IGIzIGJhc2U2NC1lbmNvZGVkdGhpcyB0ZXh0 IG2U2NC1 IGhpcyBXh0 IGNC1 lbmNvZGVkIzI
GJhc2U2NC1 lbmNvZGVkkkGVkdGhpcGIGJhcGh0 IGhpcyBXh0 IGIzIGJhcIGJhc2U2N==“
   },
   "fn": {
      "N": "-1E-130"
   },
   "foods": {
      "SS": [
         "pizza",
         "burger"
      ]
   }
}
```


10K writes per second
1WCU x 10K items = **10,000 WCU**

aws

12

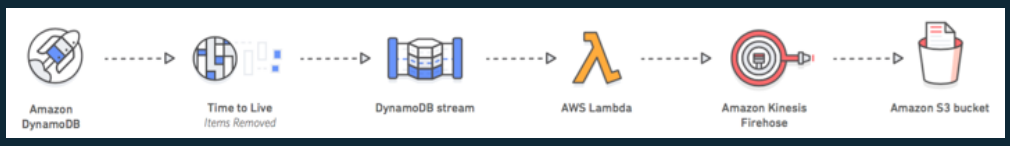
DynamoDB Streams and AWS Lambda



13

Use the power of TTL

- Expire item automatically
- Zero cost
- Zero performance impact
- Auto archive items



aws

14

Security

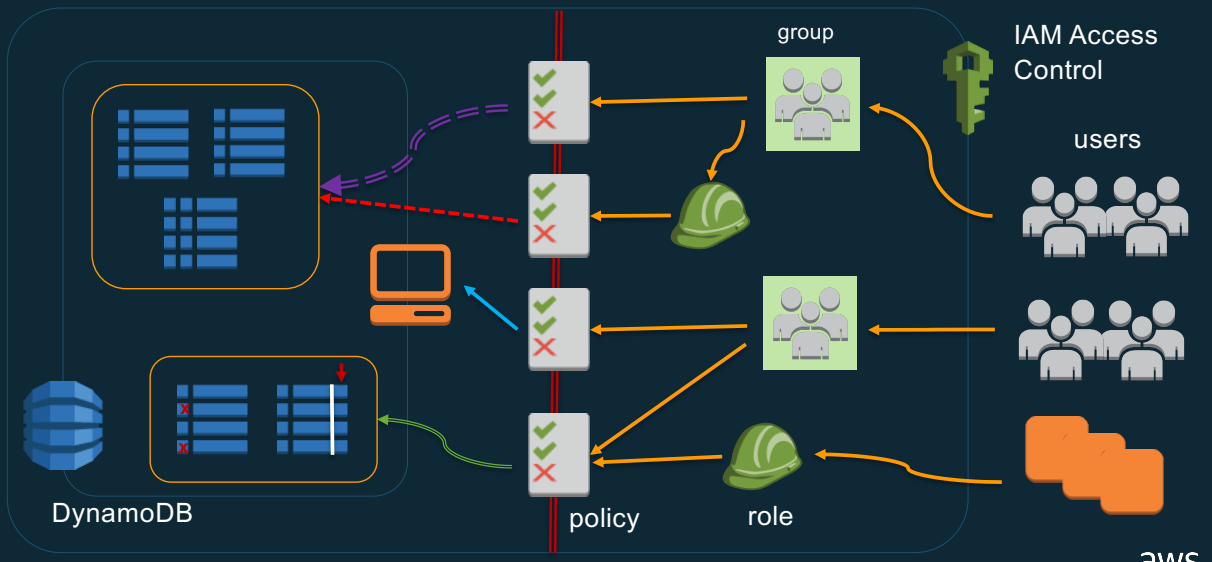
15

Security – Access Control

- AWS Identity and Access Management (IAM) provides access control
  - IAM policy is a basic protection – it's a gate
  - Create different "gates" for different parts of your "property"

16

Access Control in DynamoDB



17

Access Control for DynamoDB

- Resource ownership
  - The AWS account owns the resources created in the account
- Identity based policies
  - Resource based policies not supported
  - Policies attached to IAM identities
    - User, group, role
- Fine-grained access control (FGAC)
  - Control access to items based on primary key
  - Control access to attributes based on a condition
- Federated access

18

Access Control for DynamoDB

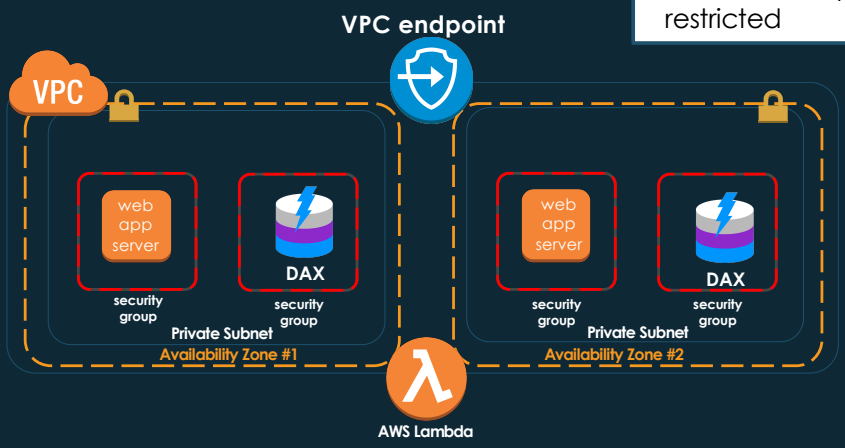
- Follow the principle of least privilege
  - Create policies with only the necessary permissions
    - Create per application policies, roles, and groups
      - Use application specific prefixes and "*"
- Protect against sensitive operations by creating special roles
  - Example: DeleteTable in production requires a role
- Split dev/test work into a separate account from prod
- Consider account separation for different workloads

aws

19

Access Control in the VPC

VPC endpoints
- DynamoDB-in-the-VPC
- IAM resource policy restricted

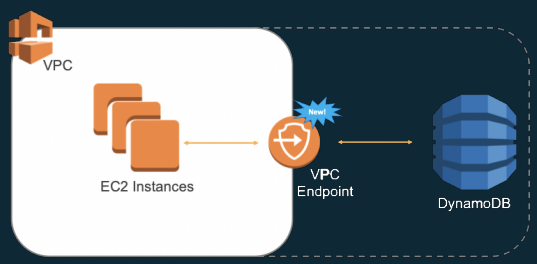


DAX
- Role-based access control
- No IGW or VPC endpoint required
- Private IP, client-side discovery

aws back

20

VPC Endpoints for DynamoDB (VPC-E)



- Access DynamoDB via secure Amazon VPC endpoint
- Customize access for each VPC endpoint with unique IAM role and permissions

- Turn off access from public Internet gateways enhancing privacy and security
- Secure data transfer between Amazon VPC and DynamoDB without IGW or NATGW
- Simplified network configuration
- Cost savings – no extra charges

aws

21

VPC Endpoints: things to know

- General endpoint limitations, e.g:
  - Endpoints are supported for IPv4 traffic only
  - Endpoint connections cannot be extended out of a VPC
  - Endpoints cannot be transferred to another VPC or service
- DynamoDB streams cannot be accessed via endpoints
- Only same region traffic supported
- Tailor the IAM access policy for your specific needs
  - Access only required resources
  - Use aws:sourceVpce condition to restrict access

aws

22

Protecting your Data in DynamoDB

Against Data Corruption
- Backup
- Table/app design

Against Disaster
- Within region: 3 AZs
- Cross-region: Global Tables

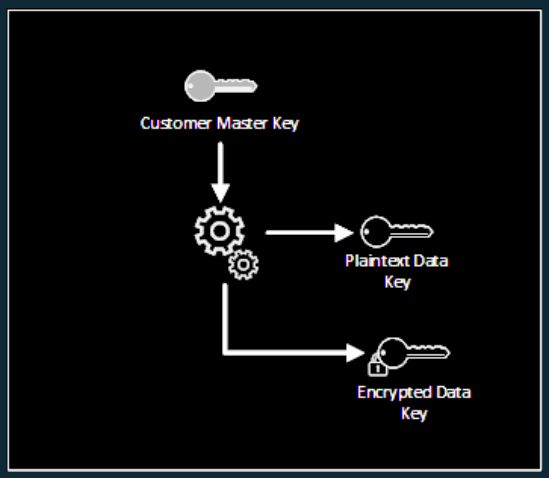
Against Disclosure
- Encryption

aws

23

Industry Standard Encryption

AES-256 Envelope Encryption



Fully integrated with KMS
- Customer Master Key for DynamoDB

Encrypts both base tables and indexes

Transparent process with minimal performance impact

No modification to application

aws

24

Encryption at rest

- Enabled on all tables by default
- Integrated with AWS KMS
  - AWS Owned Keys
  - AWS Managed CMKs
  - Customer Managed CMKs
- Key is refreshed every 5 min. per active client connection
  - KMS not called for every operation
  - For large number of callers, AWS Managed CMKs are expensive
- Data is encrypted at rest, including in Streams and in backups

aws

25

Logging and Monitoring for Security

AWS CloudTrail

Log DDL Ops:
CreateTable
DeleteTable
UpdateTable

AWS Config

Track resource config over time

DynamoDB related IAM resources

AWS CloudWatch

Watch and alert:
CreateTable
DeleteTable
UpdateTable

Auth Failures

Amazon SNS

Deliver notifications from CloudWatch alarms

aws

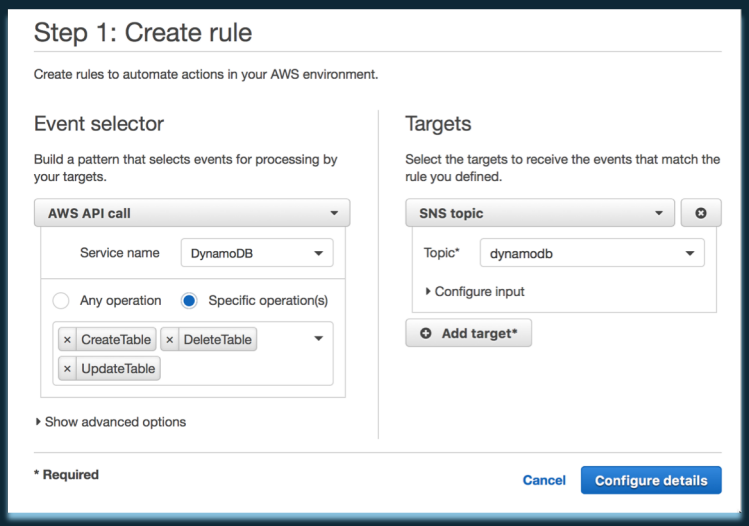
26

Logging and Monitoring for Security - Example

A CloudWatch filter rule to monitor for authorization failures in the logs

27

Logging and Monitoring for Security - Example



A CloudWatch Events rule to monitor for DynamoDB DDL operations and notify via SNS

Get notified when a table is created, deleted or updated.

28

Monitoring

29

Monitoring DynamoDB

AWS CloudTrail

Log API Calls

Send logs to CloudWatch

AWS CloudWatch

Monitor metrics and events

Receive and monitor CloudTrail logs

Create alarms on metrics and log events

Amazon SNS

Deliver notifications from CloudWatch alarms

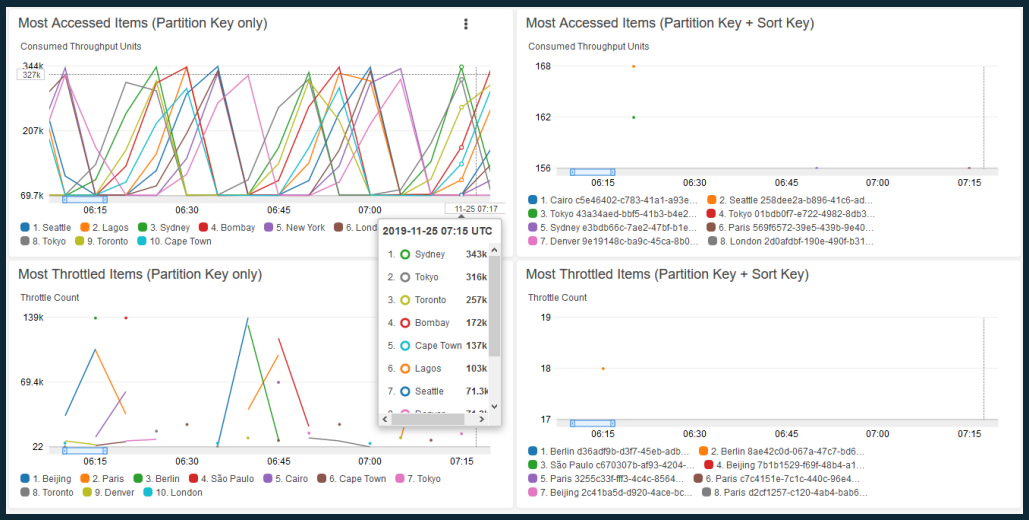
30

Monitoring DynamoDB
Operational Awareness

- https://aws.amazon.com/blogs/database/monitoring-amazon-dynamodb-for-operational-awareness/
- Follow the above blog post instructions for monitoring the most critical DynamoDB Cloudwatch Metrics and setting up alarms

31

Detecting Hot Spots
Cloudwatch Contributor Insights



32

Thank you!

aws

33