# Amazon DynamoDB Data Protection

Swetha Salunke

Senior Manager, Product Management
Amazon DynamoDB

# Origins of DynamoDB

# What was accomplished

## Last Oracle database turned off October, 2019

- 100% of Amazon proprietary systems
- 7,500 Oracle databases migrated
- Hundreds of PBs of data migrated
- Little to no downtime allowed
- No centralized IT – completely decentralized
- Each team owned their own migrations – no special SWAT team to do it for them

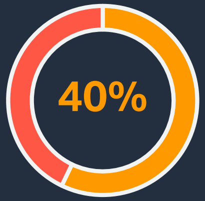
# Why we migrated

## Challenges keeping up with growing Amazon needs

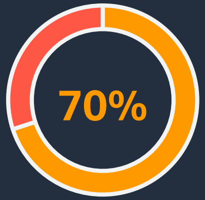
- Scalability risks: data volume, throughput, global market
- Latency risk: due to date volume and increased throughput
- Expensive and punitive Oracle licenses
- Availability risks due to legacy architectures
- Operational risks due to HW provisioning/management/lead times
- Millions of $USD in operational costs

Amazon.com cannot go down

# Overall Benefits for Amazon.com, Inc.



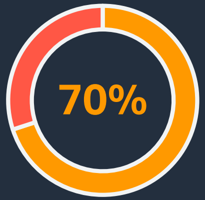
Reduction in latency, with 2x the number of transactions



Reduction in infrastructure costs

Eliminated CAPEX infrastructure costs

Transformed organization with cost model where each team now manages its own compute and storage infrastructure based on predicted usage and growth

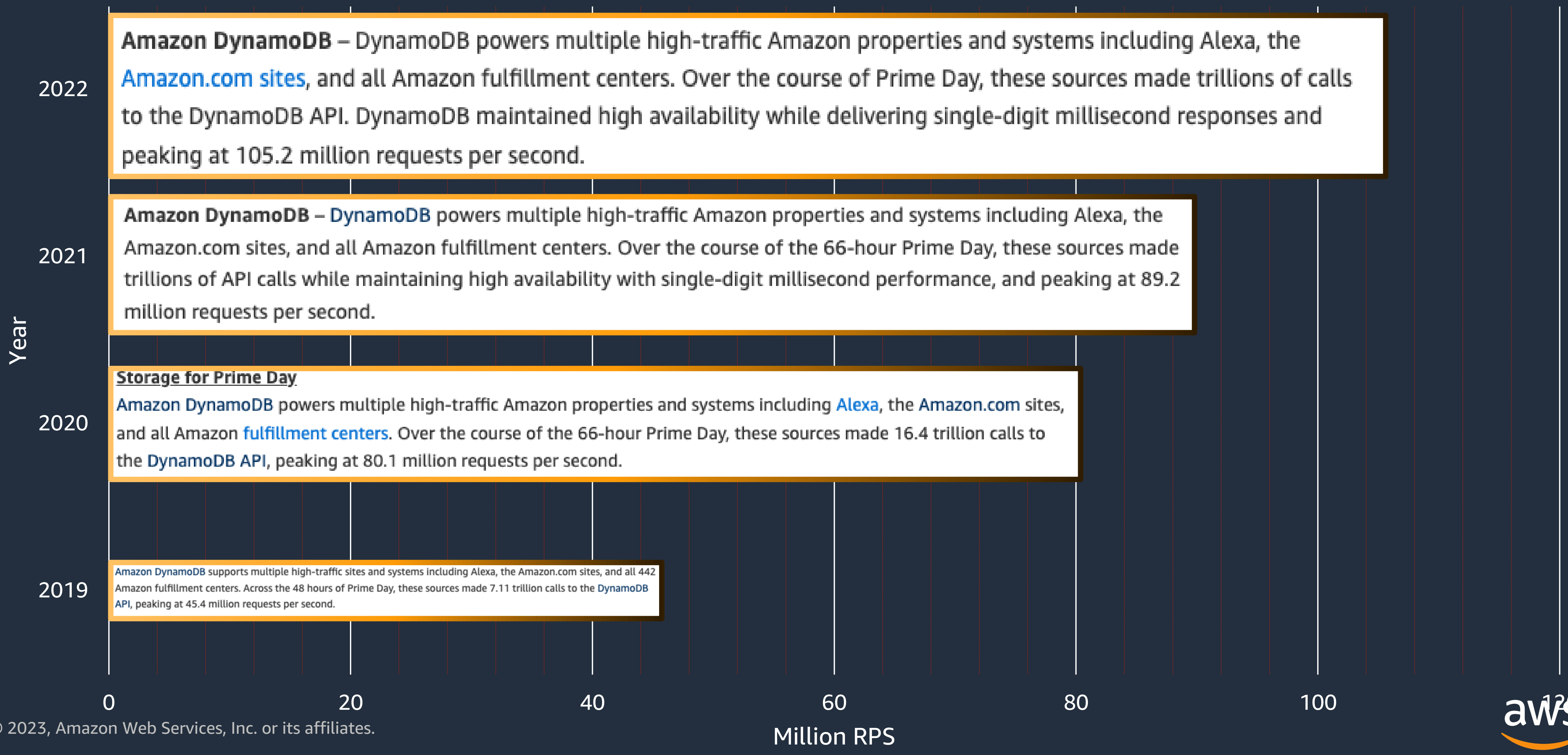


Reduction in database administration overhead and planning

Now focus on adding customer value

# DynamoDB + Scale – Amazon Prime Day

Prime Day - Peak Traffic (million RPS)



**Amazon DynamoDB** – DynamoDB powers multiple high-traffic Amazon properties and systems including Alexa, the Amazon.com sites, and all Amazon fulfillment centers. Over the course of Prime Day, these sources made trillions of calls to the DynamoDB API. DynamoDB maintained high availability while delivering single-digit millisecond responses and peaking at 105.2 million requests per second.

**Amazon DynamoDB** – DynamoDB powers multiple high-traffic Amazon properties and systems including Alexa, the Amazon.com sites, and all Amazon fulfillment centers. Over the course of the 66-hour Prime Day, these sources made trillions of API calls while maintaining high availability with single-digit millisecond performance, and peaking at 89.2 million requests per second.

**Storage for Prime Day**

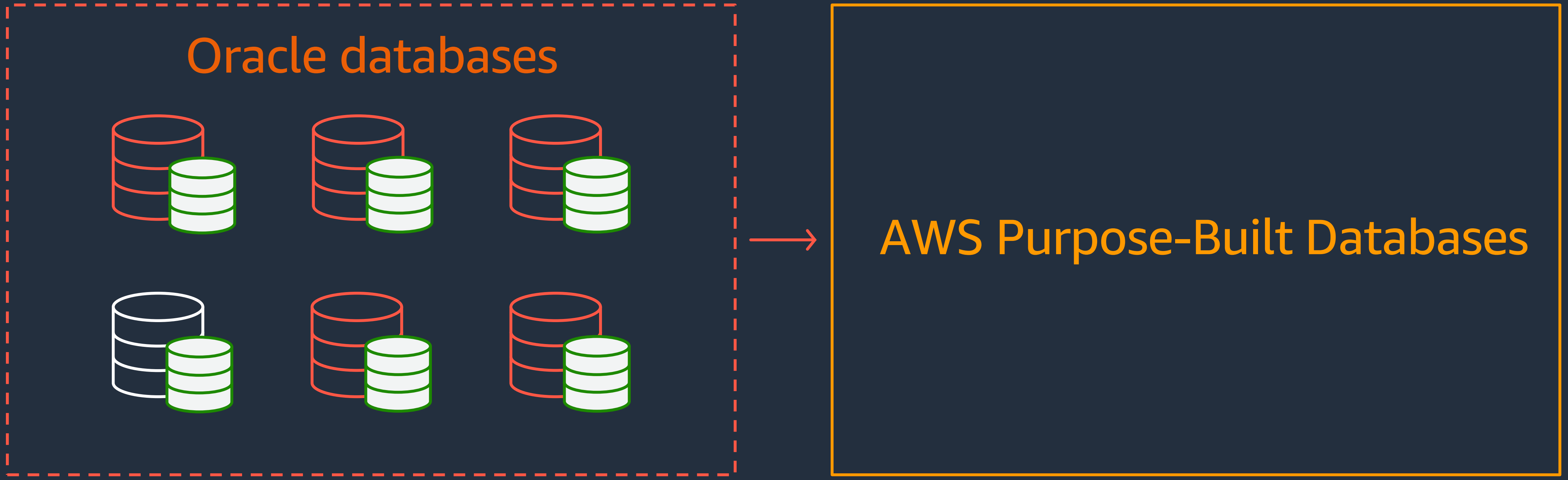
Amazon DynamoDB powers multiple high-traffic Amazon properties and systems including Alexa, the Amazon.com sites, and all Amazon fulfillment centers. Over the course of the 66-hour Prime Day, these sources made 16.4 trillion calls to the DynamoDB API, peaking at 80.1 million requests per second.

Amazon DynamoDB supports multiple high-traffic sites and systems including Alexa, the Amazon.com sites, and all 442 Amazon fulfillment centers. Across the 48 hours of Prime Day, these sources made 7.11 trillion calls to the DynamoDB API, peaking at 45.4 million requests per second.

# WHERE

## are we going?

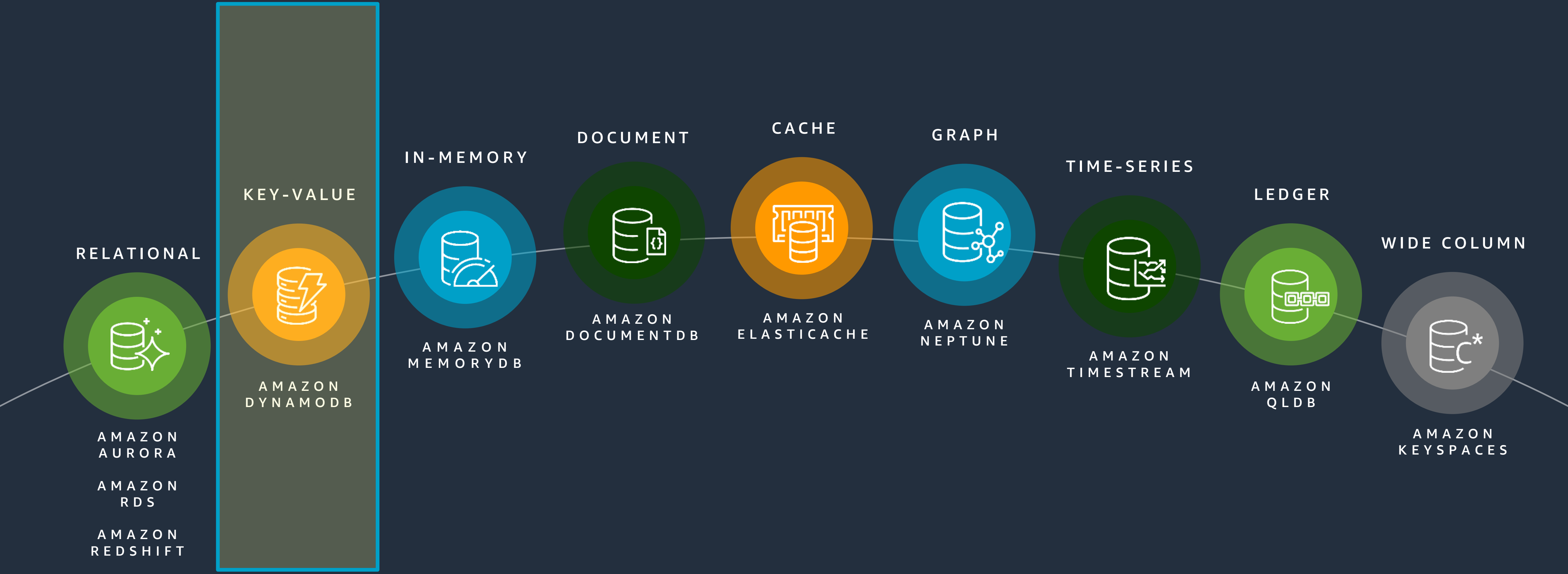
# Mission: Break free from Oracle



From Oracle, to what?

PURPOSE

# Purpose-built databases



RELATIONAL

AMAZON AURORA

AMAZON RDS

AMAZON REDSHIFT

KEY-VALUE

AMAZON DYNAMODB

IN-MEMORY

AMAZON MEMORYDB

DOCUMENT

AMAZON DOCUMENTDB

CACHE

AMAZON ELASTICACHE

GRAPH

AMAZON NEPTUNE

TIME-SERIES

AMAZON TIMESTREAM

LEDGER

AMAZON QLDB

WIDE COLUMN

AMAZON KEYSPACES

# Data Protection Strategies

# Agenda

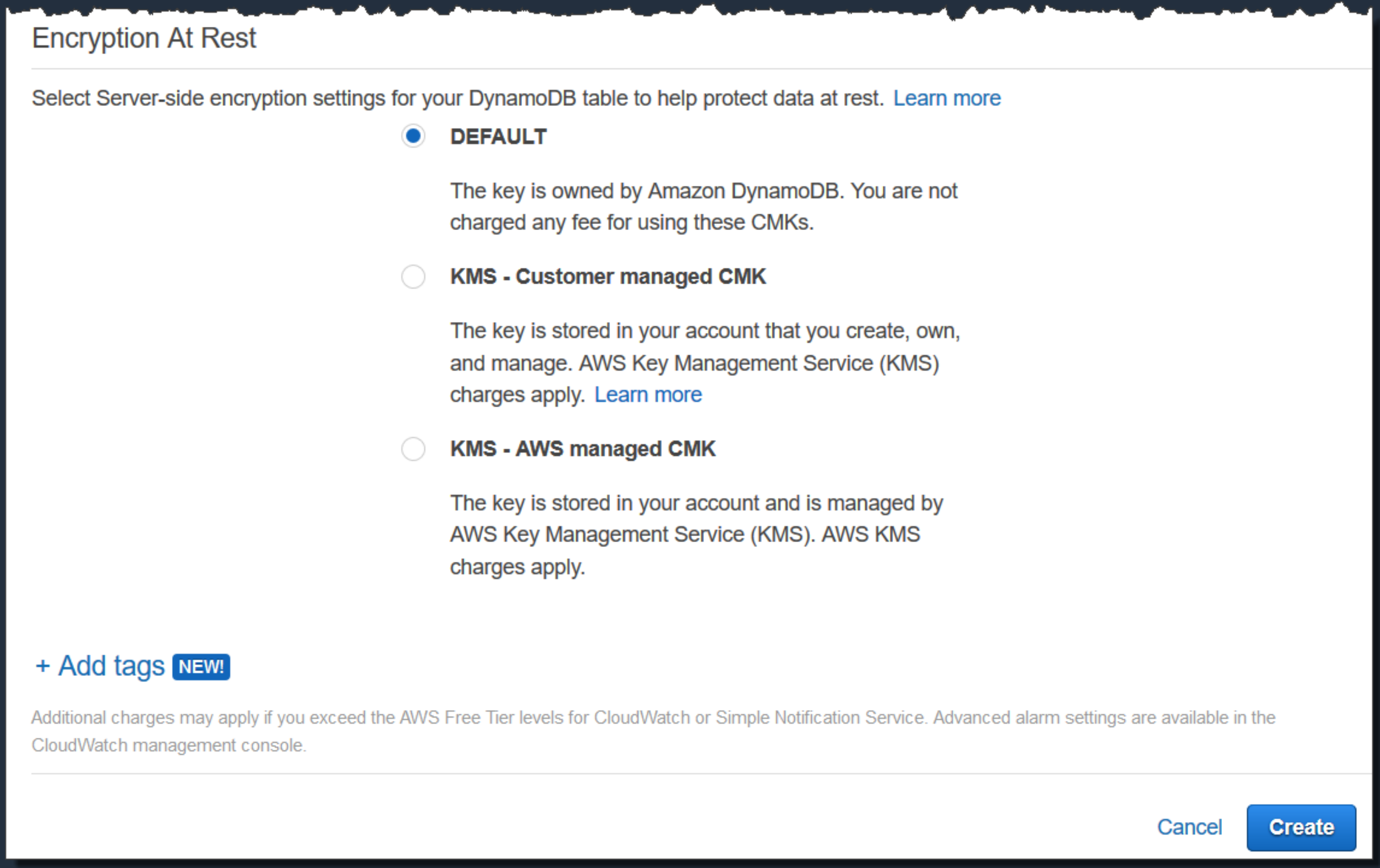
- Preventative security best practices
- Detective security best practices
- Backups
- Export to S3
- Point-in-time recovery
- Deletion protection

# Agenda

- Preventative security best practices
- Detective security best practices
- Backups
- Export to S3
- Point-in-time recovery
- Deletion protection

# Security: Preventative security best practices

## Enterprise ready



Encryption At Rest

Select Server-side encryption settings for your DynamoDB table to help protect data at rest. Learn more

● **DEFAULT**

The key is owned by Amazon DynamoDB. You are not charged any fee for using these CMKs.

○ **KMS - Customer managed CMK**

The key is stored in your account that you create, own, and manage. AWS Key Management Service (KMS) charges apply. Learn more

○ **KMS - AWS managed CMK**

The key is stored in your account and is managed by AWS Key Management Service (KMS). AWS KMS charges apply.

Additional charges may apply if you exceed the AWS Free Tier levels for CloudWatch or Simple Notification Service. Advanced alarm settings are available in the CloudWatch management console.

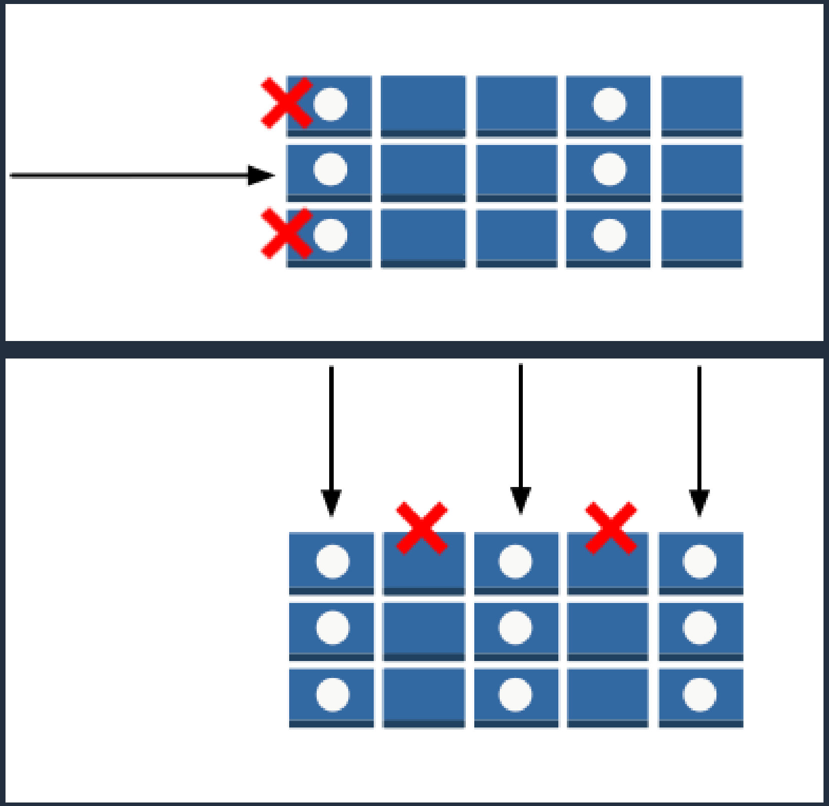
Fully integrated with AWS Identity and Access Management (IAM)

Access DynamoDB via secure Amazon VPC endpoints

All tables encrypted in transit and at rest by default

# Security: Role-Based Access Controls

## Enterprise ready



- **Permissions are set in IAM:** Integrated with access control of users/roles.
- **Fine Grained Control:** Gate access to management APIs, tables, indexes, leading keys, specific attributes, backups, etc…
- **Leverage IAM conditions:** Supports variables, i.e.: userID, Account, OrganizationID, Source IP, Time, etc

# Agenda

- Preventative security best practices
- Detective security best practices
- Backups
- Export to S3
- Point-in-time recovery
- Deletion protection

# Security: Detective security best practices with CloudTrail

## Enterprise ready

- Capture and log all control-plane operations (such as CreateTable, ListTable) and data-plane operations (such as GetItem, PutItem, DeleteItem, Query) across your DynamoDB resources for governance and auditing
- Enable compliance, operational, and risk auditing
- Record table-level and item-level activity, initiate actions when important events are detected, and analyze events and logs with Amazon Athena or CloudWatch Logs Insights

**Compliance aid**

**Visibility into activity**

**Detect data exfiltration**

**Automate security analysis**

**Troubleshoot anomalies**

**Analyze permissions**

# Agenda

- Preventative security best practices
- Detective security best practices
- Backups
- Export to S3
- Point-in-time recovery
- Deletion protection

# Backup and restore

## Enterprise ready

### Simplify backup operations

Automate backup scheduling, retention management and life cycle management

Back up PBs of data with no performance impact

Simplify cost allocation across backup operations with tagging*

### Ensure compliance & security

On-demand backups for long-term data archiving and compliance

Centrally enforce backup policies & audit backup activity across AWS services*

Secure backups with separate backup encryption – use a CMK or a service-specific default key*

### Disaster Recovery

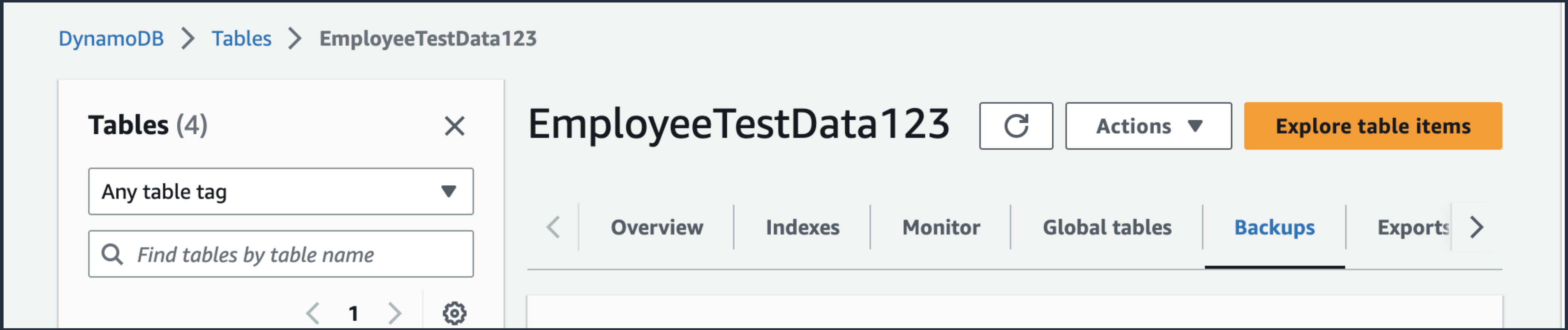
Continuous backups for point-in-time recovery (PITR)

Backup to other AWS accounts and Regions for disaster recovery planning*

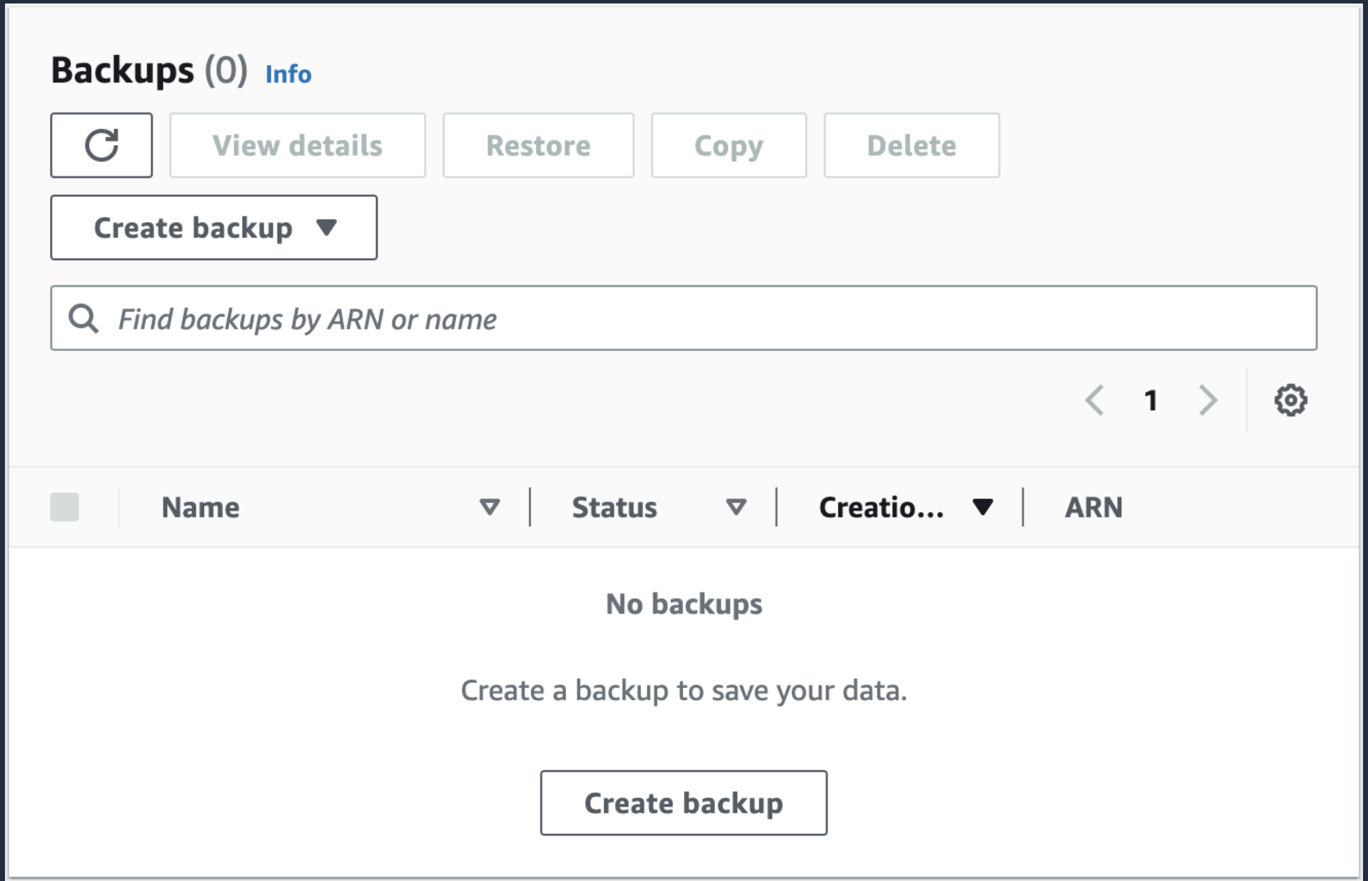
Define cold storage lifecycle preferences to optimize backup costs*

** To use these enhanced backup features, you need to opt-in to have the AWS Backup service manage your DynamoDB on-demand backups.

# Enable DynamoDB backups



# Enable DynamoDB backups

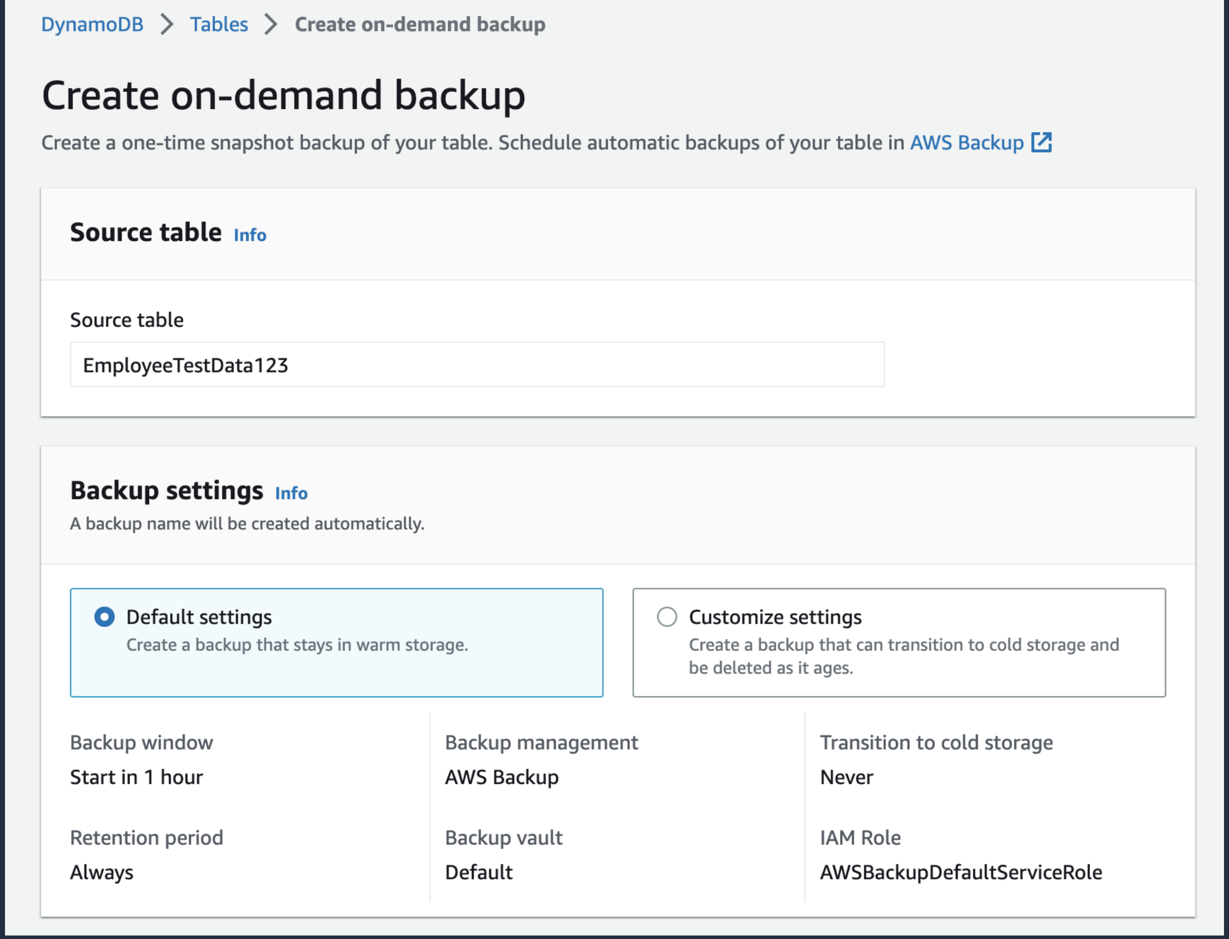


| □ | Name | Status | Creatio... | ARN |
|---|---|---|---|---|

No backups

Create a backup to save your data.

# Create an on-demand backup



## Create on-demand backup

Create a one-time snapshot backup of your table. Schedule automatic backups of your table in AWS Backup

### Source table Info

Source table

EmployeeTestData123

### Backup settings Info

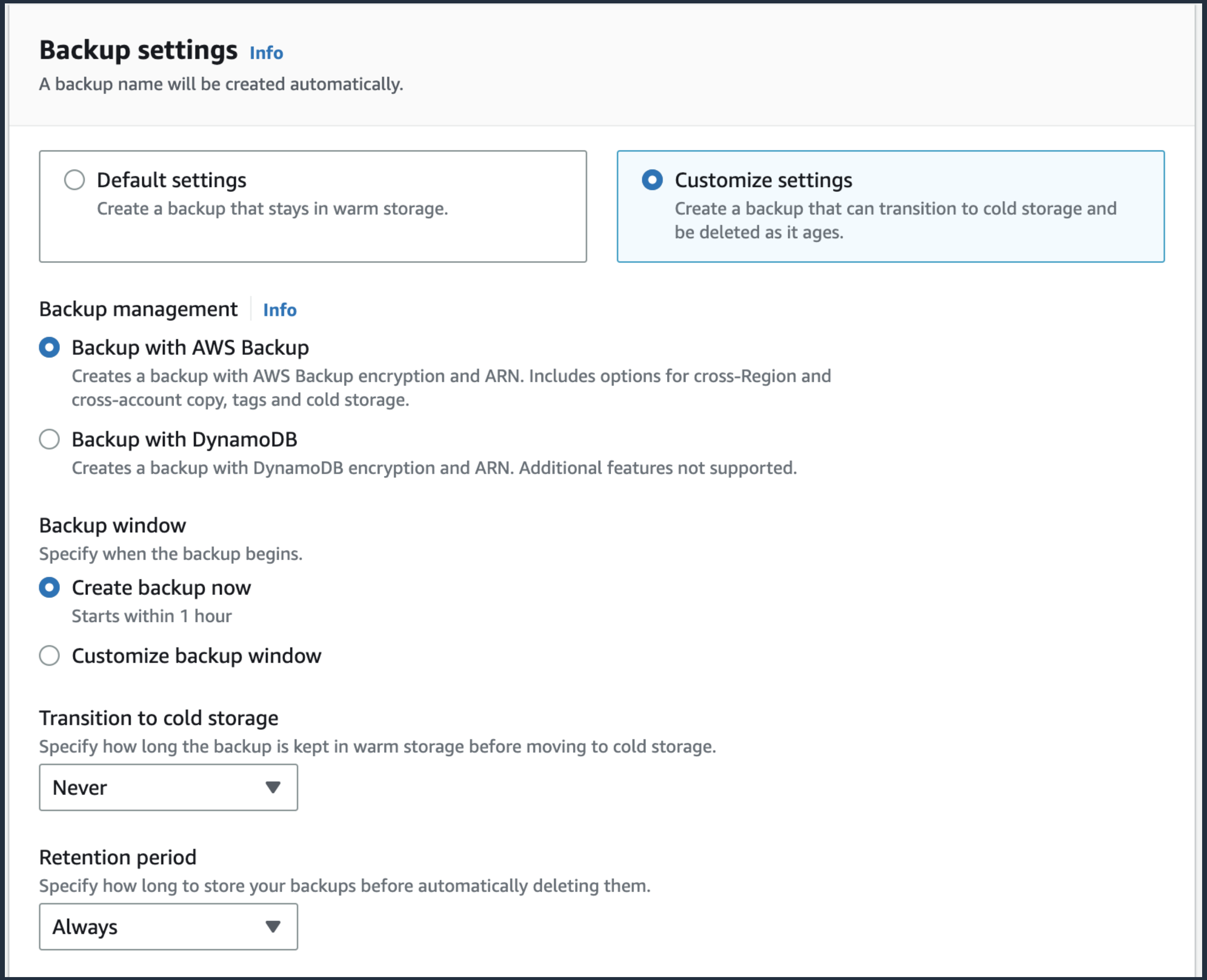
A backup name will be created automatically.

● Default settings
Create a backup that stays in warm storage.

○ Customize settings
Create a backup that can transition to cold storage and be deleted as it ages.

| | | |
|---|---|---|
| Backup window<br>Start in 1 hour | Backup management<br>AWS Backup | Transition to cold storage<br>Never |
| Retention period<br>Always | Backup vault<br>Default | IAM Role<br>AWSBackupDefaultServiceRole |

# Choose between AWS Backup and DynamoDB Backup



## Backup settings Info

A backup name will be created automatically.

○ Default settings
Create a backup that stays in warm storage.

● Customize settings
Create a backup that can transition to cold storage and be deleted as it ages.

Backup management | Info

● Backup with AWS Backup
Creates a backup with AWS Backup encryption and ARN. Includes options for cross-Region and cross-account copy, tags and cold storage.

○ Backup with DynamoDB
Creates a backup with DynamoDB encryption and ARN. Additional features not supported.

Backup window
Specify when the backup begins.

● Create backup now
Starts within 1 hour

○ Customize backup window

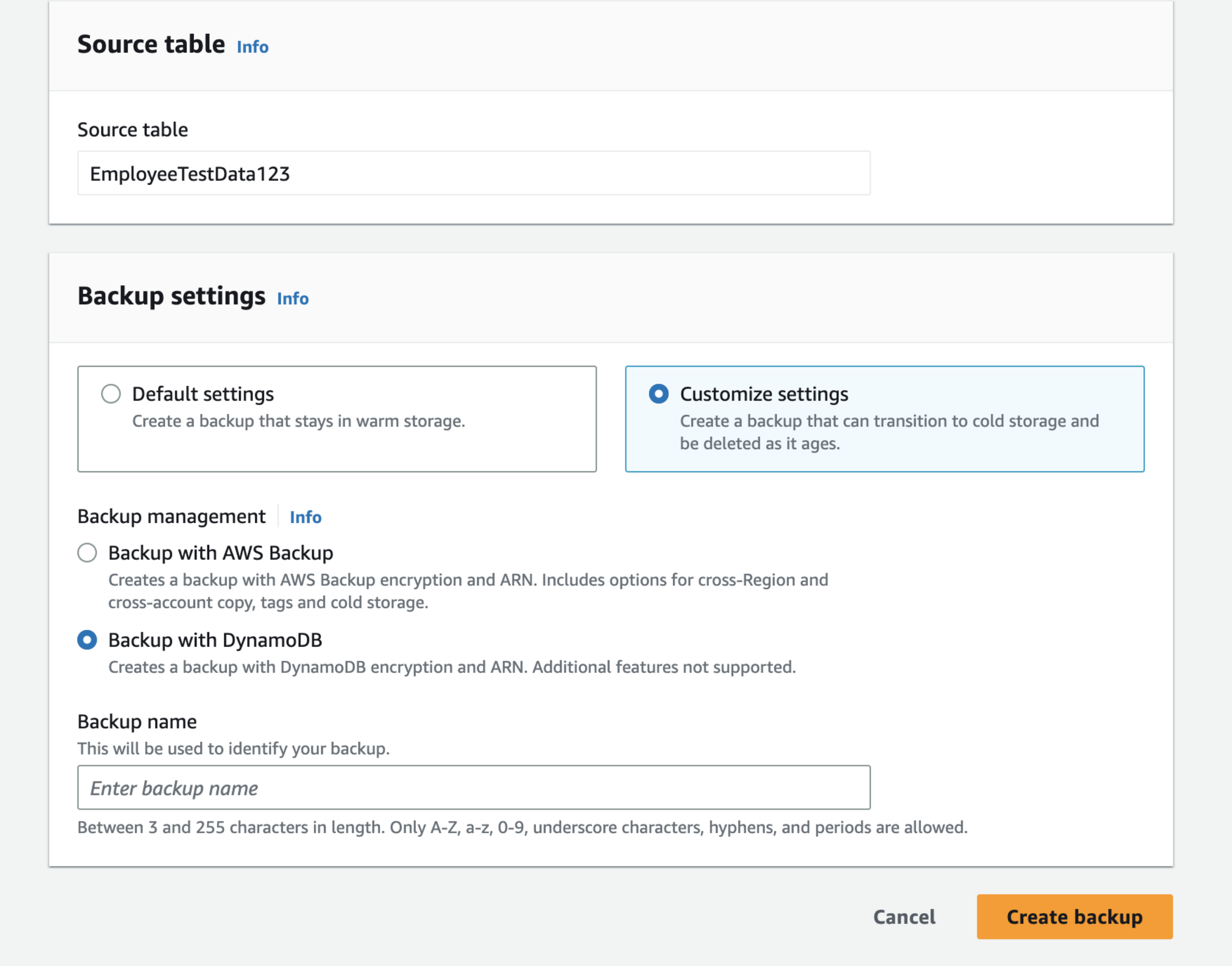
Transition to cold storage
Specify how long the backup is kept in warm storage before moving to cold storage.

Never ▼

Retention period
Specify how long to store your backups before automatically deleting them.

Always ▼

# Choose between AWS Backup and DynamoDB Backup



**Source table** Info

Source table

EmployeeTestData123

**Backup settings** Info

○ Default settings
Create a backup that stays in warm storage.

● Customize settings
Create a backup that can transition to cold storage and be deleted as it ages.

Backup management | Info

○ Backup with AWS Backup
Creates a backup with AWS Backup encryption and ARN. Includes options for cross-Region and cross-account copy, tags and cold storage.

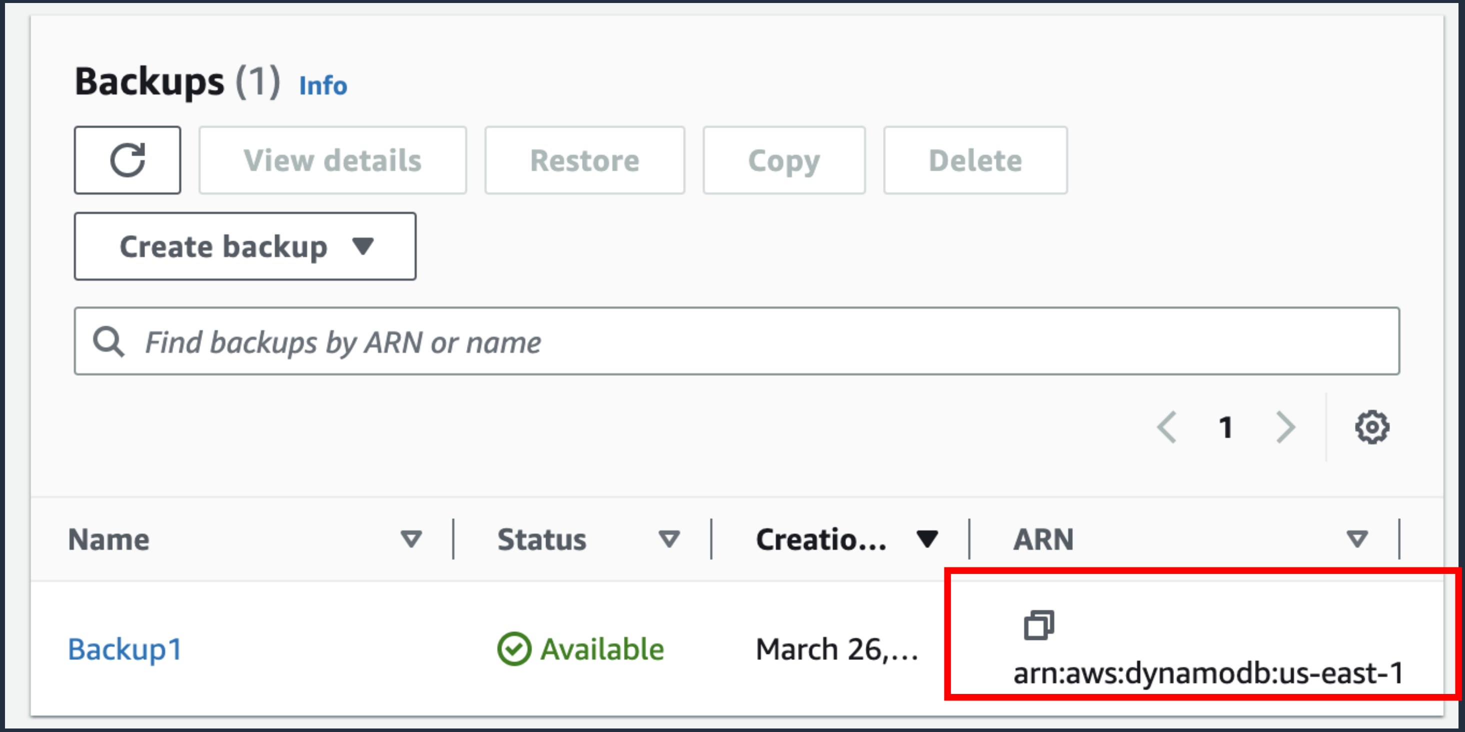
● Backup with DynamoDB
Creates a backup with DynamoDB encryption and ARN. Additional features not supported.

Backup name
This will be used to identify your backup.

*Enter backup name*

Between 3 and 255 characters in length. Only A-Z, a-z, 0-9, underscore characters, hyphens, and periods are allowed.

# Backup is created per table



| Name | Status | Creatio... | ARN |
|---|---|---|---|
| Backup1 | ✓ Available | March 26,... | arn:aws:dynamodb:us-east-1 |

# Agenda

- Preventative security best practices
- Detective security best practices
- Backups
- Export to S3
- Point-in-time recovery
- Deletion protection

# Export DynamoDB data to S3 for regulatory requirements

Enterprise ready

## Extract actionable insights

Export DynamoDB table data to your data lake in Amazon S3, then use other AWS services to analyze data and highlight key takeaways.

## Integrate with backups

To export, select a DynamoDB table that has point-in-time recovery (PITR) enabled, specify any point in the last 35 days, and choose the target Amazon S3 bucket. The output data formats supported are DynamoDB JSON and Amazon Ion.

## Work across Regions

Export data to S3 across AWS Regions and accounts to help comply with regulatory requirements, and to develop a disaster recovery and business continuity plan.

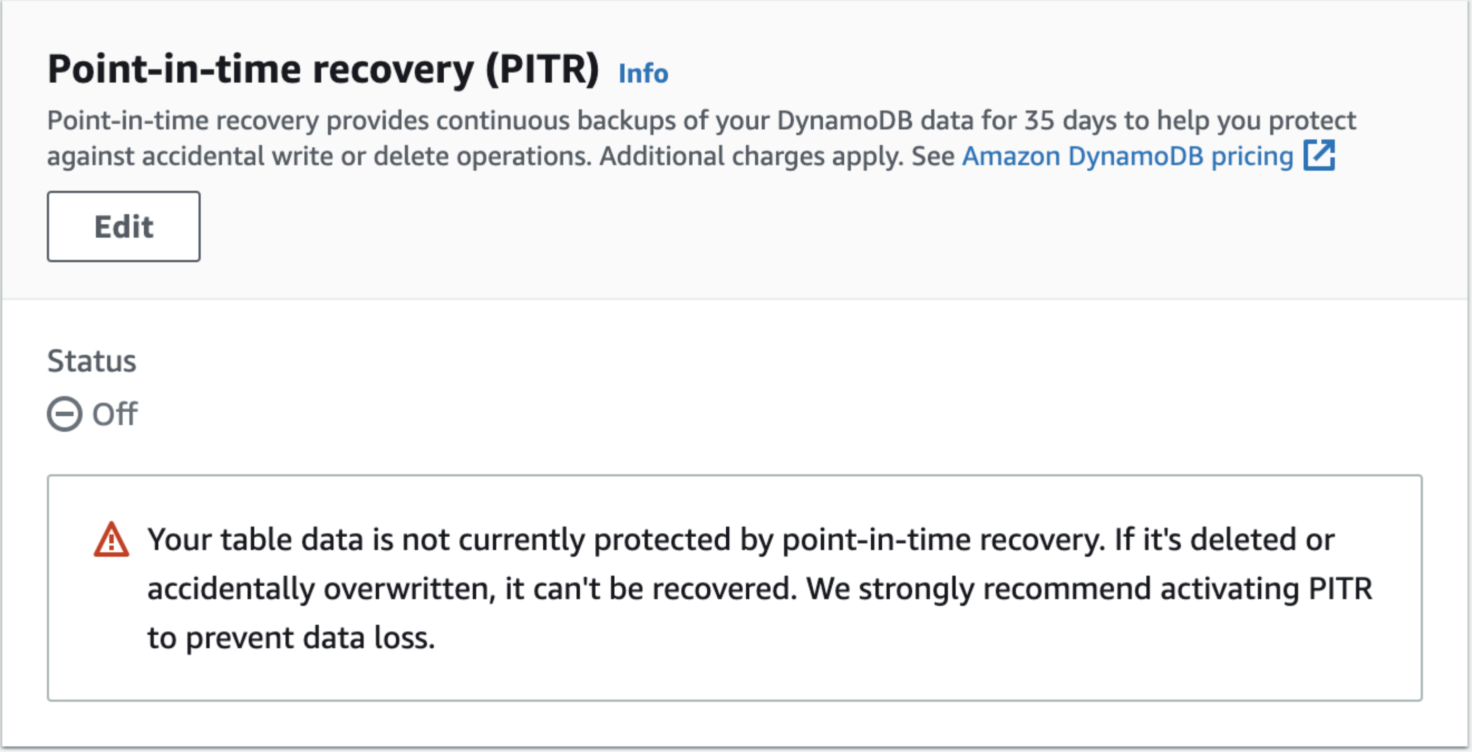
## No impact on performance

Does not consume table capacity, and has zero impact on performance and availability. All DynamoDB data added to your Amazon S3 data lake is easily discoverable, encrypted at rest and in transit, and retained in your S3 bucket until you delete it.

# Agenda

- Preventative security best practices
- Detective security best practices
- Backups
- Export to S3
- Point-in-time recovery
- Deletion protection

# Activate point-in-time recovery



## Point-in-time recovery (PITR) Info

Point-in-time recovery provides continuous backups of your DynamoDB data for 35 days to help you protect against accidental write or delete operations. Additional charges apply. See Amazon DynamoDB pricing

Status

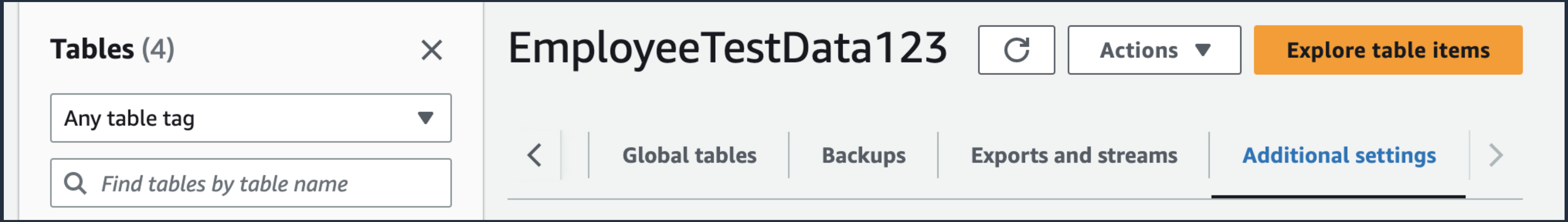
⊖ Off

⚠ Your table data is not currently protected by point-in-time recovery. If it's deleted or accidentally overwritten, it can't be recovered. We strongly recommend activating PITR to prevent data loss.

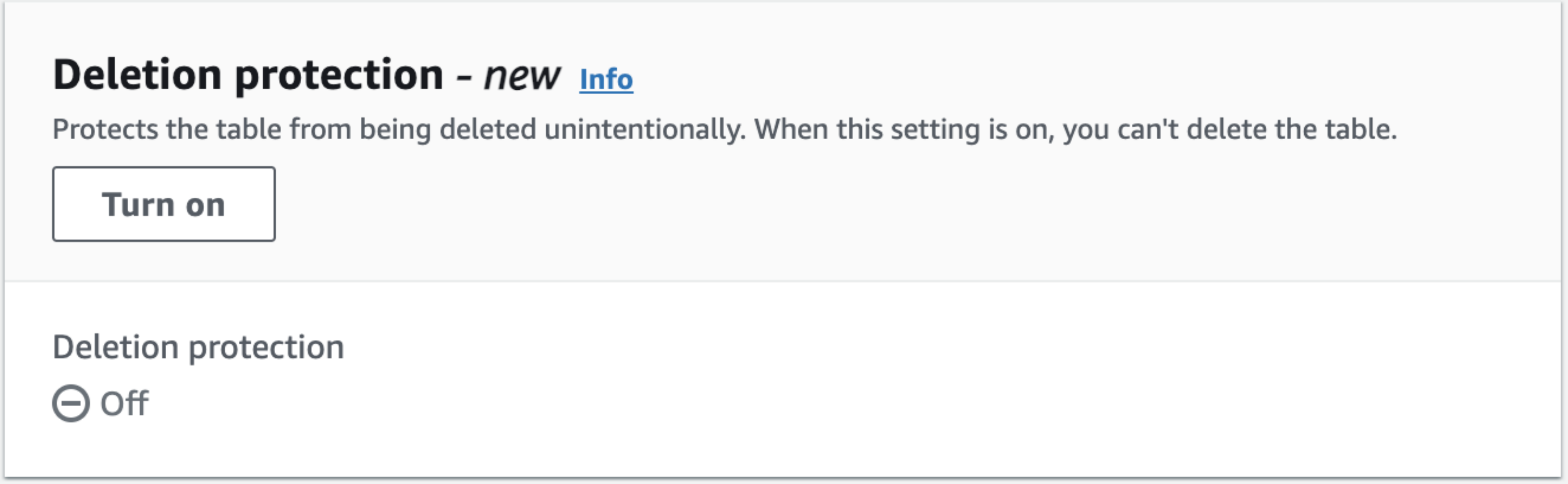
# Agenda

- Preventative security best practices
- Detective security best practices
- Backups
- Export to S3
- Point-in-time recovery
- Deletion protection

# Deletion Protection feature enables you to protect tables from accidental deletion



# Deletion Protection feature enables you to protect tables from accidental deletion



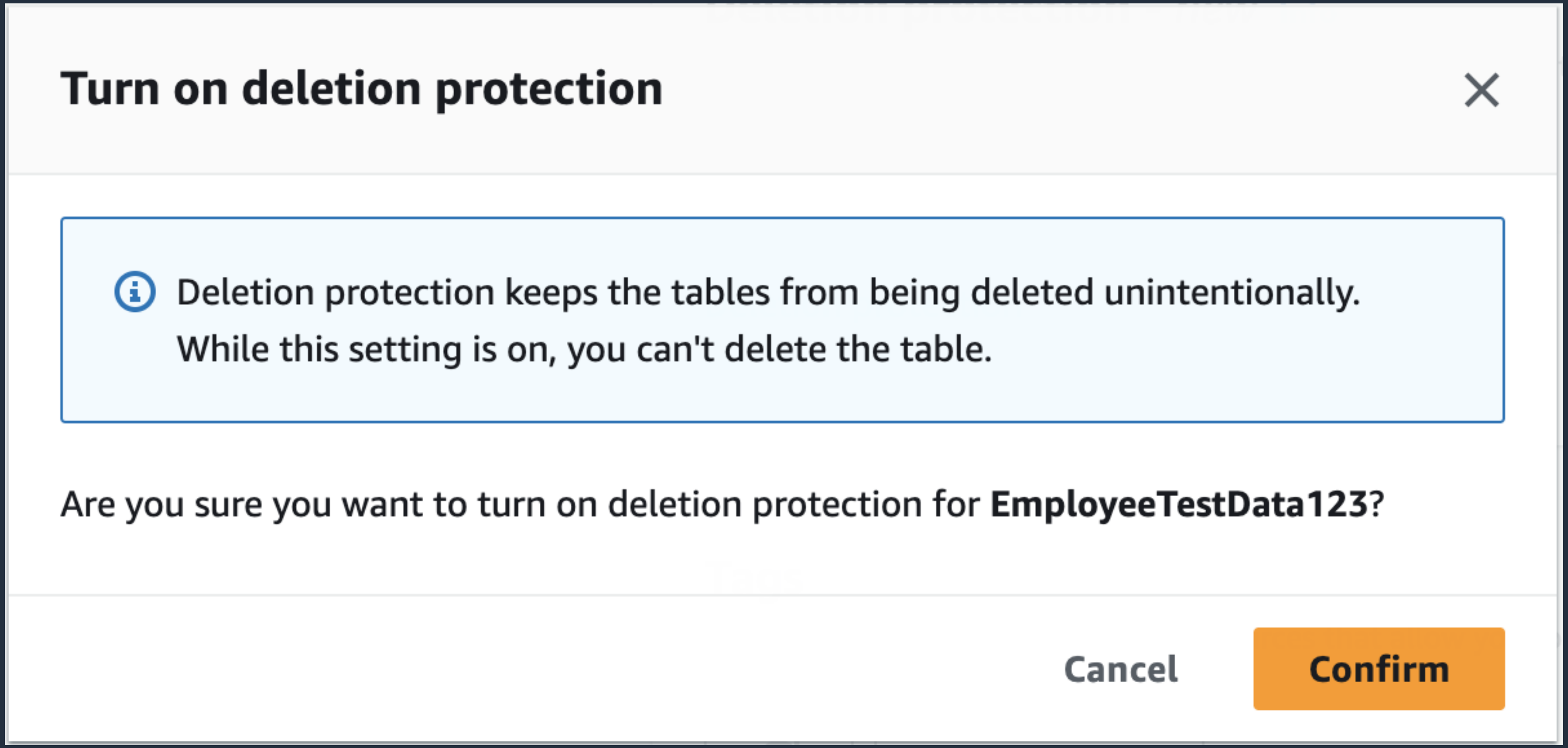
**Deletion protection** - *new* Info

Protects the table from being deleted unintentionally. When this setting is on, you can't delete the table.

Deletion protection

⊖ Off

# Deletion Protection feature enables you to protect tables from accidental deletion

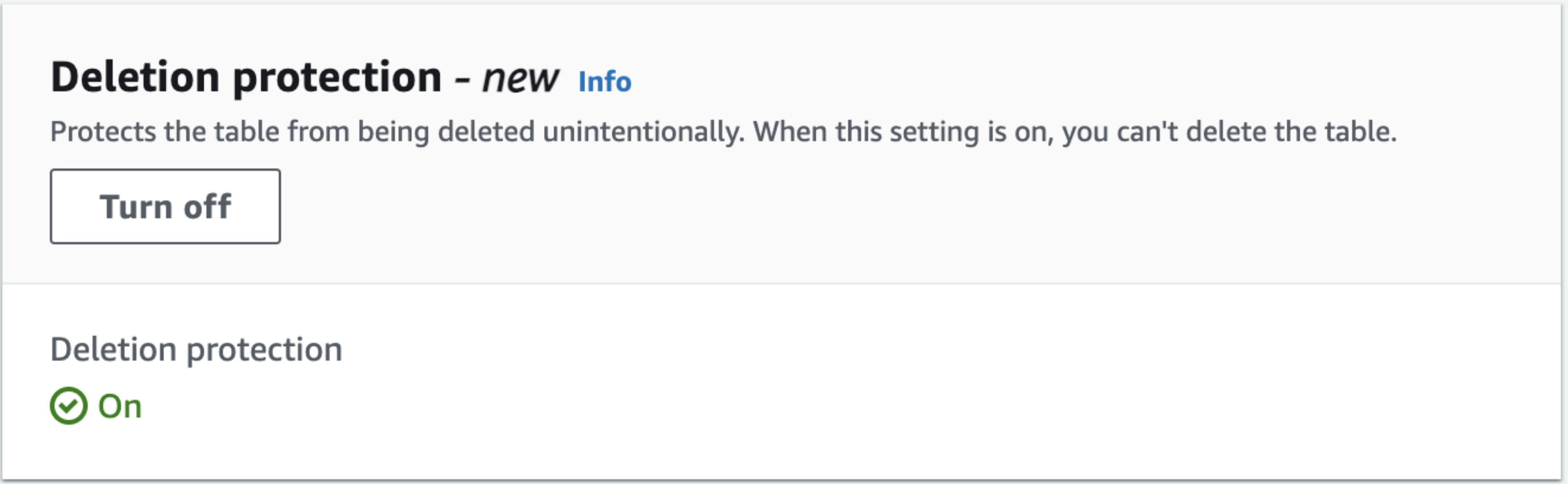


## Turn on deletion protection

Deletion protection keeps the tables from being deleted unintentionally. While this setting is on, you can't delete the table.

Are you sure you want to turn on deletion protection for **EmployeeTestData123**?

# Deletion Protection feature enables you to protect tables from accidental deletion



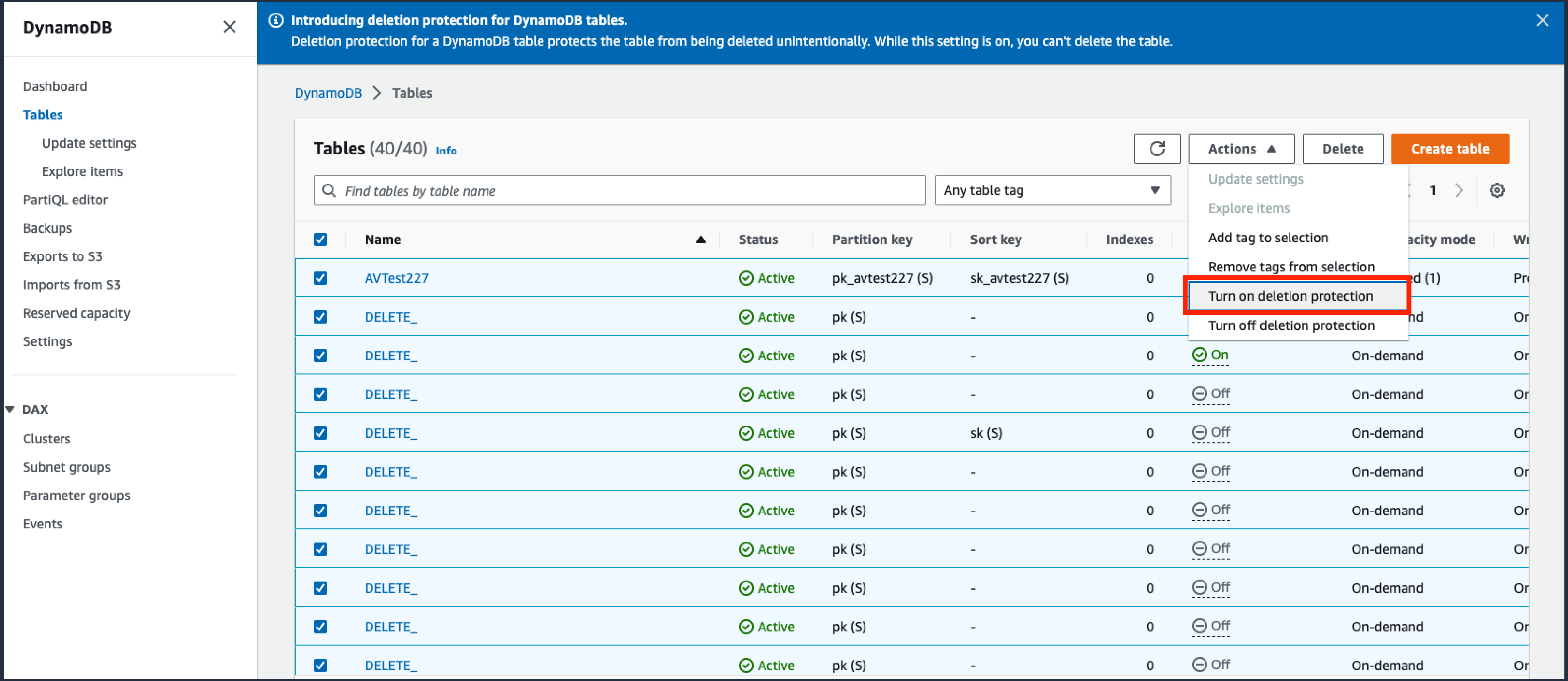
**Deletion protection** - *new* Info

Protects the table from being deleted unintentionally. When this setting is on, you can't delete the table.

Deletion protection

✓ On

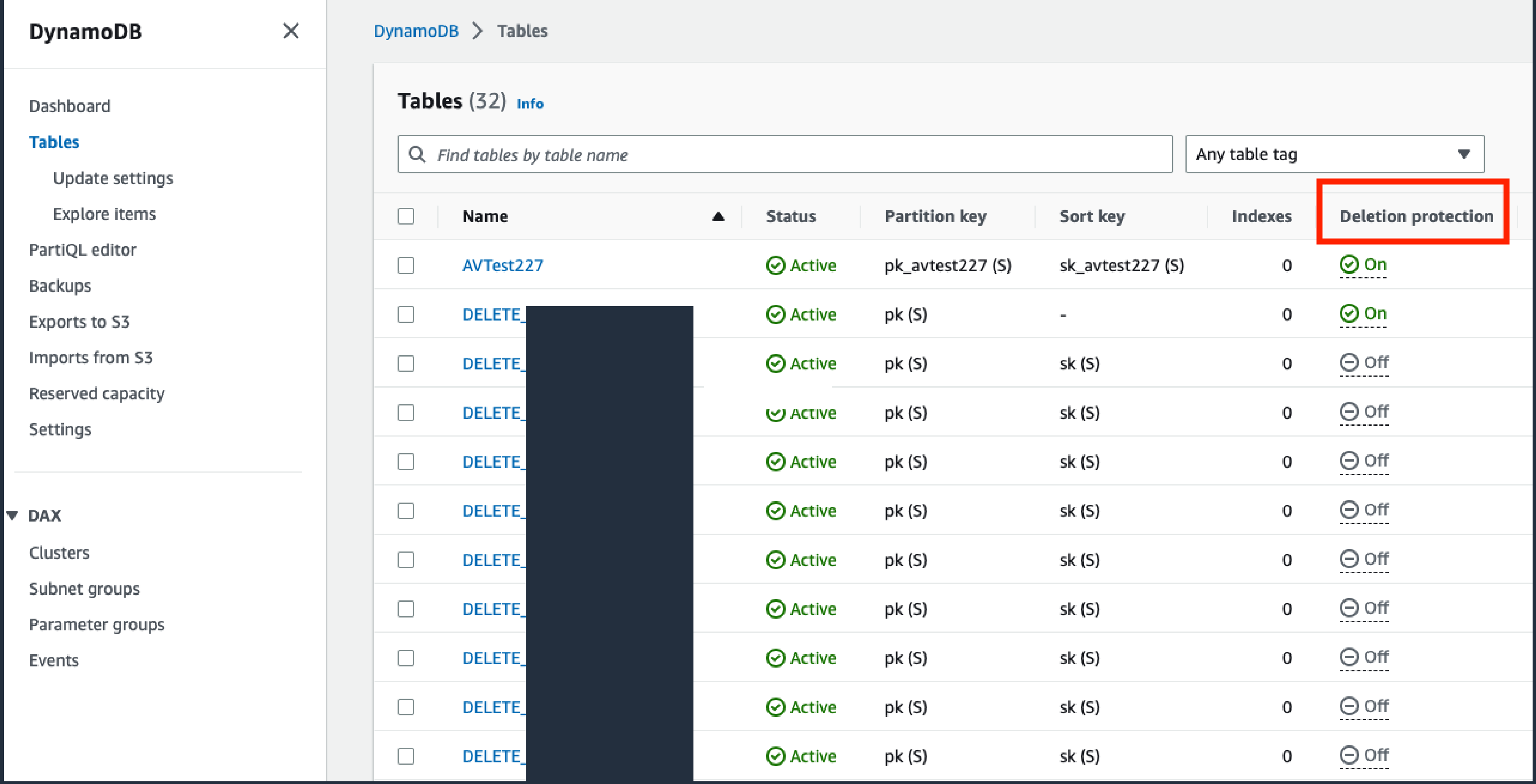
# Bulk deletion protection



**Introducing deletion protection for DynamoDB tables.**
Deletion protection for a DynamoDB table protects the table from being deleted unintentionally. While this setting is on, you can't delete the table.

| ☑ | Name | Status | Partition key | Sort key | Indexes | | acity mode | Wr |
|---|---|---|---|---|---|---|---|---|
| ☑ | AVTest227 | Active | pk_avtest227 (S) | sk_avtest227 (S) | 0 | | ed (1) | Pr |
| ☑ | DELETE_ | Active | pk (S) | - | 0 | | nd | Or |
| ☑ | DELETE_ | Active | pk (S) | - | 0 | On | On-demand | Or |
| ☑ | DELETE_ | Active | pk (S) | - | 0 | Off | On-demand | Or |
| ☑ | DELETE_ | Active | pk (S) | sk (S) | 0 | Off | On-demand | Or |
| ☑ | DELETE_ | Active | pk (S) | - | 0 | Off | On-demand | Or |
| ☑ | DELETE_ | Active | pk (S) | - | 0 | Off | On-demand | Or |
| ☑ | DELETE_ | Active | pk (S) | - | 0 | Off | On-demand | Or |
| ☑ | DELETE_ | Active | pk (S) | - | 0 | Off | On-demand | Or |
| ☑ | DELETE_ | Active | pk (S) | - | 0 | Off | On-demand | Or |
| ☑ | DELETE_ | Active | pk (S) | - | 0 | Off | On-demand | Or |

# Deletion protection status



Tables (32) Info

| □ | Name ▲ | Status | Partition key | Sort key | Indexes | Deletion protection |
|---|---|---|---|---|---|---|
| □ | AVTest227 | ✓ Active | pk_avtest227 (S) | sk_avtest227 (S) | 0 | ✓ On |
| □ | DELETE_[redacted] | ✓ Active | pk (S) | - | 0 | ✓ On |
| □ | DELETE_[redacted] | ✓ Active | pk (S) | sk (S) | 0 | ⊖ Off |
| □ | DELETE_[redacted] | ✓ Active | pk (S) | sk (S) | 0 | ⊖ Off |
| □ | DELETE_[redacted] | ✓ Active | pk (S) | sk (S) | 0 | ⊖ Off |
| □ | DELETE_[redacted] | ✓ Active | pk (S) | sk (S) | 0 | ⊖ Off |
| □ | DELETE_[redacted] | ✓ Active | pk (S) | sk (S) | 0 | ⊖ Off |
| □ | DELETE_[redacted] | ✓ Active | pk (S) | sk (S) | 0 | ⊖ Off |
| □ | DELETE_[redacted] | ✓ Active | pk (S) | sk (S) | 0 | ⊖ Off |
| □ | DELETE_[redacted] | ✓ Active | pk (S) | sk (S) | 0 | ⊖ Off |
| □ | DELETE_[redacted] | ✓ Active | pk (S) | sk (S) | 0 | ⊖ Off |

# Thank you!

Swetha Salunke

@swethasalunke