

## Use case

### Encrypt S3, set lifecycle rules, monitor logs

## Use case Description

Schedule Lambda every evening and stop running Ec2 instances to reduce billing

This use case demonstrates how to secure an S3 bucket using KMS-based encryption, implement a lifecycle rule to transition objects to S3 Glacier Instant Retrieval after 30 days, and enable basic logging for access monitoring.

### 1. Create an S3 bucket with server side encryption as

The screenshot shows the 'Create bucket' page in the AWS S3 console. The 'Encryption' section is expanded, showing options for server-side encryption. The 'Encryption type' is set to 'Server-side encryption with AWS Key Management Service keys (SSE-KMS)'. Under 'AWS KMS key', the option 'Choose from your AWS KMS keys' is selected, and the 'Available AWS KMS keys' dropdown shows 'arn:aws:kms:ap-south-1:770424767712:key/a2261426-c9e3-47ef-b1cc-cba87afdcbe1'. The 'Bucket Key' option is also selected. At the bottom, there is a 'Create bucket' button.

The screenshot shows the 'Properties' page for the bucket 's3-my-secure-bucket'. The 'Bucket overview' section displays the 'AWS Region' as 'Asia Pacific (Mumbai) ap-south-1', the 'Amazon Resource Name (ARN)' as 'arn:aws:s3::s3-my-secure-bucket', and the 'Creation date' as 'July 30, 2025, 13:03:24 (UTC+05:30)'. The 'Bucket Versioning' section shows 'Bucket Versioning' as 'Enabled'. The 'Tags' section shows 'No tags associated with this resource'. The 'Default encryption' section shows 'Encryption type' as 'Server-side encryption with AWS Key Management Service keys (SSE-KMS)' and 'Encryption key ARN' as 'arn:aws:kms:ap-south-1:770424767712:key/a2261426-c9e3-47ef-b1cc-cba87afdcbe1'. The 'Bucket Key' option is also selected.

## 2. Create a lifecycle rule

The screenshot shows the 'Create lifecycle rule' wizard in the AWS Management Console. The breadcrumb trail is 'Amazon S3 > Buckets > s3-my-secure-bucket > Lifecycle configuration > Create lifecycle rule'. The main content area has a title 'Create lifecycle rule' and a subtitle 'Choose the actions you want this rule to perform.' Below this, there are several checkboxes for actions: 'Transition current versions of objects between storage classes' (checked), 'Transition noncurrent versions of objects between storage classes', 'Expire current versions of objects', 'Permanently delete noncurrent versions of objects', and 'Delete expired object delete markers or incomplete multipart uploads'. A warning box states 'Transitions are charged per request' and a blue box states 'By default, objects less than 128KB will not transition across any storage class'. Below these, there is a section 'Transition current versions of objects between storage classes' with a dropdown for 'Choose storage class transitions' set to 'Standard-IA' and a text input for 'Days after object creation' set to '1'. A 'Remove' button is next to the input. Below this is a 'Review transition and expiration actions' section with two columns: 'Current version actions' and 'Noncurrent versions actions'. The 'Current version actions' column shows 'Day 0' with 'Objects uploaded' and 'Day 1' with a downward arrow. The 'Noncurrent versions actions' column shows 'Day 0' with 'No actions defined'.

### s3-my-secure-bucket

The screenshot shows the 'Lifecycle configuration' page in the AWS Management Console for bucket 's3-my-secure-bucket'. The breadcrumb trail is 'Objects | Properties | Permissions | Metrics | Management | Access Points'. The main content area has a title 'Lifecycle configuration' and a subtitle 'To manage your objects so that they are stored cost effectively throughout their lifecycle, configure their lifecycle. A lifecycle configuration is a set of rules that define actions that Amazon S3 applies to a group of objects. Lifecycle rules run once per day.' Below this, there is a section 'Default minimum object size for transitions' with the text 'All storage classes 128K'. Below this is a section 'Lifecycle rules (1)' with a table showing one rule: 'TransitionToGlacierIR'. The table has columns: 'Lifecycle rule name', 'Status', 'Scope', 'Current version actions', 'Noncurrent versions actions', 'Expired object delete mar...', and 'Incomplete multipart upl...'. The 'Status' column shows 'Enabled' with a green checkmark. The 'Scope' column shows 'Entire bucket'. The 'Current version actions' column shows 'Transition to Glacier Instant Reti'. The 'Noncurrent versions actions' column shows '-'. The 'Expired object delete mar...' column shows '-'. The 'Incomplete multipart upl...' column shows '-'. Below the table is a 'View lifecycle configuration' link.

## 3. To create logging, create a new S3 bucket for logging and connect it with the primary bucket

The first screenshot shows the 's3-my-access-logs-bucket' page in the AWS Management Console. The breadcrumb trail is 'Amazon S3 > Buckets > s3-my-access-logs-bucket'. The main content area has a title 's3-my-access-logs-bucket' and a subtitle 'info'. Below this, there are tabs: 'Objects', 'Properties', 'Permissions', 'Metrics', 'Management', and 'Access Points'. The 'Objects' tab is selected, showing a list of objects. The list is empty, with a message 'No objects. You don't have any objects in this bucket.' and an 'Upload' button. The second screenshot shows the 'Server access logging' configuration page in the AWS Management Console for bucket 's3-my-secure-bucket'. The breadcrumb trail is 'Amazon S3 > Buckets > s3-my-secure-bucket'. The main content area has a title 'Server access logging' and a subtitle 'Log requests for access to your bucket. Use CloudWatch to check the health of your server access logging. Learn more'. Below this, there is a section 'Server access logging' with a checkbox 'Enabled' checked. Below this is a section 'Destination bucket' with the text 's3://s3-my-access-logs-bucket'. Below this is a section 'Log object key format' with the text 'YYYY-[MM]-[DD]-[hh]-[mm]-[ss]-[UniqueString]'.