

DynamoDB (Datenbank) aufsetzen:

1. Bei AWS anmelden
2. AWS DynamoDB auswählen
3. Auf „Tabelle erstellen“ klicken

Create resources

Create an Amazon DynamoDB table for fast and predictable database performance at any scale. [Learn more ↗](#)

Create table

4. Tabellennamen einfügen und Datentyp anpassen
5. Partitionschlüssel einfügen und Datentyp anpassen
6. (Optional) Sekundärschlüssel einfügen

Tabellendetails Info
Bei DynamoDB handelt es sich um eine schemaless Datenbank, die beim Erstellen der Tabelle nur einen Tabellennamen und einen Primärschlüssel benötigt.

Tabellenname
Dies wird verwendet, um Ihre Tabelle zu identifizieren.

Zwischen 3 und 255 Zeichen; es sind nur Buchstaben, Zahlen, Unterstriche (.) und Bindestriche (-) und Punkte (.) zulässig.

Partitionsschlüssel
Der Partitionsschlüssel ist Teil des Primärschlüssels der Tabelle. Es handelt sich um einen Hash-Wert, mit dessen Hilfe Elemente aus der Tabelle abgerufen und Daten den Hosts zugewiesen werden, um die Skalierbarkeit und Verfügbarkeit zu gewährleisten.

Sortierschlüssel - optional
Sie können einen Sortierschlüssel als zweiten Teil des Primärschlüssels einer Tabelle verwenden. Mit dem Sortierschlüssel können Sie alle Elemente sortieren oder durchsuchen, die denselben Partitionsschlüssel nutzen.

7. Sonstige Einstellungen beibehalten
8. „Tabelle erstellen“ klicken

[Abbrechen](#)

Tabelle erstellen

9. Beim Dashboard auf „Tabellen“ navigieren

DynamoDB

Dashboard

Tabellen

Elemente erkunden

PartiQL-Editor

Backups

Exporte nach S3

Importe aus S3

Integrationen

Reservierte Kapazität

Einstellungen

10. Auf die gesuchte Tabelle klicken

Tabellen (3) [Info](#)

Filter by tag
Beliebiger Tag-Schlüssel

	Name	Status	Partitionsschlüssel	Sortierschlüssel	Indizes	Replika
<input type="checkbox"/>	Inventory	Aktiv	product_id (S)	-	0	0
<input type="checkbox"/>	Members	Aktiv	cognito_sub (S)	-	0	0
<input type="checkbox"/>	Order	Aktiv	order_id (S)	-	0	0

11. „Tabellenelemente erkunden“ klicken

Letzte Aktualisierung
January 19, 2026, 17:16 (UTC+1:00)

[C](#) [Star](#) [Aktionen ▾](#) **Tabellenelemente erkunden**

12. „Element erstellen“ klicken

Tabelle: Members – Zurückgegebene Artikel (8)

Der Scan wurde gestartet am Januar 19, 2026, 17:19:15

[C](#) [Aktionen ▾](#) **Element erstellen**

	cognito_sub (Zeichenfolge)	city	email	haus_nr	last_check_in	member...	monats_kosten	n_name	plz
<input type="checkbox"/>	[REDACTED]	Musterstadt	maxmuster...	2	2026-01-16T10:...	[REDACTED]	30	Mustermann	12345
<input type="checkbox"/>	[REDACTED]	<empty>	[REDACTED]	<empty>	2026-01-19T10:...	[REDACTED]	0	[REDACTED]	<empty>

13. Werte eintragen und Datentyp anpassen oder JSON-Format eintragen

14. Auf „Element erstellen“ den Datenbank erstellen

Element erstellen

Sie können die Attribute eines Elements hinzufügen, entfernen oder bearbeiten. Sie können Attribute innerhalb anderer Attribute mit einer Tiefe von bis zu 32 Ebenen verschachteln. [Weitere Informationen](#)

[Formular](#) | [JSON-Ansicht](#)

Attribute

[Neues Attribut hinzufügen ▾](#)

Attributname	Wert	Typ	Entfernen
cognito_sub - Partitionsschlüssel	<input type="text" value="Leerer Wert"/>	Zeichenfolge	

[Abbrechen](#) **Element erstellen**

Für Icons muss noch ein S3-Bucket erstellt.

1. AWS S3 Bucket auswählen
2. Auf „Bucket erstellen“ klicken

Allzweck-Buckets (3) Info

Buckets sind Container für in S3 gespeicherte Daten.

Buckets nach Namen suchen

Name	AWS-Region	Erstellungsdatum
amzn-my-export-bucket-gym2-0	Europa (Stockholm) eu-north-1	30.12.2025 07:54:13 PM CET
amzn-s3-bucket-gym2.0-icons	Europa (Stockholm) eu-north-1	07.01.2026 01:55:10 PM CET
cdk-hnb659fds-assets-380652644070-eu-north-1	Europa (Stockholm) eu-north-1	15.01.2026 02:12:32 PM CET

3. Bucket-Namen eintragen

4. Öffentlichen Zugang beschränken anpassen (siehe Bild)

"Öffentlichen Zugriff beschränken" (Bucket-Einstellungen)

Der öffentliche Zugriff auf Buckets und Objekte wird durch Zugriffssteuerungslisten (ACLs, Access Control Lists), Bucket-Richtlinien, Zugriffspunktrichtlinien oder alle diese Elemente gewährt. Um sicherzustellen, dass der öffentliche Zugriff auf alle Ihre S3-Buckets und -Objekte blockiert wird, aktivieren Sie die Blockierung jeglichen öffentlichen Zugriffs. Diese Einstellungen gelten nur für diesen Bucket und die dazugehörigen Zugriffspunkte. AWS empfiehlt, dass Sie die Blockierung jeglichen öffentlichen Zugriffs aktivieren. Vor der Anwendung einer dieser Einstellungen, stellen Sie jedoch sicher, dass Ihre Anwendungen ohne öffentlichen Zugriff ordnungsgemäß funktionieren. Sollten Sie einen bestimmten Grad des öffentlichen Zugriffs auf Ihre enthaltenen Buckets oder Objekte benötigen, so können Sie unten die einzelnen Einstellungen an Ihre spezifischen Speicheranwendungsfälle anpassen. [Weitere Informationen](#)

Blockieren des gesamten öffentlichen Zugriffs

Aus

▼ Einstellungen für „Individuelle Beschränkung des öffentlichen Zugriffs“ für diesen Bucket

- Blockieren des öffentlichen Zugriffs auf Buckets und Objekte, gewährt durch **neue Access Control Lists (ACLs, Zugriffskontrolllisten)**
S3 blockiert öffentliche Zugriffsberechtigungen für neu hinzugefügte Buckets oder Objekte und verhindert die Erstellung neuer ACLs für den öffentlichen Zugriff für vorhandene Buckets und Objekte. Diese Einstellung ändert keine vorhandenen Berechtigungen, die öffentlichen Zugriff auf S3-Ressourcen mit ACLs erlaubt.
- Blockieren des öffentlichen Zugriffs auf Buckets und Objekte, gewährt durch **jegliche Access Control Lists (ACLs, Zugriffskontrolllisten)**
S3 ignoriert alle ACLs, die den öffentlichen Zugriff auf Buckets und Objekte gewähren.
- Blockieren des öffentlichen Zugriffs auf Buckets und Objekte, gewährt durch **neue öffentliche Bucket- oder Access-Point-Richtlinien**
S3 blockiert neue Bucket- und Access-Point-Richtlinien, die öffentlichen Zugriff auf Buckets und Objekte gewähren. Diese Einstellung ändert keine vorhandenen Richtlinien, die öffentlichen Zugriff auf S3-Ressourcen erlauben.
- Blockieren des öffentlichen und kontoubergreifenden Zugriffs auf Buckets und Objekte mittels **jeglicher öffentlicher Bucket- und Access-Point-Richtlinien**
S3 ignoriert den öffentlichen und kontoubergreifenden Zugriff für Buckets oder Access Points mit Richtlinien, die öffentlichen Zugriff auf Buckets und Objekte gewähren.

5. Bucket erstellen lassen.

6. In das gewünschte Bucket navigieren.

7. Bild-Dateien hochladen

8. Dateien hochladen

Objekte (6)

Objekte sind die grundlegenden Entitäten, die in Amazon S3 gespeichert sind. Sie können [Amazon S3 Inventory](#) verwenden, um eine Liste aller Objekte in Ihrem Bucket abzurufen. Damit andere auf Ihre Objekte zugreifen können, müssen Sie ihnen explizit Berechtigungen erteilen. [Weitere Informationen](#)

Objekte nach Präfix suchen

Name	Typ	Letzte Änderung	Größe	Speicherklasse
gummibear.jpg	jpg	11.01.2026 04:04:13 PM CET	6.2 MB	Standard
MonsterEnergy.jpg	jpg	11.01.2026 04:04:19 PM CET	1.5 MB	Standard
Protein-Bar.jpg	jpg	09.01.2026 01:58:08 PM CET	2.2 MB	Standard
Protein-Shake.jpg	jpg	09.01.2026 01:58:05 PM CET	1.4 MB	Standard
VerschiedeneNüsse.jpg	jpg	11.01.2026 04:04:18 PM CET	5.1 MB	Standard
wasserflasche.jpg	jpg	11.01.2026 04:04:04 PM CET	405.4 KB	Standard