
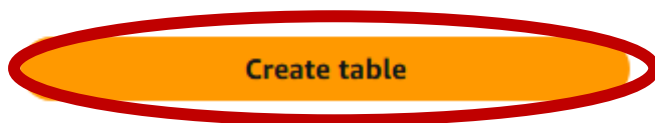


DynamoDB (Datenbank) aufsetzen:

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](#) 



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

Tabellendetails [Info](#)

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

Tabellennamen

Dies wird verwendet, um Ihre Tabelle zu identifizieren.

Zwischen 3 und 255 Zeichen; es sind nur Buchstaben, Zahlen, Unterstriche (_), 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.

Zeichenfolge ▼

1 bis 255 Zeichen, wobei zwischen Groß- und Kleinschreibung unterschieden wird.

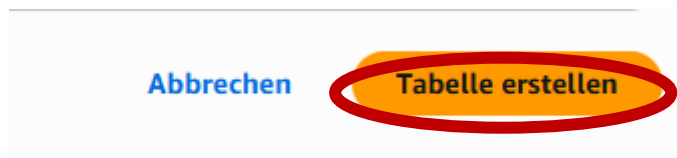
Sortierschlüssel - optional

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.

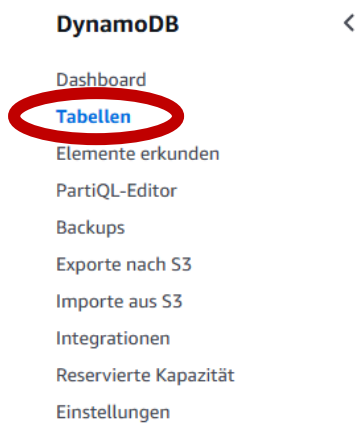
Zeichenfolge ▼

1 bis 255 Zeichen, wobei zwischen Groß- und Kleinschreibung unterschieden wird.

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



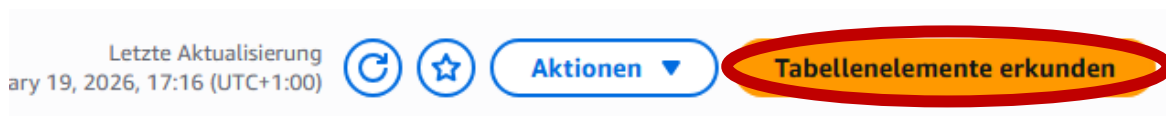
9. Beim Dashboard auf „Tabellen“ navigieren



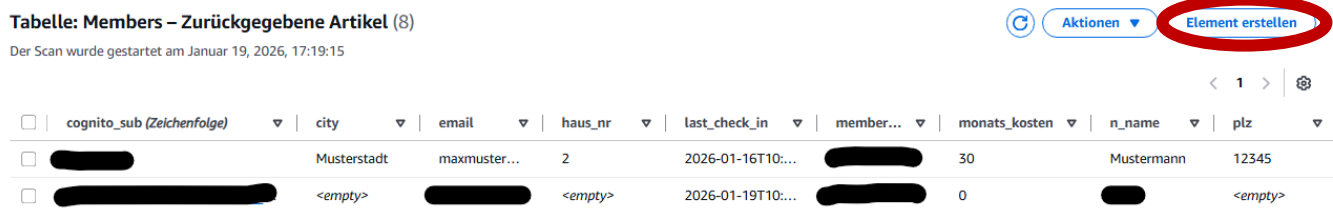
10. Auf die gesuchte Tabelle klicken



11. „Tabellenelemente erkunden“ klicken

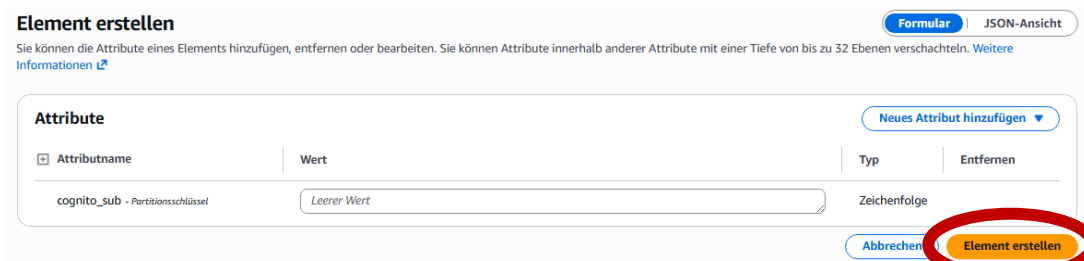


12. „Element erstellen“ klicken



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

14. Auf „Element erstellen“ den Datenbank erstellen



Für Icons muss noch ein S3-Bucket erstellt.

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

The screenshot shows the AWS S3 console's 'Allzweck-Buckets' page. At the top, there are tabs for 'Allzweck-Buckets' and 'Verzeichnis-Buckets'. Below the tabs, there's a header for 'Allzweck-Buckets (3)' with an 'info' link. To the right of the header are buttons for 'ARN kopieren', 'Leer', 'Löschen', and a red-circled 'Bucket erstellen' button. Below the header is a search bar with the placeholder 'Buckets nach Namen suchen'. A table lists the buckets with columns for Name, AWS-Region, and Erstellungsdatum. The buckets listed are 'amzn-my-export-bucket-gym2-0', 'amzn-s3-bucket-gym2.0-icons', and 'cdk-hnb659fds-assets-380652644070-eu-north-1'. The 'amzn-s3-bucket-gym2.0-icons' bucket is highlighted.

3. Bucket-Namen eintragen
4. Öffentlichen Zugang beschränken anpassen (siehe Bild)

"Öffentlichen Zugriff beschränken" (Bucket-Einstellungen)

[Bearbeiten](#)

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 erlauben.

☒ 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 kontübergreifenden Zugriffs auf Buckets und Objekte mittels jeglicher öffentlicher Bucket- und Access-Point-Richtlinien

S3 ignoriert den öffentlichen und kontübergreifenden 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)



[S3-URI kopieren](#)

[URL kopieren](#)

[Herunterladen](#)

[Öffnen](#)

[Löschen](#)

[Aktionen](#)

[Ordner erstellen](#)

[Hochladen](#)

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