limitstore.account_limit

account_id	CHAR(12)* PK:1
limit_id	BIGINT UNSIGNED PK:3 FK
region	VARCHAR(64)* PK:4 FK
int_value	INTEGER
string_value	VARCHAR(1024)

An individual limit for an account.

limitstore.limit_definition

limit_id	BIGINT UNSIGNED PK AUTO
service_name	VARCHAR(64)*
limit_name	VARCHAR(64)*
description	TEXT
value_type	VARCHAR(16)* ENUM
	INTEGER STRING
default_int_value	INTEGER
default_string_value	VARCHAR(1024)
min_value	INTEGER
max_value	INTEGER

Domain table containing the available limits.

limitstore.region

region	VARCHAR(64)* PK

Domain table containing the available regions.

Legend

REMOTE_ROLE_SYS_PRIVS	Fact (Regular) Table
REMOTE_SYSTEM_PRIVILEGES	Domain (Enum) Table
REMOTE_ACCESS_AUDIT_ENTRIES	Audit (Logging) Table
	Comment
++——o<	Identifying, one-to-many
++ – –o<	Non-identifying, one-to-many
+o – –o<	Non-identifying, one to zero or one

Identifying means the foreign key forms part of the primary key in the dependent table.

Non-identifying means the foreign key is a regular column in the dependent table.

iam.account

account_id	CHAR(12)* PK
email	VARCHAR(256)
active	BOOLEAN*
alias	VARCHAR(63) UK

An account in the partition.

iam.iam_user

user_id	CHAR(17)* PK
account_id	CHAR(12)* UK:1 FK
user_name_lower	VARCHAR(64)* UK:2
user_name_cased	VARCHAR(64)*
path	VARCHAR(512)*
permissions_boundary_managed_policy_id	CHAR(17) FK

IAM user. This table is called iam_user and not just user to avoid conflicts with SQL.

iam.iam_group

group_id	CHAR(17)* PK
account_id	CHAR(12)* UK:1 FK
group_name_lower	VARCHAR(128)* UK:2
group_name_cased	VARCHAR(128)*
path	VARCHAR(512)*
created_at	DATETIME*

IAM group.

iam.iam_role

role_id	CHAR(17)* PK
account_id	CHAR(12)* UK:1 FK
role_name_lower	VARCHAR(64)* UK:2
role_name_cased	VARCHAR(64)*
path	VARCHAR(512)*
permissions_boundary_managed_policy_id	CHAR(17) FK
description	VARCHAR(1000)
assume_role_policy_document	TEXT*
created_at	DATETIME*

IAM role.

iam.managed_policy

managed_policy_id	CHAR(17)* PK
account_id	CHAR(12)* UK:1 FK
managed_policy_name_lower	VARCHAR(128)* UK:2
managed_policy_name_cased	VARCHAR(128)*
path	VARCHAR(512)*
created_at	DATETIME*
default_version	BIGINT UNSIGNED FK
deprecated	BOOLEAN*
policy_type	VARCHAR(32)

IAM managed policy (AWS or customer). AWS policies are identified by account_id = '000000000000'.

iam.iam_user_attached_policy

user_id	CHAR(17)* PK:1
managed_policy_id	CHAR(17)* PK:2

Managed policy attached to an IAM user.

iam.iam_group_attached_policy

group_id	CHAR(17)* PK:1
managed_policy_id	CHAR(17)* PK:2

Managed policy attached to an IAM group.

iam.iam_role_attached_policy

role_id	CHAR(17)* PK:1
managed_policy_id	CHAR(17)* PK:2

Managed policy attached to an IAM role.

iam.iam_role_inline_policy

role_id	CHAR(17)* PK:1
policy_name_lower	VARCHAR(128)* PK:2
policy_name_cased	VARCHAR(128)*
policy_document	TEXT*

Inline policy attached to an IAM group.

iam.iam_user_inline_policy

user_id	CHAR(17)* PK:1
policy_name_lower	VARCHAR(128)* PK:2
policy_name_cased	VARCHAR(128)*
policy_document	TEXT*

Inline policy attached to an IAM user.

iam.iam_group_inline_policy

group_id	CHAR(17)* PK:1
policy_name_lower	VARCHAR(128)* PK:2
policy_name_cased	VARCHAR(128)*
policy_document	TEXT*

Inline policy attached to an IAM group.

iam.managed_policy_version

managed_policy_id	CHAR(17)* PK:1
managed_policy_version	BIGINT UNSIGNED PK:2
policy_document	TEXT*
created_at	DATETIME*

Version of an IAM managed policy.

iam.iam_user_login_profile

user_id	CHAR(17)* PK
password_hash_algorithm	VARCHAR(32)*
password_hash	VARCHAR(256)*
password_reset_required	BOOLEAN*
password_last_changed_at	DATETIME*
created_at	DATETIME*
last_used_at	DATETIME

IAM user passwords (hashed) for logging in to the console.

iam.iam_group_member

group_id	CHAR(17)* PK:1
user_id	CHAR(17)* PK:2

User membership in IAM groups.

iam.iam_role_token_key

access_key_id	CHAR(17)* PK
encryption_algorithm	VARCHAR(16)*
encryption_key	VARBINARY(64)*
valid_at	DATETIME*
expires_at	DATETIME*

Symmetric encryption key for decrypting session tokens.

iam.iam_user_service_specific_credential

user_id	CHAR(17)* PK:1
service_specific_credential_id	CHAR(17)* PK:2
service_name	VARCHAR(64)*
service_password	VARCHAR(64)*
active	BOOLEAN*
created_at	DATETIME*

Service-specific passwords (for CodeCommit, Cassandra)

iam.iam_user_password_history

user_id	CHAR(17)* PK:1
password_hash_algorithm	VARCHAR(32)*
password_hash	VARCHAR(256)*
password_changed_at	DATETIME* PK:2

Historical hashed passwords (to check for password reuse).

iam.deleted_managed_policy

managed_policy_id	CHAR(17)* PK
account_id	CHAR(12)*
managed_policy_name_lower	VARCHAR(128)*
managed_policy_name_cased	VARCHAR(128)*
path	VARCHAR(512)*
created_at	DATETIME*
deleted_at	DATETIME*

Historical IAM policy.

iam.iam_user_credential

user_id	CHAR(17)* PK:1
access_key_id	CHAR(17)* PK:2
secret_key	VARCHAR(256)*
active	BOOLEAN*
created_at	DATETIME*

Static access/secret key for API access.

iam.deleted_managed_policy_version

managed_policy_id	CHAR(17)* PK:1
managed_policy_version	BIGINT UNSIGNED PK:2
policy_document	TEXT
created_at	DATETIME*
deleted_at	DATETIME

Historical version of an IAM managed policy.

iam.iam_user_ssh_public_key

user_id	CHAR(17)* PK:1
public_key_id	CHAR(17)* PK:2
fingerprint	CHAR(47)*
ssh_public_key_body	TEXT
active	BOOLEAN*
created_at	DATETIME*

SSH public key (for CodeCommit).

iam.deleted_iam_user

user_id	CHAR(17)* PK
account_id	CHAR(12)*
user_name_lower	VARCHAR(64)*
user_name_cased	VARCHAR(64)*
path	VARCHAR(512)*
boundary_managed_policy_id	CHAR(17)
created_at	DATETIME*
deleted_at	DATETIME*

Historical IAM user.

iam.deleted_group

group_id	CHAR(17)* PK
account_id	CHAR(12)*
group_name_lower	VARCHAR(128)*
group_name_cased	VARCHAR(128)*
path	VARCHAR(512)*
created_at	DATETIME*
deleted_at	DATETIME*

Historical IAM group.

iam.deleted_role

role_id	CHAR(17)* PK
account_id	CHAR(12)*
role_name_lower	VARCHAR(64)*
role_name_cased	VARCHAR(64)*
path	VARCHAR(512)*
permissions_boundary_managed_policy_id	
description	VARCHAR(1000)
assume_role_policy_document	TEXT*
created_at	DATETIME*
deleted_at	DATETIME*

Historical IAM role.