Cloud Identity and Access Management (/iam/docs/overview) (IAM) allows you to control user and group access to Cloud Spanner resources at the project, Cloud Spanner instance, and Cloud Spanner database levels. For example, you can specify that a user has full control of a specific database in a specific instance in your project, but cannot create, modify, or delete any instances in your project. Using Cloud Spanner IAM allows you to grant a permission to a user or group without having to modify each Cloud Spanner instance or database permission individually.

This document focuses on the IAM *permissions* relevant to Cloud Spanner and the IAM *roles* that grant those permissions. For a detailed description of IAM and its features, see the Cloud Identity and Access Management (/iam/docs/overview) developer's guide. In particular, see its Managing IAM policies (/iam/docs/granting-changing-revoking-access) section.

Permissions allow users to perform specific actions on Cloud Spanner resources. For example, the `spanner.databases.read` permission allows a user to read from a database using Cloud Spanner's read API, while `spanner.databases.select` allows a user to execute a SQL select statement on a database. You don't directly give users permissions; instead, you grant them predefined roles (#roles) or custom roles (#custom-roles), which have one or more permissions bundled within them.

The following tables list the IAM permissions that are associated with Cloud Spanner.

The following permissions apply to Cloud Spanner instance configurations (see the instance configuration reference: REST (/spanner/reference/rest/v1/projects.instanceConfigs), RPC (/spanner/reference/rpc/google.spanner.admin.instance.v1#google.spanner.admin.instance.v1.InstanceConfig)).

Instance configuration permission name	Description
`spanner.instanceConfigs.list`	List the set of instance configurations.

Instance configuration permission name	Description
`spanner.instanceConfigs.get`	Get an instance configuration.

The following permissions apply to Cloud Spanner instances (see the instance reference: REST (/spanner/reference/rest/v1/projects.instances), RPC (/spanner/reference/rpc/google.spanner.admin.instance.v1#google.spanner.admin.instance.v1.Instance)).

Instance permission name	Description
`spanner.instances.create`	Create an instance.
`spanner.instances.list`	List instances.
`spanner.instances.get`	Get the configuration of a specific instance.
`spanner.instances.getIamPolicy`	Get an instance's IAM Policy.
`spanner.instances.update`	Update an instance.
`spanner.instances.setIamPolicy`	Set an instance's IAM Policy.
`spanner.instances.delete`	Delete an instance.

The following permissions apply to Cloud Spanner instance operations (see the instance reference: REST (/spanner/reference/rest/v1/projects.instances.operations), RPC (/spanner/reference/rpc/google.spanner.admin.instance.v1#google.spanner.admin.instance.v1.InstanceOperations)).

Instance operation permission name	Description
`spanner.instanceOperations.list`	List instance operations.
`spanner.instanceOperations.get`	Get a specific instance operation.
`spanner.instanceOperations.cancel`	Cancel an instance operation.
`spanner.instanceOperations.delete`	Delete an instance operation.

The following permissions apply to Cloud Spanner databases (see the database reference: REST (/spanner/reference/rest/v1/projects.instances.databases), RPC (/spanner/reference/rpc/google.spanner.admin.database.v1#google.spanner.admin.database.v1.Database)).

Database permission name	Description
`spanner.databases.beginPartitionedDmlTransaction`	Execute a Partitioned Data Manipulation Language (DML) statement.  Currently unavailable for IAM custom roles.
`spanner.databases.create`	Create a database.
`spanner.databases.list`	List databases.
`spanner.databases.update`	Update a database's metadata.  Currently unavailable for IAM custom roles.
`spanner.databases.updateDdl`	Update a database's schema.
`spanner.databases.get`	Get a database's metadata.
`spanner.databases.getDdl`	Get a database's schema.
`spanner.databases.getIamPolicy`	Get a database's IAM Policy.
`spanner.databases.setIamPolicy`	Set a database's IAM Policy.
`spanner.databases.beginReadOnlyTransaction`	Begin a read-only transaction (/spanner/docs/transactions#read-only_transactions) on a Cloud Spanner database.
`spanner.databases.beginOrRollbackReadWriteTransaction`	Begin or roll back a read-write transaction (/spanner/docs/transactions#read-write_transactions) on a Cloud Spanner database.
`spanner.databases.read`	Read from a database using the read API.
`spanner.databases.select`	Execute a SQL select statement on a database.
`spanner.databases.write`	Write into a database.
`spanner.databases.drop`	Drop a database.

The following permissions apply to Cloud Spanner database operations (see the database reference: REST (/spanner/reference/rest/v1/projects.instances.databases.operations), RPC (/spanner/reference/rpc/google.spanner.admin.database.v1#google.spanner.admin.database.v1.DatabaseOperations)).

Database operation permission name	Description
`spanner.databaseOperations.list`	List database operations.
`spanner.databaseOperations.get`	Get a specific database operation.
`spanner.databaseOperations.cancel`	Cancel a database operation.
`spanner.databaseOperations.delete`	Delete a database operation. ⚠ Currently unavailable for IAM custom roles.

The following permissions apply to Cloud Spanner sessions (see the database reference: REST (/spanner/reference/rest/v1/projects.instances.databases.sessions), RPC (/spanner/reference/rpc/google.spanner.v1#google.spanner.v1.Session)).

Sessions are an advanced concept that only apply to users of the REST API and those who are creating their own clie
s. Learn more in Sessions (/spanner/docs/sessions).

Session permission name	Description
`spanner.sessions.create`	Create a session.
`spanner.sessions.get`	Get a session.
`spanner.sessions.delete`	Delete a session.
`spanner.sessions.list`	List sessions.

A predefined role is a bundle of one or more permissions (#permissions). For example, the predefined role `roles/spanner.databaseUser` contains the permissions `spanner.databases.read` and `spanner.database.write`. There are two types of predefined roles for Cloud Spanner:

- Person roles: Granted to users or groups, which allows them to perform actions on the resources in your project.
- Machine roles: Granted to service accounts, which allows machines running as those service accounts to perform actions on the resources in your project.

To avoid providing machines with unnecessarily broad permissions, do not grant person roles to service accounts.

The following table lists the Cloud Spanner IAM predefined roles, including a list of the permissions associated with each role:

Role	Permissions	Description

`roles/spanner.admin`
 	
(**Person** role)
	`resourcemanager.projects.get`
	`spanner.databases.*`
	`spanner.databaseOperations.*`
	`spanner.instances.*`
	`spanner.instanceConfigs.*`
	`spanner.instanceOperations.*`
	`spanner.sessions.*`
		Recommended to grant at the Google Cloud *project* level. Has complete access to all Cloud Spanner resources in a Google Cloud project. A principal with this role can:
		• Grant and revoke permissions to other principals for all Cloud Spanner resources in the project.
		• Allocate and delete chargeable Cloud Spanner resources.
		• Issue get/list/modify operations on Cloud Spanner resources.
		• Read from and write to all Cloud Spanner databases in the project.
		• Fetch project metadata.

Role	Permissions	Description

`roles/spanner.databaseAdmin`
 	
(**Person** role)
	`resourcemanager.projects.get`
	`spanner.databases.*`
	`spanner.databaseOperations.*`
	`spanner.instances.list`
	`spanner.instances.get`
	`spanner.instances.getIamPolicy`
	`spanner.sessions.*`
		Recommended to grant at the Google Cloud *project* level. A principal with this role can:
		
		• Get/list all Cloud Spanner instances in project.
		• Create/list/drop databases in the instance on which it is granted.
		• Grant/revoke access to databases in the project.
		• Read from and write to all Cloud Spanner databases in the project.

`roles/spanner.databaseReader`
 	
(**Machine** role)
	`spanner.databases.beginReadOnlyTransaction`
	`spanner.databases.getDdl`
	`spanner.databases.read`
	`spanner.databases.select`
	`spanner.sessions.create`
	`spanner.sessions.delete`
	`spanner.sessions.get`
		Recommended to grant at the *database* level. A principal with this role can:
		• Read from the Cloud Spanner database.
		• Execute SQL queries on the database.
		• View schema for the database.

`roles/spanner.databaseUser`
 	
(**Machine** role)
	`spanner.databases.beginOrRollbackReadWriteTransaction`
	`spanner.databases.beginPartitionedDmlTransaction`
	`spanner.databases.beginReadOnlyTransaction`
	`spanner.databases.getDdl`
	`spanner.databases.read`
	`spanner.databases.select`
	`spanner.databases.updateDdl`
	`spanner.databases.write`
	`spanner.sessions.create`
	`spanner.sessions.delete`
	`spanner.sessions.get`
		Recommended to grant at the *database* level. A principal with this role can:
		• Read from and write to the Cloud Spanner database.
		• Execute SQL queries on the database, including DML and Partitioned DML.
		• View and update schema for the database.

Role	Permissions	Description

`roles/spanner.viewer`
 	
(**Person** role)
	`resourcemanager.projects.get`
	`spanner.databases.list`
	`spanner.instances.get`
	`spanner.instances.list`
		Recommended to grant at the Google Cloud *project* level. A principal with this role can:
		• View all Cloud Spanner instances (but cannot modify instances).
		• View all Cloud Spanner databases (but cannot modify databases and cannot read from databases).
		For example, you can combine this role with the **`roles/spanner.databaseUser`** role to grant a user with access to a specific database, but only view access to other instances and databases.
		This role is required at the Google Cloud project level for users interacting with Cloud Spanner resources in the Google Cloud Console.

When the assigned role is **`spanner.databaseReader`**, requests for a read-only transaction might occasionally fail w
ssions error. To resolve this problem, see Manage the write-sessions fraction
nner/docs/sessions#write-sessions-fraction).

Primitive roles are project-level roles that predate Cloud IAM. See Primitive roles (/iam/docs/understanding-roles#primitive_roles) for additional details.

Although Cloud Spanner supports the following primitive roles, you should use one of the predefined roles shown above whenever possible. Primitive roles include broad permissions that apply to all of your Google Cloud resources; in contrast, Cloud Spanner's predefined roles include fine-grained permissions that apply only to Cloud Spanner.

Primitive Role	Description

Primitive Role	Description
`roles/viewer`	Can list and get the metadata of schemas and instances. Can also read and query using SQL on a database.
`roles/writer`	Can do all that a `roles/viewer` can do. Can also create instances and databases and write data into a database.
`roles/owner`	Can do all that a `roles/writer` can do. Can also modify access to databases and instances.

If the predefined roles (#roles) for Cloud Spanner do not address your business requirements, you can define your own custom roles with permissions that you specify.

Before you create a custom role, you must identify the tasks that you need to perform. You can then identify the permissions that are required for each task and add these permissions to the custom role.

For most tasks, it's obvious which permissions you need to add to your custom role. For example, if you want your service account to be able to create a database, add the permission `spanner.databases.create` to your custom role.

However, when you're reading or writing data in a Cloud Spanner table, you need to add several different permissions to your custom role. The following table shows which permissions are required for reading and writing data.

Service account task	Required permissions
Read data	• `spanner.databases.select` • `spanner.sessions.create` • `spanner.sessions.delete`

Service account task	Required permissions
Insert, update, or delete data	• `spanner.databases.beginOrRollbackReadWriteTransaction` • `spanner.databases.write` • `spanner.sessions.create` • `spanner.sessions.delete`

To identify the list of permissions you need for a given task in the Cloud Console, you determine the workflow for that task and compile the permissions for that workflow. For example, to view the data in a table, you would follow these steps in the Cloud Console:

Step	Permissions
1. Access the project	`resourcemanager.projects.get`
2. View the list of instances	`spanner.instances.list`
3. Select an instance	`spanner.instances.get`
4. View the list of databases	`spanner.databases.list`
5. Select a database and a table	`spanner.databases.get`, `spanner.databases.getDdl`
6. View data in a table	`spanner.databases.select`, `spanner.sessions.create`, `spanner.sessions.delete`

In this example, you need these permissions:

- `resourcemanager.projects.get`
- `spanner.databases.get`
- `spanner.databases.getDdl`
- `spanner.databases.list`
- `spanner.databases.select`
- `spanner.instances.get`
- `spanner.instances.list`

- `spanner.sessions.create`
- `spanner.sessions.delete`

The following table lists the permissions required for actions in the Cloud Console.

Action	Permissions
View the list of instances on the Instances page	• `resourcemanager.projects.get` • `spanner.instances.list`
View the list on the Permissions tab of the Instance page	`spanner.instances.getIamPolicy`
Add members on the Permissions tab of the Instance page	`spanner.instances.setIamPolicy`
Select an instance from the instance list to view the Instance Details page	`spanner.instances.get`
Create an instance	• `spanner.instanceConfigs.list` • `spanner.instanceOperations.get` • `spanner.instances.create`
Delete an instance	`spanner.instances.delete`
Modify an instance	• `spanner.instanceOperations.get` • `spanner.instances.update`
View the graphs in the Monitor tab on the Instance details page or the Database details page	• `monitoring.metricDescriptors.get` • `monitoring.metricDescriptors.list` • `monitoring.timeSeries.list` • `spanner.instances.get`
View the list of databases on the Instance details page	• `spanner.databases.list`
View the list on the Permissions tab of the Database details page	`spanner.databases.getIamPolicy`
Add members on the Permissions tab of the Database details page	`spanner.databases.setIamPolicy`

Action	Permissions
Select a database from the database list and view the schema on the Database details page	• `spanner.databases.get` • `spanner.databases.getDdl`
Create a database	`spanner.databases.create`
Delete a database	`spanner.databases.drop`
Create a table Update a table schema	• `spanner.databaseOperations.get` • `spanner.databaseOperations.list` • `spanner.databases.updateDdl`
View data in the Data tab of the Database details page Create and run a query	• `spanner.databases.select` • `spanner.sessions.create` • `spanner.sessions.delete`
Modify data in a table	• `spanner.databases.beginOrRollbackReadWriteTransaction` • `spanner.databases.select` • `spanner.databases.write` • `spanner.sessions.create` • `spanner.sessions.delete`

You can get, set, and test IAM policies using the REST or RPC APIs on Cloud Spanner instance and database resources.

REST API
`projects.instances.getIamPolicy` (/spanner/reference/rest/v1/projects.instances/getIamPolicy)
`projects.instances.setIamPolicy` (/spanner/reference/rest/v1/projects.instances/setIamPolicy)
`projects.instances.testIamPermissions` (/spanner/reference/rest/v1/projects.instances/testIamPermissio

REST API
`projects.instances.databases.getIamPolicy` (/spanner/reference/rest/v1/projects.instances.databases/g
`projects.instances.databases.setIamPolicy` (/spanner/reference/rest/v1/projects.instances.databases/s
`projects.instances.databases.testIamPermissions` (/spanner/reference/rest/v1/projects.instances.datab

- Learn more about Identity and Access Management (/iam/docs/overview).
- Learn how to apply IAM roles for a Cloud Spanner database, instance, or Google Cloud project (/spanner/docs/grant-permissions).