**Confluent Cloud**, **Role-Based Access Control (RBAC)**

In **Confluent Cloud**, **Role-Based Access Control (RBAC)** provides predefined roles that grant specific sets of permissions for managing and interacting with resources such as Kafka clusters, topics, connectors, and other Confluent Cloud services. RBAC simplifies access management by assigning users or service accounts predefined roles with the required permissions.

Here are the **15 predefined roles** in Confluent Cloud RBAC:

**1. OrganizationAdmin**

* **Permissions**: Organization-wide access.
* **Use Case**: This role has the highest level of control across the organization, managing settings and resources at the organization level.
* **Responsibilities**: Manages user access, billing, environments, and roles within the organization.

**2. EnvironmentAdmin**

* **Permissions**: Full control over an environment.
* **Use Case**: Manages resources and configurations at the environment level.
* **Responsibilities**: Creates and deletes resources, including Kafka clusters, topics, and connectors, within the environment.

**3. CloudClusterAdmin**

* **Permissions**: Full control over a Kafka cluster.
* **Use Case**: Kafka administrators who need full access to manage Kafka clusters.
* **Responsibilities**: Manages Kafka brokers, topics, ACLs, and other cluster-level configurations.

**4. DeveloperRead**

* **Permissions**: Read-only access to development-related resources.
* **Use Case**: Developers who only need to read Kafka topics, consumer groups, and related resources.
* **Responsibilities**: Views Kafka topics, schemas, and consumer groups without making changes.

**5. DeveloperWrite**

* **Permissions**: Read and write access to development-related resources.
* **Use Case**: Developers who need to create and produce/consume data from Kafka topics.
* **Responsibilities**: Produces to and consumes from Kafka topics, creates topics, and manages schemas.

**6. Operator**

* **Permissions**: Limited operational control of Kafka clusters.
* **Use Case**: Operators responsible for maintaining Kafka clusters and ensuring availability.
* **Responsibilities**: Monitors cluster health, manages Kafka ACLs, and performs operational tasks without full admin privileges.

**7. ResourceOwner**

* **Permissions**: Full control over a specific resource.
* **Use Case**: Ownership of a resource like a topic, connector, or schema.
* **Responsibilities**: Manages permissions and settings for the resource they own.

**8. SecurityAdmin**

* **Permissions**: Manages security-related configurations.
* **Use Case**: Users who need to manage RBAC roles, ACLs, and security policies.
* **Responsibilities**: Creates and manages ACLs, role bindings, and security policies.

**9. SchemaRegistryAdmin**

* **Permissions**: Full control of Schema Registry.
* **Use Case**: Admins managing Schema Registry instances.
* **Responsibilities**: Creates, updates, and deletes schemas, and manages compatibility settings.

**10. SchemaRegistryDeveloper**

* **Permissions**: Manages schemas for Kafka topics.
* **Use Case**: Developers who need to work with Schema Registry.
* **Responsibilities**: Reads and writes schemas, but cannot manage schema compatibility settings.

**11. ConnectAdmin**

* **Permissions**: Full control over Kafka Connect.
* **Use Case**: Admins managing connectors in Kafka Connect.
* **Responsibilities**: Creates, updates, and deletes connectors, and manages connector configurations.

**12. ConnectOperator**

* **Permissions**: Limited control over Kafka Connect connectors.
* **Use Case**: Operators who need to monitor and manage connectors without full control.
* **Responsibilities**: Starts, stops, and restarts connectors but cannot create or delete them.

**13. ConnectViewer**

* **Permissions**: Read-only access to Kafka Connect.
* **Use Case**: Users who only need to view connectors and their statuses.
* **Responsibilities**: Views connector configurations and statuses without making changes.

**14. NetworkAdmin**

* **Permissions**: Manages networking configurations.
* **Use Case**: Users responsible for managing VPC peering, private links, and other networking setups.
* **Responsibilities**: Creates and manages networking resources such as VPC peering and private links.

**15. BillingAdmin**

* **Permissions**: Full control over billing-related settings.
* **Use Case**: Users responsible for managing the organization's billing information and invoices.
* **Responsibilities**: Views and manages billing details, payment methods, and usage reports.

**Summary of Key Roles:**

* **OrganizationAdmin**: Full control over the organization.
* **EnvironmentAdmin**: Full control over a specific environment.
* **CloudClusterAdmin**: Full control over Kafka clusters.
* **DeveloperRead/Write**: For developers with read or read-write access to Kafka resources.
* **Operator**: Manages Kafka cluster health and monitoring.
* **SecurityAdmin**: Manages security configurations (ACLs, RBAC, etc.).
* **ConnectAdmin/Operator/Viewer**: Administers or monitors Kafka Connect.

These roles provide granular control over different aspects of Confluent Cloud, making it easy to assign appropriate permissions based on specific responsibilities.