Samsung Cloud Platform

Management

IAM(Identity and Access Management)

An Enterprise-level Identity Authentication and Access Permissions Management Service

IAM is a service that controls the scope of access to services and resources within an account by verifying the identity of users registered in the Samsung Cloud Platform and granting access rights.
Account administrators can manage users, user groups, policies, and role items in detail through IAM, and can check and control the status of permission granting within an account at a glance through the dashboard.

Strong User Authentication

When accessing the console or API, Multi-Factor Authentication or access key authentication is required for users. In addition, restricting access to accounts based on IP addresses helps prevent unauthorized access.

Simplified Permission Management

Account administrators(Root users) can easily create and manage users, user groups, policies, and roles. By mapping users(IAM users) to groups and roles based on their work purpose, users' access rights are limited to the parts necessary for their work.

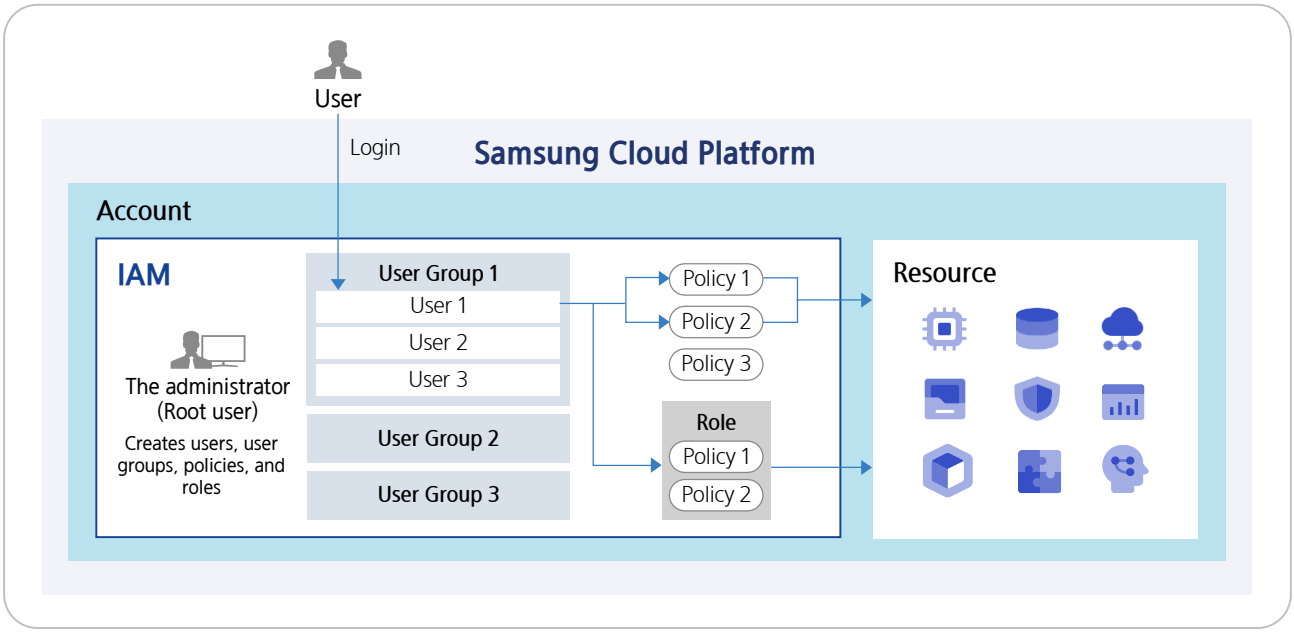
Fine-grained Access Control Policy

Users create access control policies for granular levels of control/action/resource type and authentication method/IP for each service within their account.
By applying the least privilege policy and providing userspecific access to cloud resources, IAM limits access by user type.

Access control through temporary credentials

Account administrators can create roles with temporary credentials to grant only the minimum privileges needed. By providing users with only the privileges they need for a limited time with temporary credentials, a high level of centralized management is possible for a large number of users.

Service Architecture



Key Features

- **Sign-up and security credential**
  - Sign up through additional authentication and enable MFA during login
  - Block unauthorized access attempts based on authentication key and access control
- **Manage permissions by user group**
  - Account-based user group setup and policy assignment
  - Easy management through user and policy mapping by user group
- **Access control policy**
  - Detailed management of task types by service and access rights by individual resources
  - Policy-based access control, access control by applying authentication
- **Create and switch roles**
  - Setting the account and SRN(SCP Resource Number) target role subject
  - Enhance security by assigning temporary credential through role switching

SAMSUNG SDS

www.samsungsds.com / cloud.samsungsds.com
contact.sds@samsung.com / scp_sales@samsung.com
youtube.com/samsungsds

Copyright 2025. Samsung SDS Co., Ltd. All rights reserved.