IBM Cloud Object Storage System
Components that are simple to manage and flexible to deploy

Manager	IBM Accesser*	IBM Slicestor*
• Fault management	• S3 interface	• Storage for slices
• Reporting	• Encrypts data	• Single site or multi-site
• Provisioning	• Slices data	• Capacity-based pricing
• Performance monitoring	• Disperses data	• Data integrity management
• Storage configuration	• Retrieves data	
• Single pane of glass	• Stateless	

Supported as an IBM appliance

Supported as Software Defined Storage (SDS)

IBM
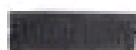
Cisco, Dell EMC, HPE, Lenovo, Supermicro

Easy to certify new models as a supported IBM configuration

IBM Cloud

Catalog   Docs   Support   **Manage**

Search for resource...   IBM

Getting started New

Setting up

Creating buckets

Access management

Buckets

Endpoint

Service credentials

Connections

Usage details

Plan

Access Management

IBM® Cloud Identity & Access Management (IAM) enables you to securely authenticate users and control access to all cloud resources consistently in the IBM Cloud Platform.

Invite Users   **Create credential**

Identity and Access Management

The concept of access management in IBM Cloud consists of a few interrelated components, including users, resources, policies, roles, actions, and the Cloud IAM control system, which allow users to take actions on resources within an account.

Learn more

Users

All users are identified by their IBMid.

Service IDs

Service IDs are the Cloud IAM feature that is used to provide a separate identity for services and applications. You can create a service ID to be used by an application that needs access to your IBM Cloud services so that individual user credentials do not have to be used.

Cloud Resource Name (CRN)

Exist exclusively within an IBM Cloud Service Instance. In a Cloud Object Storage instance, a bucket is a resource.

Access at the Instance level

Using IAM you can manage access at the IBM® Cloud Object Storage service instance, where a user or Service ID can have access to buckets in the instance.

Access at the bucket level

Using IAM you can manage access at the bucket level, where a user or Service ID can have access to bucket only