

Concepts and definitions

Term / Concept	Description
Account Recycling	The process of cleaning and reusing sandbox accounts after they hit budget or time limits. This reduces AWS account sprawl, optimises resource use, and minimises administrative work by resetting accounts for new users.
Account Template	A preconfigured set of sandbox rules and settings that define how an account can be used. Templates can include approval requirements, budgets, alert thresholds, lease durations, and automatic enforcement actions. Admins and managers create templates, and users request new sandbox leases by selecting from the available templates.
AWS Nuke	An open-source automation tool that systematically deletes AWS resources across an account. It is used during account recycling to ensure no residual resources or configurations remain before reassigning the account.
Budget threshold	A predefined spending limit set by the customer. When spending reaches this threshold, Sandbox Studio can trigger automated actions such as sending alerts, stopping running resources, or blocking new deployments to prevent budget overruns.
Guardrails	Preventive and detective controls that help maintain security, compliance, and operational standards within sandbox accounts. Guardrails can include service restrictions, security configurations, and automated checks that detect or prevent policy violations.
Hub Account	A centralised AWS account used by Sandbox Studio to coordinate sandbox operations. The hub hosts shared resources, enforces configuration, and orchestrates automation across all sandbox accounts.
Lease	A temporary allocation of an AWS account to a user for a set time or budget. During the lease period, the user can run experiments or projects. When the lease expires, the account is reclaimed or recycled according to predefined rules.
Organisation Management Account	The management account is the top-level account in an AWS Organisation. It is automatically created when you set up the organisation and has full administrative control over all member accounts.

Term / Concept	Description
Organisational Unit (OU)	A logical grouping of AWS accounts within AWS Organisations that lets you organise accounts in a hierarchy and apply governance policies. Sandbox Studio creates separate OUs for active sandbox accounts and for recycled (cleaned and reusable) accounts, simplifying management and policy enforcement.
Permission set	A collection of IAM Identity Center permissions that define what a user can do within an AWS account. Permission sets are centrally managed and applied to users or groups to ensure consistent, controlled access.
Resource controls	Automated policies and mechanisms that manage the lifecycle of AWS resources. These controls enforce creation limits, modification rules, and automated cleanup based on budgets, time limits, and security requirements.
Sandbox environment	A controlled, isolated AWS environment that allows teams to experiment, test, and learn without affecting production systems. Sandboxes provide a safe space to try new services, prototype solutions, or run training exercises, with built-in limits and guardrails to prevent accidental overuse or security risks.
Service Control Policies (SCPs)	Organisation-wide permission boundaries that define the maximum available AWS permissions for accounts within an OU. SCPs are used to enforce consistent security, restrict high-risk services, and ensure sandbox accounts cannot bypass established rules.

Revision #8

Created 2025-07-14 21:03:09 UTC

Updated 2025-08-24 06:18:05 UTC by Andy