Solution overview

The overview describes the Features and Benefits, Use cases and concept and definitions.

Overview

What is Sandbox Studio?

Sandbox Studio is a web-based solution that helps cloud administrators manage **temporary AWS sandbox environments**. It automates the enforcement of **security policies**, **governance rules**, **budget controls**, and **account recycling settings** — all through an easy-to-use web interface.

The solution allows organisations to give teams a safe space to **experiment**, **learn**, and **prototype** with AWS services in **production-isolated AWS accounts** that are cleaned and recycled after use.

Key Capabilities

Sandbox Studio automatically configures a **sandbox Organizational Unit (OU)** in AWS Organizations. This OU is preloaded with AWS best practices for **workload isolation** and **governance**. When deployed, it applies a standard set of **policies**, **guardrails**, and **controls** to all sandbox accounts.

The platform provides:

- **Automated cost controls**
  - Sends alerts when spending approaches budget limits.
  - Can trigger automated actions (e.g., resource shutdowns) when limits are reached.
- **Account recycling**
  - Allows accounts to be used for a **fixed duration** or until a **spend threshold** is met.
  - Cleans and resets accounts at the end of the sandbox period.
- **Security restrictions**
  - Limits access to expensive or sensitive AWS actions within sandbox accounts.

Common Use Cases

Sandbox Studio supports a wide range of scenarios where teams need safe, temporary AWS environments. These environments can be pre-configured, budget-limited, and automatically cleaned up — making them ideal for experimentation, learning, and short-term projects. Below are some of the most common ways organisations use Sandbox Studio.

Development and Innovation Experiments

Typical users: Developers, product engineers
Create small-scale, temporary AWS setups to try out new services or features before committing to

a production build. Teams can quickly explore possibilities, validate technical approaches, and demonstrate value without the overhead of a full deployment pipeline.

Train and Test GenAI Models

Typical users: Machine learning engineers, data scientists
Work with pre-configured environments to train and fine-tune generative AI models. Sandbox Studio makes it easy to run experiments with different training datasets, apply reinforcement learning techniques, and monitor outcomes in a safe, isolated space.

Test Environments

Typical users: QA/test engineers
Spin up a clean, disposable environment for thorough application testing. These sandboxes are ideal for verifying integrations, reproducing defects, running regression suites, and testing API updates — all without risking production stability.

Higher Education Training Labs

Typical users: Professors, lecturers, academic department heads
Set up classroom-ready AWS accounts for students to explore cloud computing hands-on. Instructors can control spending, reset environments between sessions, and ensure each student gets a fresh workspace for assignments or exams.

Research and Development (R&D)

Typical users: University researchers, enterprise R&D teams
Provide a controlled cloud platform for research teams to run experiments and gather data. These sandboxes make it possible to test hypotheses, simulate real-world conditions, and analyse results without long-term infrastructure commitments.

Employee Onboarding and Training

Typical users: Training leads, HR onboarding teams
Launch short-lived AWS environments to give new hires or existing staff practical experience with tools, workflows, or new technologies. Ideal for structured training sessions, internal workshops, or skills refreshers.

Hackathons

Typical users: Enterprise IT teams
Run organisation-hosted hackathons in AWS accounts you own and control. This enables participants to work on real challenges while keeping sensitive or proprietary data inside your

security boundaries.

Demo Environments

Typical users: Engineers, solution architects
Set up temporary environments to showcase applications or solutions. These can be pre-loaded with sample data and configurations to deliver smooth, predictable demos to clients or stakeholders.

Software Vendor Trials

Typical users: Software vendors, sales engineers
Offer time-limited or budget-restricted AWS environments so customers can test your software. This ensures a consistent experience for every trial while keeping operational costs under control.

Who Should Use This Guide

This installation guide is designed for:

- **Solution architects**
- **DevOps engineers**
- **AWS account administrators**
- **Cloud operations teams**

It provides:

- An **architecture overview**
- **Planning considerations** before deployment
- **Step-by-step configuration instructions** for launching Sandbox Studio in your AWS environment

Core Capabilities

Sandbox Studio provides a range of tools to make AWS sandbox account management fast, safe, and cost-effective. The table below explains the core capabilities of the platform, how it works, and the specific benefits it can bring to your teams.

Capability	What It Does	Benefit
Instant Account Access	• Launch AWS sandbox accounts in seconds with all required configurations already applied. • Accounts are ready for use immediately without any manual setup.	• Start projects right away without waiting for environments to be built. • Enable rapid experimentation, testing, or proof-of-concept work.
Stay on Budget	• Define spending limits for each account so costs are controlled automatically. • Receive alerts in real time before spending thresholds are exceeded.	• Prevent budget overruns before they happen. • Keep sandbox activity predictable and aligned with financial goals.
Simplified Account Cleanup	• Automatically remove all deployed resources when an account reaches its budget or time limit. • Reset the account back to a clean, ready-to-use state.	• Reduce manual cleanup effort and free up team time. • Ensure accounts are always safe to reuse for the next activity.
Built-in Security	• Apply service control policies (SCPs) to restrict services, regions, or actions. • Configure IAM permissions automatically for each sandbox account.	• Enforce security and compliance rules without manual setup. • Reduce the risk of unauthorised access or unsafe configurations.
Flexible Permissions	• Assign role-based IAM permissions tailored to each account type. • Limit user access to only the resources and actions they need.	• Prevent accidental or unwanted changes to environments. • Match account access precisely to each team member’s responsibilities.

Capability	What It Does	Benefit
Ready-to-Launch Environments	• Pre-provision AWS accounts with infrastructure for specific events or learning activities. • Perfect for hackathons, training workshops, and tutorials.	• Eliminate setup delays before events begin. • Provide a consistent, ready-made environment for participants.
Controlled Access	• Allow managers to oversee and manage specific accounts or groups. • Define permissions in detail to control exactly who can do what.	• Maintain a clear hierarchy of control across accounts. • Balance flexibility with governance requirements.
Easy Management	• Manage all sandbox accounts from a single, centralised dashboard. • Interface is designed to be simple for both technical and non-technical users.	• Give all team members the ability to manage sandboxes confidently. • Reduce reliance on technical specialists for basic account tasks.

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.