Choosing the hub account

Sandbox Studio requires multiple AWS accounts to function. These accounts follow a **hub-and-spoke model**, where a central **hub account** manages a pool of **sandbox accounts**. The **organisation management account** also plays a key role, as certain AWS services can only be controlled from this top-level account.

There are three types of AWS accounts involved:

Organisation Management Account

- This is the top-level account in an AWS Organisation.
- It is automatically created when you set up the organisation.
- It has full administrative control over all member accounts.
- AWS recommends avoiding workloads in this account; instead, use it primarily for governance and management (e.g. running AWS Control Tower).

Why Sandbox Studio needs this account

Sandbox Studio requires limited components to be deployed into the organisation management account because:

1. **Organisational Units (OUs) and Service Control Policies (SCPs):**
   Only the management account can create and manage OUs and SCPs. Sandbox Studio uses these to organise accounts and enforce guardrails. Accounts are automatically moved between OUs during their lifecycle (e.g. from “Active” to “Cleanup”).
2. **Identity setup:**
   The initial set of IAM Identity Center roles and groups for Sandbox Studio is created in the management account. These are used for authentication and authorisation of users.
3. **Cost management:**
   The management account provides access to consolidated billing and Cost Explorer data. Sandbox Studio uses this to query costs for sandbox accounts in bulk, reducing overhead compared to querying accounts individually.

> **Important:** Two of the seven CloudFormation stacks **must** be installed in the organisation management account. See CloudFormation templates section for more details.

Hub Account

- A dedicated member account used to host most of the Sandbox Studio solution.
- Acts as the **central hub** that manages sandbox accounts (the “spokes”).
- Runs shared infrastructure, automation, and orchestration services.

Benefits of using a hub account

- Keeps the organisation management account clean and reserved for governance only.
- Separates operational workloads from core AWS Organisation functions.
- Provides a secure, centralised place for automation and account lifecycle management.

Sandbox Accounts

- These are the accounts actually handed out to users.
- They are recycled and reused through an automated lifecycle.
- Administrators create a pool of accounts, then onboard them into Sandbox Studio.
- Once onboarded, the accounts are considered **managed** by Sandbox Studio.

The system controls their lifecycle by:

- Assigning them to OUs (e.g. “Active” or “Cleanup”).
- Applying SCPs and guardrails.
- Resetting and recycling them after a lease expires.

Note: Sandbox accounts are intended for non-production use. If your users are looking for ways to provision production ready accounts, consider alternative solutions.

Deployment Options

You have two choices when deploying Sandbox Studio:

1. **Deploy everything into the organisation management account**
   - Simplifies the setup.
   - Not recommended by AWS, as it mixes governance functions with workloads.
2. **Split the deployment between management and hub accounts (recommended)**
   - Management account runs only the required governance components.
   - Hub account runs the main solution.
   - Provides better alignment with AWS best practices for multi-account security and governance.

Revision #8
Created 2025-07-14 21:15:40 UTC
Updated 2025-08-30 01:04:10 UTC by Andy