**aws**

AWS Reference Architecture Diagram

# AWS Innovation Sandbox

# AWS Innovation Sandbox: AWS Reference Architecture Diagram

# Table of Contents

# AWS Innovation Sandbox

Publication date: **August 9, 2021 ([Diagram history](#))**

This architecture enables you to deploy secure, self-contained, isolated environments to allow developers, security professionals, and infrastructure teams to safely experiment with AWS services and third-party applications that run on AWS. This architecture can also be [deployed on AWS](#) using AWS CloudFormation templates that launch and configure the AWS services required to deploy this solution using AWS best practices for security and availability.

## AWS Innovation Sandbox
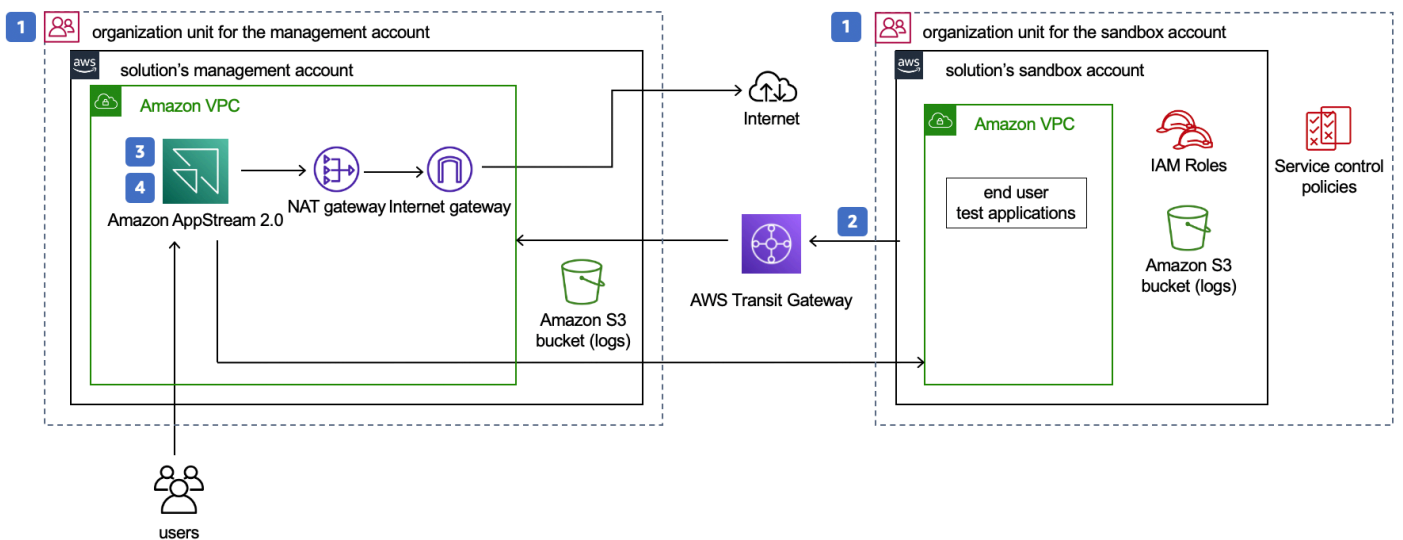


1. An **AWS CloudFormation** template creates two new AWS accounts and two new organizational units (OUs):

   - An organizational unit containing the management account, an **Amazon Virtual Private Cloud** (Amazon VPC) running a NAT gateway, an **AWS Transit Gateway**, and an internet gateway.
   - An organizational unit containing the sandbox account and an Amazon VPC.

2. The solution's sandbox account has no direct access to the Internet. Ingress and egress traffic to this sandbox account are routed through **AWS Transit Gateway** to the solution's management account. Access to the sandbox account is restricted via the **AWS Identity and Access Management** (IAM) condition key aws:SourceIp, to allow access only from the management account (allowing for a self-contained environment

3. An **Amazon AppStream 2.0** image is created by the customer with required applications and tools.

4. A second **CloudFormation** template uses the image created in Step 3 to launch an instance fleet, where **AppStream 2.0** end users connect to access the sandbox account.

# Download editable diagram

To customize this reference architecture diagram based on your business needs, download the ZIP file which contains an editable PowerPoint.

# Create a free AWS account

Sign up now

Sign up for an AWS account. New accounts include 12 months of AWS Free Tier access, including the use of Amazon EC2, Amazon S3, and Amazon DynamoDB.

# Further reading

For additional information, refer to

- AWS Architecture Icons
- AWS Architecture Center
- AWS Well-Architected

# Diagram history

To be notified about updates to this reference architecture diagram, subscribe to the RSS feed.

| Change | Description | Date |
| --- | --- | --- |
| Initial publication | Reference architecture diagram first published. | August 9, 2021 |

> ⓘ **Note**
>
> To subscribe to RSS updates, you must have an RSS plugin enabled for the browser you are using.