Roles deployed by the solution

Sandbox Studio installs multiple roles in your environment, each serving different purposes

Role name	Account created in	Purpose	Can be assumed by
OrgMgtRole - *SandboxStudio-{Namespace}-OrgMgtRole*	Management Account	For operations on the org management account (Move accounts between OUs, etc.)	IntermediateRole in Hub Account
IntermediateRole - *SandboxStudio-{Namespace}-IntermediateRole*	Hub Account	For functions, step functions, etc to assume to then be able to assume the Org Management Role	Roles starting with SandboxStudio-Compute-* and SandboxStudio-API-*
IdcRole - *SandboxStudio-{Namespace}-IdcRole*	Management Account	For operations in Identity Center	IntermediateRole in Hub Account
SandboxAccountRole - *SandboxStudio-{Namespace}-SandboxAccountRole*	Member accounts	For Hub Accounts to control member accounts	IntermediateRole in Hub Account
CodeBuildDeployRole	Member accounts	To allow launch templates in member accounts	Step function to create launch templates
LaunchTemplateExternalAccessRole	Hub Account	Allows access to S3 buckets in external accounts	CodeBuildDeployRole

More info on LaunchTemplateExternalAccessRole

This role is a bit particular in the sense that it is created with the following policy:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Condition": {
                "StringNotEquals": {
                    "aws:ResourceAccount": "<HUB ACCOUNT ID>"
                }
            },
```

```
            "Action": [
                "s3:GetObject",
                "s3:ListBucket"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

This gives the role permissions to list buckets and get objects in every buckets that are NOT the Hub Account (The account where the role is created).

The purpose of this is to allow you to grant this role access to your own bucket should you have resources in other accounts.

For example, let's say you want to launch a template in a Sandbox Account with resources coming from an external S3 bucket (resources, CloudFormation templates, ...). You can grant access to your external bucket to this role through **Bucket policy**.

The codebuild task running your launch template will assume this role which in turn can access your resources in a secure manner.

Revision #6
Created 2025-10-16 10:00:23 UTC by Paul
Updated 2025-10-21 05:54:59 UTC by Paul