include::attributes.txt[]

// Attributes

[.topic] [#deploy-troubleshoot] = Troubleshoot {aws} CDK deployments :info\_titleabbrev: Troubleshoot CDK deployments :keywords: {aws} CDK, Deploy, Troubleshoot

== [abstract]

## Troubleshoot common issues when deploying {aws} Cloud Development Kit ({aws} CDK) applications.

// Content start

Troubleshoot common issues when deploying {aws} Cloud Development Kit ({aws} CDK) applications.

[#deploy-troubleshoot-sp] == Incorrect service principals are being created at deployment

When deploying CDK applications that contain {aws} Identity and Access Management (IAM) roles with service principals, you find that incorrect domains for the service principals are being created.

The following is a basic example of creating an IAM role that can be assumed by Amazon CloudWatch Logs using its service principal:

== [source,javascript,subs=“verbatim,attributes”]

import \* as cdk from ‘aws-cdk-lib’; import \* as iam from ‘aws-cdk-lib/aws-iam’; import { Construct } from ‘constructs’;

export class MyCdkProjectStack extends cdk.Stack { constructor(scope: Construct, id: string, props?: cdk.StackProps) { super(scope, id, props);

…. // Create an IAM role for CloudWatch Logs to assume const cloudWatchLogsRole = new iam.Role(this, ‘CloudWatchLogsRole’, { assumedBy: new iam.ServicePrincipal(‘logs.amazonaws.com’), // This is for CloudWatch Logs managedPolicies: [ iam.ManagedPolicy.fromAwsManagedPolicyName(‘service-role/AWSCloudWatchLogsFullAccess’) ] });

// You can then use this role in other constructs or configurations where CloudWatch Logs needs to assume a role } } —- ….

When you deploy this stack, a service principal named logs.amazonaws.com should be created. In most cases, {aws} services use the following naming for service principals: <service>.amazonaws.com.

[#deploy-troubleshoot-sp-causes] === Common causes

If you are using a version of the {aws} CDK older than v2.150.0, you may encounter this bug. In older {aws} CDK versions, the naming of service principals were not standardized, which could lead to the creation of service principals with incorrect domains.

In {aws} CDK v2.51.0, a fix was implemented by standardizing all automatically created service principals to use <service>.amazonaws.com when possible. This fix was available by allowing the @aws-cdk/aws-iam:standardizedServicePrincipals feature flag.

Starting in {aws} CDK v2.150.0, this became default behavior.

[#deploy-troubleshoot-sp-resolution] === Resolution

Upgrade to {aws} CDK v2.150.0 or newer.

If you are unable to upgrade to {aws} CDK v2.150.0 or newer, you must upgrade to at least v2.51.0 or newer. Then, allow the following feature flag in your cdk.json file: @aws-cdk/aws-iam:standardizedServicePrincipals.