AWS CloudFormation: Core Concepts & Importing Existing Resources

Introduction

CloudFormation enables infrastructure as code (IaC) in AWS, allowing users to define, provision, and manage AWS infrastructure using declarative YAML or JSON templates. With the new IaC generator feature, CloudFormation now supports automatic generation of templates from existing resources, easing the transition to IaC for legacy workloads.

Overview

CloudFormation provides a template-driven orchestration model for AWS infrastructure, enabling version control, automation, and repeatable deployments. The IaC generator extends this by allowing you to scan existing AWS resources and generate CloudFormation templates for them.

Pre-requisites

- IAM permissions for CloudFormation scans and relevant resource read access
- Familiarity with basic AWS services (EC2, RDS, IAM, etc.)
- AWS CLI installed (optional for automation)

Key Concepts

- **Template**: A YAML or JSON file describing AWS resources
- **Stack**: A deployed instance of a template
- **IaC Generator**: A feature that scans deployed resources and builds CloudFormation templates from them
- **Scan Types**:
  - Full Scan: Scans all supported resources in a Region
  - Partial Scan: Scans a selected subset of resource types

IaC Generator Workflow

1. **Start a Resource Scan**
   - Full scan or partial scan based on desired scope
   - Up to 100,000 resources, 10 scans/day (<10k resources)

    - CLI: `aws cloudformation start-resource-scan`
2. **Create or Modify Template**
    - Use scanned resources to start from scratch or extend an existing template
    - Select related resources for complete workloads
    - Console and CLI supported
3. **Generate Template**
    - CLI: `aws cloudformation create-generated-template`
    - Templates are stored and listed with: `list-generated-templates`
4. **Preview & Visualize with Infrastructure Composer**
    - Visual canvas to examine architecture
    - Identify write-only properties before final import
5. **Create Stack & Import Resources**
    - Use generated template to create or update a CloudFormation stack
    - CLI: `aws cloudformation import-resources`

Permissions Required

- `cloudformation:StartResourceScan`, `DescribeResourceScan`, `CreateGeneratedTemplate`, etc.
- Read permissions for each scanned resource type
- Example: `ec2:DescribeInstances`, `s3:GetBucketPolicy`, etc.

Migrate to AWS CDK

- Use `cdk migrate` to convert CloudFormation templates into CDK apps
- Manage resources in your preferred language (TypeScript, Python, Java, etc.)
- Follow CDK migration documentation: https://docs.aws.amazon.com/cdk/v2/guide/migrate.html

Considerations

- **Write-only Properties**: These cannot be recovered and must be added manually
- **Template Size Limits**: Max 500 resources per generated template
- **Scan Retention**: Scans are valid for 30 days
- **Limitations**: Only resources supported by Cloud Control API are eligible
- **IAM Scope**: Scans are limited to resources the caller can read

Common CLI Commands

```
Unset
aws cloudformation start-resource-scan --region us-east-1

aws cloudformation describe-resource-scan
--resource-scan-id <scan-id>

aws cloudformation list-resource-scan-resources
--resource-scan-id <scan-id>

aws cloudformation list-resource-scan-related-resources
--resource-scan-id <scan-id> --resources
file://resources.json

aws cloudformation create-generated-template
--generated-template-name MyTemplate --resources
file://resources.json

aws cloudformation list-generated-templates
```

Documentation

- What is CloudFormation: https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/Welcome.html
- IaC Generator: https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/generate-IaC.html
- Cloud Control API: https://docs.aws.amazon.com/cloudcontrolapi/latest/userguide/what-is-cloudcontrolapi.html
- CDK Migration: https://docs.aws.amazon.com/cdk/v2/guide/migrate.html