

Syntree Flosports | Subdomain Delegation

Introduction

We have multiple accounts, a Management Account that contains the HostedZone for example `flo-infra.net`. We need to delegate subdomains to hosted zones in the child accounts.

e.g., the Subdomain pattern will look like `{app}.{account}.flo-infra.net` so for the flo360 account it would need `flo360.flo-infra.net` as apps can add its primary Hosted Zone and subdomains as they use them.

We will use cloudformation template to delegate subdomains to hosted zones in each child account. This cloudformation template will add the subdomain in A record once it is created as a hosted zone in the child account automatically.

Steps to delegate subdomains to hosted zones

First, we need to set up the Lambda function and SNS trigger in the master account to delegate subdomains to hosted zones in the child account.

Master account configuration

Step 1: Go to Cloudformation and select Create Stack, select With New resource

Step 2: Put the object URL of the template and select next.

The screenshot shows the AWS CloudFormation console's 'Create stack' wizard. The left sidebar shows the progress: Step 1 (Create stack), Step 2 (Specify stack details), Step 3 (Configure stack options), and Step 4 (Review). The main content area is titled 'Create stack' and has a sub-header 'Prerequisite - Prepare template'. Under 'Prepare template', there are three radio buttons: 'Template is ready' (selected), 'Use a sample template', and 'Create template in Designer'. Below this is the 'Specify template' section, which includes a 'Template source' dropdown (set to 'Amazon S3 URL'), an 'Upload a template file' button, and a text field for the 'Amazon S3 URL' containing the URL `https://flo-controltower-bucket.s3.amazonaws.com/hosted-zone-delegation/hosted-zone-delegation.yml`. At the bottom, there is a 'View in Designer' button and 'Cancel' and 'Next' buttons.

- **Step 3:** Fill all the details such as
Stack name: Name of the stack
- AuthorisedAccount: List of authorised account where you want to delegate subdomains
e.g: 111111111111, 222222222222
- HostedZoneId: Main hosted zone Id
- S3Bucket: S3 bucket name where we shored template

- S3Key: S3 key of zip file

select next

Specify stack details

Stack name: hostedZoneDelegation

Parameters:

- AuthorizedAccounts: 321459047448, 649752860538, 773285077662, 672384404487
- HostedZoneId: Z0002711BAPIBELUWEHZ
- S3Bucket: flo-controltower-bucket
- S3Key: hosted-zone-delegation/index.zip

Buttons: Cancel, Previous, Next

Step 4: Review all the details, check the terms and conditions box, and select submit.

This stack will create a Lambda function and trigger SNS topic for delegated subdomains.

Child account configuration

Step 1: Go to Cloudformation and select Create Stack, select With New resource

Step 2: Upload the cloudformation template of the child account configuration and select next.

Create stack

Prerequisite - Prepare template

Prepare template

Every stack is based on a template. A template is a JSON or YAML file that contains configuration information about the AWS resources you want to include in the stack.

☒ Template is ready
 ☐ Use a sample template
 ☐ Create template in Designer

Specify template

A template is a JSON or YAML file that describes your stack's resources and properties.

Template source

Selecting a template generates an Amazon S3 URL, where it will be stored.

☐ Amazon S3 URL
 ☒ Upload a template file

Upload a template file

Choose file

JSON or YAML formatted file

S3 URL: https://s3-us-east-1.amazonaws.com/cf-templates-1mdvm1x01s5q-us-east-1/2023-09-18T112647.1932vtf-hosted-zone.yml

Buttons: Cancel, Next

Step 3: Fill all the details

DomainName: Subdomain that you want to delegate

MasterAccountId: Master account ID.

select Next

The screenshot shows the AWS CloudFormation console interface. The top navigation bar includes the AWS logo, 'Services', a search bar, and the user's profile. The main content area is titled 'Specify stack details' and is part of a multi-step process. On the left, a sidebar lists the steps: Step 1 (Create stack), Step 2 (Specify stack details), Step 3 (Configure stack options), and Step 4 (Review hostedZoneDelegation). The 'Specify stack details' section contains two main input areas. The first is 'Stack name', where the value 'hostedZoneDelegation' is entered. Below this, a note states: 'Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-)'. The second area is 'Parameters', which includes 'DomainName' set to 'flo360.flo-infra.net' and 'MasterAccountid' set to '799900115832'. At the bottom right of the form, there are three buttons: 'Cancel', 'Previous', and 'Next'.

Step 4: Review all the configuration and select submit

The screenshot shows the 'Review hostedZoneDelegation' step in the AWS CloudFormation console. The interface is divided into three main sections. The first section, 'Rollback configuration', includes 'Monitoring time' (set to '-') and 'CloudWatch alarm ARN' (set to '-'). The second section, 'Notification options', shows 'SNS topic ARN' (set to '-') and a message: 'No notification options. There are no notification options defined.' The third section, 'Stack creation options', includes 'Timeout' (set to '-') and 'Termination protection' (set to 'Deactivated'). At the bottom left, there is a 'Quick-create link' and a 'Create change set' button. At the bottom right, there are three buttons: 'Cancel', 'Previous', and 'Submit'.

This will create a hosted zone for the subdomain in child account.

References

[Managing Cross-Account DNS with Route 53, Lambda, and CloudFormation](https://github.com/martijnvandongen/blog-managing-cross-account-dns-with-route-53-lambda-and-cloudformation)

<https://github.com/martijnvandongen/blog-managing-cross-account-dns-with-route-53-lambda-and-cloudformation>