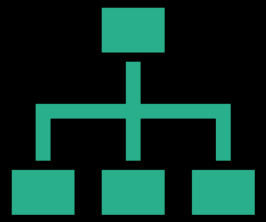


Organization Formation

Better than landing zones!

Features

- 15+ features in managing organizations
- 25+ features in managing resources
- 14+ features in automation
- And then some….

Managing organizations

1. Manage your organization using IaC

```
      Accounts:
        - !Ref SharedUsersAccount
        - !Ref SharedServicesAccount

  SharedUsersAccount:
    Type: OC::ORG::Account
    Properties:
      RootEmail: users-2@olafconijn.awsapps.com
      Alias: org-formation-users
      AccountName: Shared Users Account
      PasswordPolicy: !Ref PasswordPolicy
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL 1: zsh

```
→  examples git:(master) ✗ org-formation update organization.yml --profile org-formation
OC::ORG::Account              | SharedUsersAccount          | Update
OC::ORG::Account              | SharedUsersAccount          | CommitHash
OC::ORG::Account              | SharedServicesAccount       | Update
OC::ORG::Account              | SharedServicesAccount       | CommitHash
OC::ORG::OrganizationalUnit   | SharedOU                    | Update
OC::ORG::OrganizationalUnit   | SharedOU                    | CommitHash
INFO: done
→  examples git:(master) ✗
```

2. Create AWS Accounts in code

```
51      RootEmail: shared-services-2@olafconijn.awsapps.com
52      Tags:
53        budget-alarm-threshold: '20'
54        account-owner-email: olaf@email.com
55
56    Production1:
57      Type: OC::ORG::Account
58      Properties:
59        RootEmail: production1@olafconijn.awsapps.com
60        AccountName: Production 1 Account
61
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL 1: zsh

```
→  examples git:(master) ✗ org-formation update organization.yml --profile org-formation
OC::ORG::Account                | Production1                    | Create (353550728234)
OC::ORG::Account                | Production1                    | CommitHash
INFO: done
→  examples git:(master) ✗
```

3. Create Organizational Units in code

```
57      Type: OC::ORG::Account
58      Properties:
59        RootEmail: production1@olafconijn.awsapps.com
60        AccountName: Production 1 Account
61
62    ProductionOU:
63      Type: OC::ORG::OrganizationalUnit
64      Properties:
65        OrganizationalUnitName: production
66
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL 1: zsh

```
→  examples git:(master) ✗ org-formation update organization.yml --profile org-formation
OC::ORG::OrganizationalUnit   | ProductionOU                  | Create (ou-amf0-sr80xn5x)
OC::ORG::OrganizationalUnit   | ProductionOU                  | CommitHash
INFO: done
→  examples git:(master) ✗
```

4. Create SCPs in code

```
    Type: OC::ORG::OrganizationalUnit
    Properties:
      OrganizationalUnitName: production

  RestrictUnusedRegionsPolicy:
    Type: OC::ORG::ServiceControlPolicy
    Properties:
      PolicyName: RestrictRegions
      Description: Restrict Unused regions
      PolicyDocument:
        Version: '2012-10-17'
        Statement:
          - Sid: DenyUnsupportedRegions
            Effect: Deny
            NotAction:
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL 1: zsh

```
→  examples git:(master) ✗ org-formation update organization.yml --profile org-formation
OC::ORG::ServiceControlPolicy | RestrictUnusedRegionsPolicy   | Create (p-8yi9k8jd)
INFO: done
→  examples git:(master) ✗
```

5. Add Accounts to OU in code

```
54        account-owner-email: olaf@email.com
55
56    Production1:
57      Type: OC::ORG::Account
58      Properties:
59        RootEmail: production1@olafconijn.awsapps.com
60        AccountName: Production 1 Account
61
62    ProductionOU:
63      Type: OC::ORG::OrganizationalUnit
64      Properties:
65        OrganizationalUnitName: production
66        Accounts:
67          - !Ref Production1
68
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL 1: zsh

```
➜  examples git:(master) ✗ org-formation update organization.yml --profile org-formation
OC::ORG::OrganizationalUnit   | ProductionOU                  | Attach Account (Production1)
OC::ORG::OrganizationalUnit   | ProductionOU                  | CommitHash
INFO: done
➜  examples git:(master) ✗
```

6. Add SCPs to Accounts and OUs in code

```yaml
      ServiceControlPolicies:
        - !Ref RestrictUnusedRegionsPolicy

  ProductionOU:
    Type: OC::ORG::OrganizationalUnit
    Properties:
      OrganizationalUnitName: production
      ServiceControlPolicies:
        - !Ref RestrictUnusedRegionsPolicy
      Accounts:
        - !Ref Production1

  RestrictUnusedRegionsPolicy:
    Type: OC::ORG::ServiceControlPolicy
    Properties:
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL 1: zsh

```
INFO: done
→  examples git:(master) ✗ org-formation update organization.yml --profile org-formation
OC::ORG::Account              | Production1                  | Attach Policy (RestrictUnusedRegionsPolicy)
OC::ORG::Account              | Production1                  | CommitHash
OC::ORG::OrganizationalUnit   | ProductionOU                 | Attach Policy (RestrictUnusedRegionsPolicy)
OC::ORG::OrganizationalUnit   | ProductionOU                 | CommitHash
```

7. Add SCPs to Organization Root in code

examples > organization.yml

```
39  SharedServicesAccount: ...
48
49  Production1: ...
56
57  ProductionOU: ...
65
66  OrganizationRoot:
67    Type: OC::ORG::OrganizationRoot
68    Properties:
69      ServiceControlPolicies:
70      - !Ref RestrictUnusedRegionsPolicy
71
72  RestrictUnusedRegionsPolicy:
73    Type: OC::ORG::ServiceControlPolicy
74    Properties:
75      PolicyName: RestrictRegions
76      Description: Restrict Unused regions
77      PolicyDocument:
78        Version: '2012-10-17'
79        Statement:
80        - Sid: DenyUnsupportedRegions
```

8. Add Tags to Accounts in code

```
39  SharedServicesAccount: …
48
49  Production1:
50    Type: OC::ORG::Account
51    Properties:
52      RootEmail: production1@olafconijn.awsapps.com
53      AccountName: Production 1 Account
54      ServiceControlPolicies:
55        - !Ref RestrictUnusedRegionsPolicy
56      Tags:
57        budget-alarm-threshold: '100'
58        account-owner-email: olaf@email.com
59
60  ProductionOU: …
68
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL 1: zsh

```
→  examples git:(master) ✗ org-formation update organization.yml --profile org-formation
OC::ORG::Account                | Production1                    | Update
OC::ORG::Account                | Production1                    | CommitHash
INFO: done
→  examples git:(master) ✗
```

9. Add IAM Alias to Accounts in code

```
27
28  SharedUsersAccount: …
38      Olaf Conijn, 4 months ago • added temp to git
39  SharedServicesAccount: …
48
49  Production1:
50    Type: OC::ORG::Account
51    Properties:
52      RootEmail: production1@olafconijn.awsapps.com
53      AccountName: Production 1 Account
54      Alias: my-production1
55      ServiceControlPolicies:
56        - !Ref RestrictUnusedRegionsPolicy
57      Tags:
58        budget-alarm-threshold: '100'
59        account-owner-email: olaf@email.com
60
61  ProductionOU: …
69
70  OrganizationRoot: …
75
```

10. Create IAM Password Policy in code

```
128
129 >   RestrictUnusedRegionsSCP: …
151
152     PasswordPolicy:
153       Type: OC::ORG::PasswordPolicy
154       Properties:
155         MaxPasswordAge: 30
156         MinimumPasswordLength: 12
157         RequireLowercaseCharacters: true
158         RequireNumbers: true
159         RequireSymbols: true
160         RequireUppercaseCharacters: true
161         PasswordReusePrevention: 5
162         AllowUsersToChangePassword: true
163
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL 1: zsh

```
→  examples git:(master) ✗ org-formation update organization.yml --profile org-formation
OC::ORG::Account                | Production1                    | Update
OC::ORG::Account                | Production1                    | CommitHash
INFO: done
→  examples git:(master) ✗
```

11. Add IAM Pwd Policy to Accounts in code

```
48
49      Production1:
50        Type: OC::ORG::Account
51        Properties:
52          RootEmail: production1@olafconijn.awsapps.com
53          AccountName: Production 1 Account
54          Alias: my-production1
55          PasswordPolicy: !Ref PasswordPolicy
56          ServiceControlPolicies:
57            - !Ref RestrictUnusedRegionsPolicy
58          Tags:
59            budget-alarm-threshold: '100'
60            account-owner-email: olaf@email.com
61
62      ProductionOU: …
70
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL 1: zsh

```
➜  examples git:(master) ✗ org-formation update organization.yml --profile org-formation
OC::ORG::Account                | Production1                    | Update
OC::ORG::Account                | Production1                    | CommitHash
INFO: done
➜  examples git:(master) ✗
```

12. Use Yaml substitutions

```
    Type: OC::ORG::OrganizationalUnit
    Properties:
      OrganizationalUnitName: production

  RestrictUnusedRegionsPolicy:
    Type: OC::ORG::ServiceControlPolicy
    Properties:
      PolicyName: RestrictRegions
      Description: Restrict Unused regions
      PolicyDocument:
        Version: '2012-10-17'
        Statement:
          - Sid: DenyUnsupportedRegions
            Effect: Deny
            NotAction:
```

TODO

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL 1: zsh

```
→  examples git:(master) ✗ org-formation update organization.yml --profile org-formation
OC::ORG::ServiceControlPolicy | RestrictUnusedRegionsPolicy   | Create (p-8yi9k8jd)
INFO: done
→  examples git:(master) ✗
```

13. Create change sets

```
48
49      Production1:
50        Type: OC::ORG::Account
51        Properties:
52          RootEmail: production1@olafconijn.awsapps.com      You, a few seconds ago • Uncommitted changes
53          AccountName: Production 1 Account
54          Alias: my-production1
55          PasswordPolicy: !Ref PasswordPolicy
56          ServiceControlPolicies:
57            - !Ref RestrictUnusedRegionsPolicy
58          Tags:
59            budget-alarm-threshold: '100'
60            account-owner-email: olaf@email.com
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL 1: zsh

```
→  examples git:(master) ✗ org-formation create-change-set organization.yml --profile org-formation
{
  "changeSetName": "1b3620de-fef8-4154-9651-b759d1e6d0af",
  "changes": [
    {
      "logicalId": "Production1",
      "type": "OC::ORG::Account",
      "action": "Update"
    }
  ]
```

14. Apply change sets

```
48
49      Production1:
50        Type: OC::ORG::Account
51        Properties:
52          RootEmail: production1@olafconijn.awsapps.com
53          AccountName: Production 1 Account
54          Alias: my-production1
55          PasswordPolicy: !Ref PasswordPolicy
56          ServiceControlPolicies:
57            - !Ref RestrictUnusedRegionsPolicy
58          Tags:
59            budget-alarm-threshold: '100'
60            account-owner-email: olaf@email.com
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL 1: zsh

```
➜  AwsOrganizationFormation git:(master) ✗ org-formation execute-change-set 1b3620de-fef8-4154-9651-b759d1e6d0af --
e org-formation

OC::ORG::Account                | Production1                    | Update
OC::ORG::Account                | Production1                    | CommitHash
➜  AwsOrganizationFormation git:(master) ✗
➜  AwsOrganizationFormation git:(master) ✗
```

15. Generate template in CLI

```
    RootEmail: production1@olafconijn.awsapps.com
    Alias: my-production1
    Tags:
      budget-alarm-threshold: '100'
      account-owner-email: olaf@email.com

  SharedUsersAccount:
    Type: OC::ORG::Account
    Properties:
      AccountName: Shared Users Account
      AccountId: '998174572440'
      RootEmail: users-2@olafconijn.awsapps.com
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL 1: zsh

```
➜  examples git:(master) ✗ org-formation init ./organization.yml --region eu-central-1 --profile org-formation
➜  examples git:(master) ✗
```

Managing resources

1. Apply templates to multiple accounts/regions

```
  # default region(s) for bindings.
  DefaultOrganizationBindingRegion: eu-central-1

  # default account binding
  DefaultOrganizationBinding:
    Account:
    - !Ref SharedServicesAccount
    - !Ref SharedUsersAccount

> Parameters: ...

> OrganizationBindings: ...
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL 1: zsh

```
→  examples git:(master) ✗ org-formation update-stacks ./roles.yml \
--stack-name example-roles \
--profile org-formation

INFO: stack example-roles successfully updated in 998174572440/eu-central-1.
INFO: stack example-roles successfully updated in 516455415878/eu-central-1.
INFO: done
→  examples git:(master) ✗
→  examples git:(master) ✗
```

2. Use YAML Substitutions

```
  # default region(s) for bindings.
  DefaultOrganizationBindingRegion: eu-central-1

  # default account binding
  DefaultOrganizationBinding:
    Account:
    - !Ref SharedServicesAccount
    - !Ref SharedUsersAccount

> Parameters: ...

> OrganizationBindings: ...
```

TODO

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL 1: zsh

```
➜  examples git:(master) ✗ org-formation update-stacks ./roles.yml \
--stack-name example-roles \
--profile org-formation

INFO: stack example-roles successfully updated in 998174572440/eu-central-1.
INFO: stack example-roles successfully updated in 516455415878/eu-central-1.
INFO: done
➜  examples git:(master) ✗
➜  examples git:(master) ✗
```

3. Specify default Binding (Accounts/Regions)

```
  # default region(s) for bindings.
  DefaultOrganizationBindingRegion: eu-central-1

  # default account binding
  DefaultOrganizationBinding:
    Account:
    - !Ref SharedServicesAccount
    - !Ref SharedUsersAccount

> Parameters: …

> OrganizationBindings: …
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL 1: zsh

```
➜  examples git:(master) ✗ org-formation update-stacks ./roles.yml \
--stack-name example-roles \
--profile org-formation

INFO: stack example-roles successfully updated in 998174572440/eu-central-1.
INFO: stack example-roles successfully updated in 516455415878/eu-central-1.
INFO: done
➜  examples git:(master) ✗
➜  examples git:(master) ✗
```

4. Specify Binding per Resource

```
31
32      CloudTrailS3Bucket:
33        OrganizationBinding:
34          Region: eu-central-1
35          Account: !Ref SharedComplianceAccount
36        DeletionPolicy: Retain
37        Type: AWS::S3::Bucket
38        Properties:
39          BucketName: !Sub 'cloudtrail-${SharedComplianceAccount}'
40
41      CloudTrailLogGroup:
42        OrganizationBinding:
43          Region: eu-central-1
44          Account: '*'
45          IncludeMasterAccount: true
46        Type: 'AWS::Logs::LogGroup'
47        Properties:
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL 1: zsh

```
➜  examples git:(master) ✗ org-formation update-stacks ./cloudtrail.yml \
--stack-name cloudtrail \
--profile org-formation
INFO: stack cloudtrail successfully updated in 295223382687/eu-central-1
```

5. Specify named Bindings

```yaml
Organization: !Include ./organization.yml

OrganizationBindings:
  CloudTrailBucketBinding:
    Region: eu-central-1
    Account: !Ref SharedComplianceAccount

  CloudTrailAccountsBinding:
    Region: eu-central-1
    Account: '*'
    IncludeMasterAccount: true

Resources:

  CloudTrailS3Bucket:
    OrganizationBinding: !Ref CloudTrailBucketBinding
    DeletionPolicy: Retain
    Type: AWS::S3::Bucket
    Properties:
```


PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL 1: zsh

6. Specify list of Accounts in binding

```
6   # default region(s) for bindings.
7   DefaultOrganizationBindingRegion: eu-central-1
8
9   # default account binding
10  DefaultOrganizationBinding:
11    Account:
12    - !Ref SharedServicesAccount
13    - !Ref SharedUsersAccount
14
15  > Parameters: ...
24
25  > OrganizationBindings: ...
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL 1: zsh

```
➜  examples git:(master) ✗ org-formation update-stacks ./roles.yml \
--stack-name example-roles \
--profile org-formation

INFO: stack example-roles successfully updated in 998174572440/eu-central-1.
INFO: stack example-roles successfully updated in 516455415878/eu-central-1.
INFO: done
➜  examples git:(master) ✗
➜  examples git:(master) ✗
```

7. Specify Accounts of OU in Binding

```
4       Olaf Conijn, 4 months ago • added temp to git
5   OrganizationBindings:
6     CloudTrailBucketBinding:
7       Region: eu-central-1
8       Account: !Ref SharedComplianceAccount
9
10    CloudTrailAccountsBinding:
11      Region: eu-central-1
12      OrganizationalUnit: !Ref SharedOU
13
14  Resources:
15
16    CloudTrailS3Bucket:
17      OrganizationBinding: !Ref CloudTrailBucketBinding
18      DeletionPolicy: Retain
19      Type: AWS::S3::Bucket
20      Properties:
21        BucketName: !Sub 'cloudtrail-${SharedComplianceAccount}'
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL 1: zsh

```
→  examples git:(master) ✗ org-formation update-stacks ./cloudtrail.yml \
--stack-name cloudtrail \
```

8. Specify Accounts with Tag in Binding

```
10
11  > Parameters: ⋯
16
17    Resources:
18
19      Budget:
20        Type: AWS::Budgets::Budget
21        OrganizationBinding:
22          AccountsWithTag: budget-alarm-threshold
23        Properties:
24          Budget:       Olaf Conijn, 4 months ago • added temp to git
25            BudgetName: !Sub '${resourcePrefix}-budget-${AWSAccount.Alias}'
26            BudgetLimit:
27              Amount: !GetAtt AWSAccount.Tags.budget-alarm-threshold
28              Unit: USD
29            TimeUnit: MONTHLY
30            BudgetType: COST
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL 1: zsh

```
➜  examples git:(master) ✗ org-formation update-stacks ./budget-alarms.yml \
> --stack-name budget-alarms \
> --profile org-formation
INFO: stack budget-alarms successfully updated in 507468909204/eu-central-1.
```

9. Exclude Accounts from Binding

```
16
17  Resources:      Olaf Conijn, 4 months ago • added temp to git
18
19    Budget:
20      Type: AWS::Budgets::Budget
21      OrganizationBinding:
22        AccountsWithTag: budget-alarm-threshold
23        ExcludeAccount:
24        - !Ref MasterAccount
25      Properties:
26        Budget:
27          BudgetName: !Sub '${resourcePrefix}-budget-${AWSAccount.Alias}'
28          BudgetLimit:
29            Amount: !GetAtt AWSAccount.Tags.budget-alarm-threshold
30            Unit: USD
31          TimeUnit: MONTHLY
32          BudgetType: COST
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL 1: zsh

```
INFO: done
➜  examples git:(master) ✗ org-formation update-stacks ./budget-alarms.yml \
--stack-name budget-alarms \
--profile org-formation
```

10. Always explicitly include Master Account

```
    Region: eu-central-1
    Account: !Ref SharedComplianceAccount

  CloudTrailAccountsBinding:
    Region: eu-central-1
    OrganizationalUnit: !Ref SharedOU
    IncludeMasterAccount: true

Resources:

  CloudTrailS3Bucket:
    OrganizationBinding: !Ref CloudTrailBucketBinding
    DeletionPolicy: Retain
    Type: AWS::S3::Bucket
    Properties:
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL 1: zsh

```
INFO: done
➜  examples git:(master) ✗ org-formation update-stacks ./cloudtrail.yml \
--stack-name cloudtrail \
--profile org-formation
INFO: stack cloudtrail successfully updated in 295223382687/eu-central-1.
```

11. Use any CloudFormation syntax

```
40      Type: AWS::Route53::RecordSet
41      OrganizationBinding:
42        Region: eu-west-1
43        IncludeMasterAccount: true
44      ForeachAccount:
45        AccountsWithTag: 'subdomain'
46      Properties:
47        Type: NS
48        HostedZoneName: !Sub '${rootHostedZoneName}.'
49        Name: !Sub '${CurrentAccount.Tags.subdomain}.${rootHostedZoneName}.'
50        TTL: 86400
51        ResourceRecords: !GetAtt MasterAccount.Resources.HostedZone.NameServers
52
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL 1: zsh

```
➜  examples git:(master) ✗ org-formation update-stacks ./guardduty.yml \
--stack-name guardduty \
--profile org-formation
ERROR: circular dependency on stack guardduty for targets 516455415878/eu-central-1, 295223382687/eu-central-1, 507
204/eu-central-1, 998174572440/eu-central-1
➜  examples git:(master) ✗
```

12. Use !Ref, !GetAtt, !Sub across accounts/regions

```yaml
    DeletionPolicy: Retain
    Type: AWS::S3::Bucket
    Properties:
      BucketName: !Sub 'cloudtrail-${SharedComplianceAccount}'

  CloudTrail:
    OrganizationBinding: !Ref CloudTrailAccountsBinding
    Type: AWS::CloudTrail::Trail
    DependsOn: …
    Properties:
      S3BucketName: !Ref CloudTrailS3Bucket
      IsLogging: false
      IncludeGlobalServiceEvents: true
```

```yaml
Outputs:
  cloudtrailDashCloudTrailS3Bucket:
    Value:
      Ref: CloudTrailS3Bucket
    Description: Cross Account dependency
    Export:
      Name: cloudtrail-CloudTrailS3Bucket
```

```yaml
Parameters:
  CloudTrailS3Bucket:
    Description: Cross Account dependency
    Type: String
    ExportAccountId: '295223382687'
    ExportRegion: eu-central-1
    ExportName: cloudtrail-CloudTrailS3Bucket
```

13. Create references to List<string>

```
116
117       OrganizationBinding:
118         Region: eu-west-1
119         IncludeMasterAccount: true
120       Properties:
121         Type: NS
122         HostedZoneId: !Ref RootHostedZone
123         Name: !Sub 'data-dev.${hostedZoneName}.'
124         TTL: 86400
125         ResourceRecords: !GetAtt OtherHostedZone.NameServers
126
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL 1: zsh

```
Outputs:
  hostedzoneDashOtherHostedZoneDashNameServers:
    Value:
      Fn::Join:
      - ", "
      - Fn::GetAtt:
        - OtherHostedZone
        - NameServers
    Description: Cross Account dependency
```

```
trail.yml \
```

```
Parameters:
  OtherHostedZoneDotNameServers:
    Description: Cross Account dependency
    Type: CommaDelimitedList
    ExportAccountId: '516455415878'
    ExportRegion: eu-west-1
    ExportName: hostedzone-OtherHostedZone-NameSer
```

14. Create references to Resource with Cond.

```
192     Type: AWS::SecretsManager::Secret
193     Condition: createPrd
194     Properties:
195       Name: !Sub '${orgPrefix}-secrets-${serviceName}-prd/${secretName}'
196       KmsKeyId: !Ref prdKmsKeySecurityAccount
197
198   PrdSecretResourcePolicy:
199     Type: AWS::SecretsManager::ResourcePolicy
200     Condition: createPrd
201     Properties:
202       SecretId: !Ref PrdSecret
203 >     ResourcePolicy: …
213
214   PrdSecretAccessPolicy:
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL 1: zsh

```
→  examples git:(master) ✗ org-formation update-stacks ./cloudtrail.yml \
--stack-name cloudtrail \
--profile org-formation
INFO: stack cloudtrail successfully updated in 295223382687/eu-central-1.
INFO: stack cloudtrail successfully updated in 507468909204/eu-central-1.
INFO: stack cloudtrail successfully updated in 516455415878/eu-central-1.
INFO: stack cloudtrail successfully updated in 998174572440/eu-central-1.
INFO: done
```

16. Create references manually

```
30    createPrd:
31      Type: String
32      AllowedValues: [ true, false ]
33
34    dtaKmsKeySecurityAccount:
35      Type: String
36      ExportName: my-secrets-kms-keys-dta-kms-key-arn
37      ExportAccountId: !Ref SecurityAccount
38      ExportRegion: eu-central-1
39
40    prdKmsKeySecurityAccount:
41      Type: String
42      ExportName: my-secrets-kms-keys-prd-kms-key-arn
43      ExportAccountId: !Ref SecurityAccount
44      ExportRegion: eu-central-1
45
46
47  Conditions:
48
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL 1: zsh

17. Specify dependency on Account explicitly

```
      OrganizationBinding:
        Account: '*'
        IncludeMasterAccount: true
    Properties:
      Enable: 'true'
  Master:
    DependsOnAccount: !Ref MasterAccount
    Type: AWS::GuardDuty::Master
    OrganizationBinding:
      Account: '*'
    Properties:
      DetectorId: !Ref Detector
      MasterId: !Ref MasterAccount
  Member:
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL 1: zsh

```
→  examples git:(master) ✗ org-formation update-stacks ./cloudtrail.yml \
--stack-name cloudtrail \
--profile org-formation
INFO: stack cloudtrail successfully updated in 295223382687/eu-central-1.
INFO: stack cloudtrail successfully updated in 507468909204/eu-central-1.
INFO: stack cloudtrail successfully updated in 516455415878/eu-central-1.
INFO: stack cloudtrail successfully updated in 998174572440/eu-central-1.
INFO: done
```

18. Check for circular dependencies

```
      Type: AWS::GuardDuty::Detector
      DependsOnAccount: !Ref SharedUsersAccount
      OrganizationBinding:
        Account: '*'
        ExcludeAccount: !Ref SharedUsersAccount
        IncludeMasterAccount: true
      Properties:      Olaf Conijn, 2 months ago • added bunch of testcases on template. added support fo
        Enable: 'true'
    Master:
      DependsOnAccount: !Ref MasterAccount
      Type: AWS::GuardDuty::Master
      OrganizationBinding:
        Account: '*'
      Properties:
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL 1: zsh

```
→  examples git:(master) ✗ org-formation update-stacks ./guardduty.yml \
--stack-name guardduty \
--profile org-formation
ERROR: circular dependency on stack guardduty for targets 516455415878/eu-central-1, 295223382687/eu-central-1, 507
204/eu-central-1, 998174572440/eu-central-1
→  examples git:(master) ✗
```

19. Reference Resources from specific Account

```
    Type: AWS::Route53::RecordSet
    OrganizationBinding:
      Region: eu-west-1
      IncludeMasterAccount: true
    ForeachAccount:
      AccountsWithTag: 'subdomain'
    Properties:
      Type: NS
      HostedZoneName: !Sub '${rootHostedZoneName}.'
      Name: !Sub '${CurrentAccount.Tags.subdomain}.${rootHostedZoneName}.'
      TTL: 86400
      ResourceRecords: !GetAtt MasterAccount.Resources.HostedZone.NameServers

```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL 1: zsh

```
➜  examples git:(master) ✗ org-formation update-stacks ./guardduty.yml \
--stack-name guardduty \
--profile org-formation
ERROR: circular dependency on stack guardduty for targets 516455415878/eu-central-1, 295223382687/eu-central-1, 507
204/eu-central-1, 998174572440/eu-central-1
➜  examples git:(master) ✗
```

20. Reference AccountId by logical name

```
53  CloudTrailLogGroupRole: …
80
81    CloudTrailS3Bucket:
82      OrganizationBinding: !Ref CloudTrailBucketBinding
83      DeletionPolicy: Retain
84      Type: AWS::S3::Bucket
85      Properties:
86        BucketName: !Sub
87        - 'cloudtrail-${accountId}'
88        - {accountId: !Ref SharedComplianceAccount}
89
90    CloudTrail:
91      OrganizationBinding: !Ref CloudTrailAccountsBinding
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL 1: zsh

```
→  examples git:(master) ✗ org-formation update-stacks ./cloudtrail.yml \
--stack-name cloudtrail \
--profile org-formation
INFO: stack cloudtrail successfully updated in 295223382687/eu-central-1.
INFO: stack cloudtrail successfully updated in 507468909204/eu-central-1.
INFO: stack cloudtrail successfully updated in 516455415878/eu-central-1.
INFO: stack cloudtrail successfully updated in 998174572440/eu-central-1.
INFO: done
```

21. Reference Account Tag, Email, etc

```
52
53  > CloudTrailLogGroupRole: …
80
81    CloudTrailS3Bucket:
82      OrganizationBinding: !Ref CloudTrailBucketBinding
83      DeletionPolicy: Retain
84      Type: AWS::S3::Bucket
85      Properties:
86        BucketName: !Sub
87        - 'cloudtrail-${accountAlias}'
88        - {accountAlias: !GetAtt SharedComplianceAccount.Alias}
89
90    CloudTrail:      Olaf Conijn, 4 months ago • added temp to git
91      OrganizationBinding: !Ref CloudTrailAccountsBinding
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL 1: node

```
→  examples git:(master) ✗ org-formation update-stacks ./cloudtrail.yml \
--stack-name cloudtrail \
--profile org-formation
```

22. Element for each Account in binding

```yaml
    Properties:
      DetectorId: !Ref Detector
      MasterId: !Ref MasterAccount
  Member:
    Type: AWS::GuardDuty::Member
    OrganizationBinding:
      IncludeMasterAccount: true
    ForeachAccount:
      Account: '*'
    Properties:
      DetectorId: !Ref Detector
      Email: !GetAtt CurrentAccount.RootEmail
      MemberId: !Ref CurrentAccount
      Status: Invited
      DisableEmailNotification: true
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL

```
--profile org-formation
INFO: template for stack cloudtrail account 5164554158
INFO: template for stack cloudtrail account 5074689092
INFO: template for stack cloudtrail account 9981745724
INFO: template for stack cloudtrail account 2952233826
```

```yaml
    DetectorId:
      Ref: Detector
    Email: users-2@olafconijn.awsapps.com
    MemberId: '998174572440'
    Status: Invited
    DisableEmailNotification: true
MemberSharedServicesAccount:
  Type: AWS::GuardDuty::Member
  Properties:
    DetectorId:
      Ref: Detector
    Email: shared-services-2@olafconijn.awsapps.com
    MemberId: '516455415878'
    Status: Invited
    DisableEmailNotification: true
MemberSharedComplianceAccount:
  Type: AWS::GuardDuty::Member
  Properties:
    DetectorId:
      Ref: Detector
    Email: shared-compliance-2@olafconijn.awsapps.com
    MemberId: '295223382687'
    Status: Invited
```

23. Create string array foreach Account

```
64  - Sid: ReadAccessBucket
65      Action:
66      - s3:Get*
67      - s3:List*
68      Effect: "Allow"
69      Resource:
70      - !Sub '${Bucket.Arn}'
71      - !Sub '${Bucket.Arn}/*'
72      Principal:      Olaf Conijn, 16 days ago • added new syntax to Fn::EnumTargetAccounts and F
73        AWS: Fn::EnumTargetAccounts ReadAccessAccountBinding arn:aws:iam::${account}:root
74    - Sid: 'Write operations on bucket' ⋯
83    - Sid: 'Any operation on bucket' ⋯
92
93  S3BucketReadAccessPolicy: ⋯
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL 1: zsh

```
→  examples git:(master) ✗
```

24. Create string array foreach Region

```
86      Properties:
87        ManagedPolicyName: !Sub '${resourcePrefix}-${secretName}-get-value-policy'
88        PolicyDocument:
89          Version: 2012-10-17
90          Statement:
91            - Effect: Allow
92              Action: secretsmanager:GetSecretValue
93              Resource: Fn::EnumTargetRegions SecretAccountBinding arn:aws:secretsmanager:${region}:${sec
94            - Effect: Allow
95              Action:
96              - kms:Decrypt
97              - kms:DescribeKey
98              Resource: !GetAtt SecretKey.Arn
99
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL 1: zsh

```
→  examples git:(master) ✗
```

25. Print resulting templates

```
→  examples git:(master) ✗ org-formation print-stacks ./cloudtrail.yml \
--stack-name cloudtrail \
--profile org-formation
template for account 295223382687 and region eu-central-1
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Parameters": {},
  "Resources": {
    "CloudTrailS3BucketPolicy": {
      "Type": "AWS::S3::BucketPolicy",
      "DependsOn": "CloudTrailS3Bucket",
      "Properties": {
        "Bucket": {
          "Ref": "CloudTrailS3Bucket"
        },
        "PolicyDocument": {
          "Version": "2012-10-17",
          "Statement": [
            {
              "Sid": "AWSCloudTrailAclCheck",
              "Effect": "Allow",
              "Principal": {
                "Service": "cloudtrail.amazonaws.com"
              },
              "Action": "s3:GetBucketAcl",
              "Resource": {
                "Fn::Sub": "arn:aws:s3:::${CloudTrailS3Bucket}"
```

26. Validate resulting templates (cfn validate)

```
87        ManagedPolicyName: !Sub '${resourcePrefix}-${secretName}-get-value-policy'
88        PolicyDocument:
89          Version: 2012-10-17
90          Statement:
91            - Effect: Allow
92              Action: secretsmanager:GetSecretValue
93              Resource: Fn::EnumTargetRegions SecretAccountBinding arn:aws:secretsmanager:${region}:${sec
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL 1: zsh

```
            "CloudTrailLogGroupRole",
            "Arn"
          ]
        }
      }
    }
  },
  "Outputs": {}
}
➜  examples git:(master) ✗ org-formation validate-stacks ./cloudtrail.yml \
--stack-name cloudtrail \
--profile org-formation
INFO: template for stack cloudtrail account 516455415878/eu-central-1 valid.
INFO: template for stack cloudtrail account 507468909204/eu-central-1 valid.
INFO: template for stack cloudtrail account 998174572440/eu-central-1 valid.
INFO: template for stack cloudtrail account 295223382687/eu-central-1 valid.
```

27. Describe stacks

```
6   # default region(s) for bindings.
7   DefaultOrganizationBindingRegion: eu-central-1
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL 1: zsh

```
➜  examples git:(master) ✗ org-formation describe-stacks --stack-name example-roles --profile org-formation
{
  "example-roles": [
    {
      "accountId": "998174572440",
      "region": "eu-central-1",
      "stackName": "example-roles",
      "lastCommittedHash": "1bd54ea13234aa7540c4022fb45385d5",
      "logicalAccountId": "SharedUsersAccount",
      "terminationProtection": false
    },
    {
      "accountId": "516455415878",
      "region": "eu-central-1",
      "stackName": "example-roles",
      "lastCommittedHash": "1bd54ea13234aa7540c4022fb45385d5",
      "logicalAccountId": "SharedServicesAccount",
      "terminationProtection": false
    }
  ]
}
➜  examples git:(master) ✗
```

28. Delete stacks

```
  # default region(s) for bindings.
  DefaultOrganizationBindingRegion: eu-central-1

  # default account binding
  DefaultOrganizationBinding:
    Account:
    - !Ref SharedServicesAccount
    - !Ref SharedUsersAccount

> Parameters: …

> OrganizationBindings: …

  Resources:
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL 1: zsh

```
      "logicalAccountId": "SharedServicesAccount",
      "terminationProtection": false
    }
  ]
}
➜  examples git:(master) ✗ org-formation delete-stacks --stack-name example-roles --profile org-formation
INFO: stack example-roles successfully deleted from 516455415878/eu-central-1.
INFO: stack example-roles successfully deleted from 998174572440/eu-central-1.
```

Automation

1. Specify a list of tasks that can be executed

```
42  > CrossAccountBuckets: …
48
49  > CrossAccountSecret: …
56
57  > CrossAccountLambda: …
63
64    HostedZone:      Olaf Conijn, a month ago • added dependsOn to task runner taks
65      Type: update-stacks
66      Template: ./hosted-zone.yml
67      StackName: hosted-zone
68      StackDescription: 'Hosted Zone example template'
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL 1: zsh

```
→  examples git:(master) ✗ org-formation perform-tasks ./build-tasks.yml --profile org-formation
INFO: executing: update-organization organization.yml
INFO: organization up to date, no work to be done.
INFO: task OrganizationUpdate ran successfully
INFO: executing: update-stacks cloudformation-setup.yml cloudformation-setup
INFO: stack cloudformation-setup already up to date.
INFO: task CloudformationSetup ran successfully
INFO: executing: update-stacks roles.yml roles
INFO: stack roles already up to date.
INFO: task Roles ran successfully
INFO: executing: update-stacks budget-alarms.yml budget-alarms
INFO: stack budget-alarms already up to date.
```

2. Specify DependsOn for tasks

```
35  TemplateURL: ./cross-account.yml
36    StackName: MyBucket
37    Parameters:
38      bucketName: myBucket2      You, a few seconds ago • Uncommitted changes
39
40  CrossAccountSecret:
41    Type: update-stacks
42    Template: ./cross-account-secret.yml
43    StackName: MySecret
44    DependsOn: CrossAccountBuckets
45    Parameters:
46      secretName: mySecret
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL 1: node

```
ERROR: number failed tasks 1 exceeded tolerance for failed tasks 1
→  examples git:(master) ✗ org-formation perform-tasks ./build-tasks.yml --profile org-formation
INFO: executing: update-organization organization.yml
INFO: organization up to date, no work to be done.
INFO: task OrganizationUpdate ran successfully
INFO: executing: update-stacks cloudformation-setup.yml cloudformation-setup
INFO: stack cloudformation-setup already up to date.
INFO: task CloudformationSetup ran successfully
INFO: executing: update-stacks roles.yml roles
INFO: stack roles already up to date.
INFO: task Roles ran successfully
```

3. Specify update-organization task (required)

```
You, a few seconds ago • Uncommitted changes
  OrganizationUpdate:
    Type: update-organization
    Template: ./organization.yml

> CloudformationSetup: ...

> Roles: ...
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL 1: zsh

```
INFO: stack cloudformation-setup successfully updated in 295223382687/eu-central-1.
INFO: stack cloudformation-setup successfully updated in 516455415878/eu-central-1.
INFO: stack cloudformation-setup successfully updated in 998174572440/eu-central-1.
INFO: done
INFO: task CloudformationSetup ran successfully
INFO: executing: update-stacks roles.yml roles
INFO: stack roles successfully updated in 295223382687/eu-central-1.
INFO: stack roles successfully updated in 516455415878/eu-central-1.
```

4. Specify update-stacks task (org-formation)

```
57  > CrossAccountLambda: ...
63
64    HostedZone:
65      Type: update-stacks
66      Template: ./hosted-zone.yml
67      StackName: hosted-zone
68      StackDescription: 'Hosted Zone example template'
69
70    CloudTrail:
71      Type: update-stacks
72      Template: ./cloudtrail.yml
73      StackName: cloudtrail
74      StackDescription: 'Cloudtrail example template'
75
76    # Include:
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL 1: zsh

```
➜  examples git:(master) ✗ org-formation validate-tasks ./build-tasks.yml --profile org-formation
INFO: template for stack cloudformation-setup account 998174572440/eu-central-1 valid.
INFO: template for stack cloudformation-setup account 507468909204/eu-central-1 valid.
INFO: template for stack cloudformation-setup account 516455415878/eu-central-1 valid.
INFO: template for stack cloudformation-setup account 295223382687/eu-central-1 valid.
INFO: done
```

5. Specify update-stacks task (cloudformation)

```
57  > CrossAccountLambda: ⋯
63
64    HostedZone:
65      Type: update-stacks
66      Template: ./hosted-zone.yml
67      StackName: hosted-zone
68      StackDescription: 'Hosted Zone example template'
69
70    CloudTrail:
71      Type: update-stacks
72      Template: ./cloudtrail.yml
73      StackName: cloudtrail
74      StackDescription: 'Cloudtrail example template'
75
76    # Include:
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL 1: zsh

```
➜  examples git:(master) ✗ org-formation validate-tasks ./build-tasks.yml --profile org-formation
INFO: template for stack cloudformation-setup account 998174572440/eu-central-1 valid.
INFO: template for stack cloudformation-setup account 507468909204/eu-central-1 valid.
INFO: template for stack cloudformation-setup account 516455415878/eu-central-1 valid.
INFO: template for stack cloudformation-setup account 295223382687/eu-central-1 valid.
INFO: done
```

6. Specify StackName, StackDescription in task

```
57  > CrossAccountLambda: …
63
64    HostedZone:
65      Type: update-stacks
66      Template: ./hosted-zone.yml
67      StackName: hosted-zone
68      StackDescription: 'Hosted Zone example template'
69
70    CloudTrail:
71      Type: update-stacks
72      Template: ./cloudtrail.yml
73      StackName: cloudtrail
74      StackDescription: 'Cloudtrail example template'
75
76    # Include:
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL 1: zsh

```
➜  examples git:(master) ✗ org-formation validate-tasks ./build-tasks.yml --profile org-formation
INFO: template for stack cloudformation-setup account 998174572440/eu-central-1 valid.
INFO: template for stack cloudformation-setup account 507468909204/eu-central-1 valid.
INFO: template for stack cloudformation-setup account 516455415878/eu-central-1 valid.
INFO: template for stack cloudformation-setup account 295223382687/eu-central-1 valid.
INFO: done
```

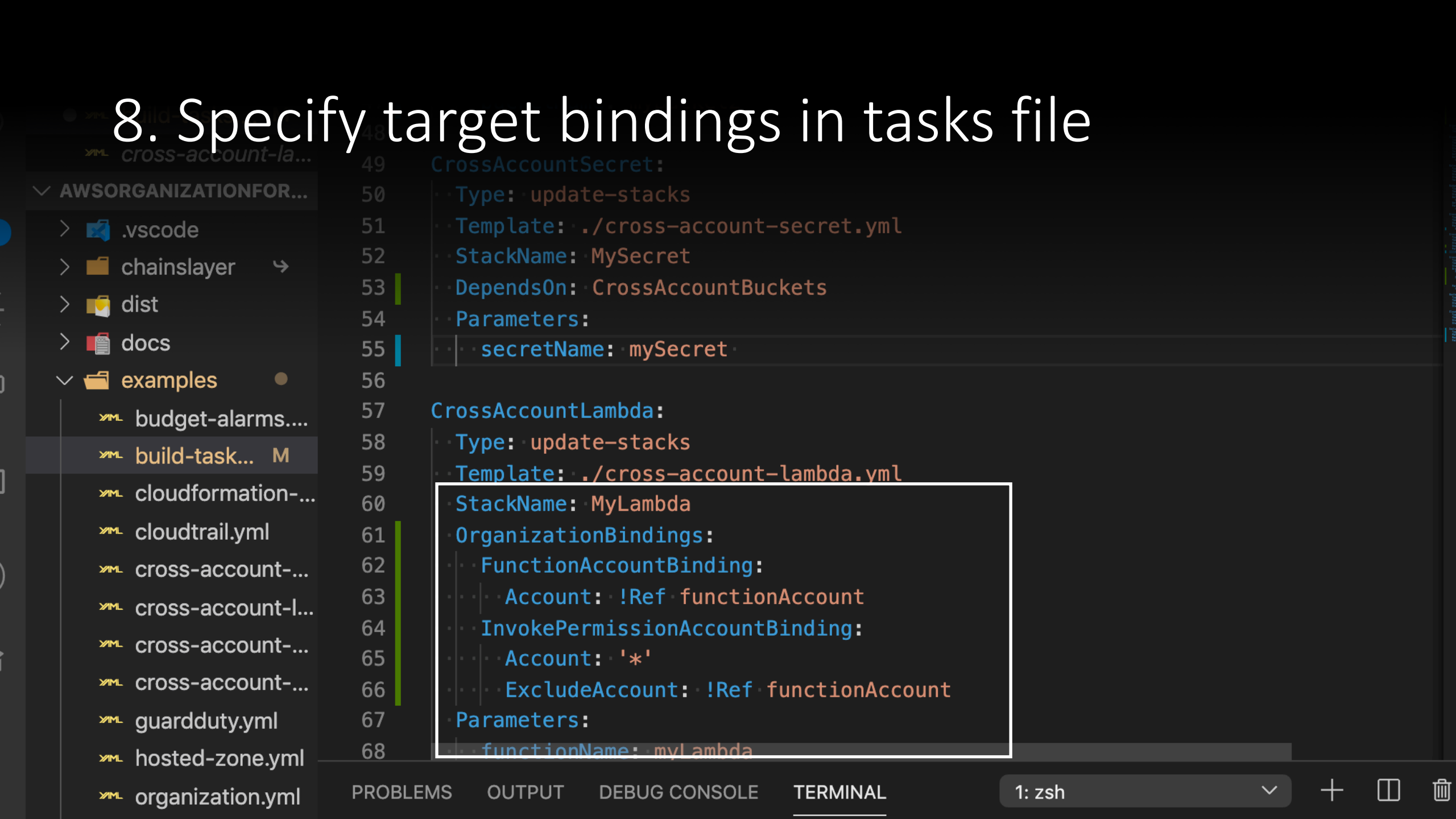
7. Specify parameters in tasks file

```
    StackName: MySecret
    DependsOn: CrossAccountBuckets
    Parameters:
      secretName: mySecret

  CrossAccountLambda:
    Type: update-stacks
    Template: ./cross-account-lambda.yml
    StackName: MyLambda
    Parameters:
      functionName: myLambda

  HostedZone:
    Type: update-stacks
    Template: ./hosted-zone.yml
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL 1: zsh

```
INFO: done
INFO: template for stack MyLambda account 998174572440/eu-central-1 valid.
INFO: template for stack MyLambda account 295223382687/eu-central-1 valid.
INFO: template for stack MyLambda account 516455415878/eu-central-1 valid.
INFO: done
INFO: template for stack hosted-zone account 516455415878/eu-west-1 valid.
```

8. Specify target bindings in tasks file



9. Enable termination protection in tasks file

12. Specify include-tasks task

```
    StackName: hosted-zone
    StackDescription: 'Hosted Zone example template'

  CloudTrail:
    Type: update-stacks
    Template: ./cloudtrail.yml
    StackName: cloudtrail
    StackDescription: 'Cloudtrail example template'

  Include:
    Type: include
    Path: ./build-tasks-include.yml
    MaxConcurrentTasks: 10
    FailedTaskTolerance: 10
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL 1: zsh

```
→  examples git:(master) ✗ org-formation validate-tasks ./build-tasks.yml --profile org-formation
INFO: template for stack cloudformation-setup account 998174572440/eu-central-1 valid.
INFO: template for stack cloudformation-setup account 507468909204/eu-central-1 valid.
INFO: template for stack cloudformation-setup account 516455415878/eu-central-1 valid.
INFO: template for stack cloudformation-setup account 295223382687/eu-central-1 valid.
INFO: done
```

13. Validate tasks file and all templates within

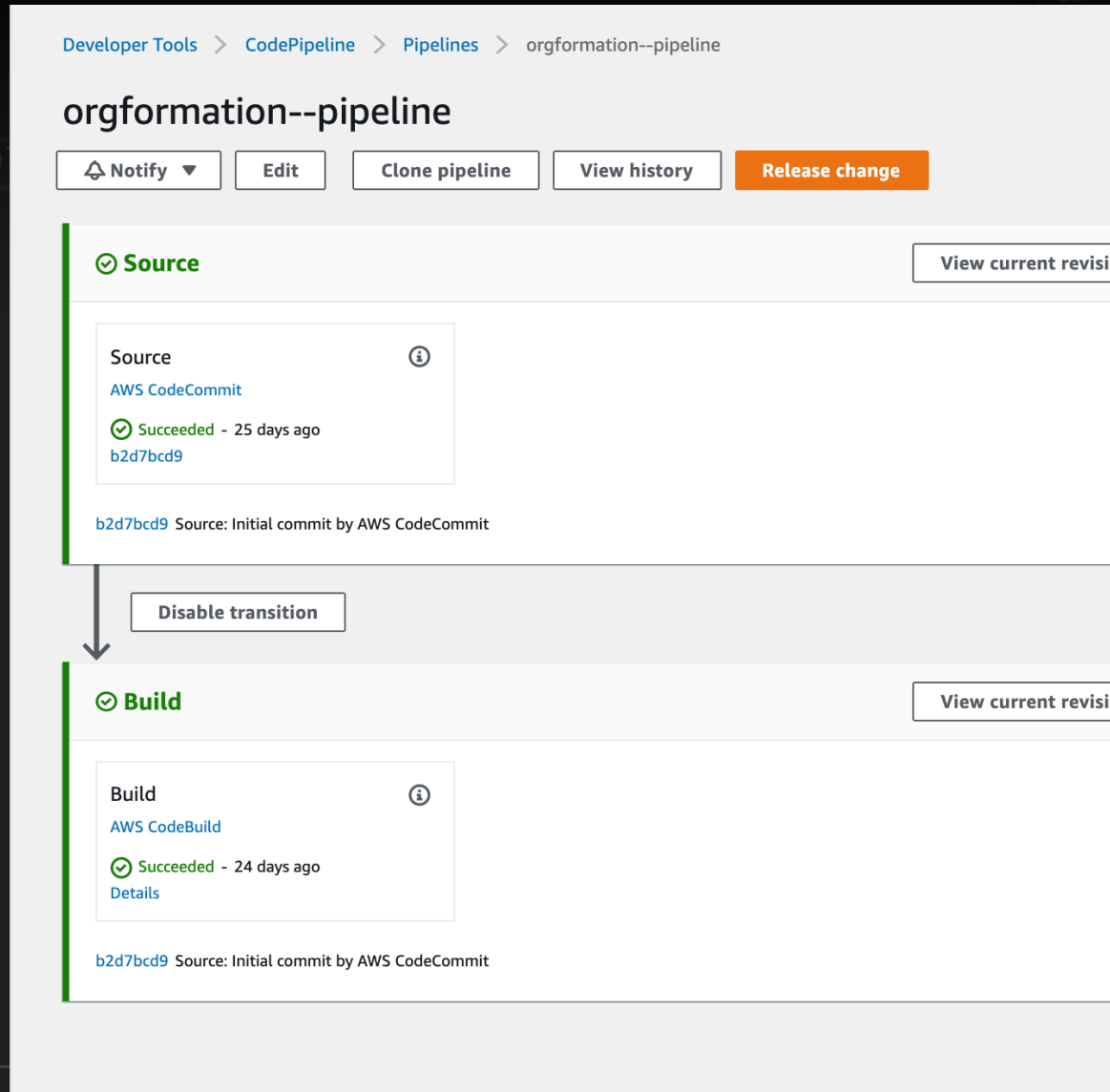
```
24
25  > Roles: ···
31
32  > BudgetAlarms: ···
41
42  > CrossAccountBuckets: ···
48
49  > CrossAccountSecret: ···
56
57  > CrossAccountLambda: ···
63
64    HostedZone:      Olaf Conijn, a month ago • added dependsOn to task runner taks
65      Type: update-stacks
66      Template: ./hosted-zone.yml
67      StackName: hosted-zone
68      StackDescription: 'Hosted Zone example template'
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL 1: node

```
→  examples git:(master) ✗ org-formation validate-tasks ./build-tasks.yml --profile org-formation
INFO: template for stack cloudformation-setup account 998174572440/eu-central-1 valid.
INFO: template for stack cloudformation-setup account 507468909204/eu-central-1 valid.
INFO: template for stack cloudformation-setup account 516455415878/eu-central-1 valid.
INFO: template for stack cloudformation-setup account 295223382687/eu-central-1 valid.
INFO: done
```

14. Generate default code commit & pipeline

```yaml
AWSTemplateFormatVersion: '2010-09-09-OC'

Organization: !Include ./organization.yml
DefaultOrganizationBindingRegion: eu-central-1

Parameters: …


OrganizationBindings:

  FunctionAccountBinding:
    Account: !Ref functionAccount

  InvokePermissionAccountBinding:
    Account: '*'
    ExcludeAccount: !Ref functionAccount


Resources:

  InvokeFunctionPolicy:
```



And then some…

And then some…

1. Every feature based on real life need
2. Gracefully handles throttling exceptions
3. Support for AWS profiles