



CloudFormation Templates in Depth

AWS CloudFormation user guide and template reference, as of 2026 | template sections, parameters and types, intrinsic functions, pseudo parameters, conditions and mappings, outputs and cross-stack exports, dynamic references, DeletionPolicy and update behaviours, quotas

CloudFormation IaC DOP-C02 DVA-C02 SAA-C03

Anatomy of a template

The sections of a template (YAML)

```
AWSTemplateFormatVersion: 2010-09-09
Description: Orders service, one stack per environment
Transform:
  - AWS::LanguageExtensions
Parameters:
  Env:
    Type: String
    AllowedValues:
      - dev
      - prod
Mappings:
  Sizing:
    dev:
      Memory: 256
    prod:
      Memory: 1024
Conditions:
  IsProd: "!Equals [!Ref Env, prod]"
Resources:
  OrdersTable:
    Type: AWS::DynamoDB::Table
    DeletionPolicy: Retain
Outputs:
  TableName:
    Value: "!Ref OrdersTable"
    Export:
      Name: "!Sub ${Env}-orders-table"
```

macros processed first (SAM, LanguageExtensions)

evaluated once per deployment from parameters

the only required section

Export makes a value importable by other stacks

Quota (as of 2026)	Value	Way around it
Resources per stack	500	nested stacks, split by lifecycle
Parameters / outputs / mappings	200 each	group into SSM parameters, fewer outputs
Template body in the API call	51 200 bytes	upload to S3: up to 1 MB with --template-url
Stacks per account and region	2 000 (raisable)	StackSets and cleanup
Logical ID	alphanumeric only, unique in the template	no dashes or underscores

Parameter declaration grammar

<LogicalName>:

Type:

<TYPE>

[Default: <VALUE>]

[AllowedValues: <LIST>]

[AllowedPattern: <REGEX>]

[NoEcho: true]

[ConstraintDescription: <TEXT>]

command

 = type exactly

literal

 = type exactly

<PLACEHOLDER>

 = you supply a value

[optional]

 = may be omitted

TYPE --- String, Number, CommaDelimitedList, List<Number>, AWS-specific (AWS::EC2::VPC::Id, AWS::EC2::KeyPair::KeyName) or AWS::SSM::Parameter::Value<String>

VALUE --- used when the caller passes nothing

LIST --- the console shows a drop-down; anything else is rejected

REGEX --- Java regex the String must match, for example [a-z0-9]+

TEXT --- error shown when a constraint fails

💡 AWS-specific and SSM parameter types

AWS::EC2::Subnet::Id validates that the subnet exists in the account and region before any resource is touched. AWS::SSM::Parameter::Value<AWS::EC2::Image::Id> with default / aws/service/ami-amazon-linux-latest/al2023-ami-kernel-default-x86_64 always resolves the latest Amazon Linux AMI at deploy time, so no AMI mapping per region is needed.

⌘ Intrinsic functions and pseudo parameters

Function (short form)	Returns	Example
!Ref	parameter value, or the resource's default ID (name, ID or ARN per type)	!Ref OrdersTable → table name
!GetAtt	a named attribute of a resource	!GetAtt OrdersTable.Arn, !GetAtt Fn.Arn
!Sub	string with \${Param}, \${Res.Attr}, \${AWS::Region} substituted	!Sub arn:\${AWS::Partition}:s3:::\${Bucket}/*
!Join / !Split / !Select	concatenate, split, pick by index	!Select [0, !GetAZs ''] → first AZ
!FindInMap	value from Mappings	!FindInMap [Sizing, !Ref Env, Memory]
!If / !Equals / !And / !Or / !Not	conditional values and conditions	!If [IsProd, 3, 1]; !Ref AWS::NoValue drops a property

<code>!ImportValue</code>	exported output of another stack (same account and region)	<code>!ImportValue prod-orders-table</code>
<code>!GetAZs / !Cidr / !Base64</code>	AZ list, CIDR blocks, base64 (user data)	<code>!Cidr [!GetAtt Vpc.CidrBlock, 6, 8]</code>
<code>Fn::ForEach,</code> <code>Fn::Length,</code> <code>Fn::ToJsonString</code>	loops and helpers (need AWS::LanguageExtensions)	one queue per name in a list parameter

Six subnets from one Fn::Cidr call

PROBLEM	A VPC has CIDR 10.0.0.0/16. The template calls <code>!Cidr [!GetAtt Vpc.CidrBlock, 6, 8]</code> and assigns subnet <code>i</code> to AZ <code>!Select [i mod 2, !GetAZs ""]</code> . Which subnets are produced and how many usable addresses does each have?
GIVEN	- count = 6 blocks, cidrBits = 8 host bits per block - prefix of each block = 32 - cidrBits - AWS reserves 5 addresses per subnet

- Prefix length**

32 - 8 = /24

Why: cidrBits is the number of host bits, not the prefix
- Blocks**

10.0.0.0/24, 10.0.1.0/24 ... 10.0.5.0/24

Why: consecutive blocks from the start of the VPC range
- Addresses per block**

2⁸ = 256 → 256 - 5 = 251 usable

Why: network, VPC router, DNS, future use, broadcast reserved
- AZ placement**

i = 0, 2, 4 → first AZ; 1, 3, 5 → second AZ

Why: Select with an index into GetAZs

ANSWER	Six /24 subnets 10.0.0.0/24 to 10.0.5.0/24, 251 usable addresses each, alternating between two AZs.
CHECK	✔ A common mistake is <code>!Cidr [..., 6, 24]</code> : that asks for 24 host bits per block, larger than the /16 VPC, and the stack fails.

AWS::NoValue — Pseudo parameter that removes a property when returned by `!If`, for example a DB snapshot identifier only in restore mode.

AWS::Partition and **AWS::URLSuffix** — `aws`, `aws-cn` or `aws-us-gov` and `amazonaws.com` or `amazonaws.com.cn`: build ARNs and endpoints that work in every partition.

🔑 Values from outside: SSM, secrets, other stacks

database.yaml (excerpt)	
1 Parameters:	
2 DbUser:	
3 Type: AWS::SSM::Parameter::Value<String>	1 SSM parameter type: value read at each deploy, versioned outside the template
4 Default: /orders/prod/db-user	
5 Resources:	
6 Db:	
7 Type: AWS::RDS::DBInstance	
8 DeletionPolicy: Snapshot	2 keep a final snapshot on delete and on replacement
9 UpdateReplacePolicy: Snapshot	
10 Properties:	
11 Engine: postgres	
12 MasterUsername: !Ref DbUser	
13 MasterUserPassword: '{{resolve:secretsmanager:prod/orders/db:SecretString:password}}'	3 dynamic reference: the password never appears in the template or console
14 VPCSecurityGroups: [!ImportValue prod-network-db-sg]	4 cross-stack import: the network stack cannot drop this export while used
15 Outputs:	
16 Endpoint:	
17 Value: !GetAtt Db.Endpoint.Address	
18 Export: {Name: !Sub '\${AWS::StackName}-db-endpoint', Value: !GetAtt Db.Endpoint.Address}	5 export names are unique per account and region

What happens to the physical resource?

Conditions	R1	R2	R3	R4	R5
Resource removed from template or stack deleted	Y	Y	Y	N	N
Property change requires replacement	--	--	--	Y	Y
Policy set	Delete	Retain	Snapshot	UpdateReplacePolicy: Delete	UpdateReplacePolicy: Retain
Actions					
Resource deleted	X		X		
Resource kept, no longer managed		X			X
Snapshot taken first			X		
New resource created, old one deleted				X	
New resource created, old one kept					X

- R1 default for most resources
R2 S3 bucket must be empty to delete anyway
R3 EBS, RDS, ElastiCache, Redshift, Neptune, DocumentDB
R4 new physical ID
R5 orphan to clean up later

Update behaviour	Meaning	Example property
No interruption	changed in place, resource keeps running	Lambda MemorySize, tags on most resources
Some interruption	changed in place with a restart or brief outage	EC2 InstanceType (stop/start, EBS-backed)
Replacement	new resource with a new physical ID, then the old one is deleted	DynamoDB KeySchema, RDS DBInstanceIdentifier, a custom BucketName

⚠ Custom names block replacement

If you set an explicit name (TableName, BucketName, FunctionName) and change a property that needs replacement, CloudFormation must create a second resource with the same name first and the update fails. Let CloudFormation generate names, or change the name in the same update.

🚩 Recap and self-test

Find the planted errors

There are 4 mistakes. They are underlined and corrected below.

The only required section is ~~Parameters~~^{Resources}. A stack holds up to ~~200~~⁵⁰⁰ resources. Exports are read with ~~Fn::GetAtt~~^{Fn::ImportValue}. Snapshot on delete needs ~~UpdatePolicy~~^{DeletionPolicy}.

Resources is the only required section
Transform runs first

Ref vs GetAtt
default ID vs a named attribute

Sub for strings, Partition for ARNs
portable templates

Secrets by dynamic reference
never as default parameters

Retain or Snapshot data
DeletionPolicy + UpdateReplacePolicy

Know what replaces
custom names block it

Q1 Which template section is mandatory?

A Resources.

Q2 What does !Ref return for an S3 bucket and for a Lambda function?

A The bucket name; the function name. Use !GetAtt X.Arn for ARNs.

Q3 Drop a property only in dev?

A !If [IsProd, value, !Ref AWS::NoValue].

Q4 Read a Secrets Manager password without exposing it?

A {{resolve:secretsmanager:name:SecretString:password}} dynamic reference.

Q5 Why can't the network stack delete an output?

A It is exported and imported by another stack; remove the import first.

Q6 Keep an RDS snapshot when an update replaces the database?

A UpdateReplacePolicy: Snapshot (DeletionPolicy covers deletion only).

Q7 Template larger than 51 200 bytes?

A Upload it to S3 and pass --template-url (up to 1 MB), or split it.

Q8 Which transform enables Fn::ForEach?

A AWS::LanguageExtensions.

Q9 Always use the latest Amazon Linux AMI without a mapping?

A Parameter of type AWS::SSM::Parameter::Value<AWS::EC2::Image::Id> pointing at the public AMI parameter.