AWS CloudFormation Best Practice

**TABLE OF CONTENTS**

[security-best-practices 1](#_Toc905685314)

[best-practices 1](#_Toc1307457945)

[Planning and organizing 1](#_Toc1183619487)

[Creating templates 1](#_Toc630369445)

[Managing stacks 1](#_Toc1248031626)

# security-best-practices

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/security-best-practices.html>

* Use IAM to control access
* Do not embed credentials in your templates  
  (side rule: DO NOT HARDCODE CUSTOMER INFORMATION IN TEMPLATES aka emails etc!)
* Use AWS CloudTrail to log AWS CloudFormation calls

# best-practices

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/best-practices.html>

## Planning and organizing

* Organize your stacks by lifecycle and ownership
* Use cross-stack references to export shared resources
* Use IAM to control access
* Reuse templates to replicate stacks in multiple environments
* Verify quotas for all resource types
* Use modules to reuse resource configurations

## Creating templates

* Do not embed credentials in your templates
* Use AWS-specific parameter types
* Use parameter constraints
* Use AWS::CloudFormation::Init to deploy software applications on Amazon EC2 instances
* Use the latest helper scripts
* Validate templates before using them

## Managing stacks

* Manage all stack resources through AWS CloudFormation
* Create change sets before updating your stacks
* Use stack policies
* Use AWS CloudTrail to log AWS CloudFormation calls
* Use code reviews and revision controls to manage your templates
* Update your Amazon EC2 Linux instances regularly