

Build it in pieces, and understand dependencies

AWS Infrastructure as Code – Deep Dive

Petri Kallberg, Sanoma CCoE

s a

n
o m

a

Build it in pieces – Cloudformation options

- Start where you have most changes
 - Building application layer for each new sw deployment (immutable infrastructure)
- Persistent data layer can be a challenge
 - You can build new db server but how do you migrate your data?
- Infrastructure as Code and manual config are not compatible
- **Build it in pieces, and understand dependencies**

Manual "copy-paste"

- No coupling. Natural dependencies between AWS resources, e.g. can not remove subnet if there are instances placed into it.
- Easy to use special parameter types like `List<AWS::EC2::Subnet::Id>`
- Easy to pick wrong parameter values. All combinations might not work (as planned).

Network configuration

VpcId vpc-072239bed36f9a13d (10.0.0.0/21) (...

VPC ID

Subnets subnet-0e6e3cfb4b854a932 (10.0.0.0/24) (sample-vpc public subnet eu-west-1a) x

Subnets

Cancel

Previous

Next

Nested stacks


- Strong coupling. Changes are automatically propagated from parent to child stacks.
- All non-default parameter value must be set in master stack.
- It is possible to update child stacks, but not recommended.
- Not possible to use special parameter types in child stacks.
- No preview for changes in child stacks.

▼ Changes

The changes CloudFormation will make if you execute this change set.

Filter			
Action	Logical ID	Physical ID	Resource Type
Modify	EC2	arn:aws:cloudformation:eu-west-1:430997289407:stack/sample-vpc-EC2-J1FI54F2U3NB/689b7790-cd5a-11e8-8c69-500c44f19ed2	AWS::CloudFormation::Stack

Update Stack ×

 Performing operations directly on a nested stack may result in an unstable state where it is out-of-sync. [Update Stack](#) to which it belongs. [Learn more](#)

Are you sure you would like to update the nested stack with the following details:

Stack name: sample-vpc-EC2-J1FI54F2U3NB

We recommend you make your updates through the root stack:

Root stack: [sample-vpc](#)

[Cancel](#) [Yes, Update](#)

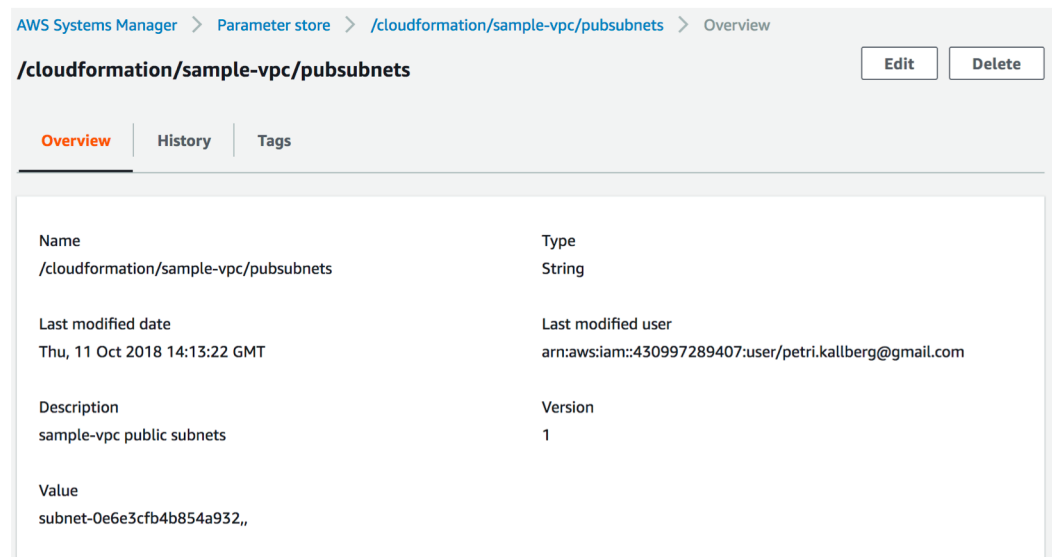
Cross stack references

- Semi-tight coupling. Exported parameters can not be changed once they are imported. This is typically found at the end of stack update and can trigger long roll-back.
- Not possible to use special parameter types.
- No parent-child –relation or automatic change propagation between stacks.
- Easy to pass correct parameter values and valid combinations (vs. manual copy-paste)

Events ▾							
Filter by: Status ▾					Search events		
2018-10-11	Status	Type	Logical ID	Status Reason			
▶ 17:01:46 UTC+0300	UPDATE_ROLLBACK_IN_PROGRESS	AWS::CloudFormation::Stack	sample-vpc	Export sample-vpc-PubSubnets cannot be updated as it is in use by sample-ec2			
▶ 17:01:42 UTC+0300	CREATE_COMPLETE	AWS::EC2::SubnetRouteTableAssociation	PubSubnetRoutingC				

SSM Parameter store

- Semi-loose coupling. Parameter store values are versioned and can be edited.
- Not possible to use special parameter types.
- No parent-child –relation or automatic change propagation between stacks.
- Easy to pass correct parameter values and valid combinations (vs. manual copy-paste)

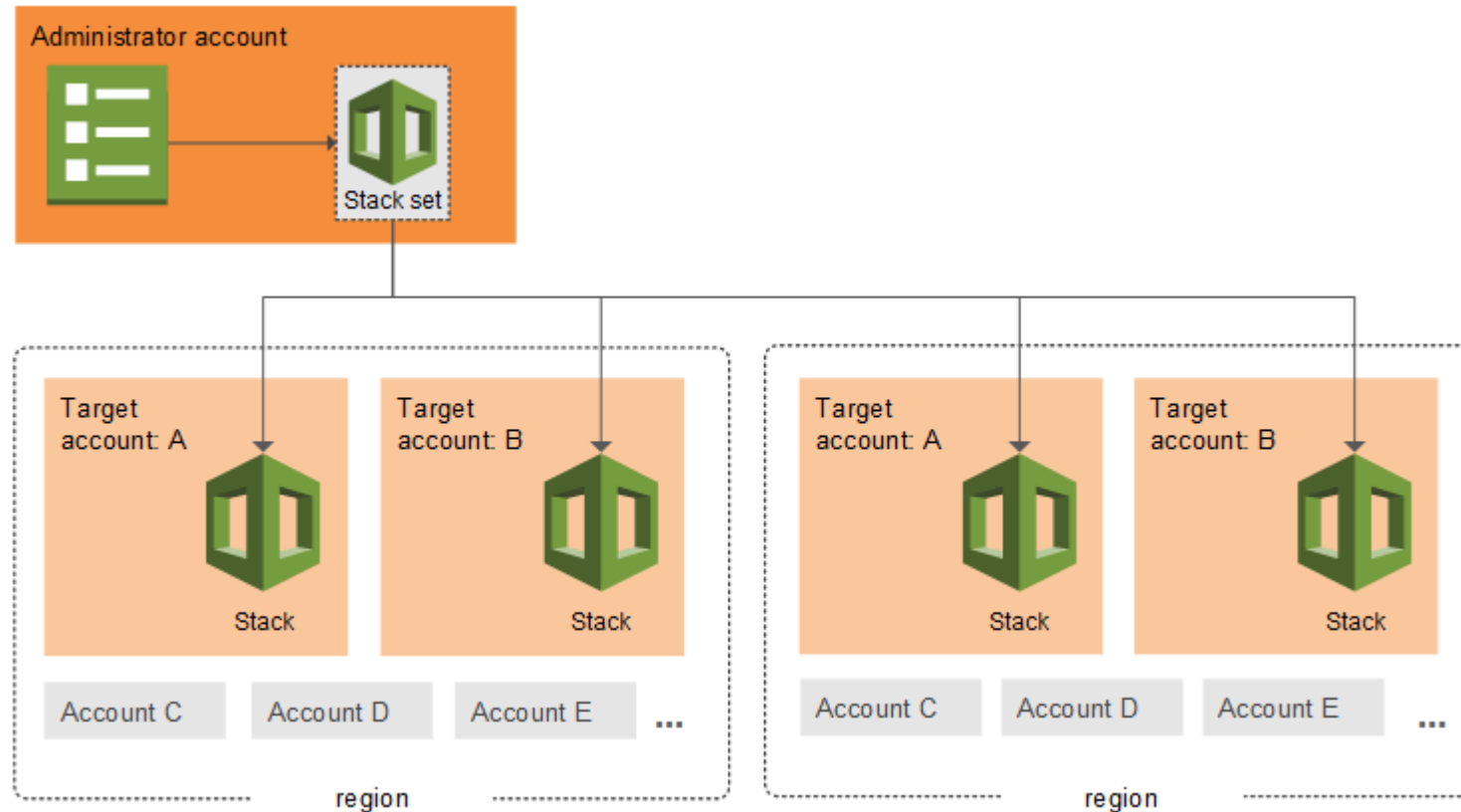


The screenshot shows the AWS Systems Manager console interface for a parameter in the SSM Parameter Store. The breadcrumb navigation at the top reads: AWS Systems Manager > Parameter store > /cloudformation/sample-vpc/pubsubnets > Overview. The parameter name is displayed as /cloudformation/sample-vpc/pubsubnets, with 'Edit' and 'Delete' buttons to its right. Below the name, there are three tabs: Overview (selected), History, and Tags. The Overview tab displays the following details:

Name	Type
/cloudformation/sample-vpc/pubsubnets	String
Last modified date	Last modified user
Thu, 11 Oct 2018 14:13:22 GMT	arn:aws:iam::430997289407:user/petri.kallberg@gmail.com
Description	Version
sample-vpc public subnets	1
Value	
subnet-0e6e3cfb4b854a932,,	

Stack sets (bonus)

- Deploy a template into multiple regions and/or accounts.
- List accounts or choose AWS Organizations unit.



Set deployment options

Configure options to deploy stacks to your accounts and regions. Stacks are deployed to regions in sequence, and the order in which stacks are deployed within regions, the maximum number of accounts in which to deploy in parallel.

Specify accounts

Identify accounts or organizational units in which you want to create stacks.

- ☒ Deploy stacks in accounts. [Learn more about required account permissions](#)

3

- ☐ Deploy stacks in AWS organizational units. [Learn more](#)

- ☐ Upload a list of valid accounts in which stacks can be deployed

Specify regions

Choose the regions in which you want to deploy stacks. Stacks are deployed in these regions in the order that you specify.

Available regions

EU (Ireland)
US West (N. California)
Asia Pacific (Singapore)
Asia Pacific (Tokyo)
US East (Ohio)
South America (Sao Paulo)
Asia Pacific (Sydney)
EU (Frankfurt)
Asia Pacific (Seoul)
Asia Pacific (Mumbai)
EU (London)
Canada (Central)

Add →

← Remove

Add all →

Deployment order

US West (Oregon)
US East (N. Virginia)