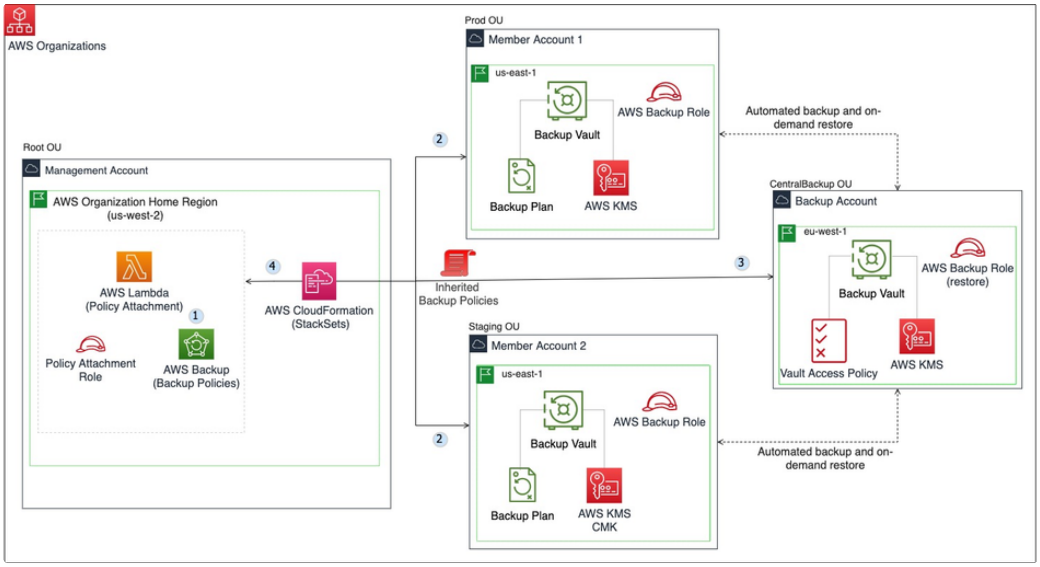
Synctree Flosports | AWS Backup

AWS Backup offers a cost-effective, fully managed, policy-based managed service that simplifies data protection at scale. AWS Backup leverages AWS Organizations to centrally automate backup policies to implement, configure, manage, and govern backup activity across supported AWS resources.

In this document, we demonstrate how you can save time using AWS CloudFormation automation to centrally automate and scale the process of implementing AWS Backup policies, backup vaults, and cross-region, cross-account replication across your multi-account AWS environment.

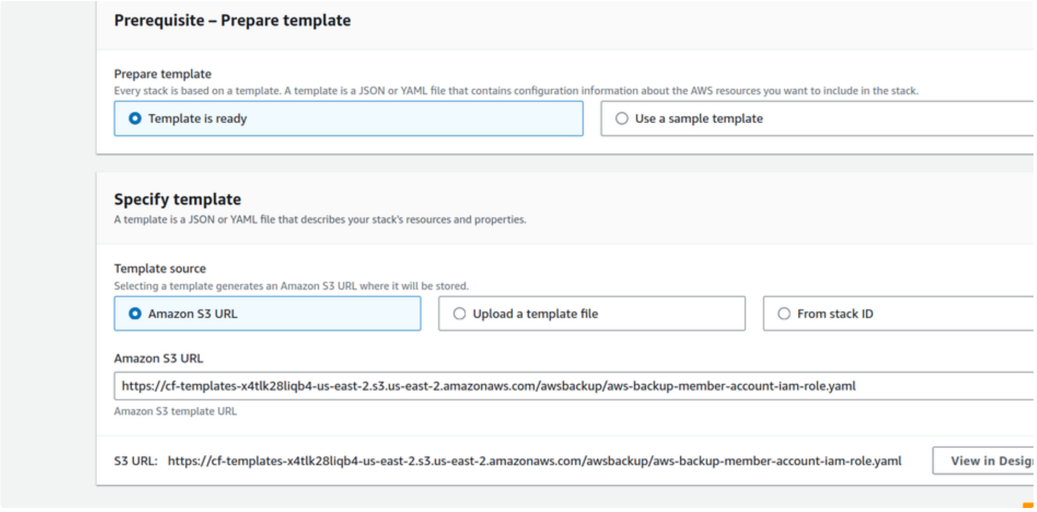


Step 1: Enable the required service in the AWS Backup service

Go to AWS Backup > Settings, and then choose Enable for Backup policies, Cross-account monitoring, and Cross-account backup.

Step 2: Deploy IAM roles across member accounts

1. Go to Cloudformation > stackset > Create stackset
2. Give the template file S3 URL and select Next.



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

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 ○ From stack ID

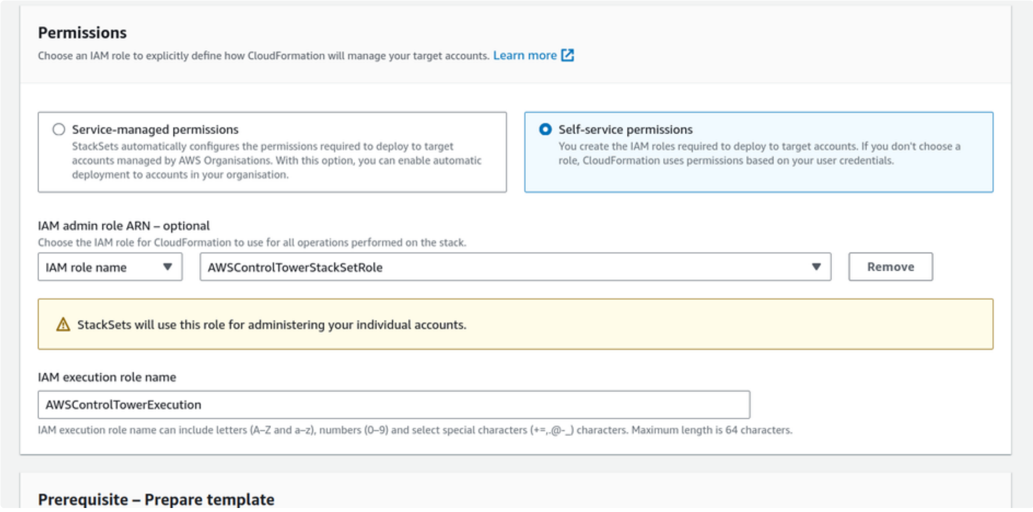
Amazon S3 URL

https://cf-templates-x4tlk28liqb4-us-east-2.s3.us-east-2.amazonaws.com/awsbackup/aws-backup-member-account-iam-role.yaml

Amazon S3 template URL

S3 URL: https://cf-templates-x4tlk28liqb4-us-east-2.s3.us-east-2.amazonaws.com/awsbackup/aws-backup-member-account-iam-role.yaml

3. Give the IAM admin role (*AWSControlTowerStackSetRole)* and IAM execution role name (*AWSControlTowerExecution)*



Permissions

Choose an IAM role to explicitly define how CloudFormation will manage your target accounts. Learn more

○ Service-managed permissions
StackSets automatically configures the permissions required to deploy to target accounts managed by AWS Organisations. With this option, you can enable automatic deployment to accounts in your organisation.

● Self-service permissions
You create the IAM roles required to deploy to target accounts. If you don't choose a role, CloudFormation uses permissions based on your user credentials.

IAM admin role ARN – optional
Choose the IAM role for CloudFormation to use for all operations performed on the stack.
IAM role name: AWSControlTowerStackSetRole

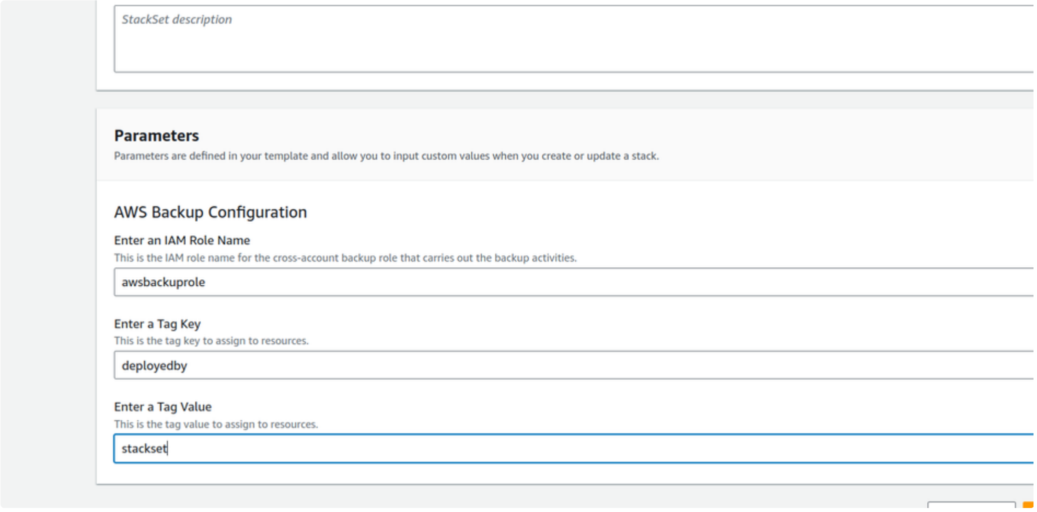
StackSets will use this role for administering your individual accounts.

IAM execution role name: AWSControlTowerExecution
IAM execution role name can include letters (A–Z and a–z), numbers (0–9) and select special characters (+=,.@-_) characters. Maximum length is 64 characters.

Prerequisite – Prepare template

4. Add all the parameters required to create CloudFormation StackSet and select Next.

- pCrossAccountBackupRole: Common role name for cross-account backup
- pTagKey1: Give the tag key
- pTagValue1: Give the tag value



StackSet description

Parameters

Parameters are defined in your template and allow you to input custom values when you create or update a stack.

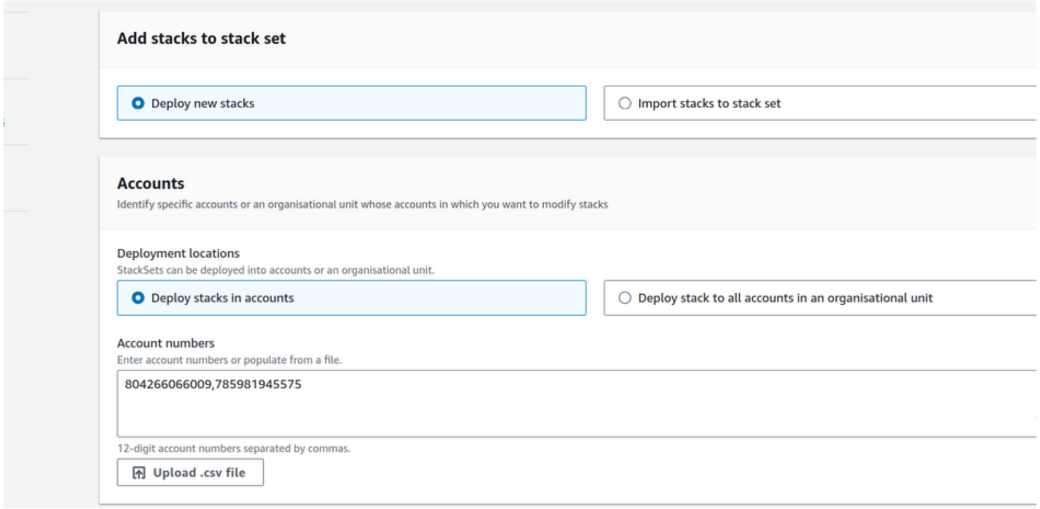
AWS Backup Configuration

Enter an IAM Role Name
This is the IAM role name for the cross-account backup role that carries out the backup activities.
awsbackuprole

Enter a Tag Key
This is the tag key to assign to resources.
deployedby

Enter a Tag Value
This is the tag value to assign to resources.
stackset

5. Set the deployment option Deploy stack in account, Give member account Ids, Specify region control tower region which is your control tower home region, and select Next.



Add stacks to stack set

● Deploy new stacks ○ Import stacks to stack set

Accounts

Identify specific accounts or an organisational unit whose accounts in which you want to modify stacks

Deployment locations

StackSets can be deployed into accounts or an organisational unit.

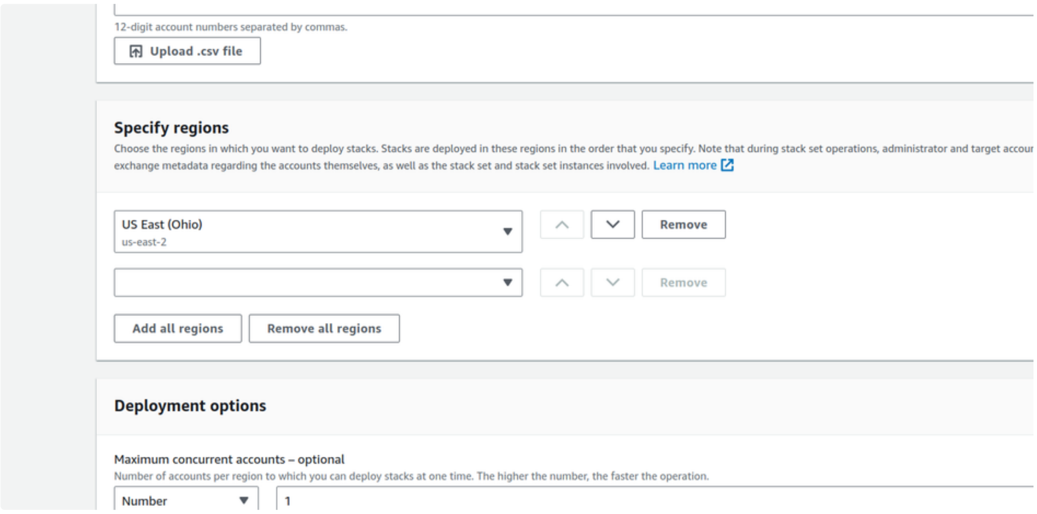
● Deploy stacks in accounts ○ Deploy stack to all accounts in an organisational unit

Account numbers

Enter account numbers or populate from a file.

804266066009,785981945575

12-digit account numbers separated by commas.



12-digit account numbers separated by commas.

Specify regions

Choose the regions in which you want to deploy stacks. Stacks are deployed in these regions in the order that you specify. Note that during stack set operations, administrator and target accour
exchange metadata regarding the accounts themselves, as well as the stack set and stack set instances involved. Learn more

US East (Ohio)
us-east-2

Deployment options

Maximum concurrent accounts – optional

Number of accounts per region to which you can deploy stacks at one time. The higher the number, the faster the operation.

Number 1

Step 3: Deploy member account resources

Deploy the following Cloudformation template using the same steps in step 2.

aws-backup-me…nt.yaml
27 Oct 2023, 04:17 pm

This stackset creates KMS keys and a Backup vault in the member accounts.

Give the following input parameters:

- pCrossAccountBackupRole: Role name that you created in step 1
- pBackupKeyAlias: Give key alias name
- pMemberBackupVaultName: Give vault name
- pOrganizationId: Organisation Id
- pTagKey1: Tag key
- pTagValue1: Tag value

Set the deployment option Deploy stack in account, Give member account IDs, Specify regions you have resources to take backup(make sure these regions are enrolled in the control tower)

Step 4: Deploy centralized backup account resources

Deploy the following Cloudformation template using the same steps in step 2.

aws-backup-ce… nt.yaml
27 Oct 2023, 04:21 pm

This stackset creates IAM role KMS keys and Backup vaults in the Centra Backup accounts which manage your backups

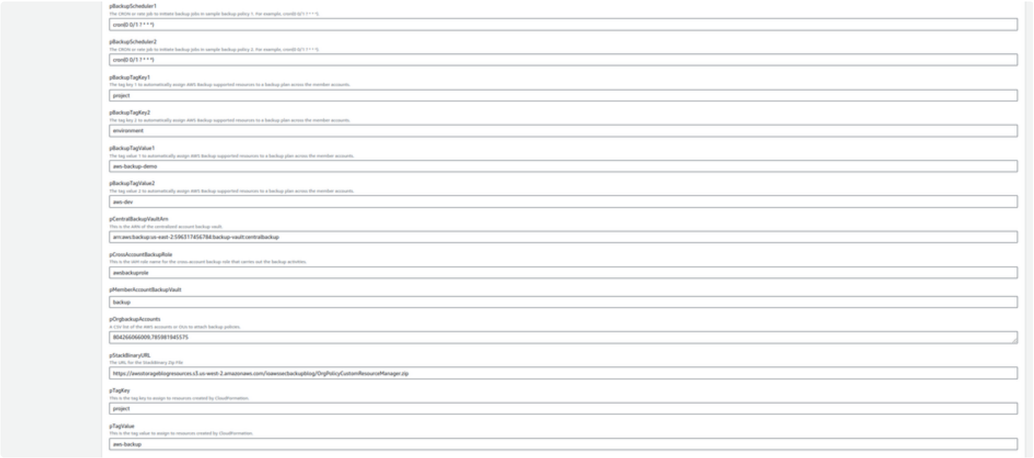
- pCrossAccountBackupRole - Give the Cross Account Backup Role name
- pBackupKeyAlias - Give key alias name
- pCentralBackupVaultName - Give vault name
- pOrganizationId: Organisation Id
- pTagKey1: Tag key
- pTagValue1: Tag value

Step 5: Deploy centralized backup account resources.

aws-backup-or… cy.yaml
27 Oct 2023, 06:09 pm

1. Go to Cloudformation>stack
2. Select create new stack
3. Give s3 template URL and select Next
4. Give all the required parameters:

- pOrgbackupAccounts: AWS accounts or OUs to attach backup policies.
- pCrossAccountBackupRole: Role name that you created in step 1
- pBackupScheduler1: The CRON or rate job to initiate backup jobs in sample backup policy 1. For example, cron(0 0/1 ? * * *).
- pBackupScheduler2: The CRON or rate job to initiate backup jobs in sample backup policy 2. For example, cron(0 0/1 ? * * *).
- pMemberAccountBackupVault: The name of the member account Backup vaults.
- pCentralBackupVaultArn: This is the ARN of the centralized account backup vault.
- pBackupTagKey1: The tag key 1 to automatically assign AWS Backup supported resources to a backup plan across the member accounts.
- pBackupTagValue1: The tag value 1 to automatically assign AWS Backup supported resources to a backup plan across the member accounts.
- pBackupTagKey2: The tag key 2 to automatically assign AWS Backup supported resources to a backup plan across the member accounts.
- pBackupTagValue2: The tag value 2 to automatically assign AWS Backup supported resources to a backup plan across the member accounts.
- pTagKey: This is the tag key to assign to resources created by CloudFormation.
- pTagValue: This is the tag value to assign to resources created by CloudFormation.
- pStackBinaryURL: 'https://awsstorageblogresources.s3.us-west-2.amazonaws.com/ioawssecbackupblog/OrgPolicyCustomResourceManager.zip'



pBackupSchedular1
The CRON or rate job to initiate backup jobs in sample backup policy 1. For example, cron(0 0/1 ? * * *).
cron(0 0/1 ? * * *)

pBackupSchedular2
The CRON or rate job to initiate backup jobs in sample backup policy 2. For example, cron(0 0/1 ? * * *).
cron(0 0/1 ? * * *)

pBackupTagKey1
The tag key 1 to automatically assign AWS Backup supported resources to a backup plan across the member accounts.
project

pBackupTagKey2
The tag key 2 to automatically assign AWS Backup supported resources to a backup plan across the member accounts.
environment

pBackupTagValue1
The tag value 1 to automatically assign AWS Backup supported resources to a backup plan across the member accounts.
aws-backup-demo

pBackupTagValue2
The tag value 2 to automatically assign AWS Backup supported resources to a backup plan across the member accounts.
aws-dev

pCentralBackupVaultArn
This is the ARN of the centralized account backup vault.
arn:aws:backup:us-east-2:596317456784:backup-vault:centralbackup

pCrossAccountBackupRole
This is the IAM role name for the cross-account backup role that carries out the backup activities.
awsbackuprole

pMemberAccountBackupVault
backup

pOrgbackupAccounts
A CSV list of the AWS accounts or OUs to attach backup policies.
804266066009,785981845575

pStackBinaryURL
The URL for the StackBinary Zip File
https://awsstorageblogresources.s3.us-west-2.amazonaws.com/ioawssecbackupblog/OrgPolicyCustomResourceManager.zip

pTagKey
This is the tag key to assign to resources created by CloudFormation.
project

pTagValue
This is the tag value to assign to resources created by CloudFormation.
aws-backup

5. Review and create stack

This stack creates a backup policy, lambda function, etc. This lambda function attaches a backup policy to member account

References

- Automate centralized backup at scale across AWS services using AWS Backup | Amazon Web Services
- File: aws-backup-org-policy.yaml