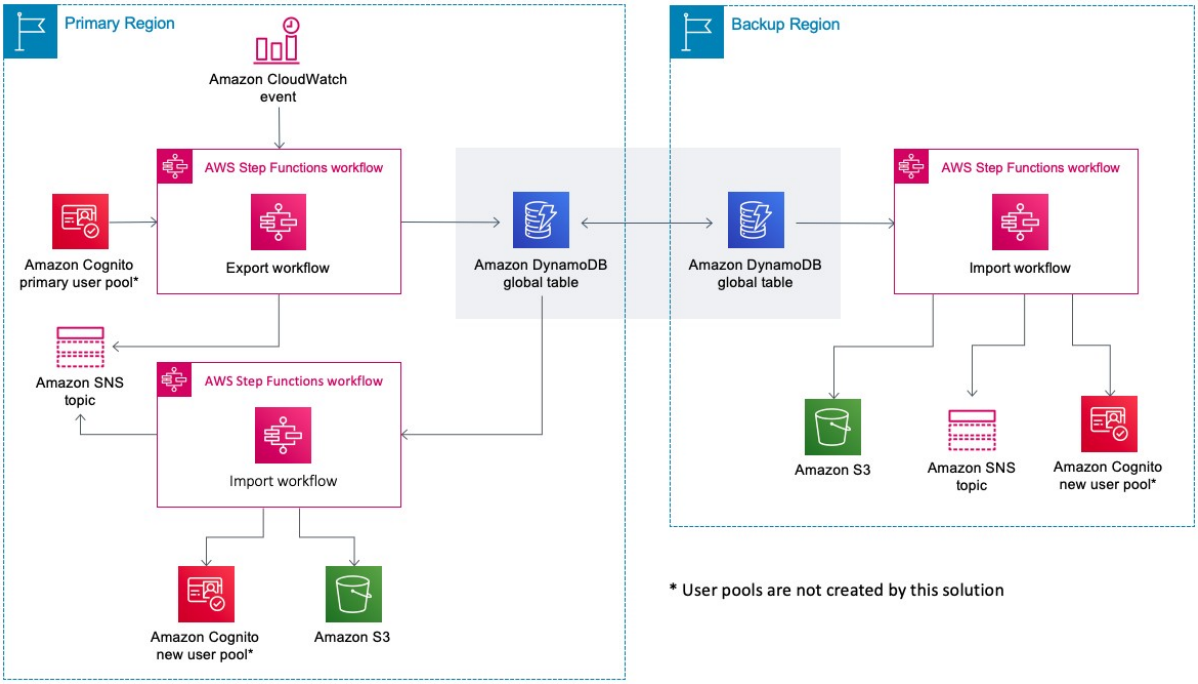
AWS Cognito cross region backup

There is no built-in cross region replication for AWS Cognito. However AWS provided a solution in form of CloudFormation template to replicate some of the users data to another region with help of DynamoDB global table.



Cost

Approximate cost equals $90.00 per month for a user pool of 500,000 users (where each user is a member of one group) and a daily export frequency.

Limitations

Passwords

This solution does not back up user passwords to DynamoDB. When signing in to the new user pool that was populated with the ImportWorkflow Step Functions workflow, users will be required to reset their passwords.

Multi-factor authentication

This solution does not support user pools with multi-factor authentication (MFA) enabled. When this solution is deployed, it checks the primary user pool's MFA setting and, if the setting is either optional or required, this solution will not launch. This solution also performs this check every time the ExportWorkflow Step Functions workflow is run and, if MFA has been enabled, the workflow will terminate. MFA is not supported because this solution is unable to replicate an end-user's MFA token that is used to configure time-based one-time passwords (TOTP) as a second factor.

Cognito sub attribute

The ImportWorkflow Step Functions workflow will create new users in the empty user pool and synchronize their user profiles with the current state in the backup DynamoDB table. These new users will be assigned new Cognito-generated unique IDs (the sub attribute). If your application is using this value to uniquely identify a user, we recommend that you copy this value to a new custom attribute in the primary user pool. This attribute will be exported to DynamoDB and available in the new user pool when the ImportWorkflow Step Functions workflow runs.

Federated users

Users who have signed in to your user pool using a third-party identity provider will not have profiles exported to DynamoDB. These users will be created in the new user pool when they next log in through the third-party identity provider. This means that custom attributes for federated users will not be exported by this solution, and the federated user will get a new value for the sub attribute when they log in to the new user pool.

Cognito advanced security features

When evaluating users as part of Cognito's advanced security features, the user history is not exported by this solution and therefore will not be available in the new user pool.

Username attributes

When a user pool is initially created, you can allow users the choice of using either an email address or a phone number as their username. However, this solution does not support user pools that are configured to allow both email addresses and phone numbers.

Group roles

AWS Identity and Access Management (IAM) roles associated with groups are not exported by this solution. If you have an IAM role attached to a group, you must create a similar role or associate that role with the group in the new user pool.

Tracked devices

This solution does not export tracked devices to the BackupTable DynamoDB table. As such, if you use the ImportWorkflow Step Functions workflow to populate a new user pool, there will be no tracked devices associated with the imported user profiles.

Deployment

Here is the link to CloudFormation template along with instructions on how to automatically deploy the stack:

https://docs.aws.amazon.com/solutions/latest/cognito-user-profiles-export-reference-architecture/automated-deployment.html