Implementation Guide

Guidance for User Profiles Export with Amazon Cognito

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Guidance for User Profiles Export with Amazon Cognito: Implementation Guide

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

Table of Contents

Guidance-overview 1

Limitations 2

Cost 2

Architecture overview 3

Guidance components 5

Export workflow 5

Backup table 5

Import workflow 6

Limitations 7

Passwords 7

Multi-factor authentication 7

Cognito sub attribute 7

Federated users 7

Cognito advanced security features 7

Username attributes 8

Group roles 8

Tracked devices 8

Design considerations 9

One-way scheduled export 9

Guidance configuration 9

Export frequency 9

Cognito transactions per second (TPS) 9

Security 12

IAM roles 12

Additional resources 13

Revisions 14

Notices 15

Build a framework for exporting user profile and group information from your Amazon Cognito user pools

This implementation guide discusses architectural considerations and configuration steps for deploying the Cognito User Profiles Export Reference Architecture Guidance in the Amazon Web Services (AWS) Cloud.

The guide is intended for IT infrastructure architects, administrators, and DevOps professionals who have practical experience architecting in the AWS Cloud.

Many Amazon Web Services (AWS) customers use Amazon Cognito user pools to provide a scalable and secure user directory for their applications. Amazon Cognito customers often need to export their users to facilitate more complex user queries, or to provide resiliency in case of regional failure or accidental deletion of their users. To assist with this, AWS offers the Cognito User Profiles Export Reference Architecture Guidance. This Guidance is designed to provide a framework for exporting user profile and group information from your user pool, allowing you to focus on extending this guidance's functionality rather than managing the underlying infrastructure operation.

This guidance uses an `ExportWorkflow` AWS Step Functions workflow to periodically export user profiles, groups, and group membership details from your user pool to an Amazon DynamoDB global table with automatic, asynchronous replication to a backup Region for added resiliency.

This guidance's `ImportWorkflow` Step Functions workflow can be used to populate a new, empty user pool with data from the global table, allowing you to easily recover user profiles, groups, and group memberships. The `ImportWorkflow` Step Functions workflow can be run in either the primary or backup Region.

Customers interested in using this guidance for both backup and recovery should be comfortable with a Recovery Time Objective (RTO) measured in hours rather than minutes since the guidance requires the `ImportWorkflow` Step Functions workflow to run in a recovery scenario. Refer to Cognito transactions per second (TPS) for performance benchmarks for different sized user pools.

The Recovery point objective (RPO) is determined by the time the `ExportWorkflow` Step Functions workflow runs in the primary Region. You will lose any updates made after the last `ExportWorkflow` Step Functions workflow run.

Limitations

Customers interested in using this guidance should be aware that it does not export sensitive information, such as user passwords; that user pools with multi-factor authentication (MFA) enabled are not supported; and that advanced security features are not supported. For a full list of limitations, refer to Limitations in the guidance components section.

Cost

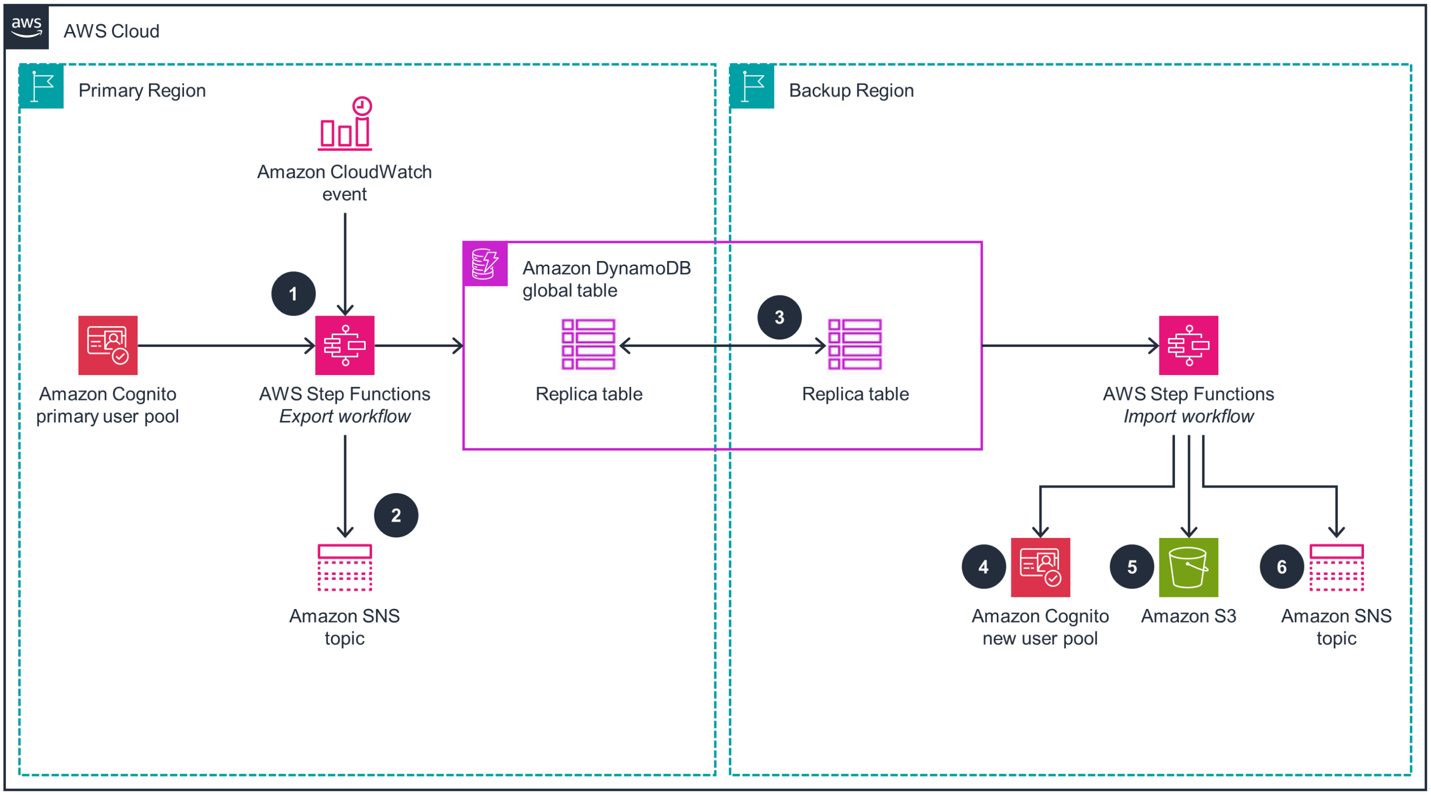
You are responsible for the cost of the AWS services used while running this guidance. As of this revision, the cost for running this guidance in the North Virginia Region with the Tokyo Region as backup is approximately **$90.00 per month** for a user pool of 500,000 users (where each user is a member of one group) and a daily export frequency. Prices are subject to change. For full details, see the pricing webpage for each AWS service you will be using in this guidance.

AWS Service	Total cost
Amazon DynamoDB	$86.00
Amazon Step Functions	$1.00
Amazon Simple Queue Service (Amazon SQS)	$1.00
Amazon Simple Notification Service (Amazon SNS)	$1.00
AWS Lambda	$1.00

IMPORTANT: When the `ImportWorkflow` Step Functions workflow is run, it will create new users with the same profiles and group memberships in a new, empty user pool that you create. These new users will be treated by Cognito as additional monthly active users (MAU) when they are initially created by the guidance. Therefore, your Cognito cost could rise significantly during any month in which you run the `ImportWorkflow` Step Functions workflow. Refer to Cognito's Pricing Page for more details on how Cognito MAUs are priced.

Architecture overview

Deploying this guidance with the default parameters builds the following environment in the AWS Cloud.


AWS Cloud
Primary Region
Backup Region
Amazon CloudWatch event
1
Amazon Cognito primary user pool
AWS Step Functions *Export workflow*
2
Amazon SNS topic
Amazon DynamoDB global table
Replica table
3
Replica table
AWS Step Functions *Import workflow*
4
Amazon Cognito new user pool
5
Amazon S3
6
Amazon SNS topic

Cognito User Profiles Export Reference Architecture architecture on AWS

1. In the primary AWS Region, an Amazon CloudWatch scheduled event invokes the AWS Step Functions export workflow, which examines the primary Amazon Cognito user pool. It stores user profiles, groups, and group membership information in the global table.

   Note: This Guidance does not create the primary user pool.

2. When the export workflow is complete, Step Functions sends a completion or error message to the Amazon Simple Notification Service (Amazon SNS) topic for logging or troubleshooting.
3. Amazon DynamoDB asynchronously replicates all data to the backup Region for added resiliency.
4. In your backup Region, use the same Step Functions import workflow as seen in Step 2 to import data from global table to populate a new, empty Amazon Cognito user pool. This enables you to easily recover user profiles, groups, and group memberships.

Note: This Guidance does not create the new user pool.

5. A mapping comma-separated values (CSV) file uploads to the guidance's Amazon Simple Storage Service (Amazon S3) bucket. This CSV file maps the line number reported by Amazon Cognito to the subattribute of the corresponding users for inclusion in the troubleshooting error message.
6. When the import workflow is complete, Step Functions sends a completion or error message to an Amazon SNS topic for logging or troubleshooting.

Guidance components

Export workflow

The `ExportWorkflow` AWS Step Functions workflow is invoked on a set schedule. This guidance includes a parameter to run the workflow daily, weekly, or every 30 days. If you prefer another schedule, you can modify the schedule in the Amazon CloudWatch console after launching this guidance.

The `ExportWorkflow` Step Functions workflow interrogates your primary user pool and performs the following actions:

- Lists all users in the primary user pool and refreshes the `BackupTable` DynamoDB table with updated user profile information (such as standard and custom attributes, and the user enabled flag), and adds new users.
- Lists all groups in the primary user pool and refreshes the `BackupTable` DynamoDB table with updated group information (such as group description and precedence value), and adds new groups.
- Lists all users in each group to identify new group members, and users that are no longer members of a group, and updates the `BackupTable` DynamoDB table accordingly.
- Checks the `BackupTable` DynamoDB table for records that were not updated during this run of `ExportWorkflow` Step Functions workflow. These records will be removed from the `BackupTable` DynamoDB table.

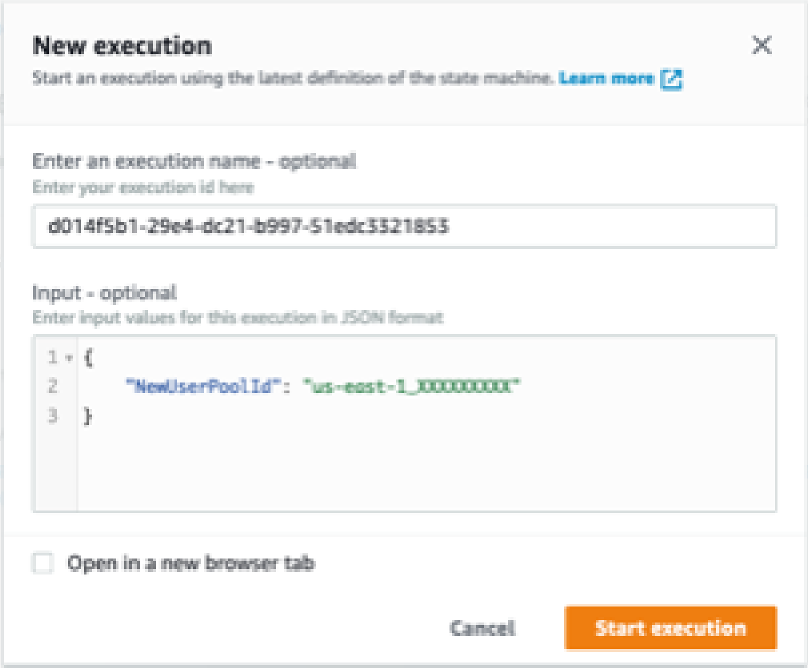
Backup table

The `BackupTable` DynamoDB table is a global table with a replica in your backup AWS Region. When data changes in the table, DynamoDB asynchronously replicates that data to the replica in your backup Region. The guidance exports the user profile, group, and group membership information to the backup Amazon DynamoDB table on a set schedule.

In the primary Region, the `BackupTable` DynamoDB table is configured to enable DynamoDB Point-in-Time Recovery, which enables you to restore the `BackupTable` DynamoDB table to any point in time during the last 35 days. For more information, refer to Point-in-Time Recovery for DynamoDB.

Import workflow

The `ImportWorkflow` Step Functions workflow populates an empty user pool with user profiles, groups, and group memberships from the DynamoDB global table. You must run the `ImportWorkflow` Step Functions workflow on demand in either the primary or backup Region. When starting the execution, you must supply a JSON object as input and supply the ID for the new user pool in the `NewUserPoolId` property.



New execution

Start an execution using the latest definition of the state machine. Learn more

Enter an execution name - optional

Enter your execution id here

d014f5b1-29e4-dc21-b997-51edc3321853

Input - optional

Enter input values for this execution in JSON format

```
{
    "NewUserPoolId": "us-east-1_XXXXXXXXX"
}
```

□ Open in a new browser tab

Amazon Cognito `NewUserPoolId` property

The `ImportWorkflow` Step Functions workflow first checks that the new user pool does not have any groups or users before proceeding. If the user pool is not empty, the `ImportWorkflow` Step Functions workflow will be halted.

Note: When a user profile is created in the new user pool, it is assigned a new Amazon Cognito generated unique ID (the sub attribute). Additionally, user passwords are not replicated by this guidance. Refer to Limitations for more details.

Limitations

Passwords

This guidance 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 guidance does not support user pools with multi-factor authentication (MFA) enabled. When this guidance is deployed, it checks the primary user pool's MFA setting and, if the setting is either optional or required, this guidance will not launch. This guidance 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 guidance 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 guidance, 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 guidance 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 guidance 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 guidance. 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 guidance 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.

Design considerations

One-way scheduled export

This guidance automatically exports data from your primary user pool to Amazon DynamoDB on a scheduled basis. If you create a new user pool and populate it by running the `ImportWorkflow` AWS Step Functions workflow, you can configure scheduled exports of this new user pool by launching a new instance of this guidance and configuring it to point to the new user pool.

Guidance configuration

There are two parameters you can use to influence the guidance's behavior.

Export frequency

This parameter sets the schedule expression for the Amazon CloudWatch Events rule that starts the `ExportWorkflow` Step Functions workflow. There are options for every day, seven days, or 30 days. If you require a different schedule, update the CloudWatch Events rule after the guidance is deployed.

Cognito transactions per second (TPS)

This parameter sets the maximum number of times an Amazon Cognito API is called per second. While the `ExportWorkflow` Step Functions workflow is running, API calls are made to list users and groups in the primary user pool. When the `ImportWorkflow` Step Functions workflow is running, it adds groups and adds users to groups. These API calls count against your existing Cognito API limits. This parameter can reduce the risk of the guidance inadvertently impacting your applications. Lowering this value results in this guidance taking longer to run.

User pool	Cognito TPS setting	Action	Approximate run time
10,000 users No groups	10	Sync workflow	2.62 minutes
		Recovery workflow	8.13 minutes

User pool	Cognito TPS setting	Action	Approximate run time
	5	Sync workflow	2.66 minutes
		Recovery workflow	8.32 minutes
10,000 users Each user in one group	10	Sync workflow	4.76 minutes
		Recovery workflow	29.24 minutes
	5	Sync workflow	4.82 minutes
		Recovery workflow	47.73 minutes
100,000 users No groups	10	Sync workflow	21.82 minutes
		Recovery workflow	56.31 minutes
100,000 users Each user in one group	10	Sync workflow	40.26 minutes
		Recovery workflow	290.24 minutes
250,000 users No groups	10	Sync workflow	54.79 minutes
		Recovery workflow	128.2 minutes
250,000 users Each user in one group	10	Sync workflow	98.65 minutes
		Recovery workflow	678.29 minutes
500,000 users No groups	10	Sync workflow	146.52 minutes
		Recovery workflow	247.63 minutes

User pool	Cognito TPS setting	Action	Approximate run time
500,000 users Each user in one group	10	Sync workflow	181.46 minutes
		Recovery workflow	1,313.31 minutes

Security

When you build systems on AWS infrastructure, security responsibilities are shared between you and AWS. This shared model reduces your operational burden because AWS operates, manages, and controls the components including the host operating system, the virtualization layer, and the physical security of the facilities in which the services operate. For more information about AWS security, visit the AWS Security Center.

IAM roles

AWS Identity and Access Management (IAM) roles enable customers to assign granular access policies and permissions to services and users in the AWS Cloud. This guidance creates IAM roles that grant the guidance's AWS Lambda functions access to create regional resources.

Additional resources

AWS services

- AWS Lambda
- Amazon CloudWatch
- Amazon Cognito
- AWS Step Functions
- Amazon Simple Notification Service
- Amazon DynamoDB
- AWS Identity and Access Management
- AWS CloudFormation
- Amazon Simple Queue Service
- Amazon Simple Storage Service

Revisions

Publication date: *August 2020*

Check the CHANGELOG.md file in the GitHub repository to see all notable changes and updates to the software. The changelog provides a clear record of improvements and fixes for each version.

Notices

Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents AWS current product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from AWS and its affiliates, suppliers or licensors. AWS products or services are provided “as is” without warranties, representations, or conditions of any kind, whether express or implied. AWS responsibilities and liabilities to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

Guidance for User Profiles Export with Amazon Cognito is licensed under the terms of the of the Apache License Version 2.0 available at The Apache Software Foundation.