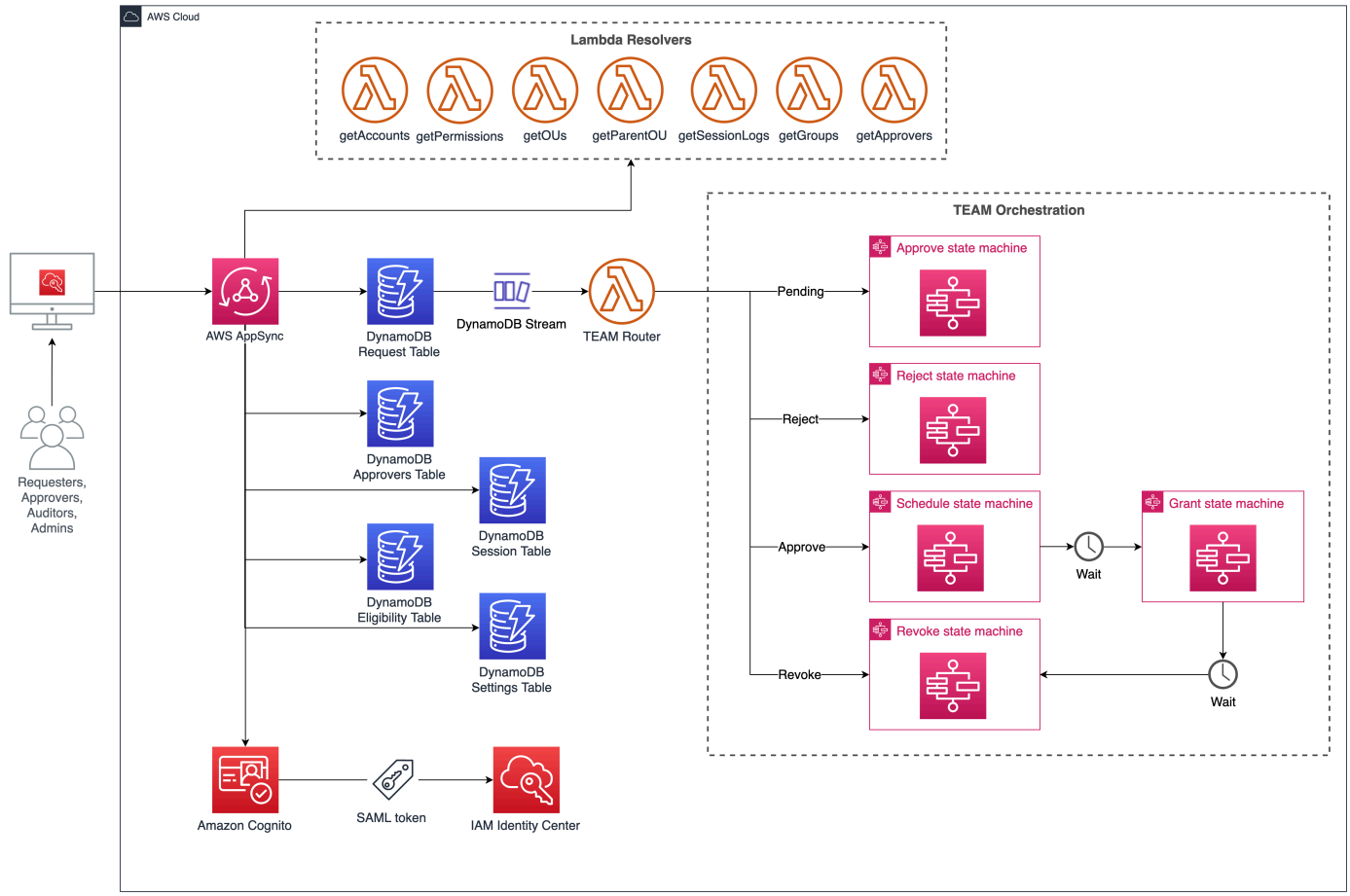
Architecture

Temporary elevated access management (TEAM) solution is a full stack, Single Page Application (SPA) that is based on React JS and powered by AWS serverless services.



Solution components

TEAM consists of the following components:

- A web interface that you can access as a Custom SAML 2.0 application on the IAM Identity Center portal. TEAM users can create, approve, monitor and manage elevated request with few clicks on the web application UI.
- A GraphQL API layer powered by AWS Appsync which responds to actions performed on the web UI and retrieves, updates and stores data from and to TEAM datastores.

- DynamoDB datastore for storing TEAM request, eligibility and approval state.
- AWS Lambda backed middleware component that contains logic for routing TEAM elevated access requests to the orchestration layer.
- AWS Step Functions orchestration workflow component that automates the process of notification, granting and removal of elevated access.
- Auditing and visibility component powered by AWS CloudTrail Lake for veiwing elevated access session activity logs.
- Security component backed by Amazon Cognito for managing group and user based authentication and application authorization.

The TEAM application is built, deployed and hosted on AWS Amplify.

TEAM DynamoDB Tables

The following DynamoDB tables are deployed as part of the solution:

- **Requests Table** - Stores information about TEAM requests, approval and elevated access status
- **Approver Table** - Stores details of Approver groups for accounts and Organizational Units
- **Eligibility Table** - Stores data relating to accounts, permission sets or roles an entity (user or group) is eligible to request access to
- **Session Table** - An ephemeral datastore that stores and manages the state of an AWS CloudTrail Lake query. This helps to provide asynchronous Pub/Sub API for retrieving session activity logs
- **Settings Table** - Stores configurable values of TEAM application wide settings such as mandatory fields, default timeouts, maximum duration, approval settings etc

TEAM Router

A TEAM request record is stored in the request DynamoDB table whenever a request is created or updated on the web UI

A TEAM request can be in one of the following states:

- ***Pending*** - A newly created TEAM request which has not been actioned
- ***Approved*** - A TEAM request approved by a member of an approver group responsible for actioning requests for an account
- ***Rejected*** - A TEAM request rejected by a member of an approver group responsible for actioning requests for an account

- ***Expired*** - A TEAM Request that has not been approved or rejected after a configurable number of hours (1 hour by default). When a TEAM request expires, a requester would be required to raise another request if they still need elevated access to an account
- ***Cancelled*** - A TEAM request cancelled by the requester before it is actioned by an approver
- ***Revoked*** - A TEAM request elevated access removed before the requested duration elapses
- ***Ended*** - A TEAM request whose request duration has elapsed and elevated access has been removed
- ***Error*** - A TEAM request whose orchestration has resulted in an error in the backend

When a TEAM request item is created or updated in DynamoDB, it triggers a DynamoDB Stream which invokes the ***TEAM router***

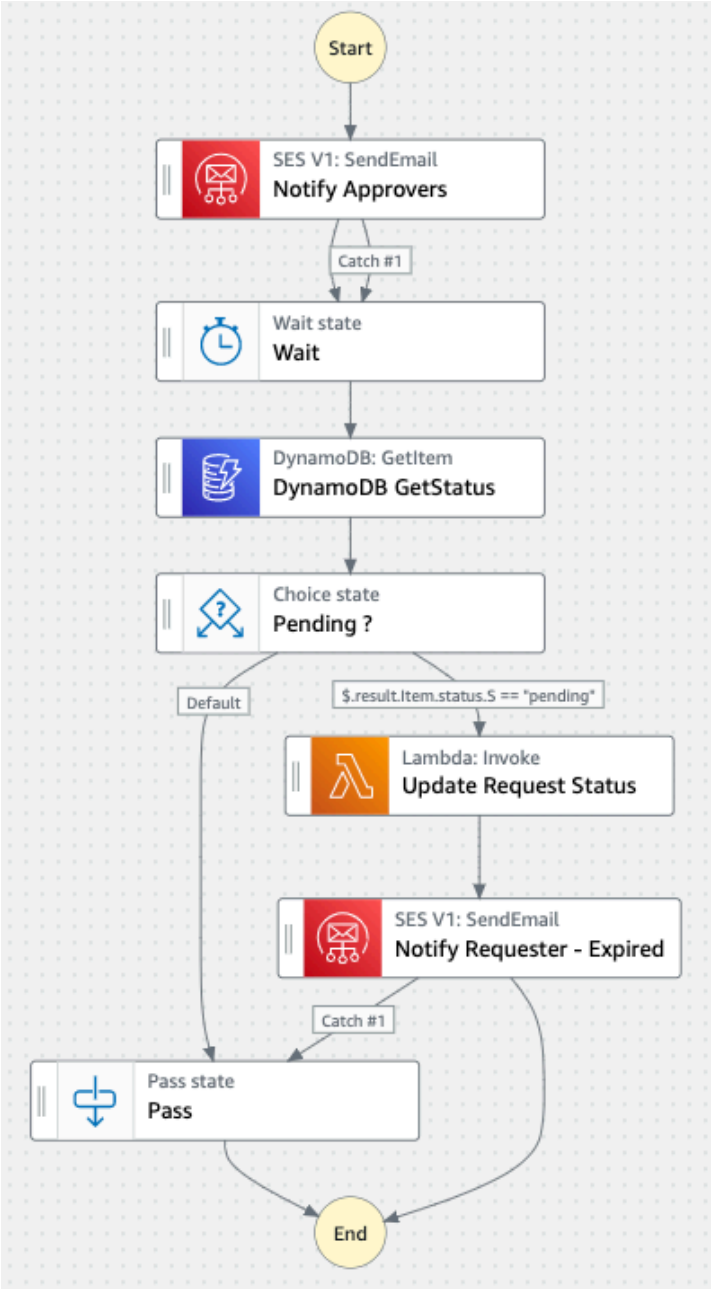
The ***TEAM router*** is a Lambda function that executes a Step Functions workflow corresponding to the state of a TEAM request. For example, the TEAM router would invoke an approval Step Functions workflow when a new request is created.

TEAM Step Function Orchestration Workflows

The TEAM orchestration workflow is made up of the step functions listed below:

Approval workflow

The Approval Step Functions workflow is invoked when a TEAM request is newly created and the request status is ***pending***.

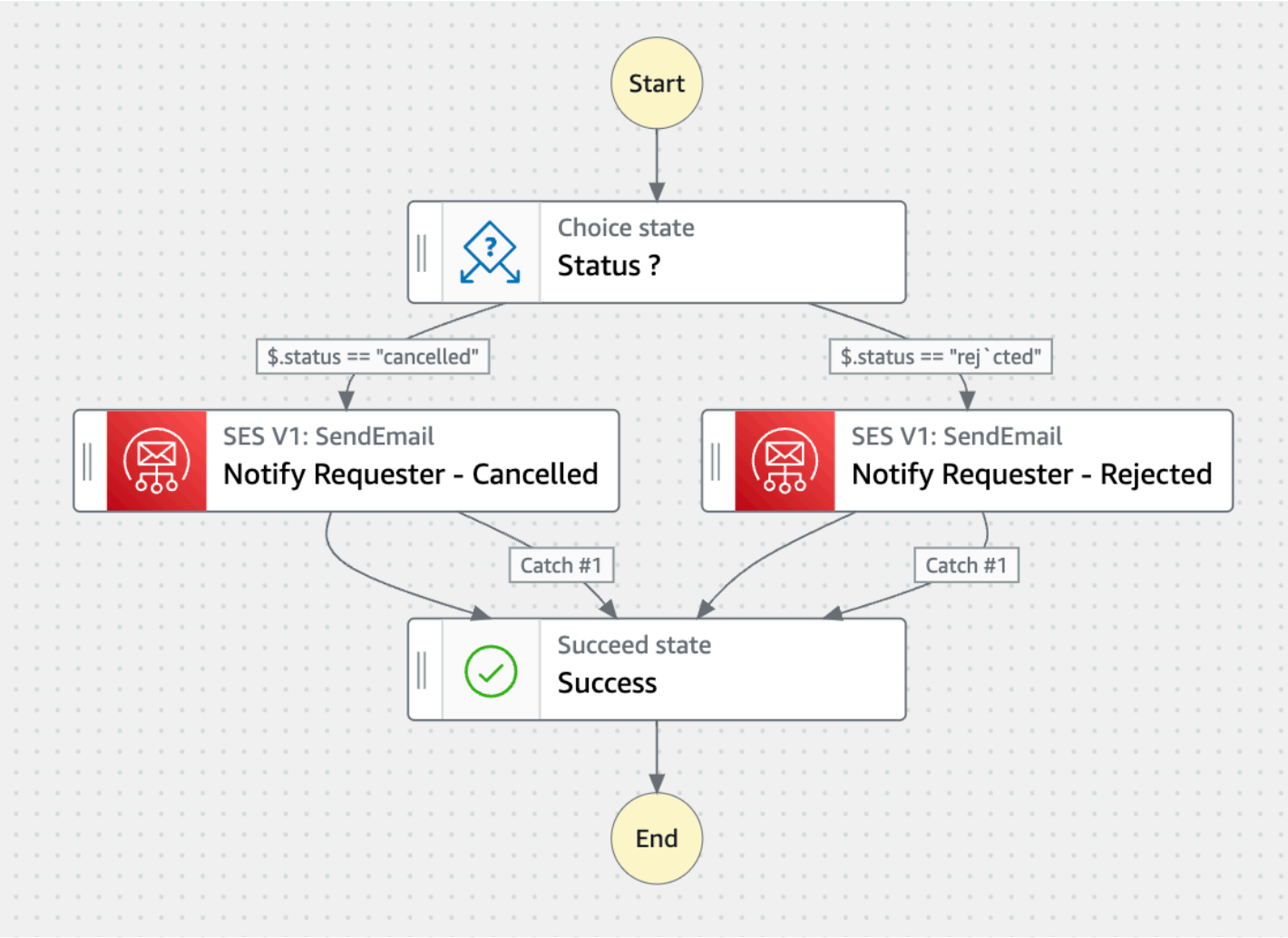


The Approval state machine performs the following functions:

- Notifies members of the approval group delegated for the requested account of the new request
- Waits for 1 hour (configurable) and checks if the request has been actioned or not.
- If the request has not been actioned it changes the status to ***expired***

Reject workflow

The Reject Step Functions workflow is invoked when a TEAM request is rejected by a member of an approver group thus changing the request status to ***rejected***. The reject workflow is also invoked when a request when has not been approved or rejected is cancelled by a requester thus changing the request status to ***cancelled***

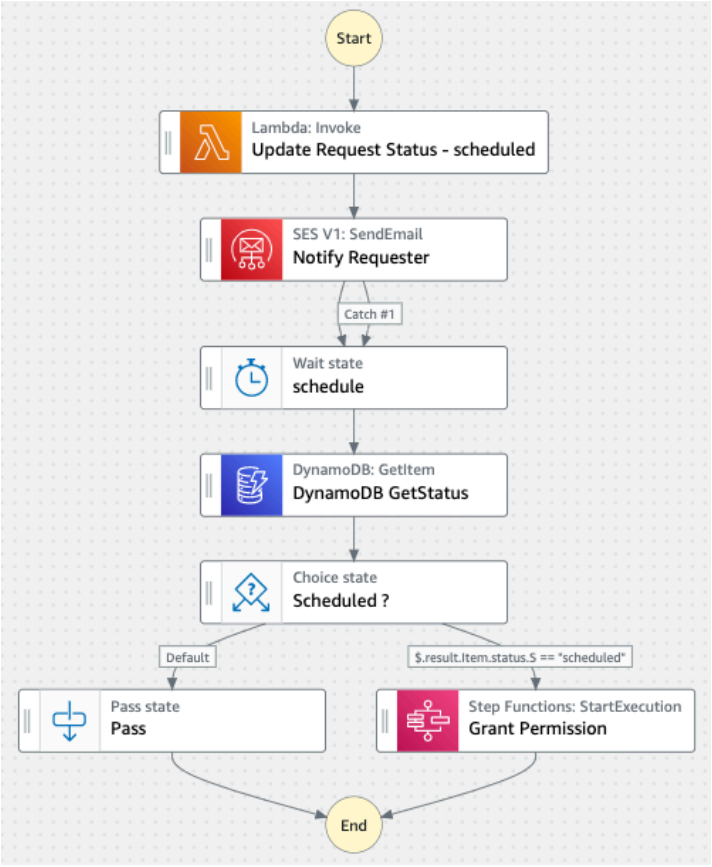


The Reject state machine performs the following functions:

- Determines if the request was ***rejected*** or ***cancelled***
- If the status is ***rejected***, notifies the requester about the request rejection
- If the status is ***cancelled***, notifies the requester and approver group that the request has been cancelled.

Schedule workflow

The Schedule Step Functions workflow is invoked when a TEAM request is approved by a member of an approver group and the request status is ***approved***.

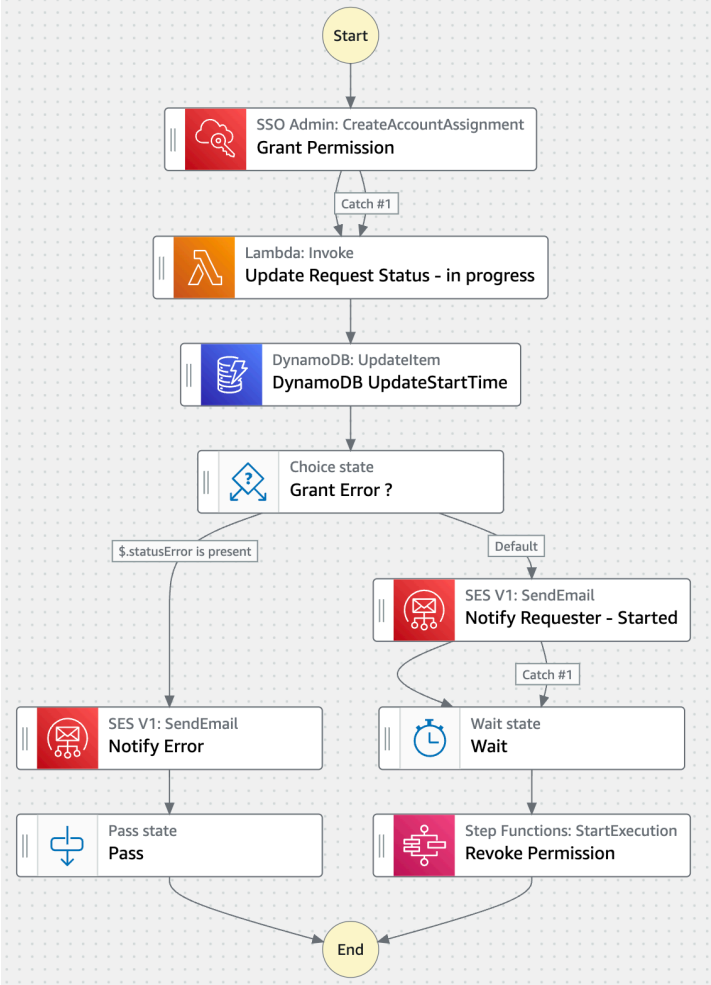


The Schedule state machine performs the following functions:

- Updates the TEAM request status to ***scheduled***
- Notifies the requester about the request approval
- Waits until the start time specified in the request
- Invoke the ***Grant*** State machine workflow at the requested elevated access start time

Grant workflow

The Grant Step Function workflow is invoked by the ***Schedule*** state machine at the session start time.

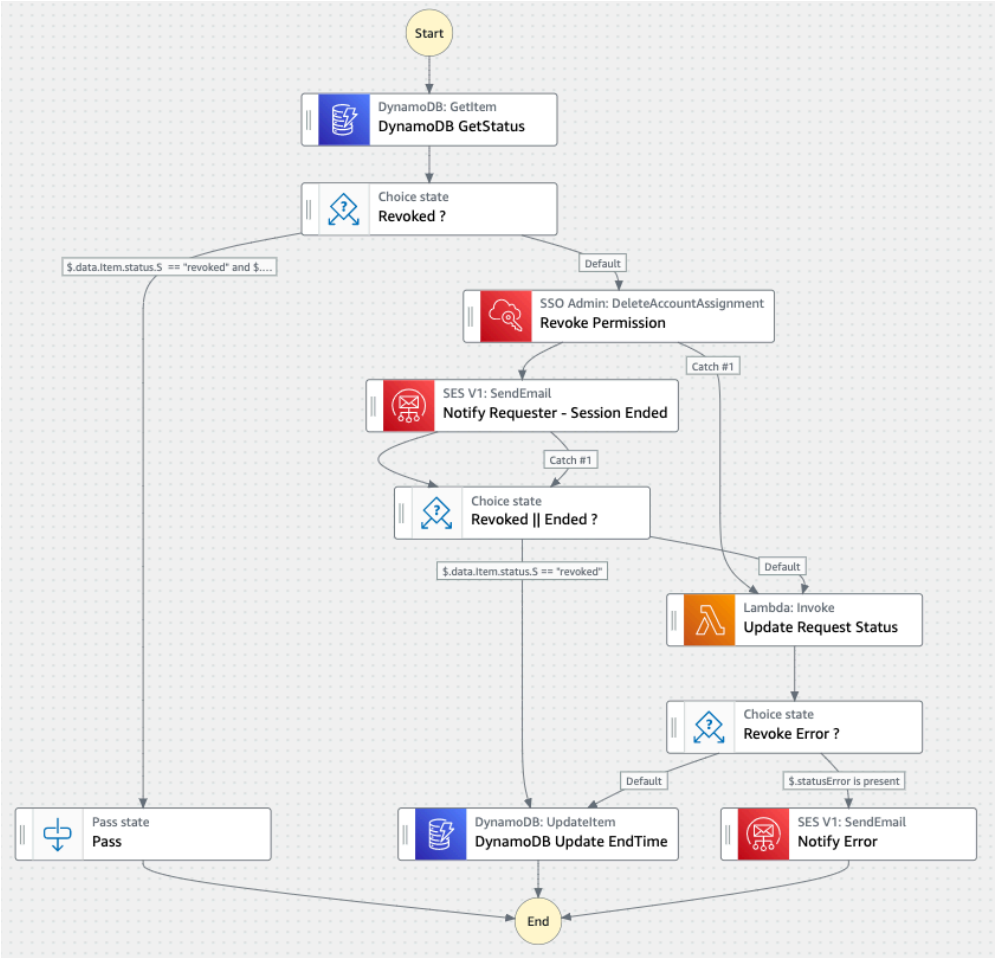


The Grant state machine performs the following functions:

- Assigns the requested permission set and account to the requester identity in IAM Identity Center, thus providing the requester elevated access to the requested account
- Updates the TEAM request status to ***in progress***
- Notifies the requester that elevated access has started
- Waits for the elevated access duration(in hours) specified in the initial request
- Invokes the **Revoke** State machine once the requested duration elapses

Revoke workflow

The Revoke Step Function workflow is invoked either by the ***Grant*** state machine (when elevated access ends) or when a user (TEAM requester or approver) revokes an active TEAM request which is **in progress**.



The Revoke state machine performs the following functions:

- Removes the requested permission set and account assigment from the requester identity in IAM Identity Center preventing the requester from being able to invoke sessions to the requested account
- Notifies the requester that elevated access has ended
- Updates the TEAM request status to ***ended***

TEAM Lambda Resolvers

The TEAM Lambda resolvers are GraphQL API components backed by Lambda functions that provide business logic to retrieve information that is rendered and consumed in the frontend of the TEAM application.

TEAM uses the following Lambda resolvers:

- **teamgetAccounts** - This Lambda function returns a list of accounts in your AWS organization
- **teamgetOUs** - This Lambda function returns a list of Organizational Units (OUs) within your AWS organization

- **teamgetPermission** - This Lambda function returns the permission sets available in IAM Identity Center within your AWS organization
- **teamgetUsers** - This Lambda function returns a list of users available in IAM Identity Center within your AWS organization
- **teamgetIdcGroups** - This Lambda function returns a list of groups available in IAM Identity Center within your AWS organization