Implementation Guide

Account Assessment for AWS Organizations

Account Assessment for AWS Organizations: Implementation Guide

Table of Contents

Use a web UI to view resource-based policy dependencies for your AWS Organizations AWS accounts

Publication date: *November 2022*. 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.

This solution allows customers to better understand AWS Organizations dependencies by finding trusted access enabled AWS services, delegated admin accounts, and identity-based, resource-based and service control policies.

Businesses are increasing their adoption of AWS Organizations to easily create accounts, allocate resources, create group accounts, and apply governance policies to accounts or groups. However, when businesses need to consolidate AWS Organizations or move AWS accounts between AWS Organizations, system administrators are often challenged to clearly understand the business impact of their account integrations. The process to manually evaluate AWS Organizations dependencies can be time consuming—potentially involving reviews of tens or even hundreds of AWS resources of individual accounts.

The Account Assessment for AWS Organizations solution performs the following functions:

- Programmatically scans all AWS accounts in an AWS Organization for identity-based, resource-based and service control policies.
- Presents scan results in a web user interface (web UI) that tracks resources in your AWS Organization.
- Enables the user to search through the scanned policies and find conditions, dependencies and specific actions in your policies across your AWS organization.
- Runs the policy scan daily to keep the information about your policies up to date.

This implementation guide provides an overview of the Account Assessment for AWS Organizations solution, its reference architecture and components, considerations for planning the deployment, and configuration steps for deploying the solution to the Amazon Web Services (AWS) Cloud.

Use this navigation table to quickly find answers to these questions:

If you want to . . .	Read . . .
Know the cost for running this solution. The estimated baseline cost for running this solution in the US East (Northern Virginia) Region is USD $45 per month, depending on your specific implementation.	Cost
Understand the security considerations for this solution.	Security
Know how to plan for quotas for this solution.	Quotas
Know which AWS Regions are supported for this solution.	Supported AWS Regions
View or download the AWS CloudForm ation template included in this solution to automatically deploy the infrastructure resources (the "stack") for this solution.	AWS CloudFormation template
Access the source code and optionally use the AWS Cloud Development Kit (AWS CDK) to deploy the solution.	GitHub repository

This guide is intended for solution architects, DevOps engineers, data scientists, and cloud professionals who want to implement Account Assessment for AWS Organizations solution in their environment.

Important

We designed this solution to aggregate scan findings for customers. This solution does not check the validity or correctness of your underlying resource-based policies. When changing policies that allow account migration to another AWS Organization, we recommend:

- Verifying that your policies work as intended before making changes.

- Using AWS Identity and Access Management (IAM) Access Analyzer to verify that your policies achieve your required permissions.
- Reviewing and updating the Condition policy element to meet your security requirements. Do not delete the `Condition` without reviewing the underlying impact.
- Engaging with AWS Solutions Architects, Technical Account Managers, and AWS Professional Services to review your AWS Organizations-based dependencies identified by the solution before initiating account migration.

Note

Dependencies outside the scope of this solution can impact the account migration between AWS Organizations (for example, quotas for AWS Organizations, resources shared by AWS Resource Access Manager [AWS RAM], and service-managed CloudFormation StackSets).

Features and benefits

The Account Assessment for AWS Organizations solution provides the following features.

Access the solution using a web UI

This solution provides a web UI to help you view scan results. For more details, see Use the solution.

Identify enabled services with AWS Organizations

In your AWS Organization, you can enable more than 30 compatible AWS services to perform operations across all of the AWS accounts. This solution finds enabled services and delegated admin accounts per service (if activated).

Explore your policies to find actions and conditions

This feature allows you to search through all the policies across your AWS Organization to find specific conditions and actions. In case an action is deprecated you need to remove or update a given action or condition across all accounts or a specific set of accounts, you can quickly find and review the policies in the solutions UI, and update them across your environment to meet your needs.

The policies included in the scans are identity-based policies, resource-based policies, and organization-based policies (such as service control policies). The daily scan will store representations of all the policies in your environment in DynamoDB on a daily basis, so you can search through them, and find the attributes you are looking for in the solution's web UI.

Assess IAM policy conditions

The `Condition` policy element lets you use keys to specify conditions for when a policy is in effect. You can use specific keys to compare the identifier or path of the requesting principal's Organization in AWS Organizations with the identifier specified in the policy. This helps you identify existing conditions and dependencies. If desired, you can use global condition keys. This solution scans conditions in the following types of policies and presents them for your review in the solution's web UI.

Assume role (trust relationship) conditions

With IAM roles, you can establish trust relationships between your trusting account (the account that owns the resource) and other AWS trusted accounts (the accounts that contain the users that need to access the resource). In this trust relationship, you can use condition keys to grant permissions to any principal in your AWS Organization.

Identity-based policy conditions

Identity-based policies are attached to a user, group, or role. Use these policies to specify permissions for a given identity.

Resource-based policy conditions

Resource-based policies are attached to a resource. Use these policies to specify who has access to the resource and what actions they can perform on it. For example, you can attach resource-based policies to Amazon Simple Storage Service (Amazon S3) buckets, Amazon Simple Queue Service (Amazon SQS) queues, Amazon Virtual Private Cloud (Amazon VPC) endpoints, and AWS Key Management Service (AWS KMS) encryption keys.

The following table provides a list of services supported by this solution.

AWS service	Policy type
Amazon API Gateway	Resource-based

AWS service	Policy type
AWS Backup	Resource-based
AWS CloudFormation	Resource-based
AWS CodeArtifact	Resource-based
AWS CodeBuild	Resource-based
AWS Config	Resource-based
Amazon Elastic Container Registry (Amazon ECR)	Resource-based
Amazon Elastic File System (Amazon EFS)	Resource-based
AWS Elemental MediaStore	Resource-based
Amazon EventBridge	Resource-based
AWS Glue	Resource-based
AWS Identity and Access Management (IAM)	Identity-based
AWS IoT Core	Resource-based
AWS Key Management Service (AWS KMS)	Resource-based
AWS Lambda	Resource-based
Amazon OpenSearch Service	Resource-based
AWS Secrets Manager	Resource-based
AWS Serverless Application Repository	Resource-based
Amazon Simple Email Service (Amazon SES)	Resource-based
Amazon Simple Notification Service (Amazon SNS)	Resource-based

AWS service	Policy type
Amazon Simple Queue Service (Amazon SQS)	Resource-based
Amazon Simple Storage Service (Amazon S3)	Resource-based
Amazon S3 Glacier	Resource-based
AWS Systems Manager (AWS Systems Manager Incident Manager)	Resource-based
Amazon Virtual Private Cloud (Amazon VPC) (VPC Endpoints)	Resource-based
AWS Resource Access Manager (Amazon RAM)	Resource-based
Amazon EventBridge Schemas	Resource-based
AWS Systems Manager Incident Manager Contacts	Resource-based
Amazon Lex	Resource-based
ACM-PCA (AWS Certificate Manager Private Certificate Authority)	Resource-based

Use cases

The following are example use cases for using this solution. You can apply this solution in innovative ways that are not limited to this list.

Mergers or acquisitions

If you are undergoing a merger or acquisition, you may need to move AWS accounts between multiple AWS Organizations and Organizational Units (OUs) while maintaining existing production workloads and avoiding downtime.

Security audits

If you are undergoing a security audit, you might want further insight into your AWS accounts, policies, trust relationships, and activated AWS services.

Centralized Policy Explorer

To evaluate policy compliance and identify security threats, search for actions, resources, effects, or principles. Use this feature to search, filter, review, and identify the policies in your AWS Organization. You can also choose to download the list for sharing purposes.

Management account change

If you plan to create a new account as your management account and change the existing management account into a member account (for example, if you have production workloads in your management account), you might want visibility into the management account's existing policies.

Concepts and definitions

This section describes key concepts and defines terminology specific to this solution:

Identity-based policy

Identity-based policies are attached to a user, group, or role. Use these policies to specify permissions for a given identity.

Resource-based policy

Resource-based policies are attached to a resource. Use these policies to specify who has access to the resource and what actions they can perform on it.

Service Control Policy Service control policies (SCPs) are a type of organization policy that are used to manage permissions in an organization, SCPs offer central control over the maximum available permissions for all accounts in the organization.

Trusted account

AWS account that contains the users that need to access the resource.

Trusting account

AWS account that owns the resource.

Principal

An entity in AWS that can perform actions and access resources. A principal can be an AWS account owner, a user, or a role.

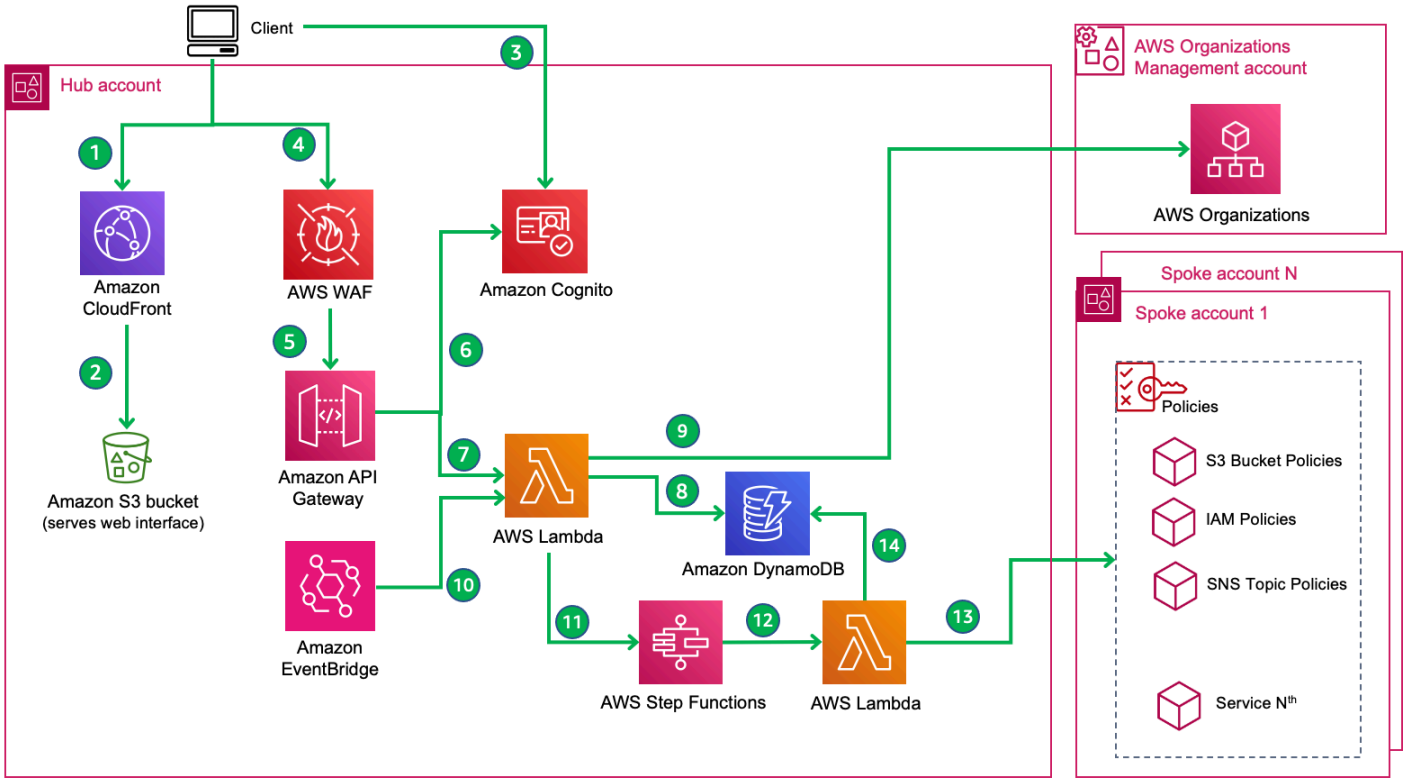
> **Note**
>
> For a general reference of AWS terms, see the AWS glossary in the *AWS General Reference*.

Architecture overview

This section provides a reference implementation architecture diagram for the components deployed with this solution.

Architecture diagram

Deploying this solution with the default parameters deploys the following components in your AWS account.



1. Users access the solution by opening the Amazon CloudFront url in their browser. CloudFront delivers the web UI content from an Amazon S3 bucket.
2. The Amazon S3 bucket hosts the web UI files and assets.
3. When the web UI is loaded, it redirects the user to the Amazon Cognito hosted login form. On successful login, Cognito grants a user access token that is stored on the client.
4. On the web UI an authenticated user can view the results of previous scans and a history of scans. To load this data or start scans, the web UI sends http requests to the solution's API. An AWS Web Application Firewall (WAF) protects the application programming interfaces (APIs)

from attacks. By default this solution uses AWS managed rule sets for the WAF. You can modify the firewall rules according to your needs via the AWS Console. The WAF also limits API access to a range of IP addresses that you define as a deployment parameter when deploying the solution.

5. An Amazon API Gateway provides the solution's API layer.
6. The Cognito Authorizer attached to the API Gateway will validate the access token in each incoming request against Amazon Cognito.
7. The API Gateway routes each request to the responsible AWS Lambda function. The solution contains one Lambda function per read operation as well as one Lambda function to start Delegated Admin scans and Trusted Access scans respectively.
8. To serve the results of a scan to the web UI, a Lambda function loads the data from the DynamoDB.
9. To scan for Delegated Admin Accounts or Trusted access, a Lambda function assumes the IAM role deployed by the OrgManagement stack of this solution. Then it will call the AWS Organizations API in the organization management account. It stores the results in DynamoDB.
10. While Delegated Admin scans and trusted access scans are started on demand through the web UI and API Gateway, the scan for policies is supposed to run once per day. For that purpose, an Amazon EventBridge rule triggers the Policy Scan Lambda function on a daily schedule.
11. The Policy Scan lambda function registers the start of a scan by writing an IN_PROGRESS record into DynamoDB, retrieves all active account ids from the AWS Organizations API, and passes the list of account ids to the Policy Scan Step Function.
12. The Step Function orchestrates the subtasks for a Policy scan:
    - It first verifies for each account id that the Spoke Role can be assumed in that account. (The Spoke Role is deployed by the spoke template of this solution.)
    - For each verified account, and for each of the AWS Services to be scanned, it calls another Lambda functions to scan the given account and service in each region.
    - Once all accounts have been iterated, the Step Function calls the Finish Job Lambda function to update the job record in DynamoDB to SUCCESS, FAILED or SUCCESS_WITH_FAILURES.
13. For each account and service, the Lambda function assumes the Spoke Role in the given account and calls the given service API once per region.
14. The Lambda function It stores a representation of the retrieved resource-based, identity-based or service control policy objects in DynamoDB. Should the call to a service API fail, it stores a "failed task" object instead. The user can now use the Policy Explorer search form on the web UI to browse all stored policies.

AWS Well-Architected design considerations

We designed this solution with best practices from the AWS Well-Architected Framework, which helps customers design and operate reliable, secure, efficient, and cost-effective workloads in the cloud.

This section describes how we applied the design principles and best practices of the Well-Architected Framework when building this solution.

Operational excellence

This section describes how the principles and best practices of the operational excellence pillar were applied when designing this solution.

- The solution pushes metrics to Amazon CloudWatch to provide observability into the infrastructure, Lambda functions, Step Functions, API Gateway, AWS S3 buckets, and the rest of the solution components.
- AWS X-Ray traces Lambda functions, Step Functions, and API Gateway. This helps you visualize the components of the state machine and analyze user requests as they travel through your Amazon API Gateway APIs to the underlying services, identify performance bottlenecks, and troubleshoot requests that resulted in an error.

Security

This section describes how the principles and best practices of the security pillar were applied when designing this solution.

- The Web UI app users are authenticated and authorized with Amazon Cognito.
- All inter-service communications use IAM roles.
- All multi-account communications use IAM roles.
- All roles used by the solution follow least-privilege access. In other words, they only contain minimum permissions required so that the service can function properly.
- The access token obtained from Amazon Cognito is used to authorize API calls.
- All data storage including Amazon S3 buckets and DynamoDB tables have encryption at rest.
- AWS WAF protects the web application and APIs from attacks using AWS managed web ACLs rule groups.

Reliability

This section describes how the principles and best practices of the reliability pillar were applied when designing this solution.

- The solution uses serverless AWS services wherever possible (such as Lambda, API Gateway, Amazon S3, and Step Functions) to ensure high availability and recovery from service failure.
- AWS protects the solution against definition errors of state machines leveraged by AWS Step Functions by running automated tests on the solution.
- Data processing uses Lambda functions. The solution stores data in DynamoDB and Amazon S3, so it persists in multiple Availability Zones by default.

Performance efficiency

This section describes how the principles and best practices of the performance efficiency pillar were applied when designing this solution.

- The solution uses serverless architecture. For additional details, refer to Reliability.
- The solution uses `Map` state in Step Functions to run concurrent iterations that scan resources in multiple AWS services across multiple AWS accounts.
- You can launch the solution in any AWS Region that supports the AWS services used in this solution (such as Lambda, API Gateway, Amazon S3, Step Functions, Amazon Cognito, CloudFront, and AWS WAF). For details, refer to Supported AWS Regions.
- The solution is automatically tested and deployed every day. Our solution architects and subject matter experts review the solution for areas to experiment and improve.

Cost optimization

This section describes how the principles and best practices of the cost optimization pillar were applied when designing this solution.

- Most of the resources used by the solution are serverless, so customers pay only for them while in use.
- The compute layer defaults to Lambda, which uses a pay-per-use model.
- DynamoDB indexes are selected to reduce throughput cost for queries.

- The DynamoDB Time to Live (TTL) feature deletes the item from your table without consuming any write throughput at a customer-defined interval.

Please note that the AWS WAF is always in use, and the AWS Step Function runs once per day. If you are not using the solution, delete the CloudFormation stack to avoid continuous cost.

Sustainability

This section describes how the principles and best practices of the sustainability pillar were applied when designing this solution.

- The solution uses managed and serverless services to minimize the environmental impact of the backend services.
- The solution's serverless design is aimed at reducing carbon footprint compared to the footprint of continually operating on-premises servers.

AWS services used in this solution

AWS service	Description
AWS Lambda	**Core.** Deploys multiple Lambda functions to support four core microservices.
AWS Step Functions	**Core.** Deploys state machine to orchestra te the multiple Lambda functions to scan resource-based policies across multiple accounts and services. The Map state allows the solution to invoke parallel Lambda functions to scan accounts and services asynchronously.
Amazon DynamoDB	**Core.** Deploys a DynamoDB table for each microservice. Each microservice reads and writes to their specific table. This allows every microservice to own its own data.

AWS service	Description
Amazon API Gateway	**Core.** Deploys API Gateway and integrates with Lambda functions for each API. The proxy integration allows change in the Lambda function implementation at any time without needing to redeploy your API.
Amazon S3	**Core.** Deploys Amazon S3 buckets to host the web UI assets.
Amazon EventBridge	**Core.** Starts a policy scan on a daily schedule.
Amazon CloudFront	**Core.** Deploys CloudFront with an Amazon S3 bucket as the origin. This restricts access to the Amazon S3 bucket so that it's not publicly accessible and prevents direct access from the bucket.
Amazon Cognito	**Supporting.** Deploys Cognito user pool to authenticate and authorize users to access the solution web UI.
AWS WAF	**Supporting.** Deploys AWS WAF web ACL to protect your API Gateway API from common web exploits, such as SQL injection and cross-site scripting (XSS) attacks.
AWS X-Ray	**Supporting.** Deploys AWS X-Ray to trace API Gateway, Step Functions, and Lambda functions, allowing you to investigate root causes of failed scans.

Plan your deployment

This section describes the cost, security, Region, and quota considerations for planning your deployment.

Supported AWS Regions

This solution uses AWS services that are not currently available in all AWS Regions. You must launch this solution in an AWS Region where these services are available. For the most current availability of AWS services by Region, refer to the AWS Regional Services List.

Account Assessment for AWS Organizations is supported in the following commercial AWS Regions, as well as GovCloud US-West:

Region Name	Region Code
Africa (Cape Town)	af-south-1
Asia Pacific (Hong Kong)	ap-east-1
Asia Pacific (Tokyo)	ap-northeast-1
Asia Pacific (Seoul)	ap-northeast-2
Asia Pacific (Osaka)	ap-northeast-3
Asia Pacific (Mumbai)	ap-south-1
Asia Pacific (Hyderabad)	ap-south-2
Asia Pacific (Singapore)	ap-southeast-1
Asia Pacific (Sydney)	ap-southeast-2
Asia Pacific (Jakarta)	ap-southeast-3
Asia Pacific (Melbourne)	ap-southeast-4
Canada (Central)	ca-central-1

Region Name	Region Code
Canada (Western)	ca-west-1
Europe (Frankfurt)	eu-central-1
Europe (Zurich)	eu-central-2
Europe (Stockholm)	eu-north-1
Europe (Milan)	eu-south-1
Europe (Spain)	eu-south-2
Europe (Ireland)	eu-west-1
Europe (London)	eu-west-2
Europe (Paris)	eu-west-3
Israel (Tel Aviv)	il-central-1
Middle East (UAE)	me-central-1
Middle East (Bahrain)	me-south-1
South America (Sao Paulo)	sa-east-1
US East (N. Virginia)	us-east-1
US East (Ohio)	us-east-2
US West (Northern California)	us-west-1
US West (Oregon)	us-west-2

Cost

> **Note**
>
> You are responsible for the cost of the AWS services used while running this solution. As of this revision, the cost for running this solution with the default settings in the US East (N. Virginia) Region is approximately **$45 per month**, based on the assumptions in Sample cost table.
> Refer to the pricing webpage for each AWS service used in this solution.

We recommend creating a budget through AWS Cost Explorer to help you manage costs. Prices are subject to change. For full details, refer to the pricing webpage for each AWS service used in this solution.

Sample cost table

The following table provides a sample cost breakdown for deploying this solution with the default parameters in the US East (N. Virginia) Region for one month.

The cost is based on the following assumptions:

- You are assessing 100 AWS accounts in 10 AWS Regions
- You are running each assessment type 30 times a month
- In each account you have a total of 1,000 policies
- You conduct on average 100 searches per month with the Policy Explorer
- You are creating 1 Cognito user

AWS service	Dimensions	Variable or fixed	Cost [USD]
Amazon API Gateway	3,000 REST API calls per month	variable	<$0.01
Amazon Cognito	1 active user per month without the	variable	<$0.01

AWS service	Dimensions	Variable or fixed	Cost [USD]
	advanced security feature		
Amazon CloudFront	1,000 requests	variable	<$1.00
Amazon S3	<1 GB storage	variable	<$1.00
AWS Lambda	90,000 requests with 1,000 ms average duration	variable	<$1.00
AWS Step Functions	189,000 state transitions	variable	$4.73
Amazon DynamoDB	20 million read capacity units, 15 million write capacity units, 0.5 GB storage	variable	$23.88
AWS WAF	1 web ACL, 1 custom rule, 7 managed rule groups	fixed	$13.00
AWS X-Ray	~150 traces recorded (3,000 API calls with default 5% sampling rate)	variable	<$0.01
		Total monthly cost:	**$44.64**

Security

When you build systems on AWS infrastructure, security responsibilities are shared between you and AWS. This shared responsibility 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 AWS Cloud Security.

> **Warning**
>
> Make sure to follow the guideline in the AWS account structure section when choosing hub and spoke accounts to install the solution in.

IAM roles

IAM roles allow you to assign granular access policies and permissions to services and users on the AWS Cloud. This solution creates IAM roles that grant the solution's Lambda functions access to create Regional resources.

Amazon CloudFront

This solution deploys a web console hosted in an Amazon S3 bucket. To help reduce latency and improve security, this solution includes a CloudFront distribution with an origin access identity, which is a CloudFront user that provides public access to the solution's website bucket contents. For more information, refer to Restricting access to an Amazon S3 origin in the *Amazon CloudFront Developer Guide*.

> **Note**
>
> If you require Transport Layer Security (TLS) 1.2, you can configure a custom domain (also called an alternate domain name) in CloudFront and API Gateway.

Amazon DynamoDB

All user data stored in DynamoDB is encrypted at rest using encryption keys stored in AWS KMS. We recommend enforcing AWS Managed Keys because they will allow you to audit key usage. Refer to Managing encrypted tables in DynamoDB for more information.

AWS WAF

AWS WAF is a web application firewall that helps protect web applications and APIs from attacks. It allows you to configure a web ACL that allows, blocks, or counts web requests based on

configurable web security rules and conditions that you define. For more information, refer to How AWS WAF Works.

You can use AWS WAF to protect your API Gateway API from common web exploits, such as SQL injection and XSS attacks. These types of attacks could affect API availability and performance, compromise security, or consume excessive resources. For example, you can create rules to allow or block requests from specified IP address ranges, requests from Classless Inter-Domain Routing (CIDR) blocks, requests that originate from a specific country or Region, requests that contain malicious SQL code, or requests that contain malicious script.

AWS Account Structure

Follow these guidelines when setting up accounts for each stack:

Hub Account

The Hub stack contains all compute and storage resources of the solution to facilitate scans. Select a member account within your AWS Organization to deploy the Hub stack. Since this account will have read access to resource names and policies in all spoke accounts, including bucket names and secret names, choose an account that you protect as carefully as the most sensitive target account you intend to scan.

Important: Avoid using the Organizations management account as your Hub account, as it's best practice to keep the management account free from operational workloads.

Spoke Accounts

Deploy the Spoke stack to any member account within your AWS Organization that requires assessment, including the Hub account itself. This stack consists of a single IAM role that grants read access to the policies of all supported services.

For efficient deployment across multiple AWS accounts, consider using CloudFormation StackSets.

Organizations Management Account

The Org-Management stack must be deployed in your Organizations management account. This stack consists of a single IAM role that will be assumed by the Hub stack's Lambda function and grants minimal required permissions to access data of the Organization. This role enables: -

Reading account information (listing accounts and their parent relationships) - Reading Delegated Administrator configurations and their services - Viewing AWS service access settings for the Organization - Reading and listing Organization policies

Quotas

Service quotas, also referred to as limits, are the maximum number of service resources or operations for your AWS account.

Quotas for AWS services in this solution

Make sure you have sufficient quota for each of the services implemented in this solution. For more information, refer to AWS service quotas.

Select one of the following links to go to the page for that service. To view the service quotas for all AWS services in the documentation without switching pages, view the information in the Service endpoints and quotas page in the PDF instead.

- Lambda
- Step Functions
- DynamoDB
- API Gateway
- Amazon S3
- Amazon CloudFront
- Cognito
- AWS WAF
- AWS X-Ray

AWS CloudFormation quotas

Your AWS account has AWS CloudFormation quotas that you should be aware of when launching the stack in this solution. By understanding these quotas, you can avoid limitation errors that would prevent you from deploying this solution successfully. For more information, refer to AWS CloudFormation quotas in the in the *AWS CloudFormation Users Guide*.

AWS Lambda quotas

In the hub account, the Step Function invokes up to 100 Lambda functions to run the scan in parallel across multiple accounts and services. Review and increase your Lambda funtion's concurrency limit to avoid throttling.

AWS Step Functions quotas

A Step Function execution failure can occur due to maximum input or output size for a task, state, or execution quota of 262,144 bytes of data as a UTF-8 encoded string, or maximum execution history size of 25,000 events in a single state machine execution history. For example:

- **Scenario 1** - You scan resources in 25 supported services with a maximum of 100 accounts in a job. If you increase the number of accounts, you will reach maximum execution history size of 25,000 events.
- **Scenario 2** - You scan 8,000 accounts with a maximum of 3 services in a job. If you add more accounts, you will reach maximum input or output size for a task, state, or execution quota of 262,144 bytes of data.

To avoid reaching the quota for large-scale scans, we recommend that you define your batch size (number of accounts • number of services) per scan.

Deploy the solution

This solution uses CloudFormation templates and stacks to automate its deployment. The CloudFormation templates specify the AWS resources included in this solution and their properties. The CloudFormation stack provisions the resources that are described in the templates.

Important

We designed this solution to aggregate scan findings for customers. This solution does not check the validity or correctness of your underlying resource-based policies. When changing policies that allow account migration to another AWS Organization, we recommend:

- Verifying that your policies work as intended before making changes.
- Using IAM Access Analyzer to verify that your policies achieve your desired permissions.
- Reviewing and updating the `Condition` policy element to meet your security requirements. Do not delete the `Condition` without reviewing the underlying impact.
- Engaging with AWS Solutions Architects, Technical Account Managers, and AWS Professional Services to review your AWS Organizations-based dependencies identified by the solution before initiating account migration.

Note

Dependencies outside the scope of this solution can impact the account migration between AWS Organizations (for example, quotas for AWS Organizations, resources shared by AWS RAM, and service-managed CloudFormation StackSets).

Deployment process overview

Important

This solution includes an option to send anonymized operational metrics to AWS. We use this data to better understand how customers use this solution and related services and

products. AWS owns the data gathered though this survey. Data collection is subject to the AWS Privacy Notice.

To opt out of this feature, download the template, modify the CloudFormation mapping section, and then use the CloudFormation console to upload your updated template and deploy the solution. For more information, see the Anonymized data collection section of this guide.

Before you launch the solution, review the cost, architecture, security, and other considerations discussed in this guide. Follow the step-by-step instructions in this section to configure and deploy the solution into your account.

Time to deploy: Approximately 30-45 minutes

Step 1: Launch the Hub stack

- Launch the AWS CloudFormation template in your Hub account.
- Enter values for the required parameters.
- Review the other template parameters and adjust, if necessary.

Step 2: Launch the Spoke stack

- Launch the AWS CloudFormation template in your Spoke accounts. Consider CloudFormation StackSets to deploy at scale.
- Enter values for the required parameters.
- Review the other template parameters and adjust, if necessary.

Step 3: Launch the Org-Management stack

- Launch the AWS CloudFormation template in your Organizations management account.
- Enter values for the required parameters.
- Review the other template parameters and adjust, if necessary.

AWS CloudFormation templates

You can download the CloudFormation templates for this solution before deploying it.

Hub stack

View template

account-assessment-for-aws-organizations-hub.template - Use this template to launch the solution and all associated components in your hub account. The default configuration deploys the AWS services in this solution and the solution web UI to view the findings, but you can customize the template to meet your specific needs.

Spoke stack

View template

account-assessment-for-aws-organizations-spoke.template - Use this template to launch the solution and all associated components in your spoke account. The default configuration deploys IAM roles.

Org-Management stack

View template

account-assessment-for-aws-organizations-org-management.template - Use this template to create an IAM role in you AWS Organizations management account. The hub account requires the role to find account IDs, delegated admin accounts, and trusted access services in your AWS Organizations.

> **Note**
>
> AWS CloudFormation resources are created from AWS Cloud Development Kit (AWS CDK) constructs.

This AWS CloudFormation template deploys the Account Assessment for AWS Organizations solution in the AWS Cloud.

Prerequisites

When your accounts are part of AWS Organizations, you must manually activate AWS RAM in the Organizations console and obtain the AWS Organizations management account ID and organization ID before deploying the Account Assessment for AWS Organizations templates.

Activate AWS RAM for AWS Organizations accounts

Follow the instructions to Enable resource sharing within AWS Organizations in the *AWS Organizations Resource access Manager User Guide.*

Step 1: Launch the Hub stack

> **Important**
>
> Launch the Hub stack before launching the Spoke stack and Org-Management stack.

Follow the step-by-step instructions in this section to configure and deploy the solution into your Hub account.

Time to deploy: Approximately 20 minutes

1. Sign in to the AWS Management Console and select the button to launch the `account-assessment-for-aws-organizations-hub.template` CloudFormation template.

1. The template launches in the US East (N. Virginia) Region by default. To launch the solution in a different AWS Region, use the Region selector in the console navigation bar.

> **Note**
>
> This solution uses Amazon Cognito that is not currently available in all AWS Regions. You must launch this solution in an AWS Region where Amazon Cognito is available. For the most current availability of AWS services by Region, refer to the AWS Regional Services List.

2. On the **Create stack** page, verify that the correct template URL is in the **Amazon S3 URL** text box, and choose **Next**.
3. On the **Specify stack details** page, assign a name to your solution stack. For information about naming character limitations, refer to IAM and AWS STS quotas, name requirements, and character limits in the *AWS Identity and Access Management User Guide*.
4. Under **Parameters**, review the parameters for this solution template and modify them as necessary. This solution uses the following default values.

Parameter	Default	Description
Solution Setup		
Provide the unique namespace value	*<Requires input>*	Chose a unique string as prefix for resource names. NOTE: Use the same namespace in the Spoke stack and Org-Management stack.
DynamoDB Configuration		
Provide Time to live (in days) for DynamoDB items	90	Time period in days all DynamoDB tables will delete stored items.
Web UI Configuration		
Provide Web UI Login User Email	*<Requires input>*	Admin user will be created at deployment time. Provide an email address to create this initial Cognito user.
Provide a prefix for the hosted Amazon Cognito domain	*<Requires input>*	Pick a globally unique prefix to become part of the url of the login page (Cognito Hosted UI)

Parameter	Default	Description
Set MFA for Cognito to "ON" or "OPTIONAL"	*<Optional input>*	`ON` - Amazon Cognito users will need to set up multi-factor authentication (MFA) on first login. `OPTIONAL` - Amazon Cognito users may opt to set up MFA
Security Configuration		
Provide CIDR ranges that allow the console to access the API	*`<Requires input>`*	Comma separated list of CIDR ranges that allow access to the API. To allow the entire internet, use the following list of two CIDR blocks as the value: `0.0.0.0/1,128.0.0.0/1`
Application Manager Configuration		
Provide the AWS Organization ID	*<Requires input>*	Organization ID to support multi-account deployment. Leave blank for single account deployments.
Management Account ID	*<Optional input>*	Account ID for the management account of the AWS Organization. Leave blank for single account deployments.

5. Choose **Next***
6. On the **Configure stack options** page, choose **Next**.
7. On the **Review and create** page, review and confirm the settings. Check the box acknowledging that the template will create IAM resources.

8. Choose **Submit** to deploy the stack.

   You can view the status of the stack in the AWS CloudFormation console in the **Status** column. You should receive a `CREATE_COMPLETE` status in approximately five minutes.

> **Note**
>
> In addition to its primary Lambda functions, this solution includes the `solution-helper` Lambda function, which runs only during initial configuration or when resources are updated or deleted.
> When you run this solution, you will notice all Lambda functions in the AWS console. Only the primary functions are regularly active. However, you must not delete the `solution-helper` function, as it is necessary to manage associated resources.

Step 2: Launch the Spoke stack

Follow the step-by-step instructions in this section to configure and deploy the solution into your Spoke account.

Time to deploy: Approximately 5 minutes

1. Sign in to the AWS Management Console and select the button to launch the account-assessment-for-aws-organizations-spoke.template CloudFormation template.

2. Launch in the same region as the Hub stack.

Parameter	Default	Description
Solution Setup		
Provide the unique namespace value	*<Requires input>*	Enter the namespace value you chose for the Hub stack.

Parameter	Default	Description
Provide the Hub Account Id	*<Requires input>*	ID of the AWS account where the Hub stack of this solution is deployed.
Application Manager Configuration		
Create Resource Association	Yes	Select No if you did not provide Application Manager Configuration details in the Hub stack.

1. Choose **Next**.
2. On the **Configure stack options** page, choose **Next**.
3. On the **Review and create** page, review and confirm the settings. Check the box acknowledging that the template will create IAM resources.
4. Choose **Submit** to deploy the stack.

   You can view the status of the stack in the CloudFormation console in the **Status** column. You should receive a CREATE_COMPLETE status in approximately five minutes.

Step 3: Launch the Org-Management stack

Follow the step-by-step instructions in this section to configure and deploy the solution into your Organizations management account.

Time to deploy: Approximately 5 minutes

1. Sign in to the AWS Management Console and select the button to launch the `account-assessment-for-aws-organizations-org-management.template` CloudFormation template.

   Launch solution

2. Launch in the same region as the Hub stack.

Parameter	Default	Description
Solution Setup		
Enter the namespace value you chose for the Hub stack.	*<Requires input>*	Unique string used as prefix for resource names. NOTE: Use the same namespace in the Hub stack and Spoke stack.
Provide the Hub Account Id	*<Requires input>*	ID of the AWS account where the Hub stack of this solution is deployed.
Application Manager Configuration		
Create Resource Association	`Yes`	Select `No` if you did not provide Application Manager Configuration details in the Hub stack.

1. Choose **Next**.
2. On the **Configure stack options** page, choose **Next**.
3. On the **Review and create** page, review and confirm the settings. Check the box acknowledging that the template will create IAM resources.
4. Choose **Submit** to deploy the stack.

   You can view the status of the stack in the CloudFormation console in the **Status** column. You should receive a `CREATE_COMPLETE` status in approximately five minutes.

Update the solution

From version v1.1.0 on, we improved the generation of the Cognito UserPool name and the AppRegistry application name to make it less likely that your deployment fails due to a name conflict. As these changes are not backwards compatible, it is not possible to update the v1.0.x Hub stack to v1.1.x in place.

If you have v1.0.x installed in your account, and you want to start using v1.1.x, take the following steps:

- Undeploy the CloudFormation stacks of your v1.0.x installation
- Before deleting the UserPool, check if there are any users (except from the default user created at deployment time) that you need to re-create in the new UserPool. Note their email addresses if needed.
- Delete the UserPool, S3 buckets and DynamoDB tables of your v1.0.x installation. As your scan data are stale, you do not need to migrate any data to the new solution version. You will be able to run a fresh scan after installing the new solution version. See uninstall instructions for details.
- Choose a new "namespace" and install v1.1.x freshly in your accounts, following the deployment instructions in this guide.

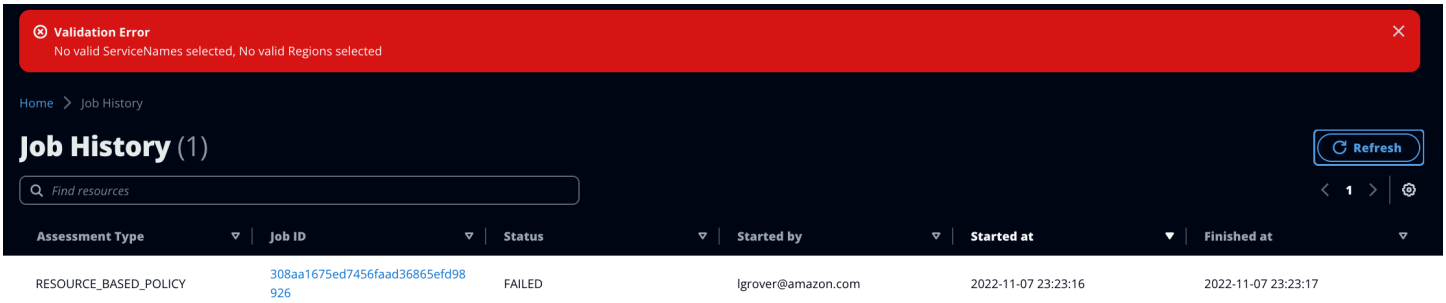
Troubleshooting

This section provides troubleshooting instructions for deploying and using the solution.

If these instructions don't address your issue, Contact AWS Support provides instructions for opening an AWS Support case for this solution.

Problem: Failed job

If a job fails for any of the assessments, the web UI will display an error message, and the **Job History** page will show the status of the job as `FAILED`.



Resolution

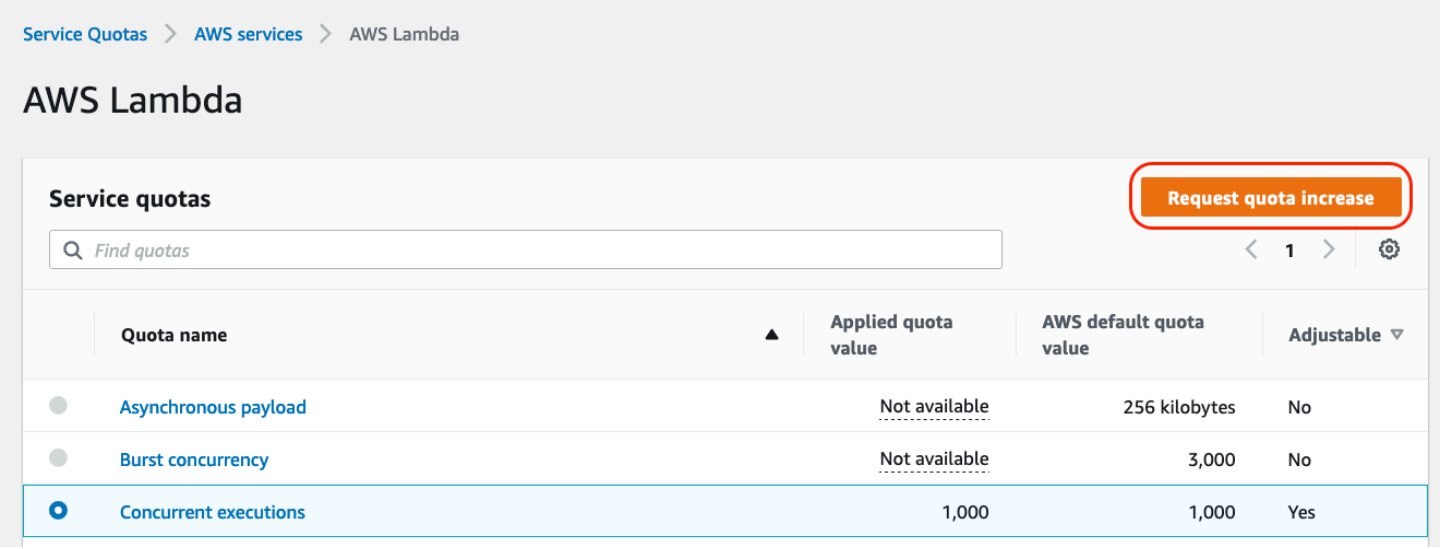
If you wish to determine the failure's root cause, you can use X-Ray traces to identify the resource that returned the error code. For example, if a Lambda function has failed to retrieve the list of delegated admin accounts, the X-Ray trace will direct you to the Lambda function and respective CloudWatch logs. Then you can examine the logs to determine the root cause. In addition, X-Ray service maps identify services where errors are occurring, connections with high latency, or traces for requests that were unsuccessful. These maps can be helpful, for example, when investigating APIs and their downstream services.

For example, if your job failed due to the following error:

```
"Error": "Lambda.TooManyRequestsException"
"Cause": "Rate Exceeded
```

this indicates that you need to check the Lambda function concurrent executions quota for the hub account. By default, this solution requires up to 100 Lambda concurrent executions. To request a

quota increase, select **Concurrent executions** and choose **Request quota increase**. See Requesting a quota increase in the *Service Quotas User Guide* for more information.

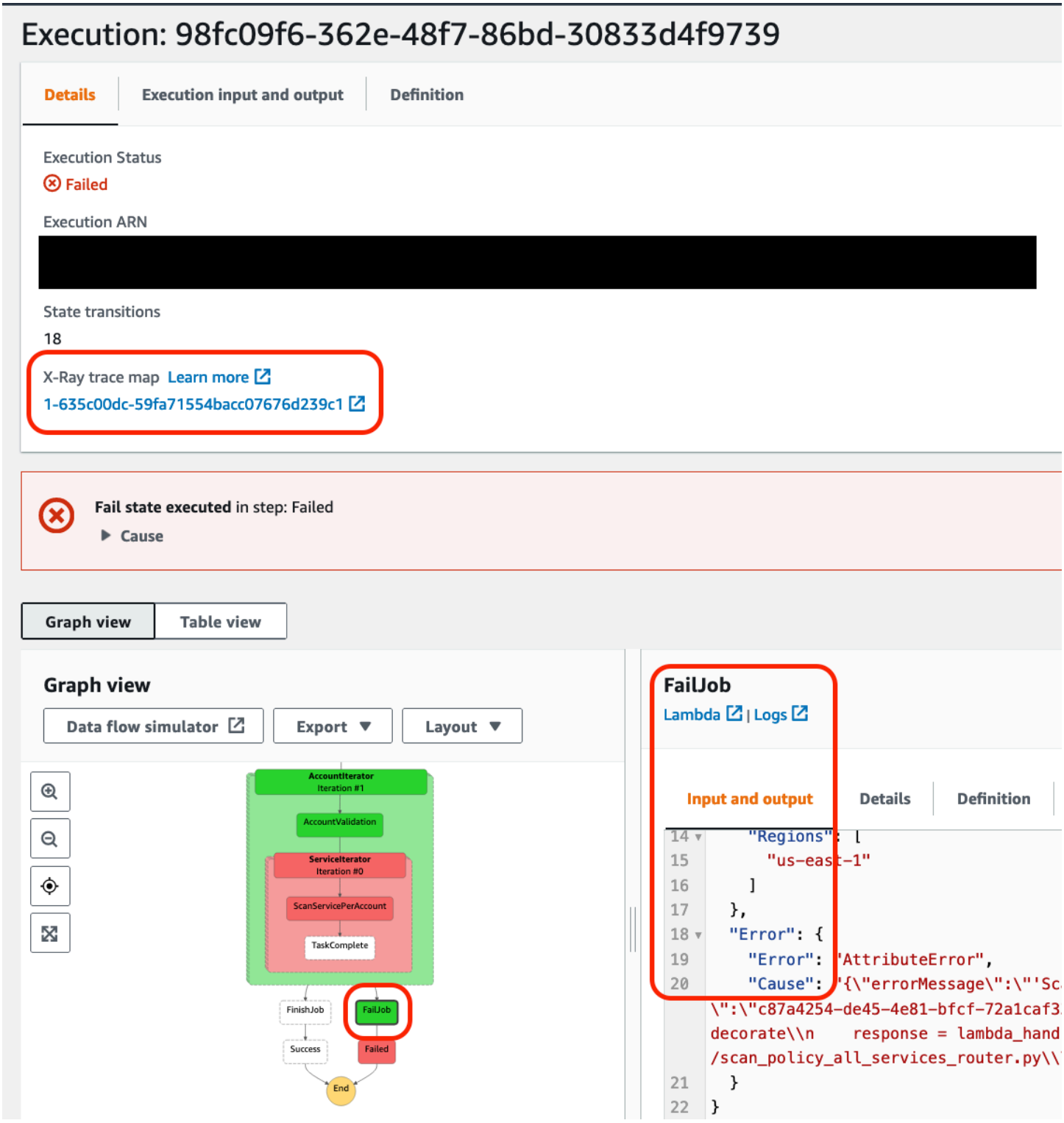


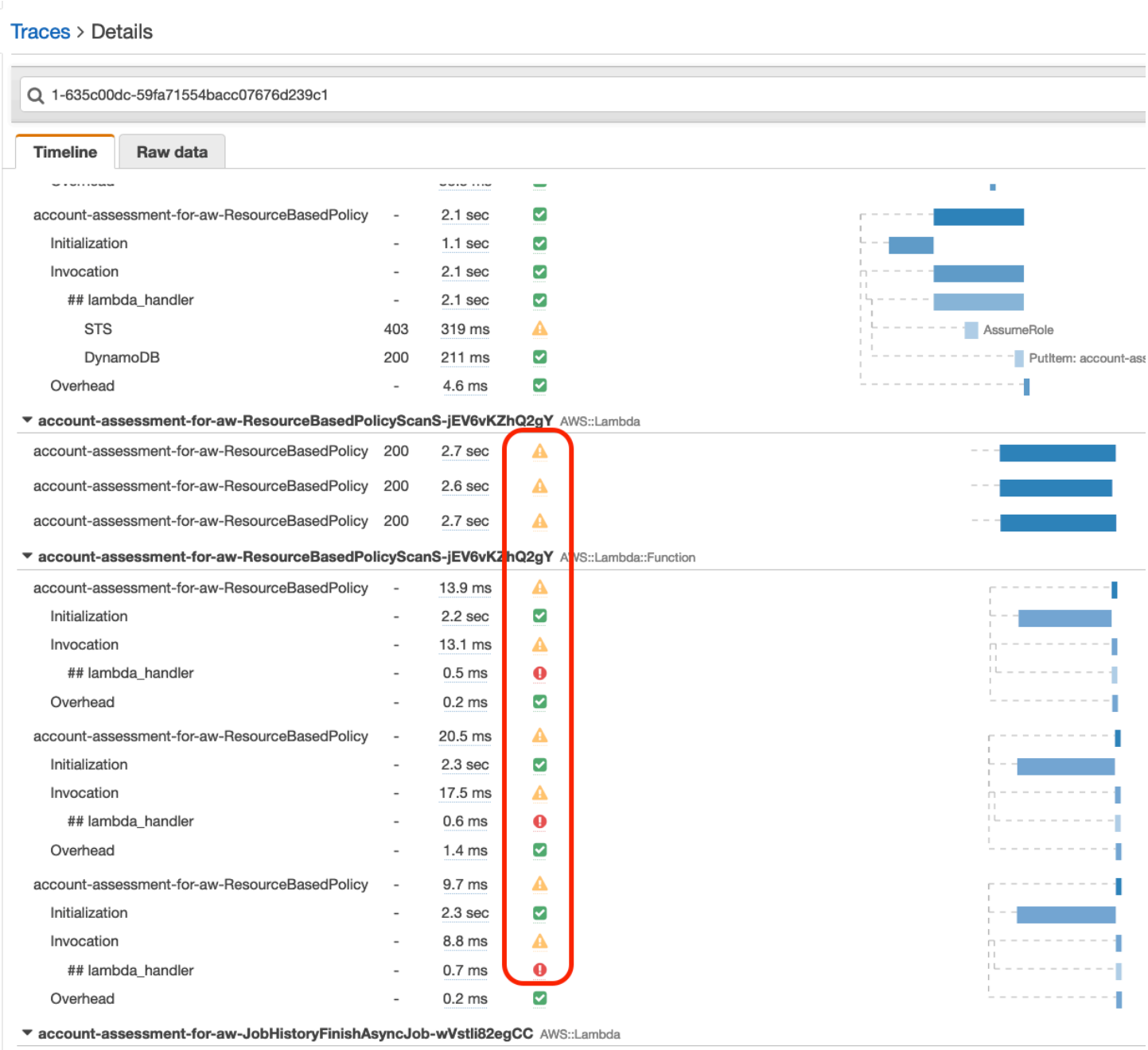
Problem: Failed Resource-Based Policies scan

This assessment type initiates an asynchronous Step Functions state machine execution to scan the resources in the spoke and member accounts.

Resolution

If the state machine execution fails, you can view the specific X-Ray trace for the failed state machine execution. You can either click on the state machine **FailJob** state to view the details in the **Input and Output** tab (see Figure 2) or use the X-Ray details to help you identify the specific resource in the state machine where the failure occurred (see Figure 3).


Execution: 98fc09f6-362e-48f7-86bd-30833d4f9739
Details
Execution input and output
Definition
Execution Status
Failed
Execution ARN
State transitions
18
X-Ray trace map Learn more
1-635c00dc-59fa71554bacc07676d239c1
Fail state executed in step: Failed
Cause
Graph view
Table view
Graph view
Data flow simulator
Export
Layout
AccountIterator
Iteration #1
AccountValidation
ServiceIterator
Iteration #0
ScanServicePerAccount
TaskComplete
FinishJob
FailJob
Success
Failed
End
FailJob
Lambda | Logs
Input and output
Details
Definition
"Regions": [
"us-east-1"
],
"Error": {
"Error": "AttributeError",
"Cause": "{\"errorMessage\":\"'Sc
\":\"c87a4254-de45-4e81-bfcf-72a1caf3
decorate\\n response = lambda_hand
/scan_policy_all_services_router.py\\
}
}



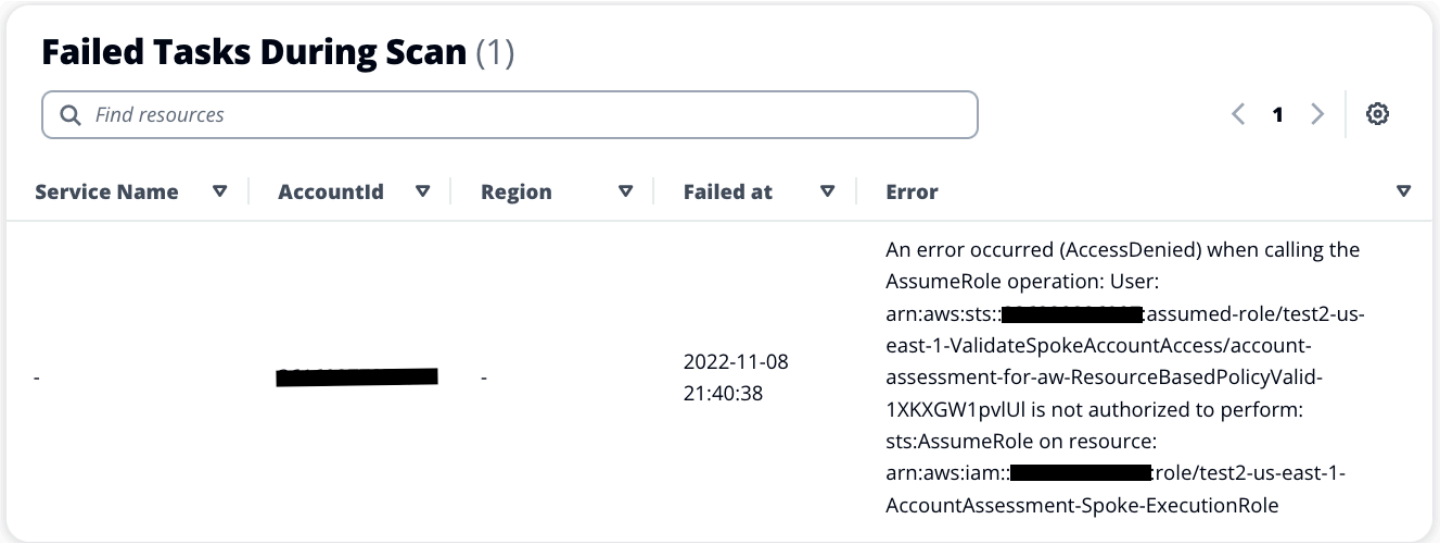
To view the error details, click on the resource and select the **Exceptions** tab. This can help you identify the Lambda function name where the failure occurred and will display the same error from the state machine output. Note that the same exception will be logged in the CloudWatch logs.

Problem: Access denied

You may receive an `AccessDenied` error for a specific account in **Failed Tasks During Scan**.

Resolution

Deploy the Spoke stack in the account to allow the scan to complete.



Problem: Undefined error

The Web UI loads, but starting scans or viewing findings causes an `undefined error`.

Resolution

The Web UI may be blocked from calling the API Gateway by AWS WAF. Check if your current IP address is within the range of valid IP addresses that you defined for the AWS WAF. Then open the AWS WAF console to investigate what reason your requests are blocked.

Problem: Access denied after redeploying Hub Stack

If you delete and redeploy the Hub Stack while leaving Spoke Stacks and Org Management Stack in place, you will receive Access Denied errors. The trust policy in the spoke role and org management role references the Hub Stack. During deletion of the Hub Stack, IAM will break those references and redeploying the Hub Stack does not restore them.

Resolution

Delete and redeploy the Spoke Stacks and the Org Management Stack after redeploying the Hub Stack.

Contact AWS Support

If you have AWS Developer Support, AWS Business Support, or AWS Enterprise Support, you can use the Support Center to get expert assistance with this solution. The following sections provide instructions.

Create case

1. Sign in to Support Center.
2. Choose **Create case**.

How can we help?

1. Choose **Technical**.
2. For **Service**, select **Solutions**.

3. For **Category**, select **Other Solutions**.
4. For **Severity**, select the option that best matches your use case.
5. When you enter the **Service**, **Category**, and **Severity**, the interface populates links to common troubleshooting questions. If you can't resolve your question with these links, choose **Next step: Additional information**.

Additional information

1. For **Subject**, enter text summarizing your question or issue.
2. For **Description**, describe the issue in detail.
3. Choose **Attach files**.
4. Attach the information that AWS Support needs to process the request.

Help us resolve your case faster

1. Enter the requested information.
2. Choose **Next step: Solve now or contact us**.

Solve now or contact us

1. Review the **Solve now** solutions.
2. If you can't resolve your issue with these solutions, choose **Contact us**, enter the requested information, and choose **Submit**.

Uninstall the solution

You can uninstall the Account Assessment for AWS Organizations solution from the AWS Management Console or by using the AWS Command Line Interface (AWS CLI). You must manually delete the Amazon Cognito user pool, DynamoDB tables, CloudWatch logs, and Amazon S3 bucket created by this solution. AWS Solutions Implementations do not automatically delete these resources in case you have stored data to retain.

Using the AWS Management Console

1. Sign in to the AWS CloudFormation console.
2. On the **Stacks** page, select this solution's installation stack.
3. Choose **Delete**.

Using AWS Command Line Interface

Determine whether the AWS Command Line Interface (AWS CLI) is available in your environment. For installation instructions, refer to What Is the AWS Command Line Interface in the *AWS CLI User Guide*. After confirming that the AWS CLI is available, run the following command for each of the Hub, Spoke, and Org-Management stacks.

```
$ aws cloudformation delete-stack --stack-name <stack-name>
```

Deleting the Amazon Cognito user pool

To prevent accidental data loss, this solution is configured to retain the solution-created Amazon Cognito user pool if you decide to delete the CloudFormation stack. After uninstalling the solution, you can manually delete the user pool if you do not need to retain the data. Follow these steps:

1. Sign in to the Amazon Cognito console to access the **User Pools** tab.
2. Choose the user pool named `account-assessment-for-aws-organizations-hub*`.

> **Note**
>
> During deployment, the stacks may truncate the user pool name (for example, `account-assess*`).

3. On that user pool's page, choose **Delete pool**.

Deleting the DynamoDB tables

To prevent accidental data loss, this solution is configured to retain the solution-created DynamoDB tables if you decide to delete the CloudFormation stack. After uninstalling the solution, you can manually delete these DynamoDB tables if you do not need to retain the data. Follow these steps:

1. Sign in to the DynamoDB console.
2. Choose **Tables** from the left navigation pane.
3. Select the `account-assessment-for-aws-organizations-hub*` table and choose **Delete**.

> **Note**
>
> During deployment, the stacks may truncate the user pool name (for example, `account-assess*`).

To delete the DynamoDB tables using AWS CLI, run the following command:

```
$ aws dynamodb delete-table <table-name>
```

Deleting the CloudWatch logs

To prevent accidental data loss, this solution is configured to retain the solution-created CloudWatch logs if you decide to delete the CloudFormation stack. After uninstalling the solution, you can manually delete the logs if you do not need to retain the data. Follow these steps:

1. Sign in to the Amazon CloudWatch console.
2. Choose **Log Groups** from the left navigation pane.

3. Locate the log groups created by the solution.
4. Select one of the log groups.
5. Choose **Actions** and then choose **Delete**.

Repeat the steps until you have deleted all the solution log groups.

Deleting the Amazon S3 bucket

To prevent accidental data loss, this solution is configured to retain the solution-created Amazon S3 bucket (for deploying in an opt-in Region) if you decide to delete the CloudFormation stack . After uninstalling the solution, you can manually delete this Amazon S3 bucket if you do not need to retain the data. Follow these steps:

1. Sign in to the Amazon S3 console.
2. Choose **Buckets** from the left navigation pane.
3. Locate the `account-assessment-for-aws-organizations-hub*` Amazon S3 bucket.

> **Note**
>
> During deployment, the stacks may truncate the user pool name (for example, `account-assess*`).

4. Select the S3 bucket and choose **Delete**.

To delete the Amazon S3 bucket using AWS CLI, run the following command:

```
$ aws s3 rb s3://<bucket-name> --force
```

Use the solution

> **Note**
>
> Dependencies outside the scope of this solution can impact the account migration between AWS Organizations (for example, quotas for AWS Organizations, resources shared by AWS RAM, and service-managed CloudFormation StackSets).

Login page

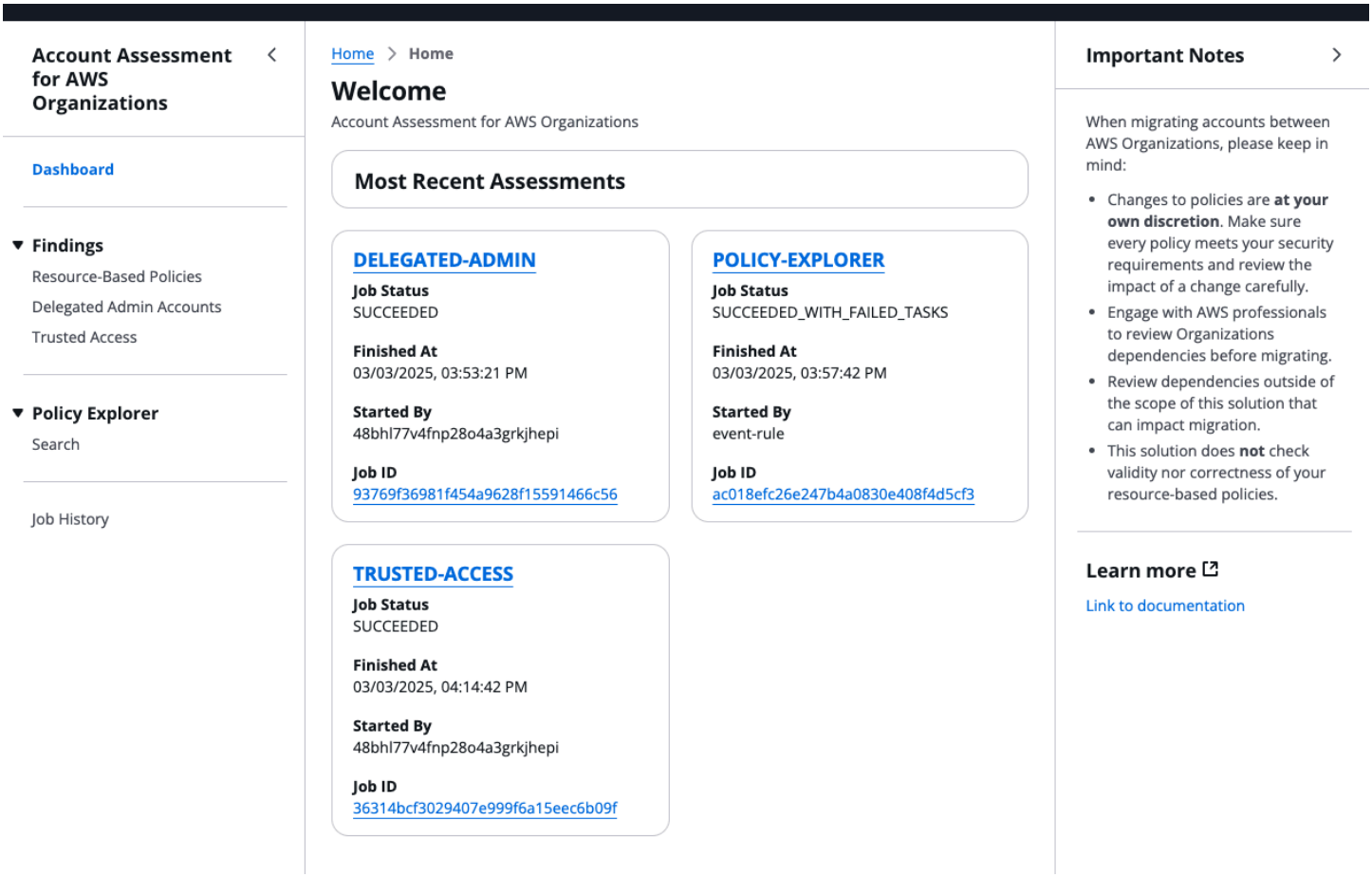
At the email address you provided for the `Provide Web UI Login User Email` input when you launched the Hub stack, you will receive an email with the subject **WebUI Credentials - Account Assessment for AWS Organizations** that contains the following:

- Your temporary login credentials
- The URL for the web UI

You may alternatively retrieve the web UI URL from the CloudFormation template outputs under `"WebUserInterfaceURL"`. To add or manage additional users, use the Cognito Service user interface in the AWS Console.

Welcome page

This page displays after you log in. If applicable, it shows your previous scan job status and assessment type for that job.



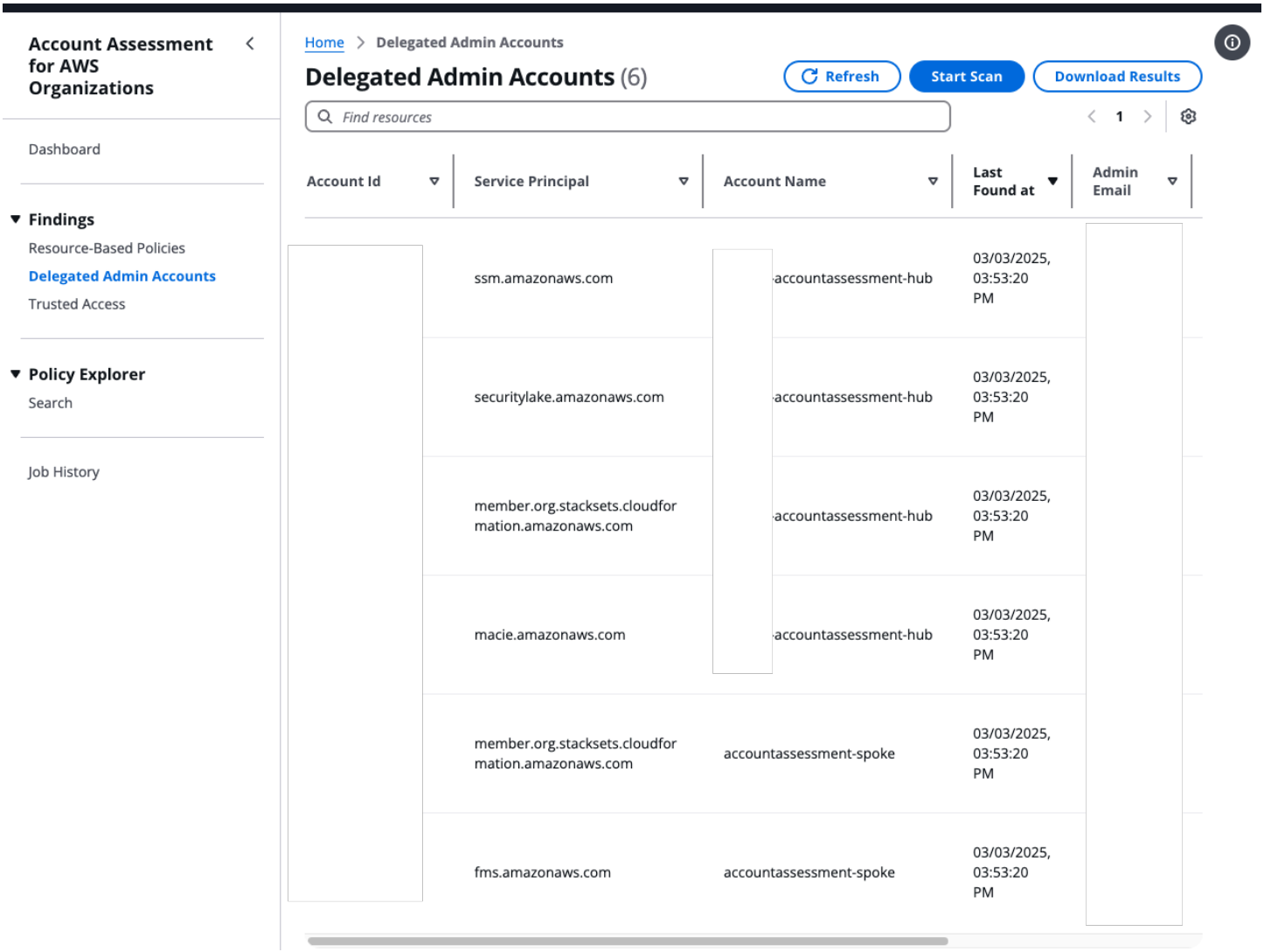
Findings

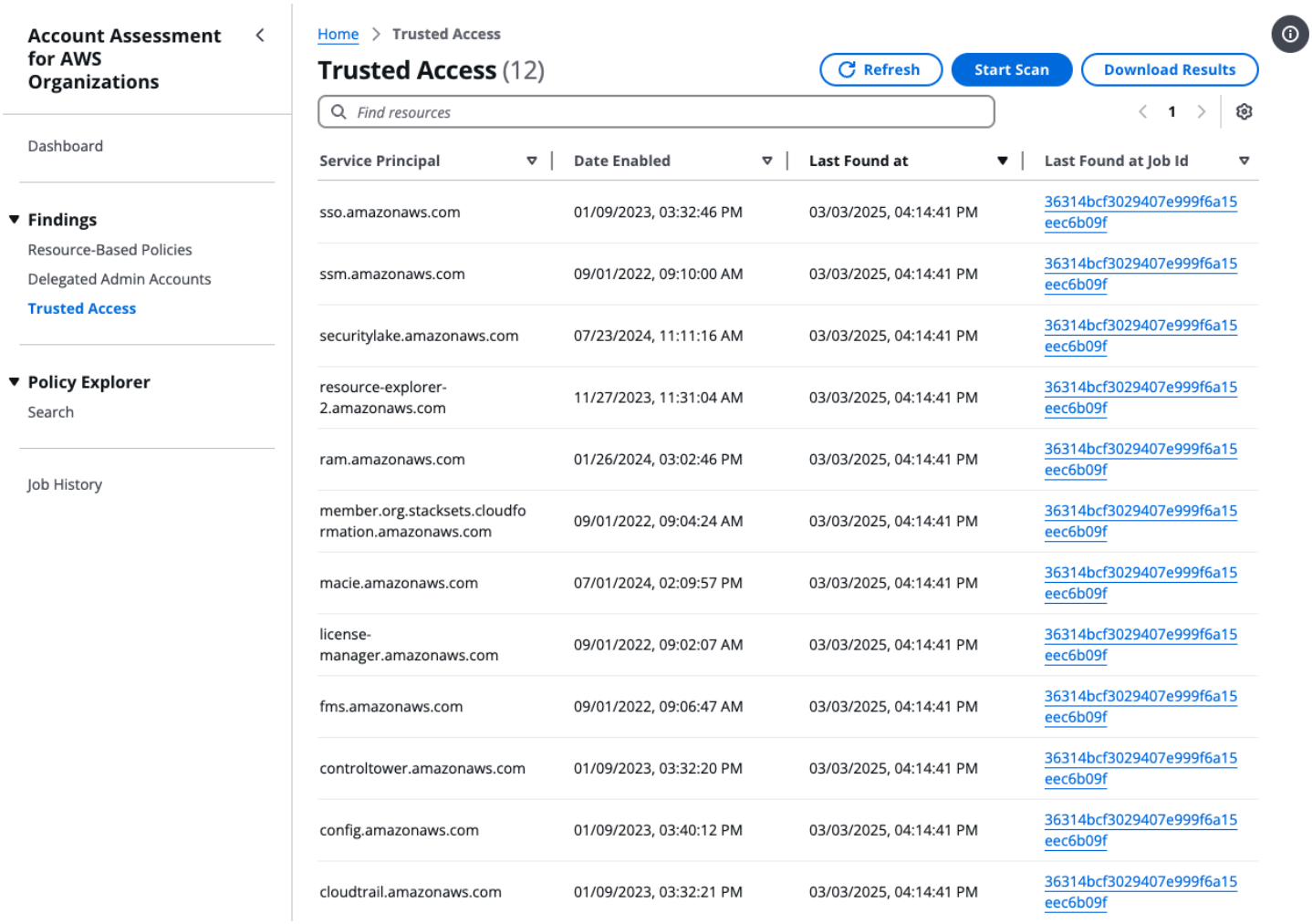
The left pane lists three types of assessments.

1. Resource-Based Polices (Deprecated, read-only page since v1.1.0)
2. Delegated Admin Accounts
3. Trusted Access

Begin an assessment by selecting **Start Scan or download the table content as .csv file by selecting Download Results**.

> **Note**
>
> You can run one active scan per assessment type at a time.

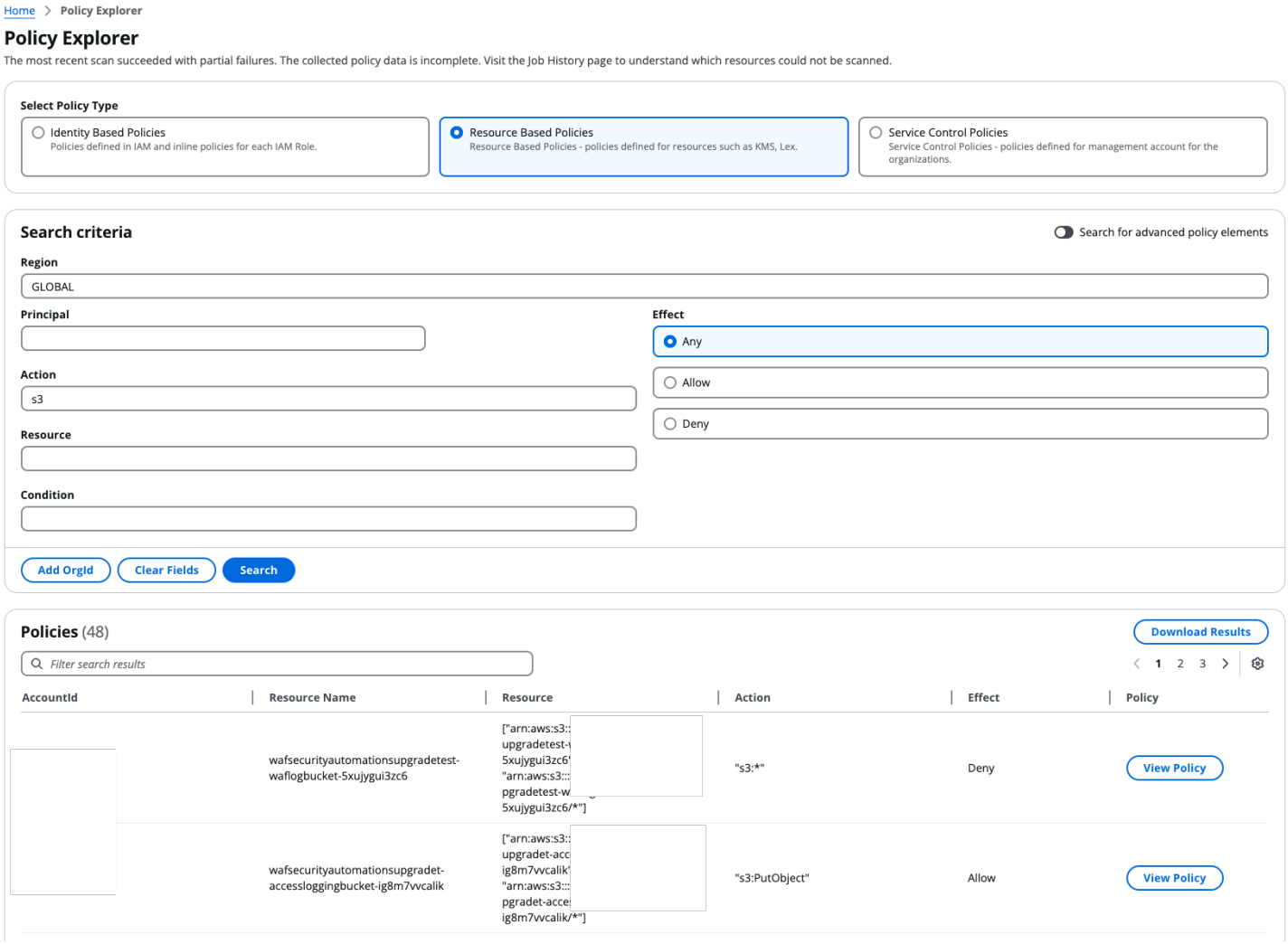

Account Assessment for AWS Organizations
Dashboard
Findings
Resource-Based Policies
Delegated Admin Accounts
Trusted Access
Policy Explorer
Search
Job History
Home
Delegated Admin Accounts
Delegated Admin Accounts (6)
Refresh
Start Scan
Download Results
Find resources
1
Account Id
Service Principal
Account Name
Last Found at
Admin Email
ssm.amazonaws.com
accountassessment-hub
03/03/2025, 03:53:20 PM
securitylake.amazonaws.com
accountassessment-hub
03/03/2025, 03:53:20 PM
member.org.stacksets.cloudformation.amazonaws.com
accountassessment-hub
03/03/2025, 03:53:20 PM
macie.amazonaws.com
accountassessment-hub
03/03/2025, 03:53:20 PM
member.org.stacksets.cloudformation.amazonaws.com
accountassessment-spoke
03/03/2025, 03:53:20 PM
fms.amazonaws.com
accountassessment-spoke
03/03/2025, 03:53:20 PM



Policy Explorer

Beginning with Account Assessment v1.1.0, the Policy Explorer allows you to conduct nuanced searches for policies in your AWS Organization.

> **Note**
>
> Policy Explorer runs a nightly scan for policies across your AWS Organization and stores a string representation of each policy in DynamoDB. Search results you see on the Policy Explorer page are not real-time, but based on the last successful scan. Consult the JobHistory page to find out when the last successful scan was conducted.



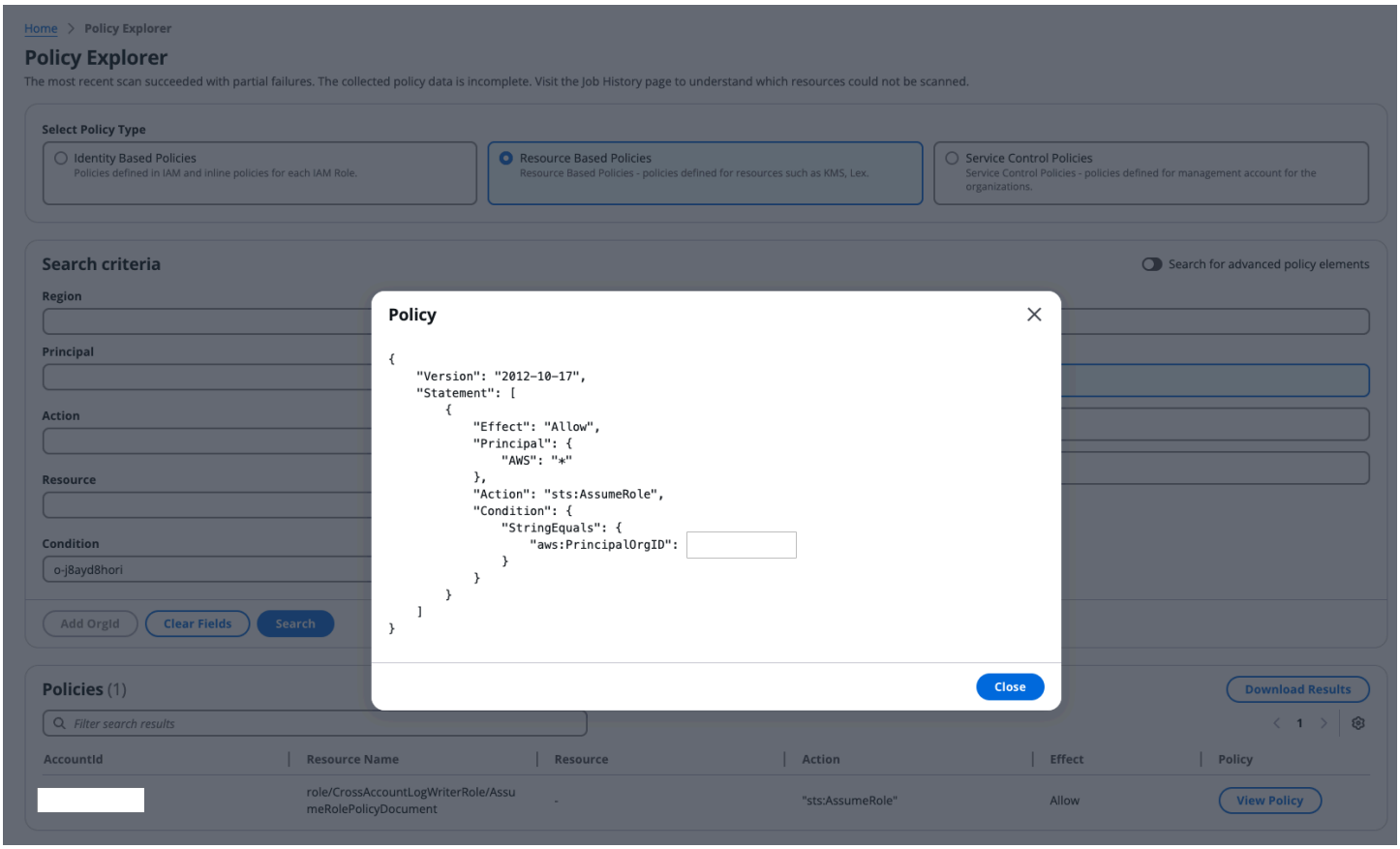
You can search for policies

- By type (Identity Based Policies, Resource Based Policies, Service Control Policies)
- By region. Use GLOBAL for region-independent policies
- By principal
- By action
- By resource
- By condition
- By effect (Allow, Deny or Both)

The matching strategy is `string contains`, e.g. a search input like `us-` will match policies in all us regions. The search criteria is applied server-side. If your search is too broad, and the amount

of result data exceeds what the frontend can handle, you will see a message asking you to narrow down the search with additional criteria.

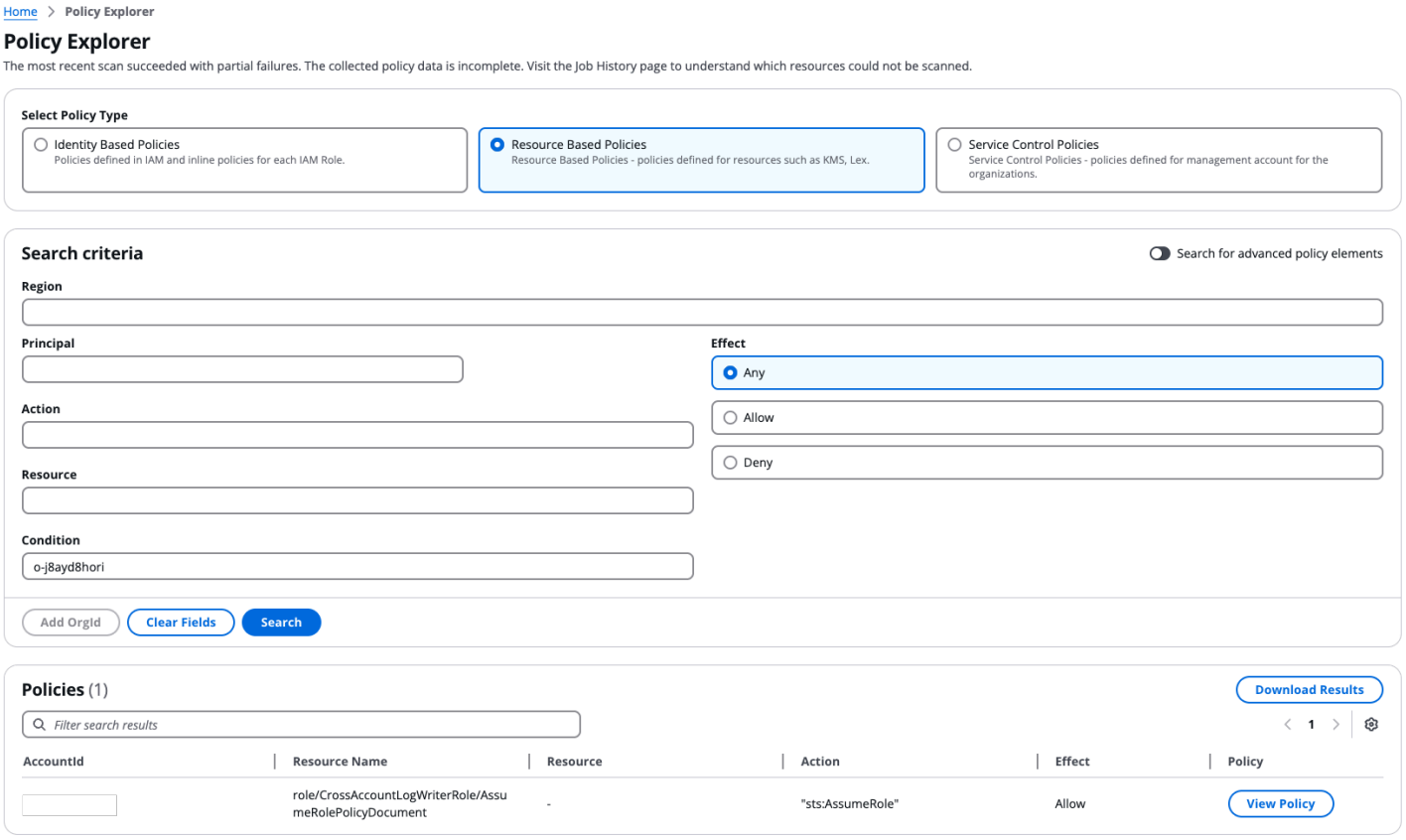
Use the `View Policies` button to see the full string representation of any policy.



Dependencies on your AWS Organization

A main use case of the "Resource-based Policy Scan" in Account Assessment prior to v1.1.0 was to find policies that contain a condition with the Organization ID, hinting at a policy that may break when the account is moved to a different AWS Organization.

This use case is now covered by PolicyExplorer. To search for Policies that contain your Organizational ID in the condition, press the button `Add OrgId` which will prepopulate the `Condition` search input field with your Org ID. Leave all other fields blank.

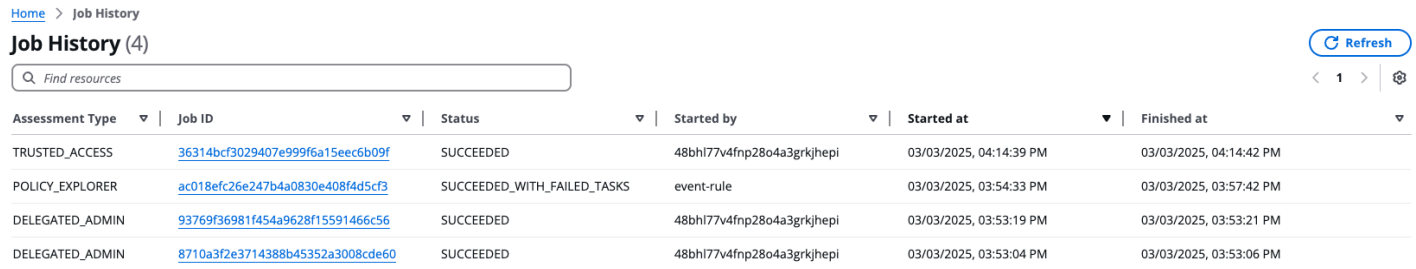


Job History

The Job History page helps you review the previous scans and their status. The solution provides four status possibilities:

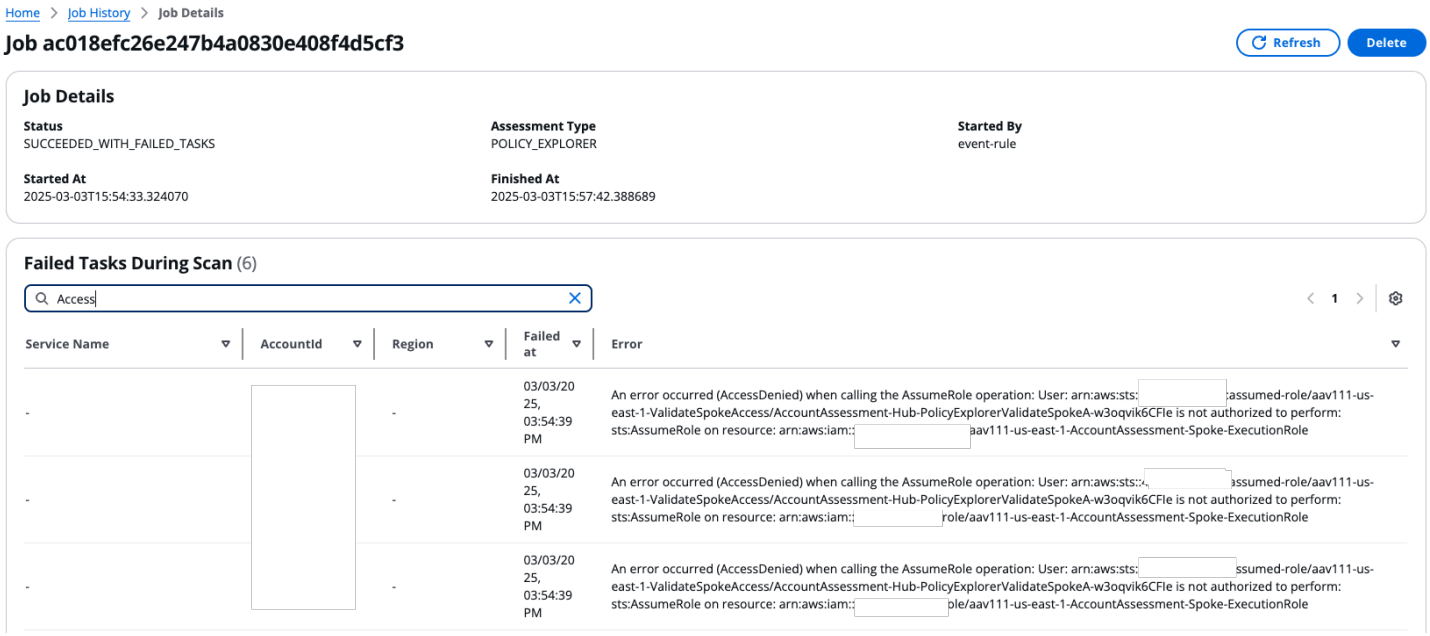
- **ACTIVE** – Scan is currently running
- **SUCCEEDED** – Scan completed successfully
- **SUCCEEDED_WITH_FAILED_TASKS** – Scan completed, but some tasks have errors
- **FAILED** – Scan failed

Select the **Job ID** to view specific findings per job.



When you select the **Job ID**, the Job Details page displays the findings and any failed tasks during your selected job. You can use this information to help you identify the resource and errors. If the error states that a certain account/region/service/resource could not be scanned, that means that there may be possible findings which the solution was not able to assess. Use your judgement to decide how to proceed.

The AccessDenied error often hints at the fact that the SpokeRole of the Account Assessment solution was not installed in the respective account, so the solution has no permission to access the account in question for a scan.



Next steps

We designed this solution to help you determine specific AWS Organizations dependencies in your underlying resource-based policies. It does not check the validity or correctness of these policies. There are myriad ways in which you can use this data, not limited to common use cases such as consolidating multiple AWS Organizations, preparing for a security audit, or changing your AWS Organization's management account.

Account migration

One of the common use cases for this solution is to help you plan for migrating your AWS Organizations accounts, such as with a company merger or acquisition. Migrating your accounts requires careful consideration. Specifically, we recommend:

- Verifying that your policies work as intended before making changes.
- Using IAM Access Analyzer to verify that your policies achieve your desired permissions.
- Reviewing and updating the `Condition` policy element to meet your security requirements. Do not delete the `Condition` without reviewing the underlying impact.
- Reviewing other dependencies outside the scope of this solution that can impact the account migration between AWS Organizations.

We recommend that you engage with AWS Solutions Architects, Technical Account Managers, and AWS Professional Services to review your AWS Organizations-based dependencies identified by the solution before initiating account migration. Additional resources include the following:

- How do I move accounts between organizations in AWS Organizations? – This blog post identifies some of the account, reporting, billing, and other considerations you will need to take when migrating accounts.
- Migrating accounts between AWS Organizations with consolidated billing to all features – This blog post provides further insights into consolidated billing and account migration.

Developer guide

This section provides the source code for the solution.

Source code

Visit our GitHub repository to download the source files for this solution and to share your customizations with others.

This solution's templates are generated using the AWS CDK. Refer to the README.md file for additional information.

Reference

This section includes information about an optional feature for collecting anonymized metrics for this solution and a list of builders who contributed to this solution.

Operational metrics

This solution includes an option to send anonymized operational metrics to AWS. We use this data to better understand how customers use this solution and related services and products.

When a Trusted Access or Delegate Admin scan is started, the following information is collected and sent to AWS:

- **Solution ID** – The AWS solution identifier
- **Unique ID (UUID)** – Randomly generated, unique identifier for each Account Assessment for AWS Organizations deployment
- **Timestamp** – Data-collection timestamp
- **Version** – Solution version deployed
- **Assessment type** – `DelegatedAdmin`, `TrustedAccess`
- **Findings count** – Number of findings found during scan
- **Services count** – Number of AWS services found during scan
- **Accounts count** – Number of accounts found during scan
- **Regions count** – Number of AWS Regions found during scan

When a search is conducted using the Policy Explorer, the following information is collected and sent to AWS:

Example data:

```
Solution ID: The AWS solution identifier
Unique ID (UUID) - Randomly generated, unique identifier for each Account Assessment
 for AWS Organizations deployment
Timestamp - Data-collection timestamp
Verion - Solution version deployed
Assessment type - "PolicyExplorerSearch"
Region - The region used as search filter
```

```
*Filters - The key for each search filter input, as well as the length of its input
 value.  The user entered value is not collected.*
```

AWS owns the data gathered through this survey. Data collection is subject to the AWS Privacy Policy. To opt out of this feature, complete the following steps before launching the Hub stack CloudFormation template:

1. Download the `account-assessment-for-aws-organizations-hub.template` AWS CloudFormation template to your local hard drive.
2. Open the CloudFormation template with a text editor.
3. Modify the CloudFormation template mapping section from:

   ```
   AnonymousData:
       SendAnonymousData:
         Data: Yes
   ```

   to:

   ```
   AnonymousData:
       SendAnonymousData:
         Data: No
   ```

4. Sign in to the AWS CloudFormation console.
5. Select **Create stack**.
6. On the **Create stack** page, **Specify template** section, select **Upload a template file**.
7. Under **Upload a template file**, select **Choose file**, then select the edited template from your local drive.
8. Choose **Next** and follow the steps in Launch the Hub stack.

Contributors

- Lalit Grover
- Thiemo Belmega
- Nikhil Reddy
- Mykhailo Markhain

Revisions

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.