Implementation Guide

Account Assessment for AWS Organizations

Account Assessment for AWS Organizations: Implementation Guide

Table of Contents

Solution overview 1
- Features and benefits 3
  - Access the solution using a web UI 3
  - Identify enabled services with AWS Organizations 3
  - Assess IAM policy conditions 3
  - Integration with AWS Service Catalog AppRegistry and Application Manager, a capability of AWS Systems Manager 6
- Use cases 6
- Concepts and definitions 6

Architecture overview 8
- Architecture diagram 8
- AWS Well-Architected design considerations 10
  - Operational excellence 10
  - Security 10
  - Reliability 11
  - Performance efficiency 11
  - Cost optimization 11
  - Sustainability 12
- AWS services 12

Plan your deployment 14
- Cost 14
  - Sample cost table 14
- Security 16
  - IAM roles 16
  - Amazon CloudFront 16
  - Amazon DynamoDB 16
  - AWS WAF 16
- Supported AWS Regions 17
- AWS accounts 17
- Quotas 18
  - Quotas for AWS services in this solution 18
  - AWS CloudFormation quotas 18
  - AWS Lambda quotas 19
  - AWS Step Functions quotas 19

Deploy the solution ... 20
Deployment process overview ... 20
AWS CloudFormation templates ... 21
Hub stack ... 22
Spoke stack ... 22
Org-Management stack ... 22
Prerequisites ... 23
Activate AWS RAM for AWS Organizations accounts ... 23
Step 1: Launch the Hub stack ... 23
Step 2: Launch the Spoke stack ... 28
Step 3: Launch the Org-Management stack ... 30
Monitor the solution ... 32
Activate CloudWatch Application Insights ... 32
Confirm cost tags associated with the solution ... 34
Activate cost allocation tags associated with the solution ... 35
AWS Cost Explorer ... 35
Troubleshooting ... 36
Problem: Failed job ... 36
Resolution ... 36
Problem: Failed Resource-Based Policies scan ... 37
Resolution ... 37
Problem: Access denied ... 40
Resolution ... 40
Problem: Undefined error ... 41
Resolution ... 41
Contact AWS Support ... 41
Create case ... 41
How can we help? ... 41
Additional information ... 41
Help us resolve your case faster ... 42
Solve now or contact us ... 42
Uninstall the solution ... 43
Using the AWS Management Console ... 43
Using AWS Command Line Interface ... 43
Deleting the Amazon Cognito user pool ... 43
Deleting the DynamoDB tables ... 44

- Deleting the CloudWatch logs ... 44
- Deleting the Amazon S3 bucket ... 45

Use the solution ... 46

- Login page ... 46
- Welcome page ... 46
- Findings ... 47
  - Resource-Based Policies scan ... 49
  - Job History ... 50
- Next steps ... 52
  - Account migration ... 52

Developer guide ... 53

- Source code ... 53

Reference ... 54

- Operational metrics ... 54
- Contributors ... 55

Revisions ... 56

Notices ... 58

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

Publication date: *November 2022 (last update: June 2024)*

This solution allows customers to better understand AWS Organizations dependencies by finding trusted access enabled AWS services, delegated admin accounts, and identity-based and resource-based 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 and resource-based policies with AWS Organization-based conditions.
- Presents scan results in a web user interface (UI) that tracks resources in your AWS Organization and the number of accounts with dependencies.
- Allows you to configure the scan by selecting specific AWS accounts, AWS services, and AWS Regions.

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.	Cost

If you want to . . .	Read . . .
The estimated baseline cost for running this solution in the US East (Northern Virginia) Region is USD $20 per month, depending on your specific implementation.	
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 CloudFormation 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 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 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, refer to Use the solution.

Identify enabled services with AWS Organizations

You can enable more than 25 compatible AWS services to perform operations across all of the AWS accounts in your AWS Organization. This solution finds enabled services and delegated admin accounts per service (if activated).

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 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 service	Policy type
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
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

Integration with AWS Service Catalog AppRegistry and Application Manager, a capability of AWS Systems Manager

This solution includes a Service Catalog AppRegistry resource to register the solution's CloudFormation template and its underlying resources as an application in both Service Catalog AppRegistry and Application Manager. With this integration, you can centrally manage the solution's resources and enable application search, reporting, and management actions.

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.

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.

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.

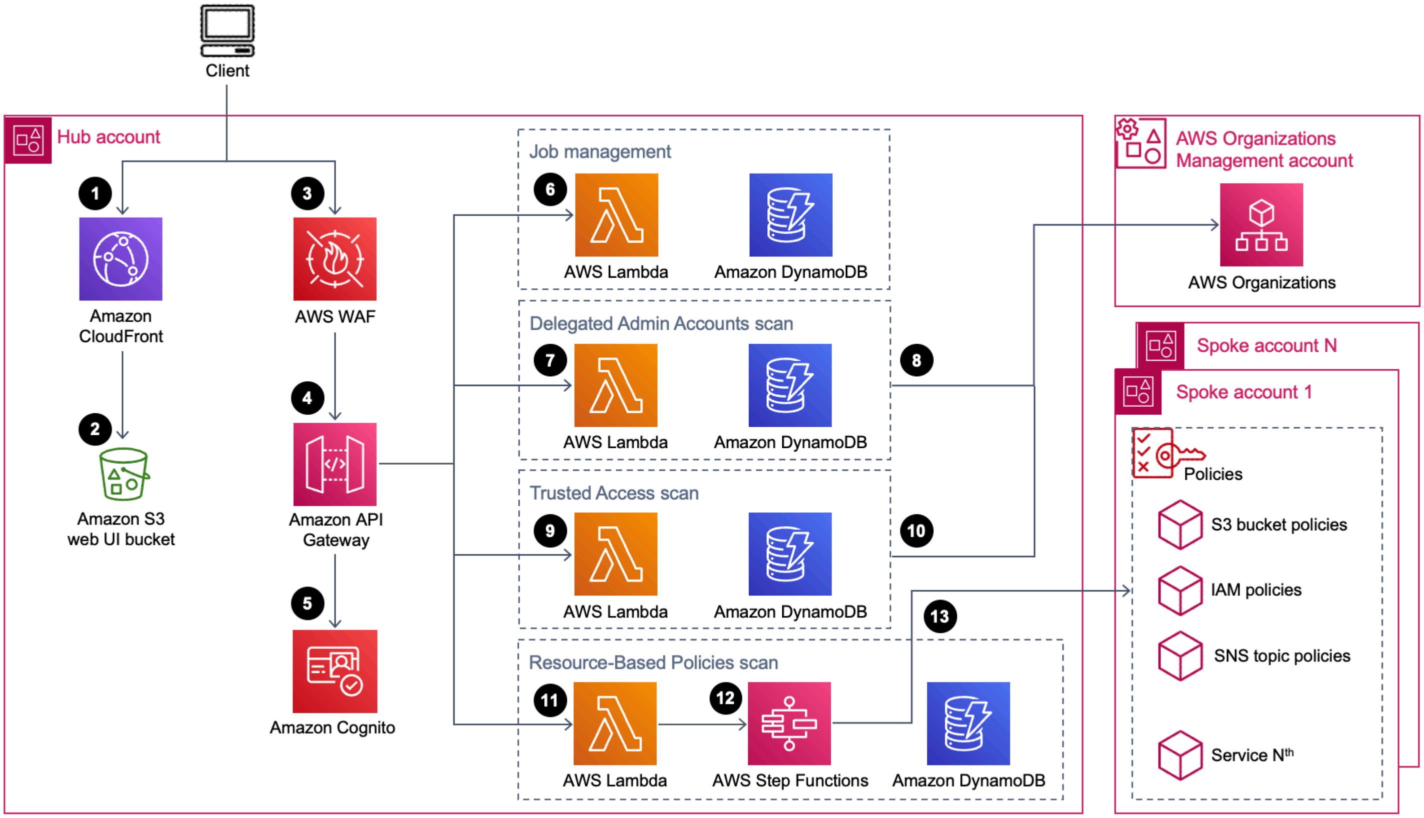
> **Note**
>
> For a general reference of AWS terms, see the AWS Glossary.

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.



Account Assessment for AWS Organizations architecture on AWS

1. Users log in to the hub account by using the web UI, and the Amazon Cognito user pool authenticates each user. Amazon CloudFront delivers the web UI content from an Amazon S3 bucket.
2. The Amazon S3 bucket hosts the web UI.
3. When you start a scan, the web UI gets a token from Amazon Cognito and sends a request to the Amazon API Gateway. AWS WAF protects the application programming interfaces (APIs)

from attacks. This solution configures a set of rules called a web access control list (ACL) that allows, blocks, or counts web requests based on configurable, user-defined web security rules and conditions.

4. An Amazon API Gateway provides the solution's API layer.
5. Amazon Cognito authenticates the token in the header of the API requests.
6. AWS Lambda serves the microservices and routes API requests to each microservice. The Job management microservice handles creation, deletion, and history of each scan job initiated by the user in the web UI.

> **Note**
>
> Steps 3–6 are repeated for each type of scan.

Delegated Admin Accounts scan

7. The Delegated Admin Accounts scan microservice finds and stores the delegated administrator account information for all the enabled AWS services in an Amazon DynamoDB table. These accounts can call the AWS Account Management API operations for other member accounts in the Organization.
8. This microservice gets the information from the Organizations management account.

Trusted Access scan

9. The Trusted Access scan microservice finds and stores the services in AWS Organizations with trusted access that allows the service to perform tasks in your Organization and its accounts on your behalf. This microservice stores the service principals in a DynamoDB table.
10. This microservice gets the information from the AWS Organizations management account.

Resource-Based Policies scan

11. The Resource-Based Policies scan microservice uses a Lambda function to start an asynchronous job and invoke AWS Step Functions.
12. The Step Functions state machine scans multiple accounts and AWS Regions in parallel to find and store resource details in the DynamoDB table. This microservice can scan up to 25 AWS services across accounts in your Organization and identify resource dependencies.

13 Each iteration in the state machine will invoke a Lambda function to assume a role in each spoke account. This microservice checks conditions in the policies that may contain Organization IDs or Organization Unit IDs.

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 solution-configured web ACLs.

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.

- The solution uses serverless architecture, and customers pay only for what they 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.

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.
- The web UI allow users to select scan parameters to perform selective scans in specific AWS accounts, Regions, and services.

AWS services used in this solution

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 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 DynamoDB	**Core.** Deploys a DynamoDB table for each microservice. Each microservice reads and

AWS service	Description
	writes to their specific table. This allows every microservice to own its own data.
AWS Lambda	**Core.** Deploys multiple Lambda functions to support four core microservices.
Amazon S3	**Core.** Deploys Amazon S3 buckets to host the web UI assets.
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 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.

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 **$20 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 10 times a month with maximum scan configuration ("full scan")
- Your usage for the web UI accounts on average for 100 single-page views per assessment
- You are creating 1 Cognito user
- Your scan for conditions in IAM policy produces 10,000 findings

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 advanced security feature	variable	<$0.01
Amazon CloudFront	1,000 requests	variable	<$1.00
Amazon S3	<1 GB storage	variable	<$1.00
AWS Lambda	33,000 requests with 1,000 ms average duration	variable	<$1.00
AWS Step Functions	58,000 state transitions	variable	$1.45
Amazon DynamoDB	10 million read capacity units, 100,000 write capacity units	variable	$2.50
AWS WAF	1 web ACL, 1 custom rule, 7 managed rule groups	fixed	$13.00
AWS X-Ray	100,000 Traces recorded for 3 services (Step Functions, Lambda, and API Gateway) with default 5% sampling rate	variable	<$0.10
		Total monthly cost:	**$20.07**

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.

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.

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 AWS Regions:

Region name	
US East (Ohio)	Asia Pacific (Tokyo)
US East (N. Virginia)	Canada (Central)
US West (N. California)	Europe (Frankfurt)
US West (Oregon)	Europe (Paris)
Asia Pacific (Singapore)	Europe (London)
Asia Pacific (Sydney)	Europe (Ireland)
Asia Pacific (Mumbai)	Europe (Stockholm)
Asia Pacific (Seoul)	South America (São Paulo)

AWS accounts

We recommend the following guidelines for each stack:

- **Hub stack –** Deploy to any member account in your AWS Organization except the Organizations management account.
- **Spoke stack –** Deploy to any member account in your AWS Organization that needs to be assessed by the solution, including the hub account.
- **Org-Management stack** – Deploy in the Organizations management account to scan for enabled services and delegated admin accounts.

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 account.
- 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.

   Launch solution

2. 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.

3. On the **Create stack** page, verify that the correct template URL is in the **Amazon S3 URL** text box, and choose **Next**.

4. 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*.

5. 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>*	Unique string used 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.

Parameter	Default	Description
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)
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		

Parameter	Default	Description
Provide the AWS Organization ID	*<Optional input>*	Organization ID to support multi-account deployment. Leave blank for single account deployments. **Note** This solution includes an Service Catalog AppRegistry resource to register the AWS CloudFormation template and underlying resources as an application in both Service Catalog AppRegistry and AWS Systems Manager Application Manager. For more information, see *Monitor the solution*.

Parameter	Default	Description
Management Account ID	*<Optional input>*	Account ID for the management account of the AWS Organization. Leave blank for single account deployments. **Note** This solution includes an Service Catalog AppRegistry resource to register the AWS CloudFormation template and underlying resources as an application in both Service Catalog AppRegistry and AWS Systems Manager Application Manager. For more information, see *Monitor the solution*.

6. Choose **Next**.
7. On the **Configure stack options** page, choose **Next**.
8. On the **Review and create** page, review and confirm the settings. Check the box acknowledging that the template will create IAM resources.
9. 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.

   Launch solution

2. 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.

3. On the **Create stack** page, verify that the correct template URL is in the **Amazon S3 URL** text box, and choose **Next**.
4. 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*.

5. 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>*	Unique string used as prefix for resource names. ⓘ **Note** Use the same namespace in the Hub stack and Org-Management 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.

6. Choose **Next**.
7. On the **Configure stack options** page, choose **Next**.
8. On the **Review and create** page, review and confirm the settings. Check the box acknowledging that the template will create IAM resources.
9. 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. 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.

3. On the **Create stack** page, verify that the correct template URL is in the **Amazon S3 URL** text box, and choose **Next**.
4. 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*.
5. 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>*	Unique string used as prefix for resource names.

Parameter	Default	Description
		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.

6. Choose **Next**.
7. On the **Configure stack options** page, choose **Next**.
8. On the **Review and create** page, review and confirm the settings. Check the box acknowledging that the template will create IAM resources.
9. 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.

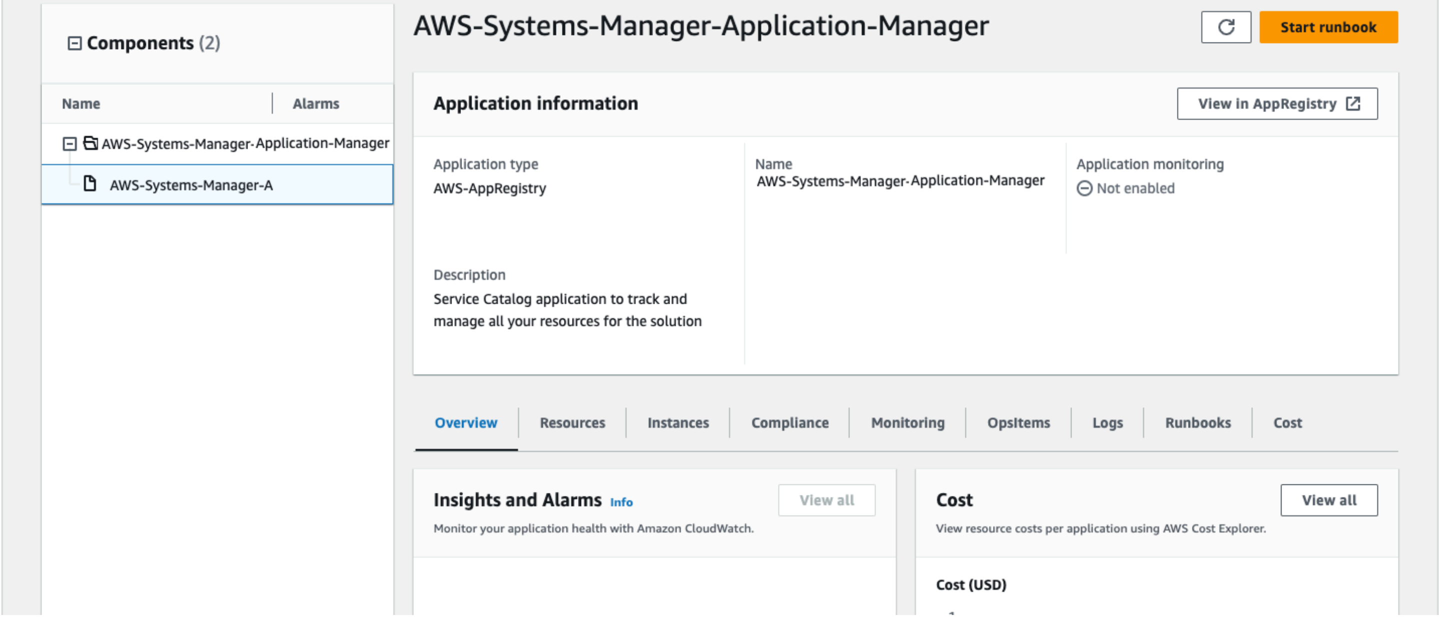
Monitor the solution with AppRegistry

The solution includes a Service Catalog AppRegistry resource to register the CloudFormation template and underlying resources as an application in both Service Catalog AppRegistry and AWS Systems Manager Application Manager.

AWS Systems Manager Application Manager gives you an application-level view into this solution and its resources so that you can:

- Monitor its resources, costs for the deployed resources across stacks and AWS accounts, and logs associated with this solution from a central location.
- View operations data for the resources of this solution in the context of an application. For example, deployment status, CloudWatch alarms, resource configurations, and operational issues.

The following figure depicts an example of the application view for the solution stack in Application Manager.



Components (2)

Name	Alarms
AWS-Systems-Manager-Application-Manager	
AWS-Systems-Manager-A	

AWS-Systems-Manager-Application-Manager

Application information

Application type: AWS-AppRegistry

Name: AWS-Systems-Manager-Application-Manager

Application monitoring: Not enabled

Description: Service Catalog application to track and manage all your resources for the solution

Insights and Alarms

Monitor your application health with Amazon CloudWatch.

Cost

View resource costs per application using AWS Cost Explorer.

Cost (USD)

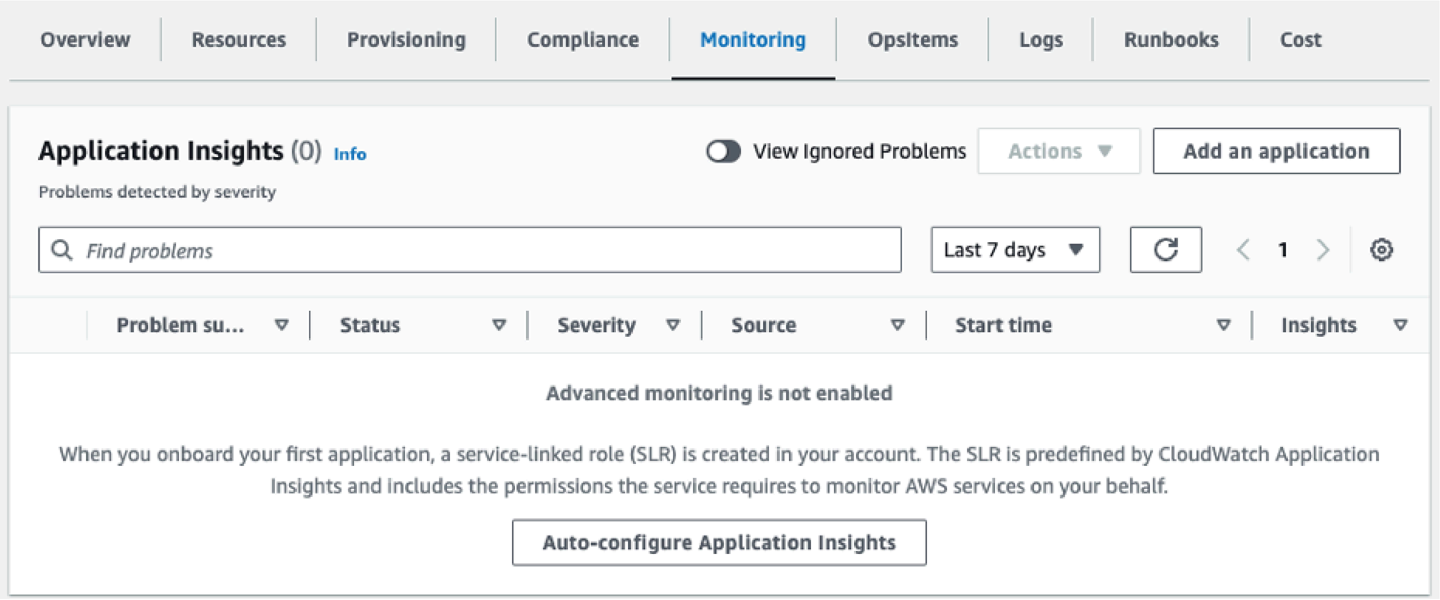
Solution stack in Application Manager

Activate CloudWatch Application Insights

1. Sign in to the Systems Manager console.

2. In the navigation pane, choose **Application Manager**.
3. In **Applications**, search for the application name for this solution and select it.

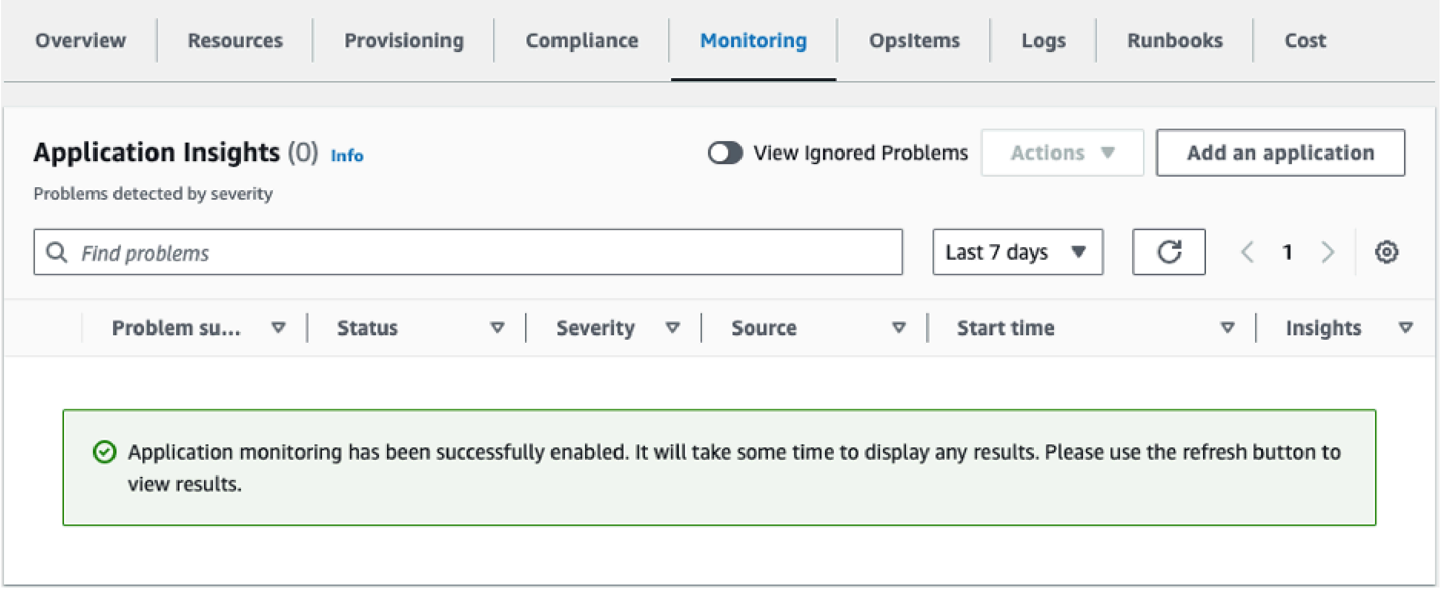
   The application name will have **App Registry** in the **Application Source** column, and will have a combination of the solution name, Region, account ID, or stack name.
4. In the **Components** tree, choose the application stack you want to activate.
5. In the **Monitoring** tab, in **Application Insights**, select **Auto-configure Application Insights**.



Advanced monitoring is not enabled

When you onboard your first application, a service-linked role (SLR) is created in your account. The SLR is predefined by CloudWatch Application Insights and includes the permissions the service requires to monitor AWS services on your behalf.

Monitoring for your applications is now activated and the following status box appears:



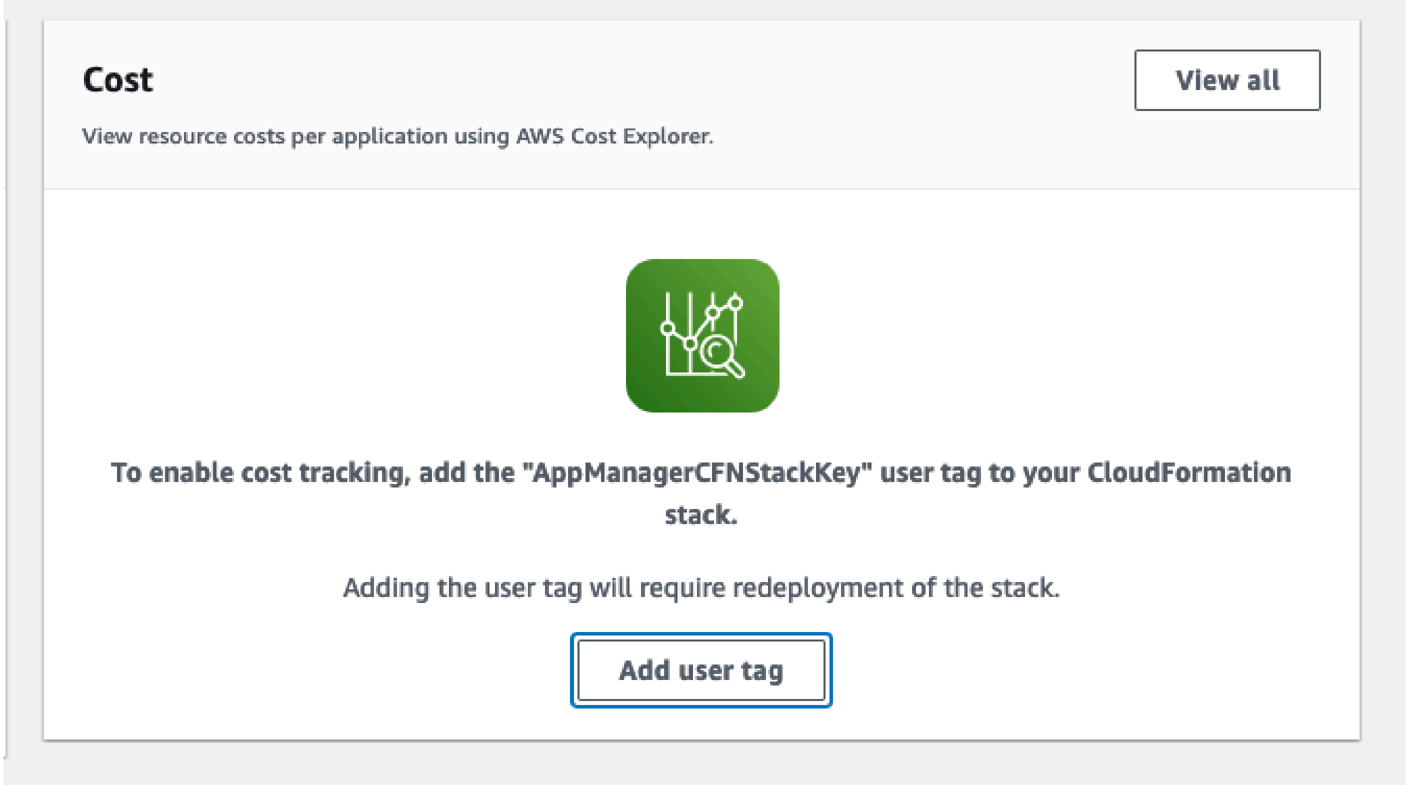
Application monitoring has been successfully enabled. It will take some time to display any results. Please use the refresh button to view results.

Confirm cost tags associated with the solution

After you activate cost allocation tags associated with the solution, you must confirm the cost allocation tags to see the costs for this solution. To confirm cost allocation tags:

1. Sign in to the Systems Manager console.
2. In the navigation pane, choose **Application Manager**.
3. In **Applications**, choose the application name for this solution and select it.

   The application name will have **App Registry** in the **Application Source** column, and will have a combination of the solution name, Region, account ID, or stack name.
4. In the **Overview** tab, in **Cost**, select **Add user tag**.



Cost

View resource costs per application using AWS Cost Explorer.

To enable cost tracking, add the "AppManagerCFNStackKey" user tag to your CloudFormation stack.

Adding the user tag will require redeployment of the stack.

5. On the **Add user tag** page, enter `confirm`, then select **Add user tag**.

The activation process can take up to 24 hours to complete and the tag data to appear.

Activate cost allocation tags associated with the solution

After you activate Cost Explorer, you must activate the cost allocation tags associated with this solution to see the costs for this solution. The cost allocation tags can only be activated from the management account for the organization. To activate cost allocation tags:

1. Sign in to the AWS Billing and Cost Management and Cost Management console.
2. In the navigation pane, select **Cost Allocation Tags**.
3. On the **Cost allocation tags** page, filter for the AppManagerCFNStackKey tag, then select the tag from the results shown.
4. Choose **Activate**.

AWS Cost Explorer

You can see the overview of the costs associated with the application and application components within the Application Manager console through integration with AWS Cost Explorer, which must be first activated. Cost Explorer helps you manage costs by providing a view of your AWS resource costs and usage over time. To activate Cost Explorer for the solution:

1. Sign in to the AWS Cost Management console.
2. In the navigation pane, select **Cost Explorer** to view the solution's costs and usage over time.

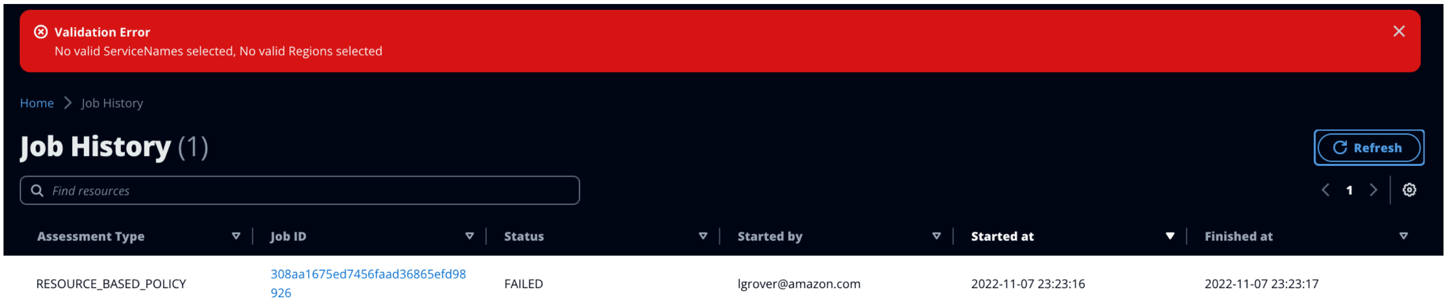
Troubleshooting

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

If these instructions don't address your issue, the section called "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`.



Validation Error

No valid ServiceNames selected, No valid Regions selected

Assessment Type	Job ID	Status	Started by	Started at	Finished at
RESOURCE_BASED_POLICY	308aa1675ed7456faad36865efd98926	FAILED	lgrover@amazon.com	2022-11-07 23:23:16	2022-11-07 23:23:17

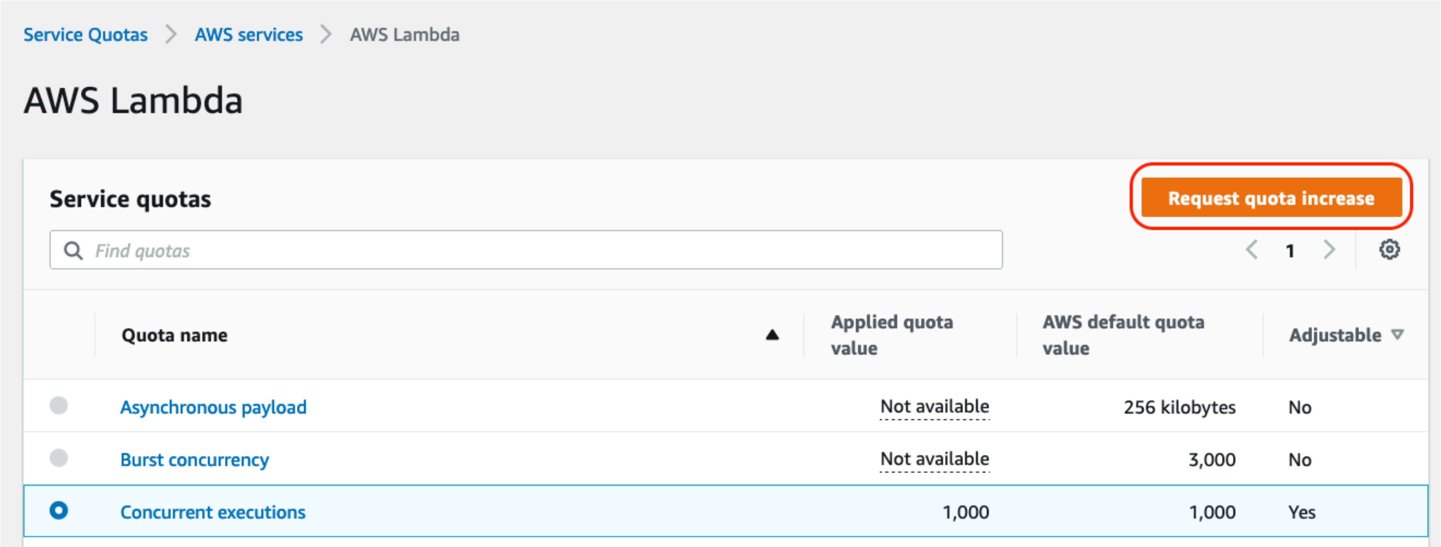
Resolution

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.



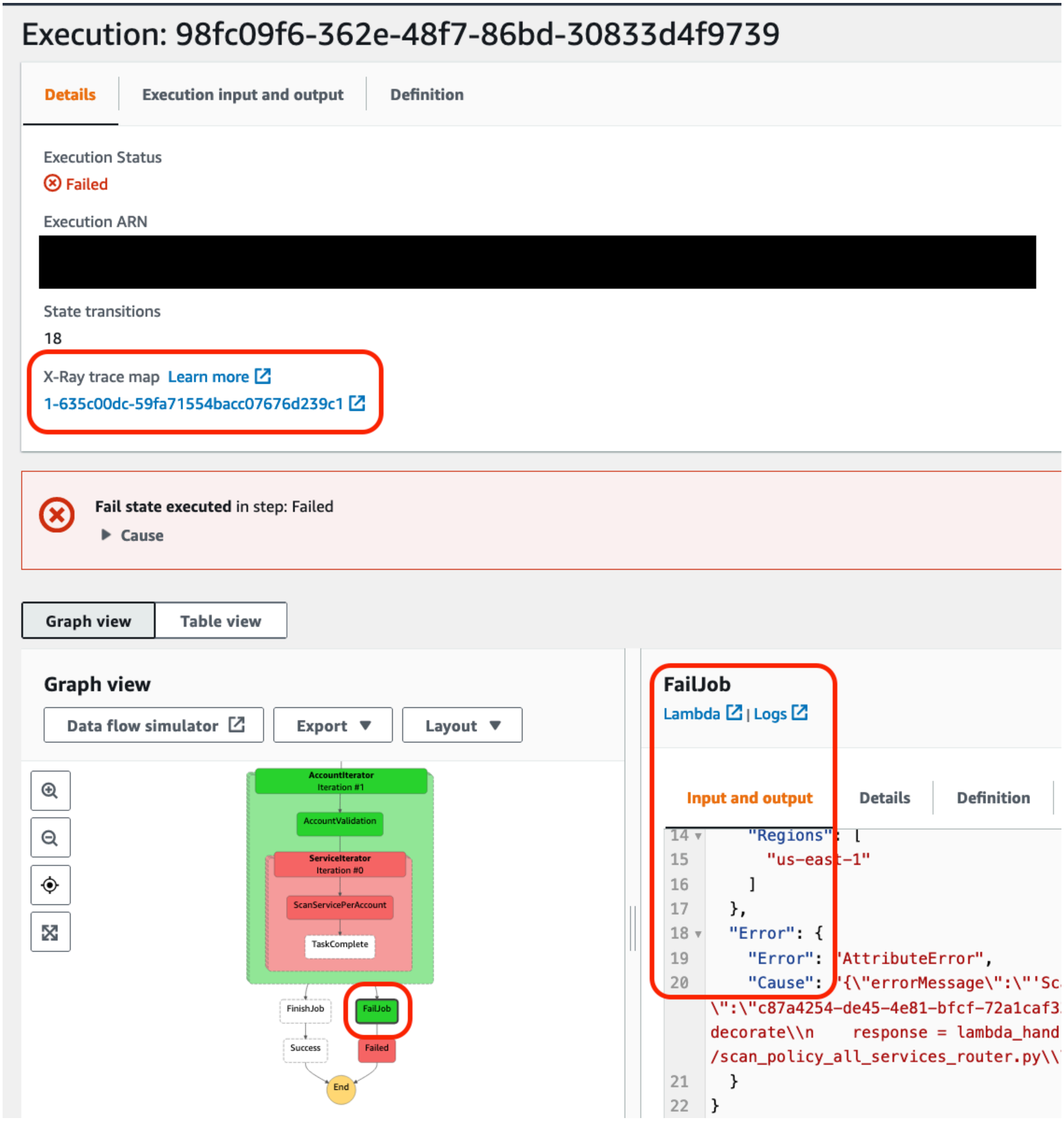
	Quota name ▲	Applied quota value	AWS default quota value	Adjustable ▽
○	Asynchronous payload	Not available	256 kilobytes	No
○	Burst concurrency	Not available	3,000	No
●	Concurrent executions	1,000	1,000	Yes

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

Execution Status

Failed

Execution ARN

[redacted]

State transitions

18

X-Ray trace map Learn more

1-635c00dc-59fa71554bacc07676d239c1

Fail state executed in step: Failed

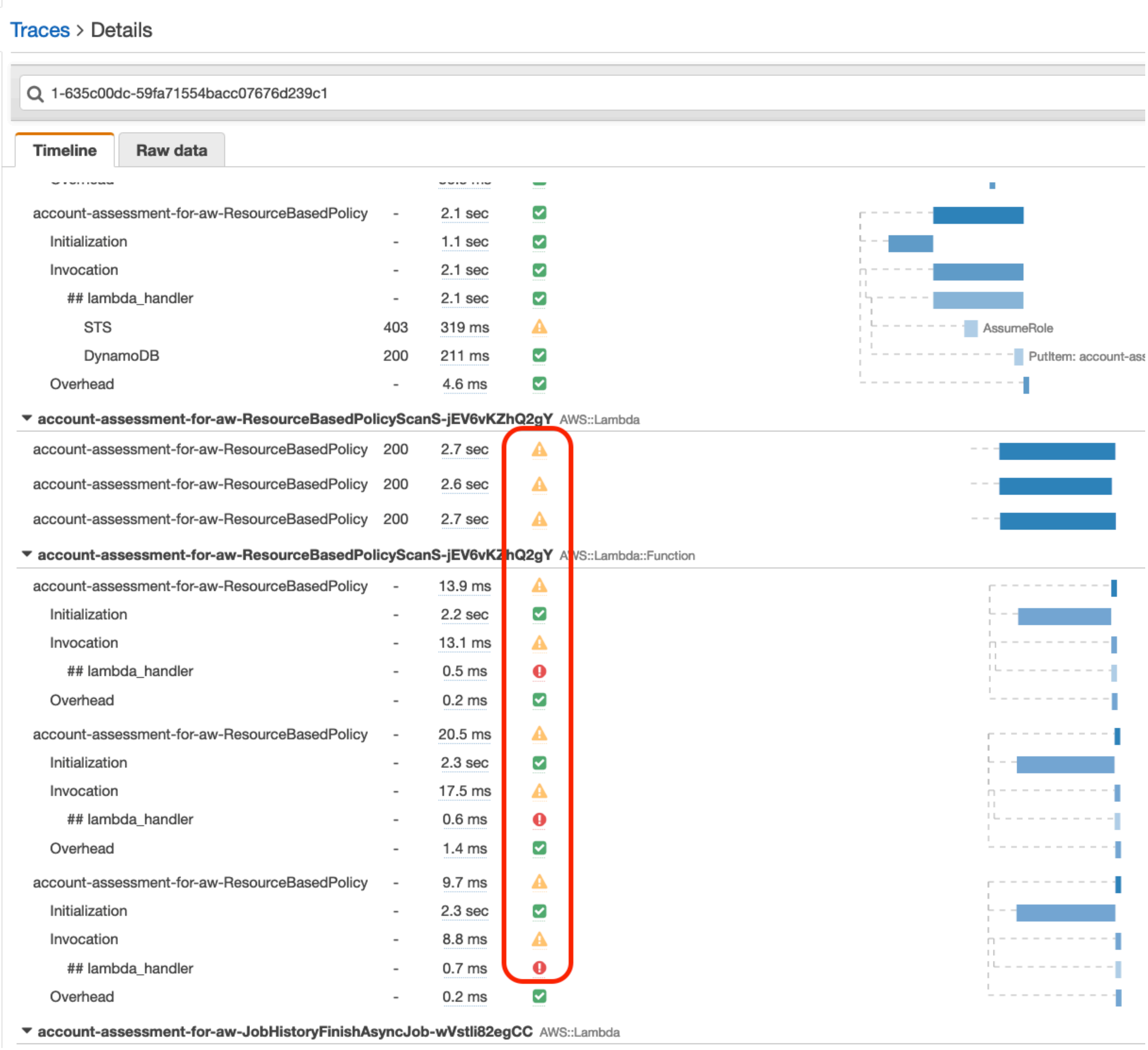
▶ Cause

FailJob

Lambda | Logs

```
    "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\\
  }
}
```

Example state machine failure details



Traces > Details

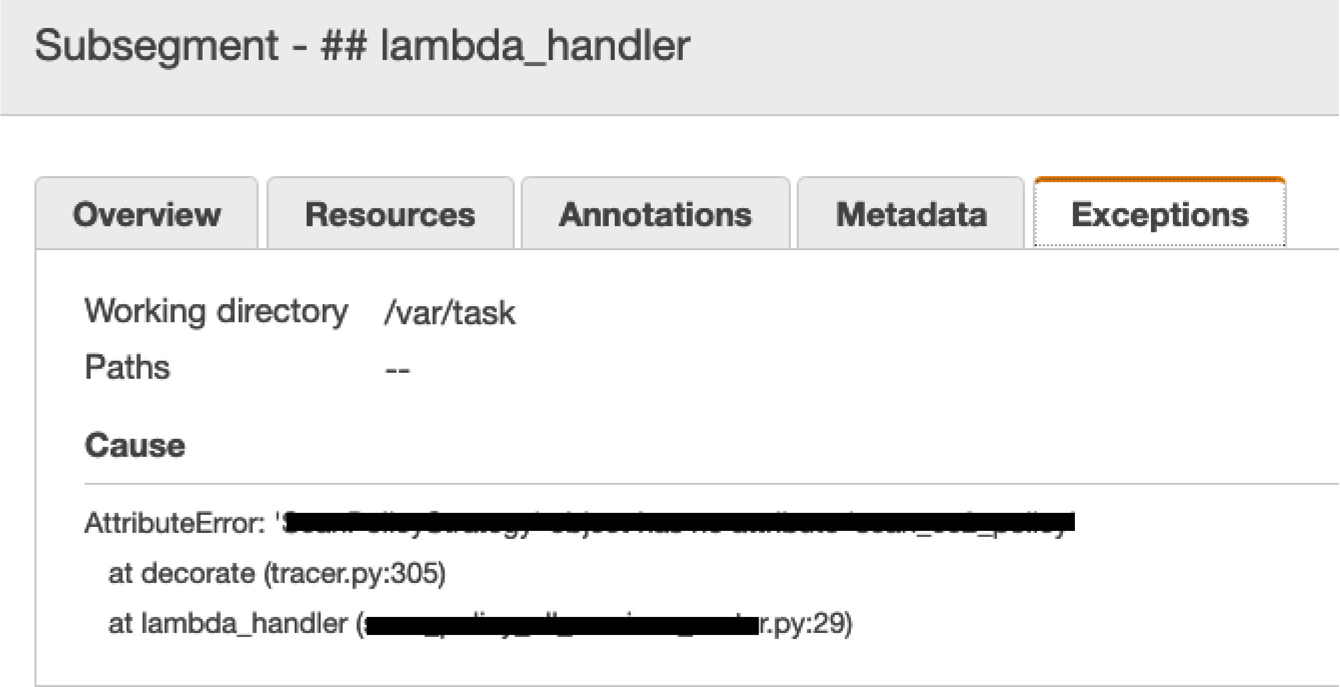
1-635c00dc-59fa71554bacc07676d239c1

Timeline | Raw data

account-assessment-for-aw-ResourceBasedPolicy	-	2.1 sec	✓
Initialization	-	1.1 sec	✓
Invocation	-	2.1 sec	✓
## lambda_handler	-	2.1 sec	✓
STS	403	319 ms	⚠
DynamoDB	200	211 ms	✓
Overhead	-	4.6 ms	✓
▼ account-assessment-for-aw-ResourceBasedPolicyScanS-jEV6vKZhQ2gY AWS::Lambda			
account-assessment-for-aw-ResourceBasedPolicy	200	2.7 sec	⚠
account-assessment-for-aw-ResourceBasedPolicy	200	2.6 sec	⚠
account-assessment-for-aw-ResourceBasedPolicy	200	2.7 sec	⚠
▼ account-assessment-for-aw-ResourceBasedPolicyScanS-jEV6vKZhQ2gY AWS::Lambda::Function			
account-assessment-for-aw-ResourceBasedPolicy	-	13.9 ms	⚠
Initialization	-	2.2 sec	✓
Invocation	-	13.1 ms	⚠
## lambda_handler	-	0.5 ms	❗
Overhead	-	0.2 ms	✓
account-assessment-for-aw-ResourceBasedPolicy	-	20.5 ms	⚠
Initialization	-	2.3 sec	✓
Invocation	-	17.5 ms	⚠
## lambda_handler	-	0.6 ms	❗
Overhead	-	1.4 ms	✓
account-assessment-for-aw-ResourceBasedPolicy	-	9.7 ms	⚠
Initialization	-	2.3 sec	✓
Invocation	-	8.8 ms	⚠
## lambda_handler	-	0.7 ms	❗
Overhead	-	0.2 ms	✓
▼ account-assessment-for-aw-JobHistoryFinishAsyncJob-wVstli82egCC AWS::Lambda			

Example state machine failure details in X-Ray

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.



Subsegment - ## lambda_handler

Working directory /var/task

Paths --

Cause

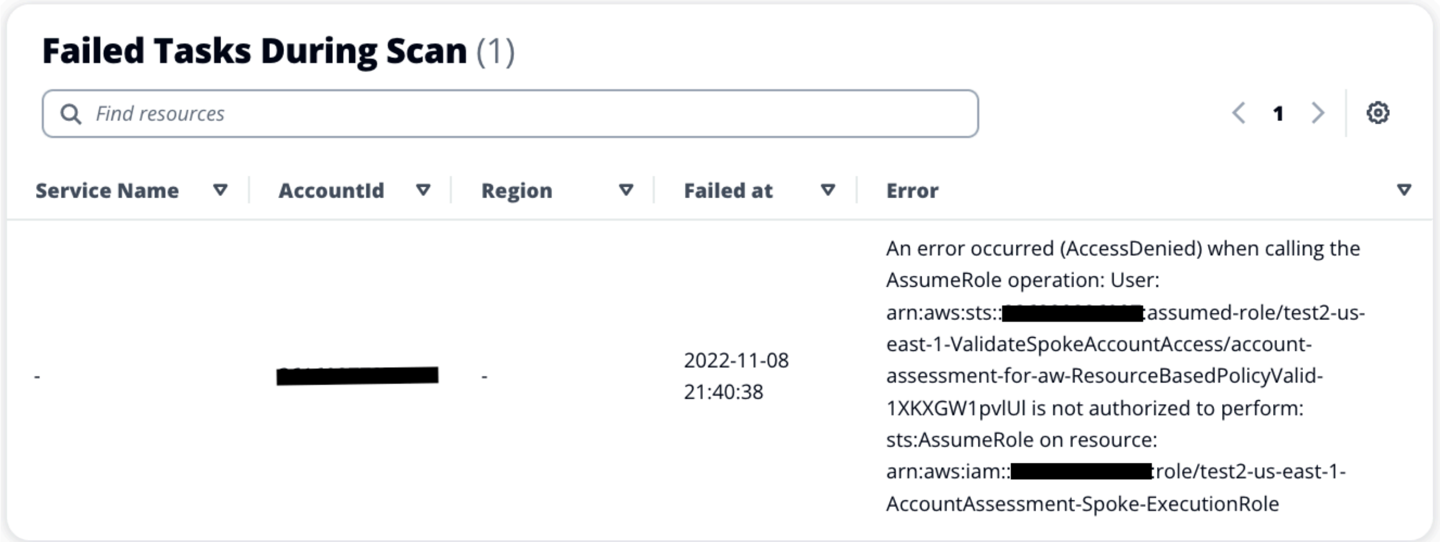
```
AttributeError: '[redacted]
  at decorate (tracer.py:305)
  at lambda_handler ([redacted]r.py:29)
```

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.



Failed Tasks During Scan (1)

Service Name	AccountId	Region	Failed at	Error
-	[redacted]	-	2022-11-08 21:40:38	An error occurred (AccessDenied) when calling the AssumeRole operation: User: arn:aws:sts::[redacted]:assumed-role/test2-us-east-1-ValidateSpokeAccountAccess/account-assessment-for-aw-ResourceBasedPolicyValid-1XKXGW1pvlUI is not authorized to perform: sts:AssumeRole on resource: arn:aws:iam::[redacted]:role/test2-us-east-1-AccountAssessment-Spoke-ExecutionRole

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.

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

The following sections describe how to use this solution's web UI.

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

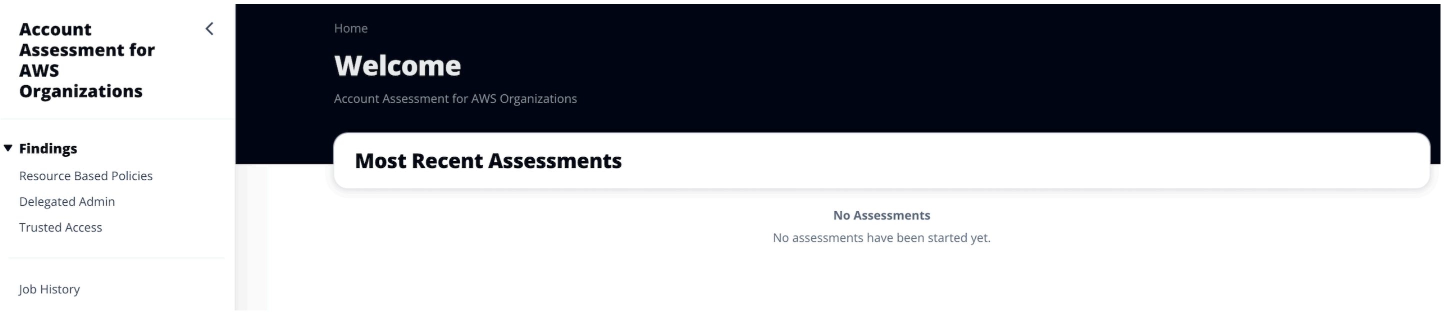
You may also retrieve the web UI URL from the CloudFormation template outputs under `"WebUserInterfaceURL"`.

Note

If needed, you can add multi-factor authentication (MFA) to a Cognito User Pool.

Welcome page

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



Account Assessment for AWS Organizations

Findings

- Resource Based Policies
- Delegated Admin
- Trusted Access

Job History

Home

Welcome

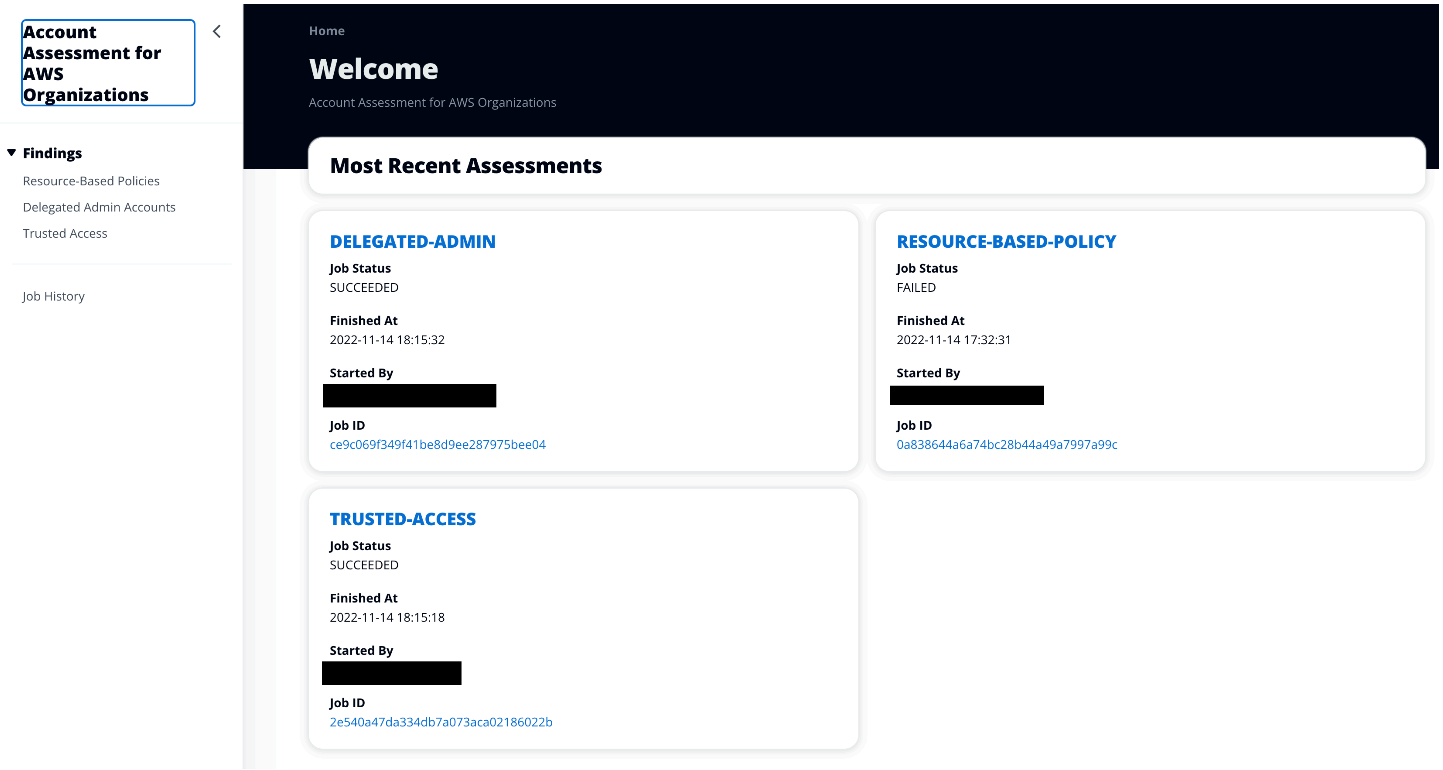
Account Assessment for AWS Organizations

Most Recent Assessments

No Assessments

No assessments have been started yet.

Figure 4: Welcome page the first time you log in



Account Assessment for AWS Organizations

Findings

- Resource-Based Policies
- Delegated Admin Accounts
- Trusted Access

Job History

Home

Welcome

Account Assessment for AWS Organizations

Most Recent Assessments

DELEGATED-ADMIN

Job Status
SUCCEEDED

Finished At
2022-11-14 18:15:32

Started By
[redacted]

Job ID
ce9c069f349f41be8d9ee287975bee04

RESOURCE-BASED-POLICY

Job Status
FAILED

Finished At
2022-11-14 17:32:31

Started By
[redacted]

Job ID
0a838644a6a74bc28b44a49a7997a99c

TRUSTED-ACCESS

Job Status
SUCCEEDED

Finished At
2022-11-14 18:15:18

Started By
[redacted]

Job ID
2e540a47da334db7a073aca02186022b

Welcome page showing most recent assessments

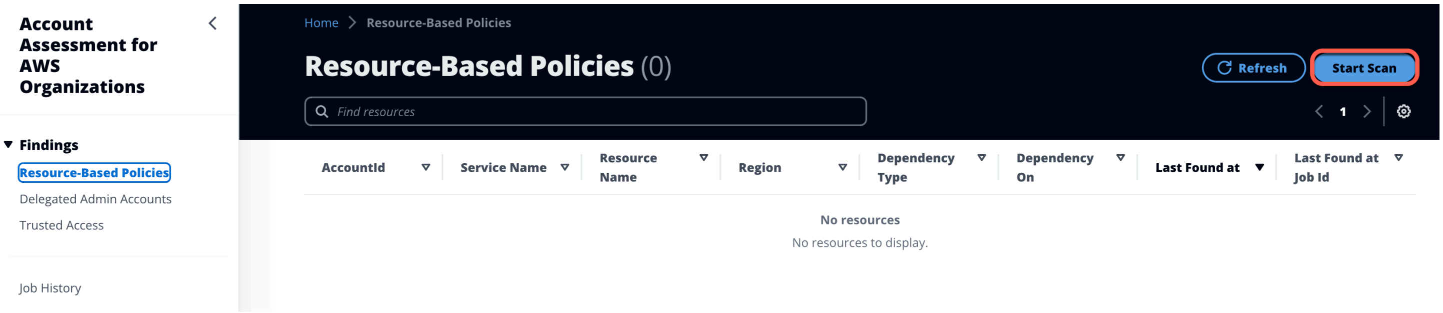
Findings

The left pane lists three types of assessments, corresponding to each of the solution’s microservices:

1. Resource-Based Polices
2. Delegated Admin Accounts
3. Trusted Access

Begin an assessment by selecting **Start Scan**.

> **Note**
>
> You can run one active scan on each microservice at a time.



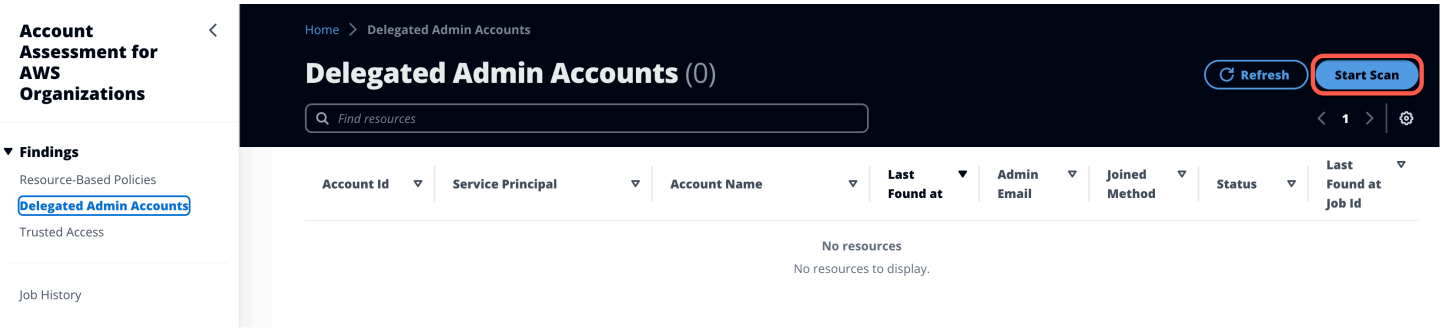
Resource-Based Policies (0)

AccountId	Service Name	Resource Name	Region	Dependency Type	Dependency On	Last Found at	Last Found at Job Id

No resources

No resources to display.

Resource-Based Polices page



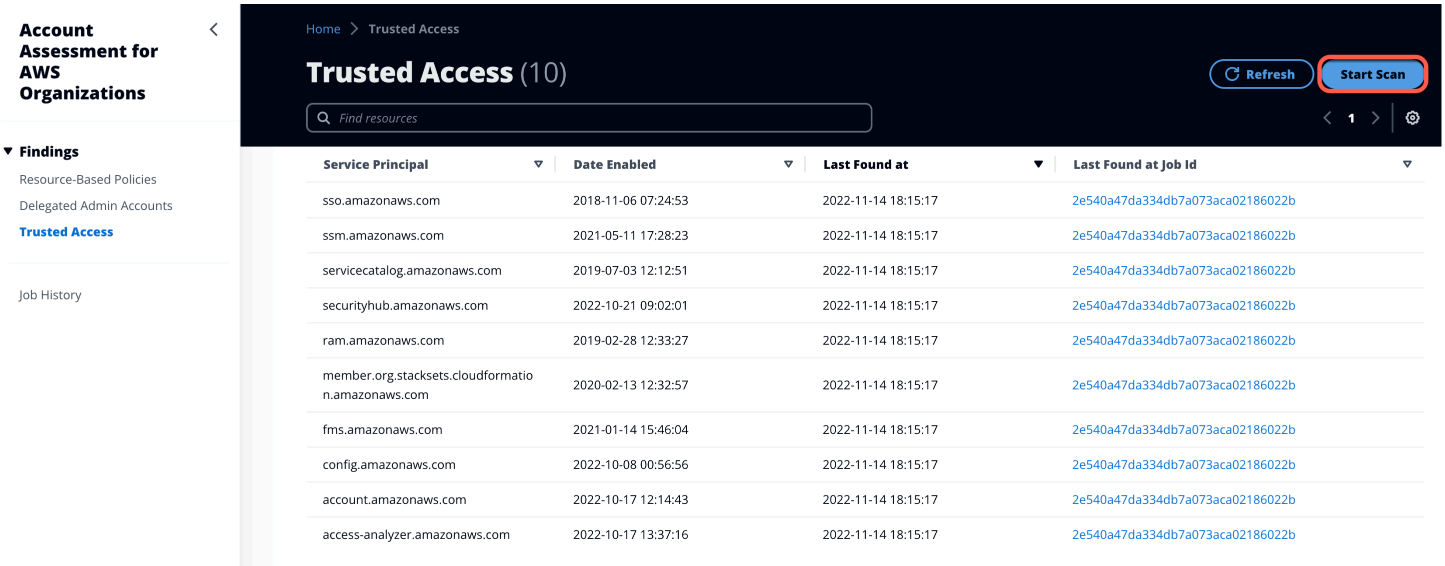
Delegated Admin Accounts (0)

Account Id	Service Principal	Account Name	Last Found at	Admin Email	Joined Method	Status	Last Found at Job Id

No resources

No resources to display.

Delegated Admin Accounts page



Trusted Access (10)

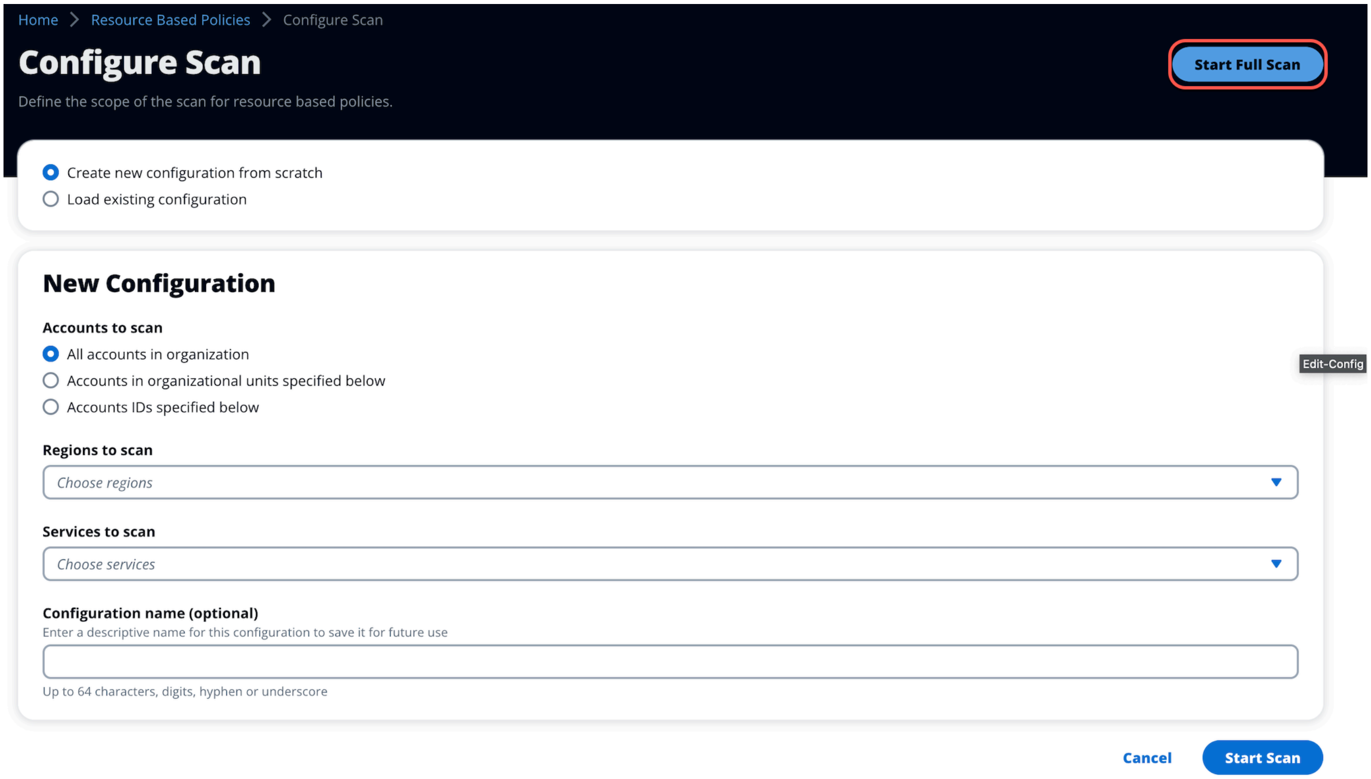
Service Principal	Date Enabled	Last Found at	Last Found at Job Id
sso.amazonaws.com	2018-11-06 07:24:53	2022-11-14 18:15:17	2e540a47da334db7a073aca02186022b
ssm.amazonaws.com	2021-05-11 17:28:23	2022-11-14 18:15:17	2e540a47da334db7a073aca02186022b
servicecatalog.amazonaws.com	2019-07-03 12:12:51	2022-11-14 18:15:17	2e540a47da334db7a073aca02186022b
securityhub.amazonaws.com	2022-10-21 09:02:01	2022-11-14 18:15:17	2e540a47da334db7a073aca02186022b
ram.amazonaws.com	2019-02-28 12:33:27	2022-11-14 18:15:17	2e540a47da334db7a073aca02186022b
member.org.stacksets.cloudformation.amazonaws.com	2020-02-13 12:32:57	2022-11-14 18:15:17	2e540a47da334db7a073aca02186022b
fms.amazonaws.com	2021-01-14 15:46:04	2022-11-14 18:15:17	2e540a47da334db7a073aca02186022b
config.amazonaws.com	2022-10-08 00:56:56	2022-11-14 18:15:17	2e540a47da334db7a073aca02186022b
account.amazonaws.com	2022-10-17 12:14:43	2022-11-14 18:15:17	2e540a47da334db7a073aca02186022b
access-analyzer.amazonaws.com	2022-10-17 13:37:16	2022-11-14 18:15:17	2e540a47da334db7a073aca02186022b

Trusted Access page

Additional steps for Resource-Based Policies scan

This assessment type offers you two ways to scan the resources in your AWS Organization.

1. Start a full scan of your AWS Organization:
   a. Select **Resource-Based Policies** in the left-hand menu.
   b. Select the **Start Full Scan** button.



Home > Resource Based Policies > Configure Scan

Configure Scan

Define the scope of the scan for resource based policies.

● Create new configuration from scratch
○ Load existing configuration

New Configuration

Accounts to scan
● All accounts in organization
○ Accounts in organizational units specified below
○ Accounts IDs specified below

Regions to scan
Choose regions ▼

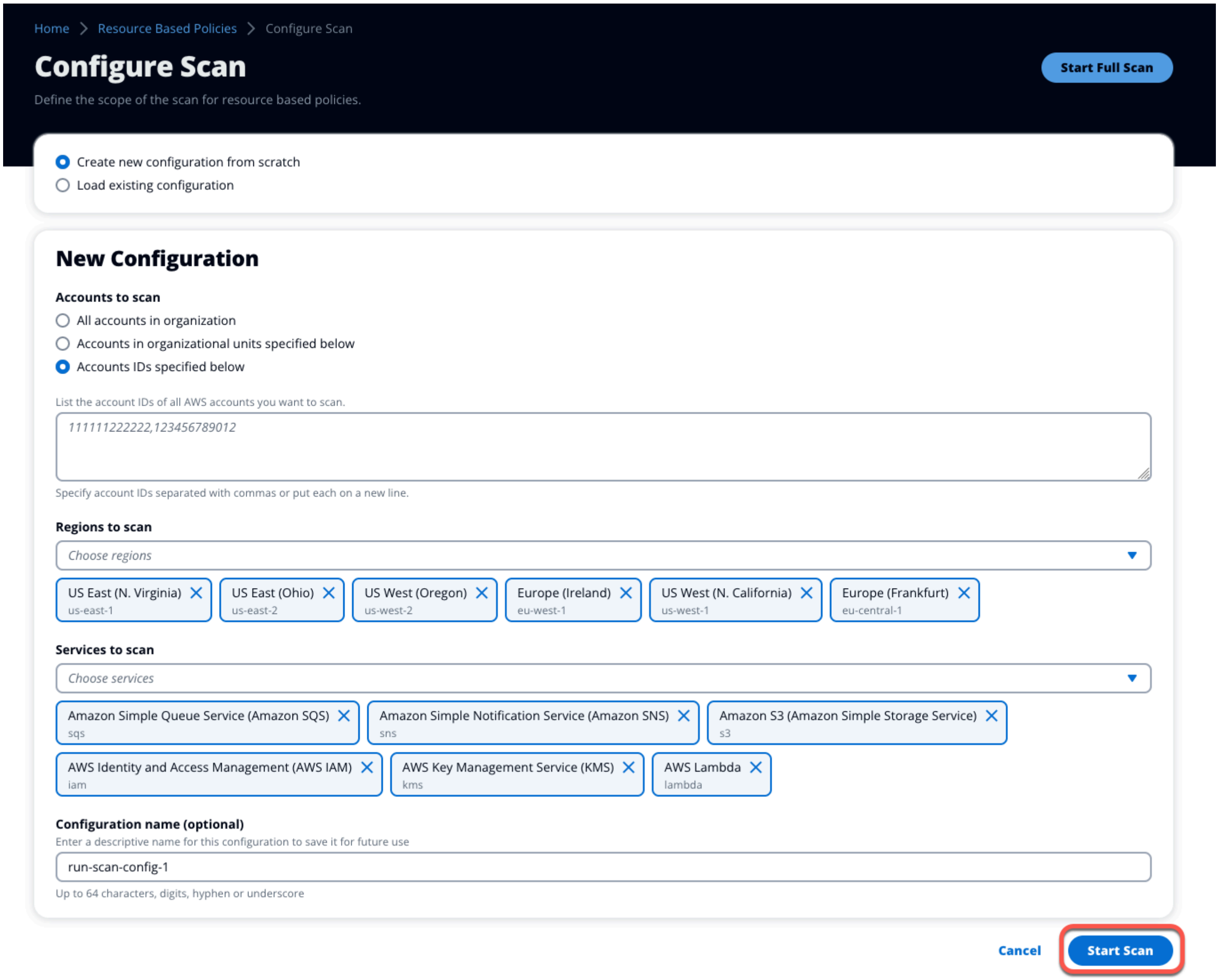
Services to scan
Choose services ▼

Configuration name (optional)
Enter a descriptive name for this configuration to save it for future use

Up to 64 characters, digits, hyphen or underscore

2. Scan specific AWS accounts, OUs, AWS Regions, or AWS services:
   a. Select **Resource Based Policies** in the left-hand menu.
   b. Select specific AWS accounts, OUs, AWS Regions, or AWS services to scan.
   c. Select the **Start Scan** button.

> **Note**
>
> If you plan to scan same configuration multiple times, you can name the configuration and load the same parameters by selecting the **Load existing configuration** radio button and entering a name.



Configure Scan

Define the scope of the scan for resource based policies.

● Create new configuration from scratch
○ Load existing configuration

New Configuration

Accounts to scan

○ All accounts in organization
○ Accounts in organizational units specified below
● Accounts IDs specified below

List the account IDs of all AWS accounts you want to scan.

111111222222,123456789012

Specify account IDs separated with commas or put each on a new line.

Regions to scan

Choose regions

US East (N. Virginia) us-east-1; US East (Ohio) us-east-2; US West (Oregon) us-west-2; Europe (Ireland) eu-west-1; US West (N. California) us-west-1; Europe (Frankfurt) eu-central-1

Services to scan

Choose services

Amazon Simple Queue Service (Amazon SQS) sqs; Amazon Simple Notification Service (Amazon SNS) sns; Amazon S3 (Amazon Simple Storage Service) s3; AWS Identity and Access Management (AWS IAM) iam; AWS Key Management Service (KMS) kms; AWS Lambda lambda

Configuration name (optional)

Enter a descriptive name for this configuration to save it for future use

run-scan-config-1

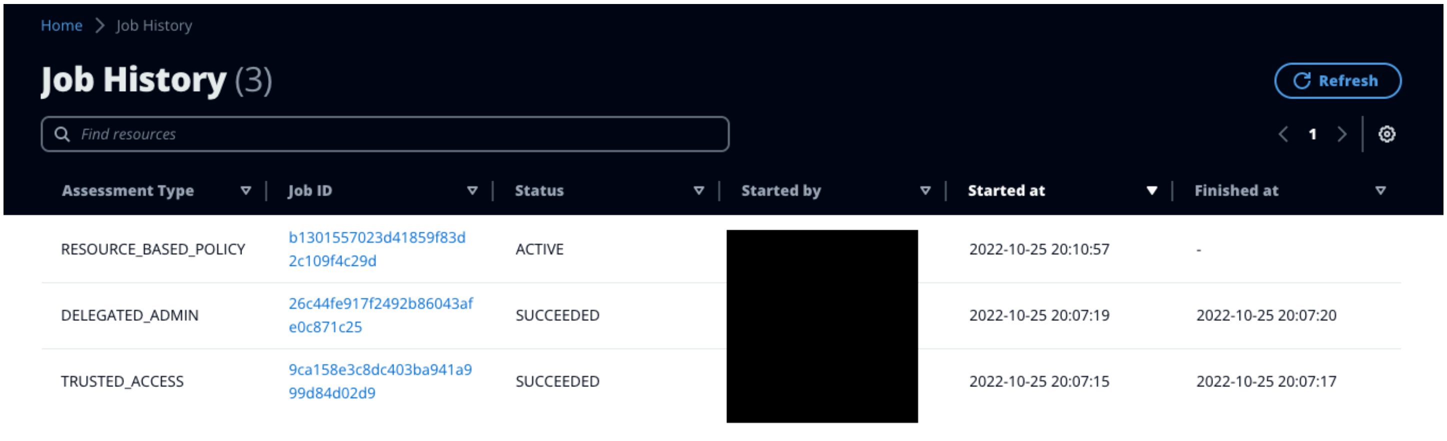
Up to 64 characters, digits, hyphen or underscore

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.



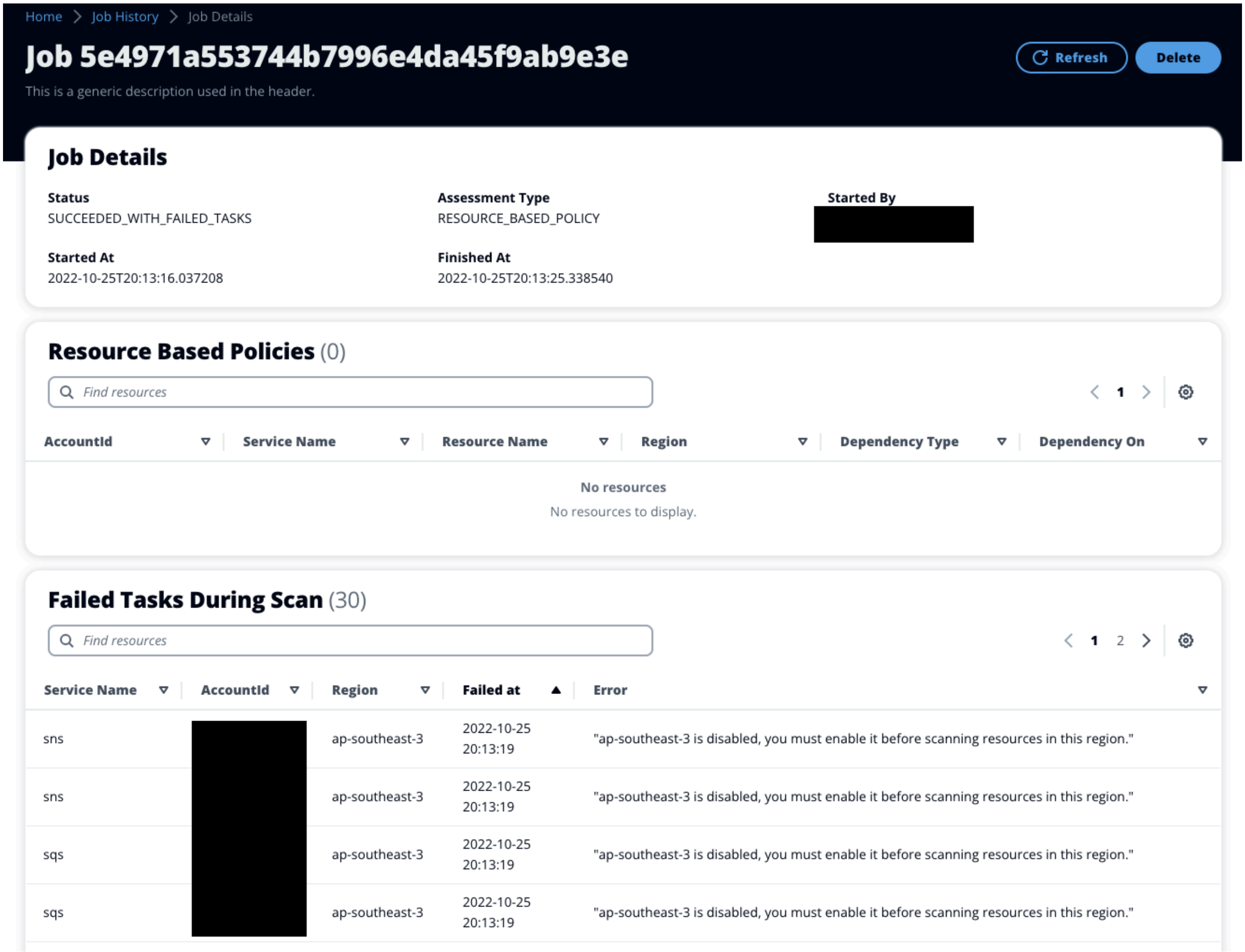
Home > Job History

Job History (3)

Find resources

Assessment Type	Job ID	Status	Started by	Started at	Finished at
RESOURCE_BASED_POLICY	b1301557023d41859f83d2c109f4c29d	ACTIVE	[redacted]	2022-10-25 20:10:57	-
DELEGATED_ADMIN	26c44fe917f2492b86043afe0c871c25	SUCCEEDED	[redacted]	2022-10-25 20:07:19	2022-10-25 20:07:20
TRUSTED_ACCESS	9ca158e3c8dc403ba941a999d84d02d9	SUCCEEDED	[redacted]	2022-10-25 20:07:15	2022-10-25 20:07:17

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.



Home > Job History > Job Details

Job 5e4971a553744b7996e4da45f9ab9e3e

This is a generic description used in the header.

Job Details

Status
SUCCEEDED_WITH_FAILED_TASKS

Assessment Type
RESOURCE_BASED_POLICY

Started By
[redacted]

Started At
2022-10-25T20:13:16.037208

Finished At
2022-10-25T20:13:25.338540

Resource Based Policies (0)

Find resources

AccountId	Service Name	Resource Name	Region	Dependency Type	Dependency On

No resources
No resources to display.

Failed Tasks During Scan (30)

Find resources

Service Name	AccountId	Region	Failed at	Error
sns	[redacted]	ap-southeast-3	2022-10-25 20:13:19	"ap-southeast-3 is disabled, you must enable it before scanning resources in this region."
sns	[redacted]	ap-southeast-3	2022-10-25 20:13:19	"ap-southeast-3 is disabled, you must enable it before scanning resources in this region."
sqs	[redacted]	ap-southeast-3	2022-10-25 20:13:19	"ap-southeast-3 is disabled, you must enable it before scanning resources in this region."
sqs	[redacted]	ap-southeast-3	2022-10-25 20:13:19	"ap-southeast-3 is disabled, you must enable it before scanning resources in this region."

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.

Anonymized data collection

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 invoked, 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`, or `ResourceBasedPolicy`
- **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

Example data:

```
AssessmentType: ResourceBasedPolicy
FindingsCount: 10
ServicesCount: 20
AccountsCount: 10
RegionsCount: 10
```

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
- Ryan Garay

Revisions

Date	Change
November 2022	Initial release
January 2023	Release 1.0.1: Security patch. For more information, refer to the CHANGELOG.md file in the GitHub repository.
February 2023	Release 1.0.2: Added support for MFA, increased unit test coverage, and implemented bug fixes. For more information, refer to the CHANGELOG.md file in the GitHub repository.
March 2023	Release 1.0.3: Added support for scanning more than five specified OpenSearch Service domains, support for scanning Amazon S3 bucket policies in the opt-in Regions, updated the AppRegistry attribute group name with a unique string. For more information, refer to the CHANGELOG.md file in the GitHub repository.
April 2023	Release 1.0.4: Mitigated impact caused by new default settings for Amazon S3 Object Ownership (ACLs disabled) for all new Amazon S3 buckets. For more information, refer to the CHANGELOG.md file in the GitHub repository.
October 2023	Release 1.0.5: Updated package versions to resolve security vulnerabilities. For more information, refer to the CHANGELOG.md file in the GitHub repository.
November 2023	Documentation update: Added Confirm cost tags associated with the solution to the

Date	Change
	Monitoring the solution with AWS Service Catalog AppRegistry section.
April 2024	Release 1.0.6: Updated package versions to resolve security vulnerabilities. For more information, refer to the CHANGELOG.md file in the GitHub repository.
June 2024	Release 1.0.7: Updated package versions to resolve security vulnerabilities. For more information, refer to the CHANGELOG.md file in the GitHub repository.
June 2024	Release 1.0.8: Updated package versions to resolve security vulnerabilities. For more information, refer to the CHANGELOG.md file in the GitHub repository.

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.