



CISCO *Live!*

DevNet Zone



The bridge to possible

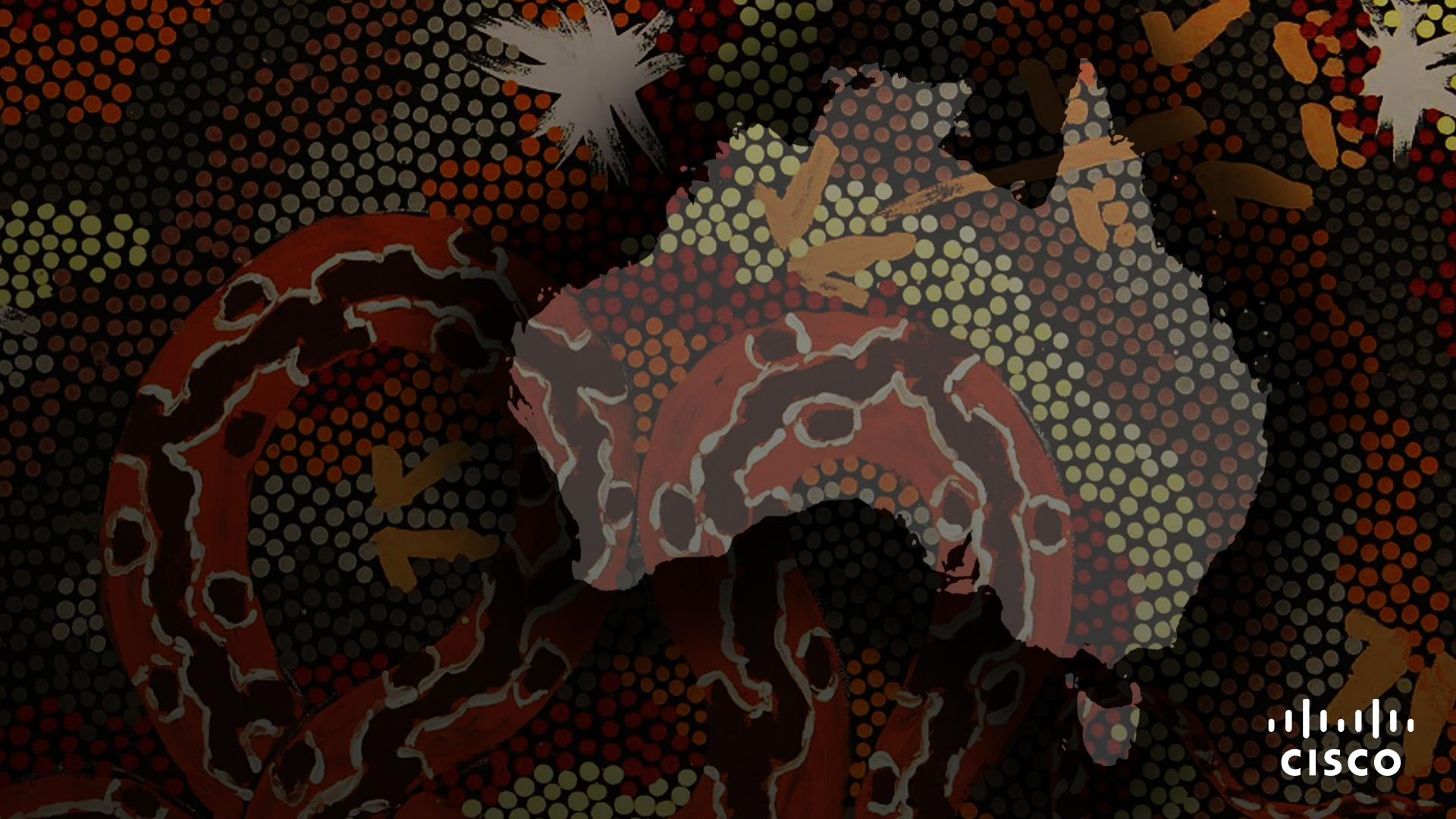
Using SecureX orchestration for Automating Public Cloud Incident Response and Remediation

Brian Sak, Technical Solutions Architect
@briansak
DEVNET-3140



DevNet Zone

#CiscoLiveAPJC



Cisco Webex App

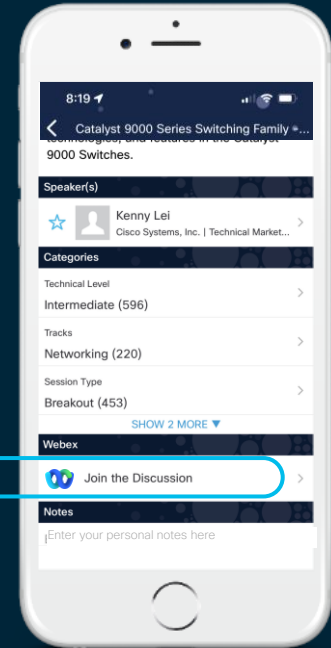
Questions?

Use Cisco Webex App to chat with the speaker after the session

How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until Thursday 22 December, 2022.





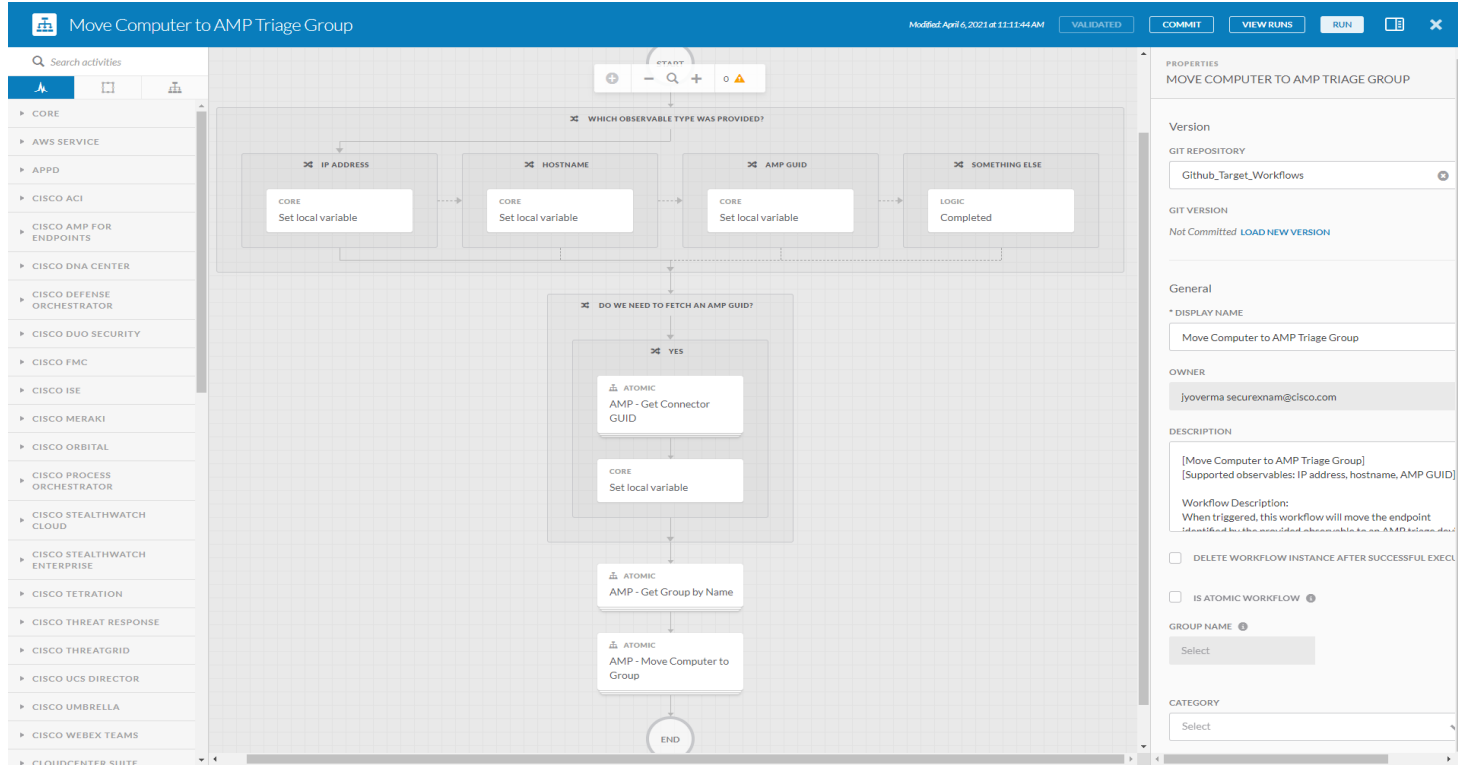
Agenda

- SecureX orchestration
- IR with Public Cloud Providers
- Building Public Cloud Workflows in SXo
- Importing and Executing a Workflow
- Response Workflows in Threat Response

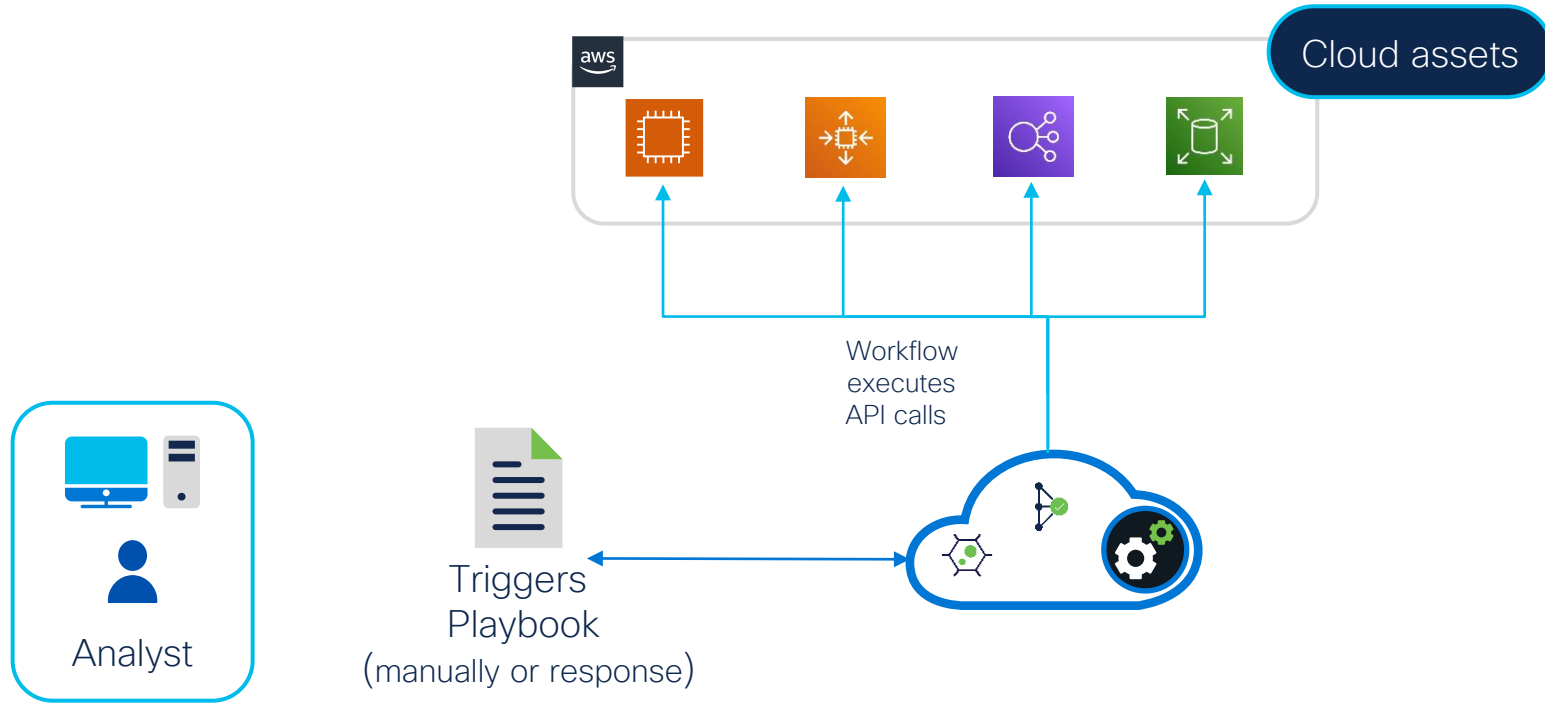
SecureX orchestration



SecureX orchestration

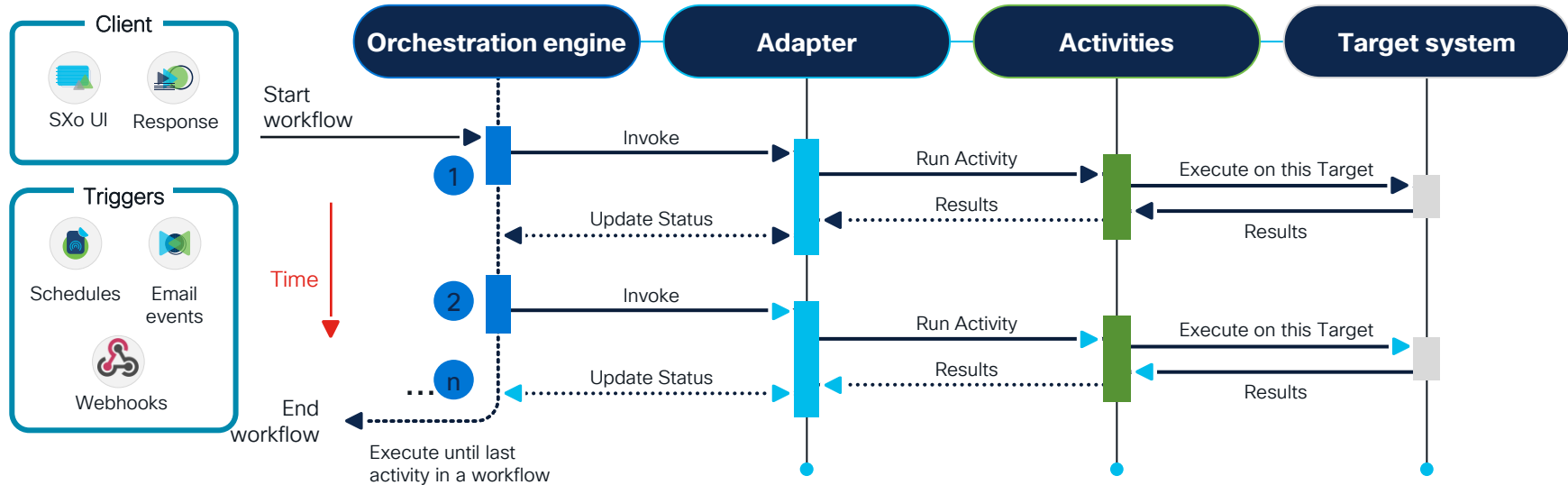


SecureX orchestration



SecureX orchestration workflow sequence

The orchestration engine invokes **adapters** to execute **activities** on the **target systems**, which returns results and **status**, then the next step in the workflow begins.



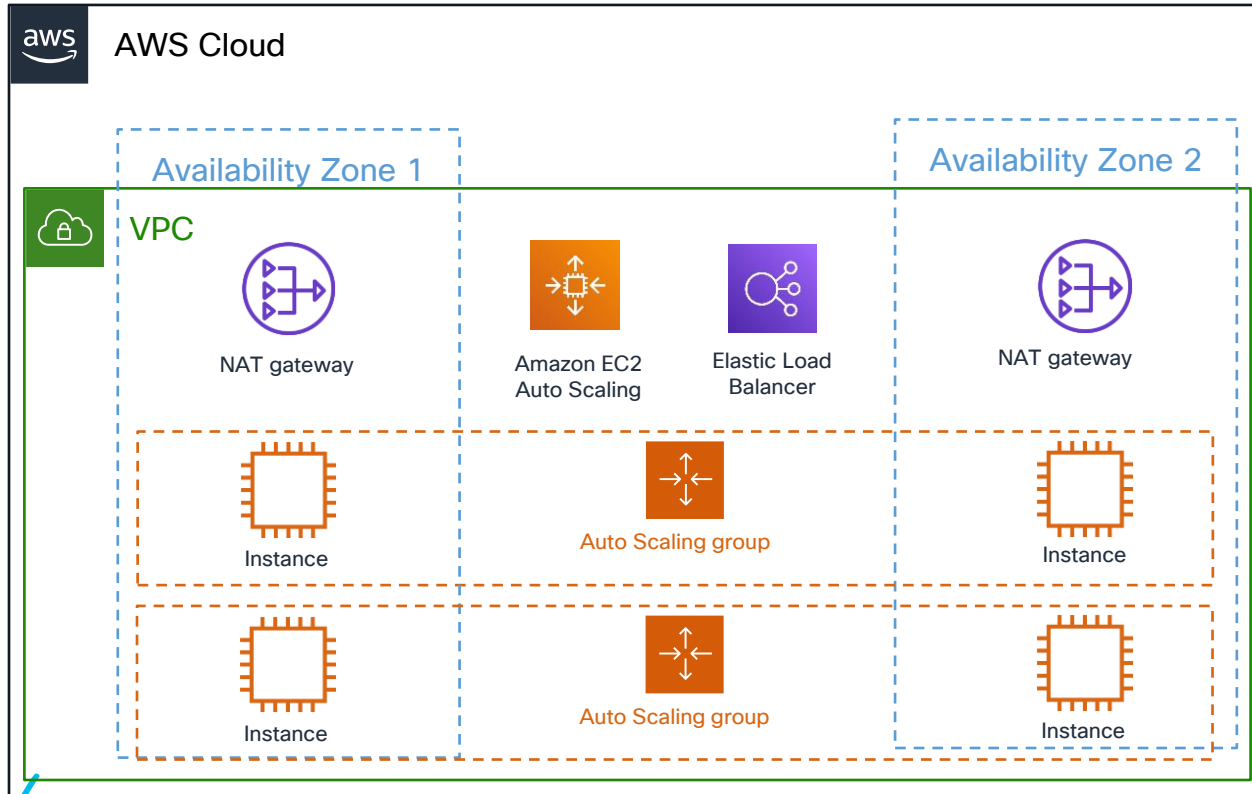
Adapter:
Integration with a target system,
provides activities to perform task
automation

Activity:
REST call, Run terminal,
Send email ... etc..

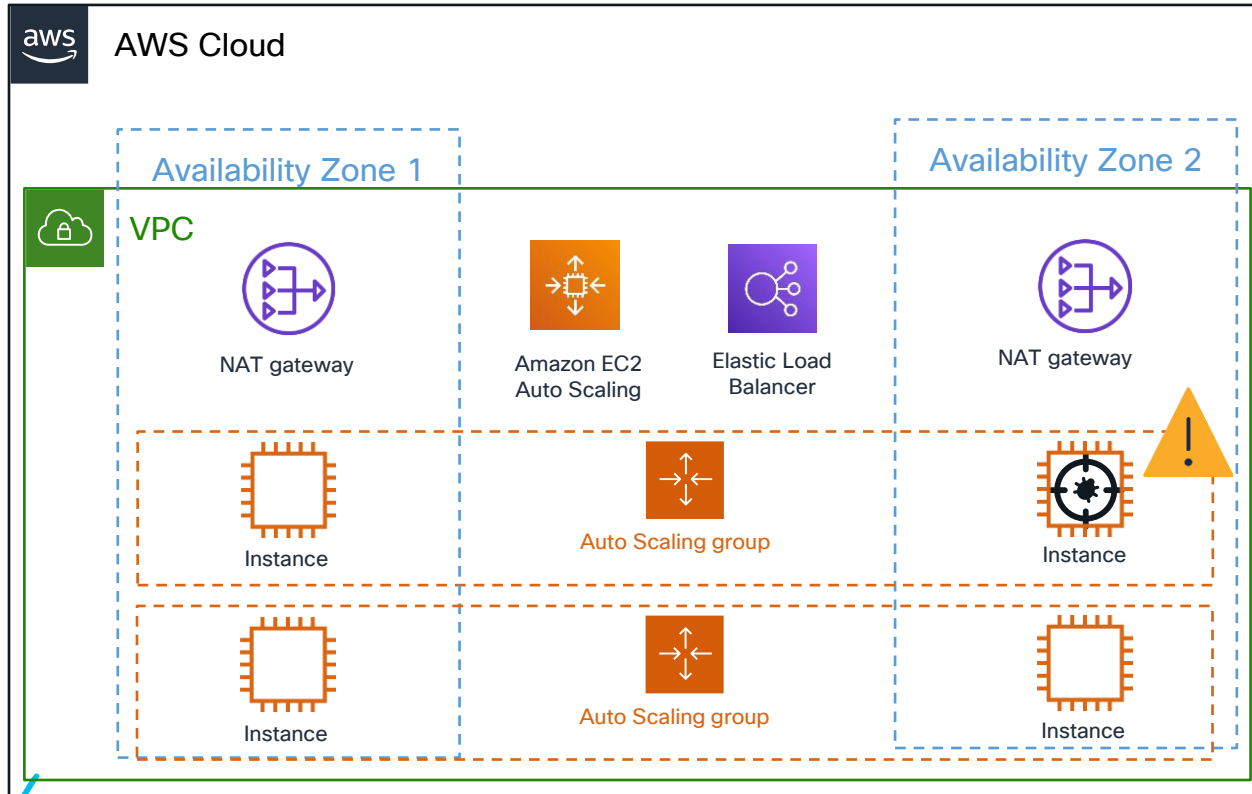
Target System:
The host/endpoint that
executes an activity

Incident Response with Public Cloud Providers

Instance Compromised in Public Cloud?



Instance Compromised in Public Cloud?



**AWS Security Incident
Response Guide
AWS Technical Guide**













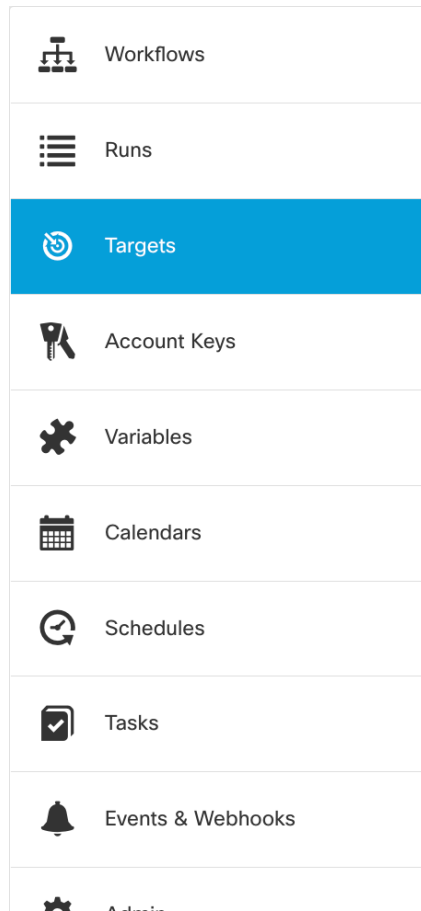
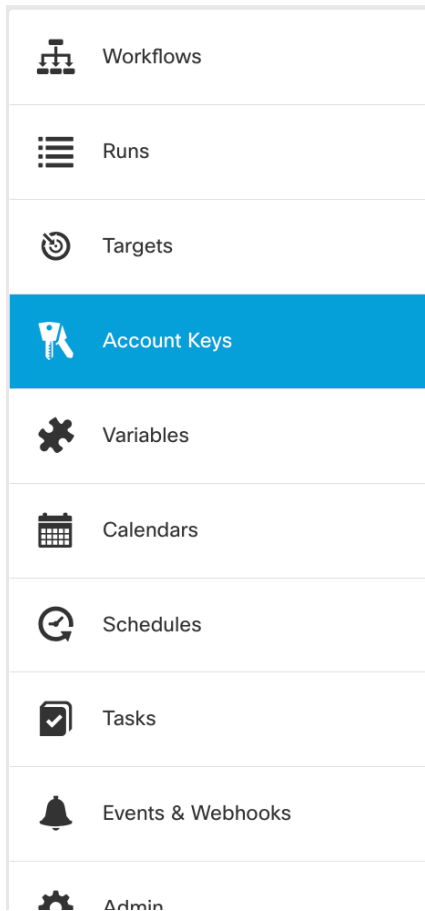
**AWS Security Incident
Response Guide**
AWS Technical Guide

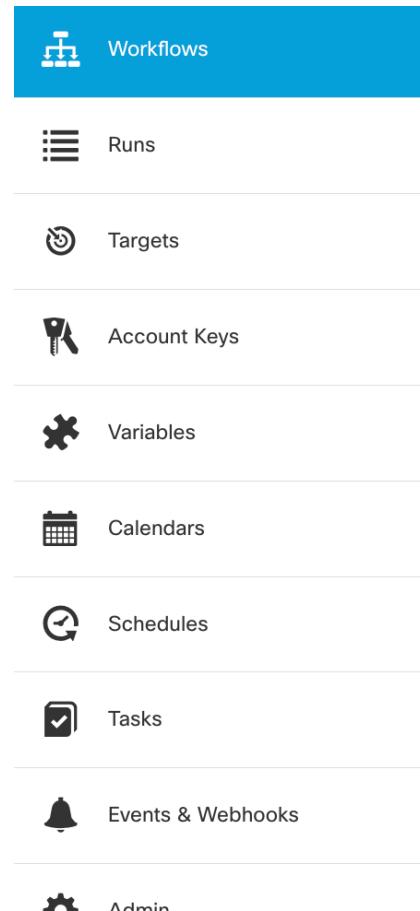
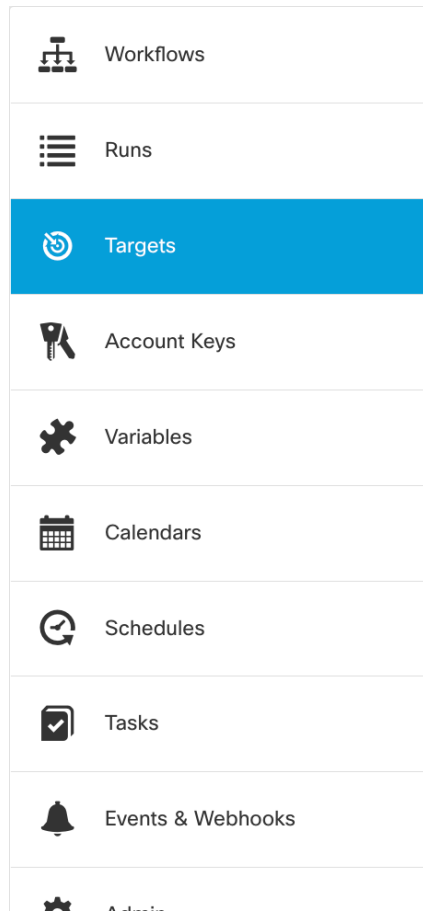
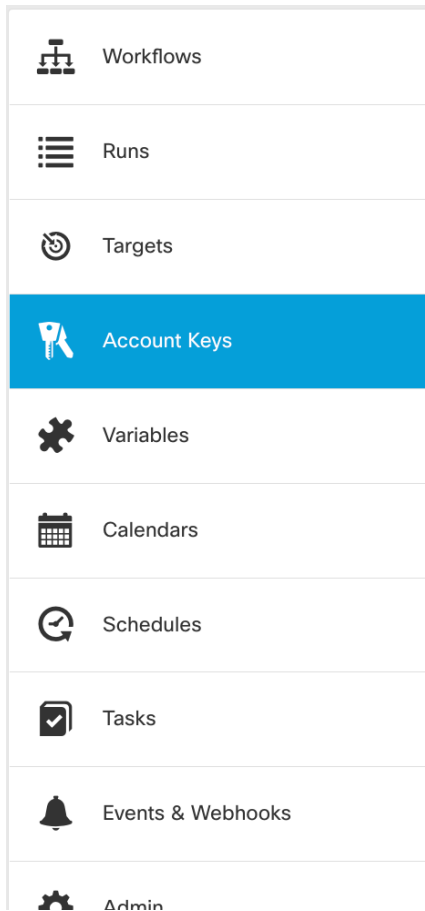


Fundamentals of Working with Public Cloud in SXo



	Workflows
	Runs
	Targets
	Account Keys
	Variables
	Calendars
	Schedules
	Tasks
	Events & Webhooks
	Admin







Workflows

Runs

Targets

Account Keys

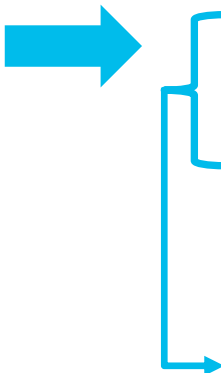
Variables

Calendars

Schedules

Tasks

Events & Webhooks



PermissionsGroups (1)TagsSecurity credentialsAccess Advisor

Sign-in credentials

Summary

User does not have console management access

Console password

Disabled | Manage

Assigned MFA device

Not assigned | Manage

Signing certificates

None

Access keys

Use access keys to make programmatic calls to AWS from the AWS CLI, Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time.

For your protection, you should never share your secret keys with anyone. As a best practice, we recommend frequent key rotation.

If you lose or forget your secret key, you cannot retrieve it. Instead, create a new access key and make the old key inactive. Learn more

Create access key

Access key ID	Created	Last used	Status	
AKIAWQ...	2021-02-16 13:40 CDT	2022-04-12 09:47 CDT with ec2 in us-ea...	Active	Make inactive x
AKIAWQ...	2021-06-07 11:44 CDT	2022-03-03 14:33 CDT with ec2 in us-ea...	Active	Make inactive x

AWS Keys

Access Key

AKIAWQ...

Secret Key

.....



Workflows



Runs



Targets



Account Keys



Variables



Calendars



Schedules



Tasks



Events & Webhooks



Google Cloud Platform My First Project Search Products, resources, docs (/)

IAM & Admin

- IAM
- Identity & Organization
- Policy Troubleshooter
- Policy Analyzer
- Organization Policies
- Service Accounts**
- Workload Identity Federat...
- Labels
- Tags
- Settings
- Manage Resources
- Release Notes

Service accounts + CREATE SERVICE ACCOUNT DELETE MANAGE ACCESS REFRESH

Service accounts for project "My First Project"

A service account represents a Google Cloud service identity, such as code running on Compute Engine VMs, App Engine apps, or systems running outside Google. [Learn more about service accounts.](#)

Organization policies can be used to secure service accounts and block risky service account features, such as automatic IAM Grants, key creation/upload, or the creation of service accounts entirely. [Learn more about service account organization policies.](#)

Filter Enter property name or value

Email	Status	Name	Description	Key ID	Key creatio	Actions
<input type="checkbox"/> cloudair@custom-vigil-340215.iam.gserviceaccount.com	✓	cloudAIR		f1523f9cebe...	Feb 3, 202	⋮
<input type="checkbox"/> 883586247119-compute@developer.gserviceaccount.com	✓	Compute Engine default service account		No keys		⋮





Workflows

Runs

Targets

Account Keys

Variables

Calendars

Schedules

Tasks

Events & Webhooks

Google Cloud Platform My First Project Search Products, resources, docs (/)

IAM & Admin

IAM

Identity & Organization

Policy Troubleshooter

Policy Analyzer

Organization Policies

Service Accounts

Workload Identity Federat...

Labels

Tags

Settings

Manage Resources

Release Notes

Service accounts

+ CREATE SERVICE ACCOUNT

DELETE

MANAGE ACCESS

REFRESH

Service accounts for project "My First Project"

A service account represents a Google Cloud service identity, such as code running on Compute Engine VMs, App Engine apps, or systems running outside Google. [Learn more about service accounts.](#)

Organization policies can be used to secure service accounts and block risky service account features, such as automatic IAM Grants, key creation/upload, or the creation of service accounts entirely. [Learn more about service account organization policies.](#)

Filter Enter property name or value

<input type="checkbox"/>	Email	Status	Name	Description	Key ID	Key creatio	Actions
<input type="checkbox"/>	cloudair@custom-vigil-340215.iam.gserviceaccount.com	✓	cloudAIR		f1523f9cebe...	Feb 3, 202	⋮
<input type="checkbox"/>	883586247119-compute@developer.gservice						⋮

Create private key for "Test"

Downloads a file that contains the private key. Store the file securely because this key can't be recovered if lost.

Key type

☒ JSON

Recommended










☐ P12

For backward compatibility with code using the P12 format

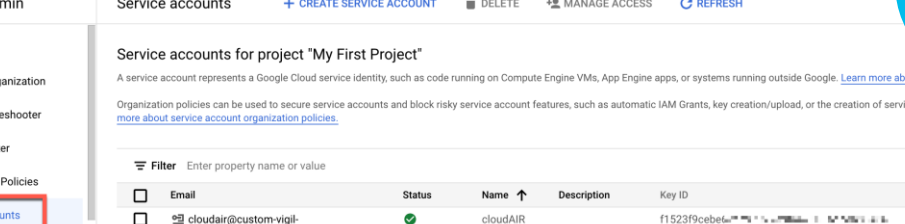
CANCEL

CREATE



-  Workflows
-  Runs
-  Targets
-  **Account Keys**
-  Variables
-  Calendars
-  Schedules
-  Tasks
-  Events & Webhooks



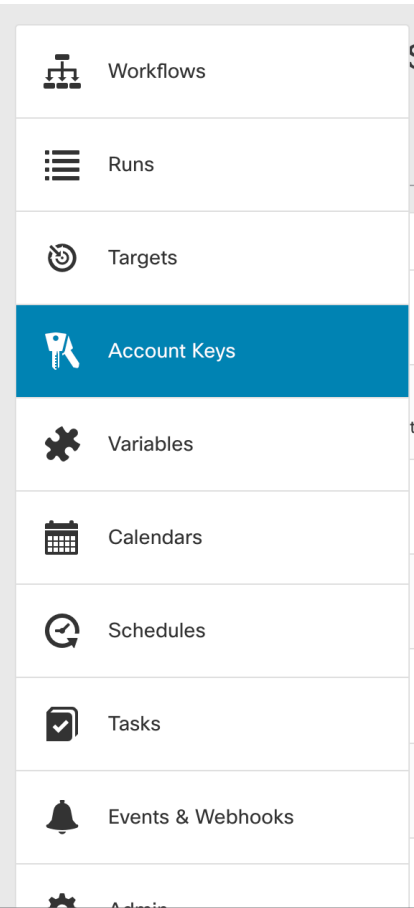


The screenshot shows the Google Cloud IAM & Admin console for project "My First Project". The left sidebar has the "Service Accounts" menu item highlighted. The main content area displays the "Service accounts for project 'My First Project'" page. It includes a table of service accounts with columns: Email, Status, Name, Description, Key ID, Key created, and Actions. One service account is listed: cloudair@custom-vigil-340215.iam.gserviceaccount.com. A modal dialog titled "Create private key for 'Test'" is open, showing a JSON key file content.

Email	Status	Name	Description	Key ID	Key created	Actions
cloudair@custom-vigil-340215.iam.gserviceaccount.com	✓	cloudAIR		f1523f9cebe...	Feb 3, 202	⋮

```

1 {
2   "type": "service_account",
3   "project_id": "custom-vigil-340215",
4   "private_key_id": "84b0982d285f2b051...",
5   "private_key": "-----BEGIN PRIVATE KEY-----\nmIIEvIBADnBqkqhkiG9w0BAQEEFAASCBKgug5KAgEAAoIBAQONk8TQTS1rNy23\nm8Yw+h3YrmQEXgKbTeCsi13Sc24g51G24IEAT7030",
6   "client_email": "test-76@custom-vigil-340215.iam.gserviceaccount.com",
7   "client_id": "115180...",
8   "auth_url": "https://accounts.google.com/g/oauth2/auth",
9   "token_url": "https://oauth2.googleapis.com/token",
10  "auth_provider_x509_cert_url": "https://www.googleapis.com/oauth2/v1/certs",
11  "client_x509_cert_url": "https://www.googleapis.com/robot/v1/metadata/x509/test-76%40custom-vigil-340215.iam.gserviceaccount.com"
12 }
  
```

Workflows

Runs

Targets

Account Keys

Variables

Calendars

Schedules

Tasks

Events & Webhooks

Alerts



```
PS /home/brian> az ad sp create-for-rbac
The underlying Active Directory Graph API will be replaced by Microsoft Graph API in Azure CLI 2.37.0. Please carefully review all breaking changes introduced during this migration: https://docs.microsoft.com/cli/azure/microsoft-graph-migration
The output includes credentials that you must protect. Be sure that you do not include these credentials in your code or check the credentials in to your source control. For more information, see https://aka.ms/azadsp-cli
{
  "appId": "c8743a24-41e1-4286-a011-123456789012",
  "displayName": "azu...",
  "password": "acRb6n...",
  "tenant": "74c1be48-1f10-4048-b87d-74f1f5e16142"
}
PS /home/brian> az account show --query id -o tsv
bac19e8c-321f-4048-b87d-74f1f5e16142
PS /home/brian>
```

```
> az ad ap create-for-rbac
```

clientId
clientSecret
tenantId

```
> az account show --query id -o tsv
```

subscriptionId

- Workflows
- Runs
- Targets
- Account Keys**
- Variables
- Calendars
- Schedules
- Tasks
- Events & Webhooks



Microsoft Azure | Search resources, services, and docs (G+ /)

Home > Subscriptions > Azure subscription 1

Subscriptions

Default Directory

+ Add Manage Policies ...

Search... Subscriptions == global filter

My role == all

Status == all

+ Add filter

Showing 1 to 1 of 1

Subscription name ↑↓

Azure subscription 1 ...

< Previous Page 1 of 1 Next >

Azure subscription 1 | Access control (IAM)

Subscription

Search (Cmd+ /)

+ Add Download role assignments Edit columns Refresh Remove

Check access **Role assignments** Roles Deny assignments Classic administrators

Number of role assignments for this subscription 2 2000

Search by name or email Type: All Role: All Scope: All scopes Group by: Role

2 items (1 Users, 1 Service Principals)

Name	Type	Role	Scope	Condition
Contributor				
<input type="checkbox"/> azure-cli-2022-01	App	Contributor	This resource	None
Owner				
<input type="checkbox"/> BS Brian Sak	User	Owner	This resource	None

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Security
Events
Cost Management
Cost analysis
Cost alerts
Budgets
Advisor recommendations
Billing
Invoices
Settings

"displayName": "azure-cli-2022-05-07-01-25-20",



Workflows



Runs



Targets



Account Keys



Variables



Calendars



Schedules



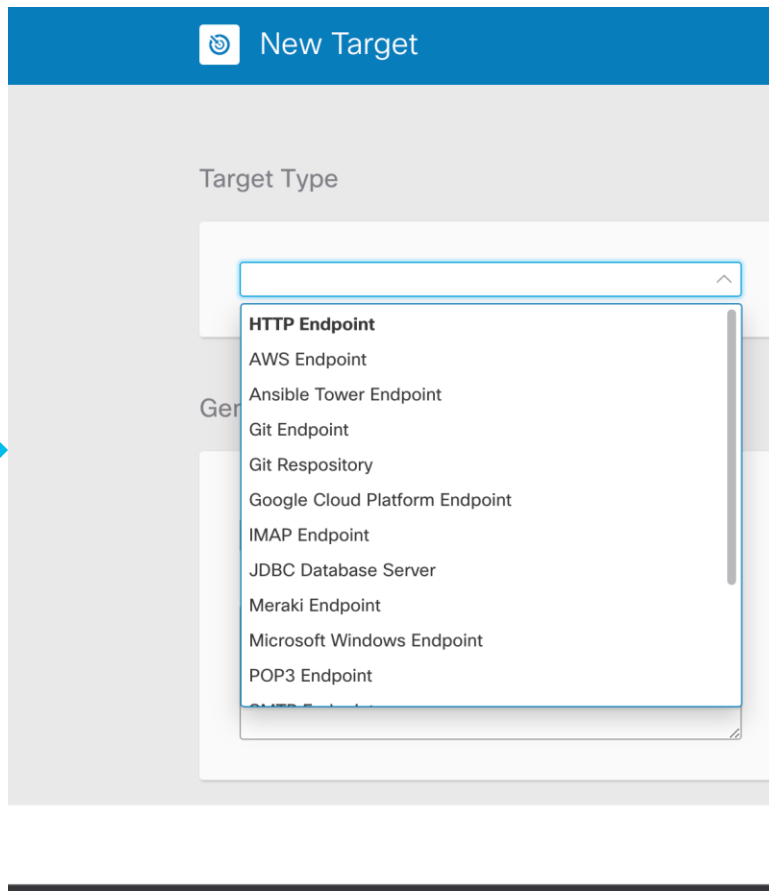
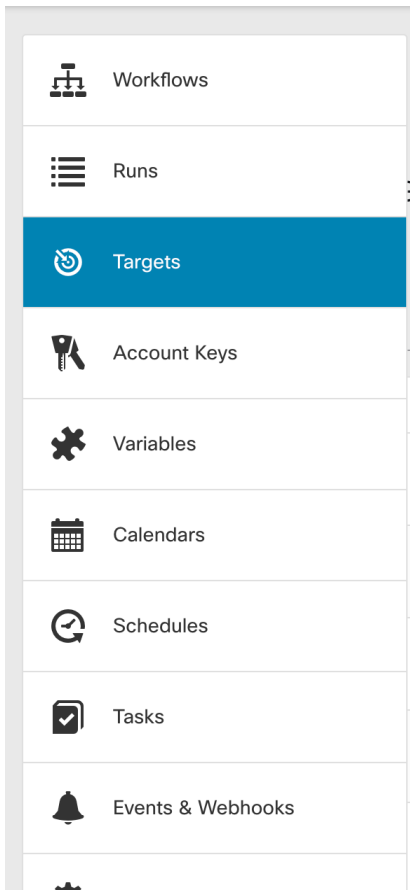
Tasks

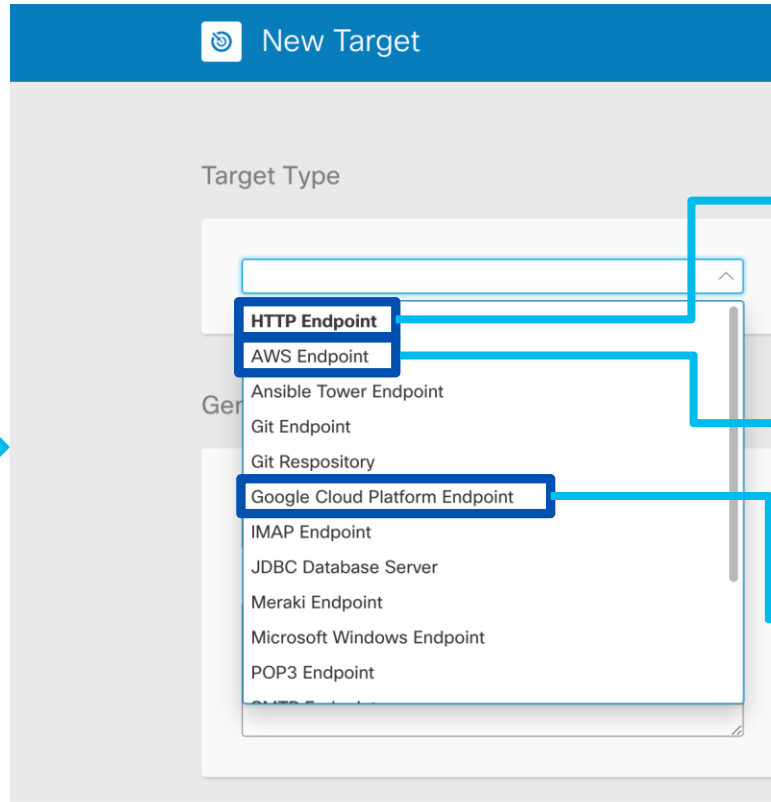
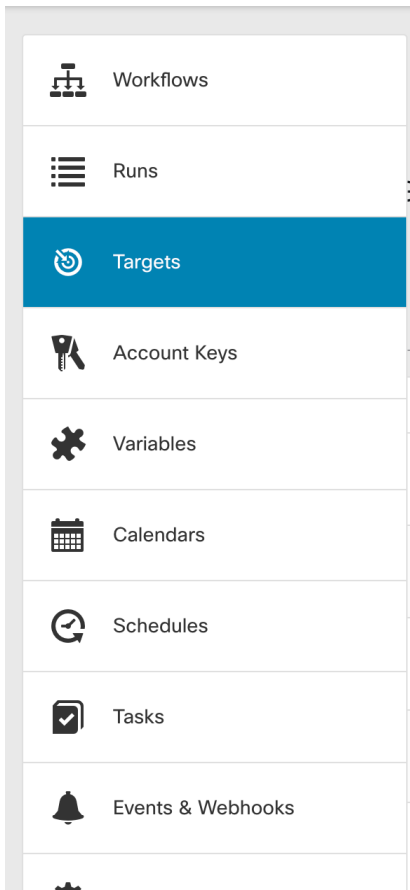


Events & Webhooks



DevNet Zone





Workflows

Runs

Targets

Account Keys

Variables

Calendars

Schedules

Tasks

Events & Webhooks



General

Display Name

AWS_Target

Description

Account Keys

* Default Account Keys

AWS_dc-sre

AWS

Region

us-east-1



CISCO Live!

DevNet Zone

#CiscoLiveAPJC DEVNET-3140

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

31



Workflows

Runs

Targets

Account Keys

Variables

Calendars

Schedules

Tasks

Events & Webhooks



General

Display Name

GCP Compute Target

Description

Account Keys

* Default Account Keys

GCP Auth

GoogleCloudPlatform

* Protocol

HTTPS

Host/IPAddress

compute.googleapis.com

Scope

https://www.googleapis.com/auth/compute

CISCO Live!

DevNet Zone

#CiscoLiveAPJC DEVNET-3140

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

32



Workflows



Runs



Targets



Account Keys



Variables



Calendars



Schedules



Tasks



Events & Webhooks



CISCO *Live!*

DevNet Zone

General

Display Name

Azure Auth

Description



Authorization

Account Keys

No Account Keys ⓘ

True

Default Account Keys

Select

HTTP

* Protocol

HTTPS

Host/IPAddress

login.microsoftonline.com

Port

Path

☐ Disable server certificate validation





Workflows



Runs



Targets



Account Keys



Variables



Calendars



Schedules



Tasks



Events & Webhooks



General

Display Name

Azure API



Actions

Description

Account Keys

No Account Keys ⓘ

True

Default Account Keys

Select

HTTP

Protocol

HTTPS

Host/IPAddress

management.azure.com

Port

Path

☐ Disable server certificate validation

CISCO Live!

DevNet Zone

#CiscoLiveAPJC DEVNET-3140

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

34

The background is a dark blue gradient. On the right side, there is a dense cluster of circles in various sizes and colors, including light blue, teal, green, orange, yellow, and red. Some circles are solid, while others are semi-transparent, creating a layered effect. The circles appear to be floating or moving towards the right.

Enough Talk, Demo Time!

Session Surveys

We would love to know your feedback on this session!

- Complete the session surveys in the Cisco Events mobile app. You'll earn some points in the Cisco Live Game and potentially win a prize.
- Complete a minimum of four session and the overall event surveys to claim a Cisco Live cable bag.

Continue your education



Visit the Cisco Showcase for related demos



Book your one-on-one Meet the Expert meeting



Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs



Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.



Learn



Cisco U.

IT learning hub that guides teams and learners toward their goals

Cisco Digital Learning

Subscription-based product, technology, and certification training

Cisco Modeling Labs

Network simulation platform for design, testing, and troubleshooting

Cisco Learning Network

Resource community portal for certifications and learning



Train



Cisco Training Bootcamps

Intensive team & individual automation and technology training programs

Cisco Learning Partner Program

Authorized training partners supporting Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training

Accelerated curriculum of product, technology, and certification courses



Certify



Cisco Certifications and Specialist Certifications

Award-winning certification program empowers students and IT Professionals to advance their technical careers

Cisco Guided Study Groups

180-day certification prep program with learning and support

Cisco Continuing Education Program

Recertification training options for Cisco certified individuals





The bridge to possible

Thank you

CISCO *Live!*

DevNet Zone

#CiscoLiveAPJC

CISCO *Live!*



#CiscoLiveAPJC