

Automating Away Your DevSecOps Toil



**Application Support and
Operations takes up to 55% of
Developer time**

DevSecOps

- Certificate Renewals
- Permissions



DevSecOps

- Certificate Renewals
- Permissions

Two Outages:
April 2023



DevSecOps



DevSecOps



DevSecOps



20:14

LTE   40%

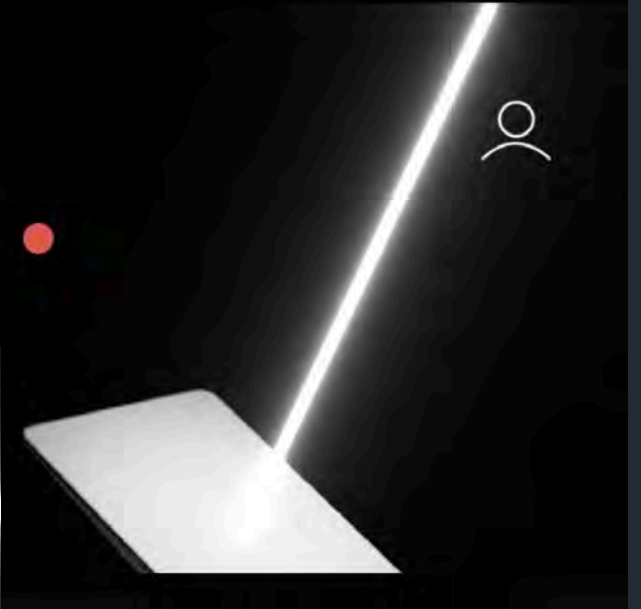
MOOSI >

OFFLINE ●

DIORO >

FUERA DE LÍNEA ●

Problema de red | Descargando actualización



DevSecOps



 **Elon Musk**   · Apr 7, 2023 

@elonmusk · [Follow](#)

Sorry, slight glitch with [@SpaceX](#) Starlink. Coming back online now.

 **Elon Musk**  

@elonmusk · [Follow](#)

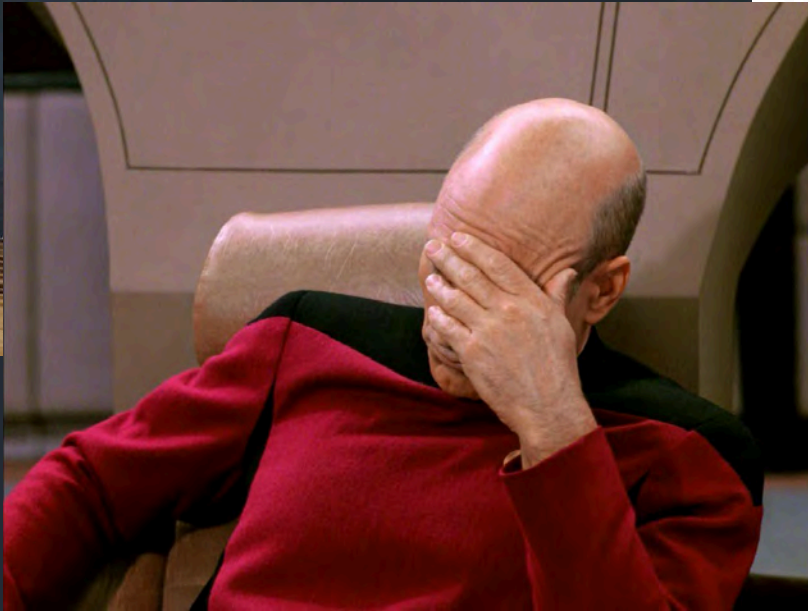
Caused by expired ground station cert. We're scrubbing the system for other single-point vulnerabilities.

9:00 PM · Apr 7, 2023 

 19.2K  Reply  Copy link

[Read 1.5K replies](#)

DevSecOps



Elon Musk   · Apr 7, 2023

@elonmusk · [Follow](#)

Sorry, slight glitch with [@SpaceX](#) Starlink. Coming back online now.



Elon Musk  

@elonmusk · [Follow](#)

Caused by expired ground station cert. We're scrubbing the system for other single-point vulnerabilities.

9:00 PM · Apr 7, 2023



19.2K



Reply



Copy link

[Read 1.5K replies](#)

DevSecOps

- Certificate Renewals
- Permissions

Two Outages:
April 2023




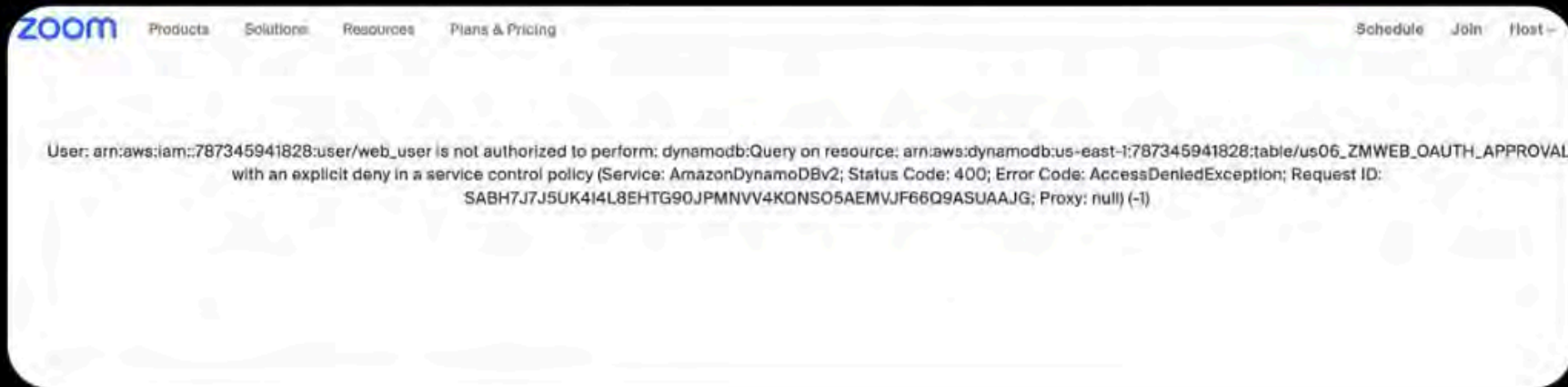
DevSecOps



Arkadiy Tetelman 

@arkadiyt

Zoom having an outage due to a misconfigured SCP. Classic 



4:10 PM · Apr 3, 2023 · **69.4K** Views

Automation

the state of being
operated automatically





UNSKRIPT, INC.



Open Source RunBook Automation



Open Source RunBook Automation

Based on Jupyter Notebooks

The screenshot displays the unSkript web interface. At the top, there is a navigation bar with the unSkript logo and various menu items: xRunBooks, Proxy, Executions, Events, Actions, Requests, and More. A user profile for 'doug' is visible in the top right. The main content area is titled 'k8s-log-healthcheck' and includes a 'Proxy: Staging' indicator, 'Undo', 'Save', 'Add', 'Parameters', 'Close', and a 'Run XRunBook' button. Below this, a 'unSkript Internal' section shows a 'Completed' status and a 'Run Action' button. The central part of the interface features a 'Kubernetes Healthcheck Runbook' with a description: 'This runbook grabs all of your K8s pods, reads the logs from them, and then output any WARNING logs from the last hour.' It includes a list of steps: Step 1: Get all of the pods; Step 2: get all of the logs for each pod; Step 3: parse the logs for warnings in the last hour; Step 4: if there are warnings, send a Slack alert. On the right side, a configuration panel for the 'Kubectl list pods' action is shown, including a 'Credential' dropdown set to 'DevEKS', a checked 'Print Output' option, and a 'Required' section with a 'Namespace*' field containing the value 'namespace'.

<http://runbooks.sh>

Jupyter Notebooks

- **Online - Collaborative**



Jupyter Notebooks

- **Online – Collaborative**
- **Python: No Domain Specific Language**

Jupyter Notebooks

- **Online – Collaborative**
- **Python: No Domain Specific Language**
- **Documentation via text/markdown**

Jupyter Notebooks

- **Online – Collaborative**
- **Python: No Domain Specific Language**
- **Documentation via text/markdown**
- **Easy Automation**

DevSecOps

- Certificate Renewals
- Permissions



Certificate Renewal



Renew AWS SSL Certificates that are close to expiration

CLOUDOPS, DEVOPS, SECOPS

Certificate Renewal



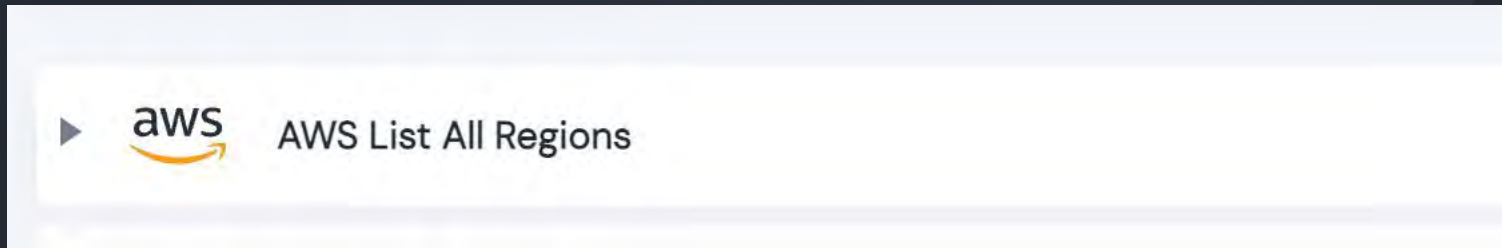
Renew AWS SSL Certificates that are close to expiration

CLOUDOPS, DEVOPS, SECOPS

| Inputs | | Outputs | |
|----------------|-----------------------------|---------|-------------------------------------|
| Name | Description | Value | Required |
| environment | Name of the environme... | Doug | <input checked="" type="checkbox"/> |
| region | List of regions which ha... | (D) [] | <input type="checkbox"/> |
| threshold_days | Threshold number of da... | 5 | <input type="checkbox"/> |

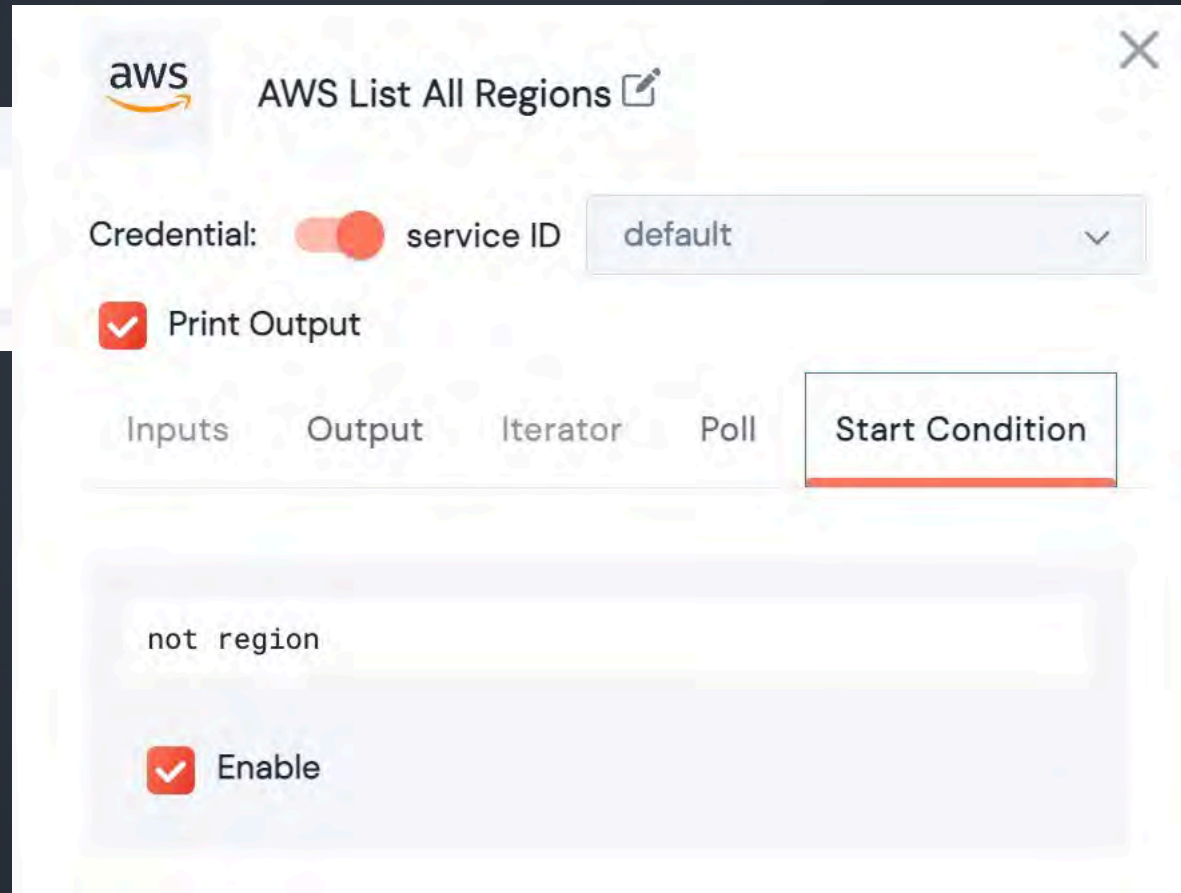
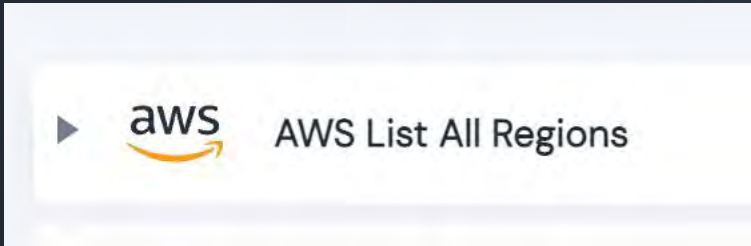
Certificate Renewal

Step 1



Certificate Renewal

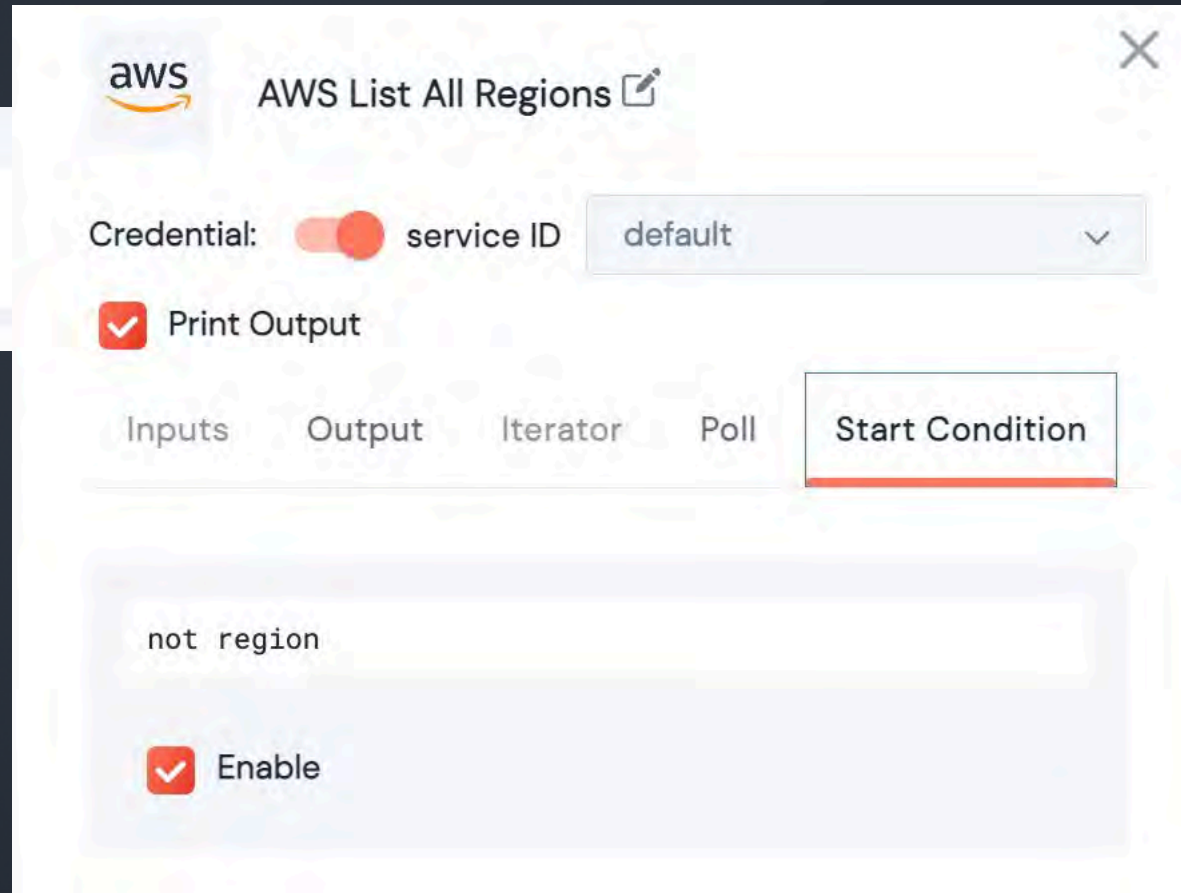
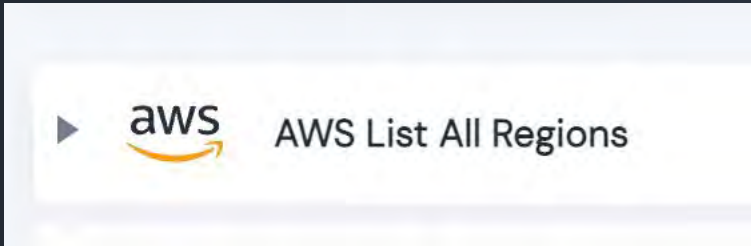
Step 1



A configuration window for the "aws" service, titled "AWS List All Regions". The window includes a close button in the top right corner. Below the title, there is a "Credential:" section with a red toggle switch, the text "service ID", and a dropdown menu currently showing "default". A "Print Output" checkbox is checked. Below this is a horizontal menu with five tabs: "Inputs", "Output", "Iterator", "Poll", and "Start Condition". The "Start Condition" tab is selected and highlighted with a red underline. The content area under the "Start Condition" tab contains a text input field with the text "not region" and an "Enable" checkbox which is checked.

Certificate Renewal

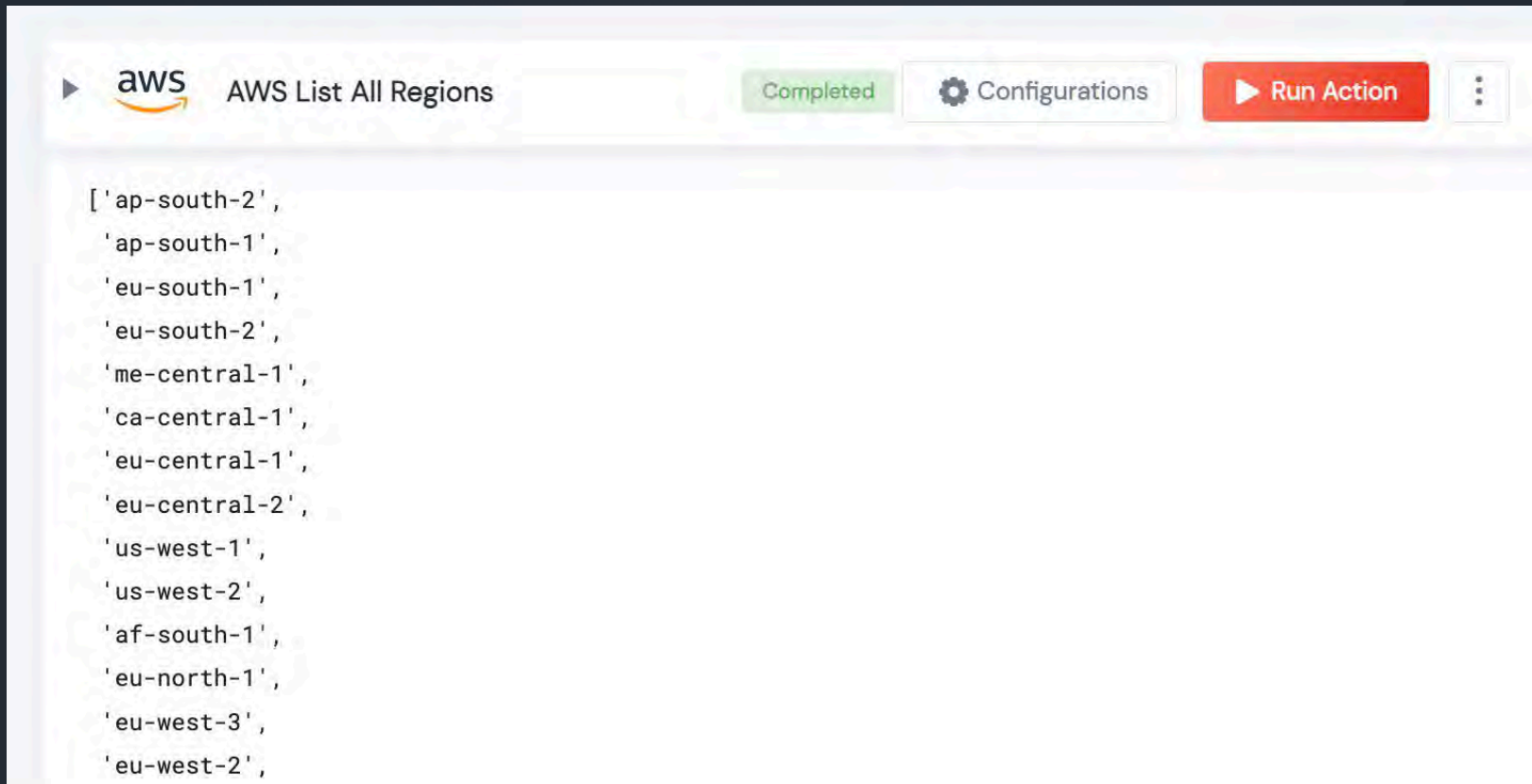
Step 1



A configuration window for the "aws AWS List All Regions" step. The window title is "aws AWS List All Regions" with a close button (X) in the top right corner. Below the title, there is a "Credential:" section with a red toggle switch, the text "service ID", and a dropdown menu showing "default". A "Print Output" checkbox is checked. Below this is a tabbed interface with tabs for "Inputs", "Output", "Iterator", "Poll", and "Start Condition". The "Start Condition" tab is selected and highlighted with a red underline. The content of the "Start Condition" tab is a text area containing the code "not region". At the bottom, there is an "Enable" checkbox which is checked.

Certificate Renewal

Step 1



The screenshot shows the AWS IAM console interface. At the top, there is a breadcrumb trail: 'aws' followed by 'AWS List All Regions'. To the right of the breadcrumb, there is a green 'Completed' status indicator, a 'Configurations' button with a gear icon, a red 'Run Action' button with a play icon, and a three-dot menu icon. Below the breadcrumb, the output of the 'List All Regions' action is displayed as a JSON array of region names, each enclosed in single quotes and separated by commas. The visible regions are: 'ap-south-2', 'ap-south-1', 'eu-south-1', 'eu-south-2', 'me-central-1', 'ca-central-1', 'eu-central-1', 'eu-central-2', 'us-west-1', 'us-west-2', 'af-south-1', 'eu-north-1', 'eu-west-3', and 'eu-west-2'.

```
[ 'ap-south-2',  
  'ap-south-1',  
  'eu-south-1',  
  'eu-south-2',  
  'me-central-1',  
  'ca-central-1',  
  'eu-central-1',  
  'eu-central-2',  
  'us-west-1',  
  'us-west-2',  
  'af-south-1',  
  'eu-north-1',  
  'eu-west-3',  
  'eu-west-2',
```

Certificate Renewal

Step 2



Certificate Renewal

Step 2

The screenshot shows the configuration for the 'List Expiring ACM Certificates' action in the AWS IAM console. The 'Credential' is set to 'service ID' with a dropdown menu showing 'default'. The 'Print Output' checkbox is checked. The 'Iterator' tab is selected, showing the 'List to Iterate' section with 'List Item Type' set to 'Single Value' and 'region' entered in the text field. The 'Loop Parameter' section also has 'region' entered in the dropdown menu.

aws List Expiring ACM Certificates

Credential: service ID default

Print Output

Inputs Output **Iterator** Poll Start Condition

List to Iterate

List Item Type: Single Value Multiple Values

region

Loop Parameter

region

Certificate Renewal

Step 2

The screenshot shows the configuration for the 'List Expiring ACM Certificates' action in the AWS IAM console. The 'Credential' is set to 'service ID' with a dropdown menu showing 'default'. The 'Print Output' checkbox is checked. The 'Iterator' tab is selected, showing the 'List to Iterate' section with 'List Item Type' set to 'Single Value' and 'region' entered in the text field. The 'Loop Parameter' section also has 'region' entered in the dropdown menu.

aws List Expiring ACM Certificates

Credential: service ID default

Print Output

Inputs Output **Iterator** Poll Start Condition

List to Iterate

List Item Type: Single Value Multiple Values

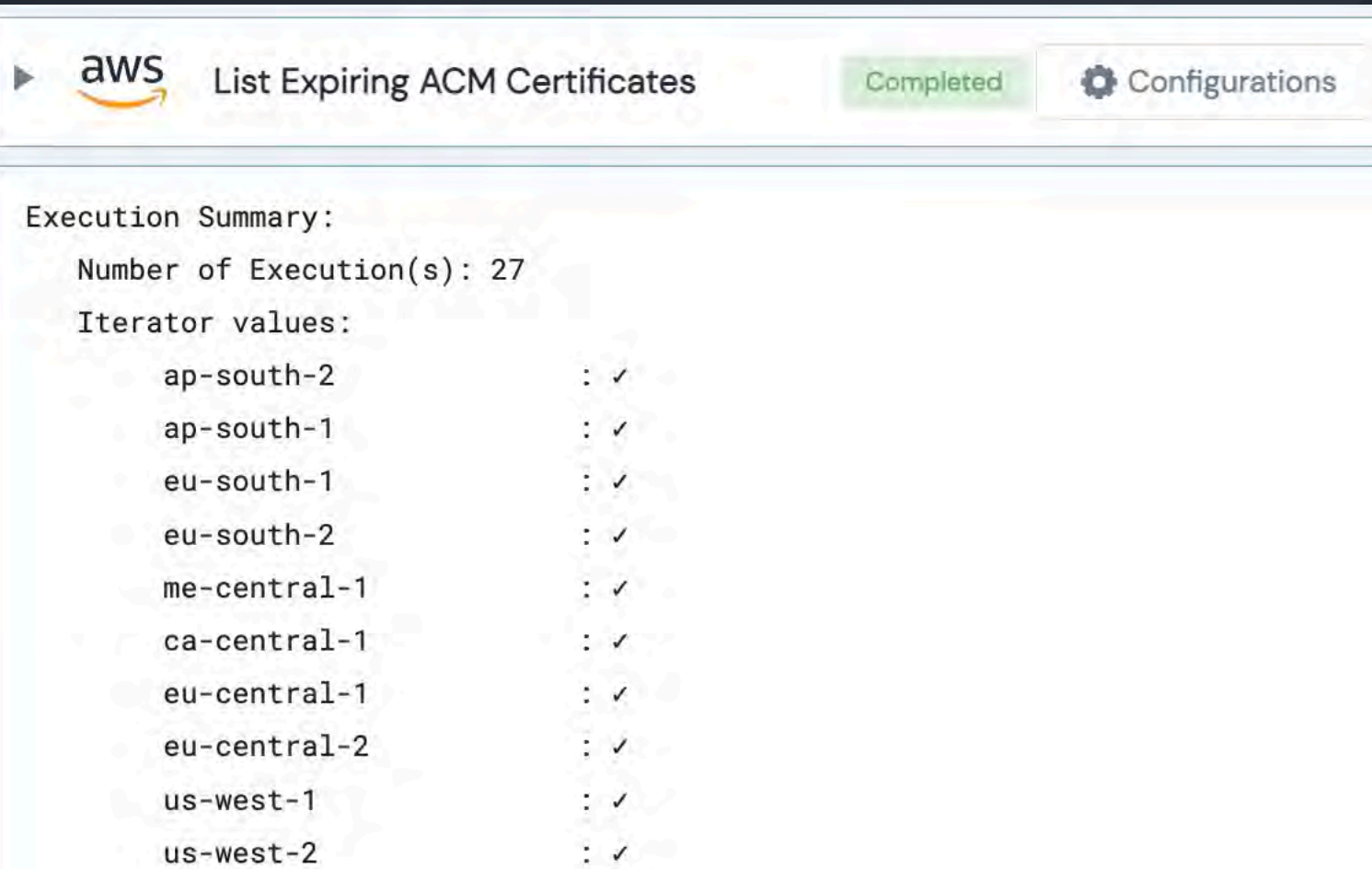
region

Loop Parameter

region

Certificate Renewal

Step 2



The screenshot shows the AWS CLI interface for the command 'aws acm list-expiring-certificates'. The command is marked as 'Completed' and has a 'Configurations' button. The output is as follows:

```
aws acm list-expiring-certificates
Completed Configurations

Execution Summary:
Number of Execution(s): 27
Iterator values:
  ap-south-2      : ✓
  ap-south-1      : ✓
  eu-south-1      : ✓
  eu-south-2      : ✓
  me-central-1    : ✓
  ca-central-1    : ✓
  eu-central-1    : ✓
  eu-central-2    : ✓
  us-west-1       : ✓
  us-west-2       : ✓
```

Certificate Renewal

Step 3

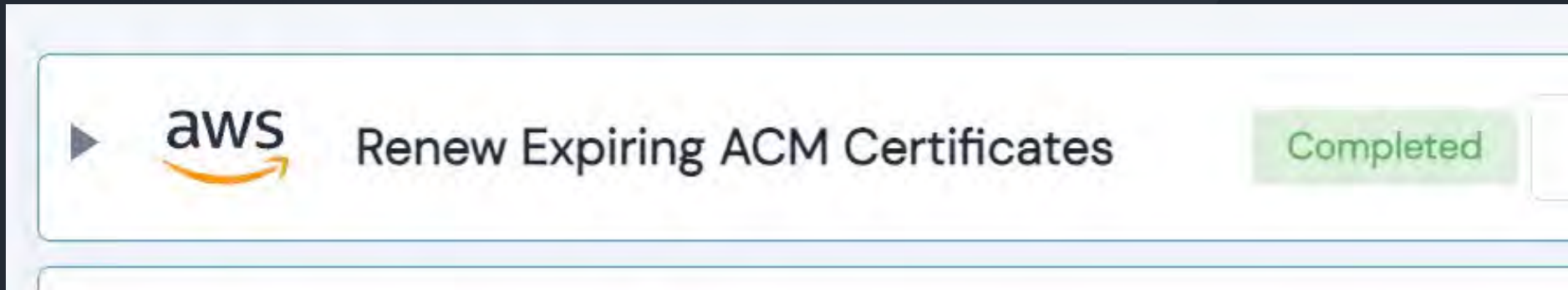
► Create List of Expiring Certificates

Completed

```
[{'region': 'us-west-2', 'certificate': ['arn:aws:acm:us-west-2:4981-8166-56e315005217']}]
```


Certificate Renewal

Step 4



Certificate Renewal

Bonus Step

Schedule Running

▶ Select xRunbook:

▼ Schedule ⓘ :

| | | |
|---------------|--------------------|---------------------|
| Minute | Hour | Day of Month |
| 0 | 15 | * |
| Month | Day of Week | |
| * | 1 | |

At 03:00 PM, only on Monday
The next run will be at 5/8/2023, 11:00:00 AM (America/New_York)

DevSecOps

- Certificate Renewals
- Permissions



Permissions Toil

The screenshot shows the AWS IAM console interface. At the top, there is a navigation bar with the AWS logo, a 'Services' menu, a search bar, and utility icons like a keyboard shortcut '[Option+S]', a refresh icon, a notification bell, a help icon, and a 'Global' region selector. The user's profile 'AdministratorAccess/doug@unskript.com' is visible in the top right.

The main content area is titled 'IAM > Policies'. It features a header for 'Policies (1157)' with an 'Info' link. Below this is a descriptive text: 'A policy is an object in AWS that defines permissions.' To the right of the text are a refresh button and an 'Actions' dropdown menu containing a prominent blue 'Create policy' button.

A search bar is present with the placeholder text 'Filter policies by property or policy name and press enter'. Below the search bar is a table with columns for 'Policy name' and 'Type'. The first row of the table shows a policy named 'AccessAnalyzerMonitorServicePolicy_DF9LDV4ZLS' with a type of 'Custom-managed'.

On the left side, there is a sidebar with a search bar for 'IAM' and a navigation menu under 'Access management' which includes 'User groups'.

Permissions Toil

editor. i

Policy editor

Visual JSON Actions ▾

▼ EC2 + -

Allow 1 Actions

Specify what actions can be performed on specific resources in EC2.

▼ Actions allowed
Specify actions from the service to be allowed.

Switch to deny permissions i

Manual actions | [Add actions](#)

All EC2 actions (ec2:*)

Access level [Expand all](#) | [Collapse all](#)

- ▶ List (Selected 164/164)
- ▶ Read (Selected 31/31)
- ▶ Write (Selected 399/399)
- ▶ Permissions management (Selected 5/5)
- ▶ Tagging (Selected 2/2)

Required permissions not selected.

AWS Permissions

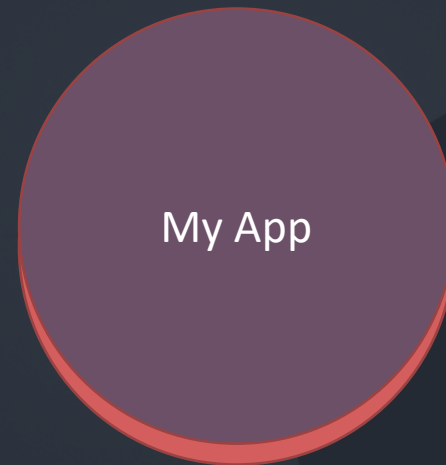


My App

AWS Permissions

Principle of Least Privilege:

Minimum access that is required for the application to run

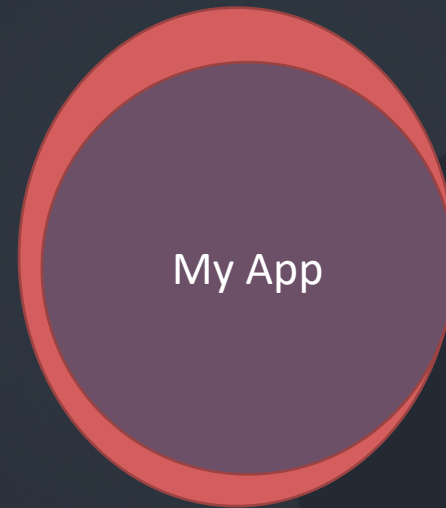


Credentials

AWS Permissions



AWS Permissions



Prod Credentials

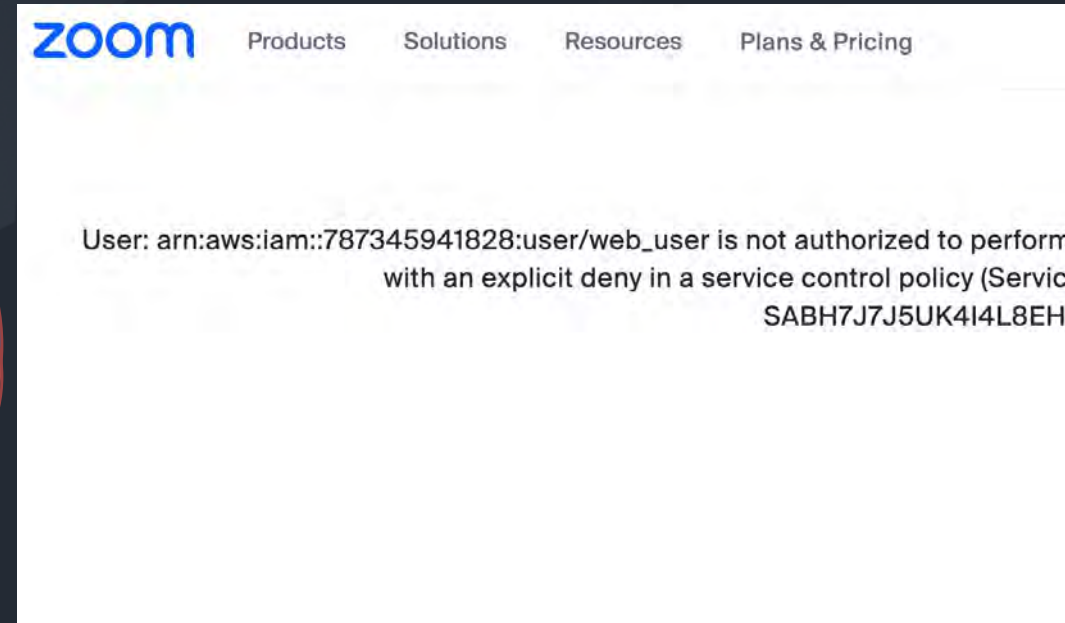
AWS Permissions

Too Little Access



AWS Permissions

Too Little Access



AWS Permissions

Too Much Access



AWS Permissions



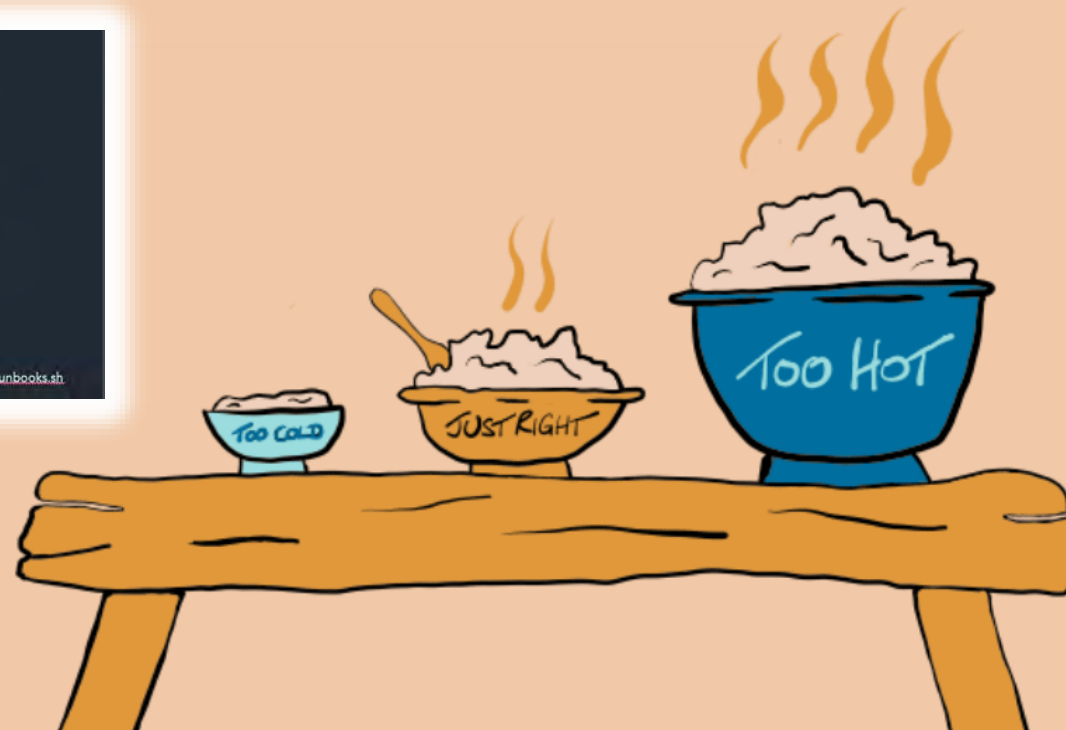
AWS Permissions

AWS Permissions

Too Little Access



<http://runbooks.sh>

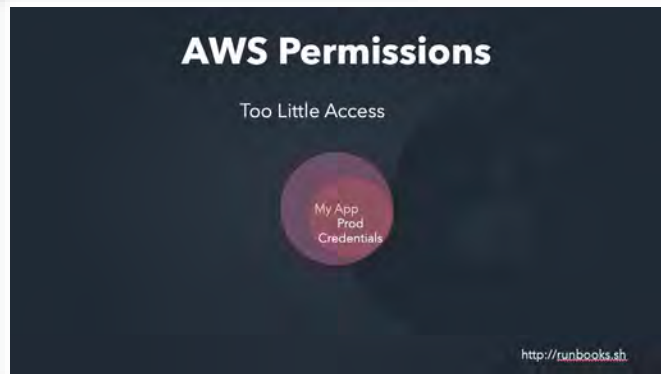
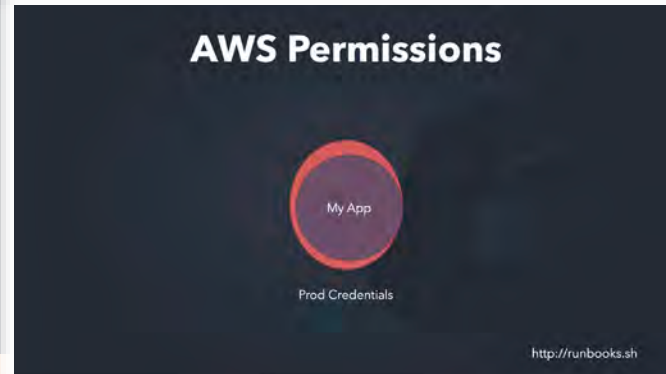


<http://runbooks.sh>

AWS Permissions



AWS Permissions



DevSecOps Toil

editor. i

Policy editor

Visual JSON Actions ▾

▼ EC2 + -

Allow 1 Actions

Specify what actions can be performed on specific resources in EC2.

▼ Actions allowed
Specify actions from the service to be allowed.

Switch to deny permissions i

Manual actions | [Add actions](#)

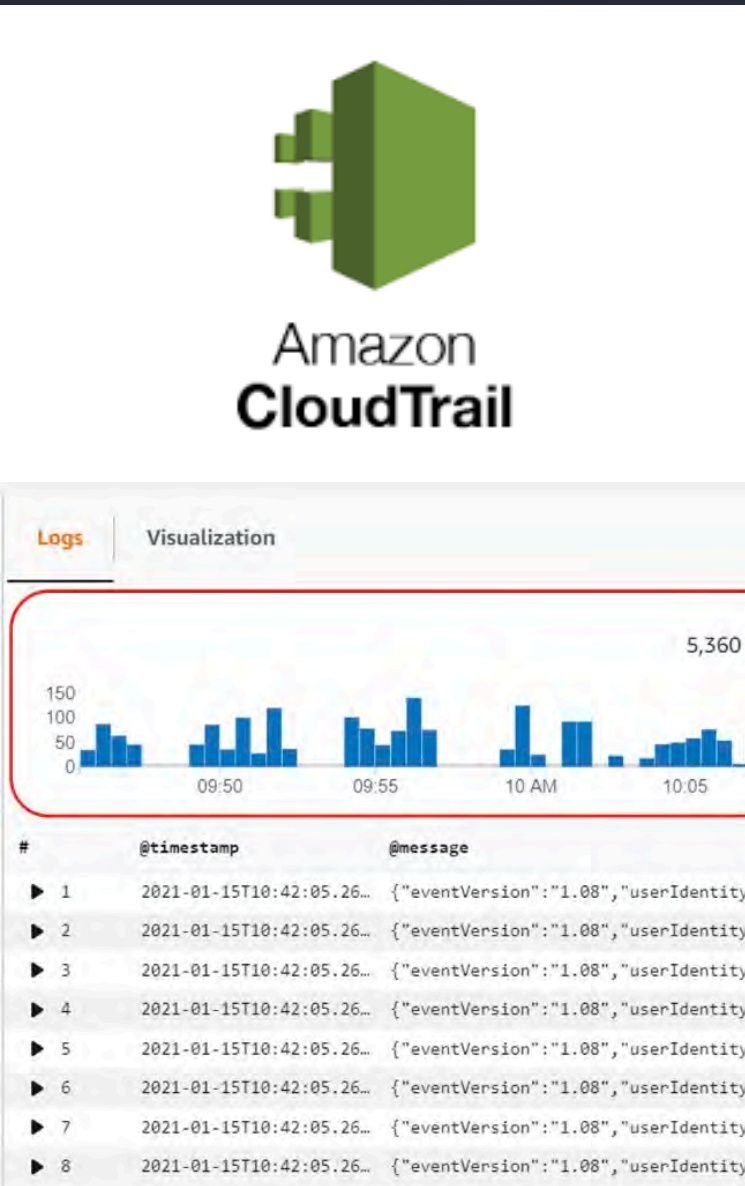
All EC2 actions (ec2:*)

Access level [Expand all](#) | [Collapse all](#)

- ▶ List (Selected 164/164)
- ▶ Read (Selected 31/31)
- ▶ Write (Selected 399/399)
- ▶ Permissions management (Selected 5/5)
- ▶ Tagging (Selected 2/2)

▲ Required permissions not selected.

AWS Permissions

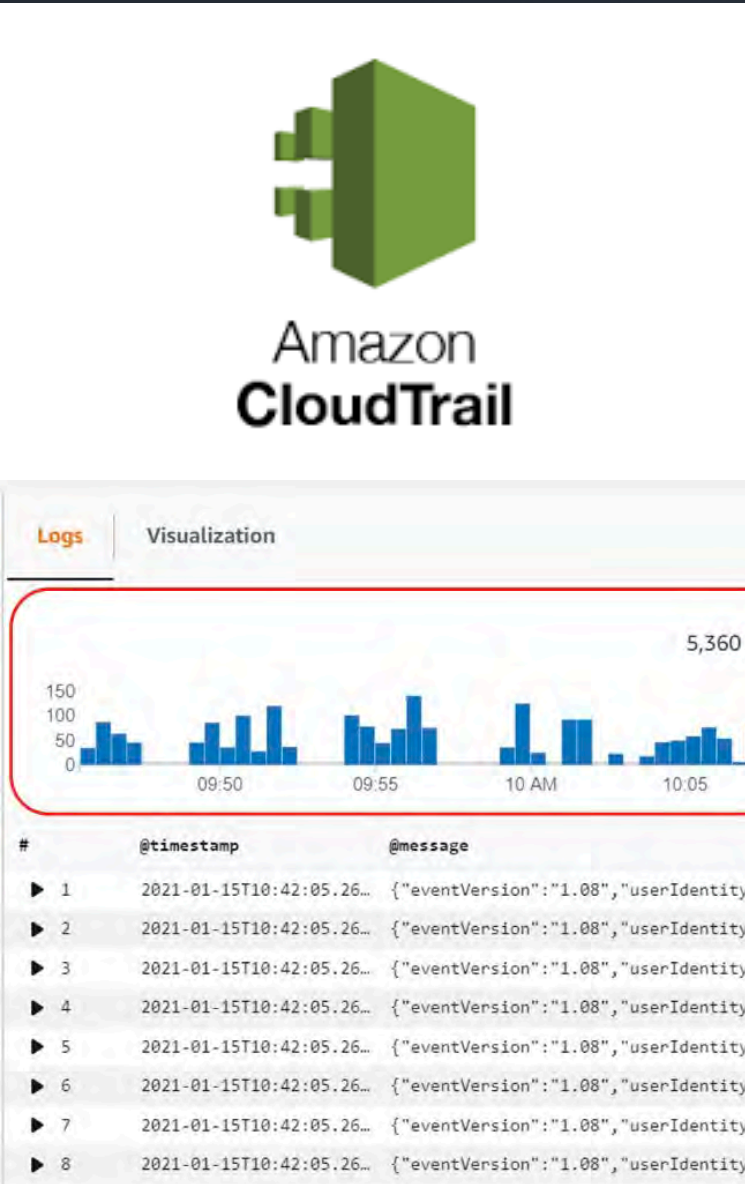


The screenshot displays the Amazon CloudTrail interface. At the top, the Amazon CloudTrail logo is visible. Below it, there are two tabs: "Logs" (selected) and "Visualization". The "Visualization" tab shows a bar chart with a y-axis ranging from 0 to 150 and an x-axis with time markers at 09:50, 09:55, 10 AM, and 10:05. The chart shows several peaks, with the highest reaching approximately 150. To the right of the chart, it indicates "5,360 re". Below the chart is a table with columns for "#", "@timestamp", and "@message". The table contains 8 rows of log entries, each starting with a play button icon and a timestamp of "2021-01-15T10:42:05.26...". The message column contains JSON objects with "eventVersion": "1.08" and "userIdentity": "...".

My App

My Dev Credentials

AWS Permissions



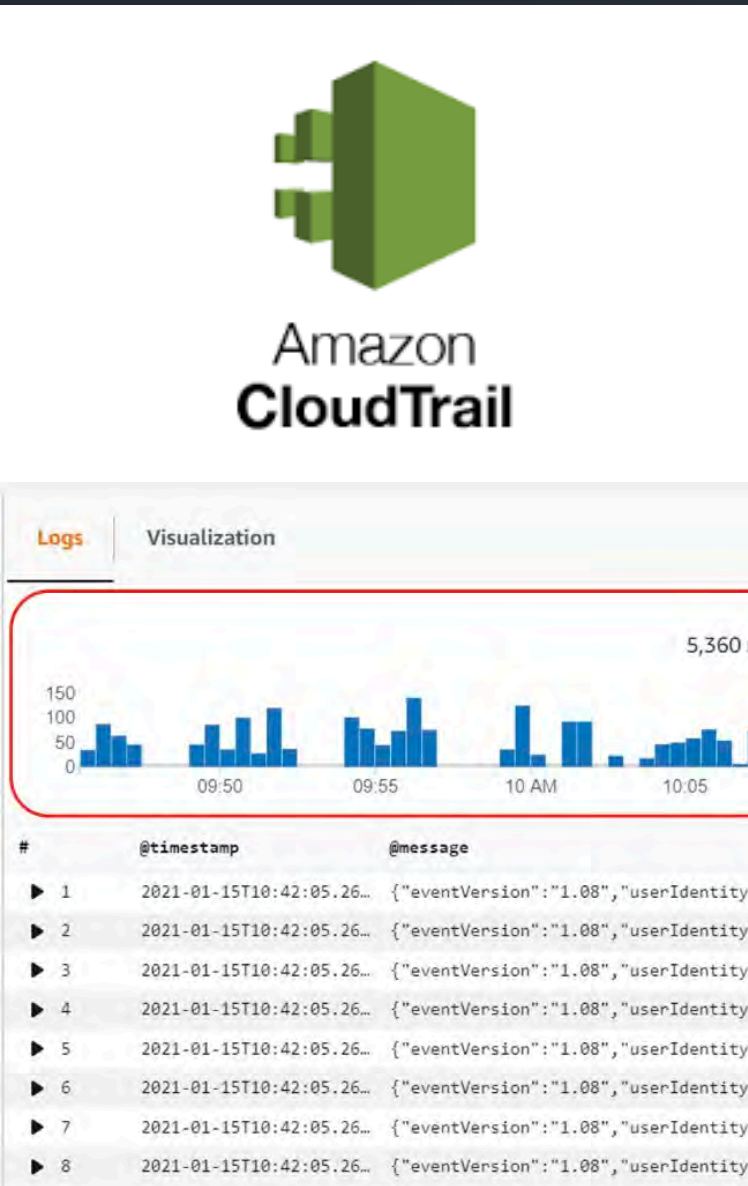
The screenshot displays the Amazon CloudTrail interface. At the top, the Amazon CloudTrail logo is visible. Below it, there are two tabs: 'Logs' (selected) and 'Visualization'. The 'Visualization' tab shows a bar chart with a y-axis ranging from 0 to 150 and an x-axis with time markers at 09:50, 09:55, 10 AM, and 10:05. The chart shows several peaks, with the highest reaching approximately 150. To the right of the chart, it indicates '5,360 re'. Below the chart is a table of log entries with columns for '#', '@timestamp', and '@message'. The first few rows of the table are visible, showing timestamps and JSON messages.

| # | @timestamp | @message |
|-----|---------------------------|--|
| ▶ 1 | 2021-01-15T10:42:05.26... | {"eventVersion":"1.08","userIdentity": |
| ▶ 2 | 2021-01-15T10:42:05.26... | {"eventVersion":"1.08","userIdentity": |
| ▶ 3 | 2021-01-15T10:42:05.26... | {"eventVersion":"1.08","userIdentity": |
| ▶ 4 | 2021-01-15T10:42:05.26... | {"eventVersion":"1.08","userIdentity": |
| ▶ 5 | 2021-01-15T10:42:05.26... | {"eventVersion":"1.08","userIdentity": |
| ▶ 6 | 2021-01-15T10:42:05.26... | {"eventVersion":"1.08","userIdentity": |
| ▶ 7 | 2021-01-15T10:42:05.26... | {"eventVersion":"1.08","userIdentity": |
| ▶ 8 | 2021-01-15T10:42:05.26... | {"eventVersion":"1.08","userIdentity": |

My App

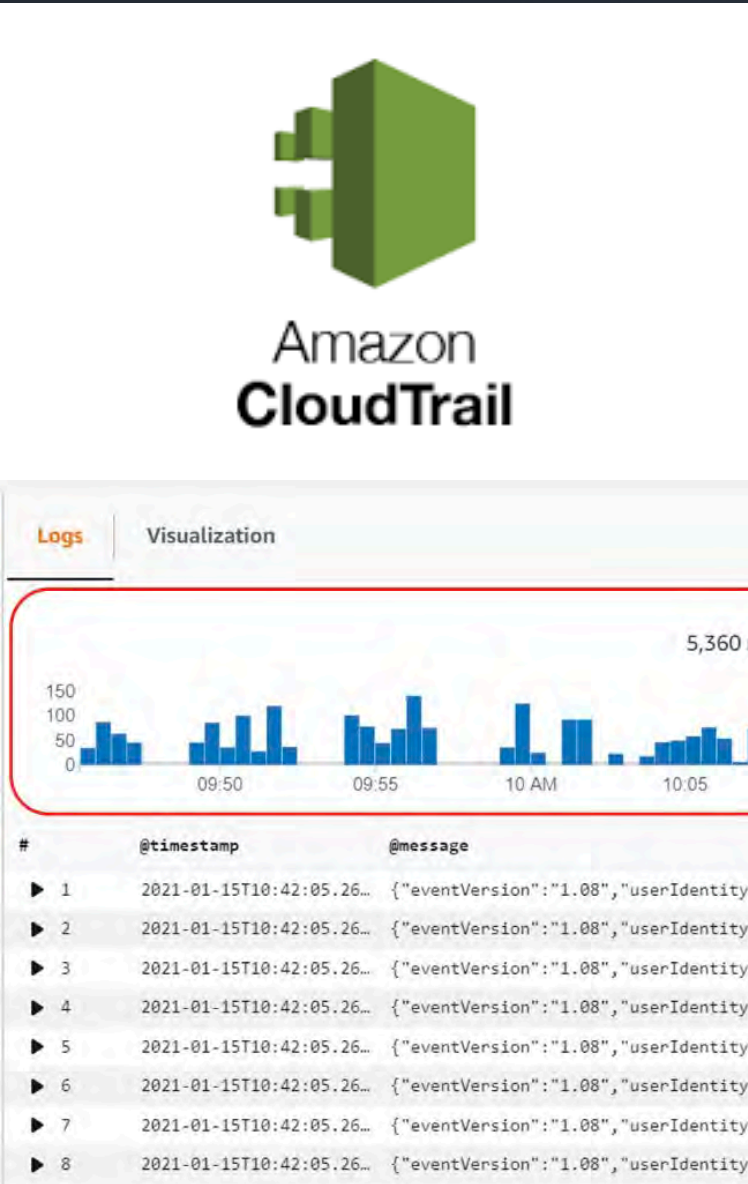
My Dev Credentials

AWS Permissions



- Create Customized Profile
- Create new IAM user

AWS Permissions



AWS Permissions



Logs

Visualization




My App

Inputs

Outputs

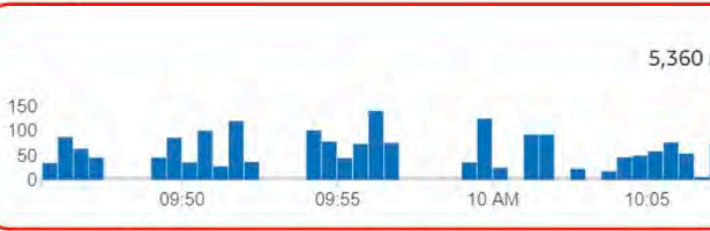
| Name | Description |
|---------------|-----------------------|
| CloudTrailArn | ARN of the CloudTrail |
| policy_name | IAM Policy to be cre |
| region | AWS Region |
| user_name | IAM user to be creat |
| principalARN | ARN to copy usage f |

AWS Permissions



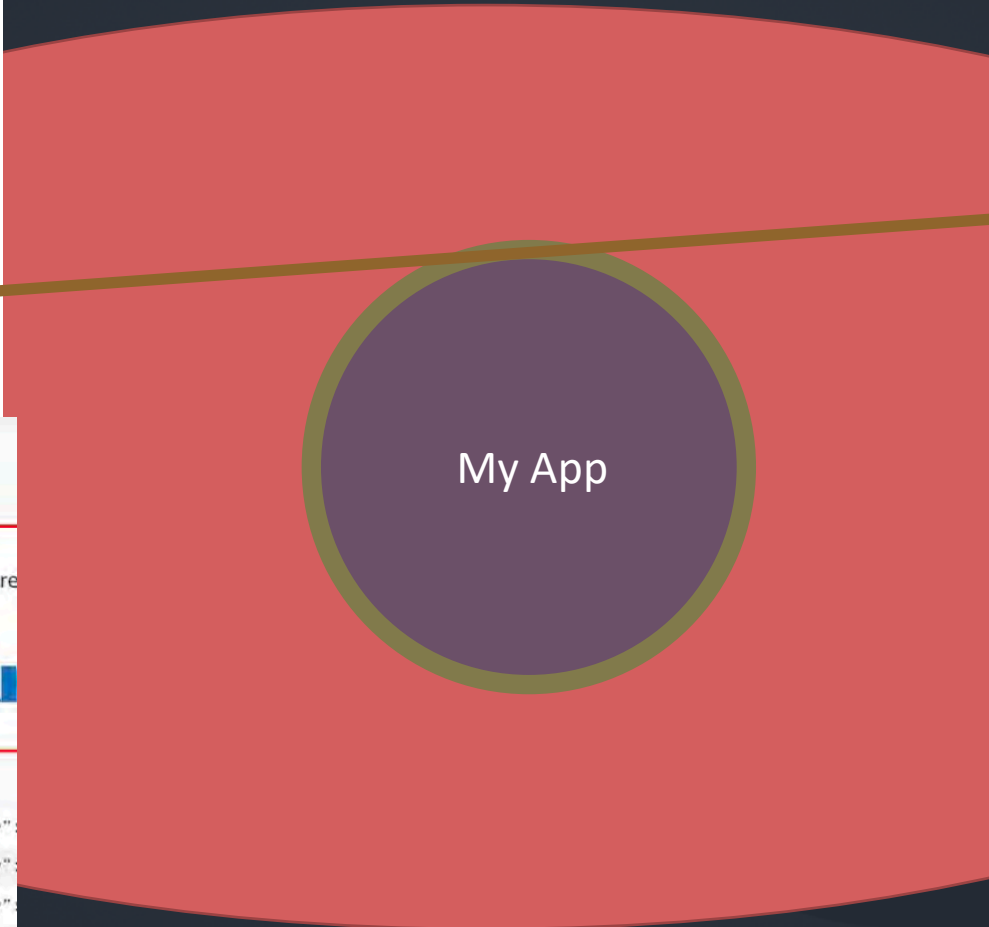
Amazon
CloudTrail

Logs Visualization




5,360 re

| # | @timestamp | @message |
|-----|---------------------------|---|
| ▶ 1 | 2021-01-15T10:42:05.26... | {"eventVersion": "1.08", "userIdentity": ...} |
| ▶ 2 | 2021-01-15T10:42:05.26... | {"eventVersion": "1.08", "userIdentity": ...} |
| ▶ 3 | 2021-01-15T10:42:05.26... | {"eventVersion": "1.08", "userIdentity": ...} |
| ▶ 4 | 2021-01-15T10:42:05.26... | {"eventVersion": "1.08", "userIdentity": ...} |
| ▶ 5 | 2021-01-15T10:42:05.26... | {"eventVersion": "1.08", "userIdentity": ...} |
| ▶ 6 | 2021-01-15T10:42:05.26... | {"eventVersion": "1.08", "userIdentity": ...} |
| ▶ 7 | 2021-01-15T10:42:05.26... | {"eventVersion": "1.08", "userIdentity": ...} |
| ▶ 8 | 2021-01-15T10:42:05.26... | {"eventVersion": "1.08", "userIdentity": ...} |



| Inputs | | Outputs | |
|---------------|--|----------------------|--|
| Name | | Description | |
| CloudTrailArn | | ARN of the CloudTra | |
| policy_name | | IAM Policy to be cre | |
| region | | AWS Region | |
| user_name | | IAM user to be creat | |
| principalARN | | ARN to copy usage f | |


AWS Permissions



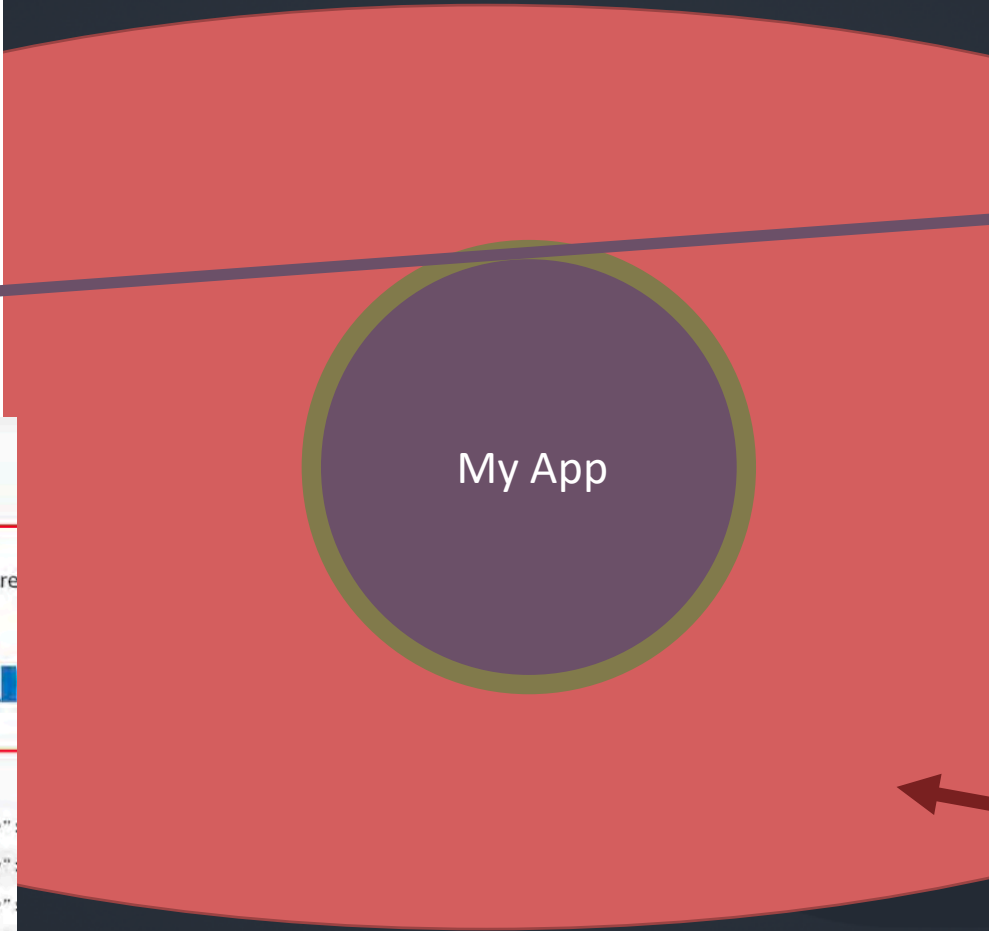
Amazon
CloudTrail

Logs Visualization

5,360 records




| # | @timestamp | @message |
|-----|---------------------------|---|
| ▶ 1 | 2021-01-15T10:42:05.26... | {"eventVersion": "1.08", "userIdentity": ...} |
| ▶ 2 | 2021-01-15T10:42:05.26... | {"eventVersion": "1.08", "userIdentity": ...} |
| ▶ 3 | 2021-01-15T10:42:05.26... | {"eventVersion": "1.08", "userIdentity": ...} |
| ▶ 4 | 2021-01-15T10:42:05.26... | {"eventVersion": "1.08", "userIdentity": ...} |
| ▶ 5 | 2021-01-15T10:42:05.26... | {"eventVersion": "1.08", "userIdentity": ...} |
| ▶ 6 | 2021-01-15T10:42:05.26... | {"eventVersion": "1.08", "userIdentity": ...} |
| ▶ 7 | 2021-01-15T10:42:05.26... | {"eventVersion": "1.08", "userIdentity": ...} |
| ▶ 8 | 2021-01-15T10:42:05.26... | {"eventVersion": "1.08", "userIdentity": ...} |



Inputs Outputs

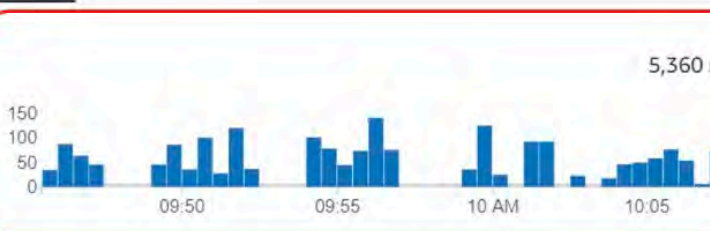
| Name | Description |
|---------------|--------------------------|
| CloudTrailArn | ARN of the CloudTrail |
| policy_name | IAM Policy to be created |
| region | AWS Region |
| user_name | IAM user to be created |
| principalARN | ARN to copy usage from |

AWS Permissions



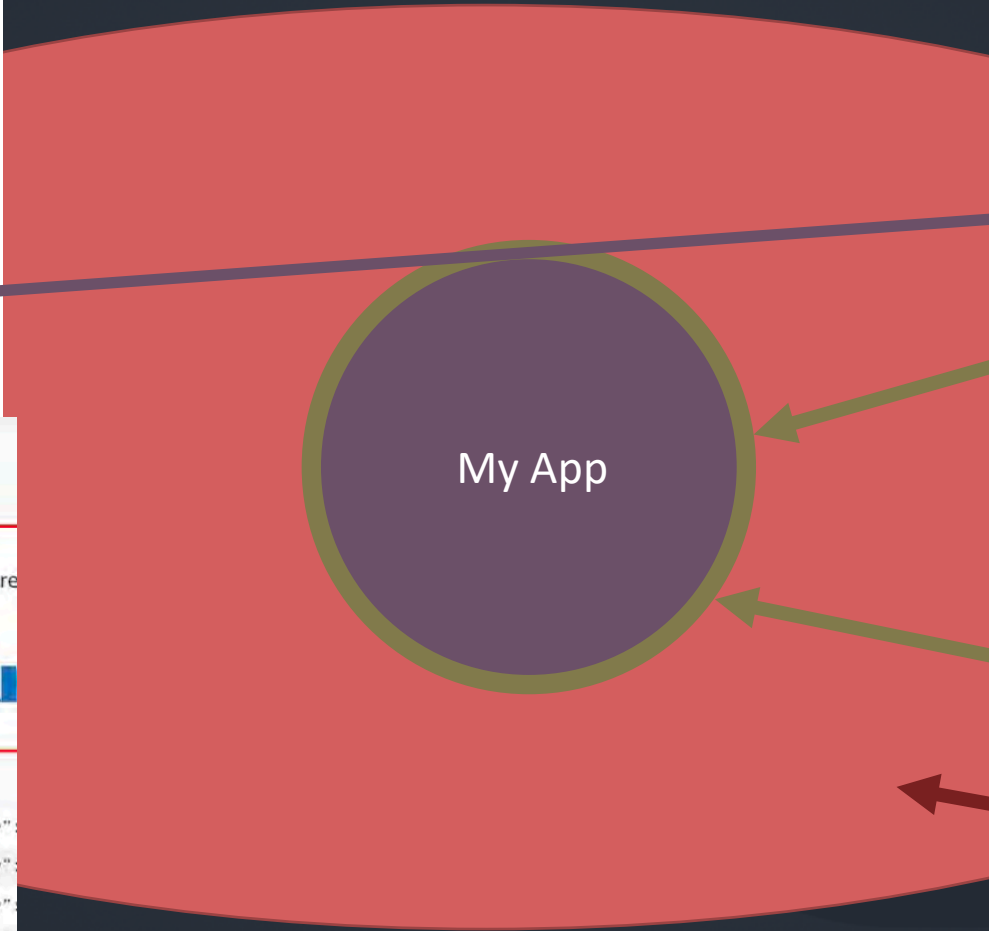
Amazon
CloudTrail

Logs Visualization



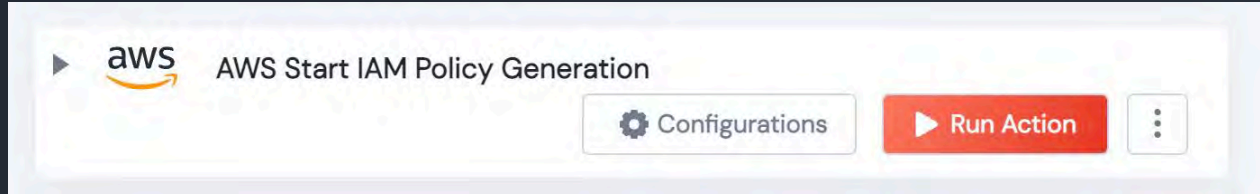
5,360 re

| # | @timestamp | @message |
|-----|---------------------------|--|
| ▶ 1 | 2021-01-15T10:42:05.26... | {"eventVersion": "1.08", "userIdentity": |
| ▶ 2 | 2021-01-15T10:42:05.26... | {"eventVersion": "1.08", "userIdentity": |
| ▶ 3 | 2021-01-15T10:42:05.26... | {"eventVersion": "1.08", "userIdentity": |
| ▶ 4 | 2021-01-15T10:42:05.26... | {"eventVersion": "1.08", "userIdentity": |
| ▶ 5 | 2021-01-15T10:42:05.26... | {"eventVersion": "1.08", "userIdentity": |
| ▶ 6 | 2021-01-15T10:42:05.26... | {"eventVersion": "1.08", "userIdentity": |
| ▶ 7 | 2021-01-15T10:42:05.26... | {"eventVersion": "1.08", "userIdentity": |
| ▶ 8 | 2021-01-15T10:42:05.26... | {"eventVersion": "1.08", "userIdentity": |





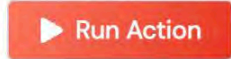

| Inputs | | Outputs | |
|---------------|--|----------------------|--|
| Name | | Description | |
| CloudTrailArn | | ARN of the CloudTra | |
| policy_name | | IAM Policy to be cre | |
| region | | AWS Region | |
| user_name | | IAM user to be creat | |
| principalARN | | ARN to copy usage f | |


AWS Permissions


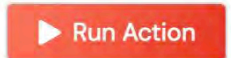



AWS Permissions

▶  AWS Start IAM Policy Generation

▶  AWS Get Generated Policy


  


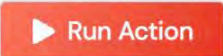

AWS Permissions


The screenshot displays four actions in the AWS IAM console, each with a 'Configurations' button, a 'Run Action' button, and a menu icon:


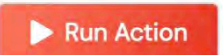

- aws** AWS Start IAM Policy Generation
- aws** AWS Get Generated Policy
- aws** AWS Get Account Number
- clean up policy


AWS Permissions


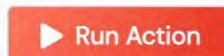

▶  AWS Start IAM Policy Generation

 Configurations  


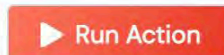

▶  AWS Get Generated Policy


 Configurations  


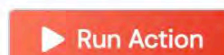

▶  AWS Get Account Number

 Configurations  


▶ clean up policy


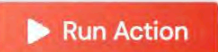

 Configurations  


▶  AWS Create IAM Policy




 Configurations  


AWS Permissions


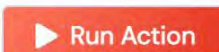

▶  AWS Start IAM Policy Generation

 Configurations  




▶  AWS Get Generated Policy


 Configurations  


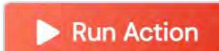

▶  AWS Get Account Number


 Configurations  



▶ clean up policy


 Configurations  



▶  AWS Create IAM Policy

 Configurations  

▶  Create New IAM User

 Configurations 

▶  AWS Attach New Policy to User

 Configurations 

AWS Permissions



Summary

- **DevSecOps:**
 - Manual processes
 - Big Implications
- **Automation**
 - Reduces Manual DevSecOps 'toil'
 - Accuracy and precise
- **Extendible beyond DevSecOps**
 - FinOps
 - DevOps
 - SRE



Resources

- **unSkript**
 - <http://runbooks.sh>
 - <https://unskript.com>



Doug Sillars
Head of Developer Relations
@doug sillars

**Learn more at:
unSkript.com**