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

Elon Musk 🌟 · Apr 7, 2023
@elonmusk · Follow
Sorry, slight glitch with @SpaceX Starlink. Coming back online now.

Elon Musk 🌟 · Apr 7, 2023
@elonmusk · Follow
Caused by expired ground station cert. We’re scrubbing the system for other single-point vulnerabilities.

9:00 PM · Apr 7, 2023
DevSecOps

Elon Musk • Follow
@elonmusk
Sorry, slight glitch with @SpaceX Starlink. Coming back online now.

Elon Musk • Follow
@elonmusk
Caused by expired ground station cert. We’re scrubbing the system for other single-point vulnerabilities.

9:00 PM • Apr 7, 2023
DevSecOps

- Certificate Renewals
- Permissions

Two Outages:
April 2023
DevSecOps

Arkadiy Tetelman
@arkadiyt

Zoom having an outage due to a misconfigured SCP. Classic 😓

with an explicit deny in a service control policy (Service: AmazonDynamoDB; Status Code: 403; Error Code: AccessDeniedException; Request ID: SABH7QJ1SUK444L8HTG90JKPMNV4KON5ORAFMUFF6Q9ASUAAJK; Proxy: null (-))

4:10 PM · Apr 3, 2023 · 69.4K Views

http://runbooks.sh
Automation

the state of being operated automatically
Open Source RunBook Automation

http://runbooks.sh
Open Source RunBook Automation
Based on Jupyter Notebooks

Kubernetes Healthcheck Runbook
This runbook grabs all of your K8s pods, reads the logs from them, and then output any WARNING logs from the last hour.

- 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: Update an .csv, and a.html file

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

http://runbooks.sh
## Certificate Renewal

Renew AWS SSL Certificates that are close to expiration

<table>
<thead>
<tr>
<th>Inputs</th>
<th>Outputs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>environment</td>
<td>Name of the environment</td>
</tr>
<tr>
<td>region</td>
<td>List of regions which have...</td>
</tr>
<tr>
<td>threshold_days</td>
<td>Threshold number of days</td>
</tr>
</tbody>
</table>
Certificate Renewal

Step 1

AWS List All Regions
Certificate Renewal

Step 1

AWS List All Regions

Credential: service ID default

Print Output

Start Condition

not region

Enable
Certificate Renewal

Step 1

AWS List All Regions

Credential: service ID default

Print Output

Start Condition

not region

Enable

http://runbooks.sh
Certificate Renewal

Step 1

AWS List All Regions

[ '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

List Expiring ACM Certificates - Completed
Certificate Renewal

Step 2

List Expiring ACM Certificates

Credential: service ID

Print Output

List to Iterate
List Item Type: Single Value

region

Loop Parameter
region
Certificate Renewal

Step 2

List Expiring ACM Certificates

Credential: service ID

Print Output

Inputs	Output	Iterator	Poll	Start Condition

List to Iterate

List Item Type: Single Value

region

Loop Parameter

region

http://runbooks.sh
## Certificate Renewal

**Step 2**

**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

Certificate Renewal

Step 4

Renew Expiring ACM Certificates
Certificate Renewal

Bonus Step

Schedule Running

- Select xRunbook:
- Schedule

<table>
<thead>
<tr>
<th>Minute</th>
<th>Hour</th>
<th>Day of Month</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>15</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Month</th>
<th>Day of Week</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
</tr>
</tbody>
</table>

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
Permissions Toil

Policy editor

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.

Manual actions | Add actions

- All EC2 actions (ec2:*)

Access level

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

Switch to deny permissions

Required permissions not selected.
AWS Permissions

My App
AWS Permissions

Principle of Least Privilege:
Minimum access that is required for the application to run
AWS Permissions

My App

My Dev Credentials
AWS Permissions

My App

Prod Credentials
AWS Permissions

Too Little Access

My App
Prod
Credentials
AWS Permissions

Too Little Access

User: arn:aws:iam::787345941828:user/web_user is not authorized to perform with an explicit deny in a service control policy (Service: S3, Function: S3:GetObject, Source: S3:GetObject)

http://runbooks.sh
AWS Permissions

Too Much Access

My App

Credentials
AWS Permissions
AWS Permissions

Too Little Access

My App Poor Calendar

http://runbooks.sh
AWS Permissions

Too Little Access

http://runbooks.sh
AWS Permissions

Too Little Access

Too Hot

Just Right

Too Cold
DevSecOps Toil

Policy editor

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.

Filter Actions

Manual actions | Add actions

- All EC2 actions (ec2:*)

Access level

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

Switch to deny permissions

Required permissions not selected.
AWS Permissions

My App

My Dev Credentials

http://runbooks.sh
AWS Permissions
AWS Permissions

- Create Customized Profile
- Create new IAM user
AWS Permissions

My App
AWS Permissions

- CloudTrailArn
- policy_name
- region
- user_name
- principalARN

http://runbooks.sh
AWS Permissions

- 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 for

http://runbooks.sh
AWS Permissions

**My App**

- **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 for
AWS Permissions

AWS Start IAM Policy Generation
- Configurations
- Run Action

AWS Get Generated Policy
- Configurations
- Run Action

AWS Get Account Number
- Configurations
- Run Action

clean up policy
- Configurations
- Run Action
AWS Permissions

My App
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
@dougsillars
Learn more at: unSkript.com