We spent some time doing some house cleaning on AWS IAM accounts.

Observations

1. We cleaned up Brian Moulton old IAM accounts (login: unico-bmoulton, key: AKIAZI2LGMLOYAPC7ONW). His main account was accessed in May, a couple of days before the events that are going to follow cf Screenhot 1.
2. By routinely checking the CloudFormation dashboard (where the Salesapp infrastructure lives), we found out a bunch of unknown CloudFormation stacks (cf screenshot 2 - *FAILED stacks at the top in red). These stacks look really dodgy to us and do not match with any activity we had on the Unico AWS account.
3. By looking at CloudTrail, we found out that these stacks have been attempted to be created from the GitHub account (which credentials we use for github actions on salesapp) from a bunch of IP addresses (one being located in Virginia - from Sollutium cloud services) and the other from an ISP in Indonesia).
4. There are a lot of denied access requests attempted on the same GitHub account in AWS (cf Cloudtrail)
5. These credentials are stored in the GitHub repo for Unico Salesapp (hosted under the StackGlobal organisation). Motif has no visibility on the activity on this GitHub organisation, so there might be some investigation to do here.
6. The root account has no MFA enabled for it.
7. The targeted GitHub account has some limited permissions (full access to CloudFront and CloudFormation but limited access to S3, EC2 and other components)
8. There is an external SSO access (screenshot 3) created on the 7th of May, which we have no knowledge of. If this is not used by Stack, it should be deleted ASAP.

Mitigation

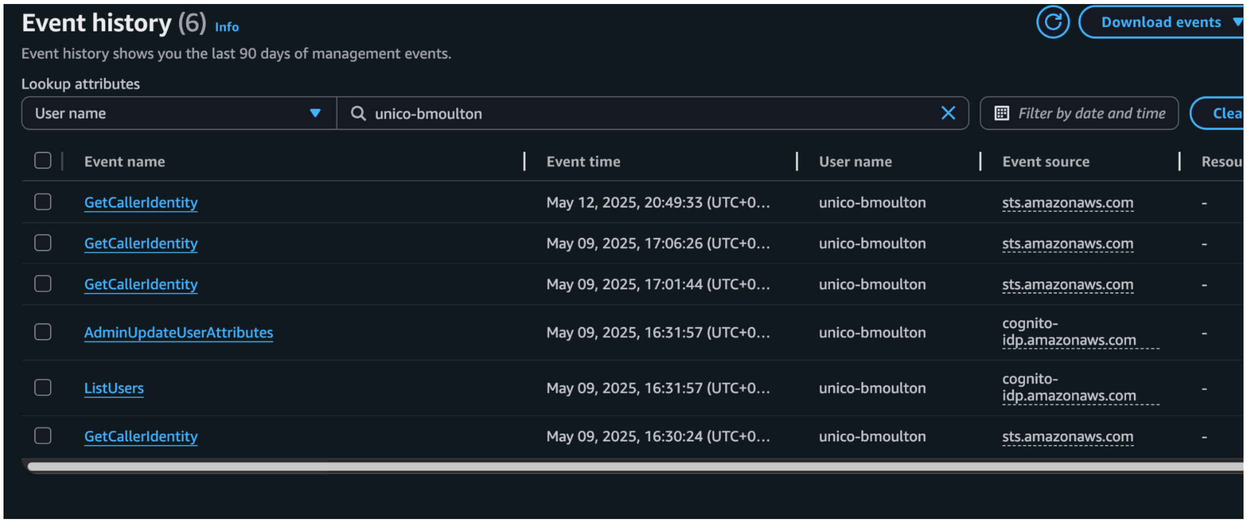
1. I have disabled the programmatic key for the GitHub account used for these requests
2. I will rotate to a new key and replace it in the salesapp GitHub account to restore auto-deploy from our side.

Recommendations

- Enforce MFA for all AWS accounts (root and IAM)
- Rotate keys for all accounts

Screenshots

Screenshot 1



Event history (6) Info

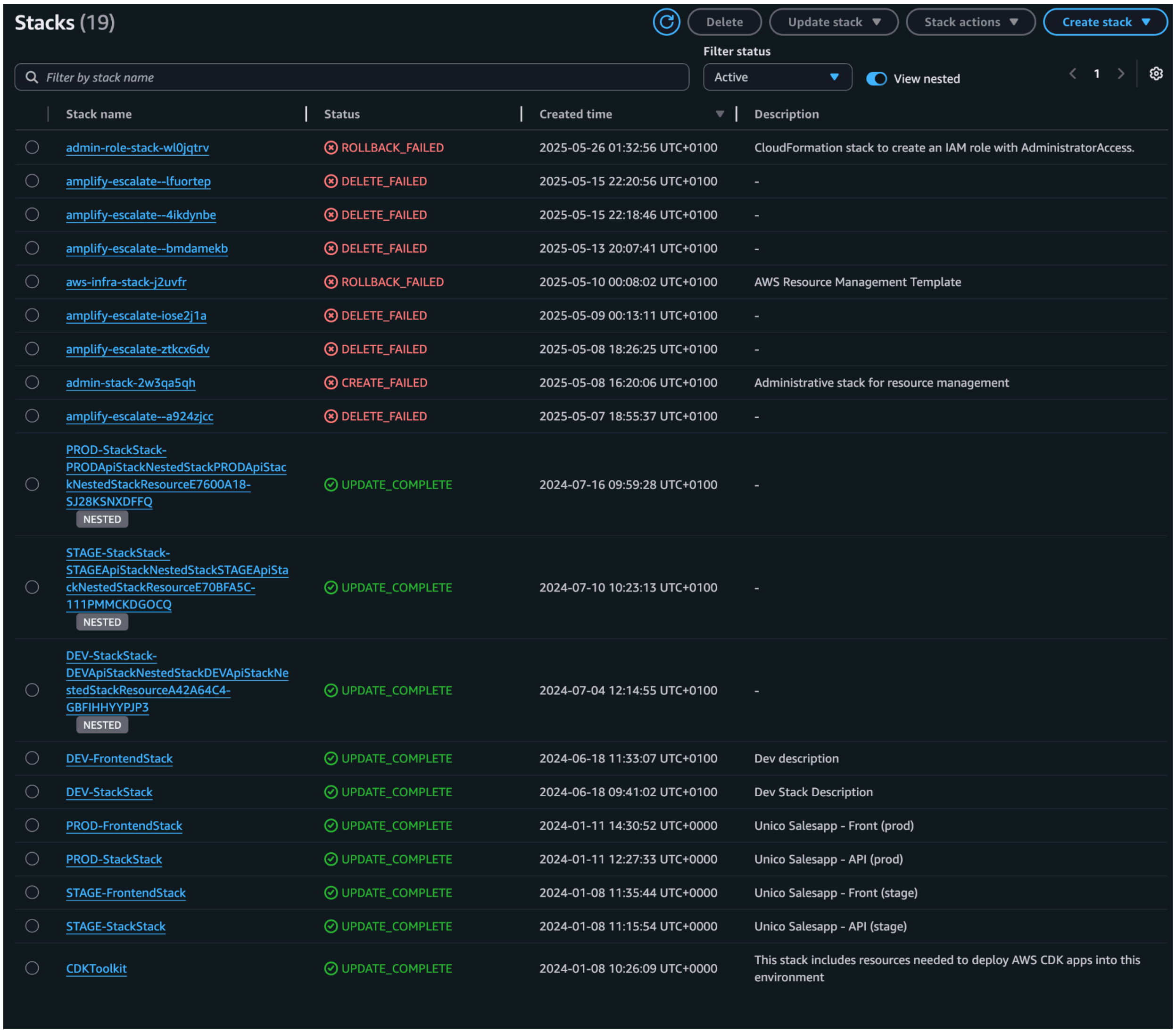
Event history shows you the last 90 days of management events.

Lookup attributes

User name: unico-bmoulton

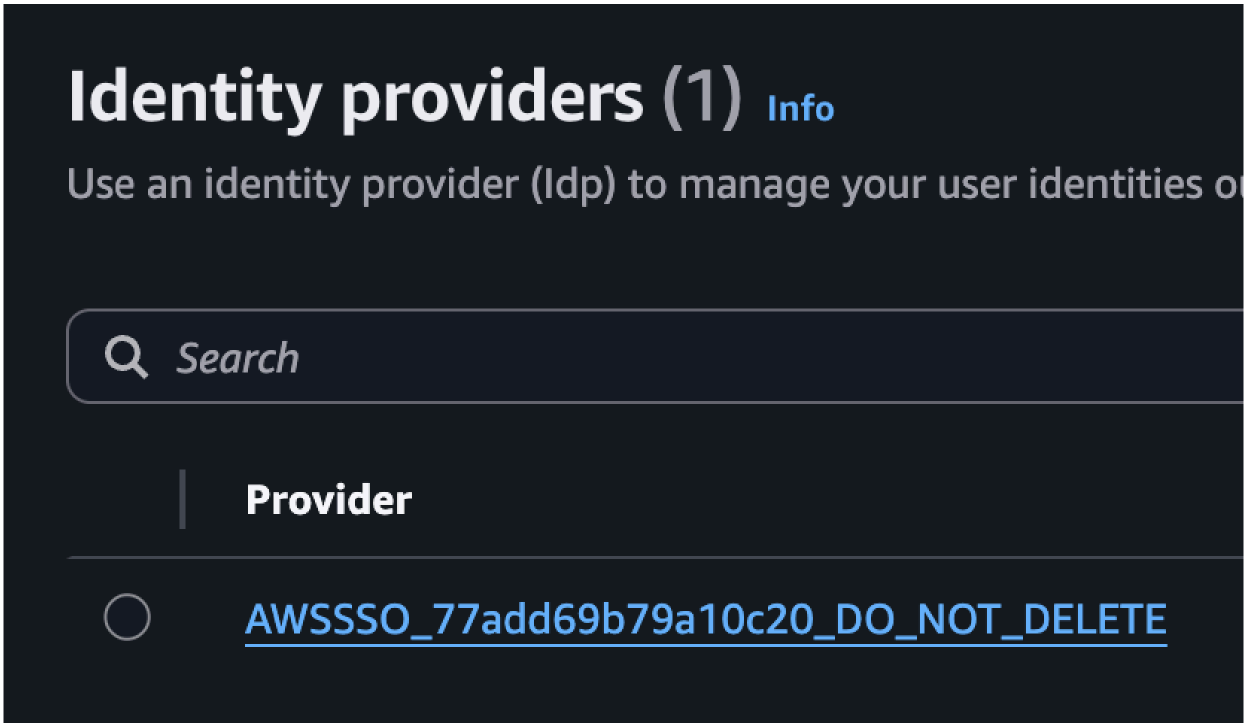
	Event name	Event time	User name	Event source	Resou
□	GetCallerIdentity	May 12, 2025, 20:49:33 (UTC+0…	unico-bmoulton	sts.amazonaws.com	-
□	GetCallerIdentity	May 09, 2025, 17:06:26 (UTC+0…	unico-bmoulton	sts.amazonaws.com	-
□	GetCallerIdentity	May 09, 2025, 17:01:44 (UTC+0…	unico-bmoulton	sts.amazonaws.com	-
□	AdminUpdateUserAttributes	May 09, 2025, 16:31:57 (UTC+0…	unico-bmoulton	cognito-idp.amazonaws.com	-
□	ListUsers	May 09, 2025, 16:31:57 (UTC+0…	unico-bmoulton	cognito-idp.amazonaws.com	-
□	GetCallerIdentity	May 09, 2025, 16:30:24 (UTC+0…	unico-bmoulton	sts.amazonaws.com	-

Screenshot 2



	Stack name	Status	Created time	Description
○	admin-role-stack-wl0jqtrv	⊗ ROLLBACK_FAILED	2025-05-26 01:32:56 UTC+0100	CloudFormation stack to create an IAM role with AdministratorAccess.
○	amplify-escalate--lfuortep	⊗ DELETE_FAILED	2025-05-15 22:20:56 UTC+0100	-
○	amplify-escalate--4ikdynbe	⊗ DELETE_FAILED	2025-05-15 22:18:46 UTC+0100	-
○	amplify-escalate--bmdamekb	⊗ DELETE_FAILED	2025-05-13 20:07:41 UTC+0100	-
○	aws-infra-stack-j2uvfr	⊗ ROLLBACK_FAILED	2025-05-10 00:08:02 UTC+0100	AWS Resource Management Template
○	amplify-escalate-iose2j1a	⊗ DELETE_FAILED	2025-05-09 00:13:11 UTC+0100	-
○	amplify-escalate-ztkcx6dv	⊗ DELETE_FAILED	2025-05-08 18:26:25 UTC+0100	-
○	admin-stack-2w3qa5qh	⊗ CREATE_FAILED	2025-05-08 16:20:06 UTC+0100	Administrative stack for resource management
○	amplify-escalate--a924zjcc	⊗ DELETE_FAILED	2025-05-07 18:55:37 UTC+0100	-
○	PROD-StackStack-PRODApiStackNestedStackPRODApiStackNestedStackResourceE7600A18-SJ28KSNXDFFQ NESTED	✓ UPDATE_COMPLETE	2024-07-16 09:59:28 UTC+0100	-
○	STAGE-StackStack-STAGEApiStackNestedStackSTAGEApiStackNestedStackResourceE70BFA5C-111PMMCKDGOCQ NESTED	✓ UPDATE_COMPLETE	2024-07-10 10:23:13 UTC+0100	-
○	DEV-StackStack-DEVApiStackNestedStackDEVApiStackNestedStackResourceA42A64C4-GBFIHHYYPJP3 NESTED	✓ UPDATE_COMPLETE	2024-07-04 12:14:55 UTC+0100	-
○	DEV-FrontendStack	✓ UPDATE_COMPLETE	2024-06-18 11:33:07 UTC+0100	Dev description
○	DEV-StackStack	✓ UPDATE_COMPLETE	2024-06-18 09:41:02 UTC+0100	Dev Stack Description
○	PROD-FrontendStack	✓ UPDATE_COMPLETE	2024-01-11 14:30:52 UTC+0000	Unico Salesapp - Front (prod)
○	PROD-StackStack	✓ UPDATE_COMPLETE	2024-01-11 12:27:33 UTC+0000	Unico Salesapp - API (prod)
○	STAGE-FrontendStack	✓ UPDATE_COMPLETE	2024-01-08 11:35:44 UTC+0000	Unico Salesapp - Front (stage)
○	STAGE-StackStack	✓ UPDATE_COMPLETE	2024-01-08 11:15:54 UTC+0000	Unico Salesapp - API (stage)
○	CDKToolkit	✓ UPDATE_COMPLETE	2024-01-08 10:26:09 UTC+0000	This stack includes resources needed to deploy AWS CDK apps into this environment

Screenshot 3



Identity providers (1) Info

Use an identity provider (Idp) to manage your user identities o

Provider

○ AWSSSO_77add69b79a10c20_DO_NOT_DELETE