1h Dec 20, 9:10 am – Dec 20, 10:10 am

Open Notebook in Datadog

Postmortem

Postmortem IR-2: Missing A record caused SEV-1 outage for account.efilecabinet.

Created by **Rachel Coleman** on Oct 4, 2021

INCIDENT PROPERTIES	
Status	resolved
Severity	SEV-1
Started	Oct 04, 2021 09:24 pm MST
Commander	Rachel Coleman
Incident Overview	IR-2

You can generate a postmortem from any resolved incident with these fields pre-filled, along with incident metadata and timeline.

What Happened?

Impact on Customers

The CNAME DNS Record in AWS account.efilecabinet.net was deleted by the Rubex Application after someone tried to change a custom branding URL. This impacted customers' ability to login and access Rubex. Sessions that were already existing may have persisted even after the DNS record was deleted.

This lasted for 13 minutes, beginning at 9:24 am.

Why Did it Happen?

Root Cause

Deleted A record in DNS record

Timeline

Oct 4, 2021 at 9:24 am

The A record for account-efilecabinet.com was deleted from our DNS zone "efilecabinet.net" by a function in AWS Route53 after being called by the rubex application

Oct 4, 2021 at 9:27 am

Datadog alerted that account.efilecabinet.com was down: https://app.datadoghq.com/monitors/47648597?to_ts=1633361238000&from_ts=1633361178000

As well as members of the #itteamsupportcollaboration channel

Oct 4, 2021 at 9:28 am

Research began on what's causing issue

Oct 4, 2021 at 9:32 am

Brian made an A/B swap to try to fix the issue.

Oct 4, 2021 at 9:34 am

We made the discovery that it was likely to do with DNS.

Oct 4, 2021 at 9:36 am

Cause of issue located and resolved in AWS

Oct 4, 2021 at 9:37 am

We started to see recovery and Brian was able to successfully get account.efilecabinet.net to resolve in the browser.

How do we prevent it in the future?

Action Items

- Ops work with Dev to resolve the issue that allows a customer to take over our account.efilecabinet.com A record.
- Development is introducing a fix (potentially short term) to resolve the issue and will push to a new build (hopefully released on 10-5-21)
- Research potential monitoring in CloudWatch (AWS) is being done by Ops
- Implementing some changes for preventative in Route53 is being done by Ops