Closed Opened 1 year ago by David Smith 🌴

RCA for about.gitlab.com 503s for certificate expired

Please note: if the incident relates to sensitive data, or is security related consider labeling this issue with security and mark it confidential.

Summary

For approximately 20 minutes on 2018-11-16 unauthenticated requests to https://gitlab.com and all requests to https://about.gitlab.com were returning 503 errors because of an expired certificate.

Impact & Metrics

The following services were impacted:

- https://about.gitlab.com
- unauthenticated requests to https://gitlab.com (because of the redirect to about.gitlab.com)

The following services remained unaffected during the outage:

- authenticated logins to https://gitlab.com
- pages, registry, api, all gitlab.com services

Detection & Response

Start with the following:

- How was the incident detected?
- Did alarming work as expected?
- How long did it take from the start of the incident to its detection?
- How long did it take from detection to remediation?
- Were there any issues with the response to the incident? (i.e. bastion host used to access the service was not available, relevant team memeber wasn't page-able, ...)

Timeline

2018-11-16

- 00:03 UTC - we started seeing expired certificate errors for about.gitlab.com
- 00:06 UTC - curl for `about.gitlab.com` cert reveals that it's good
- 00:08 UTC - curl for `about-src.gitlab.com` cert reveals that it's expired at 00:00 2018-11-16
- 00:10 UTC - started purchase process for cert renewal of `about-src.gitlab.com`
- 00:15 UTC - update chef vault for `about-gitlab-com _default` with new certs
- 00:18 UTC - manually run chef-client on `about-src.gitlab.com` to roll in new certificate
- 00:21 UTC - `about-src.gitlab.com` serving new cert now
- 00:25 UTC - modify Fastly configuration for Origin validation to accept `about-src.gitlab.com` as TLS name
- 00:27 UTC - Roll out Fastly configuration for Origin SSL TLS name change
- 00:28 UTC - about.gitlab.com is operating normally.

Root Cause Analysis

The certificate on the origin server for `about.gitlab.com` had expired causing the CDN provider to throw errors. We didn't realize the cert was expiring or about to expire because when we moved the production site `about.gitlab.com` to be fully CDN resolved we never re-branded the origin server, in stead leaving the old certificate on the server while the CDN provider generated a new one. This then was further compounded by the fact that our certificate monitoring in prometheus for advanced alerting was never reconfigured either, so it was still looking at `about.gitlab.com` rather than the origin server of `about-src.gitlab.com` for cert expiration alerting.

What went well

- Alerting triggered immediately in both Slack ad PagerDuty that there was an issue

What can be improved

- We need a more automated means to iterate over the domains that we have certs on and monitor when they're going to expire.

Corrective actions

Guidelines

- Blameless Postmortems Guideline
- 5 whys

Edited 1 year ago by John Northrup

Linked issues 1

Relates to

about.gitlab.com - 503 with certificate expired
production#574

David Smith @dawsmith marked this issue as related to production#574 (closed) 1 year ago

David Smith @dawsmith mentioned in issue production#574 (closed) 1 year ago

David Smith @dawsmith added 1 deleted label 1 year ago

David Smith @dawsmith changed milestone to %2018-12-01 Completed 1 year ago

David Smith @dawsmith added 1 deleted label 1 year ago

David Smith @dawsmith assigned to @ctbarrett and @northrup 1 year ago

David Smith @dawsmith assigned to @dawsmith 1 year ago

GitLab Bot @gitlab-bot · 1 year ago — Maintainer

Hi @northrup,

This issue does not appear to have an issue weight set.

As a general guidelines use a weight of `1` for an access request issue or a simple configuration update. Use this as a multiplier for setting the weight. If you are unsure about what weight to set it is better to add a generous estimate and change it later. If the weight on this issue is `8` or larger then it might be a good idea to consider splitting this issue up into smaller pieces.

Thanks for your help! 🖤

You are welcome to help improve this comment.

Sid Sijbrandij @sytses · 1 year ago — Owner

Via @northrup The certificate expired on the origin server for the `about.gitlab.com` content and we hadn't updated our cert monitoring to account for about having ÃŷÌ servers with certs. The Fastly served one that they renew and maintain, and our origin server that we renew and maintain.

My question is how we monitor domain expiration and prevent hijacking, since these can take much longer to reverse.

John Northrup @northrup changed title from **RCA for about.gitlab.com 503s for license expired** to **RCA for about.gitlab.com 503s for certificate expired** 1 year ago

John Northrup @northrup · 1 year ago

@sytses last year I went through the process of moving all of our domains under one registrar managed via AWS Route53. All of our domain assets are set to auto renew without needing human intervention. Once purchased, we continue renewing domain names automatically until we make a manual intervention deciding that we no longer want it.

John Jarvis @jarv changed the description 1 year ago

Sid Sijbrandij @sytses · 1 year ago Owner

@northrup do we have any international domain names that are not handled by route53?

John Northrup @northrup · 1 year ago

@sytses there are only two domains that aren't managed within Route53 due to their TLD not being services by AWS, both of those are housed within Gandi.net and set to auto renew every year. Those two are `meltano.app` and `gitlab-review.app`.

John Northrup @northrup changed the description 1 year ago

David Smith 🌴 @dawsmith changed milestone to %2018-12-16 Completed 1 year ago

John Northrup @northrup closed 1 year ago

David Smith 🌴 @dawsmith changed weight to **2** 1 year ago

Anthony Sandoval @AnthonySandoval added P1 label 11 months ago

Please register or sign in to reply