Link to 2023 ACAMP Wiki

Advance CAMP Thu. Sept 21, 2023

Room - I

Session Title: Cert Service - What are you automating?

CONVENER: Derek Eiler, Nevada System

MAIN SCRIBE(S): David @ Nevada, MikeZ,

ADDITIONAL CONTRIBUTORS:

# of ATTENDEES: about 12 people in the room

Link to Internet2 Futures survey

Link to cert service survey: https://www.surveymonkey.com/r/certservice2023

DISCUSSION:

Derek: We (NSHE System Office) initially signed up for cert service for community colleges in the system to centralize service, save money, simplify support. Delegation model made sense for the system office. We don't run all tech services for system, but wanted to set up certificate

system in a way that relieved tech staff of much (but not all) of the burden of support. We set up admin hierarchy with System Office at top and key IT staff for individual schools but with no direct access to SCM. Provided some basic info on cert concepts to IT staff. Put a lot of work in on support systems like email templates, ticket system, documentation, etc. (And then Sectigo changed UI which obsoleted our documentation)

Feedback has been generally positive, due to cost and services provided. However, what would next year(s) look like? We looked to automation so that we could have a more hands-off approach in future years. Wanted to ease certificate expirations and the DCV process.

Cert expiration batching process: What if you have an individual with 20 certs and is being bombarded with automatically generated messages from Sectigo about those certs? They'll likely start to tune those out, miss important info or instructions. I created an automation to query each school's certs, look at the expiration date, and send a digest of messages to people instead of individual messages. Saved us work, users liked the approach.

DCV for domains: Didn't have the ability to programmatically update DNS records. Created automation to dynamically register records via an API and a means to revisit the DCV progress for multiple domains. It can figure out which departments' domains need DCV, checks to see if the domain is one we own. If it is, the API can update our DNS records appropriately. If not (i.e. owned by individual schools), it'll email precise directions on how to update their DNS record to complete DCV. Started thinking about more opportunities for automation. That's what I'm looking for from this group.

Steve - Duke University - Locksmith, our home brew solution, generates the CSR and handles the request; pivots over to DNS, checks for authority in changing DNS. ACME also built on top of it. Using Grouper, the Support Group owns the certificate and its lifecycle. Multiple people in the group to deal with employee turnover.

Dhivakaran - Only have a handful of domains, so there's no automation involved in Domain Validation Process.. Manually scan for it and take care of it that way. Another process based on ACME, every system has an entry and is ansibilized to automate the CSR creation, ACME submission, etc. Multiple name certificates have a separate LDAP entry and are handled a little differently. Multiple monitoring systems, one probes 443 and notes expiration date and creates a ticket if necessary. Also, upon submission of the CSR, a common email address is used and is

turned into a ticket and assigned to someone. Workload is shared between users of that group. The ACME bot has the CSR and private key, but the ticket is created to ensure the renewal is created and certificate is actually installed (may be a different owner that does this). May need to restart services, etc. but it depends on the server/service. AUtomation also handles cleanup if needed of private key, etc.

Paul: Are you using the Service Now manager plugin for the Cert Service? Automated ticket creation process when it's time for renewals. There's a working group looking at how to automate additional processes. Available in the Service Now app store.
https://surveymonkey.com/r/certservice2023

Vlad: We (REANNZ) have automated similar to he process Dhiv described. We use the certs in a few other places like FreeRADIUS for our eduroam IdP. We monitor via scraping HTTPS end point - have a scheduled process for that. Handling change to DNS server is manual, but set up a separate server with zone file where we automatically update CNAME records. When a host's cert is about to expire we see the notification, manually revoke.

Derek: We've started to look into ACME, still rely on human responses to emails in some cases.
Vlad: Question - Let's Encyrypt finds new certs when it sees a cert for the same domain.
Dan: Don't believe our implementation has that functionality due to how SCM works.

Derek: Wanted to know if any of you have provided a custom service interface for cert issuance.
Steve: Locksmith does that.
Derek: We'd looked into coding something like that. More I thought about it, the more edge cases came up, didn't feel like I had the expertise to implement that.

Justin - We've had an internal cert tool for decades, checks for permissions if you're a domain owner. IT dept is distributed. Modernization issues, built on SOAP API. It seems to be breaking often. However, InCommon says SOAP is here to stay for now. Maybe Locksmith (Steve) can be open sourced?

Derek - Somebody is going to require 90 day TLS cert renewals. Which will be difficult for small colleges. Our solution isn't automated enough to handle something like this; it's not scalable enough. Our research institution is piloting ACME (alongside us) to see how it compares to Let's Encrypt's version as a solution. Don't want to encourage poor practices (self signed certs, etc) to get around 90 day lifetime. There's lots of unclear information on ACME certificate creation

for multiple institutions/across multiple domains. Created ACME credentials for a customer and handed them over. But are EAB credentials supposed to be used this way? Good practice would be 1x EAB creds for each server, but that becomes very unwieldy. Using one host to pull all certs and distribute them would be great for us, but not for all of our colleges

Paul: I'm reusing the EAB credentials and letting ACME do its thing. If you use an AWS instance you can spin up a machine and automate cert installation for the machine.

Sara - Will the Network Agent be the tool to fix this problem?

Derek: We gave the Network Agent a shot, but thought through Agent, vs manual, vs ACME, vs using Sectigo's API. We quickly ran into an issue where we had to give our schools access to SCM. Up until then we'd shielded them from that complexity. There was another hurdle around cases where we didn't have control of the machine that the Network Agent was installing the cert on. We're looking into using the API

Dan - confirmed it's the access issue to the web interface. Need the UI to do some things.

Derek - Decided that ACME was the way to go since it seems to be the way of the future. Considered using Sectigo's API natively. Haven't tried yet.

Sara - Planning a webinar on this topic

Derek - Anything else related to this topic that others are having pain points around or are thinking of doing something new?
Steve: Question - has anyone consider CA records?
Derek - We do. We found that nobody else within the HE system in NV had used them. So we implemented but didn't do it correctly at first.
Steve: Thinking about how to handle sensitive domains.
Vlad: We didn't opt to automate udpates/changes CA records. Too critical for operations to risk changing in unintended ways

Dhiv - The other issue we ran into was the certificate chain was sometimes incorrect in the cert bundle. Adding the SHA1 certificate causes the browser to ignore the root certificate.

ARTIFACTS / LINKS