Stockholm University Certificate Manager

Certificates

stick 'em in your ~~mouth~~ Key Management System and suck'em (down to your service)!

Agenda

1. whoami(1)
2. Stockholms universitet
3. Certifikatshantering historia
4. Certifikatshantering {nu,fram}tid
5. Stockholm University Certificate Manager
6. Demo
7. Frågor?

whoami(1)

Simon Lundström aka simlu (i jobbsammanhang) aka simmel (privat på internet)
"Teknikspecialist" på IT-avdelningen
16 år på IT-avdelningen

Jag petat på allt utom ekonomi- och HR-system
Nu mest identitetshantering men *väldigt* mycket integrationer

---

(och ja: vi har flyttat, vi har bara inte hunnit packa upp alla lådor ännu ;)

Stockholms universitet

- Humanistiska fakulteten
- Juridiska fakulteten
- Samhällsvetenskapliga fakulteten
- Naturvetenskapliga fakulteten
- Universitetsförvaltningen

107 institutioner/avdelningar

Stockholms universitet

711 aktiva certifikat

1. IT-avdelningen ~70%
2. Stockholms universitetsbibliotek ~10%
3. Institutionen för lingvistik ~5%

Lång svans

Certifikatshantering historia

SwUPKI

`handle-ssl.sh`

Lagra PGP-krypterade SSL-cert i AFS

Manuell hantering via TCS

Flera wikisidor som beskrev exakt hur man skulle göra

En grupp med "certare" som gjorde certen, lagrade dom och levererade dom till ens tjänst

Certifikatshantering historia

Sectigo REST API

Python-script som baserat på CN/SAN input skapade och hämtade cert

Leverera till tjänst och ev. ladda upp i Hashicorp Vault

Script som kunde hämta data ur Vault

Certifikatshantering historia

Infran allt mer automatiserad

- Saltstack för configuration management
- Kubernetes för containers

Fortfarande manuella steg att få cert

Certifikatshantering historia

ACME verkar bra men...

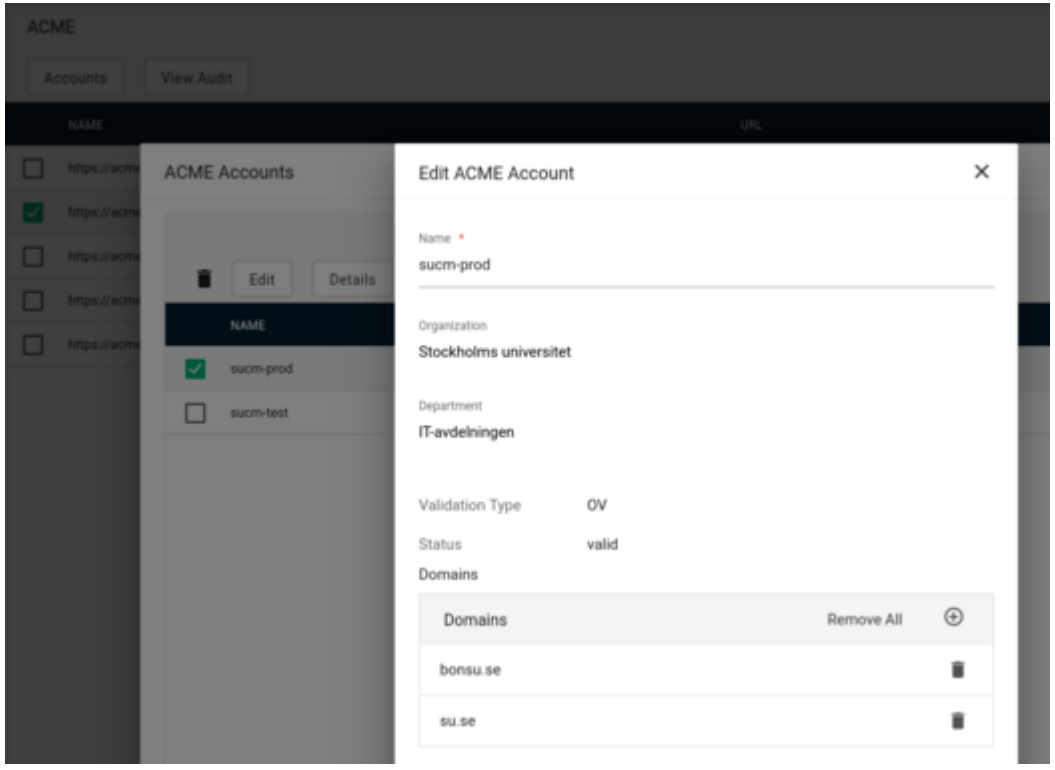
- Olika tjänster
  - VMar
  - Containers
  - HW-appliances (Brandvägg, lastbalanserare, osv)
  - SaaS-tjänster
- Olika användare
  - Linux/Windows-tekniker
  - Utvecklare
  - Tjänsteansvariga
- Lagra certen?
  - På disk? Samma cert används i LB *och* på VM

Certifikatshantering {nu,fram}tid

ACME EAB

External Account Binding

- Använder ingen "challenge" (DNS eller HTTP t.ex.)
- Skapa och förnya certen centralt, som en tjänst
- Använder ett förregistrerat konto med begränsade rättigheter



Certifikatshantering {nu,fram}tid

Lösning i sikte

- patlu drömde ihop en tjänst i ett mail innan han quittade
- Tiden gick, certen blev fler och tog mer tid
- Vi anlitade en konsult, Rasmus Thorslund, för att skriva tjänsten
- Rasmus jobbar nu mera också på SUNET =)

SU Certificate Manager

- SSO:at WebGUI som hela IT-avdelningen kommer in på
- Stödjer flera CA:s, samtidigt
- Skriv in:
  - CN
  - SAN
  - Tjänst och miljö det ska levereras till
- Certet levereras till Vault

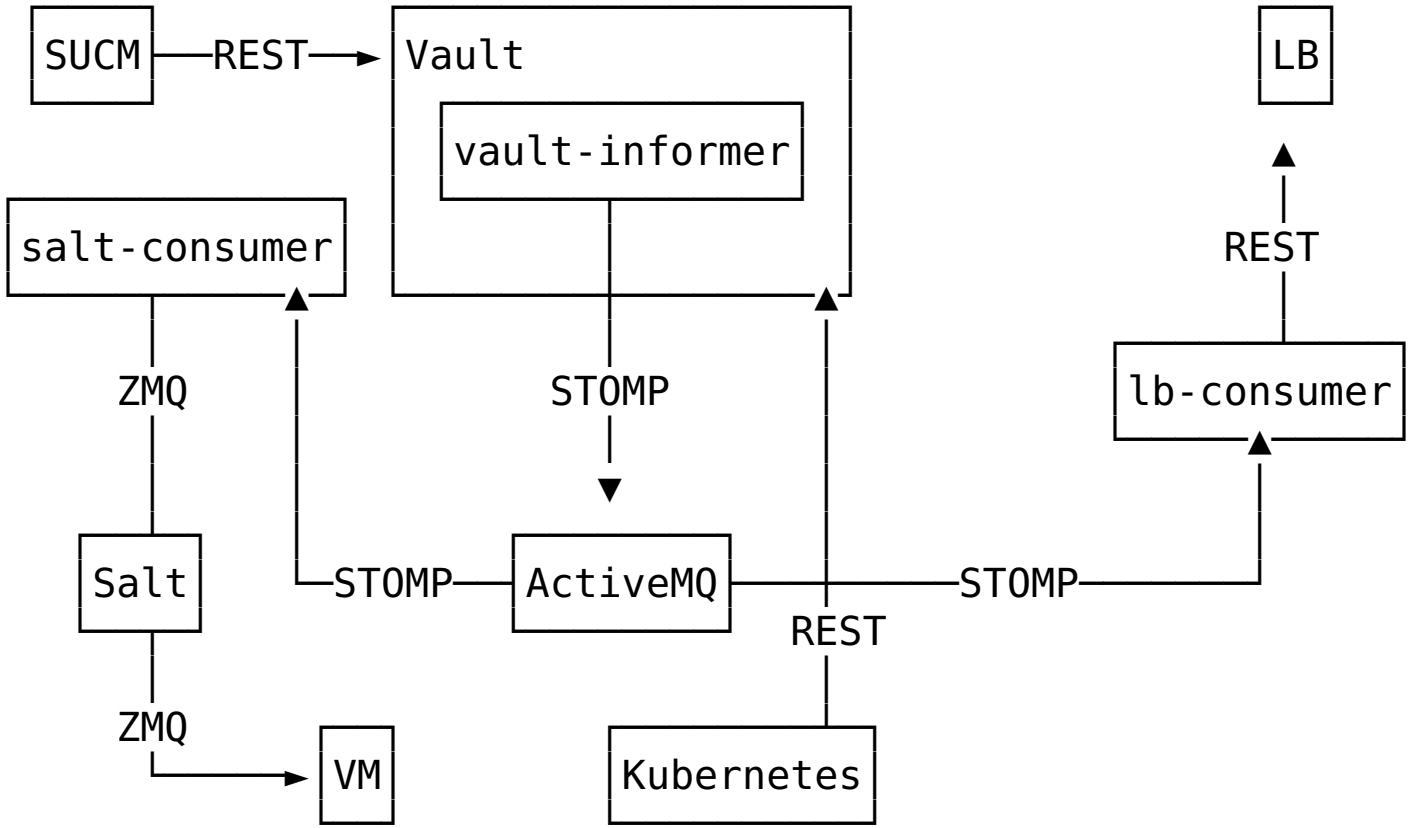
SU Certificate Manager

- Automatisk förnyelse
- Manuell förnyelse
  - Mail skickas till ansvariga™ när det är dax att förnya
  - Klicka "förnya" eller ladda upp CSR
  - Hämta från Vault/Secrets och leverera

Certifikatshantering {nu,fram}tid

- Olika tjänster
  - VMar = Saltstack via Vault
  - Containers = Kubernetes Secret Store Container Storage Interface driver Vault provider
  - HW-appliances = Hämta ev. CSR från appliance, ladda upp cert manuellt eller via API
  - SaaS-tjänster = Levereras manuellt av icke-tekniker
- Olika användare
  - Alla kan använda ett webgui
- Lagra certen?
  - I Vault!

Klistra ihop'et bara!



Demo 😈

https://sucm.it.su.se

Frågor?

Stockholm University

simlu@su.se

Slides at https://github.com/simmel/slides via https://github.com/stockholmuniversity/su-remark-template/