Automated Certificate Replacement

Venafi SaltStack Guide

Overview

If you are using the SaltStack configuration management platform, the Venafi module can be used to request a replacement certificate and deploy it directly on the affected systems. Install and configure the Venafi Salt module as described here: https://www.venafi.com/sites/default/files/2017-04/SaltStack-Venafi-Integration.pdf

Note: The following instructions assume that you have Salt Minions installed on the systems that you will be replacing certificates on.

Configure Venafi Cloud (via Web Interface)

We support certificates issued by DigiCert CertCentral; other certification authorities will be supported in the future. If you do not already have a DigiCert CertCentral account, visit https://www.digicert.com/ to get an account.

Review our Help documentation for information on how to set up a Certificate Provider, Policy, and Zone.

Request and Replace Certificates with SaltStack

1. Use the salt-run venafi.request command to request a replacement certificate:

```
salt-run venafi.request <ID of the minion that the certificate will be installed on> <certificate subject name> -z <zone name>
```

The output of this command will include a request-id that will be used to retrieve the certificate from Venafi Cloud.

2. When the certificate is issued, use the salt-run venafi.pickup command to retrieve the certificate:

```
salt-run venafi.pickup <request ID>
```

The certificate and private key will be stored in a pillar in the salt master which can then be referenced by state files.

3. Create a state file that is appropriate for the target system that the certificate will be installed on. The state file will contain the path to the certificate, certificate chain and private key on the target minion as well as the pillar that contains the replacement certificate and key. Use the state.apply command to apply the state to the target minions.