Overview

Sectigo Connector for Avi Vantage ("the connector") is a solution that automatically enrolls, imports, and renews public and private Sectigo SSL/TLS certificates on the Avi Vantage platform. This guide covers topics related to the installation of the AviCM script, certificate enrollment, renewal and revocation.

The Avi Vantage platform is a software-based load balancer that provides multi-cloud application services such as load balancing, SSL offloading, application security, autoscaling, container networking, and web application firewall. Avi automates application delivery to ensure applications are available, secure, and responsive.

The connector interacts with Sectigo Certificate Manager (SCM) to provision and renew certificates. SCM is a universal platform purpose-built to issue and manage the lifecycles of public and private digital certificates. The platform secures every human and machine identity across the enterprise.

Audience

This guide is intended for security administrators who manage the Avi Vantage platform for an organization.

Scope

This guide contains instructions for enrolling and managing Sectigo certificates on the Avi Vantage platform. It doesn't cover the configuration of Avi Vantage virtual services.

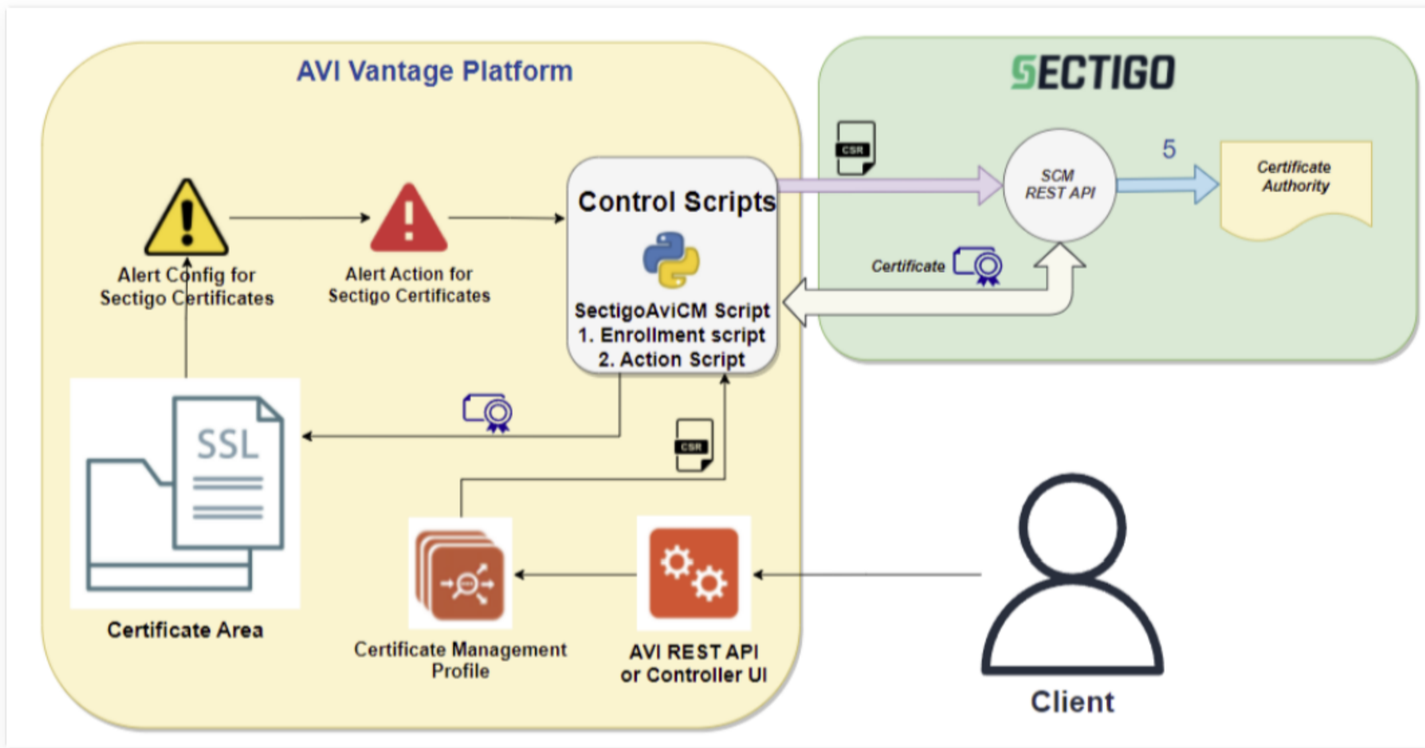
It's assumed that an Avi Vantage environment already exists and is configured with a virtual service(s) where you want to install SSL/TLS certificates.

Additional resources

- Sectigo Certificate Manager administrator's guide
- Avi Vantage architectural overview
- SSL/TLS certificates on Avi Vantage

Architecture

SCM and the Avi Vantage platform are integrated using the SCM REST API and Avi Vantage Controller API through a script to facilitate certificate management. The script can be installed on the Avi Vantage platform either through the Avi UI or by executing an installation script from a remote machine.



The script executes the following workflow for certificate management on the Avi Vantage platform:

- Connects to the Avi Controller via the REST API to authenticate the Avi Controller using valid credentials.
- Generates a key pair and certificate signing request (CSR).

> **Tip**
> We recommend you use the 2048-bit key size for RSA or secp256r1 for ECDSA.

- Transfers the CSR to the SCM backend via the SCM REST API for authentication using the client key.
- Enrolls a certificate with the CA.
- Imports the newly created server certificate and CA certificate chain to the Avi Controller repository where the certificates will be stored.

The certificate can now be used to secure communication between the Avi Controller virtual service and an external client.

Package contents

The installation package contains the following files:

- **config.json**: This file includes the configuration parameters that contain the Avi Vantage server parameters and SCM credentials.

> **Note**
> If you don't want to provide the user passwords in the `config.json` file for security reasons, set the value to an empty string (`""`). The `deploy.sh` script will request the password value during deployment.

- **deploy.sh**: This script gets the configuration parameters from the `config.json` file and deploys the connector to Avi Vantage.
- **destroy.sh**: This script removes the connector from Avi Vantage.

> **Caution**
> Before using this script, ensure that all certificates are unassigned from applications and removed from the profile.

- **enroll.sh**: This script enrolls a certificate in SCM.
- **SCM Client EULA v1.0.1.txt**: The EULA agreement. You need to accept it when running `deploy.sh` for the first time.
- **sectigo_avi_cm_script.py**: This script uploads the provisioned certificate to Avi Vantage.