

Automazione Sectigo

La crittografia a chiave pubblica (PKI) è lo standard di riferimento per la privacy, l'identità e la sicurezza digitale e dovrebbe indiscutibilmente costituire la base della sicurezza per ogni dispositivo, server, utente e applicazione nell'azienda. Tuttavia, l'uso di processi manuali per installare, monitorare e rinnovare tutti i certificati PKI oggi richiesti richiede un notevole impiego di manodopera, è tecnicamente complesso e rischioso. Inoltre, i costi possono accumularsi rapidamente. Un'installazione manuale minima di un certificato TLS/SSL (singolo server web e singola istanza di dominio) comporta diversi passaggi e può facilmente raggiungere da \$50 a \$100 per server web.

Oltre a ciò, il settore si sta orientando verso durate di vita dei certificati più brevi: prima da tre anni a due, e poi da due anni a uno. Con il prossimo passaggio all'accorciamento della durata dei certificati TLS/SSL, si prevede che i costi di installazione e gestione aumenteranno. E le tempistiche non potrebbero essere peggiori. Man mano che un numero sempre maggiore di aziende espande l'uso di dispositivi mobili, Internet delle Cose (IoT), DevOps e altri ambienti digitali, la necessità di PKI aumenta, così come l'urgenza di poter rilasciare, revocare e sostituire i certificati in modo rapido, affidabile e su scala aziendale.

Automatizzare l'installazione dei certificati TLS/SSL

Chiaramente, l'automazione è ormai fondamentale per qualsiasi sistema di gestione dei certificati. Non solo riduce il costo totale di gestione, ma impone anche la conformità crittografica e previene potenziali interruzioni del servizio causate da errori umani.

Tuttavia, considerati i diversi sistemi, applicazioni e dispositivi che utilizzano e si integrano con i certificati digitali, è improbabile che un approccio unico per tutti soddisfi le esigenze di automazione di vari casi d'uso. Ecco perché Sectigo offre diverse opzioni di automazione.

Per l'installazione dei certificati TLS/SSL, Sectigo fornisce:

- **Supporto per il protocollo ACME (Automated Certificate Management Environment):**
Sectigo Certificate Manager supporta ACME, consentendo di automatizzare il rilascio e l'installazione dei certificati per un'ampia gamma di server web, bilanciatori di carico, router, firewall e altre apparecchiature di rete. Sectigo supporta i tipi di certificato DV, OV ed EV tramite ACME e offre il controllo totale agli amministratori IT. Molti strumenti DevOps supportano ACME per registrare e gestire i certificati e a questo scopo è disponibile una miriade di strumenti open source. Questi strumenti sono popolari tra gli amministratori IT e vengono frequentemente migliorati con nuove funzionalità.

Se Sectigo implementa il lato server o Autorità di Certificazione dello standard ACME, funzionerà con i client conformi ad ACME e supporteremo qualsiasi progetto cliente che richieda tale integrazione (ciò richiede che il client sia conforme ad ACME). Consulta la tabella sottostante per un elenco delle piattaforme attualmente supportate.

- **Agente di automazione Sectigo:**

Utilizzando l'Agente di Rete di Sectigo (Network Agent), è possibile automatizzare la gestione dei certificati per una varietà di sistemi, tra cui Apache, Apache Tomcat, Windows IIS e bilanciatori di carico F5 BIG-IP. L'Agente di Rete residente presso la sede del cliente è integrato con la soluzione cloud Sectigo Certificate Manager per pianificare il rilascio, l'installazione e il rinnovo dei certificati.

- **API REST:**

In alcuni casi, le aziende preferiscono integrare le applicazioni in modo più stretto con Sectigo, il che è possibile utilizzando l'API REST di Sectigo. Sebbene ciò richieda uno sviluppo aggiuntivo dal lato dell'applicazione, consente di sfruttare la gestione dei certificati e personalizzare il flusso di lavoro.

- **Integrazione con terze parti:**

Sectigo ricerca continuamente opportunità di integrazione con fornitori terzi per aiutare i clienti a raggiungere la completa automazione. Ad esempio, il bilanciatore di carico BIG-IP di F5 fornisce un'integrazione dal suo sistema di gestione per automatizzare la gestione dei certificati da Sectigo.

Automatizzare la convalida del controllo del dominio (DCV)

Con l'accorciamento della durata dei certificati, il mantenimento dei domini convalidati è diventato un requisito continuo. I processi di convalida manuale richiedono tempo, sono soggetti a errori e insostenibili su larga scala. Sectigo Certificate Manager semplifica questo processo grazie alla convalida automatizzata del controllo del dominio (DCV) integrata, nell'ambito delle sue più ampie funzionalità di automazione del ciclo di vita dei certificati. Sfruttando i connettori DNS, SCM si integra direttamente con i provider DNS supportati per creare e convalidare automaticamente le sfide dei record CNAME. Ciò elimina l'intervento manuale, riduce il rischio di rinnovi non riusciti e garantisce che i domini rimangano continuamente convalidati.

SCM continua ad ampliare il suo elenco di provider DNS supportati, tra cui ora:

Cloudflare

Amazon Route 53

Azure DNS

GoDaddy DNS

Akamai Edge DNS

DNSimple

OVHcloud

Visualizza qui l'elenco completo dei provider DNS supportati da SCM [qui](#).



Automatizzare l'installazione dei certificati client e dispositivo

Molti sistemi, applicazioni e dispositivi utilizzano certificati non SSL. Per l'installazione di certificati non SSL, Sectigo fornisce:

- **Protocollo EST (Enrollment over Secure Transport):**

Sectigo supporta il protocollo EST, utilizzato per la gestione di apparecchiature di rete di molti fornitori. Diversi produttori hanno già il supporto EST integrato. EST è anche popolare negli ambienti Internet delle Cose (IoT) data l'efficienza del protocollo e il supporto delle chiavi con crittografia a curve ellittiche (ECC). Sono disponibili anche diversi client EST open source. Sectigo Certificate Manager visualizza e gestisce i certificati rilasciati.

- **Protocollo SCEP (Simple Certificate Enrollment Protocol):**

Nell'ambiente Sectigo, SCEP può essere utilizzato per registrare certificati in Linux, macOS e altri sistemi operativi. I dispositivi mobili, il server NDES di Microsoft e i sistemi MDM utilizzano in genere SCEP.

- **Agente di automazione Sectigo MS:**

Un agente MS Sectigo posizionato tra Active Directory Certificate Service di Microsoft e Sectigo Certificate Manager. Ascolta le richieste di certificato tramite il protocollo WCCE (Windows Client Certificate Enrollment) e fornisce automaticamente il certificato al desktop senza alcun intervento dell' dipendente.

Come puoi vedere, Sectigo offre una varietà di opzioni di installazione dei certificati, oltre alla comodità e alla sicurezza di una soluzione fluida con un unico pannello di controllo sia per il rilascio che per la gestione di certificati pubblici e privati. Inoltre, con Sectigo non incontrerai mai un limite al volume dei certificati, come potrebbe accadere con le alternative open source. Sectigo consente al tuo team di sicurezza di applicare facilmente la politica di sicurezza crittografica, proteggere le comunicazioni, prevenire la perdita di dati dovuta ad accessi non autorizzati e preparare al futuro sistemi, applicazioni e dispositivi in tutta l'azienda.



Automazione TLS/SSL con SCM:

Client ACME e integrazioni native

Rete di distribuzione dei contenuti (CDN)

Fornitore	Applicazione	Supporto ACME nativo	Client ACME utilizzato	Integrazione realizzata da Sectigo (pronta all'uso)	Tecnologia di integrazione Sectigo
Akamai	Terraform			Connettore Sectigo per Akamai Terraform	API REST
Akamai	CLI			Connettore Sectigo per Akamai CLI	API REST

Containerizzazione

Fornitore	Applicazione	Supporto ACME nativo	Client ACME utilizzato	Integrazione realizzata da Sectigo (pronta all'uso)	Tecnologia di integrazione Sectigo
Amazon	Elastic Kubernetes Service	✓	jetstack (cert-manager)		
Google	Google Kubernetes Engine	✓	jetstack (cert-manager)		
Kubernetes	Kubernetes	✓	jetstack (cert-manager)		
Microsoft	Azure Kubernetes Services	✓	jetstack (cert-manager)		
Redhat	Openshift Container Platform	✓	jetstack (cert-manager)		
Docker	Docker	✓	ACME.sh		

Strumenti DevOps

Fornitore	Applicazione	Supporto ACME nativo	Client ACME utilizzato	Integrazione realizzata da Sectigo (pronta all'uso)	Tecnologia di integrazione Sectigo
Ansible	Ansible	✓	Ansible ACME	Integrazione Sectigo Ansible	API REST
Chef	Chef			Integrazione Sectigo Chef	API REST
HashiCorp	Terraform	✓	Vancluever	Integrazione Sectigo Terraform	API REST
Jenkins	Jenkins			Integrazione Sectigo Jenkins	API REST
Jetstack	Jetstack	✓	jetstack (cert-manager)		
Puppet				Integrazione Sectigo Puppet	API REST
SaltStack				Integrazione Sectigo SaltStack	API REST



Server Web / Bilanciatori di carico / Firewall

Fornitore	Applicazione	Supporto ACME nativo	Client ACME utilizzato	Integrazione realizzata da Sectigo (pronta all'uso)	Tecnologia di integrazione Sectigo
A10	Thunder ADC	✓	Integrato in A10	Connettore Sectigo per A10	API REST
Amazon	AWS Certificate Manager			Connettore Sectigo per AWS	ACME
Apache	Apache	✓	Certbot mod_md	Agente di Rete	Agente di Rete / API REST
Cisco	Cisco FTD			Connettore Sectigo per Cisco FTD	API REST
Citrix	ADC			Connettore Citrix per Citrix	API REST
Citrix	Gateway			Connettore Citrix per Citrix	API REST
Citrix	FAS			Agente MS	APIs
F5	BIG-IP	✓	Kojot ACME	Connettore Sectigo per F5 BIG-IP Agente di Rete	ACME Agente di Rete / API REST
F5	NGINX	✓	Certbot ACME.sh		
Google	Google Load Balancer			Connettore Sectigo per GCP	ACME
HAProxy	HAProxy	✓	Certbot ACME.sh	Connettore Sectigo HAProxy	ACME
Kemp	LoadMaster	✓	ACME.sh	Connettore Sectigo Kemp	API REST
Microsoft	IIS	✓	Win-ACME posh ACME Certify the Web	Connettore Sectigo Kemp	API REST
PaloAlto	PAN OS	✓	ACME.sh		
VMWare	Avi Vantage			Connettore Sectigo per Avi Vantage	API REST

Almacén de claves (Key Vault)

Fornitore	Applicazione	Supporto ACME nativo	Client ACME utilizzato	Integrazione realizzata da Sectigo (pronta all'uso)	Tecnologia di integrazione Sectigo
Hashicorp	HashiCorp Vault			Integrazione Sectigo HashiCorp Vault	API REST
Microsoft	Azure Key Vault	✓	az-acme	SCM Agente PK	APIs

Lenguaje de programación

Fornitore	Applicazione	Supporto ACME nativo	Client ACME utilizzato	Integrazione realizzata da Sectigo (pronta all'uso)	Tecnologia di integrazione Sectigo
Golang	Golang	✓	Lets Encrypt Go		
Java	Java	✓	ACME4j	Connettore Sectigo per Java	API REST
Python	Python	✓	certbot		
Ruby	Ruby	✓	acme-client		



Altro

Fornitore	Applicazione	Supporto ACME nativo	Client ACME utilizzato	Integrazione realizzata da Sectigo (pronta all'uso)	Tecnologia di integrazione Sectigo
BeyondTrust	BeyondTrust	✓	Native Beyond Trust		
Kong HQ	Kong Gateway	✓	Nativo in Kong ACME.sh		
NodeJS	Python	✓	certbot		

Questo elenco non è esaustivo. Aggiungiamo continuamente il supporto per nuove applicazioni.
Contattaci per le informazioni più recenti.

Informazioni su Sectigo

Sectigo è leader nella gestione del ciclo di vita dei certificati (CLM) e fornisce soluzioni innovative e complete per proteggere le identità sia umane che delle macchine per alcuni dei marchi più importanti al mondo. La sua piattaforma CLM cloud-native, automatizzata e universale semplifica e potenzia la sicurezza aziendale attraverso l'emissione e la gestione di certificati digitali provenienti da tutte le autorità di certificazione (CA) affidabili. Con oltre due decenni di esperienza, Sectigo si afferma come una delle CA più grandi e affermate, al servizio di oltre 700.000 clienti in tutto il mondo.

Garantendo un livello di fiducia digitale senza pari, Sectigo continua a consentire alle organizzazioni di implementare protocolli di sicurezza robusti con efficienza e fiducia.

