

Integrazione dei certificati Sectigo per F5 tramite ACME

Le aziende si affidano agli apparati F5 per scalare le applicazioni e garantirne un'elevata disponibilità. Ogni dispositivo, sia esso autonomo o configurato in coppia ad alta affidabilità (HA), necessita di un certificato SSL/TLS per mantenere l'autenticazione e la cifratura del traffico. Con la crescita della flotta aziendale, la gestione manuale e individuale di questi certificati diventa un punto di vulnerabilità. L'emissione e la gestione del ciclo di vita devono essere automatizzate e orchestrate per tenere il passo.

Per proteggere i dispositivi F5 da attacchi e blocchi improvvisi, i team IT necessitano di una soluzione di Certificate Lifecycle Management in grado di:

- ✓ Emettere, revocare, sostituire e rinnovare certificati SSL/TLS in modo rapido, affidabile e su vasta scala.
- ✓ Proteggere gli accessi e le comunicazioni sugli apparati F5 con un'autenticazione sicura e una crittografia avanzata.
- ✓ Ridurre i costi e i tempi dedicati alle procedure manuali da parte degli amministratori IT.
- ✓ Eliminare i processi manuali soggetti ad errori nell'emissione di singoli certificati.
- ✓ Garantire la compatibilità futura con le versioni dei sistemi operativi server.



Il supporto di Sectigo

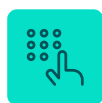
Sectigo offre un'integrazione completa dei certificati per dispositivi F5, consentendo alle aziende di emettere certificati massivamente con un solo clic e di automatizzare l'intero ciclo di vita su scala globale.

Gestione automatizzata dei certificati per F5

Le aziende richiedono una gestione del ciclo di vita dei certificati affidabile e scalabile per garantire che i dispositivi di Application Delivery critici siano sempre protetti, evitando attività amministrative complesse e il rischio di scadenze o interruzioni impreviste.

L'integrazione di Sectigo per F5 sostituisce la complessità della gestione manuale con un controllo centralizzato e un'automazione avanzata, offrendo semplicità su vasta scala per tutti gli apparati F5.

Grazie all'integrazione Sectigo per F5, i team IT beneficiano di:



Emisione scalabile di certificati SSL/TLS

Sectigo consente agli amministratori IT di automatizzare l'emissione e l'installazione di certificati validi sugli apparati F5 utilizzando lo standard di automazione ACME.



Rinnovo automatizzato dei certificati

In prossimità della scadenza, Sectigo rinnova e installa automaticamente i nuovi certificati nei dispositivi F5, evitando fermi macchina su sistemi e applicazioni mission-critical.



Gestione completa del ciclo di vita

Oltre al rinnovo, Sectigo offre funzionalità di revoca e sostituzione dei certificati, necessarie ad esempio durante la sostituzione di un server.



Visibilità e reportistica avanzate

Grazie all'integrazione ACME per F5 e a Sectigo Certificate Manager (SCM), i team IT monitorano lo stato dei certificati di tutti i dispositivi tramite un'unica schermata (single pane of glass), verificando le scadenze ed eliminando i disservizi.



Plugin semplici da usare

L'integrazione include due plugin Certbot basati sul protocollo aperto ACME (Automated Certificate Management Environment).

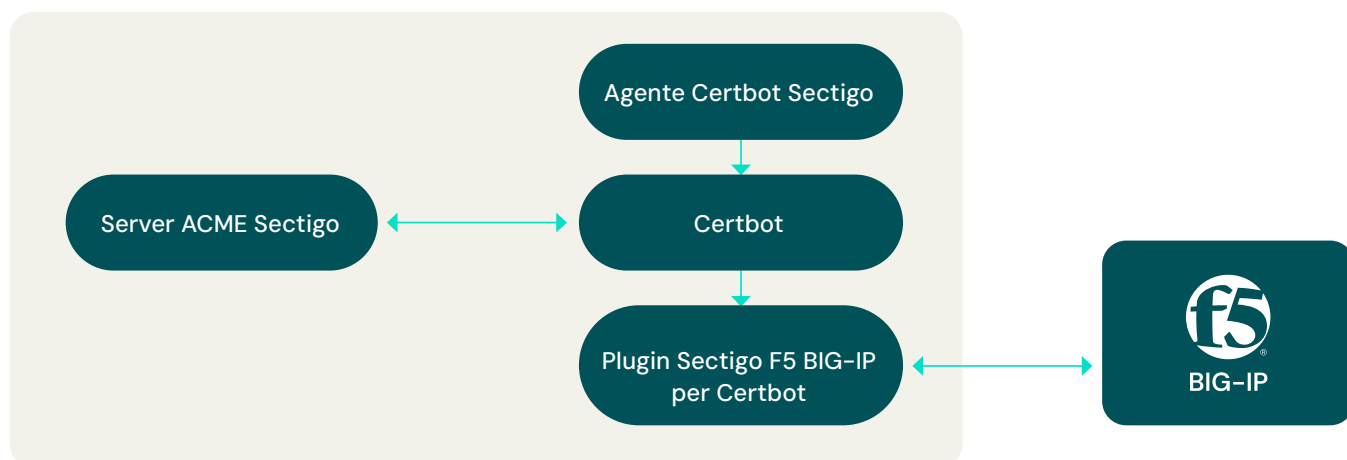


Supporto trasparente agli apparat

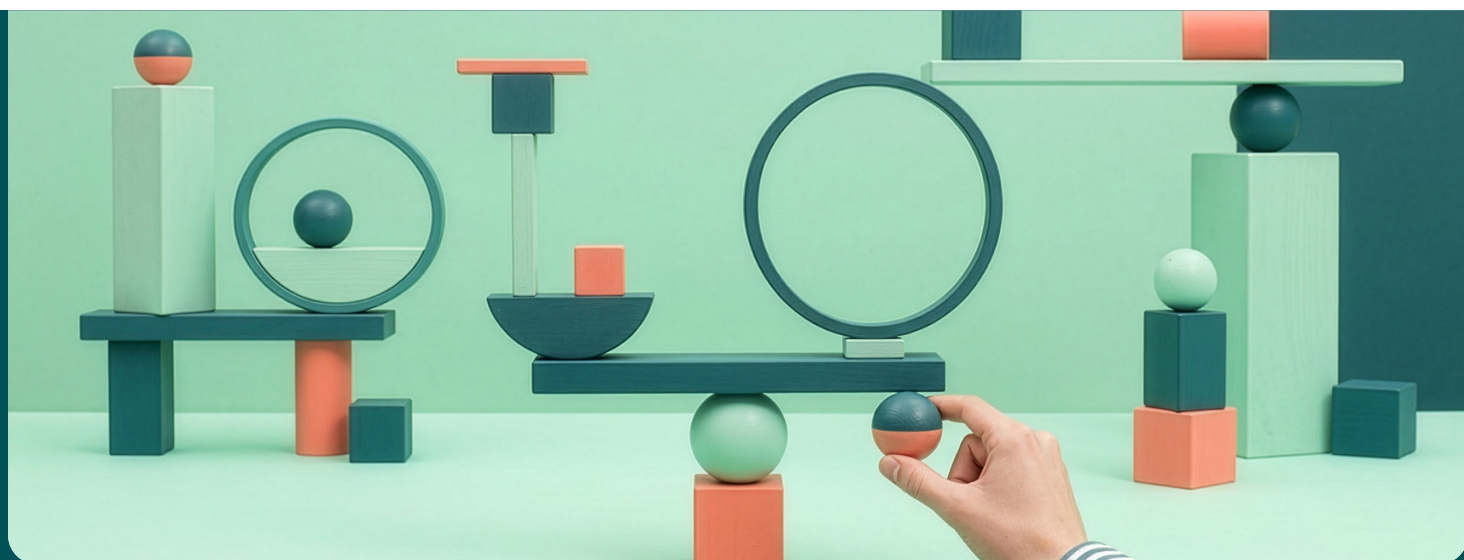
Sectigo semplifica l'integrazione con i server F5 e mantiene la piena compatibilità con i sistemi operativi supportati da Certbot.



Con i certificati SSL/TLS di Sectigo è possibile applicare una solida protezione crittografica, garantire la conformità e proteggere nel tempo gli apparati F5, riducendo al minimo i costi gestionali.



Il vantaggio di Sectigo: L'integrazione Sectigo per F5 offre il rinnovo automatico dei certificati in scadenza, scalabilità sull'intera flotta F5, supporto per algoritmi RSA ed ECDSA ed emissione automatizzata basata sulla configurazione. Le funzionalità esclusive di Sectigo includono la gestione dei profili SSL client, la protezione delle chiavi private e il rinnovo automatico dei certificati revocati.



Informazioni su Sectigo

Sectigo è un provider leader nella gestione del ciclo di vita dei certificati (CLM), che aiuta le organizzazioni a proteggere le identità umane e macchina riducendo al contempo i rischi nascosti della moderna fiducia digitale.

Con l'aumento dei volumi di certificati e la riduzione della loro durata, i certificati non gestiti stanno diventando causa di disservizi, vulnerabilità di conformità e interruzioni operative. Sectigo sfrutta l'automazione orchestrata per offrire semplicità su vasta scala (Simplicity at Scale) tramite la sua piattaforma CLM cloud-native, unendo visibilità, controllo e gestione del ciclo di vita in ambienti complessi. Con oltre 700.000 clienti, tra cui il 65% delle aziende Fortune 500, Sectigo è una delle Autorità di Certificazione più grandi e consolidate, con oltre 20 anni di eccellenza nella fiducia digitale.

Per ulteriori informazioni, visita il sito www.sectigo.com o seguici su [LinkedIn](#).

