sectigo

SOLUTION

Sectigo Orchestration Gateway pour Sectigo Certificate Manage (SCM)

Quand la complexité, la taille et la sécurité s'entrechoquent

Les entreprises exploitent aujourd'hui des environnements hybrides et multi-cloud où le raccourcissement des durées de vie des certificats, la complexité croissante des intégrations et la fragmentation des outils d'automatisation sont devenus des risques opérationnels majeurs. Les équipes s'appuient souvent sur des connecteurs multiples, des scripts fragiles et une documentation incohérente, ce qui crée des erreurs de configuration, des angles morts et des obstacles à l'automatisation à grande échelle.

Dans le même temps, le volume de certificats explose à mesure que les organisations mûrissent leurs architectures Zero Trust et étendent l'authentification machine-à-machine. Selon le rapport Sectigo **State of Crypto Agility Report 2025**, 95 % des organisations dépendent toujours de processus manuels, ce qui souligne les frictions croissantes à mesure que la surface des identités numériques s'étend dans les clouds, les appareils et les charges de travail.

L'évolution des pressions réglementaires, les exigences d'agilité cryptographique et la poussée vers la vérification continue accentuent cette urgence. Alors que les cycles de renouvellement s'accélèrent et que les environnements se diversifient, les entreprises ont besoin d'une couche d'orchestration unifiée garantissant la confiance, la conformité et l'évolutivité entre tous les fournisseurs et modèles de déploiement.

Présentation du Sectigo Orchestration Gateway (SOG) pour SCM

Le SOG est une couche d'orchestration légère conçue spécifiquement pour fonctionner avec **Sectigo Certificate Manager (SCM)**. Il exécute les tâches de déploiement et de gestion du cycle de vie des certificats au sein d'environnements complexes et multi-fournisseurs.

Géré par SCM, le SOG sert de passerelle sécurisée entre SCM et les systèmes distribués de l'entreprise. Il remplace les scripts fragiles et les connecteurs hérités par une capacité d'automatisation évolutive et pilotée par des politiques. Il automatise actuellement les opérations de certificats TLS sur un périmètre d'infrastructures large et croissant, grâce à une architecture modulaire conçue pour prendre en charge d'autres cas d'utilisation au fil du temps.*

Pourquoi les entreprises choisissent SCM avec SOG :

- Automatisent l'ensemble du cycle de vie des certificats sur les serveurs, CDN, WAF et systèmes d'accès.
- Découvrent chaque certificat grâce à une analyse combinée du cloud et du réseau local.
- Adaptent à grande échelle les opérations pilotées par des politiques pour répondre aux durées de vie raccourcies et à l'agilité cryptographique.
- Consolident les connecteurs, scripts et machines virtuelles dans une seule installation de passerelle.
- Appliquent une hygiène stricte des clés et l'extraction d'identifiants juste-à-temps via des integrations PAM et coffres-forts de clés.
- Accélèrent le déploiement sur les plateformes modernes et multi-fournisseurs.

En tant que composant d'orchestration intégré à Sectigo Certificate Manager (SCM), le Sectigo Orchestration Gateway centralise et simplifie l'automatisation en remplaçant les scripts et les intégrations ponctuelles par une solution unique et légère. Géré par les politiques de SCM, le SOG automatise les opérations du cycle de vie des certificats TLS sur les serveurs, répartiteurs de charge, CDN, WAF et systèmes d'accès privilégiés pris en charge, tout en permettant la récupération sécurisée et juste-à-temps des identifiants privilégiés. En étendant l'automatisation de SCM aux serveurs, infrastructures et coffres-forts d'identifiants, le SOG permet aux équipes d'étendre leurs opérations de confiance sans ajouter de complexité opérationnelle.

Opérations de certificats simplifiées et sécurisées

Le SOG centralise l'automatisation sur plusieurs serveurs, répartiteurs de charge et plateformes cloud, remplaçant les scripts fragmentés et les processus manuels. Il récupère de manière dynamique et juste-à-temps les identifiants privilégiés dans des coffres-forts distants, évitant de stocker des données sensibles localement.

Serveurs pris en charge :

IIS, BIG-IP, Apache Tomcat, CLOUDFLARE WAF, APACHE HTTP SERVER PROJECT, NGINX, imperva WAF, netscaler

... et plus

Coffres-forts d'identifiants pris en charge :

Delinea, CYBERARK, HashiCorp Vault, BeyondTrust Pathfinder, Local Vaults

... et plus

Pour obtenir la liste la plus récente des intégrations prises en charge, consultez notre page de documentation technique.

Empreinte légère. Déploiement rapide et prévisible

Léger et modulaire, le gateway se déploie rapidement sur les environnements Linux, Windows et Docker. Son architecture adaptable intègre de nouvelles plateformes et de nouveaux services sans nécessiter de refonte, tandis que la prise en charge des API REST permet une intégration fluide des flux de travail et un déploiement rapide sur des infrastructures distribuées.

Automatisation de bout en bout à grande échelle

La découverte, la délivrance, le renouvellement, le déploiement et la révocation des certificats TLS sont entièrement automatisés sur les serveurs, services cloud et plateformes d'entreprise compatibles avec le SOG. Les mises à jour parallèles garantissent que les opérations suivent le rythme du raccourcissement des durées de vie des certificats et des environnements à fort volume.

Sécurité renforcée à chaque étape

Chaque certificat est associé à une clé unique, éliminant les clés partagées ou stockées de manière centralisée qui augmentent les risques. Les clés sont gérées localement ou via des intégrations PAM et coffres-forts de clés, et la rotation automatisée sur les serveurs garantit une hygiène cryptographique constante. La découverte continue identifie les certificats non gérés dans les environnements cloud, réduisant la surface d'attaque et assurant la conformité.

Visibilité complète dans chaque environnement

La découverte cloud et locale fonctionnent ensemble pour identifier les certificats sur les systèmes internes et externes. Le suivi à la demande 24/7 élimine les angles morts et maintient un inventaire fiable sur les serveurs, plateformes et services exposés sur le cloud, appuyant l'application des politiques et la gestion proactive des risques.

Prêt pour l'avenir et adaptable

Le SOG est conçu pour l'agilité cryptographique : il prend en charge la transition des algorithmes, la préparation à la cryptographie post-quantique et les normes émergentes sur l'ensemble des serveurs, plateformes et protocoles pris en charge. Qu'il s'agisse de moderniser des serveurs web hérités ou de faire évoluer des charges de travail conteneurisées, les politiques d'orchestration s'appliquent de manière cohérente sans nécessiter de refonte d'intégration.

Efficacité opérationnelle avec un retour mesurable

Avec le SOG, les intégrations intégrées et l'automatisation simplifient le déploiement et les opérations quotidiennes. La consolidation des machines virtuelles d'intégration en une passerelle unique réduit l'empreinte infrastructurelle, les efforts de maintenance et les points de défaillance, accélérant le retour sur investissement. Les équipes éliminent le travail répétitif, réduisent les escalades et adaptent les opérations de certificats sans augmenter les coûts d'exploitation.

Cas d'utilisation courants du SOG avec SCM

Automatiser le TLS dans les environnements hybrides

Découvrir, délivrer, installer, renouveler et révoquer les certificats SSL/TLS sur les serveurs, répartiteurs de charge et plateformes cloud sans effort manuel.

Gérer des durées de vie de certificats accélérées

Gérer le raccourcissement des durées de vie et les mises à niveau cryptographiques grâce à une automatisation basée sur des politiques, en alignant les opérations sur les exigences de sécurité modernes.

Workflow simplifiée pour le un-vers-plusieurs

Exécuter des actions sur les certificats TLS basées sur des politiques à travers plusieurs serveurs via une passerelle centralisée unique, éliminant les tâches redondantes.

Booster l'efficacité opérationnelle

Simplifier les déploiements à fort volume, réduire les tâches répétitives et remplacer les scripts fragmentés par une automatisation centralisée.

Visibilité totale sur les certificats via SCM

Aider SCM à analyser les certificats internes et externes pour maintenir un inventaire complet sur l'ensemble des serveurs, appareils et points d'accès cloud.

Découvrir les certificats sur tous les systèmes

Combiner la découverte cloud et locale pour éliminer les angles morts et assurer une conformité continue.

Réduire la surface d'attaque des identifiants privilégiés

Récupérer les identifiants juste-à-temps via des intégrations PAM, évitant le stockage local et limitant l'exposition.

Conformité et préparation aux audits

Centraliser les politiques, automatiser la gestion des certificats et maintenir des contrôles d'audit cohérents.

Minimiser l'étalement des infrastructures

Remplacer les VM spécifiques et configurations haute disponibilité par une seule passerelle, réduisant la charge opérationnelle et les points de défaillance.

Support multi-serveurs et multi-plateformes

Déployer sur IIS, Apache, Tomcat, F5, NGINX, Netscaler, Cloudflare et Imperva via des passerelles locales ou distantes.

À propos de Sectigo

Sectigo est un leader de la gestion du cycle de vie des certificats (CLM), aidant les entreprises à sécuriser les identités humaines et machines tout en réduisant les risques masqués de la confiance numérique moderne. À mesure que les volumes de certificats augmentent et que leurs durées de vie se réduisent, les certificats non gérés deviennent une source de pannes, de faiblesses de conformité et de perturbations opérationnelles. Sectigo utilise l'Automatisation Orchestrée pour offrir la Simplicité à Grande Échelle grâce à sa plateforme CLM native dans le cloud, réunissant visibilité, contrôle et gestion du cycle de vie au sein d'environnements complexes. Avec plus de 700 000 clients, dont 65 % du Fortune 500, Sectigo est l'une des autorités de certification les plus importantes et les plus anciennes, forte de plus de 20 ans d'expérience au service de la confiance numérique.

La solution globale de gestion des certificats de Sectigo permet aux organisations d'automatiser, de sécuriser et d'optimiser en toute fluidité leur infrastructure numérique. En simplifiant les opérations complexes liées aux certificats, en renforçant les protocoles de sécurité et en répondant aux exigences de conformité, les entreprises peuvent protéger leurs environnements hybrides en toute confiance et simplifier leurs flux de travail IT.

Contactez-nous dès aujourd'hui pour obtenir une démonstration personnalisée ou écrivez-nous à sales@sectigo.com pour découvrir comment Sectigo peut transformer votre stratégie de gestion des certificats.