AuthServe

Présence en ligne supérieure, opérations simplifiées

Des services DNS de référence sont essentiels pour configurer, éditer et distribuer l'accès aux services IP (sites Web, téléchargements de vidéos, messagerie, VoIP, etc.) et sont visibles et accessibles à tous sur Internet. La toute première expérience d'un utilisateur avec un service IP démarre avec des serveurs de noms de référence apportant des informations d'adresse ou toute autre information nécessaire pour rejoindre le service. La disponibilité, les performances et la sécurité de l'infrastructure DNS de référence sont donc essentielles pour assurer une expérience utilisateur positive.

DNSi AuthServe d'Akamai est un serveur DNS de référence qui permet des services de noms hautement résilients, sécurisés et toujours disponibles. Contrairement aux serveurs DNS polyvalents, AuthServe est optimisé pour les fonctions de référence et possède une base de données conçue dans cette optique qui apporte des performances et une évolutivité inégalées. Ses fonctionnalités de gestion éprouvées sont immédiatement compatibles avec les environnements opérationnels complexes et permettent de réduire les ressources nécessaires en personnel. AuthServe automatise la gestion du cycle de vie du DNSSEC, rendant le déploiement aussi simple que de gérer des données DNS non signées. Ses caractéristiques uniques comme la visibilité en temps réel et les zones composites améliorent la visibilité et simplifient les opérations.

Performances et évolutivité

Avec l'augmentation des utilisateurs finaux et des appareils, les nouveaux services et applications, les modèles d'utilisation toujours en ligne d'Internet et les architectures de réseaux nouvelle génération, de nouvelles exigences sont demandées aux infrastructures DNS. AuthServe utilise une de base de données unique par version (VDB) intégrée à la mémoire et conçue pour fournir de hautes performances et publier des données DNS en tant que serveur de référence. La VDB gère l'utilisation de la mémoire de façon très efficace, permettant ainsi de stocker plusieurs milliards d'enregistrements, un nombre largement supérieur aux autres serveurs de noms. Sa conception exceptionnelle permet également à AuthServe de prendre en charge des fréquences élevées d'actualisation des DNS de manière fiable.

Résilience et sécurité

Les moteurs renforcés de l'AuthServe assurent des niveaux de service continus et constants. Les serveurs peuvent être mis à jour sans interruption ni indisponibilité de services. Des requêtes peuvent être immédiatement effectuées sur les enregistrements nouveaux ou mis à jour. Les redémarrages ou récupérations du serveur après défaillance du système sont presque instantanés. AuthServe n'a jamais fait l'objet d'une alerte de sécurité et ne partage aucune vulnérabilité connue avec un logiciel open source.

Services toujours en ligne

Par le passé, les serveurs de noms maîtres de référence étaient un point de défaillance unique. Lorsqu'un maître échouait, il n'était plus possible de propager les mises à jour vers les nœuds esclaves et ceux-ci n'apparaissaient pas dans le réseau. Des conceptions en veille active ou d'autres techniques pour traiter ce problème induisaient de la complexité, des délais inacceptables ou des problèmes de synchronisation incompatibles avec des services IP qui nécessitent des modifications de données DNS fréquentes tout en maintenant une disponibilité totale.

Le support à deux maîtres d'AuthServe permet de disposer de deux serveurs de noms actifs de référence en tant que maître pour une même zone. Les mises à jour envoyées vers un maître sont rapidement et automatiquement appliquées à l'autre serveur maître. Comme pour les serveurs maîtres existants, les serveurs à deux maîtres peuvent posséder des serveurs esclaves. Les serveurs sont synchronisés instantanément et en toute fluidité avec les mêmes données et ne nécessitent pas de redémarrage.

PRINCIPAUX POINTS CLÉS

- La base de données par version (VDB) conçue à cet effet fournit des performances exceptionnelles pouvant aller jusqu'à plusieurs milliards d'enregistrements de ressources
- Disponibilité totale des serveurs maîtres avec configuration en ligne (sans redémarrage nécessaire) et un déploiement des deux maîtres actifs-actifs uniques
- L'automatisation complète de la gestion du cycle de vie du DNSSEC réduit les erreurs susceptibles de provoquer la déconnexion de noms et de services
- Les fonctionnalités de gestion avancées comme le contrôle de version et les modèles de zones simplifient les opérations en cours et permettent la délivrance rapide des API.
- La visibilité en temps réel récupère les données des requêtes sans ajouter de charge excessive sur le serveur

DNSi AuthServe

Simplification des opérations

Les commandes et outils AuthServe intégrés simplifient la gestion des données des serveurs de noms, les opérations en cours, la planification et l'approvisionnement.

- Les modèles de zone simplifient la configuration et la maintenance continue des données de zone
- Le contrôle de version enregistre toutes les modifications progressives du serveur de noms, simplifiant les mises à jour où les retours à de précédentes configurations
- L'interface de ligne de commande prend en charge la configuration et les mises à jour en temps réel sans interruption de service
- Les zones de couverture et les affichages des rapports simplifient la maintenance et la configuration du serveur de noms
- Les affichages DNS partagés segmentent les données en différents groupes, comme interne et externe

Automatisation complète du DNSSEC

Le DNSSEC protège de manière cryptographique les données DNS afin que celles-ci ne puissent pas être compromises lorsqu'elles transitent sur Internet. Le protocole DNSSEC introduit également plus de complexité. Une configuration inadéquate peut avoir pour conséquence la disparition pure et simple des données d'Internet, ce qui est inacceptable pour les propriétaires de marques. La gestion du cycle de vie complet du DNSSEC dans AuthServe traite ce problème. Tout ce dont vous avez besoin pour le déploiement est intégré et entièrement automatisé. Cela réduit le nombre d'erreurs qui génèrent un afflux d'appels au support technique, ainsi que les besoins en ressources opérationnelles précieuses et rares.

AuthServe utilise des signatures à plusieurs threads : un noyau répond aux requêtes pendant que les autres noyaux signent. Le système répond toujours aux requêtes avec des performances élevées et une latence prévisible pendant que la signature bénéficie d'une puissance de calcul supplémentaire. Les données DNS signées sont également 8 à 10 fois plus volumineuses que les données non signées. C'est pourquoi la base de données AuthServe, conçue à cet effet, rend l'utilisation de la mémoire et du matériel à plusieurs processeurs extrêmement efficace et permet une évolution et des performances supérieures à celles d'autres alternatives. AuthServe prend en charge la signature en ligne et hors ligne afin d'éliminer les appareils de signature.

Visibilité en temps réel

La visibilité en temps réel (RTV) est une fonctionnalité de pointe qui tire parti de la base de données AuthServe pour collecter, corréler et regrouper les données de requêtes DNS pour prévoir, suivre, établir des tendances, analyser ou effectuer toute autre action. La surveillance par RTV est délestée vers un processus séparé des systèmes à plusieurs processeurs afin d'éliminer tout impact sur le traitement des requêtes à accès rapide. Il est possible d'analyser le trafic de requête en temps réel ou de charger des données pour une analyse hors ligne. Il est également possible d'utiliser des filtres pour rechercher des attributs spécifiques parmi les données. Des outils supplémentaires regroupent et chargent les données pour les traiter par la suite sur d'autres systèmes.

Zones composites

Les zones composites apportent une manière transparente de combiner des données DNS qui peuvent être possédées et gérées par des parties tierces sur une seule zone que l'on peut rechercher à l'aide d'une seule requête DNS. Les requêtes effectuées sur une zone composite, par exemple des passerelles de messagerie réalisant des vérifications antispam, réduisent de manière importante la charge sur les ressources du réseau. Les zones composites réduisent également de manière significative la complexité des logiciels clients dont la connaissance des règles n'est plus autant nécessaire qu'auparavant.

Akamai FASTER FORWARD

Plateforme de diffusion dans le cloud la plus fiable et la plus utilisée au monde, Akamai aide les entreprises à fournir à leurs clients des expériences digitales optimisées et sécurisées sur tous types de terminaux, à tout moment et partout dans le monde. La plateforme massivement distribuée d'Akamai bénéficie d'un déploiement inégalé avec plus de 200 000 serveurs dans 130 pays, offrant ainsi aux clients des niveaux avancés de performances et de protection contre les menaces. Les solutions de diffusion vidéo, d'accès professionnel, de sécurité dans le cloud et de performances Web et mobiles s'appuient également sur un service client exceptionnel et une surveillance 24 h/24 et 7 j/7. Pour découvrir pourquoi de grandes institutions financières, des leaders du e-commerce, des entreprises du divertissement et des médias ainsi que des organisations gouvernementales font confiance à Akamai, consultez les sites www.akamai.com, blogs.akamai.com ou @Akamai sur Twitter. Vous trouverez nos coordonnées dans le monde entier à l'adresse www.akamai.com/locations.jsp. Vous pouvez également nous contacter au +33-1 8564 4654. Publication : 03/18.