

AuthServe

Überragende Webpräsenz, einfachere Vorgänge



Autoritative DNS-Services sind wichtig, wenn es darum geht, den Zugriff für IP-Services (Websites, Videodownloads, E-Mail, VoIP usw.) zu konfigurieren, zu veröffentlichen und zu verteilen. Sie sind für jeden im Internet sichtbar und verfügbar. Das Nutzererlebnis bei einem IP-Service beginnt zunächst bei autoritativen Namensservern. Sie stellen Adressierungsdienste oder andere Informationen bereit, die für das Erreichen eines Services erforderlich sind. Daher ist die Verfügbarkeit, Performance und Sicherheit autoritativer DNS-Infrastrukturen essentiell für ein positives Nutzererlebnis.

Akamai DNSi AuthServe ist ein autoritativer DNS-Server, der äußerst robuste, sichere und immer verfügbare Namensservices bietet. Anders als Mehrzweck-DNS-Server ist AuthServe auf autoritative Funktionen mit einer maßgeschneiderten Datenbank ausgerichtet und bietet unerreichte Performance und Skalierbarkeit. Bewährte Managementfunktionen unterstützen komplexe Betriebsumgebungen und minimieren Mitarbeiteroverhead. AuthServe automatisiert das Lebenszyklusmanagement von DNSSEC, wodurch die Bereitstellung so einfach ist wie das Management vorzeichenloser DNS-Daten. Einzigartige Funktionen wie Echtzeiteinblicke (Real-time Visibility, RTV) und zusammengesetzte Zonen verbessern die Transparenz und vereinfachen betriebliche Vorgänge.

Performance und Umfang

Anwender und Gerätwachstum, neue Anwendungen und Services, jederzeit verfügbares Internet und Netzwerkarchitekturen der nächsten Generation stellen DNS-Infrastrukturen vor neue Herausforderungen. AuthServe verwendet eine einzigartige versionierte Datenbank (VDB) im Speicher, die auf Performance ausgerichtet ist und für die Veröffentlichung von DNS-Daten als autoritativer Server optimiert wurde. Durch eine VDB kann Speicher sehr effizient genutzt werden. Damit können Sie mehr als 1 Mrd. Datensätze speichern – ein Vielfaches mehr als bei anderen Namensservern. Dank des überlegenen Designs von AuthServe können Sie auch DDNS-Updates mit hohen Übertragungsraten zuverlässig durchführen.

Widerstandsfähig und sicher

Kampferprobte AuthServe-Engines erhalten kontinuierliche und konsistente Servicelevel aufrecht. Server können ohne Unterbrechung oder Ausfallzeit aktualisiert werden. Neue oder aktualisierte Datensätze sind sofort für Abfragen verfügbar. Serverneustarts oder Wiederherstellung nach Hardwareausfällen können umgehend ausgeführt werden. Noch nie tauchte AuthServe im Zusammenhang mit Problemen bei der Websicherheit auf und es gibt keine bekannten Schwachstellen bei Open-Source-Software.

Rund um die Uhr verfügbare Services

Früher waren Master-autoritative Namensserver oft ein Single Point of Failure. Wenn ein Master fehlschlug, konnten Aktualisierungen nicht in Slave Nodes verteilt und somit auch nicht im Netzwerk wiedergespiegelt werden. Aktive Standby-Designs oder andere Techniken zur Lösung dieses Problems sind wesentlich komplexer, sorgen für nicht hinnehmbare Verzögerungen oder verursachen Synchronisierungsprobleme. Damit sind sie für IP-Services, für die häufige DNS-Datenänderungen bei gleichzeitiger ständiger Verfügbarkeit erforderlich sind, nicht geeignet.

Da AuthServe duale Bereitstellungen unterstützt, können zwei aktive autoritative Namensserver als Master in derselben Zone dienen. Aktualisierungen auf einem Master werden schnell und automatisch auf den anderen Master angewendet. Für bereits vorhandene Masterserver besteht die Möglichkeit eines Slave-Servers. Die Server können sofort und nahtlos mit denselben Daten synchronisiert werden – ein Neustart ist nicht erforderlich.

HIGHLIGHTS

- Die zielgerichtete VDB liefert außergewöhnliche Performance und Skalierbarkeit für mehr als 1 Mrd. Ressourcendatensätze.
- Dauerhafte Verfügbarkeit der Master-Server mit Onlinekonfiguration (kein Neustart erforderlich) und einzigartige duale aktiv/aktiv Master-Bereitstellung
- Vollständige Automatisierung des DNSSEC-Lebenszyklusmanagement minimiert Fehler, durch die Namen und Services offline gehen könnten.
- Erweiterte Managementfunktionen wie Versionierung und Zonenvorlagen vereinfachen dauerhafte Vorgänge und APIs beschleunigen die Bereitstellung.
- RTV sammelt Abfragedaten, ohne eine zu große Belastung für den Server darzustellen.

DNSi AuthServe

Einheitliche Vorgänge

Integrierte AuthServe-Befehle und -Tools vereinfachen das Datenmanagement für den Namensserver, aber auch laufende Prozesse, Planung und Bereitstellung.

- Zonenvorlagen sorgen für einfache Konfiguration und kontinuierliche Wartung der Zonendaten.
- Die Versionierung erfasst alle inkrementellen Namensserveränderungen und vereinfacht so Updates oder Rollbacks auf vorherige Konfigurationen.
- CLI unterstützt Konfiguration in Echtzeit sowie Updates ohne Serviceunterbrechungen.
- Die Berichte decken Zonen ab und die Ansichten vereinfachen die Namensserverwartung und -konfiguration.
- Geteilte DNS-Ansichten segmentieren Daten für unterschiedliche Gruppen, wie z. B. interne oder externe Gruppen.

Vollständige Automatisierung von DNSSEC

DNSSEC schützt DNS-Daten kryptographisch, so dass diese bei Übertragungen über das Internet nicht kompromittiert werden können. DNSSEC sorgt zudem für weitere Komplexität. Falsche Konfiguration kann dazu führen, dass Domains einfach aus dem Internet verschwinden – ein untragbarer Zustand für Markeneigentümer. Die Lösung für dieses Problem: das vollständige Lebenszyklusmanagement von DNSSEC in AuthServe. Alles, was für eine Bereitstellung benötigt wird, ist integriert und vollständig automatisiert. So werden Fehler minimiert, die zu zahlreichen Anrufen beim Kundendienst führen, und der Bedarf an raren und wertvollen betrieblichen Ressourcen wird minimiert.

Bei der AuthServe-Signierung handelt es sich um Multithread-Signierung, d. h. ein Kern beantwortet Abfragen, während andere Kerne signieren. Abfragen werden immer mit hoher Performance und vorhersehbarer Latenz beantwortet und für die Signierung steht zusätzliche Computerleistung zur Verfügung. Signierte DNS-Daten sind zudem 8- bis 10-mal größer als unsignierte Daten und die zielgerichtete AuthServe-Datenbank verwendet Speicher sowie Multiprozessor-Hardware äußerst effizient und skaliert und performt somit besser als Alternativen. AuthServe unterstützt Online- und Offlinesignierung und macht so Signierungsanwendungen überflüssig.

Echtzeiteinblicke

RTV ist eine völlig neue Funktion: Sie nutzt die AuthServe-Datenbank, um DNS-Abfragedaten für Planung, Nachverfolgung, Nutzungstrends, Forensik und andere Zwecke zu sammeln, zuzuordnen und zu aggregieren. Die RTV-Überwachung wird an einen separaten Prozess im Multiprozessorsystem weitergegeben, damit Pfadabfragen immer so schnell wie möglich verarbeitet werden. Echtzeitabfrage-Traffic kann analysiert werden oder Daten können für Offlineanalysen protokolliert werden. Für bestimmte Attribute von Interesse können Filter zum Durchsuchen von Daten verwendet werden. Zusätzliche Tools können Daten aggregieren und hochladen, um diese in anderen Systemen nacheinander zu verarbeiten.

Zusammengesetzte Zonen

Zusammengesetzte Zonen bieten eine transparente Möglichkeit, DNS-Daten, für deren Verwaltung unterschiedliche Parteien zuständig sind, in einer Zone zu kombinieren. Damit können unterschiedliche Parteien die Daten verwalten und mit einer einzigen DNS-Abfrage durchsuchen. So wird die Last für Netzwerkressourcen reduziert, die die zusammengesetzte Zone abfragen. Hierbei kann es sich z. B. um E-Mail-Gateways handeln, die Anti-Spam-Checks durchführen. Zusammengesetzte Zonen reduzieren außerdem signifikant die Komplexität der Clientsoftware, da die Clients aufgrund dessen an weniger Richtlinien ausgerichtet sein müssen.



Als weltweit größte und renommierteste Plattform für die Cloudbereitstellung unterstützt Akamai seine Kunden dabei, ein optimales und sicheres digitales Erlebnis bereitzustellen – auf jedem Gerät, an jedem Ort und zu jeder Zeit. Die stark verteilte Plattform von Akamai weist mit über 200.000 Servern in 130 Ländern eine beispiellose Skalierbarkeit auf und bietet Kunden somit eine überragende Performance sowie einen umfassenden Bedrohungsschutz. Das Akamai-Portfolio für Website- und App-Performance, Cloudsicherheit sowie Unternehmenszugriff und Videobereitstellung wird durch einen herausragenden Kundenservice und Rund-um-die-Uhr-Überwachung begleitet. Warum führende Finanzinstitute, Onlinehändler, Medien- und Unterhaltungsanbieter sowie Behörden auf Akamai vertrauen, erfahren Sie unter www.akamai.com, blogs.akamai.com oder auf Twitter unter [@AkamaiDACH](https://twitter.com/AkamaiDACH) sowie [@Akamai](https://twitter.com/Akamai). Unsere globalen Standorte finden Sie unter www.akamai.com/locations. Sie können uns zudem unter der Telefonnummer +49 89 94006 308 erreichen. Veröffentlicht: März 2018