AuthServe

Superior web presence, simpler operations

Authoritative DNS services are critical to configuring, publishing, and distributing access to IP services (web sites, video downloads, email, VOIP, etc), and they are visible and available to everyone on the Internet. The initial user experience with an IP service starts with authoritative name servers, which provide addressing or other information needed to reach the service. Availability, performance, and security of authoritative DNS infrastructure are thus essential to ensuring a positive user experience.

Akamai DNSi AuthServe is an authoritative DNS server that enables highly resilient, secure, always-on name services. Unlike multi-purpose DNS servers, AuthServe is optimized for the authoritative function with a purpose-built database that delivers unmatched performance and scaling. Proven management features readily support complex operational environments and minimize staff overhead. AuthServe automates lifecycle management of DNSSEC, making deployment as simple as managing unsigned DNS data. Unique features like Real Time Visibility and Composite Zones improve visibility and simplify operations.

Performance and Scale

End user and device growth, new applications and services, always-on Internet usage patterns and next-generation network architectures place new demands on DNS infrastructure. AuthServe uses a unique in-memory Versioned Database (VDB) designed for performance and optimized for publishing DNS data as an authoritative server. VDB makes extremely efficient use of memory so more than a billion records can be stored, well beyond other nameservers. Superior design also allows AuthServe to support high DDNS update rates reliably.

Resilience and Security

Hardened AuthServe engines maintain continuous and consistent service levels. Servers can be updated without service interruption or downtime. New or updated records are instantly available for queries. Server restarts or recovery from hardware failures is near instantaneous. AuthServe has never been cited in a security advisory and shares no known vulnerabilities with open source software.

Always-On Services

In the past, master authoritative nameservers were a single point of failure. When a master failed, updates could not be propagated to slave nodes, and thus not reflected in the network. Active-standby designs or other techniques to address this problem introduce complexity, unacceptable delay, or synchronization problems, which is incompatible with IP services that require frequent changes to DNS data while maintaining 100% uptime.

AuthServe's dual-mastering support allows two active authoritative name servers to serve as masters for the same zone. Updates applied to one master are rapidly and automatically applied on the other master server. As with existing master servers, dual-mastered servers can have slave servers. Servers are instantly and seamlessly synchronized with the same data and do not require a restart.

KEY HIGHLIGHTS

- Purpose-built Versioned Database (VDB) delivers exceptional performance and scaling to more than 1 Billion Resource Records
- 100% uptime of master servers with online configuration (no restart needed) and unique active-active dual-master deployment
- Complete automation of DNSSEC lifecycle management minimizes errors that can cause names and services to go offline
- Advanced management features like versioning and zone templates simplify ongoing operations. APIs speed provisioning.
- Real Time Visibility (RTV) collects query data without excessive burden on the server

DNSi AuthServe

Streamline Operations

Built-in AuthServe commands and tools simplify nameserver data management, ongoing operations, planning, and provisioning.

- Zone templates make configuration and ongoing maintenance of zone data simple
- Versioning journals all incremental name server changes, simplifying updates or rollbacks to prior configurations
- CLI supports real-time configuration and updates without service interruption
- Reports covering zones and views simplify name server maintenance and configuration
- Split DNS views segment data for different groups, such as internal and external

Complete Automation of DNSSEC

DNSSEC cryptographically protects DNS data so it cannot be compromised as it transits the Internet. DNSSEC also introduces additional complexity, and improper configuration results in domains simply disappearing from the Internet – unacceptable for brand owners. Complete DNSSEC lifecycle management in AuthServe addresses this problem, everything needed for deployment is integrated and completely automated. This minimizes errors that create floods of support calls, reduces the need for scarce and valuable operational resources.

AuthServe signing is multithreaded, one core answers queries while other cores sign. Queries are always answered with high performance and predictable latency and signing gets additional computing horsepower. Signed DNS data is also 8 to 10 times larger than unsigned data and the AuthServe purpose-built database makes extremely efficient use of memory and multiprocessor hardware so it scales and performs better than alternatives. AuthServe supports online and offline signing to eliminate signing appliances.

Real Time Visibility

Real Time Visibility (RTV) is a cutting edge feature that leverages the AuthServe database to collect, correlate, and aggregate DNS query data for planning, tracking, usage trends, forensics or other purposes. Monitoring with RTV is offloaded to a separate process in multiprocessor systems to eliminate any impact on fast path query handling. Live query traffic can be analyzed or data can be logged for offline analysis. Filters can be used to screen data for specific attributes of interest. Additional tools aggregate and upload data for subsequent processing on other systems.

Composite Zones

Composite zones provide a transparent way to combine DNS data, which may be owned and managed by separate parties, into a single zone that can be searched with a single DNS request. This greatly reduces the load on network resources that query the composite zone, such as mail gateways doing anti-spam checks. Composite zones also significantly reduce the complexity of client software by reducing the need for clients to be policy aware.

Akamai FASTER FORWARD

Published 03/18.