



DATA SHEET



VeriSign® DIGITAL BRAND MANAGEMENT SERVICES

Ten Steps to a Robust DNS From the Leaders in DNS Management

DNS Assurance Plus

This complete solution enhances the reliability and manageability of both primary and secondary DNS data, and is optimal for minimizing upfront and lifecycle expenses associated with enterprise-class DNS management.

DNS Assurance

Organizations that manage their primary DNS in-house can maintain a continuously updated copy of their secondary DNS on the VeriSign global network of name servers, thereby creating a cost-effective way to increase redundancy and global coverage.

DNS Management Best Practices

Whether a company manages its own Domain Name System (DNS) infrastructure or outsources management to another organization, there are important guidelines to follow to ensure that the DNS is designed properly and can provide robust, uninterrupted service. VeriSign's engineering and operations teams, building on their experience managing the world's largest DNS for the .com and .net domain name registries, have developed the following checklist to ensure maximum reliability, security, and performance of DNS systems:

- Establish multiple name servers to serve zones. This approach ensures that the failure of one name server does not cut zones off from the Internet.
- Distribute name servers geographically, which serves two purposes:
 - + A network failure caused by an act of nature or other incident affecting a particular region will not take out other name servers on your network.
 - + Locating name servers closer to the user communities that need them will help users resolve Web site names more quickly. For example, a substantial user base in Asia would justify having at least one name server in Asia.
- Connect name servers to multiple Internet Service Provider (ISP) networks. Doing so ensures that the failure of one ISP does not interrupt DNS service.
- Provide name servers with fast, high-bandwidth connections to the Internet, which, in combination with geographic diversity and the use of multiple ISPs, makes DNS infrastructure highly resistant to a distributed denial-of-service attack.
- Invest in regular and up-to-date training for network operations, engineering, administration, and other DNS-related personnel to minimize configuration mistakes on complex Berkeley Internet Name Domain (BIND) servers, the most widely used name server software.
- Provide proper security for name servers, including the latest updates, security patches, and bug fixes for BIND servers.
- Maintain 24/7 technical support staff, which ensures that DNS expertise is available for unexpected events that could jeopardize continuity of operations.



Where it all comes together.™



DATA SHEET

- Monitor name servers as tightly as if they were hardware, operating systems, or applications; this task includes monitoring availability and responsiveness. There are limited off-the-shelf tools to do this, but even the simplest monitor is beneficial.
- Institute a change process to ensure that new name server configurations and zone data are tested before they are put into production.
- Create business continuity and disaster recovery plans for the DNS; this process should also include augmentation of DNS infrastructure with additional DNS servers in additional locations.

Visit us at www.Verisign.com for more information.