WEBSITE MONITORING YOU CAN TRUST
DOTCOM-MONITOR

1001 Twelve Oaks Center Drive
Wayzata, MN 55391
1-888-479-0741
www.dotcom-monitor.com

Grain Insurance and Guarantee Co. Solves Upstream DNS Problems Using Dotcom-Monitor®

Summary

Industry: Insurance/Financial

Business Challenge: Ongoing, intermittent Domain Name Server (DNS) issues, affecting website accessibility and the ability of the company to service its customers through its website.

Strategy: Dotcom-Monitor® traceroutes where used to document a problem with Grain Insurance's DNS service provider. The DNS service provider had previously been unwilling to accept responsibility for the DNS issues.

Result: As a result of Dotcom-Monitor's monitoring and error diagnostic information, the DNS service provider admitted there was issue with an upstream network provider and tasked that provider to correct the problem.

Case Study

Grain Insurance: With headquarters in Winnipeg and offices in Ontario, Nova Scotia and Saskatchewan, Grain Insurance and Guarantee Company (www.graininsurance.com) delivers insurance products throughout Canada. In business since 1920, Grain Insurance has a long reputation as an insurance innovator by developing specialized insurance programs for the changing needs of Canadian **businesses**.

Grain Insurance's website provides news, insurance information, insurance application forms and career information. Grain Insurance uses its website to provide critical business applications to its customers.

Grain Insurance uses Dotcom-Monitor to check the availability, accessibility and performance of its website and email servers. Using Dotcom-Monitor monitoring stations in Calgary, New York and London, Grain Insurance can ensure web availability for its customers and business partners in North America and the United Kingdom.

DNS resolution issues: Recently, Dotcom-Monitor alerted Grain Insurance to a problem with one of its DNS servers. The problem was detected by Dotcom-Monitor's Calgary station, which generated an SMS alert to Grain Insurance's IT group.

"The Calgary monitoring station gives us the coverage we need in our most important geographic market, so we jumped on the alert," said Guy Barnabe, IT Service Manager for Grain Insurance. "We had seen the problem before. We use a DNS service and they wouldn't admit there was any problem on their end. Part of the issue is you never know what the true impact of a DNS problem is, but it is a problem when customers can't connect to your site."

As part of its website monitoring, Dotcom-Monitor performs a DNS resolution check. A DNS resolution is a process that occurs when a web browser accesses a website for the first time.

DNS resolution checking: when a client (or end user) computer wants to connect to another website, the client computer must first perform a DNS resolution by connecting with a DNS server. The client computer connects with the DNS server in order obtain the IP address of the web server providing the website. If a DNS server in the local domain cannot resolve the request it queries other DNS servers to locate a DNS server that can. If a DNS server is not available or none are able to resolve the request, the client computer will not connect to the website.

A DNS infrastructure can be complex, especially when a chain of linked DNS servers is used to provide the end user with name resolutions. If any link in this chain breaks or becomes unavailable, a website may also be unavailable.

Dotcom-Monitor uses a proprietary process to check every link in a DNS resolution chain. Dotcom-Monitor starts with the DNS root servers (such as A.ROOT-SERVERS.NET) and propagates all the way down to an end server to retrieve the final results. If Dotcom-Monitor detects problems in any server along the way, it flags the specific step where the problem is detected and generates an alert.

Pinpointing the problem: In the case of Grain Insurance, Dotcom-Monitor provided Barnabe with a DNS trace-route as part of the automated error diagnostic process. The DNS trace-route clearly identified the server in the link causing the problem. Barnabe sent the trace-route information to his DNS service provider. Dotcom-Monitor also provided network trace-route Information that showed packet loss occurring between the Calgary monitoring station to the DNS server responsible for the DNS resolution. At the same time, a Minnesota monitoring station did not show any packet loss to the same DNS server.

Resolution: "At first the DNS service provider said they didn't have a problem. However, the trace-route showed exactly what was going on with the name look-up. Five days later the DNS service provider ran their own tests, validated the Dotcom-Monitor results, and admitted there was a problem," Barnabe said.

"Specifically, the DNS service provider said there was an upstream problem with their network provider, and that while the upstream provider normally does a really good job of handling DNS attacks, there were some underlying router table problems," he noted.

"Without Dotcom-Monitor, we might have never known there was an issue, and the impact to our business would have been incalculable. Without the error diagnostic trace-route, our DNS service wouldn't have found their issue," said Barnabe. "If the DNS service provider also used Dotcom-Monitor we wouldn't have problems like this."