



Avoiding Million Dollar Outages: Achieving High Availability For IP Applications Running on Mainframes

Customer Profile

About this Company

Like many Fortune 1000 companies, this large insurance institution relies heavily on Mainframe systems as a critical portion of their business infrastructure - accessed by thousands of employees around the world. With ten IBM 3270s running hundreds of business critical applications, these systems are tied to an estimated \$12.4 million dollars in revenue a day.

Executive Summary

With hundreds of business critical applications running on a large insurance institution's corporate Mainframes, a four hour fail-over time represented a substantial loss of revenue and productivity. Using F5 Networks 3-DNS® Controller to automatically steer corporate users to backup systems, this organization was able cut their fail-over time, while removing the need to coordinate far reaching changes throughout their enterprise. For large organizations, achieving faster fail-over with the 3-DNS product can translate to a significant increase in productivity and a savings of up to \$2.06 million dollars per outage.

Challenge

A corporate initiative dictated a move from client/server applications in favor of TCP. The scalability and stability of Mainframe systems made it an ideal platform to run their centralized, business-critical applications. Many of their legacy Mainframe applications were migrated to run over IP. On average, a single Mainframe CPU can run fifteen to twenty high volume applications. This differs from today's traditional application and Web server deployments, where scale and reliability are achieved by purchasing many servers, then load balancing or clustering them together in a pool.

"Mainframes provide all the processing power you need so that you don't have to scale boxes to get the performance," said the network administrator responsible for the project. "They also provide a very stable, established environment that can be trusted - most of the time." However, Mainframes are not exempt from all problems. Although errors such as CPU failures are infrequent, they often have a significant impact on business because of the high profile applications that they host. Compounding the problem is that fact that most Mainframe applications are usually designated to run on a single host, leaving no device to step in if the primary CPU fails. This creates a significant challenge for many large organizations.

Long Application Fail-Over Time

For this customer, each of the hundreds of applications that run on their IBM Mainframes use a single CPU. Prior to deploying the solution from F5, a CPU failure meant starting up the application on a second host. Changes to the DNS were then required throughout the enterprise so the client machines could find the application. According to the network administrator, "Typically, this process took 3-4 hours. We would have to manually change the DNS entries and then the master DNS servers had to propagate all those changes down the Local DNSes (LDNS) on the individual machines."

Further Administrative Challenges - Not All Applications Are Created Equal

While simply "rolling down" DNS changes to the client machine worked for some applications, it was not a universal solution. Several applications required manual changes on the desktops or within the applications themselves; others required rebooting at the desktop. In the end, the path to recovery depended on the application. "You can imagine how much trouble it is to get thousands of people globally to shut down, wait until it is back up, and then reboot," said the network administrator. "There's no way to handle it quickly and it creates a ripple effect throughout the organization as users begin flooding the help desk."



Maintenance Challenges

Even with the defined processes for recovering their applications, shifting applications off of the systems that needed maintenance was problematic because it still took 3-4 hours. Application volumes were lighter, but there was always a group using the application, even during planned maintenance windows. As a result, more IT resources and coordination was needed, and required maintenance was often delayed.

Solution

To solve these problems, this enterprise chose to deploy the 3-DNS Controller, F5's global load balancing solution. The 3-DNS Controller monitors the availability and health of global resources and provides top level traffic direction, enabling business continuity and global availability of IP applications running on Mainframes. Even though all of the Mainframes run in a single location, this solution was ideal because the 3-DNS Controller automatically:

- Reduced fail-over time to 3 or 4 minutes
- Eliminated the administrative burden of making global DNS changes
- Provided transparent fail-over to users throughout the enterprise

Configuration

In this company's network infrastructure, the 3-DNS Controller is deployed as the Authoritative Name Server to the applications being hosted on the ten Mainframes. The 3-DNS Controller directs users to the appropriate CPU running the desired application. Each application is configured to use the 3-DNS Controller's Global Availability load balancing mode. This mode directs all traffic to a primary device or site, and users are only failed over to a second resource if a failure is detected on the primary resource.

The 3-DNS Controller is configured with all applications defined on each Mainframe. This allows the 3-DNS Controller to use advanced health checks to automatically detect the device that is actually running the application. To monitor the availability of each system and application, the 3-DNS Controller sends a ping to each CPU, and then performs an Extended Content Verification (ECV) health check for each application. The ECV is a unique health check that allows the 3-DNS Controller to check whether the node returns specific content – a true test of the availability of that service. For example, the 3-DNS Controller can monitor a stock research application by regularly testing for a specific piece of information, like a specific stock symbol. If the expected content is not returned, the 3-DNS Controller marks the application as inactive, and no longer directs traffic there.

Using the 3-DNS Controller in this capacity, each application would show one active device (Mainframe CPU) and nine inactive devices. Users trying to access the application would then be directed to the primary CPU for that application, because it is the only one that the 3-DNS detected as active.

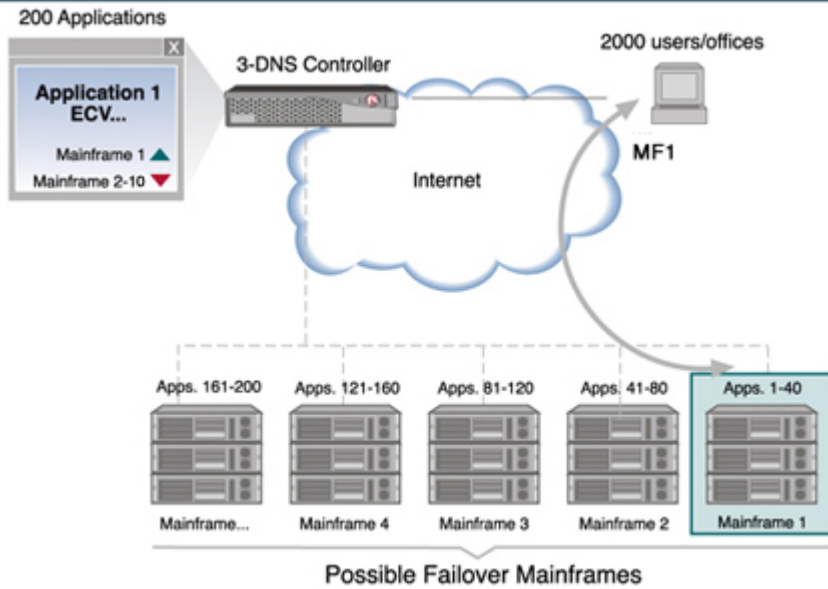


Figure 1: The 3-DNS Controller performs health checks to verify application availability on each Mainframe. The user is directed to the Mainframe 1, which is hosting the requested application.

The Results

When a Mainframe or application failure on the primary device occurs, administrators are alerted to the failure. The 3-DNS Controller shows that no available devices are serving that application. To fail it over to another device, an administrator has to launch the application on another CPU. Starting the application manually on a second device is a step that could not be automated for this site.

Once the application is up on the secondary CPU, the 3-DNS Controller automatically detects that the application is up and begins directing clients to the new device.

The 3-DNS system has been deployed in this capacity for over nine months, steering clients transparently to critical Mainframe applications and:

- Providing faster fail-over for Mainframe systems - nearly 40 times faster
- Simplifying Maintenance and Automation
- Avoiding the introduction of new inline hardware or bottlenecks
- Providing dramatic cost and time savings during system fail-overs

Automation: Minimizing Manual Changes

When this enterprise experiences an application failure, the 3-DNS Controller saves a tremendous amount of time because it requires no manual changes to the DNS infrastructure. Making changes to DNS entries or modifying applications and desktop settings are eliminated; everything is handled automatically. If the primary CPU goes down, the application only needs to be launched on another system.

Fast Fail-Over - Under 5 Minutes

Complete fail-over of thousands of clients to a new Mainframe system is now under four minutes. As soon as the application is available on another resource, the 3-DNS immediately detects it and begins directing users to the new device.

Simpler Maintenance

Performing maintenance on a Mainframe now has less overall financial impact on the organization.



SUCCESS STORY

When maintenance is required, the administrator only needs to shut down the application on one system and start it on a secondary system. All other changes are automatically handled by the 3-DNS system.

No Changes To Inline Networks

Because each of the Mainframes was located within a single data center, why did this customer choose to use 3-DNS to perform local area load balancing? While it is true that the 3-DNS is typically deployed to control traffic over multiple data centers, the solution can also provide high availability for local systems, such as Mainframes. According to the customer, "Using 3-DNS was ideal because we didn't have to introduce anything inline and we were able to leverage the existing infrastructure which was in place." With 3-DNS, distributed users receive a top level DNS direction to the available system, enabling complete fail-over within minutes and introducing no new hardware or bottlenecks into the core traffic stream.

Cost Savings: Four Employee Years of Labor and \$2.06 Million Dollars

Calculating down time costs can be difficult for many organizations. For this customer, the value of providing fast, automated fail-over represented significant value that spanned both productivity and revenue losses. While this company would not pinpoint the number or outages over a year, the impact for just one failure illustrates the widespread financial effects. Consider the following scenario which aligns to their business metrics:

Average Fail-Over Time

When a single Mainframe CPU fails, an average of 12 applications must be moved to another system. The average time it takes to fail-over and point users to a new system is four hours.

Potential Lost Labor

Each application is accessed by 2000 employees for critical job related activity. One hour of downtime represents 2000 employee hours, or one year. Given this scenario, the productivity cost of a single failure without 3-DNS was four employee years.

Potential Lost Revenue

With systems representing an estimated 12.4 million dollars a day in revenue, the cost of a failure that disrupted core business applications could be as high as \$516,666 per hour. Given this scenario, the revenue cost of a four hour failure is approximately \$2.06 million dollars.

About F5

As the pioneer and global leader in Application Traffic Management, F5 continues to lead the industry by driving more intelligence into the network to deliver advanced application agility. F5 products ensure the secure and optimized delivery of applications to any user - anywhere. Through its flexible and cohesive architecture, F5 delivers unmatched value by dramatically improving the way organizations serve their employees, customers and constituents, while lowering operational costs.