Automated Uptime Layer for Stratus ftServer Systems

Take the worry out of uptime assurance

Words every business manager dreads: *The server is down. And so are your mission-critical applications.* The bad news gets worse when nobody can find the cause. Is it a software problem? Hardware error? One thing is for sure. The longer the outage lasts, the more you stand to lose – revenue, productivity, customers, reputation.

Here's something that works much better than dealing with downtime after it's already happened: the Automated Uptime™ Layer for Stratus® ftServer® systems. Our uptime layer takes the complexity and uncertainty out of uptime assurance.

Inside every ftServer system we sell, the uptime layer constantly monitors system resources to preempt downtime and data loss. Our Automated Uptime Layer is a lot like having an engineer watching over your server 24 hours a day, seven days a week.

QUICK FACTS

WHAT OUR AUTOMATED UPTIME LAYER DOES FOR YOUR BUSINESS

- Prevents hardware and software problems from causing downtime

- Rides through faults automatically so your mission-critical applications don't miss a beat

- Reduces risk of human error

- Prevents outages from causing data loss and corruption – we even protect in-memory data

- Detects, analyzes, handles, and reports events to Stratus service experts

- Captures data for root-cause analysis, so you get fast, permanent solutions to issues

- Ensures uptime for Microsoft® Windows Server® and Hyper-V®, VMware® vSphere™ and Red Hat® Enterprise Linux® operating environments

- Works seamlessly with your existing applications and system management tools

"Investing in a solution built for maximum uptime takes the risk out of the equation."

Christophe Deslandes
CIO
KapStone Paper and Packaging Corporation

### Uptime. All the time.

Stratus®
ftServer™

No one else gives you deeper uptime protection – or makes it simpler

Detect, isolate, resolve: the Automated Uptime Layer handles it all — while your applications keep on running

Organizations like yours say uptime is more important to business than ever.* But protecting that uptime takes more time and effort because IT complexity is going up, particularly as you add virtualization and cloud technologies. We'll lighten your load with 24/7 uptime assurance that is simple and effective.

Easy to deploy and manage

Our fault-tolerant servers are known for using pairs of hardware components that eliminate single points of failure. The Automated Uptime Layer provides a **single system view** that keeps these redundant components running in perfect lockstep. Even if there's an error in one component, its partner continues to operate without interruption or loss of data.
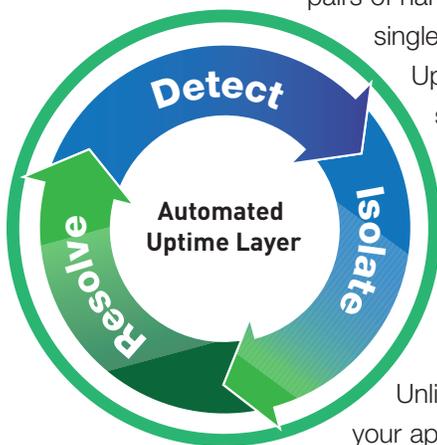
Unlike cluster technologies, you and your applications see a single system image. You don't have to modify your applications or license multiple copies of software which drives up your costs.

THE DIFFERENCE: Our single system view removes complexity. With conventional technologies like clusters, you have to configure, build, test, and maintain the high-availability system yourself.

This means you deal with the hassle of synchronizing state information between cluster nodes and between the layers of multi-tiered applications such as the Web layer, middleware, and back-end database. And your IT staff has to manage more individual physical servers.

Continuous self-diagnostics

The Automated Uptime Layer automatically analyzes more than 500 conditions that your ftServer system is instrumented to monitor. This **comprehensive monitoring and analysis** is always active, not just after an event has already caused trouble. With comprehensive diagnostic data at their fingertips, Stratus service experts determine the precise cause of hardware, system software, and operating system issues.

Conventional servers aren't built to gather, analyze, and proactively report on this depth of system health information. It takes trial and error to figure out whether the issue is due to hardware, software, network, environment, or an operator mistake. As a result, many times the root cause is never found. So, the same problem can happen again and again.

THE DIFFERENCE: Our deep diagnostics automatically capture the information needed to accurately identify the root cause of a problem to the individual hardware component or software line of code in 99% of cases.

"In our previous scenario, if we had an equipment failure, it was up to us to identify that we had an equipment failure and then report it to the vendor."

Roger Hanssen
Director, Information Technology
Ambulance Service of New South Wales

* 2010 High Availability and Virtualization Survey, November 2010, ITIC for Stratus Technologies

Detect

Isolate

Resolve

Automated Uptime Layer

Uptime. **All the time.**

Prevention is more effective than recovery

The ultimate key performance indicator

Calculated every day, our Stratus Uptime Meter℠ tracks the actual uptime of ftServer systems installed at customer sites worldwide.

You'll see that our uptime assurance keeps server down-time to less than a minute per year on average.

Early warning system
The Automated Uptime Layer evaluates and filters literally hundreds of system events in real time. It determines which issues your ftServer system can self-correct, and when to send **automatic alarms and alerts** to you and our expert Stratus service team. It's like an early warning system that preempts downtime.

THE DIFFERENCE: With most servers, the responsibility for reacting to alerts, interpreting them, and taking action is all on you.

Automatic fault handling and problem escalation
No other vendor automates fault and error handling like Stratus. Our intelligent **uptime manager** performs corrective actions like taking a failed component offline while your system keeps running. If your server needs a replacement part, the uptime manager calls home and orders the correct component — 100% of the time.

The uptime manager also opens support calls over our secure global ActiveService™ Network. You get instant access to uptime experts no matter where in the world your system is located.

THE DIFFERENCE: Your ftServer system automatically rides through transient errors and faults that cause other servers to crash, lose data, or both. And timely human help to resolve more complex problems is there for you 24/7 with ftService™ support coverage.

Reliability-tested device drivers
Device drivers that don't behave as expected are notoriously hard to diagnose and represent a significant cause of downtime. So we help **harden device drivers** as well.

We verify stability, probe for vulnerabilities, and work with our partners to make sure supported devices work as you expect. Our automated testing makes sure we don't overlook anything manual testing might miss. For example, we run thousands of tests to make sure devices can handle surprise removal and insertion while your server continues normal processing.

THE DIFFERENCE: Incompatibilities between conventional servers and third-party components often cause systems to hang or crash. We've done the platform and operating environment testing, so you can concentrate your testing on your application.

Automated change management
Changes to your server are another potential cause of unplanned downtime. The Automated Uptime Layer includes a **change control agent** that does preflight checks before bringing any new hardware or firmware online. These checks make sure any new ftServer hardware components match your server, and that system software updates are compatible.

As an option in your Windows operating environment, the uptime layer works with our Active Upgrade™ software to minimize planned downtime when you need to apply software patches and service packs or upgrade the operating system.

THE DIFFERENCE: Most servers leave all of the change control to you, which adds to your IT team's workload and increases the chance of human error.

Uptime. **All the time.**

A closer look at the Automated Uptime Layer

FEATURE	FUNCTION	RESULT
Single system view	• Presents and manages replicated ftServer components as a single system — reducing complexity and human error • Lockstep firmware	• Applications run without modification • Only a single copy of software is required – cuts software license costs • Less time on system management
Comprehensive monitoring and analysis	• Purpose-built diagnostics look at more than 500 operating conditions • Captures data / preserves system state information, enabling root-cause analysis	• Worry-free uptime assurance • Reduces "unknown" errors to less than 1% • Eliminates guesswork, trial and error approach to problems
Automatic alarms and alerts	• Evaluates and intelligently filters system events in real time • Automatic notifications to customers and authorized Stratus support personnel	• 24/7 monitoring • Proactive response • Stratus resolves 99% of issues remotely, maximizing uptime
Uptime manager	• Automates fault and error handling • Tracks inventory of server components, including revision level • Records fault history • Dynamic risk assessment	• Zero downtime • Corrective action; no human intervention • Automatic problem escalation • Orders correct replacement part 100% of the time
Hardened device drivers	• Strengthens driver hardware and software with automated error-insertion testing	• Drivers free of flaws that cause system crashes or data corruption • Third-party components tested for reliability
Change control agent	• Verifies that component versions match • Checks that self-test diagnostics complete successfully	• Enforces change control automatically, reducing the risk of human error

" If we ever have to go through any system dumps and log reports, Stratus has incredible intellectual property in that space. And they're very good at narrowing down the exact problem."

David Campbell
Chief Information Officer
Strategic Payment Services

Stratus
24 7

Stratus®
Technologies

www.stratus.com