WHITE PAPER

Stratus Uptime Assurance Architecture

Automatic 99.999% uptime for Red Hat Enterprise Linux operating environments on ftServer systems

by Stratus Technologies
August, 2011

Uptime. **All the time.**

Contents

Introduction

A robust IT infrastructure matters more than ever. Server virtualization and cloud computing have brought new benefits and capabilities to IT organizations, but not without their own set of challenges and risks. High-performance and high-density services and applications are also on the rise while multiple application interdependencies have added to the number of IT environments being described as mission- or business-critical. Today, if your servers are down, so is your business.

Despite its many advantages, virtualization software alone cannot deliver the total uptime assurance that critical production applications require. Stratus® fault-tolerant server architecture protects your infrastructure against IT business vulnerabilities and complements the resilience you can achieve with Red Hat® Enterprise Linux® and cloud computing.

Stratus' family of fault-tolerant ftServer® systems is proven to deliver industry-leading uptime of 99.999% and greater for Red Hat Enterprise Linux operating environments. Off-the-shelf Linux-based applications need not be modified in any way to benefit from Stratus' exceptional availability safeguards. This advantage represents a considerable improvement over clusters that require failover scripting, repeated test procedures, and software changes to make applications cluster-aware.

The source of this immediate, transparent availability protection is Stratus' uptime assurance technology that is built into every ftServer system. Robustness and serviceability are engineered into every aspect of the ftServer hardware and software. The result is a complete line of industry-standard, Intel® processor-based servers offering unsurpassed uptime, operational simplicity, and significant financial advantage over competing high-availability clusters.

This paper presents an overview of Stratus uptime assurance technology for ftServer Systems. Fundamentals behind the purpose-built design — resilient servers, the Automated Uptime™ Layer, and proactive availability management — are explained in detail.

The uptime assurance difference

Every Stratus ftServer system includes uptime assurance features that are the outgrowth of more than three decades' experience of ensuring uptime for demanding mission-critical and business-critical applications. All aspects of the uptime assurance design work concurrently to prevent downtime, not simply minimize it.

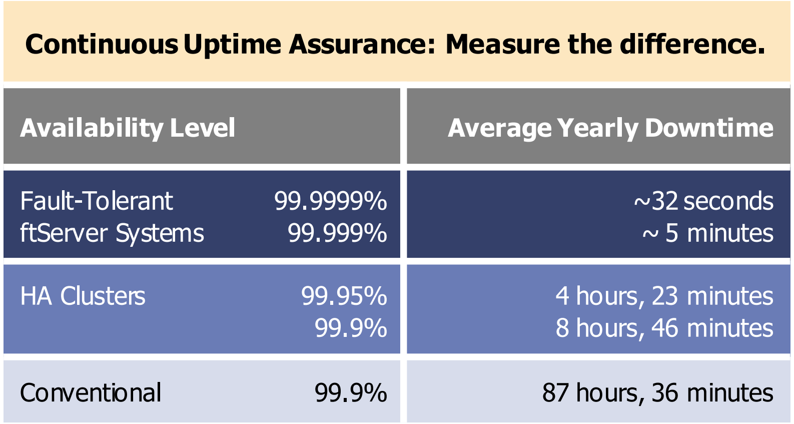
Downtime prevention

Preventing downtime is a key design point that differentiates the ftServer family from "robust" traditional servers and high-availability clusters (which use multiple servers to quickly recover from downtime after one of the servers in the cluster fails). Unlike reliability-enhancing approaches that are not integral to the server's design, built-in uptime assurance works automatically to preempt downtime and limit exposure to operator error.

Industry-leading uptime for Linux operating environments

Every ftServer system running the Red Hat Enterprise Linux OS delivers hardware and operating system availability that consistently exceeds five nines (99.999%). These measurements are based on actual production system data. Recent data shows that ftServer systems experience less than one minute of downtime per year on average.

Figure 1: Automatic Uptime Assurance for Linux Environments



Continuous Uptime Assurance: Measure the difference.

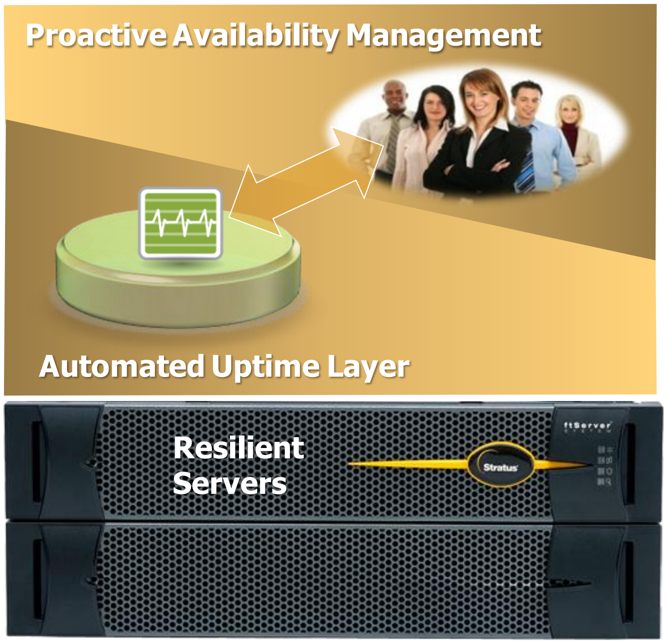
Availability Level		Average Yearly Downtime
Fault-Tolerant ftServer Systems	99.9999% 99.999%	~32 seconds ~ 5 minutes
HA Clusters	99.95% 99.9%	4 hours, 23 minutes 8 hours, 46 minutes
Conventional	99.9%	87 hours, 36 minutes

Linux applications automatically benefit from Stratus uptime assurance safeguards – without any modifications. Recent data shows that ftServer systems experience less than one minute of downtime per year on average.

Fundamentals of uptime assurance

Stratus builds uptime assurance capabilities into every ftServer system through a set of tightly integrated technologies that work together to prevent downtime and data loss. Unlike typical servers or clusters, the ftServer hardware and Automated Uptime Layer software handle most errors transparently, shielding the operating system, middleware, and application software. Another advantage of the Stratus approach is that it constantly protects and maintains in-memory data.

Figure 2. Core Elements of the Stratus Uptime Assurance Design



24/7 on-line monitoring services: people and practices

Detects, isolates and handles faults before they cause downtime

Lockstep hardware withstands faults that would cause other servers to crash

The ftServer architecture combines resilient hardware with our Automated Uptime layer and proactive availability management to deliver the industry's highest levels of uptime.

Resilient servers

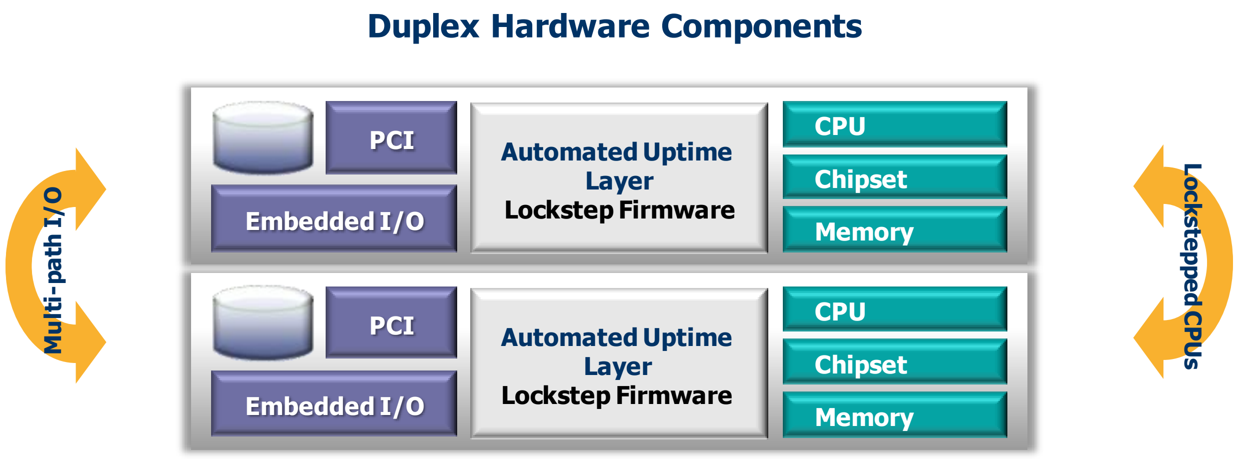
Stratus' resilient server architecture eliminates single points of failure using replicated fault-tolerant hardware components that process the same instructions at the same time. In the event of a component malfunction, the partner component acts as an active spare that continues normal operation and averts system downtime.

Lockstep technology

Using Stratus lockstep technology, ftServer systems maintain multiple CPU-memory units in precise synchronization — executing the same instructions at exactly the same clock cycle. Lockstep processing ensures that any errors, even transient errors, are detected and that the system can survive any CPU-memory unit error without interrupting processing and without losing any data or state.

Many servers offer bolt-on reliability, availability and serviceability (RAS) features that may include duplicated (N+1) power supplies, memory mirroring, and disk drives (RAID), that provide some degree of uptime assurance. These RAS features do not protect against a large portion of hardware failures, Only Stratus provides full protection for core system components that include motherboards, processors, memory, I/O buses, and I/O adapters.

Figure 3: ftServer Lockstep Technology



In the event of a component malfunction, the partner component acts as an active spare that continues normal operation and averts system downtime. The system also detects transient hardware errors that could cause software failures if left unchecked.

The fault-tolerant I/O subsystem is logically separate from the CPU-memory subsystem. Hardware logic, in the form of custom chipsets, acts as a PCI bridge between the CPU and I/O, and provides the core error detection, fault isolation, and synchronization logic for the lockstep architecture. Custom logic within the CPU/memory subsystem contains the primary PCI interfaces, interrupt control functions, and transaction ordering logic. Custom logic within the I/O subsystem contains the voting logic, secondary PCI interfaces, and error registers. The custom chipsets use a passive bus, which the ftServer systems implement in the form of a backplane, to connect the replicated CPU and I/O modules within the server.

Fault-tolerant I/O is implemented through the use of replicated PCI buses, replicated I/O adapters, and replicated devices. All critical PCI adapters are duplicated as well: SAS, Ethernet, remote management, and Fibre Channel. Internal SAS disk storage, along with expansion storage is configured as RAID, connected via two independent storage buses. Connections to external Fibre Channel hardware RAID arrays are also duplicated to ensure full fault-tolerant operation.

Multiple paths are therefore available to any logical I/O operation, including both internal and external storage operations. Any I/O operation failure will result in a retry using an alternate path that ensures successful completion of the I/O operation.

In-memory data is used extensively in many high-performance, business-critical applications; loss of this data can result in missed transactions or increased downtime. Unfortunately, cluster failover and software crashes both cause the loss of in-memory data. The ftServer system’s lockstep architecture stores memory contents in at least two separate hardware components, protecting in-memory data from hardware failures.

Dual modular redundancy (DMR)

Stratus offers ftServer systems in a standard dual modular redundancy (DMR) mode, which uses two CPU-memory assemblies (motherboards). As previously described, all motherboards run in a lockstep manner from a master/slave system clock configuration. The fault-detection and isolation logic compares I/O output from all motherboards; any miscompare indicates an error. DMR systems rely on fault-detection logic on each motherboard to determine which board is in error. If no motherboard error is signaled, a software algorithm determines which board to remove from service.

Industry-standard, modular components

The ftServer architecture leverages off-the-shelf technology in a modular physical design that optimizes price-performance, space efficiency, investment protection, and serviceability. In fact, the entire ftServer product line takes full advantage of Intel high-performance multi-core processors and technologies.

Should a component fail, the ftServer system’s hot-swappable Customer Replaceable Units (CRUs) are easily replaced without tools. And, once in place, they automatically resynchronize with their partner unit. Throughout this process, there is no disruption in application processing or loss of any data.

Common Chassis design

System components are tied into a common chassis design that includes a blindmate backplane. The backplane provides both power and signaling interconnects for CPU and I/O assemblies that slide easily in or out of the chassis. The result is that no internal cables or tools are involved in servicing the latest ftServer family.

Extensive use of status indicator LEDs and keyed components eliminate potential operator errors during service operations. And because no operator commands are required to initiate component replacement or system reconfiguration, chances for error are even further reduced.

Red Hat Linux operating environments

Stratus ftServer systems support Red Hat Enterprise Linux 5 and 6 operating systems, with additional software availability features provided by Stratus. All of these Stratus availability enhancements are implemented without affecting the Linux core operating system code. As a result, systems maintain 100% application binary interface (ABI) compatibility with Red Hat Enterprise Linux operating systems.

Stratus ftServer systems pass the same rigorous Red Hat Certification tests as other servers, offering further assurance that Linux applications will run compatibly on these systems.

Automated Uptime Layer

Leveraging more than 30 years of technology innovations, Stratus' Automated Uptime Layer creates an availability-supporting ecosystem for the ftServer family. Unique in the industry, this layer provides reliability and fault-tolerant features for motherboards, processors, memory and I/O buses and devices. It also simplifies monitoring and management of the server, and enables remote service and support.

Primary features include: a single system view that makes ftServer systems simple to install and manage; 24/7 monitoring with built-in diagnostics; alarms, alerts and uptime management features that automatically preempt downtime and data loss; hardened device drivers and change management features that add considerable reliability to the Linux environment on Stratus ftServer systems.

Figure 4: Automated Uptime Layer Features Summary

Feature	Function	Result
Single System View	• Presents and manages replicated ftServer components as a single system • Lockstep firmware	• Applications run without modification • Only a single copy of all software is required—cuts software license costs • Reduced system management costs
Comprehensive monitoring and analysis	• Purpose-built diagnostics look at more than 500 operating conditions • Captures data and 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 able to resolve ~99% of all issues remotely
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 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 server component versions match • Checks that self-test diagnostics complete successfully	• Enforces change control automatically, reducing the risk of human error

Single system view

Stratus 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.

You and your applications see a single system image, too. That means you don't have to modify your applications or license multiple copies of software. The single system view also dramatically reduces complexity, another major advantage for IT organizations struggling with budget and staffing constraints.

With conventional availability technologies like clusters, you have to configure, build, test, and maintain every node in the cluster. Clusters also require extra effort to synchronize state information between cluster nodes and between the layers of multi-tiered applications including the Web layer, middleware, and back-end database. Licensing software for each server in the cluster also drives up costs. And the IT staff has to manage more individual physical servers.

Comprehensive monitoring and analysis

The Automated Uptime Layer automatically analyzes and reports on more than 500 conditions that the ftServer system is instrumented to monitor. This comprehensive monitoring and analysis is always active, not just after an event has already caused trouble. The in-depth information provided by this Automated Uptime Layer feature enables Stratus service experts to remotely diagnose and 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 or network problems, the environment, or an operator mistake. As a result, the root cause is often not found. This means the same problem can happen again and again.

In 99% of cases, the Automated Uptime Layer's deep diagnostics automatically capture the information needed to pinpoint the root cause of problems down to the individual hardware component or software line of code. Then, Stratus support engineers work to provide a permanent fix that prevents recurrence of the issue.

Quick dump

With conventional Linux servers, users have to make an uncomfortable choice after a crash. They can keep the application down while they capture a system memory dump to be analyzed later or they can get the application back up but lose information that would help prevent a similar crash in the future.

Stratus eliminates this dilemma through "quick dump" capabilities that capitalize on the replicated hardware found in fault-tolerant ftServer systems. In the event of an operating system software failure, the system automatically reboots. The Automated Uptime Layer keeps one duplicated CPU-memory unit offline while restoring the rest of the system to normal operation. As a result, a business-critical server gets back into operation quickly without forfeiting the information required to determine the root cause of the problem.

After the system and application are back in full operation, a standard kernel memory dump is taken using the contents of the offline CPU-memory unit. When the dump is complete, the offline CPU-memory unit is brought back into normal, partnered operation. The system automatically calls the Stratus Customer Assistance Center (CAC) to report the problem and facilitate speedy root-cause analysis.

Stratus quick dump is similarly useful for obtaining a memory dump of a running system without stopping the server or any applications currently running. One of the CPU memory units is taken offline, the memory image captured to disk, then brought back online. Because the process is non-disruptive, quick dump enables convenient analysis and debugging when the system is behaving in an unusual manner.

Cumbersome shipments of dump information are avoided because ftServer systems support remote crash analysis over the Stratus ActiveService™ Network which provides a secure, continuous link to Stratus' technical experts.

Simple network management protocol (SNMP) Agent

The ftServer SNMP Agent allows third-party enterprise management consoles to remotely monitor ftServer systems. The ftServer SNMP Agent sends a notification, in the form of an SNMP trap, any time a system component changes to any of the following states: broken, fixed, removed, or inserted. An ftServer management information base (MIB) file is provided to allow the enterprise management software packages to understand Stratus alarms.

Automatic alarms and alerts

The Automated Uptime Layer evaluates and filters literally hundreds of system events, such as resource exhaustion or performance problems, 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. This allows corrective action to occur before there is a negative impact on applications.

With conventional servers, the responsibility for reacting, interpreting, and acting on alerts falls directly on the system administrator. With an ftServer system, the Automated Uptime Layer functions as an early warning system that preempts downtime without operator intervention.

Uptime Manager

No other vendor automates fault and error handling like Stratus. We've given our Uptime Manager the intelligence to perform corrective action such as taking a failed component offline. If your server needs a replacement part, the Uptime Manager initiates a request for the "correct" component — 100% of the time. Normal processing continues throughout this process.

The Uptime Manager also opens support calls over our secure global ActiveService Network, providing instant access to uptime experts no matter where in the world your ftServer system is located.

Another key advantage of the ftServer architecture is that it automatically rides through transient errors and other faults that cause conventional servers to crash, lose data, or both.

Error handling

Increasing transistor densities and lower operating voltages will continue to intensify the likelihood of transient errors. The resilient ftServer hardware and Automated Uptime Layer work together to detect, trap and handle transient hardware and software errors that a cluster node or typical server would propagate to the operating system, middleware, or application software.

In addition to the server's ability to ride through most error conditions, the Uptime Manager captures and logs information about the occurrence. If the affected component reaches a predetermined threshold, the Uptime Manager will automatically remove it from service. In that event, its partner component simply continues processing as normal.

Extended Software Protection

Stratus' automatic approach to error handling extends to the system software as well. Because software is particularly vulnerable to hardware errors, proper error handling can avert many potential software problems. In fact, with conventional servers, many problems attributed to software are actually caused by transient hardware errors.

The Automated Uptime Layer reliably distinguishes software issues from hardware issues — greatly contributing to effective and timely problem resolution. These features also assist in isolating and correcting Linux operating systems and device driver failures.

The ftServer design also incorporates reliability improvements that help prevent software-induced failures from occurring in the first place. It is worthwhile noting that conventional servers and high-availability clusters do not supply capabilities to prevent software failures. Conventional servers — even those marketed as resilient or robust — do not address prevention of software-induced failures. Clusters address this vulnerability with a restart and recovery mechanism to get software up and running again as quickly as possible.

Rapid disk resynchronization (RDR)

RDR delivers higher protection and higher availability through RAID 1+0 for mission critical applications. Without interruption to the system, the RDR utility continuously sweeps the disks for bad blocks, fixes them, and updates changes using data from the mirrored partner disk. RDR also delivers improved availability through faster remirroring of disks. If a disk or customer replaceable unit (CRU) is removed for a brief time, only the changed blocks are remirrored. Full remirroring of replacement disks is much faster when using RDR.

Fault Tolerant Server Maintenance Interface (ftsmaint)

The ftsmaint utility is a command line management utility that interfaces with the ftServer System Uptime Manager to provide a hierarchical view of the system and enable monitoring and control of system components, including the duplexed components and their states.

Hardened Drivers

Errant device drivers are acknowledged as a root cause for many Linux operating system crashes. And with the advances in Linux kernel reliability, driver problems have become an even larger issue relative to total operating-system reliability.

Stratus ftServer software alleviates this major reliability issue for Linux environments through the use of Stratus hardened driver enhancements. In the event of a problem, PCI I/O adapters are isolated from the rest of the system. Adapters are also given online diagnostic capabilities a service interface.

Stratus has either licensed the driver source code, or worked with the driver vendor to add functionality and perform further integration and fault-insertion testing for PCI adapters and drivers that are sold and supported with ftServer systems. In order to sustain maximum levels of availability, Stratus recommends that only PCI cards with hardened device drivers be used in ftServer systems. (Customers may engage Stratus Professional Services to test other PCI cards for proper operation in ftServer systems.)

The following functional enhancements harden device drivers:

- Full support for surprise removal and insertion of adapters (also known as hot removal and insertion)
- Transparent failover (except for tape)
- Ability to run online diagnostics
- Support for online firmware updates
- Monitoring and reporting through open-driver technology

Extensive testing

Stratus employs a rigorous test process that targets fully integrated systems, including all hardware and software options, in a variety of configurations including maximum configurations. Systems are tested under extreme processing and I/O loads.

Extensive transient, as well as hardware, errors are continuously simulated and injected thousands of times during testing. Automated testing procedures provide a confidence level that is difficult to achieve through manual testing. This means potential problems are identified and resolved before the system is ever installed at a customer site. Much of this error-insertion testing is exclusive to Stratus because many of the simulated errors, such as CPU or PCI bus failures, would cause conventional systems to crash.

Stratus testing uncovers errors in many different parts of the system: Stratus software, the Linux operating system, and third-party integrated products. Finding and resolving these integration and error-insertion test issues produces a higher level of software reliability for ftServer systems.

Change control agent

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 functional.

Other servers leave all of the change control to you, increasing your IT workload and the chance of human error.

Proactive availability management

An unmatched combination of proactive service capabilities enables built-in serviceability not offered by other vendors. As is true for other aspects of ftServer systems, the guiding design point of the proactive availability management is the ability to detect and resolve problems before they cause system downtime.

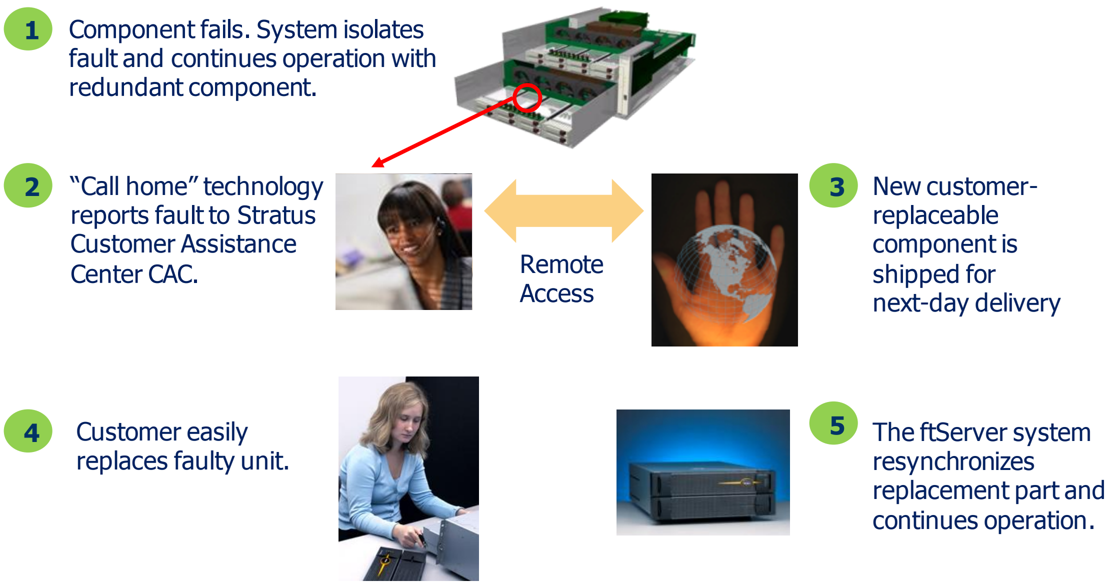
Stratus ftService support offerings ensure a level of uptime assurance that you can't get from the "break-fix" services offered by other vendors. Stratus support technicians monitor your system over our secure global ActiveService Network (ASN). Leveraging the server's fault-tolerant design features and information provided by the Automated Uptime Layer, these experts are at the ready 24/7 to remotely diagnose and remediate more complex issues.

Cost-effective ftService offerings guarantee secure access to on-demand service no matter where in the world your system is located. There are no hours of waiting for a repair technician to show up — hopefully with the right part — to get your business back online. Nearly everything a service technician can do onsite, Stratus' proactive availability management does remotely. These unique capabilities enable Stratus service engineers to troubleshoot and resolve problems online 99% of the time. All the while, your business applications and operations continue to run as normal, with no intervention from your IT team.

Built-in serviceability

Figure 5 demonstrates how Stratus' proactive availability management integrates with the technology enabled features of our resilient servers and Automated Uptime Layer software to deliver guaranteed 99.999+% uptime.

Figure 5: Problem Resolution Scenario


1
Component fails. System isolates fault and continues operation with redundant component.
2
"Call home" technology reports fault to Stratus Customer Assistance Center CAC.
Remote Access
3
New customer-replaceable component is shipped for next-day delivery
4
Customer easily replaces faulty unit.
5
The ftServer system resynchronizes replacement part and continues operation.

The ftServer systems' built-in service capabilities enable Stratus service engineers to troubleshoot and resolve problems on line 99% of the time. The system and application continue normal operations throughout the entire process.

Single source for comprehensive support

Stratus is your single source of accountability for complex inter-related platform, system software, and operating system (OS) support issues. We allow our customers to declare the severity level of incidents and we assume ownership for problem resolution throughout your system's entire life cycle. Our global crisis management system gives you priority engineering response to a telephone or web service request in as little as 15 minutes.

ActiveService Network

Like the systems it supports, Stratus' 24/7 service infrastructure was created with the express purpose of maximizing uptime for critical applications.

Every ftServer system is built to take advantage of the ActiveService Network, which provides a secure, continuous link between the servers and Stratus' technical experts and CACs worldwide. The ActiveService Network enables online, around-the-clock monitoring and remote troubleshooting of systems regardless of their location, which virtually eliminates the delays and costs associated with "truck roll" service calls.

Authorized service engineers use the ActiveService Network to access, investigate, and configure customers' ftServer systems. The network's powerful remote service management tools include: remote reset, remote console, information capture and storage, and security.

Diagnostic and analysis technologies allow the ActiveService Network to be used for determining the root cause of an event, and for uploading error logs and system dumps. Stratus service engineers can likewise use the network to install software patches, diagnostic routines, and hot fixes as needed.

Root-cause analysis prevents problem recurrence

Automated Uptime Layer reports a depth and frequency of diagnostic information that is unmatched in the industry. Hardware and software issues are captured, analyzed, and reported to Stratus. This in-depth diagnostic information gives authorized support engineers the details they need to determine the root cause of issues related to the hardware or operating environment. Engineers are also able to draw upon configuration information, including firmware revision levels and a complete incident history.

Virtual Technician Module

The ftServer system provides out-of-band management capabilities through the Virtual Technician Module (VTM). It allows for remote communication between the Stratus ActiveService Network and the customer's system, regardless of the server's state and is replicated for fault-tolerance. The VTM allows operations staff or service engineers to remotely power on/off or reset/reboot the system, and manage the security of incoming and outgoing communications through the ActiveService Network. To ensure system access, the VTM is an intelligent component that operates independently of the host computer.

The Virtual Technician Module provides many remote service capabilities including full remote keyboard, video and mouse, virtual media, and out-of-band alerts.

ActiveService Manager

Complementing the ActiveService Network is the ActiveService Manager. This Web-based service tool supports online call management for ftServer systems. Designed to provide 24/7, real-time interaction with Stratus CACs, the ActiveService Manager allows users to review call tickets that have been created automatically by the system, as well as create and update support calls that are instantly routed to the appropriate support professionals within Stratus. In addition, the ActiveService Manager displays a complete incident history of Stratus systems throughout the customer's enterprise.

Online Support Tools

The ActiveService manager gives ftService customers instant access to critical information through Stratus' comprehensive set of online support tools.

- Global incident management system: Allows you to submit, track, and resolve issues quickly and easily
- Stratus knowledgebase: Provides access to thousands of known problems and solutions based on more than 30 years of expertise in assuring uptime
- Comprehensive support library: Includes product manuals, release notes, software patches, part numbers/service designations, site planning guides, and more
- Collaborative services gateway: Features TSANet, a worldwide, multi-vendor alliance that offers an industry-wide forum for the prompt resolution of complex interrelated support issues

Mission-critical managed and professional services

Delivering mission-critical services and business processes across enterprises that span multiple networks and geographies is no easy task. Traditional managed services achieve economy of scale by standardizing operations but most fall short of providing the lifeline your organization needs.

Stratus Managed Services

Like their general-purpose counterparts, Stratus' Mission-Critical Managed Services bring operational efficiency and enable you to reduce costs. But the similarities stop there. Stratus combines certified best practices like ITIL®, COBIT®, Six Sigma®, PMI and PRINCE2™ with specialized performance management tools that include real-time dashboards and predictive analytics. The results speak for themselves. Service levels that guarantee five-nines of business process availability throughout your enterprise, year after year. To your organization, that means less than five minutes of downtime per year on average.

Stratus Professional Services

Your IT organization is pressed to do more in less time, with fewer people, and under tighter budgets. Stratus Professional Services are designed with those needs in mind. Our portfolio encompasses a range of technology-enabled services that include comprehensive development and support for end-to-end, multi-vendor environments. These capabilities allow you to supplement your IT resources with customized solutions that address your unique business requirements.

Conclusion

Stratus fault-tolerant ftServer systems deliver guaranteed service levels that exceed 99.999+%, the highest in the industry. From entry-level to mid-range to enterprise-class, resilient ftServer systems provide an effective and affordable way to achieve guaranteed uptime assurance for mission-critical, virtual, and cloud deployments running Red Hat Enterprise Linux operating environments. Every ftServer system includes Stratus lockstep technology, Automated Uptime Layer, and ActiveService Architecture — all working in concert to resolve technical issues before downtime can occur.

Every aspect of the ftServer system design is engineered to prevent downtime, not simply allow for quick recovery, as high-availability clusters and “robust” conventional servers are engineered to do. Stratus uptime assurance features operate transparently and automatically. No human intervention, additional programming, or testing is required for Linux applications to benefit from a fully fault-tolerant server environment. These automated features also minimize the risk of operator error, another contributing factor to unplanned downtime.

The latest generation of systems expands on these inherent ftServer advantages with superior price-performance, greater space efficiency, and simpler serviceability.

Outstanding operational simplicity, combined with Stratus’ remote manageability and serviceability features, makes it easy and cost-effective to deploy and manage ftServer systems. Stratus’ 24/7 service infrastructure offers comprehensive online support, Web-based event tracking, and multivendor collaborative services to ensure maximum uptime and efficient problem resolution.

A related benefit — which may be the most compelling to executives responsible for the bottom line — is that Stratus uptime assurance capabilities offer a tangible financial advantage over competing approaches by reducing costs associated with complicated deployment, unplanned downtime, and ongoing support.

Additional Resources

Stratus publishes white papers, case studies, brochures, and industry-focused collateral on the fault-tolerant ftServer family. These documents are available at in the resource library at http://www.stratus.com

Abbreviations

ABI	application binary interface
ASN	Active Service Network
CAC	(Stratus) Customer Assistance Center
CPU	central processing unit
CRU	customer replaceable unit
DMR	dual modular redundancy
I/O	input/output
MIB	management information base
PCI	Peripheral Component Interconnect
RAID	Redundant Array of Independent Disks; originally Redundant Array of Inexpensive Disks
RAS	Reliability, availability and serviceability
RDR	Rapid Disk Resynchronization
SCSI	Small Computer System Interface
SAS	Serial Attached SCSI
SNMP	Simple Network Management Protocol
TSANet	Technical Support Alliance Network
VTM	Virtual Technician Module

Specifications and descriptions are summary in nature and subject to change without notice.
Stratus, ftServer and the ftServer logo are registered trademarks; Automated Uptime, ActiveService, Active Upgrade, the Stratus Technologies logo, and the Stratus 24x7 logo are trademarks; and ftService is a service mark of Stratus Technologies Bermuda Ltd.

The registered trademark Linux is used pursuant to a sublicense from the Linux Mark Institute, the exclusive licensee of Linus Torvalds, owner of the mark on a worldwide basis. Red Hat, the Red Hat Shadowman logo and Enterprise Linux are registered trademarks of Red Hat, Inc. in the United States and other countries. Intel is registered trademark of the Intel Corporation in the United States and other countries.

X934-D